Quest® Change Auditor 7.1

Release Notes

December 2020

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

About Quest Change Auditor 7.1

Change Auditor provides total auditing and security coverage for your enterprise network. To protect your data and your business, Change Auditor Threat Detection uses advanced machine learning, user and entity behavioral analytics (UEBA), and SMART correlation technology to spot anomalous activity and identify the highest risk users in your environment. The users with the highest risk scores are then highlighted in the Threat Detection dashboard, enabling you to prioritize your response and adjust policies to strengthen your organization's security and regulatory enforcement.

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, Azure Active Directory, Office 365 Exchange Online\SharePoint Online\OneDrive For Business, Exchange, Windows File Servers, NetApp, EMC, SQL Server, VMware vCenter, SharePoint, Microsoft Skype for Business and Fluid File Systems.
- 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, Logon Activity, and Skype for Business.
- Integrate with other Quest products to track, audit, report, and alert on critical changes made using Quest Authentication Services and Quest 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 7.1.1 is a minor release, with enhanced features and functionality. See New features.

New features

Additional Office 365 Exchange Online mailbox events:

- Message opened in online shared mailbox
- Message opened in online mailbox by owner
- Message opened in online mailbox by non-owner
- Online mailbox auditing has been throttled
- Folder opened in online mailbox by owner
- Folder synchronized from online shared mailbox
- Folder synchronized from online mailbox by owner
- Folder synchronized from online mailbox by non-owner

Enhanced security auditing

- Event generated when an agent's configuration for Kerberos ticket lifetime is changed:
  - Agent configuration Kerberos Ticket Lifetime changed
- Event generated when Kerberos auditing components are not on the domain controller resulting in Kerberos authentication events not being captured:
  - Kerberos auditing components failed to load
- Ability to detect when an irregular domain replication request is performed which could indicate a potential threat:
  - Irregular domain replication activity detected
- Additional built-in searches:
  - All Irregular Domain Replication Activity Events under Shared | Built-in | All Events
  - All Kerberos user ticket events that exceed the maximum ticket lifetime in the past 30 days under Shared | Built-in | Logon Activity

Search Enhancements

- Ability to search and filter events based on the coordinator that processed them.
  - Updated Coordinator Statistics page:
    - Coordinator ID column to identify the coordinator that processes the events.
    - Hyperlinked columns to run a quick search for associated events for each coordinator.
  - Search results include the Coordinator ID to identify the coordinator that processed the event.
  - Layout tab includes a Coordinator ID column to sort and order results by coordinator.
- Ability to see failure reason and status code in Active Directory failed search results.
- Ability to see the full search folder path to identify the location for all search folder changes.

- Updated default columns for the "All Failed Logons in the last 7 days” report.
- Updated operators access when using the search commands:

  Full access when using the following commands:

  - Invoke-CASearch
  - Get-CASearches
  - Get-CASearchDefinition

  Restricted access to private searches and folders when using the following commands:

  - Set-CASearchProperties
  - Copy-CASearch
  - Add-CASearch
  - Move-CASearch
  - Remove-CASearch
  - Add-CASearchFolder
  - Remove-CASearchFolder

SIEM Tool Integration Improvements

- Ability to send the rich events gathered by Change Auditor to a Syslog server.
- Following events to monitor changes to syslog subscriptions have been added:
  - Syslog subscription added
  - Syslog subscription modified
  - Syslog subscription removed

Ability to Audit and Protect the Active Directory Database

Change Auditor allows you to monitor the Active Directory database (NTDS.dit) file for possible unauthorized access attempts. When configured, Change Auditor can also prevent copying and other tampering attempts on the Active Directory database (NTDS.dit) file.

Extraction of this file could lead to parsing of usernames and passwords resulting in a security breach. The ability to audit changes to this file reduces the risk of the user account information from being accessed and tampered with by unwanted processes or users.

The following events have been added:

- Active Directory database file access rights changed
- Active Directory database file accessed
- Active Directory database file attribute changed
- Active Directory database file auditing changed
- Active Directory database file central access policy changed
- Active Directory database file classification changed
- Active Directory database file created
- Active Directory database file deleted
- Active Directory database file last write changed
- Active Directory database file moved
- Active Directory database file ownership changed
- Active Directory database file renamed

    - Failed Active Directory database access (Sharing violation)
    - Failed Active Directory database access (Change Auditor Protection)
    - Failed Active Directory database access (NTFS permissions)

- The following built-in searches have been added:
    - All Active Directory Database Events under Shared | Built-in | All Events
    - Active Directory Database Events in last 30 days under Shared | Built-in | Security | Domain Controller Security
    - GDPR - Active Directory Database Events in last 30 days under Shared | Built-in | Regulatory Compliance |GDPR |Audit and Accountability | Active Directory
    - GDPR 32 - Active Directory Database Events in last 30 days under Shared | Built-in | Regulatory Compliance |GDPR |Security of Processing (32) | Active Directory

Ability to Audit Active Directory Federation Services

Change Auditor allows you to monitor the Active Directory Federation Services login activity and configuration changes once an Active Directory Federation Services auditing template has been created and assigned to the appropriate agent.

- The following events have been added:

NOTE: A Change Auditor Logon Activity license is required to capture the sign-in events. A Change Auditor for Active Directory license is required to capture the configuration changes events.

    - Successful Active Directory Federation Services sign-in
    - Failed Active Directory Federation Services sign-in
    - Additional authentication methods changed
    - Additional authentication method registered
    - Additional authentication method unregistered
    - Allow additional authentication providers as primary setting changed
    - Extranet authentication methods changed
    - Intranet authentication methods changed
    - Relying Party Trust added
    - Relying Party Trust changed
    - Relying Party Trust deleted
    - Relying Party Trust disabled
    - Relying Party Trust enabled
    - Active Directory Federation Services auditing template added
    - Active Directory Federation Services auditing template disabled
    - Active Directory Federation Services auditing template enabled
    - Active Directory Federation Services auditing template removed
    - Active Directory Federation Services auditing template added to agent configuration
    - Active Directory Federation Services auditing template removed from agent configuration
    - Active Directory Federation Services sign-ins auditing enabled
    - Active Directory Federation Services sign-ins auditing disabled
    - Active Directory Federation Services configuration changes auditing disabled
    - Active Directory Federation Services configuration changes auditing enabled

- The following built-in searches have been added:
  - All Active Directory Federation Services sign-ins in the last 24 hours under Shared | Built-in | Active Directory Federation Services
  - All Successful Active Directory Federation Services sign-ins in the last 24 hours under Shared | Built-in | Active Directory Federation Services
  - All Failed Active Directory Federation Services sign-ins in the last 7 days under Shared | Built-in | Active Directory Federation Services

Foreign Forest Support

The following is supported in environments where a coordinator does not exist in the foreign forest where agents are deployed:

- Ability to audit foreign forests by member of group.
- Ability to search foreign forest by member of group using the Who criteria.
- Ability to search foreign forest by member of group using the What criteria.
- Ability to expand foreign forest groups by Group Membership Expansion.
- Ability to audit Exchange mailboxes with an agent in the foreign forest.
- Ability to exclude events generated by foreign forest accounts with account exclusion.
- Ability to specify group Managed Service Account to be used for foreign forest agent to establish a coordinator connection.

Authentication Enhancements

The following authentication options are supported through the client and PowerShell:

- Certificate authentication when the client and coordinator exist in environments where NTLM restrictions are in place.
- Azure Active Directory authentication when the Change Auditor database resides on an Azure SQL Managed Instance.

Additional Platform Support

The following support has been added:

- Microsoft Exchange Server 2016 CU16, CU17, and CU18
- Microsoft Exchange Server 2019 CU5, CU6, and CU7
- Azure SQL Managed Instance (PaaS) with SQL authentication or Azure Active Directory authentication for Change Auditor coordinator
- Azure SQL Managed Instance (PaaS) with SQL authentication for Change Auditor client
- Microsoft SQL Server 2017 and 2019 for Skype for Business auditing
- Windows Server 2016 ADFS
- Windows Server 2019 ADFS
- Fluid File System 6.0.4
- GPOADmin 5.15
- CEE 8.7.7 for EMC auditing
- Dell Storage Manager 18.1 and 19.1
- Chrome 84
- Edge 84
- Firefox 78
- Safari 13.1.1

The following support has been removed:

- Windows Server 1803 Server Core
- Windows 8 for the client and workstation agent

Miscellaneous Features and Enhancements

- Share added, share deleted, and share edited events are generated when the New-SMBShare, Remove-SMBShare, and Set-SMBShare commands are run. The events are also generated when using Server Manager File and Storage Services add share task and “Stop Sharing" and "Properties" context menus.
- New Active Directory email tags for the reason and status for failed Active Directory events. (AD_STATUS_CODE and AD_FAILURE_REASON)
- Ability to see the license number for all applied licenses.
- The authentication certificates used to authentication with On Demand Audit will automatically renew as required.
- Office 365 Exchange Online events no longer display Microsoft deprecated events.
- Improved alert query performance.
- A user object's UserPrincipalName is now updated immediately following modification for enhanced reporting.
- Event generated when coordinators specified to handle scheduled purge, archive, and report jobs are unavailable: All specified coordinators that handle purge/archive/report jobs are unavailable.

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 2013 mailbox role: failed agent upgrade, unwanted RpcClientAccess service restart, or unscheduled Exchange cluster node failover.
- Exchange 2013 client access role: unwanted IIS Exchange application pool restarts.
- 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.

- **General EMC concepts:**

  Control Stations: The Control Station is a dedicated management computer that monitors and controls cabinet components and allows access to the full functionality of the Celerra or VNX Network Server software. It contains utilities for installing and configuring the Celerra or VNX Network Server, maintaining the system, and monitoring system performance. The Control Station runs a set of programs that are collectively referred to as the Control Station software. The Control Station itself uses an EMC-customized version of Linux as its operating system.

  Data Movers: Data Movers are the Celerra or VNX components that transfer data between the storage system and the network client. Data Movers are managed by using a Control Station. By default, Data Movers are named server_n, where n is the slot number of the Data Mover. For example, server_2 is the Data Mover in slot 2.

- **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 Server 2012:** By default, File and Printer sharing are not enabled on Windows Server 2012 installations. To remotely install agents to Windows Server 2012 (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 EMC Celerra/VNX/Isilon or 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
  ```
- **Blackberry Enterprise Server (or similar) services:** To eliminate auditing of automated tasks, the Change Auditor agent attempts to automatically exclude auditing of mailbox accesses by Blackberry Enterprise Server (BES) or similar service accounts. These accounts have both ‘Receive All’ and ‘Administer Information Setup’ rights on the mailbox database. If these explicit rights are granted to user accounts, those accounts are also excluded from mailbox auditing, which may not be wanted. If necessary, this automated exclusion can be disabled on a server-by-server basis.
- 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
  - Microsoft.Exchange.RpcClientAccess.Service.exe (Exchange 2013 only)
  - NPSRVhost.exe
  - Services.exe
  - ‘Server’ service
- **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
"Failed to load registry driver" error generated in agent log on Windows 2012 domain controllers.	190301
Stopping an agent with two file system auditing templates enabled, may cause Change Auditor to close unexpectedly with error 0xC0000008 (invalid handle).	222345
Login user is not displayed when logged in as the domain administrator.	223573
All agent and coordinator status panels display html error in the web client overview page.	226389
Active Directory garbage collection and dynamic object time to live (TTL) expiration for objects in the deleted objects container are audited and causing a "Failed attempt to read attributes" error.	208937
Local share added and local share permissions changed events are not generated when using Server Manager or PowerShell.	205364
URLs required to create a configuration with and send events to On Demand Audit in Canada, UK, Australia regions need to be added to the Change Auditor User Guide.	208779
When a Group Policy subsystem item is added to a search, the canonical name is displayed in the search criteria twice rather than the expected group policy name and canonical name.	162940
Azure Active Directory group events return unexpected results when filtering by Sync Type.	201932
The Add-CASearch and the Set-CASearchProperties commands are not generating internal events.	208171
When the web client is hosted on servers with non US-English regional settings, the event details “When” value displays Invalid date.	208590
The internal event "Public user search folder deleted" is not being generated.	208630
New coordinators added to an installation are not able to decrypt proxy, email, and shared folder passwords.	209296
The "ChangeAuditor Agents" domain local security group is not being created in child domains.	215144
Azure Active Directory and Office 365 template creation fails with the error "Failure setting Azure app permissions" due to "The remote server returned an error: (403) Forbidden".	217209
Get-CASearches command fails and throws an exception when it is unable to resolve a search owner in Active Directory.	10857
Newly added coordinators cannot decrypt the proxy server password and generates the following message in the Coordinator log “No Public key found matching the Coordinator key. Unable to decrypt data."	196981
Get-CASearches command does not function when run with the Change Auditor Operator role.	198784
Change Auditor displays only a single Office 365 template even though multiple templates exist.	203056
Invoke-CASearch and Add-CASearch commands do not function when run with the Change Auditor Operator role.	204180
Change Auditor client is non-responsive when enabling Active Directory client certificate authentication.	206762
Move-CASearch and Remove-CASearchFolder commands are not generating the associated internal events.	207568
Note added to documentation to inform users that a manually created database cannot be used for the coordinator. The database must be created by the coordinator installation.	199047
An Active Directory search that contains specific objects and “LIKE” objects returns only results for the specific objects. The “LIKE” objects are not returned.	6879
Change Auditor client becomes unresponsive if a number higher than 32,767 is entered in the Send Alert When field in smart alerts.	15232

Table 1. General resolved issues

Resolved issue	Issue ID
"Array dimensions exceeded supported range" error is generated and alerts are not sent when Events per Email field specifies a value higher than 99,999,999.	86249
UserMail and ADAM instance port columns are not displayed when added to the search layout.	180832
Alert variables for Azure Active Directory properties do not display values in alert emails.	199939
The error produced when the coordinator database credentials are incorrect does not provide enough detail.	199048
The “NOT LIKE” criteria for target does not function for Azure Active Directory searches.	199110
Documentation updated to fix a column label. (Deployment column label for “Foreign Forest” is shown incorrectly labeled as “Foreign”.)	199490
After enabling Event Logging, event description details are displayed incorrectly in Event Viewer.	199565
Active Directory Protection Wizard does not allow MSA or GMSA objects to be added to bypass protection.	200213
“Kerberos Ticket Lifetime” setting in agent configuration, does not handle invalid values in the same manner as other controls in the dialog.	200261
Coordinator start up fails and generates a database initialization not successful error.	202354
An Azure Active Directory query with the “NOT LIKE” option in the target column returns all data that matches any target column.	191176
Azure Active Directory auditing fails and generates error "Failed to process configuration: Object reference not set to an instance of an object" in the log file.	198588
Kerberos Ticket Lifetime (MaxKerbTicketAge) setting should be added to the output for the Get-CAConfigurations command.	198677
When an Azure Active Directory auditing template is replaced with another template for a different tenant, sign-in and risk events are not collected until the agent is restarted.	198796
F1 help in What | Add With Events | Result opens to “Can't reach this page”.	156146

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
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
You may be unable to view or gather agent logs in the client for older agents after upgrading to change Auditor 6.9.5 or later.	15954
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
Running the Change Auditor agent on Windows Server 2012 causes the system to become unresponsive if the Change Auditor Registry driver (CARegSys.sys) is added to the Driver Verifier.	371273
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

Table 2. General known issues

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
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.	
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
Change Auditor for VMware not auditing VMware Local User and Group Account events: When connecting directly to the ESXi host from a vSphere client bypassing vCenter, VMware Local User and Group Account events will not be audited by Change Auditor agent.	
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.	
Central Access Policy in protected GPO: Due to the way Microsoft is storing the configuration settings for a Central Access Policy (Windows Server 2012), 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 2. General known issues

Known issue	Issue ID
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
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.	

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
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.	
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
Delayed events using Entourage and Exchange 2013: There is a known issue with Microsoft Exchange 2013 and Entourage EWS or Outlook 2011 for Mac where content conversion may fail, and connections are dropped by the server without any response to the client. Contact Microsoft for a fix.	
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
If you host an agent on Windows Server 2012 or Windows Server 2012 R2, the connection between the agent and a NetApp filer (7-mode) may fail due to the “Secure Negotiate” added to SMB 3.0 for Windows Server 2012 which requires correct signing of error responses by all SMBv2 servers. For resolution details see the following: http://support.microsoft.com/en-us/kb/2686098.	442110
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. Change Auditor for Fluid File System known issues

Known issue	Issue ID
Duplicate FluidFS File open events may be generated when editing files on audited FluidFS clusters.	591424
When you upgrade to version 6.9.5 or later, existing FluidFS auditing templates stop auditing. **Workaround:** Save the FluidFS auditing template and update the agent configuration.	15520

Table 9. Office 365 and Azure Active Directory Auditing

Known Issue	Issue ID
Change Auditor is unable to audit Office 365 tenants operated by third-party providers. For example, Office 365 Germany and Office 365 for China use their own data centers. For more information refer to Microsoft documentation.	8267

Table 10. 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 11. Threat Detection

Known Issue	Issue ID
Integration password cannot begin with a supported special character (@ or $).	164259

System requirements

Before installing Change Auditor 7.1, 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 12. 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 2012 SP4 • Microsoft SQL Server 2014 SP3 • Microsoft SQL Server 2016 SP2 • Microsoft SQL Server 2017 • Microsoft SQL Server 2019 • Azure SQL Managed Instance (PaaS) with SQL authentication or Azure Active Directory 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 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **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 Azure Active Directory 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 4.7.1 • 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 13. 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 14. 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 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows 8.1 • Windows 10 **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 4.6.1 • 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 15. Agent 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

Table 15. Agent requirements

Requirement	Details
Installation platforms (x64) supported up to the following versions	• Windows Server 2012 • Windows Server 2012 Core • Windows Server 2012 R2 • Windows Server 2012 R2 Core • Windows Server 2016 Server Core • Windows Server 2016 • Windows Server 2019 (VMWare auditing is not supported) When auditing EMC Unity using an agent on Windows Server 2019, the lowest supported version is EMC Unity 4.4.1. • Windows Server Core 1909 (Active Directory, Windows File System, Registry, Services, and Local User and Group auditing only) • Windows Server Core 2019 (Active Directory, File system, Registry, Services, local user and group, and Exchange 2019 auditing only) • Windows Server 1809 Server Core (Active Directory, File system, Registry, Services and local user and group auditing only) • Windows Server 1903 Server Core (Active Directory, File system, Registry, Services and local user and group 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 4.6.2 • 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: 120 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: 60 to 100 MB; Agent RAM usage depends on the auditing modules you have licensed.

Table 15. 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.

Table 16. 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.
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 17. Workstation agent requirements

Requirement	Details
Processor	Dual core Intel Core i5 equivalent or better
Memory	Minimum: 2 GB RAM or better Recommended: 4 GB RAM or better

Table 17. Workstation agent requirements

Requirement	Details
Installation platforms supported up to the following versions	• Windows 8.1 (Pro and Enterprise) • Windows 10 (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	• x86 or x64 version of Microsoft's .NET Framework 4.6.2 • x86 or x64 version of Microsoft XML Parser (MSXML) 6.0 • x86 or 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. **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 8.1 and 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 18. Web client requirements

Component	Supported versions
Processor	Quad core Intel Core i7 equivalent or better
Change Auditor	Change Auditor (any license) **NOTE:** Change Auditor 6.5 (or higher) is required for using the Administration Tasks page to manage Change Auditor.
Installation platforms (x64) supported up to the following versions	• Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **NOTE:** Web Server (IIS) role must be installed.
Software and configuration	• x64 version of Microsoft's .NET Framework 4.6.1 • ASP.NET 4.5.1 or higher • x64 version of Microsoft XML Parser (MSXML) 6.0 • x64 version of Microsoft SQLXML 4.0
Browsers supported up to the following versions	• Chrome 84 • Edge 84 • Firefox 78 • Safari 13.1.1 • Internet Explorer 11 not running in Compatibility View mode **NOTE:** Versions below 11 are not supported. • Safari 9.1.2 for Mac OS (Windows Safari is not supported)
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, configuring, 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 access IT Security Search from our Autorun and begin to apply its many features.

Table 19. IT Security Search requirements

Component	Supported Versions
IT Security Search supported up to the following versions	IT Security Search 11.4.1

Auditing and permission requirements

Exchange Server auditing

Table 20. Exchange Server auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for Exchange
Exchange Servers supported up to the following versions	Windows Server 2012 • Microsoft Exchange Server 2013 CU23 • Microsoft Exchange Server 2016 CU18 Windows Server 2012 R2 • Microsoft Exchange Server 2013 CU23 • Microsoft Exchange Server 2016 CU18 Windows Server 2016 • Microsoft Exchange Server 2016 CU18 Windows Server 2019, Windows Server Core 2019 • Microsoft Exchange Server 2019 CU7 **NOTE:** MAPI over HTTP protocol is supported starting from Microsoft Exchange Server 2013 CU8.
For more information	See the Change Auditor for Exchange User Guide.

SQL Server auditing

Table 21. 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 2012 SP4 • Microsoft SQL Server 2014 SP3 • Microsoft SQL Server 2016 SP2 • Microsoft SQL Server 2017 • Microsoft SQL Server 2019 **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 22. SQL Server Data Level auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for SQL Server
SQL Servers supported up to the following versions	• Microsoft SQL Server 2012 SP4 • Microsoft SQL Server 2014 SP3 • Microsoft SQL Server 2016 SP2 • Microsoft SQL Server 2017 • Microsoft SQL Server 2019 **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:** Change Auditor SQL Data Level auditing currently only supports auditing 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. **NOTE:** Encrypted databases are not supported. **NOTE:** Change Auditor does not support auditing databases that have row and page compression applied. **NOTE:** Agent memory can increase 1.5 GB per audited database. **NOTE:** 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.
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.

Authentication Services auditing

Table 23. Authentication Services auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for Authentication Services
Authentication Services -Latest supported version	Authentication Services 4.2
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 — Latest supported version	Defender 5.9.6
For more information	See the Change Auditor for Defender User Guide.

EMC auditing

Table 25. 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 Celerra/VNX - Supported up to the following versions	EMC Common Event Enabler (CEE) Framework up to 8.7.0 **NOTE:** CEE requires .NET Framework 3.5 for EMC auditing. Ensure that it is installed on the computer where you have installed CEE. EMC Celerra Event Enabler (CEE) Framework 4.6.7 EMC VNX Event Enabled (VEE) Framework 4.8.5 (through 5.1) **NOTE:** VNXe is NOT supported. VNXe does not support CEPA currently and therefore Change Auditor for EMC does not run successfully in VNXe environments. **NOTE:** Starting with release 6.0.0.0, the VNX Event Enabler (VEE) is called the Common Event Enabler (CEE).
EMC Isilon - Supported up to the following versions	EMC Common Event Enabler (CEE) Framework up to 8.7.0 **NOTE:** CEE requires .NET Framework 3.5 for EMC auditing. 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 Unity 5.0.0 EMC Common Event Enabler (CEE) Framework up to 8.7.0 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.

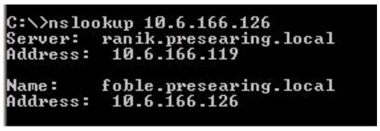
Table 25. EMC auditing requirements

Component	Supported Version
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 26. NetApp auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for NetApp
NetApp Filer	NetApp Filer with Data ONTAP 7.2 to 9.7 Cluster mode is supported as of version 8.2.1 **NOTE:** NetApp events initiated through the NFS protocol are not supported.

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’.

Required rights and permissions NetApp running in 7-mode	The provided credentials must have local **Administrator** rights on the monitored NetApp filer. You can specify these credentials in one of two ways for the Change Auditor agents assigned to the NetApp Auditing template which defines what to audit on the selected NetApp filer: • Add the Change Auditor agent service account to the local Administrators group on the NetApp filer. • Use the **Set Credentials** button on the NetApp Auditing template to specify the NetApp filer credentials to be used by the selected Change Auditor agent. If you use this method, the specified account must be an Active Directory user that is a member of the local Administrators group of the NetApp filer. **NOTE:** Enable TLS communication on the filer to allow secure communication with the Change Auditor client using the following command: options tls.enable on

Table 26. NetApp auditing requirements

Component	Supported Versions
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 that is a member of the local Administrators group of the NetApp filer. To grant ONTAPI access for the NetApp cluster for an Active Directory user, run the following command on the cluster console: security login create –vserver <vservername> -username <domain\username> -application ontapi -authmethod domain -role <rolename> Optionally, you can use the default role “vsadmin” as the rolename which has the administrator permissions of the NetApp filer. To create a new role and assign the minimum required rights, run the following commands: security login role create -vserver <vservername> -role <rolename> -cmddirname "version" -access all security login role create -vserver <vservername> -role <rolename> -cmddirname "volume" -access readonly security login role create -vserver <vservername> -role <rolename> -cmddirname "vserver fpolicy" -access all **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.
To add a new account to a NetApp filer’s local Administrators group:	1 Open Active Directory Users and Computers MMC snap-in. 2 Select the domain where the NetApp filer is located. 3 Select **Computers** from the tree and then select the filer from the list in the right pane. By default, the computer name is the same as the filer name. The actual container and the computer names are configured during CIFS setup on the filer. 4 Right-click the filer and click **Manage**. The Computer Management console opens. 5 Select **System Tools | Local Users and Groups | Groups**. 6 Double-click the **Administrators** group on the right. 7 Click **Add** to add an account to the Administrators group.
For more information	See the Change Auditor for NetApp User Guide for detailed information about installing, configuring, and using Change Auditor for NetApp.

VMware auditing

Table 27. VMware auditing requirements

Component	Supported versions
Change Auditor	Change Auditor (any license)
VMware	ESX/ESXi 5.0 to 6.0 vCenter 5.0 to 6.0
For more information	See the Change Auditor for VMWare User Guide.

SharePoint auditing

Table 28. 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 2010 SP2 SharePoint Server 2013 SP1 SharePoint Server 2016 SharePoint Server 2019 SharePoint Foundation 2010 SP2 SharePoint Foundation 2013 SP1

Table 28. SharePoint auditing requirements

Component	Supported versions
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 29. 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).
Change Auditor | Workstation agents	Change Auditor for Logon Activity Workstation
For more information	See the Change Auditor for Logon Activity User Guide.

Skype for Business auditing

Table 30. Skype for Business auditing requirements

Components	Supported Versions
Change Auditor	Change Auditor for Skype for Business **NOTE:** The Change Auditor for Lync license has been deprecated. You must obtain and import a new Change Auditor for Skype for Business license file to continue auditing Skype for Business.
Skype for Business	Microsoft Skype for Business Server 2015 Microsoft Skype for Business Server 2019 Microsoft Lync Server 2013
The SQL Server versions where the Central Management Store (CMS) is deployed	• Microsoft SQL Server 2008 SP4 • Microsoft SQL Server 2008 R2 SP3 • Microsoft SQL Server 2012 SP4 • Microsoft SQL Server 2014 SP3 • Microsoft SQL Server 2016 SP2 • Microsoft SQL Server 2017 • Microsoft SQL Server 2019 • Auditing is not supported on high availability and disaster recovery technologies such as SQL clusters and SQL Data mirroring. • Encrypted databases are not supported. • Due to some limitations on gathering logon information for SQL Server 2008 and 2008 R2, the following information may not be captured: Who and Origin.
Required rights and permissions	Each Microsoft Skype for Business Server 2015 installation requires one template assigned to the agent running on the Central Management Store (CMS) SQL Server. Ensure that the credentials for the account specified when you create a template has the following permissions: • Permission to open a connection to the CMS database. • Read permissions on CMS tables and system tables. • VIEW SERVER STATE permission. • For SQL 2012 and later: CONTROL SERVER permission and ensure that the CMS database can be opened on the target server.

Components	Supported Versions
Additional requirements	• To audit changes to security setting stored in Active Directory agents must be deployed to Active Directory domain controllers. • To audit changes to management data such as topology, configurations, and policies stored in the Central Management Store (CMS) database, agents must be deployed on the SQL server hosting the CMS. • Auditing is only supported for CMS databases in Full and Bulk logged recovery models. If the recovery model is not Full or Bulk, the transaction logs are cleaned up more aggressively and Change Auditor might not have time to capture the event resulting in missed events. An initial backup is required for both Full and Bulk logged databases before the transaction log can support auditing.
For more information	See the Change Auditor for Skype for Business User Guide.

Office 365 auditing

Table 31. Office 365 auditing requirements

Component	Supported versions
Change Auditor	Change Auditor for Exchange Change Auditor for SharePoint
Office 365 subscriptions	Change Auditor can audit the various Office 365 plans offered by Microsoft including business and enterprise subscriptions.
Windows PowerShell	Windows PowerShell version 3 on the computer where the agent is installed.
URLs	The agent configured to monitor Office 365 must be able to access the following URLs: • https://login.microsoftonline.com • https://graph.windows.net • 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 Office 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 Office 365 or Azure Active Directory 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	• For Exchange Online, the user account specified for the Auditing Configuration Account must be assigned the Exchange Administrator role. • The user account specified for the Configuration Account must be assigned the Global Administrator role. The account must also be licensed for Exchange Online (other Office 365 licenses are not required). • Change Auditor does not support accounts that have multi-factor authentication enabled. • The accounts must be sourced from Azure Active Directory. Accounts from other sources are not supported.
For more information	See the Office 365 and Azure Active Directory Auditing User Guide.

Fluid File System auditing

Table 32. Fluid File System auditing requirements

Component	Supported versions
Change Auditor	Change Auditor for Fluid File System
Dell Fluid File System supported up to the following versions	Dell Fluid File System 5.0 up to version 6.0.4 **NOTE:** Auditing is supported only for the CIFS/SMB protocol. Events initiated through the NFS or FTP protocols are not supported.

Table 32. Fluid File System auditing requirements

Component	Supported versions
Dell Enterprise Manager /Dell Storage Manager supported up to the following version	Dell Enterprise Manager version 15.3 Dell Storage Manager 18.1 and 19.1 **NOTE:** The FluidFS cluster that is going to be audited must be registered with Enterprise Manager's Data Collector service. **NOTE:** Administrator rights to Enterprise Manager are required to create, edit, delete FluidFS auditing templates in Change Auditor.
Change Auditor Configuration Service for Dell FluidFS	The Change Auditor Configuration Service for Dell FluidFS.msi is located in the Integration/FluidFS folder of the installation package. **NOTE:** The service can be installed only on 64-bit Windows 2008 R2 and later and requires Microsoft's .NET Framework 4.5.2. **IMPORTANT:** The domain of the configuration service must have a two-way trust with the domain of the auditing agent and trust the domain of the coordinator (one-way trust).
Windows PowerShell	Windows PowerShell version 4 on the computer where the Data Collector service is installed.
Agent requirements	Locate an agent close to the Dell FS8600 cluster (use fastest connection type available).

Ports	To receive events, the following ports must be open:
	• Configuration Service TCP port 9003 on the local computer where the Change Auditor Configuration Service for Dell FluidFS is installed.
	• TCP port 9004 on the agent host for inbound connections with the FluidFS cluster.
	These are default port values that are configurable.
	To change the configuration service port:
	1 Open the FluidFS.Configuration.Service.exe.config file. The default location for this file is "C:\Program Files\Quest\ChangeAuditor\FluidFS Configuration Service" where the FluidFS Configuration service is installed. Edit the port number with the following snippet in the code:
	`<appSettings>`
	`  <add key="ServicePort" value="9003"/>`
	`</appSettings>`
	2 Enter the new port in the Change Auditor FluidFS auditing template in the client by adding the name of the server followed by a colon and the port number.
	3 Refresh the agent configuration.

To change the RPC host port:

1 Change the port value using the Enterprise Manager client.

2 Save the template or run the Update-CAFluidFSConfiguration command.

The FluidFS.Configuration.Service.PowerShell module is located in the install directory of the Change Auditor Configuration Service for Dell FluidFS.

3 Refresh the agents.

Table 32. Fluid File System auditing requirements

Component	Supported versions
Encryption	If you are going to turn on encryption for auditing, the domain of the coordinator must trust the domain of the user account specified (one-way trust) during encryption configuration.
Required rights and permissions	The account used for auditing and managing your FluidFS auditing templates in Change Auditor: • Should be granted ‘Administrator’ privilege in Enterprise Manager. • Should be used to register the FluidFS cluster in Enterprise Manager.
For more information	See the Change Auditor for Fluid File System User Guide for more information about configuring and using Change Auditor for Fluid File System.

Azure Active Directory auditing

Table 33. Azure Active Directory auditing requirements

Component	Supported versions
Change Auditor	Change Auditor for Active Directory
Azure Active Directory	Change Auditor can audit the Azure Active Directory that is included with an Office 365 subscription or the Azure Active Directory Basic subscription.
URLs	The agent configured to monitor Azure Active Directory must be able to access the following URLs: • https://login.microsoftonline.com • https://graph.windows.net • https://graph.microsoft.com
Ports	• 443 (HTTPS) — for the agent to connect to the Azure Active Directory. • 8373 — for the Change Auditor coordinator service to connect to the agent computer.
Required rights and permissions	• A user account with the Global Administrator role is required for auditing configuration. The account must be sourced from Azure Active Directory. Accounts from other sources are not supported. • Change Auditor does not support accounts that have multi-factor authentication enabled.

Component	Supported versions
Synchronized environments	When auditing Azure Active Directory in a synchronized environment, Change Auditor provides more event details by mapping identities from on-premises directories with Azure Active Directory. The following conditions must be met for Change Auditor to perform the mapping: • Synchronization performed with Azure Active Directory Connect (AD Connect). • Azure AD Connect synchronization process is active in your on-premises environment and directory sync is active in your cloud environment. • An Azure Active Directory auditing 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 the Azure Active Directory. When Federation with AD FS is used as the single sign-on method, Azure 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 Active Directory User Guide.

Product licensing

As of Change Auditor 7.0 a new license key is required. Please obtain the new key before installing the new release. To obtain a new 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 Fluid File System
- 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 Skype for Business
- 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.

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, from a member server run the **autorun.exe** file to start the Quest Change Auditor autorun. See Upgrade and compatibility for more information about installing the Change Auditor components.
3. On the Install page of the autorun, click **Install** for the **Install Change Auditor Coordinator** option to start the Change Auditor Coordinator Setup wizard.
4. During the coordinator installation, you are prompted to locate the Change Auditor license files. Click **Open License Dialog** to locate and apply a license.
5. 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 7.1

- Upgrade and compatibility
- Additional resources

Upgrade and compatibility

You can upgrade to Change Auditor 7.1 from the following versions of Change Auditor: 6.0, 6.5, 6.6, 6.7, 6.8, 6.9, and 7.0.

- 6.0 through 7.0: You can upgrade directly to 7.1. 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 7.1.
- Previous versions of Change Auditor agents (6.0, 6.5, 6.6, 6.7, 6.8, 6.9, 7.0) can connect and work with the new Change Auditor coordinator.
- Change Auditor 7.1 and later agent requires Microsoft .NET Framework 4.6.2. See the Change Auditor agent (Server-side component) system requirements for the list of supported platforms.
- Change Auditor 7.0.2 and higher agents cannot connect to a coordinator version 7.0.1 or earlier. When upgrading the Change Auditor agent to 7.0.2 and higher, ensure the Change Auditor coordinator has also been upgraded to 7.0.2 and higher.
- The Threat Detection server version deployed cannot be newer than the currently deployed version of Change Auditor.
- As of Change Auditor version 7.0.4, Microsoft Graph API permissions are required for the web application to audit Office 365 and Azure Active Directory. Due to this, any existing Office 365 or Azure Active Directory templates must be updated. Office 365 and Azure Active Directory auditing will not occur if the permission requirements are not met. See the Office 365 and Azure Active Directory 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)

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 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.

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.
4 Polaris Way
Aliso Viejo, CA 92656

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

Patents

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

Trademarks

Quest, 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.**

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