Quest

Quest® Change Auditor 7.4
Technical Insight Guide

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

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

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

Legend

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

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

Change Auditor Technical Insight Guide
Updated - November 2023
Software Version - 7.4

Contents

1

Change Auditor Services

This guide is intended for IT specialists who are involved in Change Auditor deployment, configuration, and maintenance. It provides a technical insight into the product components, operations, and processes.

The tables in this section provide a brief description of each of the Change Auditor services and their functions:

- Quest Change Auditor Coordinator
- Quest Change Auditor Workstation Agent
- Quest Change Auditor Agent
- Change Auditor for EMC

Quest Change Auditor Coordinator

Table 1. Quest Change Auditor coordinator service

Service Name	Quest.ChangeAuditor.Coordinator
Display Name	Quest Change Auditor Coordinator
Description	Coordinates various stages of Change Auditor process.
Default Path	%ProgramFiles%\Quest\ChangeAuditor\Service\ChangeAuditor.Service.exe
Startup Type	Automatic
Exe Name	ChangeAuditor.Service.exe

Quest Change Auditor Workstation Agent

Table 2. Quest Change Auditor Workstation Agent

Service Name	NPSrvHost
Display Name	Quest Change Auditor Agent
Description	Quest Change Auditor Agent
Default Path	%ProgramFiles%\Quest\ChangeAuditor\Agent\NPSrvHost.exe
Startup Type	Automatic
Exe Name	NPSrvHost.exe
Other Modules	The following Change Auditor modules are part of the core Quest Change Auditor Workstation Agent service: • Change Auditor for Logon Activity

Quest Change Auditor Agent

Table 3. Quest Change Auditor agent service

Service Name	NPSrvHost
Display Name	Quest Change Auditor Agent
Description	Quest Change Auditor Agent
Default Path	%ProgramFiles%\Quest\ChangeAuditor\Agent\NPSrvHost.exe
Startup Type	Automatic
Exe Name	NPSrvHost.exe
Other Modules	The following Change Auditor modules are part of the core Quest Change Auditor Agent service: • Change Auditor for Active Directory • Change Auditor for Active Directory Queries (formerly ChangeAuditor for LDAP) • Change Auditor for Defender • Change Auditor for Exchange • Change Auditor for NetApp • Change Auditor for Authentication Services • Change Auditor for SQL Server • Change Auditor for Windows File Servers • Change Auditor for Skype for Business • Change Auditor for Logon Activity The following Change Auditor modules are started as processes and appear in Task Manager: • Change Auditor for SharePoint (SharePointPluginCA.exe)

Change Auditor for EMC

Table 4. Quest Change Auditor for EMC service

Service Name	QCeeService
Display Name	Quest Shared EMC Connector
Description	This shared component enables auditing of EMC devices by Quest products.
Default Path	%ProgramFiles%\Common Files\Quest\QCEE\QCeeService.exe
Startup Type	Automatic
Exe Name	QCeeService.exe

2

Change Auditor licensing processes

This section describes the licensing processes used within Change Auditor:

- License check process
- Component licensing
- User counts

License check process

The Change Auditor coordinator service performs a valid license check once every 5 minutes, or during service startup. The coordinator determines if:

- A valid license is installed.
- The license has an expiration date and if the current date exceeds the expiration date.
- The total user count allowed under the given license.

If a license has expired, the coordinator service notifies the Change Auditor agent service, and the agent stops collecting events for that component.

For example, If the Exchange license has expired, the Change Auditor agent service will no longer collect Exchange events. After all licenses have expired and the coordinator has no valid licenses installed, the coordinator service schedules itself to shut down 5 minutes from the time this is detected.

Component licensing

The first time an agent connects to any coordinator and retrieves the first configuration update, it sends a component license update request to the coordinator. After that, the agent requests a component license update every 24 hours from the connected coordinator. If the agent is not connected to a coordinator at the 24-hour mark, no component license update happens and the agent tries again 24 hours later.

User counts

The coordinator determines *maximum licensed users* by comparing the value associated with the component license to the total count of users in each domain. The coordinator does this by issuing LDAP queries to Active Directory using specific filters for a precise count.

Generic User Count Query (for Active Directory, File System, SQL Server, EMC, NetApp, SharePoint, Skype for Business, Logon Activity User licensing):

(&(objectCategory=Person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=512)(!userAccountControl:1.2.840.113556.1.4.803:=2))

Mail Enabled User Count Query (for Exchange licensing including Office 365 Exchange Online):

(&(samAccountType=805306368)(|(&(!userAccountControl:1.2.840.113556.1.4.803:=2)(msExchHomeServerName=*))(&(userAccountControl:1.2.840.113556.1.4.803:=2)(msExchMasterAccountSid=*))))

Workstation Installation Count (for Logon Activity licensing):

Workstation counts are based on the actual number of workstations harvested in the topology.

3

Component Start-up Considerations

This section describes installation notes and best practices:

- Start up delays

Start up delays

When set to ‘false’ the GeneratePublisherEvidence setting is used to bypass digital signature verification for programs on start-up which allows for faster start up time. This is set to false by default for the following components in Change Auditor: Coordinator, Windows client, Coordinator Configuration and Coordinator Status in the system tray.

If required, you can change this setting to 'true' to allow digital signatures to be verified, by modifying the following files:

Component	File
Coordinator	Program Files\Quest\ChangeAuditor\Service\ChangeAuditor.Service.exe.config
Windows Client	Program Files\Quest\ChangeAuditor\Client\ChangeAuditor.exe.config
Coordinator Configuration	Program Files\Quest\ChangeAuditor\Service\ConfigureDatabase.exe.config
Coordinator Status	Program Files\Quest\ChangeAuditor\Service\CoordinatorTray.exe.config

Modify the configuration file as follows to change the setting to ‘true’:

```
<configuration>
    <runtime>
        <generatePublisherEvidence enabled="true"/>
    </runtime>
</configuration>
```

4

Change Auditor network communications

This section explains the network communications used by Change Auditor including a description of how it uses Service Connection Points (SCPs) to locate the coordinator, the listening ports used for communication between the Change Auditor services, and the network encryption used to secure sensitive information.

- Service Connection Points
- Ports and protocols
- Network encryption

Service Connection Points

Change Auditor publishes SCPs in Active Directory so that clients, agents, and other third-party applications can automatically locate the coordinator. When clients or agents start up, they search Active Directory for the SCP objects to retrieve connection information for the coordinator such as host name, listening port, and other authentication information.

The SCP objects are published directly subordinate to the coordinator's computer object in Active Directory. SCP objects can be viewed and updated using Microsoft ***ADSI Edit*** MMC snap-in.

The coordinator installs and maintains two separate SCPs. The coordinator checks and updates these Active Directory objects each time the coordinator service starts up.

- CN=ChangeAuditor.Coordinator
- Ports and protocols

CN=ChangeAuditor.Coordinator

- Used by Change Auditor clients, Change Auditor agents and SDK users
- Used to publish the coordinator's FQDN, port, and installation name

The coordinator SCP contains the following key elements, which are stored in its Active Directory attributes:

Table 5. Quest.ChangeAuditor.Coordinator SCP

Attribute	Attribute Syntax	Function	Default Value
CN	String	SCP Name	CN=ChangeAuditor.Coordinator
keywords	Multi-Value	Storage for the product GUID to facilitate location of only Change Auditor SCPs	F0E51C1A-4424-4387-B7DA-3A245CCEF0 ChangeAuditor.Coordinator

Table 5. Quest.ChangeAuditor.Coordinator SCP

Attribute	Attribute Syntax	Function	Default Value
serviceBindinginformation	Multi-Value	Contains Client Port, Public SDK Port, Agent WCF Port, coordinator Version and the InstallationName	<XML>
serviceClassName	String	Used to store the service class for authentication	NPRepository4
serviceDNSName	String	FQDN of the computer running the coordinator service	<Server FQDN>
serviceDNSNameType	String	The DNS record type of the host listed in the serviceDNSName	A

Ports and protocols

Change Auditor uses the following incoming communications ports (listening ports) to establish communication:

Table 6. Change Auditor incoming communication ports

Change Auditor client	None
Change Auditor agents	None
Change Auditor coordinators	The coordinator uses the following listening ports that can be dynamically or statically assigned. • Client Port • Public SDK Port • Agent WCF Port **NOTE:** By default, the incoming ports are dynamically assigned by Windows. However, you can use the Coordinator Configuration Tool to specify static ports for each of these listening ports. To access the Coordinator Configuration Tool, right-click the coordinator system tray icon and select **Coordinator Configuration.**

The following table describes each segment of communication that occurs in the Change Auditor system along with technical details of each type of communication.

Table 7. Change Auditor communication segments

From/To	Description	Originating Port	Protocol	Destination Port
Client to Coordinator Service	WCF (Windows Communication Foundation)	Dynamic	TCP	Dynamic
Client to Agents (server and workstation agents)	WCF (Windows Communication Foundation) for configuration refresh If WCF configuration refresh call fails, falls back to WMI (DCOM) and port 135.	Dynamic	TCP	Dynamic
Client to Agents (server and workstation agents)	SCM (ServiceControlManager) for Agent Service Start\Stop	Dynamic	TCP	135
Coordinator to Server Agents	WCF for Azure/Office 365 configuration information			8373
Client to SQL Server Database	Connection for archive databases only	Dynamic	TCP	1433
Agent to Coordinator Service	WCF (Windows Communication Foundation)	Dynamic	TCP	Dynamic
Agent to SharePoint SQL Server database	OLEDB SQL Client	Dynamic	TCP	1433
SDK User\Service to Coordinator Service	WCF (Windows Communication Foundation)	Dynamic	TCP	Dynamic
Coordinator to SQL Server Database	.NET SQL	Dynamic	TCP	1433
Coordinator to Azure SQL Managed Instance Database (Private endpoint)	.NET SQL	Dynamic	TCP	1433

Table 7. Change Auditor communication segments

From/To	Description	Originating Port	Protocol	Destination Port
Coordinator to Azure SQL Managed Instance Database (Public endpoint)	.NET SQL	Dynamic	TCP	3342
Coordinator to Agents (server and workstation agents)	SMB File Share for Agent Deployment	Dynamic	TCP	445
Coordinator to Agents (server and workstation agents)	Remote Registry for Agent Deployment (RPC)	Dynamic	TCP	135
*Coordinator to Active Directory LDAP	.NET Directory Services	Dynamic	TCP	389
*Coordinator to Active Directory	Kerberos authenticated connections	Dynamic	TCP	88
*Coordinator to Active Directory GC (Global Catalog)	.NET Directory Services	Dynamic	TCP	3268
Coordinator to DNS Server	DNS name resolution for .NET Directory Services	Dynamic	TCP	53
Web Client to Coordinator	WCF (Windows Communication Foundation)	Dynamic	TCP	Dynamic
Internet Browser (for example, Chrome™ and Internet Explorer) to web client	HTTP/HTTPS	Dynamic	TCP	80/443

*The coordinator requires connectivity to domain controllers in the domain that the server is a member of and also the forest root domain.

Network encryption

Change Auditor uses the following different types of network encryption to protect sensitive information.

- SMB protocol and share encryption
- Secure password storage
- Client to coordinator connection
- Agent to coordinator connection (version 6.x and 7.0.1)
- Coordinator to SQL Server connection

SMB protocol and share encryption

Change Auditor uses the SMB protocol for file transfer for agent deployment and when the 'Get All Logs' feature is used. In these cases, the SMB protocol version configured on the agent computer is used. To ensure the SMB traffic is encrypted:

- For agent deployments, ensure that SMB3 is enabled on the agent computer or specify a custom file share which is configured to encrypt data access to use instead of the $ADMIN share. This can be configured in the Change Auditor client under the “Advanced Deployment” section.
- For the 'Get All Logs' feature, there is no workaround available. To encrypt the connection, users must ensure that SMB3 is enabled on the agent computer.

Secure password storage

Certain aspects of Change Auditor auditing require storing passwords and other confidential data. Examples of such data include access credentials to NetApp, EMC, SharePoint, Office 365, Skype for Business, and SQL DLA. To safeguard this data, Change Auditor uses RSA encryption.

NOTE: The password storage is FIPS-compliant from version 7.0.2, using only Microsoft-certified APIs compliant with FIPS 140-2 and it's annexes. Change Auditor is compatible with the "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" group policy enabled.

NOTE: If FIPS compliance is required, Change Auditor coordinators, agents and clients must all be version 7.0.2 or greater.

On startup, the agent generates a private/public key pair and stores the public key in the database. When the agent is configured to audit another network device using the supplied credentials, these credentials are encrypted using the agent's public key. This way, it is impossible for anyone but the agent itself to decrypt them.

The coordinators also store public keys in the database which are used to decrypt SMTP passwords to send alerts.

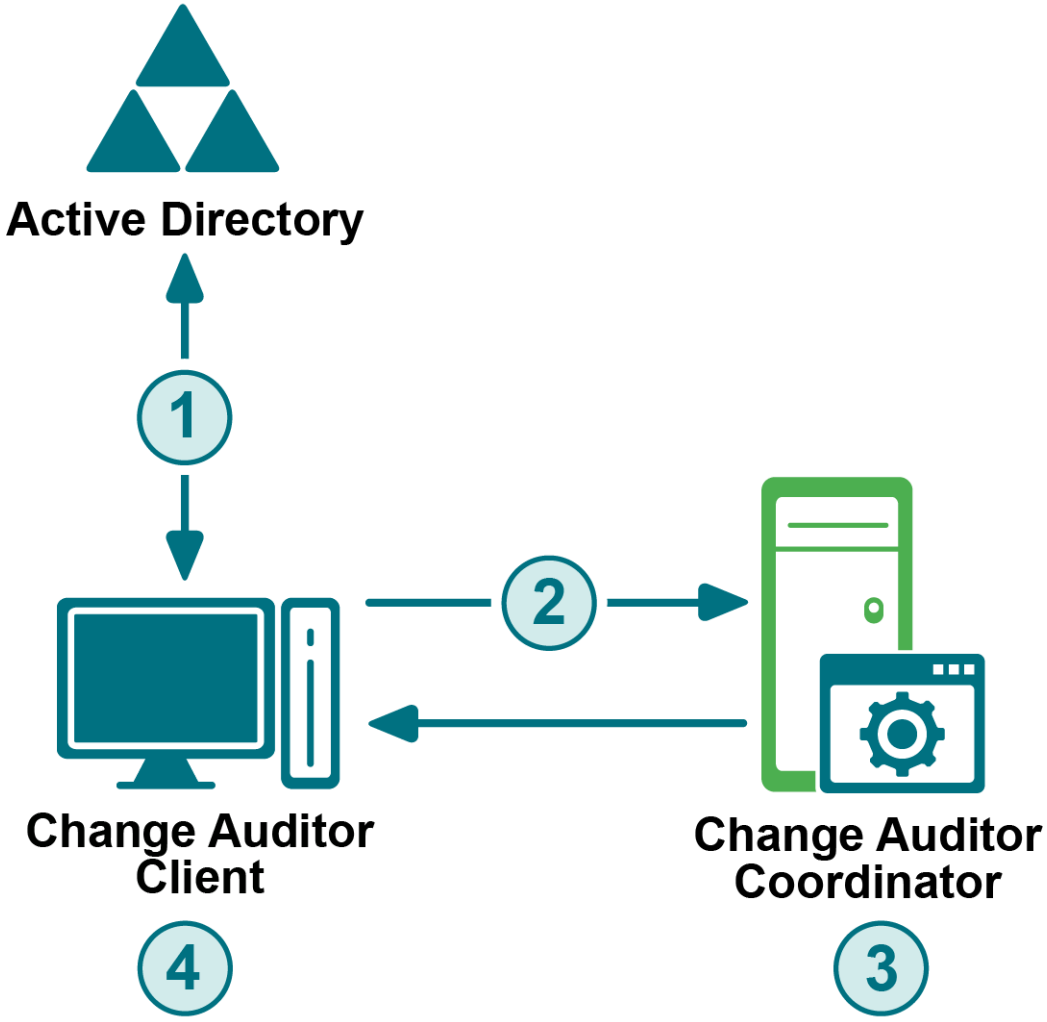
1. For user authentication and local password storage of user identities, Change Auditor uses **CryptProtectData** from http://msdn.microsoft.com/en-us/library/aa380261.aspx.

   Change Auditor uses **CryptProtectData** with a key length that is variable-dependent upon input phrase. This encryption is symmetric. This encryption is automatically enabled. This encryption cannot be used outside of Change Auditor.

2. For user authentication and database password database storage, Change Auditor uses the "Microsoft Enhanced Cryptographic Provider v1.0" (CNG or Crypto Next Generation) provider with provider type of PROV_RSA_FULL. Secrets are symmetrically encrypted with AES using a 256-bit key, and the AES key is then encrypted with RSA using a 4096-bit key before being stored with the encrypted secret.

   When upgrading the Change Auditor coordinator to version 7.0.2 or above from version 7.0.1 or less, passwords and other data protected by coordinator public keys are updated to the new, stronger encryption scheme during database upgrade at the first startup after upgrade. Passwords and other data protected by agent public keys are updated to the new encryption scheme for all connected agent versions when they connect to the upgraded coordinator. Any additional older coordinators will need to be updated to the version of the first coordinator before they will connect to the updated database.

Client to coordinator connection



1 When the client is started, it searches Active Directory for the Service Connection Point (SCP) objects to retrieve connection information for the coordinator such as host name, listening port, and other authentication information.

2 The client connects to the coordinator using Windows Communication Foundation (WCF) using Kerberos authenticated connections.Ports are dynamically assigned, but can be statically set.

3 The coordinator encrypts protected data using Microsoft RSACryptoServiceProvider (PROV_RSA_FULL) APIs.

4 The client decrypts the protected data using Microsoft RSACryptoServiceProvider (PROV_RSA_FULL) APIs.

Agent to coordinator connection (version 6.x and 7.0.1)

Change Auditor 6.x (and above) agents also search Active Directory for the SCP for connection information to the coordinator; however, they now connect to the coordinator using WCF as described here.

1. The Change Auditor 6.x (and above) agent connects to a coordinator using WCF using Kerberos authenticated connections. Ports are dynamically assigned, but can be statically set.
2. The coordinator encrypts protected data using Microsoft RSACryptoServiceProvider (PROV_RSA_FULL) APIs.
3. The agent decrypts the protected data using Microsoft RSACryptoServiceProvider (PROV_RSA_FULL) APIs.

Agent to coordinator connection (version 7.0.2)

Change Auditor 7.0.2 agents connect in the same way as 6.x agents, however encryption and decryption for database storage and communications are upgraded to meet the requirements of FIPS 140-2 and its annexes.

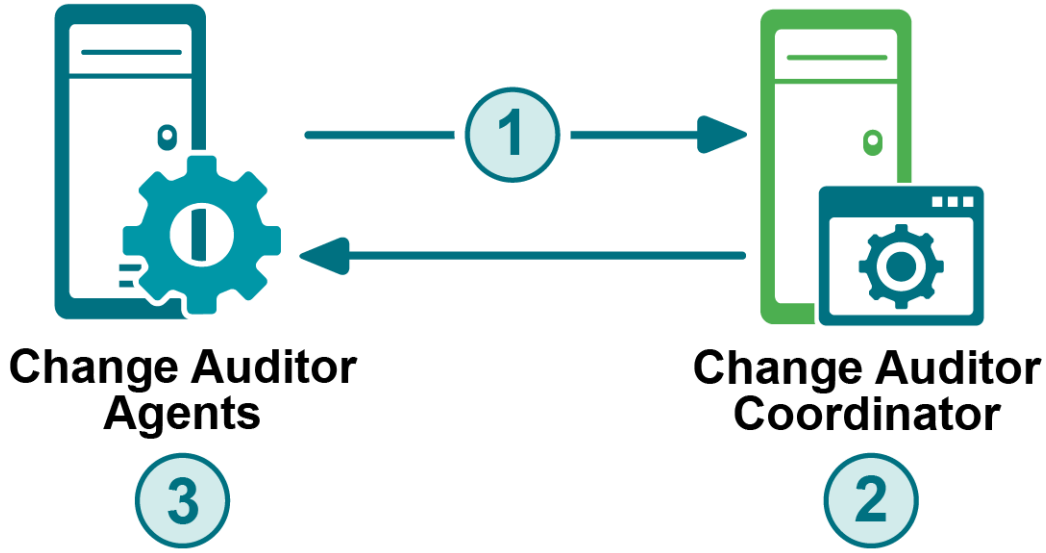
1. The Change Auditor 7.0.2 agent connects to a coordinator using WCF with Windows authentication and TCP transport security, which negotiates Kerberos for both authentication and encryption. Only Kerberos encryption algorithms allowed by the “Network security: Configure encryption types allowed for Kerberos” group policy.
2. The coordinator encrypts and decrypts protected data in database storage using the “Microsoft Enhanced Cryptographic Provider v1.0” (CNG or Crypto Next Generation) provider with a provider type of PROV_RSA_FULL and the new storage scheme described under Secure password storage.
3. The agent decrypts protected data in configuration data from the coordinator using the “Microsoft Enhanced Cryptographic Provider v1.0” (CNG or Crypto Next Generation) provider with a provider type of PROV_RSA_FULL.
4. Security for data sent from the coordinator to the agent and from agent to coordinator is provided by WCF TCP transport security using the “Microsoft Enhanced Cryptographic Provider v1.0”.
5. The Change Auditor 7.0.2 agent cannot connect to a coordinator version 7.0.1 or earlier.

Coordinator to SQL Server connection

1. Coordinators read the encrypted database connection string from the ChangeAuditor.Service.exe.config file which includes the SQL Server name \ Instance, User name, Password, and Domain if Windows authentication is selected.

   This can be configured using the Security page on the Coordinator Configuration Tool, which is accessed by right-clicking the coordinator system tray icon and selecting **Coordinator Configuration**.
2. By default, connections to the 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.



5

Coordinator internal tasks

The following table lists the internal scheduled tasks that the coordinator performs, including when the task initially starts and how often the task is repeated. This section also provides a description of each of these tasks, and if configurable the page of the client used to configure it.

Table 8. Coordinator internal tasks

Task name	Initial Start Time	Default Run Frequency	Configurable
Forest topology collection	30 seconds after startup	Every 3 hours	No
Group expansion	3 hours after startup	Every 6 hours	Yes
Alert processing – Send SMTP	30 seconds after startup	Every 60 seconds	No
Alert processing – Send SNMP	45 seconds after startup	Every 30 seconds	No
Alert processing – Send WMI	30 seconds after startup	Every 30 seconds	No
License check	30 seconds after startup	Every 5 minutes	No
Remote deployment	1 minute after startup	Every 5 minutes	No
Agent heartbeat check	10 minutes after startup	Every 5 minute	No
Refresh coordinator statistics	At startup	Every 15 seconds	No
Event aggregator	10 seconds after startup	Every 10 seconds	No
SQL upgrade monitor	15 seconds after startup	Every 15 seconds	No
Open handle	300 seconds after startup	Every 300 seconds	No
Scheduled purge job	60 seconds after startup	Every 5 minutes	No
Scheduled archive job	60 seconds after startup	Every 5 minutes	No
Scheduled report job	60 seconds after startup	Every 5 minutes	No

Forest topology collection

Change Auditor maintains a view of Active Directory in the database. Each event that Change Auditor captures is linked with a forest, domain, or server (or workgroup server) found in the topology collection. When the coordinator service starts, the topology collection begins. The following Active Directory objects are collected and stored:

- **Domain Objects** (crossref objects) found in *CN=Partitions,CN=Configuration,<Forest Root Distinguished Name>*
- **Site Objects** (site objects) found in *CN=Sites,CN=Configuration,<Forest Root Distinguished Name>*
- **Exchange Servers** (msExchExchangeServer objects) found in *CN=Microsoft Exchange,CN=Services,CN=Configuration, <Forest Root Distinguished Name>*
- **Server Objects** (computer objects) – For each domain found, Change Auditor searches the domain for the following types of server objects:
  - **Exchange servers** found in the following groups:
    - Exchange Install Domain Servers
    - Exchange Servers

- **All computer objects** found using the following filter:
  - (&(objectCategory=computer)(|(operatingSystem=*Windows*))

NOTE: If the operatingSystem field contains ‘server’, the computer is a server object. If the operatingSystem field does not contain ‘server’, the computer is a workstation object.

Group expansion

The group expansion scheduled task is for expanding nested membership of Active Directory groups that are referenced in searches (Who search criteria) or groups that are defined in the Member of Group feature. Group membership is recursively enumerated in order to determine nested group membership.

The refresh frequency can be configured using the Group Membership Expansion pane on the Coordinator Configuration page (Administration Tasks tab) of the client.

Alert processing

Change Auditor reports that have been alert enabled are run on a scheduled basis determined by the user selected alert priority. After all the reports have been processed for alerting, Change Auditor alert transport tasks (SMTP, SNMP and WMI) send the alerts.

To set the priority for an alert, use the Alert tab (one of the Search Properties tab) on the Searches page of the client.

License check

The coordinator service performs a valid license check once every 5 minutes, or during service startup. For more information on the license check process, see Change Auditor licensing processes.

Remote deployment

The coordinator remote deployment task periodically checks if there has been a user scheduled agent deployment or an automatic deployment. When agent installations, upgrades or uninstalls are required the remote deployment task remotely runs the job on the selected servers and workstations.

Automatic deployments for new domain objects are configured using the **New Servers** tool bar button on the Deployment page in the client.

Foreign Agent Credentials

When you select one or more deployed foreign agents from the Deployment tab, you can select to update the information the agent uses to connect to the coordinator. When initiated, the remote deployment task remotely runs the job on the selected servers and workstations. The agent service is restarted to complete the update. See the Change Auditor Installation Guide for more information on foreign forest agent deployment and credential updates.

Agent heartbeat check

By default, the coordinator service marks an agent as ‘inactive’ when it has not received any updates from the Change Auditor agent for 30 minutes.

This interval can be changed from the Agent Heartbeat pane on the Coordinator Configuration page (Administration Tasks tab) of the client.

Refresh coordinator statistics

The coordinator status dialog that appears as part of the coordinator system tray application contains counts of events and alerts. These statistics are periodically recalculated by the coordinator to keep the information as up-to-date as possible.

Event aggregator

The event aggreator scheduled task handles the collecting of all incoming agent events. The coordinator receives agent events (batched from the agent) and stores them in temporary storage for bulk uploading to the database. If the bulk uploading has issues (timeouts, etc.), then those events are stored in transaction logs for future uploading. The coordinator can also report to agents that it is too busy (rejects events), which defers the agents from uploading events or allows the agent to send the events to a different coordinator.

SQL upgrade monitor

The SQL upgrade monitor scheduled task checks to see if any other coordinator is in the process of trying to upgrade. If it finds a different coordinator that is trying to upgrade, it shuts down the coordinator.

Open handle

The open handle scheduled task logs the handle and thread counts to the debug log. It also logs information about the working set memory, watching for memory leaks.

Scheduled purge job

The scheduled purge job task checks every five minutes to determine if it needs to run a job. Using the Purge Jobs task on the Administration Tasks page, you can create and schedule purge jobs to delete events older than a specific calendar interval.

When the purge job runs, by default it purges a maximum of 500,000 events in that five minute period. If there are more than 500,000 events to be purged, then five minutes later another 500,000 events are purged until all of the events are purged.If there are 500,000 events or less in a purge job, then the purge job task checks again in the next five minutes and obeys the ‘next run’ time.

You cannot change the scheduled purge job task cycle; however, you can modify the **Batch Limit** setting on the Purge Job wizard to specify the maximum number of events to be purged each purge cycle.

NOTE: If SQL is slow or disk space is low, decrease this limit to 100000 or 50000. When this limit is decreased, the purge job will take longer to complete.

Scheduled archive job

Using the archive options, you can select to create a yearly archive database for older events that are no longer required to be represented in your reports.

When scheduling an archive job for the first time it may take a long time to complete (depending on how many years of data you are asking to be archived). Batch limit does not apply to an archive type job.

When running an archive job, you need to pay attention to disk space growth on the SQL server.

CAUTION: Carefully review your current jobs before creating a new job or altering an existing job, as it is possible to create purge and archive conflicts.

NOTE: If you have specific purge jobs that you want to complete before a scheduled archive, ensure that you leave enough time between the purge only jobs and the archive job.

Before scheduling a job, ensure that you have reviewed the best practice information in the Change Auditor User Guide - Purging and Archiving your Change Auditor Database: Planning your jobs section.

Scheduled report job

The scheduled report job task checks every five minutes to determine if reporting is enabled and needs to email a search query report. The scheduled reporting feature uses the same SMTP configuration defined for alerting to distribute search query reports via email. Using the Report tab (Search Properties tabs) for a search, you can enable reporting and schedule the distribution of the report. When the scheduled report job task determines a report is to be sent, the report is sent as an attachment via email to the designated recipients. The default is to zip the attachment when the report is 1 MB or greater.

6

Registry Settings

This section provides information about the different registry settings that can be used to control Change Auditor.

Force agent WCF port

Use the following registry setting to force the coordinator to use a specific port to listen for Change Auditor agent connections.

Table 9. Registry setting: Force agent WCF port

Location	Registry
Path	HKEY_LOCAL_MACHINE\SOFTWARE\Quest\ChangeAuditor\Coordinator
Value Name	Agent Wcf Port
Value Type	DWORD
Value	Port number

Force client port

Use the following registry setting to force the coordinator to use a specific port to listen for client connections.

Table 10. Registry setting: Force client port

Location	Registry
Path	HKEY_LOCAL_MACHINE\SOFTWARE\Quest\ChangeAuditor\Coordinator
Value Name	Client Port
Value Type	DWORD
Value	Port number

Force SDK port

Use the following registry setting to force the coordinator to use a specific port to listen for other integrated applications using the SDK.

Table 11. Registry setting: Force SDK port

Location	Registry
Path	HKEY_LOCAL_MACHINE\SOFTWARE\Quest\ChangeAuditor\Coordinator
Value Name	Public Port
Value Type	DWORD
Value	Port number

Use predefined GC for name resolution

Use the following registry setting to specify the Global Catalog to be used by the coordinator for lookup functions including topology, name resolution, group expansion, etc.

Table 12. Registry setting: Use predefined GC for name resolution

Location	Registry
Path	HKEY_LOCAL_MACHINE\SOFTWARE\Quest\ChangeAuditor\Coordinator
Value Name	NameResolutionGC
Value Type	String
Value	FQDN of the Global Catalog server

Allow collation switch

Use the following registry setting to allow an upgrade to proceed even if it detects a different collation between the two databases. When this is set to 0 (default), you will receive an error indicating that the server collation is different and the upgrade process will stop.

Table 13. Registry setting: Allow collation switch

Location	Registry
Path	HKEY_LOCAL_MACHINE\SOFTWARE\Quest\ChangeAuditor\Coordinator
Value Name	AllowCollationSwitch
Value Type	DWORD
Default	0 - Upon coordinator start, do not allow the detection of a collation switch to proceed.
Value	0 - Upon coordinator start, do not allow the detection of a collation switch to proceed. 1 - Upon coordinator start, allow the detection of a collation switch to proceed.

Report zip limit

Use the following registry setting to specify the maximum number of bytes that can be included in a report zip file.

Table 14. Registry setting: Report zip limit

Location	Registry
Path	HKEY_LOCAL_MACHINE\SOFTWARE\Quest\ChangeAuditor\Coordinator
Value Name	Report Zip Limit
Value Type	DWORD
Default	1024
Value	Report zip limit in bytes

SQL command timeout

Use the following registry setting to specify the maximum amount of time (in seconds) to allocate for executing a SQL command.

Table 15. Registry setting: SQL command timeout

Location	Registry
Path	HKEY_LOCAL_MACHINE\SOFTWARE\Quest\ChangeAuditor
Value Name	SQLTimeout
Value Type	DWORD
Default	30 seconds
Value	Maximum time in seconds for SQL command to run.
Note	This value is overridden by some SQL commands, which are known to be long-running.

Enable ChangeAuditor Agent service to start with the Microsoft security update (KB2264107)

In 2010, Microsoft introduced a security update (KB2264107) to disallow the loading of 'unsafe' DLLs. The update sets the CWDIllegalInDllSearch registry entry to 0xFFFFFFFF under KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager.

This computer-wide setting will not allow the Change Auditor agent service (NPSrvHost.exe) to start.

To keep the strict system-wide setting, but still allow the Change Auditor agent to start:

1. Log on as an administrator on the computer hosting the agent.
2. Open the Registry Editor.
3. In the following registry key create a new key named NPSrvHost.exe:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options.
4. Right-click the newly created key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\NPSrvHost.exe.
5. Select New | DWORD (32-bit) Value and type CWDIllegalInDllSearch.
6. Set the value of CWDIllegalInDllSearch to 1.

Table 16. Registry setting: CWDIllegalInDllSearch

Location	Registry
Path	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Value Name	CWDIllegalInDllSearch
Value Type	DWORD
Default	Not present. Change Auditor Agent service will fail to start if the computer-wide setting is present.
Value	1 – Overrides the computer-wide setting for Change Auditor Agent service, it will be allowed to start.

Adjust memory dumps settings

Change Auditor overwrites the settings in [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps\lsass.exe] causing them to be ignored.

Use the following registry setting to adjust memory dumps settings on a domain controller.

Table 17. Registry setting: Memory Dump Type

Location	Registry
Path	HKEY_LOCAL_MACHINE\SOFTWARE\Quest\ChangeAuditor for Active Directory
Value Name	• MemoryDumpType • CircularDumpCount
Value Type	DWORD

Table 17. Registry setting: Memory Dump Type

Default	Default value 2
Value	MemoryDumpType can contain values 1, 2, or any bitmask value outlined here: https://msdn.microsoft.com/en-us/library/windows/desktop/ms680519(v=vs.85).aspx

7

Change Auditor built-in fault tolerance

Fault tolerance and high availability is inherently built in to Change Auditor and no additional configuration is required.

Each component in the Change Auditor architecture is designed with high availability (fault tolerance and failover) as a goal. There will always be only one SQL database and this database is typically hosted on a Microsoft SQL Server cluster.

More than one management service (coordinator) can be installed and they automatically work together and become redundant. No additional configuration is required. An agent can connect to multiple coordinators to process events and prepare them for Change Auditor agents (version 6.x or later) which prefer available coordinators within the same site, but if none are found, all available coordinators within the same installation are considered. If one or more (depending on agent type) non-site coordinators are connected, and one or more coordinators are later discovered within the agent site, the agents connect to the site-located coordinators and drop non-site coordinator connections. If this behavior is problematic for your environment, contact Quest Technical Support to discuss possible configuration options.or insertion into the SQL database. The need for multiple coordinators depend on the event volume, number of agents, and the hardware specifications of the coordinator. If one of these servers suffers a catastrophic failure, the other continues.

Also, the auditing agent has the inherent ability to cope with service or network outages. If for any reason an agent is unable to communicate with the other components, that agent continues auditing normally and stores audit data locally until communications are restored. This outage can exist for an extended period without issue. After communications resume, the agent begins forwarding its queued events in a controlled fashion.

If a coordinator is unavailable, agents stop forwarding events. This is by design. For redundancy, or if a coordinator is not able to handle the event load, two or more coordinators can be installed. Server agents submit events to all available coordinators and load balancing occurs automatically. However, workstation agents randomly connect to a single coordinator and submit events to that coordinator.

NOTE: Change Auditor agents (version 6.x or later) prefer available coordinators within the same site, but if none are found, all available coordinators within the same installation are considered. If one or more (depending on agent type) non-site coordinators are connected, and one or more coordinators are later discovered within the agent site, the agents connect to the site-located coordinators and drop non-site coordinator connections. If this behavior is problematic for your environment, contact Quest Technical Support to discuss possible configuration options.

8

Change Auditor protection

Using multiple protection templates

This section explains how access permissions are evaluated when multiple protection templates are assigned to an object which may contain conflicting rules. The evaluation process used is for all types of protection templates (Active Directory, ADAM (AD LDS), Group Policy, File System, and Exchange Mailbox). However, there are some special considerations to keep in mind when using the Exchange Mailbox Protection feature, see How access rules are evaluated.

Protection templates can be one of two types:

- Classic (allow) templates which deny access by default, allowing access to the protected object by the override accounts explicitly specified in the protection template.
- Reverse (deny) templates which allow access by default, denying access to the protected object by the override accounts explicitly specified in the protection template.

How access rules are evaluated

When a user attempts to access a protected object, each template is evaluated separately, and the 'deny' access rule takes precedence over any 'allow' access rule. This means, that if at least one protection template evaluates to 'deny', attempts to access the protected object is denied. The following table illustrates the overall results of conflicting access rules:

Table 18. How access rules are evaluated

Based on Settings in Template 1:	Based on Settings in Template 2:	Overall Result
User is allowed access	User is allowed access	User is allowed to access protected objects
User is allowed access	User is denied access	User is denied access to protected objects
User is denied access	User is allowed access	User is denied access to protected objects
User is denied access	User is denied access	User is denied access to protected objects

For Exchange Mailbox Protection templates, you can set the **Mailbox owner can bypass protection** option to allow the object's owner to access their own mailbox, even if the protection template would normally deny access.

This override flag only affects the evaluation on a template where it is defined. It does not affect the evaluation of other protection templates.

IMPORTANT: Care should be taken when defining multiple Exchange Mailbox Protection templates. For example, even though you cannot create a duplicate Exchange Mailbox protection template for the same object name, you could be including the same mailbox in multiple templates. That is, if you define templates for the Enterprise object, the top-level domain object, an OU container and several groups, this same mailbox could be a child or member of all these objects. The access to this mailbox is evaluated for each of the templates to which it belongs.

NOTE: Exchange Mailbox protection is designed to provide protection coverage for a few high-value mailboxes. After monitoring has been enabled or changed, it may take several minutes to complete the configuration process necessary to enable the protection feature on the agent. Protecting a large number of mailboxes slows down the configuration process.

NOTE: To control memory utilization, each Exchange Mailbox Protection template can have up to 20 users selected as ‘override accounts’ that can bypass the protection feature. This number applies to both allowed and denied user accounts and includes members of groups in the list.

How scheduling and location works with denied access

You can select to have the protection to always run or have it run only during specific times and control when the protection is enabled based on the location.

This section explains how the scheduling and location options affect the user and group accounts that have been denied access to protected objects.

Scheduling option

If you have denied specific users or groups the ability to change the protected objects and you have enabled a protection schedule, those users or groups are denied access only during this time. Anytime outside of when the schedule is set to enabled, these denied accounts will be able to access the protected object.

When the schedule is turned off, all options are turned off with it, including any denied access to the specified users.

The scheduling options override all other protection settings.

Location option

If you have denied specific users or groups access to protected objects, but you have specified locations that can access the protected object, the denied user or group can access the protected objects from these locations.

The location options override all other protection settings.

9

Database Considerations

How to move the Change Auditor database and coordinator to another server

NOTE: These instructions are for Change Auditor 5.6 (or higher).

To move the database from one SQL server to another:

1 Determine the current database path
   - Open SQL Server Management Studio.
   - Go to the properties of the Change Auditor database and determine where the database files are located. You need to know this path to copy the files later.

2 Disable the coordinator
   - Go to the Change Auditor server.
   - Right-click the coordinator system tray icon and select **Disable Coordinator**.

3 Detach the database
   - Open SQL Server Management Studio.
   - Locate and right-click the Change Auditor database.
   - Select **Tasks | Detach**.
   - On the General page of the Detach Database screen, selec**Keep** and click **OK**.

4 Copy the old database to the new SQL server

   Copy the files (.mdf and .ldf) to your new SQL Server (most likely to the same location as the other database's on the new server).

5 Attach the old database
   - Open or connect to the new SQL Server.
   - Using SQL Server Management Studio, right-click **Databases** and select **Attach**.
   - On the General page of the Attach Databases screen, click **Add** and select the database you copied over.

- On the warning dialog, click **OK**.

6 Point your old Change Auditor coordinator/server to your new SQL Server

IMPORTANT: Only perform this step on the old Change Auditor server if you do not plan to replace the old coordinator. If you plan to install a new Change Auditor server to replace your old Change Auditor server, proceed to the next step and do not do anything to your old Change Auditor server yet.

- Go to the Change Auditor server.
- Right-click the coordinator system tray icon and select **Coordinator Configuration**.
- On the Security page of the Coordinator Configuration Tool, enter the following information:
  - SQL Server and instance of the new SQL Server
  - Database name of the original database
  - Credentials to access the new SQL Server

This completes the database move.

7 Start up the coordinator service.

- Go to the Change Auditor server.
- Right-click the coordinator system tray icon and select **Enable Coordinator**.

The agents should reconnect. Run the client to ensure that everything is back to normal.

To move the Change Auditor coordinator to another server after moving the SQL database:

If you plan to replace the old Change Auditor coordinator/server, install a newer version of Change Auditor and it connects your existing agents to the new Change Auditor server without a problem. Make sure that you join the existing installation.

1 Install the new version of the coordinator.

- On the Customer Installation Information page, enter the same installation name as the original.
- On the SQL Server Information page, select the (new) SQL server and (original) database name you attached earlier.

After you have completed the installation, start up the coordinator service. Agent communication is re-established.

2 Use Add or Remove Programs to uninstall the disabled coordinator from your old Change Auditor server.

This should remove the old Service Connection Point (SCP) and create a new SCP. If the new SCP is not present when you start the client (Profile field is blank on the Change Auditor Connection screen), restart the coordinator server on the new Change Auditor server.

Restarting the coordinator service on the new Change Auditor server recreates the SCP and you should be able to connect to the default profile when you start the client.

3 Open the Agent Statistics page to review the agents' status. Agents automatically reconnect. Agent activity was not interrupted.

4 You can now upgrade your agents using the Deployment page.

To move the Change Auditor coordinator/server to another Windows Server:

Use the following steps if your SQL database is already on another server and you do not plan to move it. This scenario installs a second Change Auditor coordinator and then disables and uninstalls the first one. All agents transition over to the new Change Auditor server.

1 Install a second coordinator.

- On the Product Licensing page, use the same license files used for the first coordinator.
- On the Customer Installation Information page, be sure to enter the same installation name as the first coordinator.

- On the SQL Server Information page, select the SQL Server and database name used in the first coordinator installation.

2 You now have your new Change Auditor coordinator attached to the database. Start up the coordinator service.

- Go to the new Change Auditor server.
- Right-click the coordinator system tray icon and select **Enable Coordinator**.

3 Disable the first coordinator

- Go to the first Change Auditorserver.
- Right-click the coordinator system tray icon and select **Disable Coordinator**.

4 To ensure the agents connect to the second coordinator, pen the Agent Statistics page.

5 Use Add or Remove Programs to uninstall the disabled coordinator from your first Change Auditor server.

How to estimate the required SQL server disk space

The Change Auditor database (version 6.x or later) can grow indefinitely without a decrease in performance. This makes it unnecessary to create periodic archives.

Adequate disk space should be reserved to accommodate the volume of events dictated by your compliance and retention policies. Testing shows that events take approximately 8,000 bytes per event.

- Example 1: 1,000 events = 8 MB estimated disk size required
- Example 2: 30,000 events = 240 MB estimated disk size required

In addition to the volume of events, the type of events and the volume of alerting also affect disk consumption. To predict disk consumption for your intended retention period, configure Change Auditor as you intend to use it in your environment for a period sufficient to project long-term space requirements.

How SQL Server Autogrow affects Change Auditor

The Change Auditor database (version 6.x or later) is created with SQL Server Autogrowth set to 10%. This may cause issues for large databases that require an extended amount of time to grow the database.

If you begin to see frequent timeouts in the coordinator log, check the SQL Errorlog for “Autogrow of file ‘ChangeAuditor’ in database ‘ChangeAuditor’ was cancelled by user or timed out after 30121 milliseconds.” to confirm that it is related to Autogrowth. If you see this error, consider changing the Autogrowth setting to a smaller value or implementing “Instant File Initialization” on the SQL server hosting the Change Auditor database. You can also pre-allocate a larger size for the Change Auditor database manually.

How to query an archive database

To query an archive database (version 6.x or later), you need to:

1 Create a connection profile for your archive databases.

2 Connect to an archive database.

3 Create and run searches and reports as you normally would.

To create and connect to a connection profile for an archive database:

1 Open the client.

2 On the Connection Profile screen, select **Manage**.

3 On the Manage Connection Profiles dialog, select **Add** to start the Connection wizard.

4 On the first page of the wizard, select **Database Direct** and **Next.**

5 Select the name of your SQL Server and enter the name of the archive Change Auditor database you want to connect to.

6 On the last page of the wizard, name your profile and select **Finish** to save it.

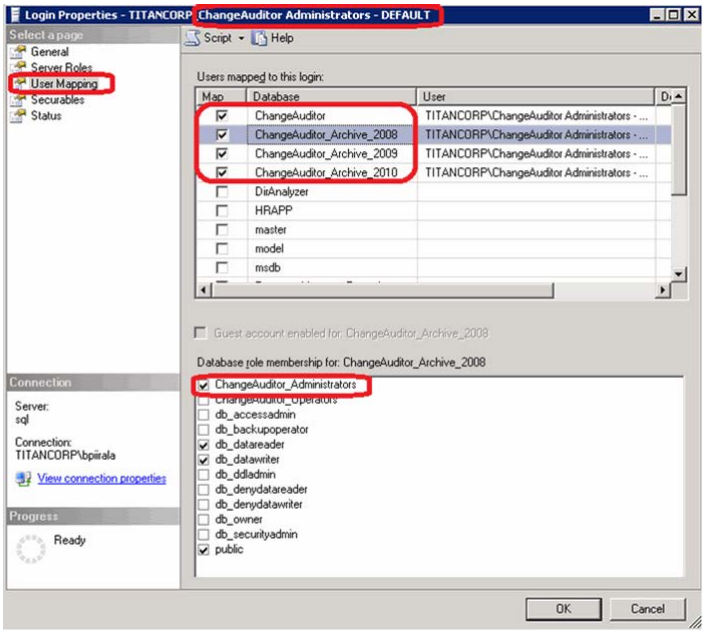
7 On the Connection Profile screen, use the Profile drop-down to select the archive database to use and click **Connect**.

8 After you connect to an archive database, you can create and run searches and reports as you normally would.

NOTE: When users connect to an archive database, they are bypassing the coordinator service and making a direct connection to the SQL Server so they need the appropriate permissions on these archive databases.

An easy way to configure the appropriate SQL security for all users is to add them to the appropriate Change Auditor database role that is created during the coordinator installation. Essentially you will use the Change Auditor security groups that were created during the coordinator installation. Create corresponding SQL logins for these two groups, and then assign each of those logins the appropriate database role for each of the archive databases:

- ChangeAuditor Administrator group to ChangeAuditor_Administrator role
- ChangeAuditor Operator group to ChangeAuditor_Operator role



For more information about adding accounts to the Change Auditor database role, see the Change Auditor Installation Guide.

10

Account exclusions best practices

Some administrative user accounts are responsible for large amounts of Exchange Server utilization, but are trusted accounts and do not need to be audited. In particular, users of BlackBerry Enterprise Server will find that the BES background processes on the Exchange Server Mailbox role consumes significant resources, particularly when the agent is running. Other such accounts may be used for mailbox backup and archiving, spam filtering, and anti-virus protection.

To limit Change Auditor's utilization and unwanted audit events, by default the BlackBerry Enterprise Server administrative accounts, and accounts with similar special Active Directory permissions, are excluded automatically from auditing. This feature can be turned off if necessary (contact Quest Technical Support); however, utilization may increase unacceptably as a result when those accounts are active.

Other trusted user accounts can be manually excluded from auditing. If you find that trusted accounts are generating large numbers of unwanted audit events, or if Exchange Server utilization is unusually high when such accounts are active **and** Change Auditor is running, Quest recommends that you exclude the accounts as described here to reduce overhead and improve performance of the agent.

To exclude user accounts from Exchange Mailbox auditing:

1. Select **View | Administration** to open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **Excluded Accounts** (under the Configuration heading) to open the Excluded Accounts Auditing page.
4. Click **Add** to start the Excluded Accounts wizard.
5. On the first page of the wizard, enter the following information:
   - **Template Name** — enter a descriptive name for the template. For example, Exclude BlackBerry Service Account.
   - **Facility/Event Class list** (middle pane) — scroll and locate the **Exchange Mailbox Monitoring** events. Select one of these events, click **Add**, and select **Add All Events in Facility**.

> **NOTE:** Using the **Add All Events in Facility** option is important because excluding the entire facility allows Change Auditor to ignore all Exchange activity for this account, reducing CPU utilization in the Exchange store or client access service. Excluding some or all individual mailbox monitoring events using the **Add This Event** option disables those events, but does not reduce utilization.

   Click **Next**.
6. On the Select Accounts to Exclude page, use the Browse or Search pages to locate and select the BES Administrative account (for example, BESAdmin, or as named by the administrator). After you have located and selected this account, click **Add** to add the selected account to the list box.
7. Click the down-arrow on the **Finish** button and select **Finish and Assign to Agent Configuration** to assign the template to the configuration that applies to the agents on the Exchange Servers hosting the Exchange Server Mailbox role.
8. On the Configuration Setup dialog, locate the Excluded Account template you just created (it is listed in the Auditing and Protection Templates section across the bottom of the dialog). Select it and then drag it onto the correct agent configuration in the left pane. The **Assigned** cell for the template should now display '**Yes**'.
9. Click **OK** to save the changes and close the dialog.

10 On the Agent Configuration page, confirm that each Exchange Server agent has **Auditing** in the **Exclude Account** column.

   If an Exchange Server agent does not have 'Auditing' in the **Exclude Account** column, select that agent from the list and click **Assign**. On the Agent Assignment dialog, select the correct configuration and click **OK**.

11 After confirming that your Excluded Account template is assigned to the correct agent configuration and is enabled, open the Deployment page (**View | Deployment**) to deploy an agent to the Exchange Servers.

NOTE: When the Change Auditor agent initially starts up, CPU utilization briefly increases in the RPC Client Access service (mailbox role). This is a normal effect of agent initialization as it forces reconnection of any open Outlook connections so they can be audited. After Outlook re connections have finished, processor utilization should stabilize.

To minimize the disruption on networks with many Outlook users, Quest recommends that scheduled installations, upgrades, and starting and stopping of agents on Exchange servers be performed during periods when relatively few users are connected.

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 Office 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.