Quest® Change Auditor 7.0

Release Notes

September 2018

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

About Quest Change Auditor 7.0

Change Auditor provides total auditing and security coverage for your enterprise network.

Change Auditor audits the activities taking place in your infrastructure and, with real-time alerts, delivers detailed information about vital changes and activities as they occur. Instantly know who made the change including the IP address of the originating workstation, where and when it occurred along with before and after values. Then automatically turn that information into intelligent, in-depth forensics for auditors and management — and reduce the risks associated with day-to-day modifications.

- Audit all critical changes across your enterprise including Active Directory, 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.

Change Auditor 7.0.1 is a minor release, with enhanced features and functionality. See New features.

New features

New features in Change Auditor 7.0.1:

GDPR built-in reports

- Over 190 GDPR built-in reports have been added to help you assess your GDPR compliance. See the Change Auditor Built-In Reports Reference Guide for the complete list.

SIEM tool integration improvements

- Ability to configure event forwarding to QRadar and ArcSight in the Change Auditor windows client. This is in preview mode for this release.
- Ability to modify the subsystems that have been added to an existing subscription.

Azure Active Directory auditing improvements

Role Auditing Improvements

The following improvements have been made to allow for better auditing and reporting of critical changes made to Azure Active Directory Roles.

- Role events have been moved to their own facility called "Azure Active Directory - Role"
- The following new role events have been added:
    - Azure Active Directory - Role event
    - Eligible member added to role
    - Eligible member removed from role
    - Role assigned to eligible member
    - Role assigned to eligible member
    - Role assigned to member
    - Role removed from eligible member
    - Role removed from member
- The following new role searches have been added:
    - Global Administrator role membership changes in the last 30 days
    - Role membership changes in the last 30 days grouped by role
    - Role membership changes in the last 30 days grouped by member
    - All Azure Active Directory role events in the past 7 days.

Group Auditing Improvements

The following improvements have been made to allow for better auditing and reporting of changes made to Azure Activity Directory Groups.

- The following new group events have been added:
    - Member added to group
    - Member removed from group
    - Owner added to group
    - Owner removed from group

- The following new group searches have been added:
  - Group membership changes in the last 30 days grouped by group
  - Group membership changes in the last 30 days grouped by member
  - Group owner changes in the last 30 days grouped by group
  - Group owner changes in the last 30 days grouped by owner

Additional Azure Active Directory columns

Additional columns and search options have been added to allow you to report on Azure Active Directory Activity Type and Category information.

- Additional columns added to the search Layout tab

Layout Tab	Search Column	Description
Azure - Activity Type	Activity Type	The activity resource type.
Azure - Category	Category	The activity category, such as Terms of use, Core Directory, Application Proxy, Account Provisioning, and Invited Users.

- You can now choose to refine your Azure Active Directory search by specifying Activity Type or Category.
- New searches have been added that group by Activity type and Category:
  - All Azure Active Directory events in the past 7 days by activity type
  - All Azure Active Directory events in the past 7 days by category

Active Directory auditing improvements

- Ability to audit Active Directory dynamic objects using the following custom user, group, and computer events:
  - Dynamic User Object Added
  - Dynamic User Object Changed
  - Dynamic User Object Removed
  - Dynamic Group Object Added
  - Dynamic Group Object Changed
  - Dynamic Group Object Removed
  - Dynamic Computer Object Added
  - Dynamic Computer Object Changed
  - Dynamic Computer Object Removed
- You can now choose to further refine your searches by specifying a server type on the Where tab. You can select domain controllers, member servers, Exchange servers, or workstations.
- Domain Controller Configuration facility has been renamed to Configuration Monitoring to better reflect the scope of events that are contained in this facility.
- The user display name will now be displayed in the "What" statement for group events where users are added or removed (in addition to the SAMAccount Name).
- Additional events to better track changes made to public searches and alerts:
  - Public user search created
  - Public user search deleted
  - Public user search moved
  - Public user search modified
  - Public user alert moved

- Public user alert created
- Public user alert deleted
- Public user alert modified
- Public user alert enabled
- Public user alert disabled
- Public user search folder moved
- Public user search folder renamed
- Public user search folder deleted

Additional platform support

- Active Roles 7.3
- Microsoft Exchange Server 2010 SP3 RU22
- Microsoft Exchange Server 2013 CU21
- Microsoft Exchange Server 2016 CU10
- NetApp 9.3
- GPOADmin 5.12
- CEE 8.5.1 for EMC auditing

Email alert updates

Email alerts have been updated to send alerts to the account that was changed and their manager:

- **Add Users** - When selected, alerts for user object changes are sent to the user; alerts for mailbox objects are sent to the mailbox owner.
- **Add Managers** - When selected, alerts for user object changes are sent to the user manager (if set); alerts for group objects are sent to the managed-by user (if set). Alerts for mailbox objects are sent to the owner's manager (if set).

Office 365 Exchange Online search improvements

- Administrative cmdlet searches can now be further filtered on a particular cmdlet parameter and value.

Miscellaneous enhancements and updates

- The following 'no from-value' EMC events have been added to audit security events asynchronously. Before upgrading agents that are auditing EMC Isilon, add the 'no from-value' events to all existing EMC Isilon templates.
  - EMC File Access Rights Changed (no from-value)
  - EMC File Ownership Changed (no from-value)
  - EMC Folder Access Rights Changed (no from-value)
  - EMC Folder Ownership Changed (no from-value)
- Prompt added to the SQL Auditing wizard that indicates that the -T1906 trace flag is required to audit SQL.
- Exchange Mailbox protection is supported when access is attempted from EWS or OWA clients.
- The agent install log will now be written to %ProgramFiles%\Quest\ChangeAuditor\Agent\Logs\ChangeAuditorAgentInstall.log.
- All available coordinators in the installation are listed in the Change Auditor Agent Status dialog available from the agent system tray.
- Help button added the auditing template wizards.
- Searches will have the search name as the file name when they are exported. The file name will no longer be a GUID.

- Multi-forest support for object selection.
    - In the Windows client, you can now select objects from more than one forest for:

      - Coordinator configuration (SMTP, shared folder, and group membership)

      - Purge and archive jobs

      - Active Directory, AD Query, ADAM (AD LDS), Exchange, and group policy searches
    - In the web client, you can now select objects from more than one forest for:

      - Coordinator configuration (SMTP and group membership)

      - Purge and archive jobs

      - Active Directory, AD Query, ADAM (AD LDS), Exchange, and group policy searches

Important information

The following is a list of important information for this release.

- **As of Change Auditor 6.x high-performance database**: With Change Auditor 6.x's new 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 6.x 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.
- **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 2010 client access role: failed agent upgrade, unwanted RpcClientAccess service restart, or unscheduled Exchange cluster node failover.
    - Exchange 2013 mailbox role: failed agent upgrade, unwanted RpcClientAccess service restart, or unscheduled Exchange cluster node failover.
    - Exchange 2010 or 2013 client access role: unwanted IIS Exchange application pool restarts.
    - Exchange 2016 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 2008/2012**: By default, File and Printer sharing are not enabled on Windows Server 2008/2012 installations. To remotely install agents to Windows Server 2008/2012 (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
  ```

- **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.

- **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.
- **"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.
- 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 article http://support.microsoft.com/kb/232199, 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 2010/2013 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
Invalid credentials error displayed when using properly configured account for Shared Folder Configuration and testing access.	23666
Invalid credentials error when using properly configured account to save scheduled reports to a shared folder.	23691
Exchange Server 2016 CU10 support.	25355
Outlook connectivity issues are seen when the Change Auditor agent is running on the Exchange server and MAPI over HTTP is enabled.	27526
Active Directory event processing may be delayed due to name resolution when processing a large number of events.	27696
Mailbox protection is supported when access is attempted from an EWS client.	26965
Mailbox protection is supported when access is attempted from an OWA client.	26964
NetApp 9.3 support.	24818
The initiator is incorrectly reported in the Change Auditor event when a deprovisioned object is undone through Active Roles.	25900
Exchange 2010 RU22 support.	26877
Exchange 2013 CU21 support.	25354
Agents do not capture Active Directory group membership changes on Windows 2016 when using the "net group" command.	25352
Unable to send events to SIEM tools through event subscriptions if Change Auditor has been upgraded from a previous version.	24309
Exchange Server 2013 CU20 support.	22194
Exchange Server 2010 RU20 support.	22193
Security updates are slow on EMC when files or folders are audited for changes to access rights or ownership. To resolve this, new 'no from-value' events have been added that allow you to audit security events asynchronously. **NOTE:** Before upgrading agents that are auditing EMC Isilon, add the 'no from-value' events to all existing EMC Isilon templates.	23951
Exchange PowerShell auditing may cause the agent to consume excessive memory when large or complex PowerShell scripts are run on Exchange.	24560

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
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 2008 R2 or 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
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.	

Table 2. General known issues

Known issue	Issue ID
Conflict with McAfee HIPS and Change Auditor agent causing server reboots: McAfee 8.0 HIPS causes a hang 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. Contact Quest Technical Support for detailed instructions.	
Junction point monitoring: Junction point creation may fail on a server with both the Symantec Backup Exec™ CPS Agent version 12.0 and the Change Auditor agent. **Workaround:** To resolve the problem, upgrade CPS Agent to 12.5 or later.	
Client CPU usage: Client CPU usage on Windows Server 2008 is dramatically increased when grouping columns by Agent Status on the Deployment tab during agent deployment operations.	
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
Multiforest 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 in a MultiForest setup and when using a SQL account with minimal permissions. In a multiforest coordinator configuration where each coordinator uses the same Change Auditor database using a SQL account with limited permissions for the database connection. 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.” Do the following if this error is displayed: ***Run the 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).	
Exchange 2010 - Missing Exchange events from OWA (Outlook Web Access): If the OWA functionality is being hosted from a server different than an Exchange Server that has an agent installed, the server running OWA needs an agent to be installed as well. OWA Mailbox events are generated through the IIS service and therefore an agent is needed for their collection. The following are the events that would not be audited for users connecting through an OWA server without an agent: • Appointment Read by Non-Owner • Appointment Read by Owner • Calendar Opened by Non-Owner • Calendar Opened by Owner • Contact Read by Non-Owner • Contact Read by Owner • Contacts Opened by Non-Owner • Contacts Opened by Owner • Inbox Opened by Non-Owner • Inbox Opened by Owner • Mailbox Opened by Non-Owner • Mailbox Opened by Owner • Message Read by Non-Owner • Message Read by Owner • Task Read by Non-Owner • Task Read by Owner • Tasks Opened by Non-Owner • Tasks Opened by Owner	
Exchange 2010 - Mailbox events may show incorrect path names: Occasional incomplete folder path names in Exchange Mailbox events have been reported by a few users. The events are otherwise accurate.	
OWA protection: If protection is enabled while a user already has an active OWA session on the newly protected mailbox, protection does not prevent the user from deleting the items in the active folder. New OWA sessions established after protection is enabled are properly protected.	
Missing Exchange event detail: Some Exchange Active Directory changes that are detected on domain controllers may be reported with missing information. To capture this detail, add the Domain Controllers group to the Exchange View-Only Administrators group.	

Table 5. Change Auditor for Exchange known issues

Known issue	Issue ID
Exchange 2010/2013/2016 scripting extensions: When a Change Auditor 5.6 (or higher) agent is deployed on Exchange Server 2010/2013/2016, 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 2010/2013: There is a known issue with Microsoft Exchange 2010/2013 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. There is a fix available by calling Microsoft Support (1-800-Microsoft) and requesting the fix. See this Technet post for details: http://social.technet.microsoft.com/Forums/en-US/exchange2010/thread/352776de-ab8a-400f-9f09-fb13cfa89f52/	
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

Table 6. Change Auditor for NetApp known issues

Known issue	Issue ID
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
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 7. Change Auditor for SQL Server known issues

Known issue	Issue ID
Auditing events on SQL Server 2008 SP1 Update 5 (or higher): Due to a hotfix Microsoft released for SQL Server 2008 SP1 Update 5 (or higher), Change Auditor agents no longer capture SQL-related events unless the following action is taken on the SQL Server: • **SQL Server 2008:** Using SQL Server Configuration Manager, add the string ";-T1906" to the end of the SQL Server Startup Parameters on the Advanced tab in the SQL Server Properties dialog. • **SQL Server 2012 and newer:** 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.** See this article for more information: http://blogs.msdn.com/b/joaol/archive/2009/09/30/sql-server-2008-does-not-start-after-sp1-with-etw-enabled.aspx	
Due to some limitations on gathering login information for SQL Server 2008 and 2008 R2, the following information may not be captured: • Origin • Application name • Who (Login user)	445996

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

System requirements

Before installing Change Auditor 7.0, ensure that your system meets the following minimum hardware and software requirements.

- Change Auditor coordinator (Server-side component)
- Change Auditor client (Client-side component)

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

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

Change Auditor coordinator (Server-side component)

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

Table 11. Coordinator requirements

Requirement	Details
Processor	Quad core Intel Core i7 equivalent or better
Memory	Minimum: 8 GB RAM or better Recommended: 32 GB RAM or better
SQL database supported up to the following versions	• Microsoft SQL Server 2008 R2 SP3 • Microsoft SQL Server 2012 SP4 • Microsoft SQL Server 2014 SP2 • Microsoft SQL Server 2016 SP1 • Microsoft SQL Server 2017 **NOTE:** Change Auditor supports SQL AlwaysOn Availability Groups and SQL Clusters.
Installation platforms (x64) supported up to the following versions	• Windows Server 2008 R2 SP1 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 **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:** 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 4.6.1 • 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 12. Coordinator minimum permissions

Account	Minimum permissions
User account performing the coordinator installation	The user account that is installing the coordinator requires the appropriate permissions to perform the following tasks on the target server: • Windows permissions to create and modify registry values. • Windows administrative permissions to install software and stop and start services. **NOTE:** The user account performing the installation, must be a member of the **Domain Admins** group in the domain where the coordinator is being installed.
Service account running the coordinator service (LocalSystem by default)	The service account running the coordinator service must have the following permissions: • Active Directory permissions to create and modify SCP (Service Connection Point) objects under the computer object that is running the Change Auditor coordinator. • Local Administrator permissions on the coordinator server. **NOTE:** If you are running the coordinator under a service account (instead of LocalSystem), use a Manual connection profile that specifies the IP address of the server hosting the Change Auditor coordinator whenever you start the client. See the Change Auditor User Guide or online help for more information about defining and selecting a connection profile.
SQL Server database access account specified during installation	An account must be created to be used by the coordinator server on an ongoing basis for access to the SQL Server database. This account must have a **SQL Login** and be assigned the following SQL permissions: • Must be assigned the **db_owner** role on the Change Auditor database • Must be assigned the SQL Server role of **dbcreator** **NOTE:** If you are using AlwaysOn Availability Groups and SQL server authentication the SQL Login account must be assigned the sysadmin role on every SQL server in the Availability Group.

Change Auditor client (Client-side component)

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

Table 13. Client requirements

Requirement	Details
Processor	Dual core Intel Core i5 equivalent or better
Memory	Minimum: 4 GB RAM or better Recommended: 8 GB RAM or better
Installation platforms (x64) supported up to the following versions	• Windows Server 2008 R2 SP1 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows 7 • Windows 8 and 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 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 14. 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 14. Agent requirements

Requirement	Details
Installation platforms (x64) supported up to the following versions	• Windows Server 2008 R2 SP1 • Windows Server 2008 R2 Core SP1 • Windows Server 2012 • Windows Server 2012 Core • Windows Server 2012 R2 • Windows Server 2012 R2 Core • Windows Server 2016 Server Core • Windows Server 2016 **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:** Starting with Change Auditor 6.9, the Change Auditor agent cannot be installed on the following Operating Systems: Windows 2003 SP2, Windows 2003 R2, or Windows 2008 SP2. During an agent install, if one of these operating systems is detected, the latest version of the agent that supports the operating system is installed. After the deployment, you will see a previous version of an agent in the Version cell if you installed the agent on an unsupported platform. **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:** **Change Auditor agent requires File and Printer Sharing on Windows Server 2008 R2.** By default, File and Printer sharing are not enabled on Windows Server 2008 R2installations. To remotely deploy agents to Windows Server 2008 R2, 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 must also be enabled for remote deployment. **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 4.5.2
	• 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 14. Agent requirements

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

Table 15. Agent minimum permissions

Account	Permissions
User account deploying agents	The Agent Deployment wizard runs under the security context of the currently logged on user account. Therefore, you must have administrative authority to install software on every target machine. This means you must be a **Domain Admin** in every domain that contains servers that you are targeting for installation. If you are targeting domain controllers only, membership in the **Enterprise Admins** group grants you authority to all domain controllers in the forest. In addition, all users responsible for deploying Change Auditor agents must also be a member of the ChangeAuditor Administrators group in the specified ChangeAuditor installation. If you are not a member of this security group for this installation, you get an access denied error.
System account running on agent	Change Auditor agents must run as Local System.

Change Auditor workstation agent (optional component)

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

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

Table 16. Workstation agent requirements

Requirement	Details
Processor	Dual core Intel Core i5 equivalent or better
Memory	Minimum: 2 GB RAM or better Recommended: 4 GB RAM or better
Installation platforms supported up to the following versions	• Windows 7 SP1 (Pro, Enterprise and Ultimate) • Windows 8 and 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 4.5.2 (or higher) • 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 7, Windows 8/8.1, 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 17. 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 2008 R2 SP1 with Application Server and Web Server roles • Windows Server 2012 with Application Server and Web Server roles • Windows Server 2012 R2 with Application Server and Web Server roles • Windows Server 2016
Software and configuration	• x64 version of Microsoft's .NET 4.6.1 • x64 version of Microsoft XML Parser (MSXML) 6.0 • x64 version of Microsoft SQLXML 4.0
Browsers supported up to the following versions	• Chrome 59 • Edge 38 • Firefox 54 • 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 18. IT Security Search requirements

Component	Supported Versions
IT Security Search	IT Security Search 11.3

Auditing requirements

Table 19. Exchange Server auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for Exchange
Exchange Servers supported up to the following versions	Windows Server 2008 R2 SP1 • Microsoft Exchange Server 2010 SP3 RU22 • Microsoft Exchange Server 2013 CU21 Windows Server 2012 • Microsoft Exchange Server 2010 SP3 RU22 • Microsoft Exchange Server 2013 CU21 • Microsoft Exchange Server 2016 CU10 Windows Server 2012 R2 • Microsoft Exchange Server 2013 CU21 • Microsoft Exchange Server 2016 CU10 Windows Server 2016 • Microsoft Exchange Server 2016 CU10 **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 for information about using Change Auditor for Exchange.

Table 20. SQL Server auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for SQL Server
SQL Servers supported up to the following versions	• Microsoft SQL Server 2008 SP4 • Microsoft SQL Server 2008 R2 SP3 • Microsoft SQL Server 2012 SP3 • Microsoft SQL Server 2014 SP2 • Microsoft SQL Server 2016 SP1 **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.
For more information	See the Change Auditor for SQL Server User Guide for information about using Change Auditor for SQL Server.

Table 21. SQL Server Data Level auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for SQL Server
SQL Servers supported up to the following versions	• Microsoft SQL Server 2008 SP4 • Microsoft SQL Server 2008 R2 SP3 • Microsoft SQL Server 2012 SP4 • Microsoft SQL Server 2014 SP2 • Microsoft SQL Server 2016 SP1 • Microsoft SQL Server 2017 **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:** Due to some limitations on gathering login information for SQL Server 2008 and 2008 R2, the following information may not be captured: • Origin • Application Name • Who (Login user) **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:** 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. Ensure that the credentials for the Windows authentication or SQL Server account specified when you create a template has the sysadmin server role.
For more information	See the Change Auditor for SQL Server User Guide for information about using Change Auditor for SQL Server.

Table 22. Authentication Services auditing requirements

Component	Supported Versions
Change Auditor	Change Auditor for Authentication Services
Authentication Services -Latest supported version	Authentication Services 4.1

Table 23. Defender auditing requirements

Components	Supported Versions
Change Auditor	Change Auditor for Defender
Defender — Latest supported version	Defender 5.8.2

Table 24. 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 8.5.1 **NOTE:** CEE requires .NET 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	EMC Common Event Enabler (CEE) Framework up to 8.4 **NOTE:** CEE requires .NET 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	EMC Unity 4.1.0 EMC Common Event Enabler (CEE) Framework up to 8.4 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**.
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.

Table 25. NetApp auditing requirements

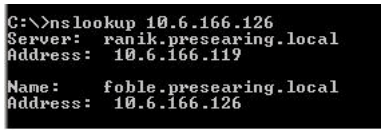
Component	Supported Versions
Change Auditor	Change Auditor for NetApp
NetApp Filer	NetApp Filer with Data ONTAP 7.2 to 9.3 Cluster mode is supported as of version 8.2.1 **NOTE:** NetApp events initiated through the NFS protocol are not supported.
Agent	• Locate a Change Auditor agent close to the NetApp 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:  • If Windows Firewall is enabled on the server hosting the Change Auditor agent responsible for capturing the NetApp events, it must be configured to allow 'File sharing'.
Rights and permissions NetApp running in 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 25. 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.

Table 26. 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

Table 27. 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 the environment of the similar 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 Foundation 2010 SP2 SharePoint Foundation 2013 SP1
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.

Table 28. 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

Table 29. 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 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 SP2 • Microsoft SQL Server 2016 SP1 • 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.
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. • 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. • 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 for more information about Exchange Online auditing.

Table 30. 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
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 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.

Table 31. 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 version 5.0 Dell Fluid File System version 6.0 **NOTE:** Auditing is supported only for the CIFS/SMB protocol. Events initiated through the NFS or FTP protocols are not supported.

Table 31. 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 version 16.3 **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 .NET 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 31. 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.

Table 32. 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 agent computer.
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.

Table 32. Azure Active Directory auditing requirements

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 for more information about Azure Active Directory auditing.

Product licensing

This new release of Change Auditor requires a new license key. Please obtain the new key before installing the new release. To obtain a new key, refer to the License Key Upgrade page: https://support.quest.com/my-account/licensing.

NOTE: You will need your current license numbers. 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 code is the same for all and 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 Authentication Services
- Change Auditor for Defender
- 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 in 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 7.0

- Upgrade and compatibility
- Additional resources

Upgrade and compatibility

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

- 6.0 through 6.9: You can upgrade directly to 7.0. 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 7.0.
- 5.9 and below: Upgrade to 6.8 first and wait for all 5.x events to upgrade before proceeding with upgrade to 7.0.
- Previous versions of Change Auditor agents (5.8, 5.9, 6.0, 6.5, 6.6, 6.7, 6.8, and 6.9) can connect and work with the new Change Auditor coordinator.
- The Change Auditor 7.0 agent requires .NET 4.5.2. See the Change Auditor agent (Server-side component) system requirements for the list of supported platforms.
- Starting with Change Auditor 6.9, the Change Auditor agent cannot be installed on the following Operating Systems: Windows 2003 SP2, Windows 2003 R2, or Windows 2008 SP2. During agent install, if one of these operating systems is detected, the latest version of the Change Auditor agent that supports the operating system is installed.

For example, when you upgrade a 6.7 agent with Change Auditor 7.0 on a Windows 2012 server, the 7.0 agent is deployed. When you upgrade a 6.7 agent with Change Auditor 7.0 on a Windows 2008 SP2 server, the upgrade is to the latest 6.8 agent.

If you are upgrading a 6.8 agent on an unsupported platform, the agent is upgraded to a newer 6.8 agent if it determines that the deployed agent is older than the 6.8 agent that is included with this version.

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/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

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

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.

Legend

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

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