Quest

Quest® Change Auditor 7.0

What's New

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, 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.

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

Change Auditor What's New
Updated - September 2018
Software Version - 7.0

Contents

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

1

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.

What's New in Change Auditor 6.9.5

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 platform support

The following support has been added:

- Exchange 2016 CU6
- Exchange 2013 CU17
- NetApp Filer with Data ONTAP 9.2 for NetApp auditing
- GPOADmin 5.11.1
- Active Roles 7.2

Ability to configure agents to function with proxy servers

You can now configure a proxy server for agents that audit Azure Active Directory and Office 365.

Enhanced ability to share and save search results

- Ability to print or save search results to a cvs or pdf for future reference from within the web client.
- Ability to send scheduled reports to a network share.

Additional coordinator status information

- The Coordinator status page now provides the available free space in the coordinator database.
- The Coordinator status page now provides the public SDK port (the port number assigned for external applications to access the coordinator) and the agent port (the port number assigned to the agents to communicate with the coordinator).

3

What's New in Change Auditor 6.9.4

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.

Additional platform support

The following support has been added:

- Microsoft SQL Server 2014 SP2 for Skype for Business auditing
- Change Auditor client screen resolution 1280 x 800 with at least 256 colors
- IT Security Search 11.3
- EMC Unity 4.1.0

New Azure Active Directory events

IMPORTANT: To capture sign-in risk events, you need to create a new template and select the Sign-ins option. These events are not captured automatically by an existing Azure Active Directory template.

The following events have been added.

Table 1. Azure Active Directory User events

Event	This event is triggered when....
Failed Azure Active Directory sign-in	A user fails to sign-in to an application. The event details show the user whose attempt failed, their location, and the application they attempted to access.
Successful Azure Active Directory sign-in	A user successfully signs-in to an application. The event details show the user whose attempt failed, their location, and the application they attempted to access.
Azure Active Directory - sign-in event	Sign-in activity is detected that does not have a corresponding event defined in Change Auditor.
Active risk event detected	An event occurs that could indicate a compromised user account.
Active risk event status changed to closed	An active risk event is closed as a result of being marked as: • Resolved: The issue has been addressed and has been safely closed. • False positive: The issue has been incorrectly identified as a risk and has been safely closed. • Ignore: The issue has been removed from the active list. This event helps you to understand why a risk event has been manually closed.

Table 1. Azure Active Directory User events

Event	This event is triggered when....
Closed risk event status changed to active	A closed risk event is reactivated.
Closed risk event detected	A risk event is detected in a closed state. It has been marked as resolved, a false positive, set to ignore, closed (remediated), closed (login blocked), closed (automatic multi-factor authentication), or closed (multiple reasons).

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 events in the past 7 days
- All Azure Active Directory events in the past 7 days by activity
- All Azure Active Directory sign-ins in the last 24 hours
- All Azure Active Directory risk event changes in the past 7 days

4

What's New in Change Auditor 6.9.3

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.

Additional platform support

The following support has been added:

- Change Auditor components can be deployed on Windows environments with Secure Boot enabled.
- Change Auditor components can be deployed on virtual machines running in Infrastructure as a Service (IaaS), such as Amazon Web Services and Microsoft Azure.
- NetApp Filer with Data ONTAP 9.1 for NetApp auditing.
- Exchange 2016 CU5 and Exchange 2013 CU16
- GPOADmin 5.11 and 5.10.1
- Active Roles Server 7.0.4 and 7.1
- Dell Enterprise Manager version 16.3
- Microsoft Edge 38

NOTE: Auditing Exchange 2007 support has been removed:

Generic Office 365 and Azure Active Directory events

The Azure Active Directory audit reports and the Office 365 audit logs are continuously evolving. To ensure that Change Auditor is in synch with these updates, generic events have been introduced. Each Azure AD and Office 365 facility in Change Auditor has one generic event defined.

The generic event is generated each time an activity occurs that does not have a corresponding event defined in Change Auditor. For example, "Azure Active Directory - User event" is generated when activities such as "Reset password (self-service)" or "Unlock user account" are performed in Azure Active Directory. Activity information is populated in additional columns and the description for the event (What statement) is dynamically constructed based on the Azure AD/Office 365 activity and target object name.

When working with these events, you can add additional columns to the search layout to view information about the activity.

Table 1. Available columns

Layout Tab	Search Column Name	Description
Azure - Activity Name/Operation	Activity Name/Operation	Represents the activity that was performed as part of the event.
Azure - Activity Details	Activity Details	Provides additional information about audited activity. For example, for 'Self-serve password reset flow activity progress' it shows what step the user is performing.

Azure Active Directory Auditing Wizard

Auditing templates for Azure Active Directory can now be configured in the Windows client.

New Azure Active Directory events

The following events have been added.

Table 2. Azure Active Directory User events

Event	This event is triggered when....
User AlternativeSecurityId property changed	Created when a user's alternate security ID is changed as part of the Azure Active Directory external account workflow.
User MSExchRemoteRecipientType property changed	Created when mailbox type is changed. For example, an on-premises mailbox was migrated to Exchange Online or archive mailbox was added.
User LicenseAssignmentDetail property changed	Created when the license detail assigned to a user is changed.
User UserPrincipalName property changed	Created when the UPN for a user account is changed.
User UserType property changed	Created when the user type is changed. The available type includes member, guest, or viral.
User UserStateChangedOn property changed	Created when the timestamp of the last change to the UserState is changed as part of the Azure Active Directory external account workflow.
User UserState property changed	Created when the user state is changed as part of the Azure Active Directory external account workflow. (PendingApproval/PendingAcceptance/Accepted/ PendingVerification)
User StsRefreshTokensValidFrom property changed	Created when a user's StsRefreshTokenValidFrom property is changed. For example, when a user's authorization token should be invalidated.
User StrongAuthenticationPhoneAppDetail property changed.	Created when a user's phone application used for multi-factor authentication and password reset verification have been changed
User ProxyAddresses property changed	Created when one of the user proxy addresses is changed, added, or removed.
User PreferredDataLocation property changed	Created when the preferred location for the user data is changed.

Additional Office 365 and Azure Active Directory event details

The event details pane contains the following additional information to help gain a better understanding of the activities taking place in Microsoft Office 365 Exchange Online, SharePoint Online, OneDrive for Business, and Azure Active Directory.

Table 3. Event details

Tab	Available information
Overview	Displays a high-level view of the activity that is generated for each event. You can quickly see when the event occurred, who made the change, what changed, where the change originated, the activity as defined by the Azure Active Directory reporting APIs schema, the target, target synchronization type, activity type, category, and action.
Target (Azure Active Directory events only)	Displays details on the property updates with the old and new value when available. It also displays information about multiple targets affected by a single event. For example, when a user added to a group, you can see both the user and the group as affected targets. When there are multiple targets, the target that best matches the activity type is displayed as the primary target in the Overview tab.
Details	Displays all available properties for a deeper analysis of the activity. It contains raw data from Azure Active Directory Reporting API.
Parameters (Exchange Online Administration events only)	Displays the parameters used to run the Office 365 Administrative command.

Search improvements

For Office 365, you can select to search all Office 365 services, or filter on SharePoint Online or OneDrive for Business or both. You can further refine the search by specifying the operation, file, folder, or site to search.

For Azure Active Directory, you can search all activity with the new Azure Active Directory subsystem or choose to refine your search by specifying the activity name, activity details, target, activity origin, or target sync type.

What's New in Change Auditor 6.9.2

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.

Additional platform support

The following support has been added:

- Microsoft SQL Server 2016 SP1 for the coordinator database.
- Microsoft SQL Server 2016 SP1 for SQL and SQL Data Level Auditing.
- Microsoft Exchange Server 2010 RU16, 2013 CU15, 2016 CU4.
- EMC Common Event Enabler (CEE) Framework up to 8.0 for auditing EMC Celerra/VNX and EMC Isilon.
- Dell™ Fluid File System is now supported up to version 5.0 and version 6.0 and Dell Enterprise Manager version 16.2 for FluidFS auditing.
- NetApp Filer with Data ONTAP 7.2 to 9.0 for NetApp auditing.
- Change Auditor certificate compliant with Microsoft's SHA-2 certificate update.

Office 365 auditing configuration and subsystem updates

Along with Exchange Online, Change Auditor now audits user and administration activity for SharePoint Online and OneDrive for Business that correspond to the events in the Office 365 Security & Compliance Center unified audit log. You can track, report, and create alerts on activity such as when files and folders are accessed, created, deleted, uploaded, move, renamed, and checked in and out of sites. See Office 365 SharePoint Online events and Office 365 OneDrive for Business for the complete list of new audited events.

To configure auditing, you only need to create a single Office 365 template and select the Exchange Online, SharePoint Online, and OneDrive for Business services as required.

To facilitate the creation of Office 365 searches and reports and viewing events, the Office 365 Exchange Online subsystem has been renamed to Office 365 with the associated facilities — Office 365 Exchange Online Mailbox, Office 365 Exchange Online Administration, Office 365 SharePoint Online, and Office 365 OneDrive for Business.

Office 365 SharePoint Online events

The Event Details pane includes an Overview section that displays a high-level view of the activity that generated each event. For example, you can quickly see at a glance when the event occurred, who made the change, what changed, where the change originated (IP address), the activity as defined by the Office 365 Management API

schema (operation), event ID, object site, path, or other identifier, record type, source relative Url, and user agent. Other fields may be displayed on an event-specific basis, for instance "From" and "To" for move and copy events.

You can see more information, by selecting the Details tab.

Table 4. Office 365 SharePoint Online file events

Event	Description
File accessed in SharePoint Online	Created when a user or system account accesses a file in a SharePoint Online site.
File checked in in SharePoint Online	Created when a user checks a file back in to a document library after they have completed their edits.
File checked out and discarded in SharePoint Online	Created when a file check out is undone resulting in no edits to the file in the document library.
File checked out in SharePoint Online	Created when a user checks out a file from a document library to ensure it is not accessed by others while being edited.
File copied in SharePoint Online	Created when a file is copied from a SharePoint Online site.
File deleted in SharePoint Online	Created when a file is deleted from a SharePoint Online site.
File downloaded in SharePoint Online	Created when a file is downloaded from a SharePoint Online site.
File modified in SharePoint Online	Created when file contents or properties are changed by a user or system account in a SharePoint Online site.
File moved in SharePoint Online	Created when a file is moved in a SharePoint Online site.
File previewed in SharePoint Online	Created when a file is viewed by a user or system account in a SharePoint Online site.
File renamed in SharePoint Online	Created when a file is renamed in a SharePoint Online site.
File restored in SharePoint Online	Created when a deleted file is restored in a SharePoint Online site.
File uploaded in SharePoint Online	Created when a file is uploaded to a SharePoint Online site.

Table 5. Office 365 SharePoint Online folder events

Event	Description
Folder accessed in SharePoint Online	Created when a user or system account accesses a folder in a SharePoint Online site.
Folder created in SharePoint Online	Created when a folder is created in a SharePoint Online site.
Folder deleted in SharePoint Online	Created when a folder is deleted from a SharePoint Online site.
Folder modified in SharePoint Online	Created when a folder property is changed in a SharePoint Online site.
Folder moved in SharePoint Online	Created when a folder is moved in a SharePoint Online site.
Folder renamed in SharePoint Online	Created when a folder is renamed in a SharePoint Online site.

Table 6. Office 365 SharePoint Online uncategorized event

Event	Description
Uncategorized Office 365 SharePoint Online audit event	Created when SharePoint Online activity is detected that is not included in existing Change Auditor events.

Office 365 OneDrive for Business

The Event Details pane includes an Overview section that displays a high-level view of the activity that generated each event. For example, you can quickly see at a glance when the event occurred, who made the change, what changed, where the change originated (IP address), the activity as defined by the Office 365 Management API schema (operation), event ID, object site, path, or other identifier, record type, source relative Url, and user agent. Other fields may be displayed on an event-specific basis, for instance "From" and "To" for move and copy events.

You can see more information, by selecting the Details tab.

Table 7. Office 365 OneDrive for Business file events

Event	Description
File accessed in OneDrive for Business	Created when a user or system account accesses a file in a OneDrive for Business site.
File checked in in OneDrive for Business	Created when a user checks in a file to a document library.
File checked out and discarded in OneDrive for Business	Created when a file check out is undone resulting in no edits to the file in the document library.
File checked out in OneDrive for Business	Created when a user checks out a file from a document library.
File copied in OneDrive for Business	Created when a file is copied from a OneDrive for Business site.
File deleted in OneDrive for Business	Created when a file is deleted from a OneDrive for Business site.
File downloaded in OneDrive for Business	Created when a file is downloaded from a OneDrive for Business site.
File modified in OneDrive for Business	Created when file contents or properties are changed by a user or system account in a OneDrive for Business site.
File moved in OneDrive for Business	Created when a file is moved in a OneDrive for Business site.
File previewed in OneDrive for Business	Created when a file is viewed by a user or system account in a OneDrive for Business site.
File renamed in OneDrive for Business	Created when a file is renamed in a OneDrive for Business site.
File restored in OneDrive for Business	Created when a deleted file is restored in a OneDrive for Business site.
File uploaded in OneDrive for Business	Created when a file is uploaded to a OneDrive for Business site.

Table 8. Office 365 OneDrive for Business folder events

Event	Description
Folder accessed in OneDrive for Business	Created when a user or system account accesses a folder in a OneDrive for Business site.
Folder created in OneDrive for Business	Created when a folder is created in a OneDrive for Business site.
Folder deleted in OneDrive for Business	Created when a folder is deleted from a OneDrive for Business site.
Folder modified in OneDrive for Business	Created when a folder property is changed in a OneDrive for Business site.
Folder moved in OneDrive for Business	Created when a folder is moved in a OneDrive for Business site.
Folder renamed in OneDrive for Business	Created when a folder is renamed in a OneDrive for Business site.

Table 9. Office 365 OneDrive for Business Uncategorized event

Event	Description
Uncategorized Office 365 OneDrive for Business audit event	Created when OneDrive for Business activity is detected that is not included in existing Change Auditor events.

Additional internal events and built-in reports

The following internal events have been added to help you detect auditing issues and to identify changes made to your templates:

Table 10. New events

Event	This event is triggered when....
Office 365 auditing template added	Created when an Office 365 auditing template is added to Change Auditor.
Office 365 auditing template agent changed	Created when the agent for an existing Office 365 auditing template is changed. The event details include the old and new agent FQDN.
Office 365 auditing template disabled	Created when an Office 365 auditing template is disabled.
Office 365 auditing template enabled	Created when an Office 365 auditing template is enabled.
Office 365 auditing template removed	Created when an Office 365 auditing template is removed from Change Auditor.
Office 365 auditing web application changed	Created when the web application is changed for an existing Office 365 template. The event details display the old and new web application ID GUID. **NOTE:** An Office 365 auditing web application key change event is also generated since the key is a property of the web application.
Office 365 auditing web application key changed	Created when the web application key is changed for an existing Office 365 template.
Office 365 OneDrive for Business auditing disabled	Created when OneDrive for Business is disabled in an Office 365 auditing template.
Office 365 OneDrive for Business auditing enabled	Created when OneDrive for Business is enabled in an Office 365 auditing template.
Office 365 SharePoint Online auditing disabled	Created when SharePoint Online is disabled in an Office 365 auditing template.
Office 365 SharePoint Online auditing enabled	Created when SharePoint Online is enabled in an Office 365 auditing template.

The following built-in reports have been added to help you quickly get a sense of the Office 365 activity within your organization and sites:

NOTE: Office 365 — Operation and Office 365 Site URL columns are now available to include as layout options to help you access information quickly.

- All Office 365 events in the past 7 days
- All Office 365 Exchange Online events in the past 7 days
- All Office 365 OneDrive for Business events in the past 7 days

- All Office 365 OneDrive for Business events in the past 7 days grouped by operation
- Office 365 OneDrive for Business file activity events in the past 7 days
- Office 365 OneDrive for Business folder activity events in the past 7 days
- All Office 365 SharePoint Online events in the past 7 days
- All Office 365 SharePoint Online events in the past 7 days grouped by operation
- Office 365 SharePoint Online file activity events in the past 7 days
- Office 365 SharePoint Online folder activity events in the past 7 days

Updated Office 365 PowerShell commands

The PowerShell commands have been updated to allow you to manage auditing of the supported Office 365 services.

- New-CAO365Template

  Use this command to create a template for auditing Office 365 Exchange Online, SharePoint Online, and OneDrive for Business.

- Set-CAO365Template

  Use this command to edit the account used to access Office 365 Exchange Online, the type of service and events to audit, and select a new agent.

- Get-CAO365Templates

  Use this command to see all the Office 365 templates available within your installation.

New Azure Active Directory events

The following events have been added.

Table 11. Azure Active Directory User events

Event	This event is triggered when....
User AccountEnabled property changed	Created when a user's sign-in status is changed. (Administrators can set the status to allowed and blocked.)
User AssignedPlan property changed	Created when a user's service plan and application are changed as a result of a license change.
User AssignedLicense property changed	Created when a user's product licenses has been edited. (Administrators can assign, reassign, or remove licenses as required.)
User license changed	Created when the license assigned to a user in the directory is changed.
User Mobile property changed	Created when a user's mobile phone number is changed.
User OtherMail property changed	Created when a user's alternate email address is changed.
User OtherMobile property changed	Created when a user's alternate mobile phone number is changed.
User TelephoneNumber property changed	Created when a user's telephone number is changed.

Table 11. Azure Active Directory User events

Event	This event is triggered when....
User StrongAuthenticationMethod property changed	Created when the multi-factor authentication for verification method has been changed for a user. Available methods include call to phone, text message to phone, notification through mobile application, and verification code from mobile application.
User StrongAuthenticationUserDetail property changed	Created when a user's phone number, alternative phone number, or email address used for multi-factor authentication and password reset verification have been changed.
User StrongAuthenticationRequirement property changed	Created when multi-factor authentication is enforced, enabled, or disabled for a user. Turning on multi-factor authentication changes the state to enabled. The state changes to enforced when the user signs in and authenticates.

Table 12. Azure Active Group events

Event	This event is triggered when....
Group Description property changed	Created when the group description is changed.
Group DisplayName property changed	Created when the group display name (friendly name) is changed.
Group GroupType property changed	Created when the group type (Office 365, Distribution List, or Security) and the group membership type (assigned or dynamic) is changed. **NOTE:** • Office 365 groups have a group type property of 'Unified' and security groups and distribution lists display an empty group type. • If the Group Membership assignment is dynamic, the group type property displays DynamicMembership'. If the Group Membership is assigned, the group type property is empty.
Group IsPublic property changed	Created when the group privacy setting (public or private) is changed.
Group MailNickName property changed	Created when the nickname is changed for an address book object.
Group MembershipRule property changed	Created when the criteria that determines which members should belong to a dynamic group is changed. **NOTE:** This option is only available with an Azure Active Directory premium license and is set through configuring a group's dynamic membership settings.
Group MembershipRuleProcessingState property changed	Membership Rule Processing state is an enumeration which is set to be either on or paused. If dynamic membership has been enabled for a group, the membership rule processing state determines whether the membership rule is applied. Created when the status of membership processing state is changed for a group. **NOTE:** This value can only be changed through PowerShell.

New Office 365 and Azure Active Directory auditing guides

Office 365 and Azure Active Directory auditing and event information consolidated into dedicated guides.

- All information about the additional Office 365 (and Azure Active Directory) auditing features that are available when a valid Change Auditor for Exchange, Change Auditor for SharePoint, or Change Auditor for Active Directory license has been applied are available within the Office 365 and Azure Active Directory Auditing User Guide.
- A description of all Office 365 (and Azure Active Directory) events that can be captured when you have licensed Change Auditor for Active Directory, Change Auditor for Exchange, and Change Auditor for SharePoint are found in the Office 365 and Azure Active Directory Auditing Event Reference Guide.

6

What’s New in Change Auditor 6.9.1

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 platform support

The following support has been added:

- Change Auditor coordinator now supports Windows Server 2016.
- Change Auditor client now supports Windows Server 2016.
- Change Auditor agent now supports Windows Server 2016 Server Core and Windows Server 2016.

Ability to search on selected mailboxes when creating and editing an Office 365 Exchange Online template

To facilitate Office 365 Exchange Online template creating and editing (adding and removing mailboxes and modifying the events to audit), you can narrow the search on your already selected mailboxes based on the type of activities being audited:

- Non-owner only

  This allows you to quickly locate all mailboxes being audited for "Non-owner" activity to remove them or add owner auditing if required.

- Owner

  This allows you to find all mailboxes being audited for "Owner" activity so you can remove them from auditing or remove the auditing of owner activity.

- All

  This allows you to search all mailboxes that are being audited regardless of the type of activity to remove them or edit the activities being audited.

Additional Office 365 Exchange Online internal events and built-in reports

The following Office 365 Exchange Online internal events and built-in search have been added to help you detect auditing issues and to identify changes made to your templates:

Table 13. New events

Event	This event is triggered when....
Office 365 Exchange Online mailbox auditing configuration changed by an external application Built-in report: Office 365 Exchange Online mailbox auditing configuration changed by an external application in the last 24 hours	Auditing configuration is changed by an application other than Change Auditor. When this is detected, the configuration for the tenant will be reset to settings in the Office 365 Exchange Online template.
Office 365 Exchange Online administrative activity auditing setting changed	Administrative Activity setting is enabled or disabled for an existing Office 365 Exchange Online auditing template.
Office 365 Exchange Online “All mailboxes for non-owner events” auditing setting changed	“All mailboxes for non-owner events” auditing setting is changed in an existing Office 365 Exchange Online auditing template.
Office 365 Exchange Online auditing configuration account changed	Exchange Administration account used to configure auditing is changed in an existing Office 365 Exchange Online auditing template.
Office 365 Exchange Online auditing configuration account password changed	Exchange Administration account password used to configure auditing is changed in an existing Office 365 Exchange Online auditing template.
Office 365 Exchange Online auditing template agent changed	The agent for an existing Office 365 Exchange Online auditing template is changed. The event details include the old and new agent FQDN.
Office 365 Exchange Online auditing web application changed	The web application is changed for an existing Office 365 Exchange Online auditing template. The event details display the old and new web application ID GUID.
Office 365 Exchange Online auditing web application key changed	The web application key is changed for an existing Office 365 Exchange Online auditing template.
Office 365 Exchange Online mailbox added to auditing template	A mailbox is added to an existing Office 365 Exchange Online auditing template.
Office 365 Exchange Online mailbox auditing type changed	The type of activity (owner and non-owner) to audit for a mailbox has changed in an existing Office 365 Exchange Online auditing template.
Office 365 Exchange Online mailbox removed from auditing template	A mailbox is removed from an existing Office 365 Exchange Online auditing template.

Additional Azure Active Directory events

Directory roles (also known as administrator roles) represent a specific sets of rights within Azure Active Directory. Users access to Azure Active Directory features depends on the roles they have been assigned. The following events are available:

- Role member added

  This event is triggered when a user or service principal is added to a directory role.
- Role member removed

  This event is triggered when a user or service principle is removed from a directory role.
- Role enabled

  This event is triggered when a directory role is enabled in Azure Active Directory.

Additional Active Directory custom user monitoring events

The following events have been added to provide additional details on the UserAccountControl attribute that controls whether certain properties for a user are enabled or not.

- User's ability to update their password has changed

  This event is triggered when the user’s ability to update his/her password has changed.
- User's home folder requirement has changed

  This event is triggered when the UserAccountControl attribute property flag that determines whether a user must have a home folder is changed.
- User's requirement for a password has changed

  This event is triggered when the UserAccountControl attribute property flag that determines whether a user must have a password has changed.

Azure Active Directory and Office 365 Exchange Online historical event collection

Azure Active Directory and Office 365 Exchange Online keeps track of events that have occurred in the past. Using PowerShell, you can now also collect these events by specifying how many hours or days the agent should go back in time to start event collection.

Ability to detect Skype for Business agent status and configuration

The Change Auditor Agent Status dialog that is in place to help you determine if the Change Auditor agent is running and what version is installed now includes the Skype for Business module.

The agent configuration page now indicates a whether a particular agent has been assigned a Skype For Business auditing template.

What's New in Change Auditor 6.9

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 platform support

The following support has been added:

- Microsoft SQL Server 2016 is supported for the coordinator database.
- Windows 10 is a supported operating system.
- Auditing Microsoft Exchange Server 2016 is now supported.
- Auditing Microsoft SQL Server 2016 is now supported for SQL and SQL Data Level Auditing.

Office 365 Exchange Online auditing

Change Auditor for Exchange simplifies the audit process by tracking, auditing, reporting and alerting on Microsoft Office 365 Exchange Online configuration and permission changes. To ensure Office 365 compliance, you can automatically generate intelligent, in-depth reports, protecting you against policy violations and avoiding the risks and errors associated with day-to-day modifications.

Change Auditor for Exchange audits all critical changes to Office 365 Exchange Online including log ons, permission changes and non-owner and owner mailbox access. Change Auditor correlates activity across the on-premises and cloud environment making it easy to search all events regardless of where they occurred. Make Exchange auditing easier than ever with audits that protect your organization's security policies as well as prevent compliance violations, system downtime, and productivity losses.

Office 365 Exchange Online events audited by Change Auditor include:

- Office 365 Exchange Online Administration
  - Office 365 Exchange Online administrative cmdlet executed
  - Office 365 Exchange Online administrative cmdlet executed by external user

- Office 365 Exchange Online Mailbox
  - Folder moved in online mailbox by non-owner
  - Folder moved in online mailbox by owner
  - Folder moved in online shared mailbox
  - Folder moved to Deleted Items in online mailbox by owner
  - Folder moved to Deleted Items in online shared mailbox
  - Folder moved to Deleted Items in online mailbox by non-owner
  - Folder opened in online mailbox by non-owner
  - Folder opened in online shared mailbox
  - Folder opened in online mailbox by owner
  - Folder hard-deleted in online mailbox by non-owner
  - Folder hard-deleted in online mailbox by owner
  - Folder hard-deleted in online shared mailbox
  - Folder soft-deleted in online mailbox by owner
  - Folder soft-deleted in online mailbox by non-owner
  - Folder soft-deleted in online shared mailbox
  - Message copied in online mailbox by non-owner
  - Message copied in online shared mailbox
  - Message created in online mailbox folder by non-owner
  - Message created in online shared mailbox
  - Message created in online mailbox by owner
  - Message hard-deleted in an online mailbox by non-owner
  - Message hard-deleted in online mailbox by owner
  - Message hard-deleted in online shared mailboxMessage moved in online mailbox by non-owner
  - Message moved in online mailbox by owner
  - Message moved in online shared mailbox
  - Message moved to Deleted Items in online mailbox by non-owner
  - Message moved to Deleted Items in online shared mailbox
  - Message moved to Deleted Items in online mailbox by owner
  - Message opened in online mailbox by non-owner
  - Message opened in online shared mailbox
  - Message sent as another user in online mailbox by owner
  - Message sent as another user in online shared mailbox
  - Message sent as another user in online mailbox by non-owner
  - Message sent on behalf of another user in online mailbox by owner
  - Message sent on behalf of another user in online mailbox by non-owner
  - Message sent on behalf of another user in online shared mailbox
  - Message soft-deleted in online mailbox by non-owner
  - Message soft-deleted in online mailbox by owner
  - Message soft-deleted in online shared mailbox
  - Message updated in online mailbox by non-owner
  - Message updated in online mailbox by owner
  - Message updated in online shared mailbox
  - Online Mailbox login by owner
  - Uncategorized Office 365 Exchange Online audit event

Azure Active Directory auditing

Change Auditor for Active Directory simplifies the audit process by tracking, auditing, reporting and alerting on changes and activity in Microsoft® Azure® Active Directory® that impact your environment. Change Auditor correlates activity across the on-premises and cloud directories, providing you a single pane-of-glass view of your hybrid Active Directory environment and making it easy to search all events regardless of where they occurred.

To ensure Active Directory and Azure Active Directory compliance, you can automatically generate intelligent and in-depth reports, protecting you against policy violations and avoiding the risks and errors associated with day-to-day modifications.

Skype for Business auditing

Change Auditor for Skype for Business allows you to audit configuration and security setting changes in Microsoft Skype for Business Server 2015 and Microsoft Lync Server 2013, providing change notifications for Skype user setup, permissions and application configuration from the Microsoft Skype for Business Server 2015 / Microsoft Lync Server 2013 Central Management Store (CMS).

The Change Auditor for Lync license has been deprecated. To audit Microsoft Skype for Business Server 2015 and Microsoft Lync Server 2013, you must obtain and import a new Change Auditor for Skype for Business license.

In previous versions of Change Auditor, Lync administration events were generated under the Active Directory subsystem. Starting with Change Auditor 6.9, the Lync Administration facility has been renamed to Skype for Business Administration facility and the administration events are found under the Skype for Business subsystem. The Change Auditor for Lync license and built-in searches have been deprecated and replaced with the Change Auditor for Skype for Business license and Skype for Business built-in searches.

Previous Lync administration events are still supported in Change Auditor for Skype for Business.

You can now audit the following event that are generated by changes to the management data (such as topology, configuration and policy information) in the Central Management Store (CMS) SQL Server:

- Topology: Active URL changed
- Topology: Central Management Sever changed
- Topology: Default SIP domain changed
- Topology: Pool changed
- Topology: Pool server collection changed
- Topology: SIP domains changed
- Topology: Simple URL changed
- Topology: Site changed
- Ringing Policy changed
- Voice: Dial Plan changed
- Voice: Dial Plan - Conferencing Region changed
- Voice: Dial Plan - External Access Prefix changed
- Voice: Dial Plan - Normalization Rule changed
- Voice: Dial Plan - Normalization Rule - Pattern to Match changed
- Voice: Dial Plan - Normalization Rule - Translation Rule has changed
- Voice: Dial Plan - Normalization Rule - Internal Extension changed
- Voice: Dial Plan - Optimize Device Dialing option changed
- Voice: Voice Policy changed
- Voice: Voice Policy - Calling Feature changed
- Voice: Voice Policy - PSTN Usage changed
- Voice: Voice Policy - PSTN Voicemail Escape Timer changed
- Voice: Voice Policy - Call Forwarding and Simultaneous
- Voice: Voice Policy - Call Forwarding and Simultaneous Ringing Custom PSTN changed
- Voice: Route has changed
- Voice: Route - Matching Pattern changed
- Voice: Route - Suppress Caller ID changed
- Voice: Route - Alternate Caller Number changed
- Voice: Route - Trunk changed
- Voice: Route - PSTN Usage changed
- Voice: Route - Configuration Enable Location Based Routing at the Global Scope changed
- Voice: Route - Priority changed
- Voice: Trunk Configuration changed
- Voice: Trunk Configuration - Policy changed
- Voice: Trunk Configuration - Max Early Dialogs changed
- Voice: Trunk Configuration - Network Site ID changed
- Voice: Trunk Configuration - PSTN Usage changed
- Voice: Trunk Configuration - Translation Rule changed
- Voice: Trunk Configuration - Translation Rule Pattern to Match changed
- Voice: Trunk Configuration - Translation Rule - Translation Pattern changed
- Voice: Trunk Configuration - SIP Response Code Translation Rule - List changed
- Voice: Trunk Configuration - SIP Response Code Translation Rule - Received Response Code changed
- Voice: Trunk Configuration - SIP Response Code - Translation Rule Received ISUP Cause Value changed
- Voice: Trunk Configuration - SIP Response Code - Translation Rule -Translated Response Code changed
- Voice: Trunk Configuration -Encryption Support Level changed
- Voice: Trunk Configuration - Support Referral changed

New PowerShell capabilities

The following PowerShell commands have been added to help manage searches, Office 365 Exchange Online auditing, Azure Active Directory auditing, and Skype for Business auditing.

Table 14. Available commands to manage Office 365 Exchange Online auditing

Command	Description
New-CAO365ExchangeTemplate	Use this command to create a new template for auditing Office 365 Exchange Online.
Get-CAO365ExchangeTemplates	Use this command to edit the account used to access Office 365 Exchange Online, the type of events to audit, and select a new agent.

Table 14. Available commands to manage Office 365 Exchange Online auditing

Command	Description
Set-CAO365ExchangeTemplate	Use this command to see all the Office 365 Exchange Online templates available within your installation.
Get-CAO365ExchangeMailboxes	Use this command to find specific mailboxes that can be added to an existing Office 365 Exchange Online template.
Add-CAO365ExchangeTemplateMailboxes	Use this command to audit specific mailboxes in your organization by adding them to an existing Office 365 Exchange Online template.
Remove-CAO365ExchangeTemplateMailboxes	Use this command to remove mailboxes from an existing Office 365 Exchange Online template.
Get-CAO365ExchangeTemplateMailboxes	Use this command to retrieve a list of mailboxes being audited by a particular Office 365 Exchange Online template.

Table 15. Available commands to manage Azure Active Directory auditing

Command	Description
New-CAAzureADTemplate	Use this command to create a new template for auditing Azure Active Directory.
Get-CAAzureADTemplates	Use this command to edit the web application key and ID, as well as the agent in an existing Azure Active Directory template. This also allows you to replace an expired or revoked web application.
Set-CAAzureADTemplate	Use this command to see all the Azure Active Directory templates available within your installation.
Get-CAAzureADObjects	Use this command to find specific Azure Active Directory objects.

Table 16. Available commands to manage Skype for Business auditing

Command	Description
Get-CASkypeEventClassInfo	Use this command to see the list of event classes available for the Skype for Business subsystem.
New-CASkypeTemplate	Use this command to add a new Skype for Business template to Change Auditor.
Get-CASkypeTemplates	Use this command to see all the Skype for Business templates that have been created.
Set-CASkypeTemplate	Use this command to update the properties of an existing Skype for Business template.
Remove-CASkypeTemplate	Use this command to remove a Skype for Business template.

Table 17. Available commands for searches

Command	Description
Get-CASearches	Use this command to view information on all available searches and identify a search info object that is required for some other commands.
Get-CASearchDefinition	Use this command to obtain the search definition from an existing search. The search definition is XML that can be modified and used to create a new search.
Set-CASearchProperties	Use this command to update the name, default folder, or limit of a public or private search from the installation.
Copy-CASearch	Use this command to copy a search in the installation.
Add-CASearch	Use this command to create a new search in the installation.
Move-CASearch	Use this command to move a search from one folder path to another in the installation.
Remove-CASearch	Use this command to remove a public or private search from the installation.
Add-CASearchFolder	Use this command to create a new search folder in the installation.
Remove-CASearchFolder	Use this command to remove a public or private folder from the installation.

IT Security Search

IT Security Search is a web-based interface that correlates disparate 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 leverage its many features.

System requirement changes in Change Auditor 6.9

Change Auditor coordinator

- Windows Server 2008 SP2 is no longer a supported operating system.
- Microsoft SQL Server 2016 is now a supported database.
- Updated Microsoft's .NET requirement to version 4.6.1.

Change Auditor client

- Windows 10 is now a supported operating system.
- Updated Microsoft's .NET requirement to version 4.6.1.
- Windows Server 2008 SP2 is no longer a supported operating system.

Change Auditor agent

- Windows Server 2003 SP2, Windows Server 2003 R2 SP2, and Windows Server 2008 SP2 are no longer supported operating systems.

  NOTE: During an agent install, if one of these operating systems is detected, the latest version of the Change Auditor agent that supports the operating system will be installed.

- Updated Microsoft's .NET requirement to version .NET 4.5.2.

Change Auditor workstation agent

- Windows 10 is now a supported operating system.
- Updated Microsoft's .NET requirement to version .NET 4.5.2.

Change Auditor web client

- Updated Microsoft's .NET requirement to version .NET 4.6.1.
- Updated browser support: Chrome 52, Firefox 48, Safari 9.1.2 for Mac OS.
- Internet Explorer versions below 11 are not supported.

Change Auditor for Exchange

- Microsoft Exchange Server 2016 is now supported.

Change Auditor for SQL Server

- Microsoft SQL Server 2016 is now supported.
- Microsoft SQL Server 2005 is no longer supported.

Change Auditor for SQL Server Data Level Auditing

- Microsoft SQL Server 2016 is now supported.

Change Auditor for NetApp

- Updated support for NetApp Filer with Data ONTAP to version 8.3.2.

Change Auditor for Skype for Business

- Support for Microsoft Skype for Business Server 2015 has been added.
- Microsoft Lync 2010 is no longer supported.

Miscellaneous

- Improved event consolidation for Microsoft Word, Excel, Visio, and PowerPoint (Microsoft Office version 2010, 2013, and 2016) files. Change Auditor has improved how it filters out events for temporary office files that are created when you are working with the documents.

- For Windows File Server auditing you can now select to ignore the folder opened and file opened events generated by tooltips as users browse remotely through the network.
- A direct upgrade from Change Auditor 5.9 is not supported. To upgrade from Change Auditor 5.9 you must follow this upgrade path: 5.9 to 6.8 to 6.9. Direct upgrades to Change Auditor 6.9 are only supported from versions 6.0, 6.5, 6.6, 6.7, and 6.8.

8

What's New in Change Auditor 6.8

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.

Client authentication method

Ability to specify the authentication method that all clients will use to access Change Auditor. The following two methods available:

- Windows Forms Authentication (enabled by default)

  When this option is enabled, Change Auditor uses the standard login entry form where users specify login Windows credentials in both the Change Auditor clients. Credentials are securely verified with Active Directory to authenticate user access to Change Auditor.

- Active Directory Client Certificate Authentication

  When this option is enabled, authentication is performed with client browser certificates. This permits users to log into Change Auditor clients using Smart Card-based authentication technologies.

  Once this option has been selected users will be prompted for credentials each time they log in. They can enter a user name and password or connect using a smart card and enter their personal identification number.

NOTE: Smart card authentication is used only to log on to Change Auditor clients. For any other areas within Change Auditor where you are required to supply credentials (such as agent deployment and management, template creation, and restore values), you must enter a user name and password.

IMPORTANT: Changing the authentication method affects all clients and requires an update and re-deployment of some components. Because of this, you should only modify the authentication method as part of an overall change to the Change Auditor deployment as a result of new requirements or architectural changes.

Dell Fluid File System (FluidFS) auditing

Quest Change Auditor for Fluid File System tracks, audits, reports and alerts on file and folder changes in real time, translating events into simple text and eliminating the time and complexity required by native auditing. The auditing scope can be set on an individual file or folder or an entire file system recursive or non-recursive. Change Auditor also allows you to include or exclude certain files or folders from the audit scope in order to ensure a faster and more efficient audit process.

Change Auditor for Fluid File System captures events and provides detailed information relating to the following activities on the FluidFS cluster:

- File and folder access
- File and folder creation, deletion and renames

- File and folder permission changes
- Content changes, such as file opens and writes

NOTE: Change Auditor for Fluid File System audits only SMB operations on FluidFS clusters.

NOTE: FluidFS auditing is supported only for Dell Fluid File System version 5.0.10.

Improved DNS auditing

An improved DNS auditing system has been added that will better capture who and where (origin) the change was made for each DNS event. These changes are now tracked through DNS services, as opposed to the earlier auditing of lower-level systems like the Windows registry, file system or Active Directory. Auditing for those systems is still in place to cover changes made by tools like REGEDIT, ADSIEdit and text editors. The new and old auditing systems now augment each other, providing more complete information than either one alone.

What's New in Change Auditor 6.7

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.

Start page

When you open Change Auditor, you are presented with a page where you can view and access relevant information regarding Change Auditor including news and updates, support and knowledge base content, online documentation (release notes and guide), links to the latest releases, and essential contact links.

System requirements evaluation utility

A requirements evaluation tool is available from the autorun. Running this tools allows you to ensure that your system meets the minimum coordinator requirements before beginning the installation. A green check denotes that your system meets the requirements and a red "X" means that it does not meet the minimum and should be addressed before continuing with the installation.

Upgrade and migration updates

In previous versions of Change Auditor, the Data Migration Tool was used to migrate events from a legacy 5.9 to 6.x database. You no longer need the Data Migration Tool for this. Change Auditor 6.7 introduces an enhanced in-place migration option so you can perform a direct upgrades from version 5.9, without losing any configuration data.

The following migration paths are supported through an in place migration during upgrade:

- 5.9 to 6.7 – migrate events from 5.9 to a new or existing 6.7 database. If you have Change Auditor 5.8 or below you must upgrade to 5.9 first.
- 6.x to 6.7 – migrate events from 6.x database to a new or existing 6.7 database.

You can, however, still use the Data Migration Tool for the following situations:

- To consolidate multiple Change Auditor databases.
- To move legacy archived databases.
- If you plan to redesign your Change Auditor deployment by installing a new database and moving existing audited events into it.

SQL Data Level auditing and reports

SQL auditing has been augmented to include data level changes. SQL Data Level auditing allows you to audit changes to databases and tables. A separate SQL Data Level auditing templates must be defined for each target database to be audited by Change Auditor.

You can audit the following events:

- Row added to a table
- Row updated in a table
- Row removed from a table
- Procedure added
- Procedure removed
- Procedure altered
- Table added
- Table removed
- Table altered
- Table truncated
- Index added to a table
- Index removed from a table
- View added
- View removed
- View altered
- Check constraint added to a table
- Check constraint removed from a table
- Trigger added
- Trigger removed
- Trigger altered
- Foreign key added to a table
- Foreign key removed from a table
- Type added
- Type removed
- Statistics added to a table
- Statistics removed from a table
- Function added
- Function removed
- Function altered
- Rule added
- Rule removed
- Object renamed
- Primary key added to a table
- Primary key removed from a table
- Default object added
- Default object removed
- Default constraint added to a table
- Default constraint removed from a table
- User added
- User removed

The following built-in reports are available:

- SQL Data Level Events in the last 24 hours
- SQL Data Level Row Change Events in the last 24 hours
- SQL Data Level Structure Change Events in the last 7 days

The following internal events have also been added:

- SQL Data Level Auditing Template Added
- SQL Data Level Auditing Template Deleted
- SQL Data Level Auditing Template Enabled
- SQL Data Level Auditing Template Disabled
- SQL Data Level Auditing Template Modified

Archiving capabilities

You can now schedule both the purging of events from your database and archiving older data to an archive database. Automating database cleanup allows you to keep critical and relevant data online and current while eliminating or archiving events that are no longer required. This not only prevents your database from growing in size, but it increases overall operational efficiency by speeding up searches and data retrieval from the database.

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

The following internal events have been added to this release:

- Purge and Archive Job Added

- Purge and Archive Job Changed
- Purge and Archive Job Disabled
- Purge and Archive Job Enabled
- Purge and Archive Job Removed

Protection updates

Active Directory and File System protection has been updated to allow you to:

- Schedule when the protection will be enforced. You can either select to have the protection always run or have it run only during specific times.
- Control when the protection is enabled based on the location.
  - Protect access from all locations: Protection is always enabled regardless of the client location.
  - Protect access only from select locations: Protection is only enabled for the specified locations.
  - Disable protection only for select locations: Protection is disabled for the selected locations. Enabled everywhere else.
  - Protect access from all unknown locations: All Active Directory requests from locations that cannot be determined by the Change Auditor agent will be protected.
- Import a list of Active Directory objects into a protection template.

Ability to ignore file open actions

Because not all actions/events provide beneficial auditing data, you can select to filter out non-essential information. Specifically, you have the option to ignore events generated when browsing files and folders locally:

- Folder open events that are generated by tooltips (folder content information that is displayed when you hover your mouse over a folder) because Windows Explorer navigates the folder tree for all the sub-folders when you hover over the parent folder to see the tooltip.
- File open events that are generated by file scans because Windows Explorer opens and reads the header of all files contained in an opened folder for information to display in the window.

Support for MAPI over HTTP protocol

MAPI over HTTP protocol on Exchange 2013 CU8 or later servers is now supported for the following:

- Exchange mailbox protection from unauthorized access.
- Exchange message, contact, appointment, task and object delete events.
- Exchange folder delete events.
- Exchange message, contact, appointment, task and object read events.
- Exchange folder created and folder and mailbox open events.
- Exchange message, contact, appointment, task and object moved and copied events.
- Exchange message, contact, appointment, task and object created events.
- Exchange folder renamed, moved and copied events.
- Exchange message marked unread events.

- Exchange folder permission changed events.
- Exchange message, appointment, contact, task and object modified events.

SRS reporting

Change Auditor supports Microsoft's Microsoft SQL Server Reporting Services (SRS). You can create SRS templates that define all the necessary Report Server information (URL and credentials) and Change Auditor data source information for publishing reports. You can then publish any report to SRS using these settings. This allows you to interact with a web-based reporting portal and simply subscribe to the reports you want to see.

The following internal events have been added:

- SRS URL added to reporting services template
- SRS URL attribute changed

PowerShell commands

Change Auditor comes with a PowerShell module for you to use to manage your environment. It is installed when you install the Change Auditor client.

NOTE: Windows PowerShell version 3.0 or higher is required.

Table 18. Available commands

Use these commands...	When you want to...
• Install-CACoordinator • Install-CAWebClient	Install Change Auditor components.
• Find-CAInstallations • Find-CACoordinators • Find-CASuitableCoordinator	Find the Change Auditor installations and coordinators available in your Active Directory environment.
• Connect-CAClient • Disconnect-CAClient	Connect to and disconnecting from Change Auditor installations and coordinators.
• Get-CACoordinator • Get-CACoordinators • Get-CAInstallation • Get-CAAgents	Gather Change Auditor system information to help you to manage your installation components.
• Install-CAAgent • Uninstall-CAAgent • Update-CAAgent	Manage your agent deployments. You must be a member of Administrators role to use these commands. Any changes affecting configuration are audited with internal events.

Change Auditor logon internal events

Change Auditor logon events are now available for the various client platforms so that access to Change Auditor data can be audited.

The following internal events have been added:

- Change Auditor PowerShell Client Logon
- Change Auditor SDK Client Logon

- Change Auditor Unknown Client Logon
- Change Auditor Web Client Logon
- Change Auditor Windows Client Logon

Dell Data Protection internal event

Change Auditor integrates with Dell Data Protection|Cloud Edition (DDP|CE) to audit activity performed in sync folders of cloud storage providers.

When the workstation agent is unable to connect to the Dell Data Protection service, the following new internal event with a high severity will be generated:

- Agent is unable to connect to the Dell Data Protection service

Updated compliance reports - HIPAA, PCI, SOX

The IT compliance regulatory landscape is constantly evolving. The built-in searches have been updated to ensure they are up-to-date (as of the date of release - HIPAA - March 2015 / PCI - version 3.0 / SOX - version 5.0) in relation to the latest HIPAA, PCI, SOX regulations.

Additional updates

- A new dashboard that displays file system objects with the most permission changes.
- Increased search abilities. After selecting a specific event from the results of a search, the Event Details pane will allow you to further refine your search criteria. Expand the Add to Search tool bar button to display the available options for refining your current search. These options are produced from the details of the selected event and may differ between event types.
- File and folder auditing support for NetApp cluster mode (as of version 8.2 and later).
- Meaningful information (specifically, the name of the host or server) is now displayed in the event details when DNS records are added, removed, or modified.
- A dedicated Change Auditor for Cloud Storage User guide and cloud storage events added to SCOM pack.

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.