Quest® Change Auditor 7.4

What’s New

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

Quest Software Inc.
Attn: LEGAL Dept.
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 Software, Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

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

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

Change Auditor What's New
Updated - November 2023
Software Version - 7.4

Contents

What's New in Change Auditor 7.4

As a result of ongoing research and development, and in response to customer feedback, the following enhancements have been made in this release of Quest Change Auditor.

- Support for modern authentication
- PowerShell enhancements
- Performance improvements
- Integration with Quest Security Guardian
- Additional platform support
- Miscellaneous features and enhancements

Support for modern authentication

- Ability to configure email alerts to be sent using Microsoft 365.
- Additional associated internal events:
  - Microsoft 365 Mail Alert Failed
  - Microsoft 365 Mail alerting Azure Directory Name changed
  - Microsoft 365 Mail alerting enabled
  - Microsoft 365 Mail alerting disabled
  - Microsoft 365 Mail alerting web application ID changed
  - Microsoft 365 Mail alerting web application key changed
  - Microsoft 365 Mail alerting web application successfully created
  - Microsoft 365 Mail alerting web application failed to be created

PowerShell enhancements

- Ability to manage GPO Protection using the following PowerShell commands:
  - New-CAGPOProtectionTemplate
  - Get-CAGPOProtectionTemplates
  - Set-CAGPOProtectionTemplates
  - Remove-CAGPOProtectionTemplate
- Internal events are generated when managing Active Directory protection templates using PowerShell commands.
- Get-CASearchDefinition command will now export the email addresses configured on the alert and report tabs of a search.

Performance improvements

- Event sending for SIEM subscriptions will now fail-over between available coordinators when an allowed coordinator can no longer communicate with the SIEM appliance.
- Improved performance when reading agent configuration.
- Improved performance when processing Azure events.
- Added retry logic to agent installations when an issue, such as a locked file, is encountered.

Integration with Quest Security Guardian

Security Guardian is an integrated On Demand solution that enables you to manage Tier Zero assets and identify vulnerabilities in your organization's Active Directory to help you keep it secure. If Change Auditor version 7.4 is integrated with Security Guardian, you can protect Tier Zero objects from unauthorized or accidental modifications or deletions by creating Change Auditor protection templates from the Security Guardian interface.

Additional platform support

The following support has been added:

- Windows 11 (Pro and Enterprise for workstation agents and client installations)
- Integration with Active Roles 8.1
- NetApp 9.13 auditing
- Integration with GPOADmin 5.18
- Microsoft Exchange Server 2019 CU13
- Microsoft SQL Server 2022 for coordinator database and as an auditing target
- EMC Common Event Enabler (CEE) Framework 8.9.8.2

The following support has been removed:

- Windows 8.1
- Windows Server 2012 and 2012 R2
- Exchange 2013
- SharePoint 2013
- Removal of the Change Auditor SCOM management pack
- FluidFS auditing
- Autorun

Miscellaneous features and enhancements

- Ability to allow a Group Managed Service Account (GMSA) as an override account for Group Policy, Exchange Mailbox, and File system protection templates.
- Ability to manage and update foreign forest agent credentials from the Deployment tab.
- Refresh GPOs list to include "Enterprise" scope GPO protection so that a newly added GPOs are protected.
- Updated list of columns published to SQL Reporting Services

2

What’s New in Change Auditor 7.3

As a result of ongoing research and development, and in response to customer feedback, the following enhancements have been made in this release of Quest Change Auditor.

- SQL Extended Events auditing (Preview)
- Active Directory Database auditing enhancements
- Active Directory Database protection enhancements
- Event forwarding to Microsoft Sentinel
- Security improvements
- Logon Activity auditing enhancements
- PowerShell improvements
- Subscription failover support
- Additional platform support
- Miscellaneous features and enhancements

SQL Extended Events auditing (Preview)

Ability to audit SQL Extended events using the following PowerShell commands:

- Get-CASQLExtendedEventsInfo
- New-CASQLExtendedEventsFilter
- New-CASQLExtendedEventsObject
- New-CASQLExtendedEventsTemplate
- Get-CASQLExtendedEventsTemplates
- Remove-CASQLExtendedEventsTemplate

The following events are audited:

- SQL Server Admin Extended Event
- SQL Server Analytic Extended Event
- SQL Server Operational Extended Event

The following internal events are available:

- SQL Extended Events auditing template added
- SQL Extended Events auditing template deleted

The following built-in searches are available:

- All SQL Extended Events in the last 24 hours

- All SQL Operational Extended Events in the last 24 hours
- All SQL Analytic Extended Events in the last 24 hours
- All SQL Admin Extended Events in the last 24 hours

Active Directory Database auditing enhancements

Ability to manage Active Directory Database auditing using the following PowerShell commands:

- New-CAADDatabaseTemplate
- Get-CAADDatabaseTemplates
- Remove-CAADDatabaseTemplate
- Set-CAADDatabaseTemplate

Active Directory Database protection enhancements

Ability to manage Active Directory Database auditing using the following PowerShell commands:

- New-CAADDProtectionTemplate
- Get-CAADDProtectionTemplates
- Remove-CAADDProtectionTemplate
- Set-CAADDProtectionTemplate

Event forwarding to Microsoft Sentinel

- Ability to configure the integration through the Windows client and PowerShell commands.
- Ability to manage the integration using the following PowerShell commands:
    - New-CASentinelEventSubscription
    - Get-CASentinelEventSubscriptions
    - Set-CASentinelEventSubscription
    - Remove-CASentinelEventSubscription
- Internal events are available to track changes to the subscription:
    - Microsoft Sentinel subscription added
    - Microsoft Sentinel subscription modified
    - Microsoft Sentinel subscription removed

Security improvements

- The following event is generated when the encryption level used by Kerberos service ticket requests do not meet the expected level of security: A Kerberos service ticket was created with an unsafe encryption type.
- The following built-in search is available:
  - All Kerberos service ticket events for unsafe encryption type in the last 7 days.

Logon Activity auditing enhancements

- Ability to include and exclude events performed by users with the Administrator right in search results by filtering on the“Is Administrator” column.
- The following built-in search is available:
  - All Logons by administrators in the past 24 hours.

PowerShell improvements

Commands have been added to:

- Import and export the Change Auditor configuration.
  - Import-CAConfigurations
  - Export-CAConfigurations
- Manage Active Directory protection templates.
  - Remove-CAProtectedObject
  - Set-CAADProtectionTemplate

Subscription failover support

If a coordinator detects that the event sending to a SIEM subscription has been consistently failing for a specified period of time, it will try another coordinator that has been configured to send events to a SIEM tool. If the second coordinator successfully sends events to the SIEM subscription, it will continue performing the task.

Additional platform support

The following support has been added:

- Microsoft Exchange Server 2016 CU23
- Microsoft Exchange Server 2019 CU12
- Microsoft SQL Server 2016 SP3
- Windows Server 2022 for auditing on all subsystems
- Windows 10 Enterprise for Virtual Desktops for workstation agents
- Active Roles 7.5.1, 7.6, and 8.0
- NetApp ONTAP 9.9 and 9.10

- GPOADmin 5.17
- EMC Common Event Enabler (CEE) Framework 8.9.7.1

The following support has been removed:

- SQL Server 2012 for the coordinator and auditing
- Internet Explorer 11
- Ability to publish to the Quest Knowledge portal

Miscellaneous features and enhancements

- Ability to ignore GPOADmin working copies in Group Policy protection templates and the addition of the following associated internal events:
    - Do not enforce protection for GPOADmin working copy option disabled.
    - Do not enforce protection for GPOADmin working copy option enabled.
- Ability to globally protect all GPO links unless change comes from an override account.
- Additional internal events generated when a coordinator is unable to send events to a SIEM subscription:
    - Event forwarding subscription disabled due to webhook receiver error.
    - Event forwarding suspended due to webhook error.
    - Event forwarding has resumed.
- Additional logging when a foreign agent is unable to connect to the coordinator.
- Additional support in the Windows client for accessibility tools such as screen readers.
- Updated import and export functionality to support certificate authentication in Office 365 templates.
- Performance improvements to the purge process.
- Delete events are recorded for each object contained in an OU when the "Use Delete Subtree server control" option is selected when deleting an OU.

3

What’s New in Change Auditor 7.2

As a result of ongoing research and development, and in response to customer feedback, the following enhancements have been made in this release of Quest Change Auditor.

- Cyber security enhancements
- Certificate authentication for Office 365
- Active Directory Federation Services auditing enhancements
- Foreign forest support
- Additional events
- Additional platform support
- Miscellaneous features and enhancements

Cyber security enhancements

Additional Active Directory events and built-in searches that can be used as indicators of possible cyber security attacks.

- The following events have been added:
  - Different domain SID added to user object sIDHistory
  - Different domain SID removed from user object sIDHistory
  - Well-known SID added to user object sIDHistory
  - Well-known SID removed from user object sIDHistory
  - Same domain SID added to user object sIDHistory
  - Same domain SID removed from user object sIDHistory
  - Different domain SID added to group object sIDHistory
  - Different domain SID removed from group object sIDHistory
  - Well-known SID added to group object sIDHistory
  - Well-known SID removed from group object sIDHistory
  - Same domain SID added to group object sIDHistory
  - Same domain SID removed from group object sIDHistory
  - adminCount attribute changed on Computer object
  - adminCount attribute changed on User object
  - adminCount attribute changed on Group object
  - ServicePrincipalName removed from user object
  - ServicePrincipalName added to user object

- Irregular domain controller registration activity detected. This event could identify a possible DCShadow threat. DCShadow is a command within Mimikatz that simulates the behavior of a domain controller to push changes to an Active Directory domain through replication, bypassing most of the common security controls.

- The following searches have been added:
  - Users SIDHistory changed in the last 30 days search
  - Users high severity SIDHistory changed in the last 30 days search
  - Group SIDHistory changed in the last 30 days search
  - Group high severity SIDHistory changed in the last 30 days search
  - AdminCount changed on user in the last 30 days search
  - AdminCount changed on group in the last 30 days search
  - AdminCount changed on computer in the last 30 days search
  - Users servicePrincipalName changed in the last 30 days search
  - All Irregular Domain Controller Registration events in the last 7 days search
- Ability to create an Active Directory protection template and select a root domain object to prevent users from linking GPOs.

Certificate authentication for Office 365

Due to the fact that basic authentication has been deprecated by Microsoft for Office 365 Exchange Online, certificate authentication is now required for Office 365 auditing. Newly created auditing templates and the associated web application will have the required permissions and certificate. However, If you are using an existing web application, you will need to provide a certificate and ensure that it has the required permissions. See the Change Auditor Office 365 and Azure Active Directory Auditing User Guide for details.

NOTE: Microsoft's .NET Framework 4.7.1 is required for Office 365 auditing templates in the Windows client or through PowerShell commands.

The following events have also been added:

- Azure Active Directory web application certificate created
- Office 365 auditing web application certificate changed

Active Directory Federation Services auditing enhancements

New Active Directory Federation Services - Endpoints events:

- Endpoint enabled
- Endpoint disabled
- Endpoint Proxy enabled
- Endpoint Proxy disabled

New Active Directory Federation Services - Server Farm events:

- Server Farm Node added
- Server Farm Node Primary Computer Name changed

- Server Farm Node Primary Computer port changed
- Server Farm Node removed
- Server Farm Node Role changed
- Server Farm Node Synchronization Frequency changed

New Active Directory Federation Services - Claims Provider Trust events:

- Claims Provider Trust added
- Claims Provider Trust deleted
- Claims Provider Trust enabled
- Claims Provider Trust disabled
- Claims Provider Trust changed

New built-in searches:

- All Authentication Method events in the last 30 days
- All Relying Party Trust events in the last 30 days
- All Endpoint events in the last 30 days
- All Claims Provider Trust events in the last 30 days

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 select objects in a foreign forest in the Exchange protection wizard.
- Ability to select objects in a foreign forest in the Group Policy protection wizard.
- Users are notified in the client when the foreign forest cannot be contacted when performing a “Force Refresh”.
- Support for foreign forest objects in the Add-CASearch and Set-CASearchProperties commands.

Additional events

Events to audit when a change is made to the coordinators selected for purge, archive or report jobs:

- Coordinator added to scheduled task processing
- Coordinator removed from scheduled task processing
- Scheduled task processing assignment changed
- Scheduled task processing setting changed

Events to audit failed client logons:

- Change Auditor unknown client logon failed
- Change Auditor Windows client logon failed
- Change Auditor web client logon failed
- Change Auditor PowerShell client logon failed

Events to audit changes to the “Inheritance” option on the security tab for Active Directory objects:

- Inheritance setting changed on computer object

- Inheritance setting changed on group object
- Inheritance setting changed on user object
- Inheritance setting changed on AdminSDHolder object
- Inheritance setting changed on OU object
- Inheritance setting changed on group policy object

Internal events are now generated when changes are made to file system templates through PowerShell commands. Previously these events were only generated when changes were made through the Windows client.

Additional platform support

The following support has been added:

- Microsoft Exchange Server 2016 CU19, CU20, CU21, and CU22
- Microsoft Exchange Server 2019 CU8, CU9, CU10, and CU11
- Windows Server 2022 for Active Directory, Registry, Group Policy, Service, Local Account, AD Query, Logon Activity, and ADFS auditing
- Windows 11 for client installations
- CEE 8.7.8.2 for EMC auditing
- One Identity Defender 5.11
- Active Roles 7.4 and 7.5
- Authentication Services 5.0 and 5.0.1
- NetApp 9.8
- GPOADmin 5.16

The following support has been removed:

- NetApp auditing on 7-Mode servers
- NetApp cluster mode auditing on servers older than 8.1
- Windows Serve Core 1809, 1903, 1909
- Auditing of SharePoint 2010
- Auditing of VMware. Note that auditing will still be supported with 7.1.1 (and older) agents.

Miscellaneous features and enhancements

- Update to the label on the SIEM and On Demand Audit event subscription pages to indicate that “Last event time” is show in UTC time.
- Performance improvements in sending of events to Splunk.
- Added the email address and the “managed by” property of a user as new columns available for searches. Additional associated email tags are also available: %AD_USERMAIL% and %AD_MANAGEDBY%.
- Performance improvements made to the process of retrieving the site information when doing a topology scan in environments that have a large number of subnets.

4

What’s New in Change Auditor 7.1.1

As a result of ongoing research and development, and in response to customer feedback, the following enhancements have been made in this release of Quest Change Auditor.

- Additional Office 365 Exchange Online mailbox events
- Enhanced security auditing
- Search enhancements
- SIEM tool integration improvements
- Ability to audit and protect the Active Directory Database
- Ability to audit Active Directory Federation Services
- Foreign forest support
- Additional platform support
- Miscellaneous features and enhancements

Additional Office 365 Exchange Online mailbox events

The following events have been added:

- 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.
- 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:

> ℹ **NOTE:** A Change Auditor Logon Activity license is required to capture the sign-in events; 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.

5

What’s New in Change Auditor 7.1

As a result of ongoing research and development, and in response to customer feedback, the following enhancements have been made in this release of Quest Change Auditor.

- Azure Active Directory and Office 365 updates
- Active Directory updates
- Foreign forest support
- On Demand Audit integration updates
- Authentication and Logon activity updates
- Additional platform support
- Miscellaneous features and enhancements

Azure Active Directory and Office 365 updates

- Change Auditor has implemented the updated Microsoft graph API which has resulted in the following additional built-in reports for risky events:
    - All Azure Active Directory sign-in from anonymous IP address events in the past 7 days
    - All Azure Active Directory sign-in from confirmed compromised user events in the past 7 days
    - All Azure Active Directory sign-in from IP address with malicious activity events in the past 7 days
    - All Azure Active Directory sign-in from IP address with suspicious activity events in the past 7 days
    - All Azure Active Directory sign-in from malware-infected device events in the past 7 days
    - All Azure Active Directory sign-in with impossible travel events in the past 7 days
    - All Azure Active Directory sign-in with valid credentials from blocked IP address events in the past 7 days
    - All Azure Active Directory sign-in with unfamiliar location or properties events in the past 7 days
    - All Azure Active Directory suspicious manipulation or rules in user's inbox events in the past 7 days
    - All Azure Active Directory user activity with known sign-in attack pattern events in the past 7 days
    - All Azure Active Directory user activity with known attack pattern events in the past 7 days
    - All Azure Active Directory unlikely travel between sign-in source locations events in the past 7 days
    - All Azure Active Directory users sign-in with leaked credentials events in the past 7 days
- Increased performance of Azure Active Directory auditing allowing for more events to be processed.
- Office 365 auditing page now displays whether SharePoint Online and OneDrive for Business events are being monitored.

- Office 365 event details Item tab added that displays Id, rights, SID, Upn, name and path details for Exchange Online permission additions, removals, or modifications.
- Additional Info tab added for Azure Active Directory risky events that displays information such as user agent, related event time in UTC, related user agent, device information, related location, request ID, correlation ID.
- Ability to set whether or not mailbox auditing settings specified in the auditing template overwrite the existing mailbox auditing settings specified in the Office 365 tenant.
- Ability to create a custom Azure Active Directory search based on location.

Active Directory updates

- Ability to audit changes to Active Directory temporary groups where the members have a specified time to live. The time to live for each member is also reported in the event.
- Ability to allow Managed Service Accounts to access protected Active Directory objects.

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 harvest the foreign forest topology.
- Ability to deploy agents through the Change Auditor client.
- Ability to audit logon activity with an agent in the foreign forest.
- Ability to audit and protect Windows File System with an agent in the foreign forest.
- Ability to audit and protect Active Directory objects with an agent in the foreign forest.
- Ability to audit Active Directory attributes with an agent in the foreign forest.
- Ability to select objects from the foreign forest in object pickers for search queries.
- Ability to include and exclude objects from the foreign forest in AD queries.

On Demand Audit integration updates

- Ability to send the Change Auditor version and list of coordinators to On Demand Audit after an upgrade so that On Demand Audit can display the most current Change Auditor information.
- New events generated when event forwarding to On Demand Audit is suspended due to an error and then resumed:
  - On Demand Audit subscription has suspended
  - On Demand Audit subscription has resumed
- New events generated when an On Demand administrator makes changes to the Change Auditor event forwarding settings within On Demand Audit:
  - Event sending to On Demand Audit paused
  - Event sending to On Demand Audit resumed
  - On Demand Audit configuration removed
- New event generated when Change Auditor connects to On Demand Audit:

  - On Demand Audit configuration added

Authentication and Logon activity updates

- Additional events:
  - User performed a successful NTLM V1 logon is created when a user successfully logged into a server through NTLM V1.
  - User performed a successful NTLM V2 logon is created when a user successfully logged into a server through NTLM V2.
  - User authenticated through NTLM (or User failed to authenticate through NTLM) is created when a user successfully authenticates (or fails to authenticate) to a domain controller using NTLM authentication.
- Additional built-in searches:
  - All Kerberos Authentication Activity in the past 24 hours
  - All NTLM Authentication Activity in the past 24 hours
  - All NTLM version 1 logons in the last 7 days
- Ability to search logon events by the failure reason or status code.
- Ability to set Kerberos ticket lifetime in agent configuration and detect possible golden ticket use. When a Kerberos ticket lifetime that exceeds the value specified in the agent configuration is detected, the "Kerberos user ticket that exceeds the maximum lifetime detected" domain controller authentication event is generated. A valid Change Auditor Logon Activity User license is required.

Additional platform support

The following support has been added:

- Windows Server Core 1909 (Active Directory, Windows File System, Registry, Services, and Local User and Group auditing only)
- Microsoft Exchange Server 2016 CU15
- Microsoft Exchange Server 2019 CU4
- Microsoft SQL Server 2019 CU2 (coordinator database, SQL and SQL DLA auditing)
- .NET Framework 4.6.2 for the agent
- NetApp 9.7
- Defender 5.9.6
- GPOADmin 5.14
- Active Roles Server 7.4.2
- Fluid File System 6.0.3

The following support has been removed:

- Microsoft Exchange Server 2010 is no longer supported for auditing or protection
- Windows Server 2008 R2 is no longer supported for agent installations
- Windows server 2008 SP2 is no longer supported for legacy agent installations

Miscellaneous features and enhancements

- Ability to manually specify a service name in the Services Auditing Template wizard.
- Performance improvements when auditing a high volume of AD Query events.
- Performance improvements have been made to the "Discard duplicate queries occurring within" event consolidation to reduce the amount of required memory. Note: Although improved, the agent will still consume considerably more memory when auditing high volume Active Directory Query events over longer periods of time compared to baseline agent memory usage.
- SMTP Alert Failed event created when an SMTP alert notification fails enabling you to identify and fix SMTP server configuration issues.
- Defender and Authentication Services auditing no longer requires a Change Auditor for Defender or a Change Auditor for Authentication Services license. Auditing for these applications is now enabled and disabled on a configuration basis from through the configuration setup. (After an agent upgrade from version 7.0.4 or earlier, you will need to update your configuration setup to enable Defender or Authentication Services auditing where required.)
- Ability to use autofill software with the Change Auditor web client log on.
- The "Refresh Status" button on the Deployment tab will now use the credentials defined in "Set credentials" dialog.

What’s New in Change Auditor 7.0.4

As a result of ongoing research and development, and in response to customer feedback, the following enhancements have been made in this release of Quest Change Auditor.

- Foreign forest support
- Additional internal events
- Azure Active Directory and Office 365 updates
- Threat Detection enhancements
- SIEM subscription updates and enhancements
- Additional platform support
- Miscellaneous features and enhancements

Foreign forest support

If required, agents running on a computer can connect to coordinators in a foreign Active Directory forest if there is no coordinator present in the current forest. Review the level of support, installation, and management information in the Change Auditor Installation Guide.

Additional internal events

- Events to monitor the status of Change Auditor licenses:
  - A Change Auditor license will expire soon
  - A Change Auditor license has expired
- Events to monitor the status of Azure Active Directory and Office 365 auditing:
  - Change Auditor Azure AD auditing has suspended
  - Change Auditor Azure AD auditing has resumed
  - Change Auditor Office 365 auditing has suspended
  - Change Auditor Office 365 auditing has resumed
- Events to monitor scheduled reports:
  - Scheduled report failed
- Events to monitor purge and archive jobs
  - Purge job completed
  - Archive job completed
  - Purge and archive job completed

Azure Active Directory and Office 365 updates

- Change Auditor now uses the Microsoft Graph API, a more current API for gathering of Azure Active Directory and O365 events, which requires a new set of web application permission. Because of this update, existing Azure Active Directory and Office 365 must be recreated so that a new web application is created with the appropriate permissions.
- High-level view of the activity generated for O365 Exchange Online Mailbox events is now available from the Overview tab on the event details pane.
- Additional troubleshooting information added to the Azure Active Directory and Office 365 User Guide.

Threat Detection enhancements

- Alerts generated from Active Roles or GPOADmin events, display the name of the account that initiated the event (rather than the associated Service Account) in the Threat Detection portal.
- Built-in searches for critical Threat Detection events:
  - All Threat Detection critical alerts in the last 24 hours
  - All Threat Detection critical risky users in the last 24 hours
- Change Auditor events for critical Threat Detection alerts display a 'Critical' severity in Change Auditor. Previous versions of Change Auditor showed these events with a 'High' severity.

SIEM subscription updates and enhancements

- Ability to configure event forwarding to Quest IT Security Search in the Change Auditor windows client.

Additional platform support

The following support has been added:

- Windows Server 1903 Server Core (Active Directory, File system, Registry, Services and local user and group auditing only)
- SharePoint 2019
- Microsoft Exchange 2016 CU14
- Microsoft Exchange 2019 CU3
- Microsoft Skype for Business Server 2019
- Active Roles Server 7.4
- NetApp 9.6
- EMC Unity 5.0.0
- EMC CEE 8.7.0

- Support for SQL row and page compression for the coordinator database and SQL auditing

Miscellaneous features and enhancements

The following enhancements have been added that include the ability to:

- See the 'Logon Status Code' and 'Logon Failure Reason' for failed logon events by adding these new columns to logon searches.
- Specify the containers to include in Active Directory query auditing.
- Specify which coordinators should process purge, archive, and scheduled report jobs for improved load balancing.
- Audit TTL (Time To live) on ShadowPrincipal members.
- See the subsystem associated with events in the Audit Events table in the windows client.
- Import a .csv (comma separated value) file containing a list of directory objects and optional values for a custom search through the client or PowerShell (Set- CASearchProperties command).

7

What’s New in Change Auditor 7.0.3

As a result of ongoing research and development, and in response to customer feedback, the following enhancements have been made in this release of Quest Change Auditor.

- Change Auditor and On Demand Audit integration
- Azure Active Directory and Office 365 enhancements
- Threat Detection enhancements
- Additional internal events
- Additional platform support
- Miscellaneous features and enhancements

Change Auditor and On Demand Audit integration

Quest On Demand Audit is a Software as a Service (SaaS) application, available through quest-on-demand.com that provides extensive, customizable auditing of critical activities and detailed alerts about vital changes taking place in Microsoft Office 365 and Azure Active Directory.

By integrating with Change Auditor and sending Active Directory event data to On Demand Audit, you can gain visibility into on premise changes (including events gathered up to 30 days prior to installing or upgrading Change Auditor 7.0).

You will gain access to:

- Granular, delegated access to tenants, workloads, and reports.
- Interactive, rich visualizations of on-premises and cloud events.
- Responsive search across tenants that delivers immediate results.
- Long-term storage of audit data.

Azure Active Directory and Office 365 enhancements

- The following Exchange Online events have been added:
  - Calendar delegation added to online mailbox by owner
  - Calendar delegation removed from online mailbox by owner
  - File synchronized from OneDrive for Business to a local OneDrive folder event

  - File synchronized from a local OneDrive folder to OneDrive for Business event
  - Folder permissions added in online mailbox by owner
  - Folder permissions added in online mailbox by non-owner
  - Folder permissions added in online shared mailbox
  - Folder permissions modified in online mailbox by owner
  - Folder permissions modified in online mailbox by non-owner
  - Folder permissions modified in online shared mailbox
  - Folder permissions removed in online mailbox by owner
  - Folder permissions removed in online mailbox by non-owner
  - Folder permissions removed in online shared mailbox
  - Inbox rule added to online mailbox by owner
  - Inbox rule added to online mailbox by non-owner
  - Inbox rule added in online shared mailbox
  - Inbox rule modified in online mailbox by owner
  - Inbox rule modified in online mailbox by non-owner
  - Inbox rule modified in online shared mailbox
  - Inbox rule removed from online mailbox by owner
  - Inbox rule removed from online mailbox by non owner
  - Inbox rule removed from online shared mailbox
- The following SharePoint Online events have been added:
  - Group member added in SharePoint Online
  - Group member removed in SharePoint Online
  - Member added to group in SharePoint Online
  - Member removed from group in SharePoint Online
- Ability to specify the generic events to exclude from auditing based on their operations. (The Office 365 OneDrive for Business event, Office 365 SharePoint Online event, and Office 365 Exchange Online event are generic dynamically constructed events created when associated activity is detected that does not have a corresponding event defined in Change Auditor.)
- Ability to search on the group membership changes for SharePoint Online and OneDrive by specifying the group or member.
- Audit event columns added so that both target and subject (secondary target) display names can be included in a search.
  - Azure - Subject Sync Type
  - Azure - Subject Display Name
  - Azure - On-premises Subject
  - Subject Name
- Ability to use subject as search criteria in the "Target" field for Azure Active Directory searches.

Threat Detection enhancements

- Ability to upgrade your existing Threat Detection server through PowerShell using the Update-CAThreatDetectionServer command.
- High risk user details are displayed in the Threat Detection dashboard including their photo, display or logon name, job title, department, and their address. When investigating a user or an alert for a specific user, you will also see details such email and their manager's email address, department, and office.
- Local date and time is displayed in the Threat Detection dashboard.

Additional internal events

- Events to track changes to Application user interface role definitions, task definitions, and application groups.
- Event generated when a purge and archive jobs fail.
- Events to track changes to Splunk, QRadar, ITSS and ArcSight subscriptions.

Additional platform support

The following support has been added:

- Windows Server 2019 for web client and Logon Activity auditing
- Windows Server 2019 Server Core (Active Directory, File system, Registry, Services, local user and group and Exchange 2019 auditing only)
- Microsoft SharePoint Server 2016
- Microsoft Exchange Server 2010 RU26 and RU27
- Microsoft Exchange Server 2013 CU22 and CU23
- Microsoft Exchange Server 2016 CU13
- Microsoft Exchange Server 2019 and 2019 CU1
- Microsoft SQL Server 2012 SP4 for SQL auditing
- Microsoft SQL Server 2014 SP3 for SQL and SQL DLA auditing, and coordinator database
- Microsoft SQL Server 2017 for SQL auditing
- .NET 4.7.1 Framework for the coordinator
- SCOM 2012 and 2016
- GPOADmin 5.13.5
- Active Roles Server 7.3.2
- EMC Unity 4.5.0
- NetApp 9.5
- One Identity Defender 5.9.3
- Safeguard Authentication Services 4.2

The following are no longer supported:

- Windows 7 for the Change Auditor windows client
- Windows Server 2008 R2 for all components except agents

- SQL Server 2008 and SQL Server 2008 R2 for coordinator database, direct database connection, SQL and SQL DLA auditing
- SCOM 2007

Miscellaneous features and enhancements

- Ability to not send blank reports to email or shared folders for scheduled reports.

What’s New in Change Auditor 7.0.2

As a result of ongoing research and development, and in response to customer feedback, the following enhancements have been made in this release of Quest Change Auditor.

- Threat Detection updates and enhancements
- SIEM subscription updates and enhancements
- Additional PowerShell commands
- Ability to search based on authentication type and port
- Enhanced security between Change Auditor components (FIPS compliance)
- Azure Active Directory and Office 365 enhancements
- Additional platform support
- Miscellaneous features and enhancements

Threat Detection updates and enhancements

The following updates are included for your Threat Detection deployment:

- Access to an update script and configuration commands to easily upgrade the Threat Detection server.
- Support for deploying the Threat Detection server on Hyper-V.
- Ability to enable single sign-on access for the Threat Detection dashboard.
- Ability to specify a root password during the Threat Detection server deployment.
- Ability to review the Threat Detection configuration status in the Change Auditor client (configuration page).
- New events listed under the “Threat Detection - Risky User" facility and the "Threat Detection - Alert" facility:
  - Risky user identified
  - Risky user severity increased
  - Risky user severity decreased
  - Threat Detection alert added
  - Threat Detection alert marked as "actual risk"
  - Threat Detection alert marked as "not a risk"
- Additional events details including:
  - Alert name, score, severity, and the number of alerts.
  - When the Threat Detection server started processing the alert.
  - Name of indicators associated with the alert.

    - User risk score and severity.
    - The number of points the alert adds to the user risk score (contribution to user score).
    - Old and new severity values.
    - Tags that identify whether the user is an administrator or a watched user.
    - Comments that identify when an alert is set to 'not a risk' or 'actual risk'.
- A link to the Threat Detection dashboard from the event details pane to quickly gain more information on the potential threat.
- Additional built-in searches:
    - All Threat Detection events in the last 7 days.
    - All Threat Detection risky user events in the last 7 days.
    - All Threat Detection alert events in the last 7 days.
    - All Threat Detection risky user and alert events in the last 24 hours.

SIEM subscription updates and enhancements

The following features have been added to improve your SIEM tool integrations:

- Ability to modify the subsystems included in a SIEM subscription.
- Ability to encrypt QRadar subscriptions with TLS/SSL.
- Ability to include and display the raw JSON event details provided by Microsoft for Office 365 and Azure Active Directory events.
- Ability to forward events to Quest IT Security Search (Preview mode).

Additional PowerShell commands

The following commands are available to help you manage your Change Auditor deployment:

Table 1. PowerShell commands

Function	Command
Assign, remove, and get an auditing template for a Change Auditor configuration.	• Add-CATemplateToConfiguration • Remove-CATemplateFromConfiguration • Get-CAConfigurationTemplates
Assign an auditing configuration to a Change Auditor agent.	• Set-CAAgentConfiguration
Run a search.	• Invoke-CASearch

Table 1. PowerShell commands

Function	Command
Manage Windows file system auditing.	• New-CAWindowsFSAuditObject • New-CAWindowsFSAuditTemplate • Remove-CAWindowsFSAuditTemplate • Set-CAWindowsFSAuditTemplate, • Get-CAWindowsFSAuditTemplates • Get-CAWindowsFSEventClassInfo
Create and manage a Quest IT Security Search event subscription. These commands are in preview mode for this release.	• New-CAITSSEventSubscription • Get-CAITSSEventSubscriptions • Set-CAITSSEventSubscription • Remove-CAITSSEventSubscription

Ability to search based on authentication type and port

For Active Directory, AD Query, and Exchange events, you can search events based on the authentication type and port. By default, **All Transports** is selected indicating that all events regardless of the transport protocol used are included in the search. However, you can clear the **All Transports** option and select individual options. The transport options available are:

- **All Transports** - select to include all events regardless of the transport protocol used (Default)
- **SSL/TLS** - select to include LDAP operation or LDAP queries that are secured using SSL or TLS technology
- **Kerberos**- select to include LDAP operation or LDAP queries that are signed using Kerberos-based encryption
- **Simple Bind** - select to include LDAP operation or LDAP queries that are secured using simple bind authentication (neither SSL\TLS or Kerberos used)
- **Port** - select to identify a specific port used for communication

Enhanced security between Change Auditor components (FIPS compliance)

FIPS compliant practices are implemented in Change Auditor wherever possible. The following subsystems guarantee FIPS compliant communications:

- Active Directory
- AD Queries
- AD LDS
- Windows File Server
- SharePoint
- SQL
- Exchange

- Logon Activity

All other subsystems are not considered completely FIPS compliant due to limitations related to handling and passing of data through communications with external products.

Azure Active Directory and Office 365 enhancements

The following enhancements have been added for Azure Active auditing:

- Ability to enable Windows event logging for Azure Active Directory auditing.
- Ability to use an existing Azure web application when creating an Azure Active Directory or Office 365 auditing template.
- Additional Azure Active Directory details available for email alerts (%OWNER% (user) and %MANAGER%).

Additional platform support

The following support has been added:

- Exchange 2016 CU12
- Exchange 2010 RU24
- GPOADmin 5.13
- NetApp 9.4
- EMC Unity 4.4.1
- ArcSight Enterprise Security Manager (ESM)
- IT Security Search 11.4.1
- Windows Server 2019 for coordinator and client installations
- Windows Server 2019 for agent installations (Active Directory, ADAM (AD LDS), Azure Active Directory, Office 365 Exchange Online, SharePoint Online and OneDrive for Business, AD Query, Skype for Business Server 2015, SQL Server, SQL Data Level, File System, Registry, Services, Local Account (Local User/Group), NetApp, Dell Fluid FS, EMC Isilon, and EMC Unity (4.4.1) auditing only)
- Windows Server 1803 Server Core (Active Directory, File system, Registry, Services and local user and group auditing only)
- Windows Server 1809 Server Core (Active Directory, File system, Registry, Services and local user and group auditing only)

Miscellaneous features and enhancements

- Ability to open the protection wizard from the event details pane.
- New Managed Person license. The Seats Licensed in the About dialog displays the count of managed persons; Seats Used displays as N/A since this type of license does not count seats.
- Enable and disable the ability to restore values when viewing events in the event details pane.
- Ability to enable the option which disconnects the client after 30 minutes of inactivity.
- Ability to configure Active Directory Protection templates to protect specific user Account Control flags instead of the whole attribute.
- The file name for an exported search matches the search name.
- The Change Auditor agent can be run on computers with Virtualization-based security enabled.

What’s New in Change Auditor 7.0.1

As a result of ongoing research and development, and in response to customer feedback, the following enhancements have been made in this release of Quest Change Auditor.

GDPR built-in reports

Over 190 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

The following improvements have been added:

- 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 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

Table 1. Additional columns

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
    - 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).

Improved tracking of changes to searches

New 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

The following support has been added:

- 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 improvements

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
  - Email alert configuration

  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

10

What’s New in Change Auditor 7.0

As a result of ongoing research and development, and in response to customer feedback, the following enhancements have been made in this release of Quest Change Auditor.

Updated license format

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.

Ability to forward event to third party tools

Change Auditor administrators can configure Change Auditor to send events to a third party tool using webhook technology. This technology allows you to integrate Change Auditor with SIEM tools or any other tool that accepts webhook notifications.

Currently, you can create and manage a subscription for managed and unmanaged Splunk Cloud and Splunk Enterprise editions through the Change Auditor client.

PowerShell commands are available to configure event forwarding to IBM QRadar (on premises deployments) and Micro Focus Security ArcSight Logger. These commands are in preview mode for this release.

> **NOTE:** The connection between Change Auditor and ArcSight/QRadar does not currently support TLS/SSL for secured connections. Only unsecured connections are supported for the preview release of event forwarding to ArcSight and QRadar.

Enhanced data security between the SQL Server and the coordinator

During coordinator configuration, you can select to use SSL encryption for all data sent between the coordinator and the SQL server. To use this option, the SQL server must have a certificate installed and the format of the SQL server name specified must be an exact match to the name format used in the certificate (for example FQDN or NetBios).

Ability to manage Active Directory protection with PowerShell commands

The following commands have been added to enable you to manage Active Directory protection templates:

- New-CAADProtectionTemplate for creating an Active Directory protection template.
- New-CAProtectedObject for creating a protected object to include in a protection template.
- New-CAScheduledTimeRange for scheduling when to enforce the protection.
- Get-CAADProtectionTemplates for listing existing Active Directory protection templates.
- Remove-CAADProtectionTemplate for removing an Active Directory protection template.

Ability to identify Read-Only Domain Controllers

Through the Deployment page you can:

- Select to include a column that shows if the domain controller is read-only.
- Select to display only read-only domain controllers in the forest.
- Configure how to handle auto-deployment and read-only domain controllers. If you enable the option ‘Do Not Deploy on Read-Only DCs’, when a read-only domain controller is added to the domain, the agent is not installed on it. By default, this is disabled so when a read-only domain controller is added to the domain, the agent is installed on it.

Search enhancements

The following search enhancements have been implemented:

- Additional columns to allow you to display extra information through the search Layout tab:
  - Origin - AD Site Name: The Active Directory site of the computer from which the event originated.
  - User- IsAdministrator: ‘Yes’ indicates that the user is a direct or indirect member of the local Administrators, Active Directory Administrators, Domain Admins or Enterprise Admins groups.
- For Active Directory searches, you can select to search for events based on group membership.

New built-in searches

The following built-in reports have been added to help you quickly get a sense of the activity within your Azure Active Directory deployment:

- All Azure Active Directory user events in the past 7 days
- All Azure Active Directory group events in the past 7 days
- All Azure Active Directory directory events in the past 7 days
- All Azure Active Directory policy events in the past 7 days
- All Azure Active Directory application events in the past 7 days

- All Azure Active Directory synchronized events in the past 7 days
- All Azure Active Directory self-service activity events in the past 7 days

Additional platform support

The following support has been added:

- SQL Server 2017 for the coordinator database
- SQL Server 2012 SP4 for the coordinator database
- CEE 8.4 for EMC auditing
- SQL Server 2017 for SQL DLA auditing
- SQL Server 2012 SP4 for SQL DLA auditing
- Exchange 2010 RU 19
- Exchange 2013 CU19
- Exchange 2016 CU9
- Active Roles 7.2.1
- GPOADmin 5.12

Miscellaneous enhancements and updates

- SQL AlwaysOn Availability Groups is a supported SQL high availability solution for the Change Auditor and archive databases. Direct database connection to database in a SQL AlwaysOn Availability Group is also supported.
- Ability to see “who” is responsible for shutting down an agent.
- Improved performance when processing many AD Query events.
- Improved performance when processing many NetApp events.
- Ability to use a Group Managed Service Account (gMSA) for database connection, agent deployment, and sending reports to a network share.

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.