Quest® Change Auditor 7.6.3

Release Notes

August 2026

These release notes provide information about the Quest Change Auditor release.

- About Quest Change Auditor 7.6.3
- New features
- Important information
- Resolved issues
- Known issues
- System requirements
- Product licensing
- Getting started with Change Auditor 7.6.3
- About us

About Quest Change Auditor 7.6.3

Change Auditor provides total auditing and security coverage for your enterprise network. Change Auditor audits the activities taking place in your infrastructure and, with real-time alerts, delivers detailed information about vital changes and activities as they occur. Instantly know who made the change 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 all critical changes across your enterprise including Active Directory, Microsoft Entra ID, Microsoft 365 Exchange Online\SharePoint Online\OneDrive For Business, Exchange, 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 compliance initiatives including 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 (lock down) 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.
- Modular approach allows separate product deployment and management for key environments including Active Directory, Exchange, Windows File Servers, NetApp, EMC, SQL Server, Active Directory Queries, SharePoint, and Logon Activity.
- Integrate with other Quest products to track, audit, report, and alert on critical changes made using Safeguard Authentication Services and One Identity Defender.

- Integrate with On Demand Audit to gain access to rich visualizations of on-premises and cloud events, responsive search across tenants, and long-term storage of audit data.

Change Auditor 7.6.3 is a minor release, with enhanced features and functionality.

New features

The following enhancements and features are available in this release:

- Logon and authentication event suppression for noisy accounts

  To help reduce audit noise and improve event processing efficiency, Change Auditor will automatically detect accounts that generate high volumes of identical logon or authentication events and temporarily suppress those events once the threshold is exceeded.

  Change Auditor will generate suppression lifecycle events to indicate when suppression starts, provide milestone counts of suppressed events, and report when suppression ends.

- Additional logon activity events

  To improve security, the following events have been added that identify unsafe encryption types when Kerberos authentication tickets (TGTs) and service tickets are requested.

  - A Kerberos authentication ticket (TGT) was requested with an unsafe encryption type
  - A Kerberos service ticket was requested with an unsafe encryption type

  The new events leverage Windows Security Events 4768 and 4769 to provide detailed encryption information. These events require the corresponding Windows auditing policies to be enabled. These events replace the existing “A Kerberos service ticket was created with an unsafe encryption type” event.

- Improved Stability and Diagnostics for Change Auditor Hooks

  Enhanced the reliability of Change Auditor agents on domain controllers by disabling dump file generation by default and reducing the default dump file size. Additional diagnostic logging has been added to assist with troubleshooting. Any agent hook that consistently fails is now automatically disabled.

  This also includes a new internal event: A Change Auditor hook was disabled because exceptions occurred.

Important information

- With Change Auditor database structure, you have access to larger volumes of data online without the need to archive data regularly. Here are a few pointers on auditing and accessing “big data”:
  - When building custom searches, keep in mind that the new schema organizes its event indexes in “hourly blocks”. The smaller the window of time in the when criteria, the better performance in the client for returning a result set.
  - While Change Auditor provides efficient event auditing with our agents, it is highly recommended that you maintain “focused” auditing. This ensures high performance when accessing large amounts of data in the Change Auditor client.

    If excessive audits are received within the same hour, performance may decrease dramatically depending on the criteria selected.
- **General Exchange concepts:**

  Outlook “Show New Mail Desktop Alert” triggers the “Message Read by Owner” event: When this option is enabled, new email that arrives flashes a semi-transparent “alert” near the desktop system tray. Change Auditor captures a Message Read by Owner event when this occurs. The new email alert window opens each new email message as it arrives to build the alert. Note: The “Message Read by Owner” event is disabled by default in Audit Event configuration.

Microsoft Outlook/Exchange add-Ins: Change Auditor may be incompatible with Microsoft Outlook or Exchange “add-ins” (commercial or custom) that interact with Exchange Servers. While Quest makes every effort to ensure proper functionality and performance, we are unable to validate against the many add-ins available for Microsoft Outlook or Exchange Server.

“By Owner” auditing feature: Selecting ‘By Owner’ auditing for many mailboxes can produce many events. This adversely affects Change Auditor auditing and in severe cases the performance of the Exchange Server itself. In extreme cases, Outlook connections may be slowed or dropped. Select owner auditing for at most only a few critical mailboxes.

Auditing mailboxes with many delegates: Auditing normal mailboxes where access permission is granted to many delegates (more than 10), can produce large numbers of non-owner events. This will adversely affect Change Auditor auditing and in severe cases, the performance of the Exchange Server itself. If these mailboxes need to be audited, add them to the Shared Mailbox list (User Defined tab) to reduce unwanted non-owner events and to improve performance.

SMTP alert notifications on owner mailbox “event storm”: It is highly recommended that mailboxes configured to receive SMTP alerts are excluded from auditing “by Owner” events. An “event storm” could occur when a new SMTP alert is received on an audited mailbox by owner, generating a never-ending cycle of “Inbox opened by owner” and “Message read by owner” events.

Upgrading agents on high volume Exchange Servers: It is critical that 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.

Attempting to upgrade the agent on a busy Exchange Server may result in:

- Exchange 2016 or 2019 mailbox role: failed agent upgrade, unwanted RpcClientAccess or IIS application pool restarts, or unscheduled Exchange cluster node failover.

To eliminate the possibility of unscheduled Exchange Server downtime, perform agent upgrades to Exchange Servers during periods of low or no mailbox activity.

- **Troubleshooting EMC events:** If EMC events are not being audited by the Change Auditor agent, first check to see if the EMC CAVA agent service is running on your Windows Server where the EMC events are being collected. Second, check to see if the CEPP service on the EMC Data Mover is running or if the state is offline, by using the command:

  ```
  server_cepp {mover_name} -p -i
  ```

  Resulting output of this command should be similar to the following:

  IP = {mover IP}, state = ONLINE... etc

  If the CEPP service is OFFLINE, you can fix this by first restarting the EMC CAVA service on the Windows Server. If that does not work, restart the EMC CEPP services on the Data Mover by using the following command:

  ```
  server_cepp {mover_name} -service -start
  ```

- **Change Auditor agent requires File and Printer Sharing on Windows Servers:** By default, File and Printer sharing are not enabled on Windows Server installations. To remotely install agents to Windows Servers (Full UI and Server Core), enable the File and Printer Sharing (SMB-in) Inbound rule in the Windows Firewall (Port 445) on the target host machine.

  The File and Printer Sharing for Microsoft Networks service on the network adapter is also required to be enabled for remote deployment.

- **File System auditing for NAS and mapped network drives:** Change Auditor does not support File System auditing on NAS devices or mapped network drives other than NetApp Data ONTAP filers.

- **Microsoft Office files:** Since the Change Auditor for Windows File Servers, NetApp, and EMC drivers capture events related to file activity, it is possible that a folder containing files being opened and edited by Microsoft Office products (Word, Excel, PowerPoint, and so on) will generate unexpected results. Understanding how MS Office products interact with the file system might help explain some of the audit events captured. See http://support.microsoft.com/kb/211632 for more details.

- **File System Auditing for SAN:** Support and engineering will attempt to troubleshoot and resolve issues to the best of their ability when the SAN is attached to a Windows-based file server such that it appears as a local drive on that host. In this configuration, the SAN generally behaves as an extra disk drive on the server which can be audited by a Change Auditor agent on that server. Success in this configuration depends on many factors and is not guaranteed.
- **File System auditing:** Change Auditor does not audit files with a size of zero (0) bytes.
- **Recompiling the Change Auditor MOF file:** Change Auditor no longer ships with a MOF file as part of the coordinator installer. Should the CA WMI namespace become corrupt, or should there be an installation failure, the file can be recompiled using the following command line:

  ```
  ChangeAuditor.Service.exe --install
  ```

- Changes to domain administration level security objects may generate subsequent DACL changes reported with Changed By information as “NT AUTHORITY\ANONYMOUS LOGON” up to an hour after the original change. According to Microsoft, an Active Directory domain controller that holds the primary domain controller (PDC) operations master role runs a thread every hour to check the access control lists of members of several built-in administrative groups. If a user account is a member of one of these administrative groups, even if only because of its membership with a distribution group, the user account's ACL is checked when the thread is run and may be reset to the ACL of the CN=AdminSDHolder,CN=System,DC=<*domain*> object.
- **Exclude Change Auditor components and monitored processes from antivirus software:** Quest recommends excluding the following Change Auditor components and monitored processes from any antivirus software that uses technology similar to “Buffer Overrun Protection” or “On Access Scanner”:
  - DSAMain.exe
  - Lsass.EXE
  - NPSRVhost.exe
  - Services.exe
  - ‘Server’ service
  - Microsoft.Exchange.RpcClientAccess.Service.exe (Exchange Server)
- **Change Auditor coordinator service running under a service account (instead of Local System):**

  If the coordinator service is running under a service account (instead of Local System):
  - The user must re-save existing Forest or GC profiles using the Change Auditor client's connection wizard. This updates the SPN with the correct information.
  - The user must enter the coordinator’s IP address instead of its DNS name in the connection settings in:

    The web.config for the Change Auditor web client

    The manual option in the Change Auditor client's connection wizard

Resolved issues

The following is a list of issues addressed in this release.

Table 1. General resolved issues

Resolved issue	Issue ID
Change Auditor now avoids unnecessary FPolicy reconfiguration after connection closures, preventing potential reconfiguration loops and improving connection stability.	635162
Unable to install the client on hosts that were not joined to a domain.	540735
Agent generating excessive "Could not find volume info" warning messages when processing NetApp events related to ~snapshot directories.	644504

Table 1. General resolved issues

Resolved issue	Issue ID
Event name lookup failures when processing NTLM and Kerberos authentication events. In some environments, Change Auditor was unable to correctly resolve certain event names, resulting in unnecessary warnings and incomplete event information.	629247
Repeated TTL hook failures generating excessive mini dumps.	658322
Canonical names of Foreign Security Principal (FSP) objects are not displayed when viewing protection templates in the Change Auditor client.	618663
Dynamic Object Removal events generated warnings on Windows Server 2022 and Windows Server 2025 domain controllers after the June 2026 Windows updates.	648966
Irregular Domain Replication Activity events are not generated correctly on Windows Server 2016 and Windows Server 2019 domain controller agents after the July 2026 Windows updates.	659396

Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

Table 2. General known issues

Known issue	Issue ID
Agent causes a fatal error during an upgrade installation of VMWare Tools.	483095
Actions caused by the Search-Mailbox command are not audited by Change Auditor.	6893
Change Auditor agents are not compatible with Kaspersky Endpoint Security 11.	323242
An error stating that the “Object already exists” may be encountered when attempting to create a SharePoint or SQL DLA template. **Workaround:** Delete the “Quest ChangeAuditor 5.5” key container using the following command in the CMD Prompt. A new “Quest ChangeAuditor 5.5” key container will be automatically created: %windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis –pz “Quest ChangeAuditor 5.5”	7801
Unable to restart an agent from the Statistics tab. **Workaround:** Use the Stop and Start options instead.	652516
Some web client features do not function correctly in Internet Explorer if the web client address contains an underscore.	494521
When using smartcard authentication you may receive a ‘Credentials are not valid’ error when re-connecting Change Auditor client after it has been disconnected. **Workaround:** Close and reopen the client and try to connect again.	510330
When in Active Directory Client Certificate Authentication mode, manual connection method fails if the client is in a domain that does not have a trust in place with the domain where the Change Auditor coordinator is installed.	503383
Launching Change Auditor using a local account displays the Windows Forms Authentication login screen even if Active Directory Client Certificate Authentication is enabled. **Workaround:** Use RunAs.exe to run the client as a user who has access to the appropriate domains and can read the information in the service connection points.	503374
Upgrade fails if your previous version installation name was longer than 22 characters.	422945
The Change Auditor client sets the incorrect time when the Active Directory subsystem is added with a prompt.	420042
When the Coordinator server runs a command to insert an event, it looks for the event that matches a certain criteria and has a time detected that occurred before the current time on the Change Auditor database server. If the agent time is ahead of the Coordinator time, alerts are not sent because of issues with the event query. **Workaround:** Update time on the servers.	422986
SQL Server tempdb. The SQL Server tempdb grows to accommodate Change Auditor queries, scheduled reports, and purge jobs. Quest recommends following Microsoft best practices regarding tempdb management, including allocating the tempdb and transaction logs on a separate drive from user database files. **NOTE:** The minimum tempdb drive space for Change Auditor is 100 GB.	

Table 2. General known issues

Known issue	Issue ID
Conflict with McAfee HIPS and Change Auditor agent causing server reboots: McAfee 8.0 HIPS causes the system to become unresponsive with the ServicesHook.dll which caused the server to reboot every time the Change Auditor agent started. **Workaround:** Exclude the services.exe and lsass.exe from HIPS protection.	226903
AD Protection wizard in the web client: The Web Client does not provide the right-click option from the Forest level to display Peer Domains within the AD Protection wizard.	342993
IRPStackSize issues: After an agent is upgraded on a domain controller, Quest recommends to reboot the domain controller before doing another upgrade. This removes an old ITAD driver from memory. As of Change Auditor 6.0, agents cannot be upgraded after two (2) upgrades have occurred without a reboot on domain controllers. This is to prevent the domain controller from becoming inaccessible. To identify this condition, the DC's system log shows EventID 2011: *The server's configuration parameter "irpstacksize" is too small for the server to use a local device. Increase the value of this parameter*.	
Running coordinator service with a service account: If you are running the coordinator service under a service account, you must move the ServicePrincipalName role holder in order for Kerberos authentication to function correctly. See the Change Auditor Installation Guide for detailed instructions.	
WHO by Group Membership: When setting up a search based on WHO is in a particular group, you must consider the time it takes for AD replication to occur and the time the Change Auditor coordinator needs to add that configuration to the coordinator.	
Coordinator configuration with limited SQL account: The Change Auditor coordinator SQL account must have access to the sys.dm_tran_locks view to resolve host names when using a SQL account with minimal permissions. If two users from two different clients select the same item in the client, one of the users will be displayed with a Change Auditor dialog message along with an "exception" notification stating "Error: 297, Procedure: usp_SQL_Lock_Read, Message: The user does not have permission to perform this action.". If this error is displayed, run the following SQL query: *USE Master;* *GO* *GRANT VIEW SERVER STATE TO {your limited SQL account};* *GO*	
Web Client: Repeatedly switching back and forth between the grid and timeline view keeps increasing the timeline counts by the factor of the original displayed amount.	386038
Report Alerts: Report Alerting cannot be enabled through the web client. **Workaround:** Enable this feature within the Windows client.	386918

Table 3. Change Auditor for Active Directory known issues

Known issue	Issue ID
Server Farm Node added event does not list the original user who added the farm node to Active Directory Federation Services server. The Active Directory Federation Services service account is listed in the WHO field.	247446
Server Farm Node added event is not audited when Active Directory Federation Services is deployed using the SQL Server database option.	248149
If a maintenance utility such as Ntdsutil.exe is used to move the Active Directory database (Ntds.dit file) to a different location, Change Auditor cannot audit or protect the Active Directory database from NinjaCopy (raw volume access) until the Change Auditor agent service is restarted.	230019

Table 3. Change Auditor for Active Directory known issues

Known issue	Issue ID
Custom Active Directory attribute auditing: If audit configurations where custom Active Directory attribute auditing are used, and a new Change Auditor database is created during installation or upgrade with the same installation name, data storage anomalies may occur. See the Upgrade and compatibility for more information.	
Central Access Policy in protected GPO: Due to the way Microsoft is storing the configuration settings for a Central Access Policy, it appears that an unauthorized account can add or remove a Central Access Policy that is in a protected Group Policy container. You do not get an 'Access is denied' warning message explaining the change was not saved similar to what you get when attempting to access other group policy objects within the protected Group Policy container. However, unauthorized changes to the configuration settings for a Central Access Policy are not saved and generates a 'Failed Group Policy Container Access (Change Auditor Protection)' event within Change Auditor.	

Table 4. Change Auditor for EMC known issues

Known issue	Issue ID
Change Auditor for EMC supports single CIFS servers per data mover: The Change Auditor agent does not audit events from another CIFS server that is under the same data mover and has the same shares as the CIFS server used in the CA for EMC policy.	
Change Auditor for EMC is not compatible with EMC "CQM": The Change Auditor for EMC agent does not support running concurrently with EMC Content Quota Management. To ensure that the EMC auditing is successful, disable EMC CQM.	
Client unable to connect to EMC devices after Putty default settings changed: The Change Auditor client uses SSH APIs to connect to EMC devices. Changing the "Default Settings" saved session in the Putty client prevents the Change Auditor client from connecting to the correct server. **Workaround:** Remove any host name or IP address saved in the stored session named "Default Settings" in the Putty client.	159492

Table 5. Change Auditor for Exchange known issues

Known issue	Issue ID
"Appointment created in shared mailbox' event is not recorded when the appointment is auto-created.	20245
No event is recorded and an exception is logged when adding appointment to shared calendar through OWA.	20246
Service Accounts generating excessive Exchange Mailbox events: Bulk operations generated by third-party products that use MAPI transports to scan or modify Exchange mailboxes can cause system slowdowns if not excluded from auditing. Exchange internal requests are automatically excluded from monitoring, as are Blackberry Enterprise Server and similar MAPI synchronization services. Quest recommends adding service accounts of third-party MAPI services to the Account Exclusion list, with the entire Exchange Mailbox facility selected, or with no event classes or facilities selected (indicating all events are excluded for the account).	
OWA protection: If protection is enabled while a user already has an active OWA session on the newly protected mailbox, protection does not prevent the user from deleting the items in the active folder. New OWA sessions established after protection is enabled are properly protected.	
Missing Exchange event detail: Some Exchange Active Directory changes that are detected on domain controllers may be reported with missing information. To capture this detail, add the Domain Controllers group to the Exchange View-Only Administrators group.	

Table 5. Change Auditor for Exchange known issues

Known issue	Issue ID
Exchange scripting extensions: When a Change Auditor 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 a Change Auditor agent be installed on ALL Exchange servers to ensure that all servers are using the same scripting agent. See these TechNet posts for more information regarding the Scripting Agent: • http://technet.microsoft.com/en-us/library/dd297951.aspx • http://technet.microsoft.com/en-us/library/dd298167.aspx	168683
Exchange mailbox permission changes are reported as the System account: When a user is created prior to creation of the mailbox in Exchange Server, the MMC snap-in for Active Directory Users and Computers handles changes to the user attribute msExchMailboxSecurityDescriptor directly, and “Who” information is available. After the Exchange Server actually creates the mailbox, when the first Outlook or OWA client opens it, MMC Users and Computers delegates msExchMailboxSecurityDescriptor changes to another process from which no “Who” information is available. All mailbox permission changes after this point will be generated by the server’s Local System account. There is currently no workaround.	
“Message Read by Owner/Non-Owner” events on mailbox moves: When moving user mailboxes from one message store to another in your Exchange environment, Quest recommends temporarily disabling the audit events for “Message Read by Owner/Non-Owner” in the Audit Event configurations to prevent generating large numbers of Message Read events during the move. Change Auditor is unable to differentiate those system events from normal user activity.	
Auditing of non-primary email addresses is not supported: The use of alternate email addresses throughout audited modules is not supported.	366968

Table 6. Change Auditor for NetApp known issues

Known issue	Issue ID
Resource access is blocked when agent configuration is refreshed. Note: When the agent detects that access to the filer is blocked, it disconnects itself from the filer and reconnects. This resolves the issue.	446000
For NetApp filers in cluster mode, you are unable to change the security on a file immediately after changing the file itself.	439040
For NetApp filers in cluster mode, you are unable to change security on a file from the same computer as the Change Auditor agent hosting the FPolicy server.	439038
Change Auditor for NetApp drops connection to FPolicy Server: If CIFS signing is enabled for communication between the filer and FPolicy server, the filer drops its connection to the FPolicy server with Data ONTAP 7.3.1. This happens when multiple requests are pending from the filer to the FPolicy server without getting a response for the requests sent. When the responses to the multiple requests arrive, the signing check fails due to a bug in ONTAP. Since the signing check fails, the filer turns off signing and tries to send the subsequent requests to which the server responds with an access denied error. **Workaround:** Disable signing on the FPolicy server. See http://support.microsoft.com/kb/887429 for the steps to turn off signing on the FPolicy server.	

Table 7. Change Auditor for SQL Server known issues

Known issue	Issue ID
“Audit Add DB User” and “Audit Drop DB User” events are not always captured by SQL Server when “Create User” and “Drop User” is executed on the SQL Server and therefore will not be seen in Change Auditor.	55123
The SQL Data Level Auditing wizard may not display all valid servers when selecting the instance to audit. **Workaround:** Manually enter the server or instance name when configuring your templates.	478983
SQL Data Level does not support auditing encrypted databases.	463669
When the Event Viewer sorts the SQL Data Level logs, some events are not included and the details no longer match the records in the Event Viewer interface.	453519
The SQL Data Level event details for some object types and operations will not display the “textdata” field if the changed data exceeds the limit (16K bytes) that Change Auditor can handle.	450412
The test credentials option available in SQL Data Level auditing templates will not validate Windows Authentication credentials when the Change Auditor client is running on the SQL Server to be audited.	448942
Due to a limitation with the command used to retrieve transaction log records, data changes larger than 8000 bytes result in a truncated transaction log record. An event is still recorded with the application name, event class, who and where information but the resulting audit event may not show from and to values and text data information. From/to values larger than 4096 characters and text data larger than 8192 characters are truncated by default for performance purposes but this limit can be customized via the registry.	446624
Modifications to SQL data columns of type TEXT, NTEXT, or IMAGE are not supported. Changes to these types may produce no events, or if an event is generated the changed values may not be recorded in the event details in Change Auditor.	449373

Table 8. Microsoft 365 and Microsoft Entra ID Auditing

Known Issue	Issue ID
Unable to edit an existing Microsoft 365 template when connected to a coordinator that was added after the template was created. In this case the Windows client will display an incorrect error message stating that an unsupported version of PowerShell is being used.	325309
Change Auditor is unable to audit Microsoft 365 tenants operated by third-party providers. For example, Microsoft 365 Germany and Microsoft 365 for China use their own data centers. For more information refer to Microsoft documentation.	8267

Table 9. QRadar integration

Known Issue	Issue ID
Destination IP and Source IP will show the same value when the FQDN is specified for QRadar host in a QRadar event subscription.	23859

Table 10. Windows File System

Known Issue	Issue ID
When a folder is protected via location protection, access is incorrectly granted after the agent is restarted (if that folder was being accessed from a computer in the deny access list). Access will be correctly denied when the user logs off the remote computer.	418022
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.	606041
If File Deleted events are enabled in the Windows File System auditing template but File Created events are not, Windows File System File Deleted event is recorded when Save As is used to create a new file.	130156
File opened events are recorded for unopened .exe files when browsing shared folder if the file does not have a custom icon.	125671

System requirements

Before installing Change Auditor 7.6.3, ensure that your system meets the following minimum hardware and software requirements.

- Change Auditor coordinator (Server-side component)
- Change Auditor client (Client-side component)
- Change Auditor agent (Server-side component)
- Change Auditor web client (optional component)

NOTE: Change Auditor components can be deployed on virtual machines running in Infrastructure as a Service (IaaS), such as Amazon Web Services and Microsoft Azure.

Change Auditor coordinator (Server-side component)

The Change Auditor coordinator is responsible for fulfilling client and agent requests and for generating alerts.

Table 11. Coordinator requirements

Requirement	Details
Processor	Quad core Intel Core i7 equivalent or better
Memory	Minimum: 8 GB RAM or better Recommended: 32 GB RAM or better
SQL database supported up to the following versions	• Microsoft SQL Server 2016 SP3 • Microsoft SQL Server 2017 • Microsoft SQL Server 2019 • Microsoft SQL Server 2022 • Azure SQL Managed Instance (PaaS) with SQL authentication or Microsoft Entra authentication **NOTE:** Performance may vary depending on network configuration, topology, and Azure SQL Managed Instance configuration. **NOTE:** Change Auditor supports SQL AlwaysOn Availability Groups, SQL Clusters, and databases that have row and page compression applied.
Installation platforms (x64) supported up to the following versions	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025 **NOTE:** Microsoft Windows Data Access Components (MDAC) must be enabled. (MDAC is part of the operating system and enabled by default.)
Coordinator software and configuration	For the best performance, Quest strongly recommends: • Install the Change Auditor coordinator on a **dedicated** member server. • The Change Auditor database should be configured on a **separate, dedicated** SQL server instance. **NOTE:** Microsoft ODBC Driver 17 for SQL Server is required when the Change Auditor database resides on Azure SQL Managed Instance and Microsoft Entra authentication is selected. **NOTE:** Do not preallocate a fixed size for the Change Auditor database. In addition, the following software and configuration is required: • The coordinator must have LDAP and GC connectivity to all domain controllers in the local domain and the forest root domain. • x64 version of Microsoft's .NET Framework 4.8 • x64 version of Microsoft XML Parser (MSXML) 6.0 • x64 version of Microsoft SQLXML 4.0
Coordinator footprint	• Estimated hard disk space used: 1 GB • Coordinator RAM usage is highly dependent on the environment, number of agent connections, and event volume. • Estimated database size varies depending on the number of agents deployed and audited events captured.

Table 12. Coordinator minimum permissions

Account	Minimum permissions
User account performing the coordinator installation	The user account that is installing the coordinator requires the appropriate permissions 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 and start services. **NOTE:** 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)	The service account running the coordinator service must have the following permissions: • Active Directory permissions to create and modify SCP (Service Connection Point) objects under the computer object that is running the Change Auditor coordinator. • Local Administrator permissions on the coordinator server. **NOTE:** If you are running the coordinator under a service account (instead of LocalSystem), use a Manual connection profile that specifies the IP address of the server hosting the Change Auditor coordinator whenever you start the client. See the Change Auditor User Guide or online help for more information about defining and selecting a connection profile.
SQL Server database access account specified during installation	An account must be created to be used by the coordinator server 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**

Change Auditor client (Client-side component)

The client connects to a coordinator and queries the audited event database for the desired results.

Table 13. Client requirements

Requirement	Details
Processor	Dual core Intel Core i5 equivalent or better
Memory	Minimum: 4 GB RAM or better Recommended: 8 GB RAM or better
Installation platforms (x64) supported up to the following versions	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025 • Windows 10 • Windows 11 **NOTE:** Microsoft Data Access Components (MDAC) must be enabled. MDAC is part of the operating system and is enabled by default.
Screen resolution	• 1280 x 800 with at least 256 colors
Client software and configuration	• x64 version of Microsoft's .NET Framework 4.8 • x64 version of Microsoft XML Parser (MSXML) 6.0 • x64 version of Microsoft SQLXML 4.0
Ports	• Ports 139 and 445 must be opened on the domain controller.
Client footprint	• Estimated hard disk space used: 140 MB • Estimated physical memory RAM) used: 150 to 500 MB Client RAM usage depends on the number of tabs you have open. **NOTE:** Queries that return much data can cause the client to use as much memory as required to store the results in RAM.

Change Auditor agent (Server-side component)

A Change Auditor agent can be deployed to domain controllers (DCs) and member servers to monitor the configuration changes made on these servers. The agents report the audit events to the coordinator which inserts the event details into the Change Auditor database.

Table 14. Agent requirements

Requirement	Details
Processor	Dual core Intel Core i5 equivalent or better
Memory	Minimum: 8 GB RAM or better Recommended: 24 GB RAM or better

Table 14. Agent requirements

Requirement	Details
Installation platforms (x64) supported up to the following versions	• Windows Server 2016 Server Core (Active Directory, File system, Registry, Services, Local Account, and Exchange auditing only.) • Windows Server 2016 • Windows Server 2019 • Windows Server Core 2019 (Active Directory, File system, Registry, Services, Local Account, and Exchange 2019 auditing only.) • Windows Server 2022 • Windows Server Core 2022 (Active Directory, File system, Registry, Services, Local Account, and Exchange 2019 auditing only.) • Windows Server 2025 • Windows Server Core 2025 (Active Directory, File system, Registry, Services, Local Account, and Exchange 2019 auditing only.) **NOTE:** Change Auditor components can be deployed on Windows environments with Secure Boot enabled. **NOTE:** Microsoft Data Access Components (MDAC) must be enabled. MDAC is part of the operating system and is enabled by default. **NOTE:** Windows File System auditing is supported in a Windows failover cluster configuration. However, the agent is not aware of the cluster and only audits the active nodes in the cluster where agents are deployed. **NOTE:** Auditing of some Exchange events requires the latest Exchange service pack. See the Change Auditor for Exchange Event Reference Guide for the minimum service packs required for Exchange events.
Agent software and configuration	• x64 version of Microsoft's .NET Framework 4.8 • x64 version of Microsoft XML Parser (MSXML) 6.0 • x64 version of Microsoft SQLXML 4.0 • The agent must have LDAP and GC connectivity to all domain controllers in the local domain and the forest root domain. • The Change Auditor agent service depends on the following Windows services to be running: ▪ DNS Client ▪ Remote Procedure Call (RPC) ▪ Windows Event Log **NOTE:** Ensure communication over RPC between coordinators and agents.
Agent footprint	• Estimated hard disk space used: 220 MB + local database size + log size. • Change Auditor agent log retention and content is configurable. That is, you can define how many files to retain and the level of logging. • Estimated physical memory (RAM) used: 200 to 500 MB; Agent RAM usage depends on the auditing modules you have licensed.

Table 14. Agent requirements

Requirement	Details
Agent installation is NOT compatible with the following applications	Chang Auditor agent cannot be installed on the same server as agents from Quest products that were precursors to Change Auditor including: • InTrust for Active Directory • InTrust for ADAM • InTrust for Exchange • InTrust for File Access • DirectoryLockdown • SecurityManager These products are no longer available, but if their agents are still installed they should be removed before installing Change Auditor. Due to the way Change Auditor integrates with Active Directory to capture all change details, there may be incompatibilities with third party agents that integrate with Active Directory in a similar way such as Active Directory auditing tools from other vendors. Change Auditor may be incompatible out-of-the-box with agents that are designed to detect suspicious software such as anti-virus tools. In these cases, it may be necessary to configure the third party product to exclude the Change Auditor process from its scope. If Change Auditor is going to be installed alongside products that conform to either of these patterns, Quest recommends that the installation is tested in a non-production environment first to identify any incompatibilities and adjust the product configurations as necessary before deploying to production. By default, Microsoft Defender has the “Block credential stealing from the Windows local security authority subsystem” rule enabled. This setting must be disabled on the agent computer for Change Auditor to audit events. This does not affect workstation agents.

Table 15. Agent minimum permissions

Account	Permissions
User account deploying agents	The user account used to deploy agent must have: • Administrative authority to install software on every target computer. • Interactive logon rights.
System account running on agent	Change Auditor agents must run as Local System.

Change Auditor workstation agent (optional component)

You can deploy workstation agents to capture authentication activity and logon session events from monitored workstations when the Change Auditor for Logon Activity Workstation license is applied.

NOTE: The recommended installation for domain workstations is from the Deployment tab of the Change Auditor Windows client. However, for non-domain workstations you must manually install the workstation agent. See the Change Auditor Installation Guide for recommendations and instructions on manually deploying workstation agents.

Table 16. Workstation agent requirements

Requirement	Details
Processor	Dual core Intel Core i5 equivalent or better
Memory	Minimum: 8 GB RAM or better Recommended: 16 GB RAM or better
Installation platforms supported up to the following versions	• Windows 10 (Pro and Enterprise) • Windows 11 (Pro and Enterprise) **NOTE:** Microsoft Data Access Components (MDAC) must be enabled. MDAC is part of the operating system and is enabled by default.
Agent software and configuration	• Microsoft's .NET Framework 4.8 • Microsoft XML Parser (MSXML) 6.0 • Microsoft SQLXML 4.0 • The agent must have LDAP and GC connectivity to all domain controllers in the local domain and the forest root domain. • The Change Auditor agent service depends on the following Windows services to be running: ▪ DNS client ▪ Remote Procedure Call (RPC) ▪ Windows event log **NOTE:** Ensure communication over RPC between coordinators and agents. **NOTE:** For workstation log management (such as Get Logs or View Agent Log), the following must be enabled on the workstation: • Windows Management Instrumentation (WMI) must be enabled in firewall rule set (usually domain) on the workstation. • Network Discovery and File Sharing must be enabled. • Remote Registry service must be set to 'Start Automatically'. By default, this service is stopped and set to 'Manual' for Windows 10.
Authentication Activity auditing	To capture Authentication Activity events, you must first enable (that is, set to Success, Failure) the 'Audit Logon events' audit policy for all servers or workstations: • Domain - Group Policy Default Domain Policy\Computer Configuration\Windows Settings\Security Settings\Local Policy\Audit Policy\Audit logon events • Workgroup - Local Group Policy Local Computer Policy\Computer Configuration\Windows Sercurity\Security Settings\Local Policies\Audit Policy\Audit logon events
For more information	See the Change Auditor for Logon Activity User Guide for more information about using Change Auditor for Logon Activity.

Change Auditor web client (optional component)

The Change Auditor web client is an optional component that is installed on the Internet Information Services (IIS) web server to provide users access to Change Auditor through a standard or mobile web browser.

Table 17. Web client requirements

Component	Supported versions
Processor	Quad core Intel Core i7 equivalent or better
Change Auditor	Change Auditor (any license)
Installation platforms (x64) supported up to the following versions	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025 **NOTE:** Web Server (IIS) role must be installed.
Software and configuration	• x64 version of Microsoft's .NET Framework 4.8 • ASP.NET 4.5.1 or higher • x64 version of Microsoft XML Parser (MSXML) 6.0 • x64 version of Microsoft SQLXML 4.0
Browsers	• Chrome • Edge • Firefox
Change Auditor role	To install the web client, you must have at minimum the operator role.
For more information	See the Change Auditor Web Client User Guide for more information about installing and using the web client.

IT Security Search requirements

IT Security Search is a web-based interface that correlates IT data from numerous systems and devices into an interactive search engine for fast security incident response and forensic analysis. As a Change Auditor customer, you can use IT Security Search and apply its many features.

Table 18. IT Security Search requirements

Component	Supported Versions
IT Security Search supported up to the following versions	IT Security Search 11.6

Auditing and permission requirements

Exchange Server auditing

Table 19. Exchange Server auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for Exchange
Exchange Servers supported up to the following versions	• Microsoft Exchange Server 2016 CU23 • Microsoft Exchange Server 2019 CU15 • Microsoft Exchange Server SE
For more information	See the Change Auditor for Exchange User Guide.

SQL Server auditing

Table 20. SQL Server auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for SQL Server
SQL Servers supported up to the following versions	• Microsoft SQL Server 2016 SP3 • Microsoft SQL Server 2017 • Microsoft SQL Server 2019 • Microsoft SQL Server 2022 **NOTE:** Change Auditor supports auditing databases that have row and page compression applied. **NOTE:** Auditing is supported on SQL clusters only when they are not using high availability technologies. In this configuration, the agent is not aware of the cluster and only audits the active nodes in the cluster where agents are deployed. **NOTE:** Due to a hotfix Microsoft released for SQL Server, Change Auditor agents no longer capture SQL-related events unless the following action is taken on the SQL Server: Using SQL Server Configuration Manager, add the startup parameter "-T1906" on the Startup Parameters tab in the SQL Server Properties dialog. **This requires a SQL Server service restart.**
For more information	See the Change Auditor for SQL Server User Guide.

SQL Server Data Level auditing

Table 21. SQL Server Data Level auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for SQL Server
SQL Servers supported up to the following versions **NOTE:** • Agent memory can increase 1.5 GB per audited database. • SQL Data Level auditing templates are assigned to an agent when you create the template. Each audited database requires one template assigned to a single agent.	• Microsoft SQL Server 2016 SP3 • Microsoft SQL Server 2017 • Microsoft SQL Server 2019 • Microsoft SQL Server 2022 **NOTE:** • .Net 4.8 is required on the SQL Server where auditing will take place. • Auditing is supported on SQL clusters only when they are not using high availability technologies. In this configuration, the agent only audits the active nodes in the cluster where agents are deployed. • Auditing is only supported for databases in Full and Bulk logged recovery models. Minimally logged operations performed in bulk logged recovery model may not produce auditing events. An initial backup is required for both Full and Bulk logged databases before the transaction log can properly support auditing. • Encrypted databases are not supported. • Auditing databases that have row and page compression applied is not supported.
Required permissions	The account specified in the auditing template that is used to access the SQL Server instance must have the following database permissions: • Permission to open a connection to the targeted database. • Read permissions on targeted tables and system tables. • VIEW SERVER STATE permission. • SYSADMIN server role. • CONTROL SERVER permission.
For more information	See the Change Auditor for SQL Server User Guide.

SQL Server Extended Events auditing (Preview)

Table 22. SQL Server Extended Events auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for SQL Server
SQL Servers supported up to the following versions	• Microsoft SQL Server 2016 SP3 • Microsoft SQL Server 2017 • Microsoft SQL Server 2019 • Microsoft SQL Server 2022 **NOTE:** Auditing is supported on SQL clusters only when they are not using high availability technologies. In this configuration, the agent only audits the active nodes in the cluster where agents are deployed. **NOTE:** Encrypted databases are not supported. **NOTE:** Change Auditor does not support auditing databases that have row and page compression applied.

Table 22. SQL Server Extended Events auditing requirements

Component	Supported Versions
Required permissions	User running Change Auditor client must hold the CA Administrator Role, or a custom role that includes the 'View SQL Templates' operation The specified SQL login account must have the following SQL Server permissions: • Alter any event session • View server state • Connect SQL • View any database Alternatively, the account must have a SQL server role that contains these permissions, for example 'Sysadmin'. **NOTE:** • If using Windows authentication for the SQL Login account, and the specified agent for the auditing template is not installed on the target SQL server, the agent host computer account must also be added to the SQL Security Logins on the target SQL server with the same permissions requirement as the specified SQL login account for the auditing template. • If using Windows authentication for the SQL Login account, and the agent for the auditing template is installed on the target SQL server, the local computer 'NT AUTHORITY\SYSTEM' account must be added to the SQL Security Logins on the target SQL server with the "View Server State" permission granted. Both SQL and Windows authentication are supported.
For more information	See the Change Auditor for Change Auditor PowerShell Command User Guide or the Change Auditor for SQL User Guide for details.

Authentication Services auditing

Table 23. Authentication Services auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for Authentication Services
Authentication Services	Authentication Services latest verison
For more information	See the Change Auditor for Authentication Services User Guide.

Defender auditing

Table 24. Defender auditing requirements

Components	Supported Versions
Change Auditor	Change Auditor for Defender
Defender	Defender latest version
For more information	See the Change Auditor for Defender User Guide.

Active Roles Integration

Table 25. Active Roles integration requirements

Components	Supported Versions
Change Auditor	Change Auditor for Active Directory The integration scripts must be deployed to a server running Active Roles. **NOTE:** • Change Auditor agents do not need to be installed on Active Roles servers. • If Active Roles replication is configured correctly, you only need to deploy the integration script to one Active Roles server. • The Change Auditor agents must be installed on all domain controllers in the environment to ensure that the Active Directory changes are picked up.
Active Roles	Active Roles 8.0 to 8.3
Additional requirements	• PowerShell 2.0 must be installed on the target Active Roles server. • PowerShell Execution policy must be set to 'AllSigned', 'RemoteSigned' or 'Unrestricted' on the target Active Roles server. (For more information, see https://technet.microsoft.com/en-us/library/ee176961.aspx.)

Components	Supported Versions
Rights and permissions	• Active Roles administrator right is required to deploy the integration scripts. • The Active Roles service account (or the override account) must be authorized to access the Change Auditor SDK. That is, add the Active Roles server service account to the ChangeAuditor Administrators security group. **NOTE:** If you use a role with the minimum permissions, use the Application User Interface page on the Administration Tasks tab to define a role that contains the 'Add Sdk' and 'View Sdk' operations. For more information about using the Application User Interface page to define a new role, see the Change Auditor User Guide.
For more information	See the Change Auditor for Active Directory User Guide.

GPOADmin Integration

Table 26. GPOADmin integration requirements

Components	Supported Versions
Change Auditor	Change Auditor for Active Directory
GPOADmin	GPOADmin 5.19 to 5.21
Additional requirements	If you must use a role with the minimum permissions, use the Application User Interface page on the Administration Tasks tab to define a new role that contains the 'Add Sdk' and 'View Sdk' operations. Also, the GPOADmin service account must be added to the ChangeAuditor Administrators group for integration to function properly. **NOTE:** For more information on using the Application User Interface page to define a new role, see the Change Auditor User Guide.
For more information	See the Change Auditor for Active Directory User Guide.

EMC auditing

Table 27. EMC auditing requirements

Component	Supported Version
Change Auditor	Change Auditor for EMC **NOTE:** Change Auditor for EMC 6.5 (or higher) is required for EMC Isilon auditing.
EMC Isilon - Supported up to the following versions	EMC Common Event Enabler (CEE) Framework up to 8.9.9.0 **NOTE:** CEE versions 8.8.1.0 and higher require .Net Framework 4.0 or later. Earlier versions of CEE require .Net Framework 3.5. Ensure that it is installed on the computer where you have installed CEE. **NOTE:** Isilon Server pre-configured for auditing. See the EMC User Guide for more information.
EMC Unity - Supported up to the following versions	EMC Common Event Enabler (CEE) Framework up to 8.9.9.0 To enable auditing, you must configure CEE using EMC Unisphere: • Select **STORAGE | File | NAS Servers**. Open the server properties and select **Event Publishing**. Select to **Enabling Common Event Publishing.** Add the CEPA Server where the CEE is installed, select **All Events**, and save the settings. • Select **File System** you want to audit and choose the **Advanced** tab. Under the **Events Notifications,** select **Enable SMB Events publishing**. **NOTE:** When auditing EMC Unity using an agent on Windows Server 2019, the lowest supported version is EMC Unity 4.4.1.
EMC PowerScale - Supported up to the following versions	EMC Common Event Enabler (CEE) Framework up to 8.9.9.0
Agent	Locate the Change Auditor agent near the EMC device (use fastest connection type available). • Quest recommends to have 1 Gbps network connectivity (or faster connection type) between the monitored EMC device and the computer where the Change Auditor agent service is running. Use a direct or one-switch connection. Use multiple CPU hosts for Change Auditor agent service (at least 2 CPUs or 2 CPU core).
Rights and permissions	• Administrative rights on the EMC Control Station to create or modify the cepp.conf file on the EMC file server (CIFS). • The computer account where the Change Auditor agent is running must have permissions on the EMC Virus Checking policy.
For more information	See the Change Auditor for EMC User Guide for detailed information about installing, configuring, and using Change Auditor for EMC.

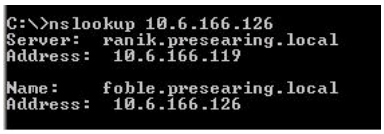
NetApp auditing

Table 28. NetApp auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for NetApp
NetApp Filer	NetApp Filer ONTAP 9.6 to 9.16 **NOTE:** NetApp events initiated through the NFS protocol are not supported.

Table 28. NetApp auditing requirements

Component	Supported Versions

Agent	• Locate a Change Auditor agent close to the NetApp filer (use fastest connection type available).
	  ▪ Quest recommends to have 1 Gbps network connectivity (or faster connection type) between the monitored NetApp filer and the computer where the Change Auditor agent service is running. Use a direct or one-switch connection.
	• Use a multiple CPU host for Change Auditor agent service (at least 2 CPUs or 2 CPU core).
	• In order for the NetApp filer to properly send events to the Change Auditor agent, reverse DNS zone must be configured for the Change Auditor agent server's IP address. This can be configured in the Reverse Lookup Zone of the DNS server used by the NetApp filer. To verify you can look up a Change Auditor agent using its IP address, use the **nslookup** command as illustrated below:
	 
	`C:\>nslookup 10.6.166.126`
	`Server:  ranik.presearing.local`
	`Address:  10.6.166.119`
	`Name:  foble.presearing.local`
	`Address:  10.6.166.126`
	• If Windows Firewall is enabled on the server hosting the Change Auditor agent responsible for capturing the NetApp events, it must be configured to allow 'File sharing'.

Rights and permissions NetApp running in cluster mode	Use the Set Credentials button on the NetApp Auditing template. The account should be an Active Directory user with permissions to configure the NetApp Fpolicy and have access to check the security access control list (ACL) of the NetApp files and folders. HTTP application access must be assigned for the Active Directory user account specified in the auditing template. For NetApp 9.9 and before, ONTAPI access is also required. You may assign the vsadmin role to the specified Active Directory user account or you can create a custom rest role using NetApp OnCommand System Manager with the following minimum role attributes and access (REST API path and Access Level): • Read-only access to /api/storage/volumes • Read-only access to /api/svm/svms • Read/Write access to /api/protocols/fpolicy **NOTE:** domain\username and password are case-sensitive, so the credentials used with the NetApp auditing template must match. See the NetApp user guide for more details on enabling Active Directory domain users access to the cluster.
For more information	See the Change Auditor for NetApp User Guide for detailed information about installing, configuring, and using Change Auditor for NetApp.

SharePoint auditing

Table 29. SharePoint auditing requirements

Component	Supported versions
Change Auditor	Change Auditor for SharePoint **IMPORTANT:** The Change Auditor for SharePoint module processes all activities happening on all site collections within the audited SharePoint farm. When auditing a large SharePoint farm with much activity, the Change Auditor agent may experience performance-related issues including slowness in loading the plugin, slowness in capturing events, or the potential for missed events. Factors that can impact Change Auditor performance include the number of site collections in the farm and the volume of activity taking place in the SharePoint environment. Quest recommends performing a test in an environment that is similar in size and configuration to determine if your farm is suitable to be audited by Change Auditor.
SharePoint	SharePoint Server 2016 SharePoint Server 2019
Required rights and permissions	When selecting the agent to capture SharePoint events, you must enter the credentials to use to access the selected SharePoint farm. This account must have the following permissions: • Local Administrator on the Change Auditor Agent\SharePoint Central Administration server • SharePoint Farm Administrator • The following mappings on the SQL Server that contains the SharePoint databases: ▪ SharePoint_Config SharePoint_Shell_Access SPDataAccess ▪ WSS_Content SPDataAccess ▪ SharePoint_AdminContent SPDataAccess
For more information	See the Change Auditor for SharePoint User Guide for detailed information about installing, configuring, and using Change Auditor for SharePoint.

Logon Activity auditing

Table 30. Logon Activity auditing requirements

Component	Supported versions
Change Auditor	Change Auditor for Logon Activity User license for auditing server agents Change Auditor for Logon Activity Workstation license for auditing workstation agents
Change Auditor | Server agents	Change Auditor for Logon Activity User **NOTE:** See Change Auditor agent (Server-side component).

Table 30. Logon Activity auditing requirements

Component	Supported versions
Change Auditor | Workstation agents	Change Auditor for Logon Activity Workstation
For more information	See the Change Auditor for Logon Activity User Guide.

Microsoft 365 auditing

Table 31. Microsoft 365 auditing requirements

Component	Supported versions
Change Auditor	Change Auditor for Exchange Change Auditor for SharePoint
Microsoft 365 subscriptions	Change Auditor can audit the various Microsoft 365 plans offered by Microsoft including business and enterprise subscriptions.
Windows PowerShell	Windows PowerShell version 5.1 on the computer where the agent is installed.
URLs	The agent configured to monitor Microsoft 365 must be able to access the following URLs: • https://login.microsoftonline.com • https://manage.office.com • https://outlook.office365.com/powershell-liveid • https://graph.microsoft.com
Ports	• A firewall outbound exception for remote port 443 (https) must exist for every agent computer used for Microsoft 365 auditing. Port 443 is used for communicating with the Microsoft cloud. • If an agent is separated from the coordinator by a firewall, you must create a firewall exception for port 8373 on every agent computer to be used for Microsoft 365 or Microsoft Entra ID auditing. Port 8373 is the default port that enables the coordinator to communicate with the agent. A different port number can, however, be specified by running Set-CAConfiguration command. For details, see the Change Auditor PowerShell Command Guide.
Required rights and permissions	• When creating an Microsoft 365 or Microsoft Entra ID auditing template that requires Microsoft Entra web application creation the user will be prompted to log in with Microsoft Entra administrator credentials.
For more information	See the Microsoft 365 and Microsoft Entra ID Auditing User Guide.

Microsoft Entra ID auditing

Table 32. Microsoft Entra ID auditing requirements

Component	Supported versions
Change Auditor	Change Auditor for Active Directory
Microsoft Entra ID	Change Auditor can audit the Microsoft Entra ID that is included with an Microsoft 365 subscription or the Microsoft Entra ID Basic subscription.

Component	Supported versions
URLs	The agent configured to monitor Microsoft Entra ID must be able to access the following URLs: • https://login.microsoftonline.com • https://graph.microsoft.com
Ports	• 443 (HTTPS) — for the agent to connect to the Microsoft Entra ID. • 8373 — for the Change Auditor coordinator service to connect to the agent computer.
Required rights and permissions	• When creating an auditing template that requires Microsoft Entra web application creation, the user is prompted to log in with Microsoft Entra administrator credentials.
Synchronized environments	When auditing Microsoft Entra ID in a synchronized environment, Change Auditor provides more event details by mapping identities from on-premises directories with Microsoft Entra ID. The following conditions must be met for Change Auditor to perform the mapping: • Synchronization performed with Microsoft Entra Connect. • Microsoft Entra Connect synchronization process is active in your on-premises environment and directory sync is active in your cloud environment. • A Microsoft Entra template has been created to audit your online environment that is being synchronized with on-premises Active Directory. • The agent that is specified in the auditing template, must be a member server of the forest that is being synchronized with Microsoft Entra ID. When Federation with AD FS is used as the single sign-on method, Microsoft Entra logon events will no longer be generated since the authentication is done by the on-premises AD FS instance.
For more information	See the Change Auditor for Microsoft 365 and Microsoft Entra ID User Guide.

Product licensing

If you need a new license key, refer to the License Key Upgrade page.

You will need the license number from each license that is applied. To get this information, select the license in the License Manager and choose Details.

If you purchased multiple Change Auditor products, you only need one instance of the Change Auditor product. The license keys determine what features are enabled and disabled in the product.

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

- Change Auditor for Active Directory
- Change Auditor for Active Directory Queries
- Change Auditor for EMC
- Change Auditor for Exchange
- Change Auditor for Logon Activity User (to capture logon activity from server agents)
- Change Auditor for Logon Activity Workstation (to capture logon activity from workstation agents)
- Change Auditor for NetApp
- Change Auditor for SharePoint
- Change Auditor for SQL Server
- Change Auditor for Windows File Servers

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

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.

To enable a trial or purchased commercial license:

1. Copy the Change Auditor license files to your desktop, or other convenient location.
2. If you have not installed the Change Auditor components, 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. During the coordinator installation, you are prompted to locate the Change Auditor license files. Click **Open License Dialog** to locate and apply a license.
4. Review your installed licensed components by right-clicking the coordinator icon in the system tray and selecting **Licensing** or by selecting **Help | About | Licensing** in the client.

To apply 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.

Getting started with Change Auditor 7.6.3

- Upgrade and compatibility
- Additional resources

Upgrade and compatibility

IMPORTANT: Agent upgrade

- As of version 7.6.2, Change Auditor utilizes SQLite for the agent's local event storage. If upgrading from 7.6.1 or earlier directly to 7.6.3, 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 7.6.3 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.

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

- For versions prior to 6.8: You can upgrade directly to 7.6.3. 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 7.6.3.
- Previous versions of Change Auditor agents (6.x through 7.x) can connect and work with the new Change Auditor coordinator.
- Change Auditor requires Microsoft .NET Framework 4.8 for all components.
- A Microsoft Entra application with Microsoft Graph API permissions is required to audit Microsoft 365 and Microsoft Entra ID. As a result, when updating from Change Auditor 7.0.3 or earlier, any existing Microsoft 365 or Microsoft Entra ID auditing templates must be updated by the Change Auditor administrator. See the Microsoft 365 and Microsoft Entra ID auditing User Guide for details on updating the templates and the required permission.

Additional resources

NOTE: For installation and upgrade procedures, refer to the Change Auditor Installation Guide.

Additional information is available from the following:

- Online product documentation (https://support.quest.com/change-auditor/technical-documents)
- Quest Community (https://www.quest.com/community/change-auditor)

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

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.

© 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. ALL RIGHTS RESERVED.

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. ALL RIGHTS RESERVED.
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. ALL RIGHTS RESERVED. 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.