Quest®

Quest® Change Auditor 7.0

Quick Start Guide

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 Quick Start Guide
Updated - May 2018
Software Version - 7.0

Contents

Change Auditor Overview

Overview

This guide has been prepared to assist you in installing and becoming familiar with Change Auditor. Even though most this content refers to Change Auditor for Active Directory, it also steps you through the process of setting up Quest Change Auditor for Exchange and Quest Change Auditor for Windows File Servers.

This guide is intended to be used to set up a test lab environment. It is not intended as a stand-alone guide and makes references to supporting product documentation that you should use when deploying the Change Auditor in your production environment.

Business challenges

Challenge 1:

Microsoft Active Directory is at the heart of your mission-critical network infrastructure. Do not leave Active Directory management, support, and administration to chance. Issues with your directory can result in unplanned and costly service disruptions and business-crippling network downtime, as well as harmful security breaches and noncompliance with critical government regulations such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), and Health Insurance Portability and Accountability Act (HIPAA). Organizations must be notified of critical changes to Active Directory.

Challenge 2:

Your file systems contain critical and sensitive information. Typically, it is difficult to track and enforce who has access to which documents and most violations of information security policies and misuse of access rights go undetected. Similar to Active Directory issues, issues with your file systems can also result in unplanned and costly service disruptions, business-crippling network downtime, harmful security breaches, and noncompliance with critical government regulations.

Challenge 3:

Email is used for communications within and between organizations. As a result, it serves as a repository of information — some of it sensitive and vulnerable to misuse. Many organizational policy violations go undetected because most security actions are not audited. This can result in lost productivity and system

downtime — a risk no organization should take. Companies need in-depth auditing and reporting for Exchange security and compliance to prove regulatory compliance and drive efficiencies.

Business solutions

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

Change Auditor uses a modular approach which allows for separate product deployment and management for key environments including Active Directory, Windows File Servers, and Exchange.

Change Auditor for Active Directory drives the security and control by tracking, auditing, reporting, and alerting on the changes that impact your directory including changes to users, groups, nested groups, GPOs, computer, services, registry, local users, and groups and DNS — without the overhead of native auditing.

In addition, you can lock down critical Active Directory, ADAM (AD LDS), and Group Policy objects, to protect them from unauthorized or accidental modifications or deletions.

Change Auditor for Active Directory also audits activity in Microsoft Azure Active Directory.

Correlating activity across the on-premises and cloud directories, provides a single pane-of-glass view of your hybrid environment and makes it easy to search all events regardless of where they occurred.

Change Auditor for Windows File Servers enables administrators to achieve the comprehensive auditing coverage of native auditing tools without the mass of cumbersome data that native event logs generate. Change Auditor for Windows File Servers includes auditing for Windows file server activity related to files and folders, shares, and changes to permissions. Granular selection allows the auditing scope to be set on an individual file or folder and the entire subtree recursive or nonrecursive. Change Auditor for Windows File Servers also allows you to include or exclude certain files or folders from the audit scope to ensure a faster more efficient audit process.

Change Auditor for Windows File Servers also provides an access control model that permits administrators to protect business-critical files and folders on the file server.

Change Auditor for Exchange is the watchful eye that proactively tracks, audits, reports, and alerts on Exchange configuration and permission changes — without the need for native auditing. Change Auditor for Exchange audits for critical changes to Exchange including administrative groups, mailbox policies, public and private information store auditing, organizational changes such as ActiveSync mailbox policy changes, distribution list changes and more. Using the Exchange Mailbox Monitoring feature you can also audit for non-owner activity access and get complete visibility into these types of changes, including who accessed someone else's mailbox, what message they accessed, and what they did with the message (read, delete, move, and so on). Continually being in-the-know helps you to prove compliance, drive security, and improve uptime while proactively auditing changes to Exchange Server configurations and permissions.

Through the Exchange Mailbox protection feature, you can prevent unwanted access to Exchange mailboxes, making it much more difficult for rogue administrators to access critical mailboxes.

You can also audit Office 365 Exchange Online configuration and permission changes.

What is Change Auditor?

Change Auditor provides complete, real-time change management that drives network availability and productivity with proactive auditing, in-depth forensics, and comprehensive reporting on all key configuration changes in Windows — including Active Directory, Windows File Servers, and Exchange.

- Enables enterprise-wide change management from a single client.
- Ensures a secure and compliant networking environment by tracking all critical changes in real time.

- Automates procedures to continually track and report on compliance initiatives.
- Strengthens internal controls through real-time insight into both authorized and unauthorized changes.
- Drives availability by enabling proactive troubleshooting.
- Turns information into intelligent in-depth forensics for auditors and management.

How does Change Auditor work?

Change Auditor consists of four components:

- Agents
- Coordinators
- Clients
- Microsoft SQL Server database

Agents are deployed to all servers (domain controllers and member servers) tracking configuration changes in real time. When a change is made on a server running an agent, the change information (audit event) is captured, batched and forwarded to a coordinator, which then inserts the event details into the database.

NOTE: If the Change Auditor for Logon Activity Workstations auditing is licensed, you will also deploy agents to the workstations to monitor.

For each configuration change detected, Change Auditor creates an audit event entry in the database with the following information:

- The type of configuration change event
- The time and date of the configuration change event
- The identity of the machine the change was made on
- The identity of the managed object the change pertains to
- The old and the new value of the change (if applicable)
- The IP address of the workstation and client computer where the change originated

The coordinator is responsible for fulfilling client and agent requests and for generating alerts. Multiple coordinators can be installed in a single forest and an agent can be connected to multiple coordinators simultaneously. All connected coordinators can participate in receiving events from the agent, allowing a high volume of events to be distributed for processing.

NOTE: Server agents submit events to all available coordinators and load balancing occurs automatically. However, workstation agents randomly connect to a single coordinator. This design enables ‘scaling out’ options for large workstation agent deployments within a single site.

The client is the user interface that provides immediate access to key configuration change information. From the client you can perform tasks such as:

- Install, upgrade, or uninstall agents
- Define search criteria to return specific events and view the search results
- Enable and disable alerts and view the events that triggered these alerts
- Enable and schedule email reporting for individual search queries
- View agent and coordinator statistics
- Define custom Active Directory and ADAM (AD LDS) object and attribute auditing
- Define the hosts to audit for VMware auditing
- Define the farm and paths to audit for SharePoint auditing

- Define file system auditing for Windows File Servers, EMC, and NetApp devices
- Define auditing for Fluid File System clusters
- Specify the SQL instances to audit dfor SQL Server auditing
- Specify the mailboxes to audit for Exchange mailbox auditing
- Specify the mailboxes or administration cmdlets to audit for Office 365 Exchange online auditing
- Specify the containers to exclude from Active Directory query auditing
- Configure object protection for Active Directory, Exchange, File Systems, and Group Policies
- Define and assign agent configurations
- Configure SMTP for alerting and reporting
- Create and schedule purge jobs for maintaining the database
- Define who is authorized to use the Change Auditor client (Windows and web) features

System requirements

To ensure a successful installation, Quest strongly suggest creating a clean Windows test environment (virtual or physical). If this is not possible, ensure that your test environment is healthy and the following requirements are met.

See the Change Auditor Release Notes for the hardware and software requirements for the Change Auditor components.

2

Install Change Auditor

The procedures provided in this topic are intended to be used to install Change Auditor in a test lab environment. For more detailed installation instructions, see the Change Auditor Installation Guide.

- Before you begin an installation
- Installation overview
- Web client — Optionally, install the web client on the IIS web server.
- Step 2: Install the client
- Step 3: Add user accounts to Change Auditor security groups
- Step 4: Start the client
- Step 5: Deploy agents

Before you begin an installation

Quest recommends that you perform the following steps before you begin installing Change Auditor:

- If you do not already have Change Auditor, you can download it from the Quest web site at https://support.quest.com/.
    - Before you can download the product, you must register with Quest. If you are a registered Quest user, log on using your email address and password.
    - Once you have registered or logged in, locate the product and version that you want to download from the product list.
    - On the download window, click the link and save the file to an appropriate directory (such as c:\temp).

    NOTE: If you have purchased multiple Change Auditor products, download one instance of Change Auditor only. The code is the same for all and the license keys determine what features are enabled or disabled.
- Review the system requirements
- Review the complete installation process
- Review Installation Notes and Best Practices in the Change Auditor Installation Guide
- Read the Release Notes for updated information
- Ensure that you have the appropriate license files to enable Change Auditor auditing modules. (A separate license file is required to enable the functionality of each of the Change Auditor auditing modules.)

    NOTE: Change Auditor prompts you for a valid license during the coordinator installation. You cannot proceed with an invalid or expired license.

Installation overview

Quest recommends installing the Change Auditor components in the following order:

- Database (SQL Server) — Ensure the SQL server is available and the installation account has SQL Server role as dbcreator. To host the Change Auditor database on a SQL instance other than the default instance of the selected SQL Server, create the instance before running the installer.

  NOTE: The database name must not include embedded spaces, special characters, or supplementary characters. For more details, see Microsoft's database identifier documentation.

- Coordinator — When prompted, specify the SQL server to use and the installation account. The Change Auditor database is created remotely on this server during the installation.

  NOTE: During the coordinator installation, you are have the option of adding the current user to the Change Auditor Administrators security group. If you did not add the current user during the installation process or want to add extra user accounts to the Change Auditor security groups, add them before running the client. We also recommend that you then add these security groups to the appropriate SQL database role (that is, Change Auditor Administrators — <*InstallationName*> group to the Change Auditor_Administrators role and ChangeAuditor Operators — <*InstallationName*> group to the ChangeAuditor_Operators role). See *Add Users to Change Auditor Security Groups* in the *Change Auditor Installation Guide* for more information.

- Client — After you have confirmed that the coordinator is functioning correctly, install the client.

  TIP: Quest recommends that you install the first coordinator and client, but do not deploy agents until after you have installed required coordinators. When deploying agents, you can select which installation to use for each of the agents.

- Agents — Open the client to deploy agents to your domain controllers and member servers. Also, if you have Change Auditor for Logon Activity Workstation licensed, deploy agents to the domain to monitor for logon activity.
- Web client — Optionally, install the web client on the IIS web server.

Step 1: Install a coordinator

IMPORTANT: Minimum permissions

User account installing the coordinator:

The user account that is installing the coordinator must have permission to perform the following tasks on the target server:

- Windows permissions to create and modify registry values.
- Windows administrative permissions to install software and stop or start services.

The user account must also be a member of the **Domain Admins** group in the domain where the coordinator is being installed.

Service account running the coordinator service (LocalSystem by default):

- Active Directory permissions to create and modify SCP (Service Connection Point) objects under the computer object that is running a Change Auditor coordinator.
- Local Administrator permissions on the coordinator server.

If you are running the coordinator under a service account (instead of LocalSystem), define a **Manual** connection profile where you can specify the IP address of the server hosting the coordinator. You can specify and select connection profiles whenever you open the Change Auditor client. See the Change Auditor User Guide or online help for more information about defining and selecting a connection profile.

SQL Server database access account specified during installation:

Create an account that the coordinator service can use on an ongoing basis for access to the SQL Server database. This account must have a **SQL Login** and be assigned the following SQL permissions:

- Must be assigned the **db_owner** role on the Change Auditor database
- Must be assigned the SQL Server role of **dbcreator**

NOTE: If you are using AlwaysOn Availability Groups and SQL server authentication the SQL Login account must be assigned the sysadmin role on every SQL server in the Availability Group.

To install a coordinator:

1. Verify that the user account used to run the coordinator installation is at least a **Domain Admin** in the domain to which the coordinator server belongs.

   NOTE: Membership in the Enterprise Admins group is not required, but can make agent deployment to domain controllers in multiple domains easier. Deploying agents to member servers requires that you must be a Domain Admin in every domain that contains servers that you are targeting for installation.

2. Use an existing account or create a user account in Active Directory that Change Auditor will use to access the SQL Server.
3. Create a SQL Login for this Active Directory user account and assign the following permissions to this login: Server role: **dbcreator**
4. From the member server, insert the Change Auditor DVD or if you downloaded the product from the Quest website, run the **autorun.exe** file.
5. Click **Install** for the **Install Change Auditor Coordinator** option to open the Change Auditor Coordinator Setup wizard.
6. Enter the information requested in the Coordinator Setup wizard.

   Review the table for additional information. This table only covers unfamiliar information. It does not include all the wizard screens or field descriptions.

Table 1. Coordinator Setup wizard

Product Licensing screen	
Licenses	Click **Open License Dialog** to locate and apply a license. **NOTE:** Change Auditor 7.0 requires a new license for all modules.
Installation Name screen	
After licensing the product, the setup wizard prompts you to enter a unique installation name to identify the database to which the coordinator will connect.	
ChangeAuditor Installation Name	Enter a unique Change Auditor installation name that identifies the current installation within your Active Directory environment. An installation name is required; has a limit of 22 characters; can only contain alphanumeric characters and underscores; and is converted to all caps. **NOTE:** Quest recommends that you use the default (DEFAULT) installation name. **NOTE:** If you entered an existing installation name, confirm that you want to join this component to an existing installation. Click **Yes** to proceed or **No** to reenter a unique installation name. **NOTE:** If you plan to add the Change Auditor database to a SQL AlwaysOn Availability Group, ensure that the availability group has already been configured and then specify the name of the availability group listener for SQL server name.
SQL Server Information screen	
SQL Server and Instance	Enter the server name or IP address (member server running the SQL instance) and the SQL instance name for the Change Auditor coordinator database such as, <*FQDN of the SQL server*>\<*instance name*>. Or browse your Active Directory network to locate the required instance. **NOTE:** If you are using Windows security to access your SQL Server, ensure that the domain user is granted access to the SQL Server.
Name of database catalog	Enter the name to assign to the Change Auditor database. **NOTE:** If an existing Change Auditor database is present, you should provide a unique name for the Change Auditor database. If a database with the name entered is found, a warning message explains the need to provide a unique name for your new Change Auditor database. On this warning dialog, click **Cancel** to specify a different database name. Clicking **OK** proceeds to the Ready to Install the Program screen.
Authentication/ Credentials	Use the authentication section to specify whether to use Windows authentication or SQL authentication when communicating with the SQL database instance. (The authentication method is set up when SQL is installed.) **NOTE:** If **Windows Authentication** is used to access the designated SQL instance, a verification screen is displayed. Verify that the server name, SQL instance name, and credentials are correct before proceeding. Incorrect entries cause the Change Auditor coordinator service to fail on startup.

Table 1. Coordinator Setup wizard

ChangeAuditor Administrators screen	
Add the current user to the “ChangeAuditor Administrators - <*InstallationName*>” security group	This check box is selected by default and adds the current user to the ChangeAuditor Administrators — <*InstallationName*> group. Any user that is running a Change Auditor client must be added to either this security group or the ChangeAuditor Operators security group. In addition, users responsible for deploying Change Auditor agents must be a member of the ChangeAuditor Administrators group in the specified ChangeAuditor installation. See Add Users to Change Auditor Security Groups for more information about these security groups and how to add more user accounts.
Specify Port Information screen	
By default Change Auditor dynamically assigns communication ports to use to communicate with each installed coordinator. However, using the port settings on this screen you can specify static SCP listening ports to use instead. **NOTE:** A zero (0) indicates that a dynamic port is being used. These port assignments can also be set using the Coordinator Configuration Tool which is accessed by right-clicking the Change Auditor coordinator system tray icon.	
Client Port	Enter the static port number for the Change Auditor client to communicate with the coordinator. **TIP:** If you are planning on installing the Change Auditor web client, enter a static client port.
Public SDK Port	Enter the static port number for external applications to access the coordinator.
Agent Port (Legacy)	Enter the static port number for legacy (5.x) Change Auditor agents to communicate with the coordinator.
Agent Port	Enter the static port number for Change Auditor 6.x agents to communicate with the coordinator.

7 After you have entered all the requested information, click **Install** to start the installation process.

8 Verify that the coordinator service has been installed by right-clicking the Change Auditor coordinator icon in the system tray and clicking **Coordinator Status**. Check for the correct version and that the Coordinator Status is 'Running'.

9 If you are using the SQL AlwaysOn Availability Groups functionality, you now need to put the database in an SQL availability group.

   a Stop the coordinator.

   b Put the database is in full recovery mode.

   c Backup the database.

   d Move the database to a previously configured availability group.

   e Allow database replication to complete.

   f Start the coordinator.

Step 2: Install the client

The client connects directly to the coordinator or to an archive database and is the user interface that provides immediate access to key configuration change information.

1 On a workstation, laptop or member server, insert the Change Auditor DVD or run the **autorun.exe** file.

2 On the Install page, select **Install Change Auditor Client** to open the Change Auditor Client Setup wizard.

3 Enter the information requested on the Client Setup wizard pages:

- When prompted, read and accept the license agreement.
- On the Select Installation Folder page, click **Next** to accept the default installation path (%ProgramFiles%\Quest\ChangeAuditor\).
- On the Configure Shortcuts page, select the locations where you'd like to create shortcuts for the client.
- On the Ready to Install page, click **Install** to begin the client installation.
- On the last page of the setup wizard, click **Finish** to exit the wizard.

4 Use Add/Remove Programs to verify that the Change Auditor client was successfully installed.

Step 3: Add user accounts to Change Auditor security groups

During the coordinator installation process, you were presented with the option to add the current user to the ChangeAuditor Administrators security group in the specified Change Auditor installation. If you elected not to add the current user during the installation process or wish to add additional user accounts, please use the following procedure; otherwise skip to Step 4: Start the client.

1 Once the coordinator and client are installed, you must add all of the user accounts who will be running the client to one of the following security groups:

- ChangeAuditor Administrators - <*InstallationName*> Group - provides access to all aspects of Change Auditor and to roll out Change Auditor agents
- ChangeAuditor Operators - <*InstallationName*> Group - provides access to Change Auditor with the exception of making configuration changes

2 In addition, all users responsible for deploying agents must also be a member of the ChangeAuditor Administrators group in the specified Change Auditor installation.

3 Use one of the following applications to add the appropriate user accounts to the Change Auditor security groups:

- Domain in Native Mode: Use the Active Directory Users and Computers MMC snap-in.
- Domain in Mixed Mode: Use the Microsoft Computer Management native tool.

> **NOTE:** For more detailed instructions on adding user accounts to security groups, refer to the Change Auditor Installation Guide.

4 To apply the change, logout and back in.

5 All users running a Change Auditor client must have also the proper SQL credentials for accessing the Change Auditor database.

6 One way of accomplishing this would be to add the ChangeAuditor Administrators and ChangeAuditor Operators groups to the appropriate SQL database roles which were also created during the coordinator installation:

- ChangeAuditor_Administrators
- ChangeAuditor_Operators

7 Open the Microsoft SQL Management Studio and connect to the SQL database server.

8 Create a SQL login for the ChangeAuditor Administrators group and assign this login to the ChangeAuditor_Administrators role for the Change Auditor database.

9 Create a SQL Login for the ChangeAuditor Operators group and assign this login to the ChangeAuditor_Operators role for the Change Auditor database.

> **NOTE:** For more detailed instructions on adding groups to SQL database roles, see the Change Auditor Installation Guide.

Step 4: Start the client

After completing the installation (which includes installing a coordinator and at least one client), the next step is to ensure that you can connect to the coordinator.

1 Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client**.

The Connection screen opens where you can connect to the 'default connection' profile or define or specify a different connection profile.

A connection profile defines the connection method used to connect to a coordinator in trusted or untrusted forests, or to the database directly without connecting with the coordinator. See Manage Connection Profiles in the Change Auditor User Guide for more information about defining connection profiles.

2 Initially, select **Connect** to use the default connection profile.

After you have defined alternate connection profiles, select the appropriate profile from the drop-down list and click **Connect**.

> **TIP:** If you cannot connect, ensure that the Quest Change Auditor Coordinator service is running and that you are a member of either the ChangeAuditor Administrators or ChangeAuditor Operators security group.

3 If you do not have the proper credentials required for access, the appropriate credentials dialogs will be displayed allowing you to enter the required credentials.

4 Once connected, you will be presented with the Start page. Select the Deployment tab to select the servers to which agents are to be deployed.

Step 5: Deploy agents

To deploy agents:

1 Verify that the user account you are using to deploy agents is at least a **Domain Admin** in every domain that contains servers or workstations where agents will be deployed.

2 Verify that the user account is a member of the ChangeAuditor Administrators group in the specified Change Auditor installation.

3 Open the client. If agents have not yet been deployed, select the **Deployment** tab. Otherwise, use **View | Deployment**.

The Deployment page is populated with the servers (domain controllers and member servers) and workstations in your Active Directory environment.

> **NOTE:** The Deployment page may initially be empty until the current forest's server topology has been initially harvested. Topology scan takes a long time when the environment contains many workstations. This page is automatically refreshed after this task has completed.

4 From this list, select an entry and use the **Credentials | Set** tool bar button or right-click command to enter the proper user credentials for installing agents on the selected domain.

On the Domain Credentials dialog, select the domain from the list and click **Set**. On the Logon Credentials dialog, enter the credentials of a user with administrator rights on the selected domain.

5 After entering the proper credentials, select the entry back on the Deployment page and select **Credentials | Test**. If you get a **Valid Creds** status in the **Deployment Result** column, you can start deploying agents to that domain.

If you get a **Logon Failure** status in the **Deployment Result** column, use the **Credentials | Set** command to enter the proper credentials for installing agents.

6 By default, the Change Auditor agent folders (Agent, Systray) are installed to %ProgramFiles%\Quest\ChangeAuditor\. You can, however, change the location of the installation folder by clicking **Advanced Options**.

7 Select one or more servers or workstations on the Deployment page and click **Install or Upgrade**.

8 On the Install or Upgrade dialog select one of the following options to schedule the deployment task:

- Now (default)
- When

If you select the **When** option, enter the date and time when you want the deployment task to initiate. Click **OK** to initiate or schedule the deployment task.

Back on the Deployment page, the **Agent Status** column displays 'Pending' and the **When** column displays the date and time specified.

NOTE: To cancel a pending deployment task, select the server or workstation and then click **Install or Upgrade**. On the Install or Upgrade dialog, click **Clear Pending**.

9 As agents are successfully connected to the coordinator, the corresponding **Deployment Result** cell displays 'Success', the **Agent Status** cell displays 'Active' and a desktop notification displays in the lower right-hand corner of your screen.

NOTE: To deactivate these desktop notifications, select **Action | Agent Notifications**.

Once agents are deployed and you open the client, the Overview page opens and provides a real-time stream of events based on a 'favorite' search definition and other summary information.

NOTE: After the deployment, the Version cell might display a previous version of an agent if you installed the agent on an unsupported platform.

3

Change Auditor Walkthrough

Check agent status

Once agents have been deployed, the next step is to ensure that all the agents have checked in.

1. From within the client, use the **View | Statistics | Agent** menu command to open the Agent Statistics page.
2. A list of all deployed agents are displayed. Check to ensure that the status of each agent is 'Active'.

   NOTE: If an agent's status is not connected, ensure that the agent service is running on that domain controller or member server.

Change Auditor client overview

The client connects directly to the Change Auditor database and provides immediate access to key configuration change information. The following table describes the tasks that can be performed.

Table 2. Change Auditor tasks by page

Tabbed page:	Tasks that can be performed on page:
Overview	• Access valuable information about the application (for example, agent status, coordinator status, top agent activity) • View real-time results for your 'favorite' search
Deployment	• Install or upgrade agents and view deployment results • Uninstall an existing agent service • Enable auto deployment to new servers and workstations • Modify default agent installation location and settings • View associated agent and coordinator logs • Print the contents of the Deployment page

Table 2. Change Auditor tasks by page

Tabbed page:	Tasks that can be performed on page:
Searches	• View list of available searches • View or modify the properties of a search query • Create custom searches • Run searches • Set a search as a 'favorite' • Enable and disable alerting for individual search queries • View alert history • Enable and schedule email reporting for individual search queries • Define client and report content for individual search results • Publish search query results to Quest Knowledge Portal • Print the contents of the Searches page
Search Results	• View search results • View event details or search properties • Copy, email, or print event details • Display a knowledge base topic for an event • Add comments to an event • Disable an event • Request more information about the user object of an event • Run extra search queries related to an event • Preview results based on changes made to a search • Compare results side by side • Print search results
Agent Statistics	• Get a global view of all installed agents • Review status and statistics for each agent • View properties of managed resources • Stop, start, and restart an agent • Retrieve associated trace logs • Print agent statistics
Coordinator Statistics	• Get a global view of all installed coordinators • Review status and statistics for each coordinator • Retrieve associated trace logs • Print coordinator statistics
Log	• View selected trace log • Search selected trace log
Administration Tasks	Configuration task list: • Define and assign agent configurations • Configure coordinator email notifications • Define group expansion • Create and schedule purge jobs • Disable private alerts and reports • Create report layout templates that define the header and footer information to be displayed in reports • Define who is authorized to use the client features (Windows client and web client) • Create event subscriptions to send events to SIEM products

Table 2. Change Auditor tasks by page

Tabbed page:	Tasks that can be performed on page:
Administration Tasks	Auditing task list: • Enable and disable event auditing and modify an event's severity level or description • Create Excluded Accounts templates to define individual accounts to exclude from auditing • Define custom Active Directory object class auditing • Define custom AD attribute auditing • Define a Member of Group auditing list to specify the users to audit based on their group membership • Define Active Directory containers to exclude from Active Directory query auditing • Define custom ADAM (AD LDS) object class auditing • Specify ADAM (AD LDS) attributes for auditing • Define an Exchange Mailbox auditing list to specify what directory objects' mailbox activities to audit • Create Office 365 auditing templates to specify the type of Exchange Online, SharePoint Online, and OneDrive for Business activity to audit. • Create Azure Active Directory auditing templates to define the Azure Active Directory activity to audit. • Create SQL auditing templates to define the SQL instances and operations to audit • Create SQL Data Level auditing templates audit changes to databases and tables. • Create VMware auditing templates to specify the VMware vCenter or ESX hosts to audit • Create SharePoint auditing templates to define the SharePoint farm and paths to audit • Create File System auditing templates to define the files and folders to audit • Create Registry auditing templates to define the registry keys to audit • Create Service auditing templates to specify the system services to audit • Create EMC auditing templates for each EMC file server (CIFS) to audited • Create NetApp auditing templates for each NetApp filer to audit • Create Skype for Business auditing templates to audit configuration and security setting changes in Microsoft Skype for Business Server 2015 and Microsoft Lync Server 2013.
Administration Tasks	Protection task list: • Define protection for critical Active Directory objects • Define protection for critical ADAM (AD LDS) objects • Define protection for critical Group Policy objects • Define protection for critical Exchange Mailboxes • Define protection for critical File System files, folders, and shares
Alert History	• View details regarding the events that triggered an SMTP alert

Client walkthrough

The following scenarios introduce you to some of Change Auditor's functionality.

Set up your testing environment, by performing the following tasks:

- Use the Searches page to run a report and generate a Search Results page
- Use the Coordinator Configuration page (on the Administration Tasks tab) to set up email notification and reporting
- Use the Searches page to enable an SMTP alert
- Use the Searches page to enable and schedule reporting

NOTE: These scenarios assume that Change Auditor for Active Directory is licensed. If it is not licensed, changing Active Directory will not generate any of the events mentioned.

Make changes to Active Directory and run a query

1. Make changes to Active Directory, for example:
   - Open Active Directory Users and Computers and add an OU called 'Quest Test'. This OU can be at any level within the AD topology.
   - Create and link a new GPO called 'Sample GPO' to the Quest Test OU.

     NOTE: If you are using Windows Server® 2008 R2, use the Group Policy Management Console to create a GPO.
   - Add a new user to the Domain Admins security group.
   - Finally, open Active Directory Sites and Services and expand the Inter-Site Transport folder, then the IP folder. Double-click the DEFAULTSITELINK and change the replication interval.
2. Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client**.
3. Click the **Searches** tab.
4. Expand the **Shared | Built-in** folder and then the **All Events** folder.
5. In the right pane, locate **All Active Directory Events** and double-click the entry. This runs the selected report.
6. A new Search Results page is displayed populated with the Active Directory events generated.
7. Ensure that the following events were generated for each of the Active Directory changes made:
   - A new OU was added.
   - A new GPO was created, renamed, and linked to an OU (three events).
   - A new user was added to the Domain Admins security group (two events).
   - The DEFAULTSITELINK was changed.
8. To display more details for an event, double-click the event entry in the results grid of the Search Results page.

Set up email alert notifications and reporting

To use the alerting and reporting features, first enable SMTP and define the Mail Server to use in the SMTP Configuration pane on the Coordinator Configuration page.

NOTE: The following procedure assumes that SMTP has been configured to receive Change Auditor notifications.

To configure STMP Mail Server for alerting and reporting:

1. Select **View | Administration** to open the Administration Tasks page.
2. Click **Configuration** task button at the bottom of the navigation pane (left pane).
3. Select **Coordinator** in the Configuration task list to open the Coordinator Configuration page.
4. On the SMTP Configuration pane, select the **Enable SMTP for Alerts and Reporting** check box to enable email notifications.
5. Checking this option activates the remaining fields on this pane to configure email notifications. Enter the following information:
   - Mail Server - enter the name or IP address of the Mail Server
   - From Address - enter or click the browse button to the far right of this field to specify the email address from which email notifications are to originate
   - Reply To (optional) - enter or click the browse button to the far right of this field to specify the email address where replies to email notifications are to be sent (leave blank for this scenario).
   - Subject Line (leave default entry for this scenario)
6. If the specified Mail Server requires authentication, select the **My Server Requires Authentication** check box and enter the account information.

   NOTE: Leave the Exchange Host information blank for this scenario. Providing this additional information allows you to look up user accounts in Exchange and Active Directory.
7. Click **Test SMTP** to test the Mail Server configuration.
8. After the Mail Server configuration is verified, click **Apply Changes** to save the configuration.
9. Now that SMTP is enabled and configured, you can enable email alerts for individual search definitions. In addition, you can also enable email reporting for individual searches.

Enable email alerts for 'all events'

Using the Searches page, you can enable and disable alert notifications for individual search definitions and dispatch them via SMTP (email).

To enable email alerting:

1. Click the **Searches** tab.
2. In the left pane, expand the **Shared | Built-in** folder and then the **All Events** folder.
3. In the right pane, locate the **All Events** search definition, right-click, and select the **Alert | Enable Transport | SMTP** command.
4. Click **Yes** to confirm that you want to enable alerting for the selected search.
5. On the Alert Custom Email dialog, enter the email address of the persons who are to receive the alert.

   NOTE: To send an alert to the user who initiated the change that triggered the alert, select the **Add Who** check box at the bottom of the Alert Custom Email dialog.

   To later disable the alerts, return to the **Searches** tab, right-click the **All Events** search definition and select **Alert | Disable Alert**. Click **Yes** to confirm that you want to disable the alert.

Enable and schedule email reporting for ‘all events’

When reporting is enabled, a report containing the search results of an individual search is sent as an attachment via email to the designated recipients.

To enable and schedule reporting:

1. Open the Searches page.
2. In the left pane, expand the **Shared | Built-in** folder and then the **All Events** folder.
3. In the right pane, locate and select the **All Events** search definition.
4. Open the Report tab, select the **Send to a mailbox** option, enter a valid email address in the **To** field and then select the **Report Enabled** check box.
5. Specify the report configuration settings:
   - Layout: Select the report layout template to be used. Leave this set to **Default**.
   - Report: Specify when the report is to be generated/sent (that is, on a weekly or monthly schedule).
   - Run Time: Specify the time at which the report is to be run.
   - Attach: Select the report format to be used. PDF is the default.
   - Columns: Define how the report content is to fill the page. Leave this set to **Fit to Page**.
   - Time Zone: Select the time zone to be used for the report’s time stamp in the report email. By default, the time zone of the computer where the client resides is used.
6. Click **Save**.

   To later disable reporting, return to the **Searches** tab, right-click the **All Events** search definition and select **Report | Disable Report**. Click **Yes** to confirm that you want to disable reporting for the selected search.

To test the alerting and reporting:

1. To test alerting and reporting, undo the Active Directory changes previously made:
   - Open Active Directory Users and Computers and delete the 'Quest Test' OU.
   - Delete the 'Sample GPO' GPO.
   - Remove the user you added to the Domain Admins security group.
   - Open Active Directory Sites and Services and expand the Inter-Site Transport folder, then the IP folder. Double-click the DEFAULTSITELINK and change the replication interval back to its original setting.
2. Wait approximately two minutes for the coordinator to pick up the events and trigger the alert and report to be sent. (This time may be quicker or slower depending on email latency.)

4

Change Auditor for Active Directory

The scenarios presented in this section show you how to use some additional Active Directory auditing features offered in Change Auditor for Active Directory.

- Audit custom user attributes
- Audit users based on their group membership

NOTE: Active Directory auditing is only available if you have licensed the Change Auditor for Active Directory auditing module. You will not be prevented from specifying Active Directory auditing; however, associated events will not be captured unless the proper license is applied.

See Change Auditor Product Specific Features for the list of features/functionality dependent on the different product licenses. For more detailed information on Active Directory auditing, see the Change Auditor for Active Directory User Guide.

Audit custom user attributes

Active Directory Attribute auditing allows you to specify individual schema attributes to audit.

To define custom attribute auditing:

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **Attributes** under Active Directory in the Auditing task list to open the Active Directory Attribute Auditing page.
4. Select an object class from the list located across the top of this page. Selecting an entry in this list, will populate the list boxes across the bottom of the dialog with the applicable attributes.

   For example, select the **group** object.
5. In the Unmonitored Attribute list box, located in the lower left pane of this page, select one or more attributes and use the **Add** button to select them for auditing.

   For example, select the **description** attribute.
6. To change the severity level assigned to an attribute, in the right-hand list box, place your cursor in the **Severity** cell and use the drop-down arrow to select the severity you want to assign to the selected attribute.
7. To remove an attribute from auditing, select the attribute from the right pane and click **Remove** to move the selected attribute back into the Unmonitored Attribute list box.
8. Once you have selected at least one attribute for auditing, the associated Monitored Attributes column in the list box across the top of this page will display the number of custom attributes selected for auditing. This value will also be displayed in the Monitor Attributes column back on the Active Directory Auditing page.

   NOTE: The default attributes which are automatically being audited for each object are NOT included in the Monitored Attributes counts.

9 To test these events, make a change to the attribute selected for auditing.

For example, launch Active Directory Users and Computers and change the description of a user.

10 Go back to the client and re-run the **All Events** report.

- Open the **Searches** tab.
- Expand the **Shared | Built-In | All Events** folder in the left pane.
- Locate and double-click **All Events** in the right pane.
- This will display a new Search Results page displaying the events.

Audit users based on their group membership

The Member of Group auditing feature allows you to audit specific users based on their group membership.

To define a Member of Group Auditing list:

1 Open the Administration Tasks tab.

2 Click **Auditing**.

3 Select **Active Directory** under the Auditing task list to display the Active Directory Auditing page.

4 From this page, select the **user** object class and click the **Delete** tool bar button. (By default, Change Auditor monitors all users; therefore, to use this feature, you must first delete the user object class.)

5 From the left pane of the Administration Tasks tab, select **Member of Group** under Active Directory in the Auditing task list to display the Member of Group Auditing page.

6 Click **Add** to display the Member of Group Auditing wizard.

7 Use the Browse and Search pages to locate and select a group and click **Add** to add the selected group to the Selected Objects list at the bottom of the wizard.

Repeat this step until you have selected all of the groups you want to add to the Member of Groups Auditing list. Then click **Select** to save your selections, close the wizard and return to the Member of Group Auditing page, where your selections will now be listed.

8 To test the auditing of users based on their group membership, make one or more changes to a user object that is included in the previously defined Member of Groups Auditing list.

You can also make changes to a user object that is not in the list to verify that no events will be generated for that user.

9 Go back to the Change Auditor client and re-run the **All Events** report.

- Open the **Searches** tab.
- Expand the **Shared | Built-In | All Events** folder in the left pane.
- Locate and double-click **All Events** in the right pane.
- This will display a new Search Results page displaying the events.

10 Ensure that the changes you made to the user objects in the list are displayed and that the changes you made to the user objects not in the list are not displayed.

5

Change Auditor for Windows File Servers

Change Auditor for Windows File Servers allows you to search, report and alert on changes to a specific file or folder or all volumes. You can receive real-time alerts whenever someone tries to access a secure file or folder. The scenarios in this chapter show you how to set up file system auditing.

- Getting started
- Create a File System Auditing template
- Make file system changes and run a query

NOTE: File System auditing is only available if you have licensed the Change Auditor for Windows File Servers auditing module. You will not be prevented from specifying file system auditing; however, associated events will not be captured unless the proper license is applied.

See Change Auditor Product Specific Features for a list of features/functionality dependent on a specific product license. For more detailed information about file system auditing, see the Change Auditor for Windows File Servers User Guide.

Getting started

1. Verify that Change Auditor for Windows File Servers is licensed.
2. To view applied licenses, select **Help | Licensing** from the client.

   OR

   To view and apply a license, right-click the coordinator icon in the system tray and select **Licensing**. If required, click **Select License** to locate and apply the license.
3. Create a new folder on the C: drive of an agented server and then add a new .txt file in this folder. This folder will be used in the following scenarios as an auditing target.
4. In order to capture File System events in Change Auditor, you must first complete the following steps to define the files/folders to be audited and the operations to be captured:
   - Create a File System Auditing template which specifies the files/folders and operations to be audited.
   - Add this template to an agent configuration.
   - Assign the agent configuration to Change Auditor Agents.

   Refer to the procedures on the following pages to perform these tasks.

Create a File System Auditing template

For this scenario, we will create a template to audit all changes made to the folder you just created.

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **File System** in the Auditing task list to open the File System Auditing page.
4. Click **Add** to launch the File System Auditing wizard which will step you through the process of creating a File System Auditing template.
5. On the first page of the wizard, enter the following information:
   - Enter a name for the template.
   - Select the **Folder** option.
   - Enter the name of the folder or click the browse button to select the folder you previously created on the C: drive.

   Click **Add** to add the specified folder to the selection list (middle of the page). This new entry is automatically selected in the list, which enables the following settings/tabs:
   - By default, the scope of coverage for the selected folder will be **This Object and All Child Objects.** Leave this setting for this scenario; however, if you wanted to change this setting, use the drop-down arrow in the **Scope** cell.
   - On the Events tab, select the **File Events** and **Folder Events** check boxes to track all changes made to the selected folder.
   - Open the Inclusions page, enter * and click **Add** to add it to the Included Names list. Entering * will audit all files and folders in the selected folder.
   - Skip the Exclusions tab. In this scenario, we will not be excluding any subfolders or files from auditing.
6. (Optional) If you want to define any processes that are to be allowed to change audited objects without generating an event, click **Next**. Select one or more processes from the list at the top of the page and click **Add** to add them to the list box at the bottom of the page.
7. To create the template and assign it to an agent configuration, expand the **Finish** button and select **Finish and Assign to Agent Configuration**.
8. On the Configuration Setup dialog select the agent configuration (right pane) to which the template is to be assigned and ‘drag and drop’ it onto the newly created template**.**

   The **Assigned** cell for the template will change to **Yes**.
9. Click **OK** to save your selection, close the dialog and display the Agent Configuration page.
10. If this configuration is not assigned to any agents, you will need to assign it to one or more installed agents at this time.
    - On the Agent Configuration page, select one or more agents from the agent list and click the **Assign** tool bar button.
    - On the Agent Assignment dialog, select the configuration definition to be assigned to the selected agents and click **OK**.
11. On the Agent Configuration page, select the agents assigned to use the modified agent configuration and click **Refresh Configuration**. This will ensure the agents use the latest configuration.

    NOTE: If you do not refresh the agent’s configuration, the client will automatically check for a new agent configuration based on the polling interval setting (located on the Systems Setting tab of the Configuration Setup dialog). The default is every 15 minutes.

Make file system changes and run a query

1. To test file system auditing, make some changes to the folder specified above, for example:
   - add a .docx file
   - change the security permissions on a file (right-click file, open the Security tab and add another user with full control)
   - delete the sample .txt file
   - add a sub-folder
   - change the security permission of the new folder
2. Go back to the client to review the events generated. You can display them by either:
   - Opening the Agent Statistics tab, locating the agent where these changes were made and clicking the number link in the **Events Today** column.
   - Opening the Searches tab and running the **All File System Events** report.
     - Expand the **Shared | Built-in | All Events** folder in the left pane.
     - Locate and double-click **All File System Events** in the right pane.

6

Change Auditor for Exchange

Change Auditor for Exchange provides extensive, customizable auditing and reporting for all critical changes to Exchange, including administrative groups, mailbox policies, public and private information store auditing, organizational changes such as ActiveSync mailbox policy changes, distribution list changes and more. The scenarios in this chapter introduce you to Exchange auditing and how to set up Exchange mailbox auditing for your Exchange environment.

- Getting started
- Make changes in Exchange and run a query
- Enable Exchange mailbox auditing

NOTE: Exchange auditing is only available if you have licensed the Change Auditor for Exchange auditing module. You will not be prevented from specifying Exchange auditing; however, associated events will not be captured unless the proper license is applied.

See Change Auditor Product Specific Features for a list of Quest features/functionality dependent on a specific product license. For more detailed information about Exchange auditing, see theChange Auditor for Exchange User Guide.

Getting started

1. Verify that Change Auditor for Exchange is licensed.
2. To view applied licenses, select **Help | Licensing** from the client.

   OR

   To view and apply a license, right-click the coordinator icon in the system tray and select **Licensing**. If required, click **Select License** to locate and apply the license.
3. Verify that Change Auditor is setup to monitor all users in the domain.
   - Launch the Change Auditor client and open the Administration Tasks tab.
   - Open the Active Directory Auditing page. Verify that the user object class is listed. (*This object class is included by default, however, we removed the user object class as part of the 'Auditing Users Based on Their Group Membership' scenario from the Change Auditor for Active Directory Auditing section.*)
   - If it is not listed, click **Add** to add it. Restart the agent to use the latest configuration.

Make changes in Exchange and run a query

1 Create a new test user with an Exchange mailbox.

2 Make some changes to the test user just created. For example:

- Create a new alternate SMTP address (e.g., alternate@yourcompany.com).
- Create a new primary SMTP address (e.g. primary@yourcompany.com).
- Set the address created above as the primary SMTP address.
- Change the **Delivery Options** to specify a user to send email on behalf of.

3 Make some additional changes to Exchange. For example:

- Add a new filter to catch emails sent from spam@spam.com.
- Create a new Administrative Group called 'Test'.

4 Launch the Change Auditor client and run the 'All Exchange Events in the last 24 hours' report to view the events generated from the changes made above.

- Open the Searches tab.
- Expand the **Shared | Built-In | Recommended Best Practice | Exchange** folder in the left pane.
- Locate and double-click **All Exchange Events in the last 24 hours** in the right pane.

This will display a new Search Results page displaying the events.

Enable Exchange mailbox auditing

To enable Exchange mailbox auditing, you must first define whose mailbox activities (users or groups) are to be audited.

To define an Exchange mailbox auditing list:

1 Open the **Administration Tasks** tab.

2 Click **Auditing**.

3 Select **Exchange Mailbox** in the Auditing task list to open the Exchange Mailbox Auditing page.

4 Click **Add** to display the Exchange Mailbox Auditing wizard.

5 If not already selected, select the **This Object** option at the top of the first page.

Use the Browse and Search pages to locate and select a directory object (i.e., User, Group, Container, DomainDNS, OrganizationalUnit, BuiltinDomain) and click the **Add** button to add the selected object to the Selected Object list at the bottom of the page.

Repeat this step until you have selected all the directory objects you want added to the Exchange Mailbox Auditing list.

6 Click **Finish** to close the wizard and return to the Exchange Mailbox Auditing page, where your selections will now be listed.

7 If you specified to audit an individual user's mailbox and you want to audit for 'by owner' events, place your cursor in the **Events** cell, click the arrow controls and select the **Owner, Non-Owner** option from the drop-down list.

8 In addition, some of the Exchange Mailbox Monitoring events are disabled by default due to the potentially high volume of events that can occur. If you want to capture any of these events, you will need to enable them.

- Open the Administration Tasks tab and open the Audit Events page (select **Audit Events** under the Auditing task list).
- Locate the Exchange Mailbox Monitoring events to be enabled. You can sort the event list in one of the following ways:
  - Click on the **Status** column heading to sort the list by Disabled/Enabled -- bringing the disabled events to the top of the list.
  - Click in the data filtering cell under the Facility Name heading and start typing **Exchange Mailbox Monitoring**. As you type, this will filter the list to display only those events included in the Exchange Mailbox Monitoring facility.
  - If there is a specific event, click in the data filtering cell under the Event Class heading and start entering the name of the event. As you type, this will filter the list to include only those events that match the characters entered.
- Select the entry to be enabled and click the **Enable** tool bar button.

9 To test the Exchange Mailbox Monitoring events, open Outlook and perform various mailbox activities for any of the users included in your Exchange Mailbox Auditing List.

10 Go back to the Change Auditor client and run the **All Exchange Events** report.

- Open the Searches tab.
- Expand the **Shared | Built-In | All Events** folder in the left pane.
- Locate and double-click **All Exchange Events** in the right pane.

This will display a new Search Results page displaying the events.

7

Customizing Change Auditor

Now that you are familiar with running searches and viewing the results received, let's discuss some additional features which allow you to customize what is being audited by Change Auditor and the results you are receiving.

- Create a custom search
- Group and filter data
- Create a Change Auditor events list
- Exclude accounts from auditing

Create a custom search

If you do not see a Built-in Report that suits your needs, it is very easy to create a custom report under the **Private** or **Shared** folder in the explorer view (left pane of the Searches page). Private searches are those that only you can run and view, whereas Shared searches can be run and viewed by all Change Auditor users.

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

3 Click **New** at the top of the Searches page to display and activate the Search Properties tabs, where you can define the search criteria.

See the table below for a brief description of the tabs available and how to define search criteria. For more detailed information, refer to the Change Auditor User Guide.

Table 3. Search Properties tabs used to define search criteria

Tab	Description	How to add criteria
Info	Name your search	1 Enter name 2 Optionally enter description
Who	Search for events generated by a specific user, computer or group. By default, Change Auditor searches for events generated by all users, computers and groups.	1 Click **Add** 2 Select the user/computer/group 3 Click **Add** to add criteria to selection list 4 Click **Select** to save the selection **NOTE:** To use a wildcard expression to specify a user or group, expand the **Add** tool bar button and select **Add Wildcard Expression**.

Table 3. Search Properties tabs used to define search criteria

Tab	Description	How to add criteria
What	Search for events based on subsystem, event class, object class, severity or results. By default, all entities will be included in a new search definition.	1 Click **Add** 2 Use drop-down menu to select an entity 3 Select scope, actions and/or entity (depending on dialog) 4 Click **Add** to add criteria to selection list 5 Click **OK** to save selection
Where	Search for events captured by a specific agent or within a specific domain or site. By default, all agents will be included in a new search.	1 Click **Add** 2 Select the agent, domain, or site 3 Click **Add** to add criteria to selection list 4 Click **OK** to save the selection **NOTE:** To use a wildcard expression to specify a domain, site or agent, expand the **Add** tool bar button and select **Add Wildcard Expression**.
When	Search for events that occurred during a specific date/time range. By default, new searches will include the events captured this week.	1 Check date interval option and enter dates 2 Optionally enter time interval
Origin	Search for events originating from a specific workstation or server. By default, Change Auditor searches for all events regardless of where they originated.	1 Click **Add** 2 Enter a wildcard expression to search for a workstation or server 3 Click **OK** to save the selection

4 Once you have defined the search criteria, click the **Run** tool bar button from one of the Search Properties tabs to save and run the search.

Group and filter data

Using the column headings in the data grids throughout the client, you can customize the content displayed by defining the sort order or sort criteria, moving or hiding columns. In addition, you can group data to create a collapsed view or filter the data to limit the data displayed in the grids to locate specific information.

To group data:

1 Select a column heading (the column heading will pop off the table) and drag that column heading to the space above the table. For example, use the left mouse button to click the **Subsystem** heading and drag that column heading to the space above the table.

2 Optionally, repeat this step to select additional headings to create a hierarchy of groupings.

This will collapse the table and display the groupings that can be expanded to view the detailed information that applies to that group.

3 To expand a group and display the individual events listed, click on the + sign to the left of the label.

4 When a grouping is in place, you can use the **Pie Chart** or **Bar Graph** icons, located at the top of the grid, to redisplay the data.

NOTE: The pie chart and bar graph displays are only available when a single level grouping has been applied to the data grid.

5 In either of these views, use the **Data Grid** icon to redisplay the data in the grid format.

6 To remove a grouping, select the heading and drag it back down into the table area or right-click a group heading (in area above the grid) and select one of the remove commands.

To filter data:

Throughout the client, you will see a row of data filtering cells under the headings row in each of the data grids. These cells provide data filtering options which allow you to filter and sort the data displayed.

1 Place your cursor in one of the cells, and click **Click here to filter data.**

2 In the selected cell, enter the word or string of characters to be used to filter the data displayed. Filtering will take place as you type your entry.

3 By default, Change Auditor will use either the 'starts with' or 'contains' expression to filter the data. However, if you click the search criteria button, you can select a different expression.

4 To remove the filtering and return to the original data grid, click the **Remove Filter** button to the far left of the cells.

5 To remove the filtering of an individual cell, click the **Remove Filter** button to the right of that cell.

Create a Change Auditor events list

From the client, you can print or save the contents of the currently displayed page using the **File | Print** menu commands or the **Print** tool bar buttons. In addition to using the print feature, these procedures introduce some additional heading controls that can be used to customize the content being displayed.

To create an Excel spreadsheet of all Change Auditor events:

1 Open the Administration Tasks tab (**View | Administration**).

2 Click **Auditing**.

3 Select **Audit Events** under the Configuration task list to open the Audit Events page.

4 Optionally, use the heading controls to sort the list, resize or rearrange the columns. (Keep in mind, the print feature prints/saves whatever is displayed in the active Change Auditor page.)

- To change the sort criteria, click on the column heading to be used for the sort criteria.
- To resize a column, place your cursor on the boundary between column headings, click and hold the left mouse button dragging the column boundary to the desired size.
- To move a column, use the left mouse button to click the heading to be moved. Drag the column heading to the desired location.

5 Click the arrow to the right of the **Print** tool bar button and select **Print to File**.

6 On the Save As dialog enter the following information:

- Use the navigation pane (left pane) to select the location where the file is to be saved.
- **File name:** Enter a name for the file. Default is **Events Configuration.<***extension***>**.
- **Save as type:** Click the arrow control and select **Excel files (*.xls)** or **Excel 2007 files (*.xlsx)**.

Click **Save**.

To create a PDF file of all Change Auditor for Exchange events:

1 Open the Audit Events page on the Administration Tasks tab.

2 Use the **License Type** column to filter the events list:

- Place your cursor in the cell directly beneath the **License Type** heading.
- Enter **Exchange.**

You now have an event list that only contains the Exchange events.

3 Optionally, use the heading controls to sort the list, resize or rearrange the columns.

> **NOTE:** Keep in mind, the print feature prints/saves whatever is displayed in the active Change Auditor page.

- To change the sort criteria, click on the column heading to be used for the sort criteria.
- To resize a column, place your cursor on the boundary between column headings, click and hold the left mouse button dragging the column boundary to the desired size.
- To move a column, use the left mouse button to click the heading to be moved. Drag the column heading to the desired location.

4 Click the arrow to the right of the **Print** tool bar button and select **Page Setup**. On the Page Setup page, change the following settings:

- Orientation: Landscape
- Margins (inches): Left: 0.25 Right: 0.25

Click **OK** to save the page setup settings.

5 Select the **Print | Print Preview** option to preview the report. Click the **x** in the Print Preview tab to close the preview page.

6 Back on the Audit Events page, select the **Print** | **Print to PDF** option.

7 On the Save As dialog enter the following information:

- Use the navigation pane (left pane) to select the location where the file is to be saved.
- **File name:** Enter a name for the file. Default is **Events Configuration**.
- **Save as type:** This field is pre-filled with **PDF files (*.pdf)**.

Click **Save**.

Exclude accounts from auditing

Using account exclusions, you can define a list of trusted accounts which are to be excluded from the auditing process. This enables you to exclude events generated by accounts that make a large number of changes via scripting or by accounts which are trusted.

To use the account exclusion feature, you must first complete the following steps to define the user/computer accounts that can make changes without triggering an event in Change Auditor:

1 Open the Administration Tasks tab.

2 Click **Auditing**.

3 Select **Excluded Accounts** under the Auditing task list to open the Excluded Accounts Auditing page.

4 Click the **Add** tool bar button to launch the Excluded Accounts wizard which will step you through the process of creating an Excluded Accounts template.

- On the first page of the wizard, enter a name for the template and optionally select the facilities/event classes to be excluded.

  > **NOTE:** To include ALL event classes/facilities in this Excluded Accounts definition, leave the list box across the bottom of this page empty.

- On the second page of the wizard, use the Browse or Search pages to locate and select the user or computer accounts that are to be excluded from Change Auditor auditing. Click the **Add** button to add these accounts to the list box at the bottom of this page.

5 To create the template and assign it to an agent configuration, expand the **Finish** button and select **Finish and Assign to Agent Configuration**.

6 On the Configuration Setup dialog select the agent configuration (right pane) to which the template is to be assigned and ‘drag and drop’ it onto the newly created template.

The **Assigned** cell for the template will change to **Yes**.

7 Click **OK** to save your selection, close the dialog and display the Agents Configuration page.

8 If this configuration is not assigned to any agents, you will need to assign it to one or more installed agents at this time.

- On the Agent Configuration page, select one or more agents from the agent list and click the **Assign** tool bar button.
- On the Agent Assignment dialog, select the configuration definition to be assigned to the selected agents and click **OK**.

9 On the Agent Configuration page, select the agents assigned to use the modified agent configuration and click **Refresh Configuration**.

Verify that **Auditing** is displayed in the Exclude Account column.

> **NOTE:** If you do not restart the agent, the client will automatically check for a new agent configuration based on the polling interval setting (located on the System Settings tab of the Configuration Setup dialog). The default is every 15 minutes.

10 Use a user account that is included in the exclusion list to make changes to Active Directory, File Systems and/or Exchange.

11 Run the **All Events** report to ensure that the changes you made are NOT reported.

- Open the Searches tab.
- Expand the **Shared | Built-In | All Events** folder in the left pane.
- Locate and double-click **All Events** in the right pane.

8

Change Auditor Product Specific Features

This section provides a summary of the features and functionality that is dependent upon a specific Change Auditor product license.

If a feature/functionality is not listed here, it works in Change Auditor regardless of the license applied.

NOTE: The product will not prevent you from performing any of the administration tasks on the Administration Tasks tab; however, associated events will not be captured and/or associated protection will not occur unless the proper license is applied.

To hide unlicensed Change Auditor features from the Administration Tasks tab (including unavailable events throughout the client), use the **Action | Hide Unlicensed Components** menu command.

Table 4. Change Auditor product specific features

Change Auditor feature/functionality	Change Auditor product license required
Facilities (Searches/Events)	
Authentication Activity	Change Auditor for Logon Activity **NOTE:** Change Auditor for Logon Activity User license is required for capturing authentication activity on server agents; Change Auditor for Logon Activity Workstation license is required for capturing authentication activity on workstation agents.
Authentication Services Monitoring	Change Auditor for Authorization Services
Azure Active Directory - Administrative Units	Change Auditor for Active Directory
Azure Active Directory - Application	Change Auditor for Active Directory
Azure Active Directory - Device	Change Auditor for Active Directory
Azure Active Directory - Directory	Change Auditor for Active Directory
Azure Active Directory - Group	Change Auditor for Active Directory
Azure Active Directory - Policy	Change Auditor for Active Directory
Azure Active Directory - Risk Event	Change Auditor for Active Directory
Azure Active Directory - Role	Change Auditor for Active Directory
Azure Active Directory -Sign-in	Change Auditor for Active Directory
Azure Active Directory - User	Change Auditor for Active Directory
Connection Object	Change Auditor for Active Directory
Custom AD Object Monitoring	Change Auditor for Active Directory
Custom Computer Monitoring	Change Auditor for Active Directory
Custom File System Monitoring	Change Auditor for Windows File Servers
Custom Group Monitoring	Change Auditor for Active Directory
Custom Object Monitoring	Change Auditor for Active Directory
Custom User Monitoring	Change Auditor for Active Directory

Table 4. Change Auditor product specific features

Change Auditor feature/functionality	Change Auditor product license required
Defender	Change Auditor for Defender
DNS Service	Change Auditor for Active Directory
DNS Zone	Change Auditor for Active Directory
Domain Configuration	Change Auditor for Active Directory
Domain Controller Authentication	Change Auditor for Logon Activity **NOTE:** Change Auditor for Logon Activity User license is required for capturing domain controller authentication activity on server agents.
Domain Controller Configuration	Change Auditor for Active Directory
Dynamic Access Control	Change Auditor for Active Directory
EMC	Change Auditor for EMC
Exchange ActiveSync Monitoring	Change Auditor for Exchange
Exchange Administrative Group	Change Auditor for Exchange
Exchange Distribution List	Change Auditor for Exchange
Exchange Mailbox Monitoring	Change Auditor for Exchange
Exchange Organization	Change Auditor for Exchange
Exchange Permission Tracking	Change Auditor for Exchange
Exchange User	Change Auditor for Exchange
Forest Configuration	Change Auditor for Active Directory
FRS Service	Change Auditor for Active Directory
Group Policy Item	Change Auditor for Active Directory
Group Policy Object	Change Auditor for Active Directory
IP Security	Change Auditor for Active Directory
AD Query	Change Auditor for Active Directory Queries
Logon Session	Change Auditor for Logon Activity **NOTE:** Change Auditor for Logon Activity User license is required for capturing logon session activity on server agents; Change Auditor for Logon Activity Workstation license is required for capturing logon session activity on workstation agents.
Skype for Business Administration	Change Auditor for Skype for Business
Skype for Business Configuration	Change Auditor for Skype for Business
NetApp	Change Auditor for NetApp
NETLOGON Service	Change Auditor for Active Directory
NTDS Service	Change Auditor for Active Directory
Organizational Unit (OU)	Change Auditor for Active Directory
Office 365 Exchange Online Administration	Change Auditor for Exchange
Office 365 Exchange Online Mailbox	Change Auditor for Exchange
Office 365 SharePoint Online	Change Auditor for SharePoint
Office 365 OneDrive for Business	Change Auditor for SharePoint
Replication Transport	Change Auditor for Active Directory
Schema Configuration	Change Auditor for Active Directory
SharePoint Document	Change Auditor for SharePoint
SharePoint Document Library	Change Auditor for SharePoint

Table 4. Change Auditor product specific features

Change Auditor feature/functionality	Change Auditor product license required
SharePoint Farm	Change Auditor for SharePoint
SharePoint Folder	Change Auditor for SharePoint
SharePoint List	Change Auditor for SharePoint
SharePoint List Item	Change Auditor for SharePoint
SharePoint Permission	Change Auditor for SharePoint
SharePoint Security Group	Change Auditor for SharePoint
SharePoint Site	Change Auditor for SharePoint
SharePoint Site Collection	Change Auditor for SharePoint
Site Configuration	Change Auditor for Active Directory
Site Link Bridge Configuration	Change Auditor for Active Directory
Site Link Configuration	Change Auditor for Active Directory
SQL Broker Event	Change Auditor for SQL Server
SQL CLR Event	Change Auditor for SQL Server
SQL Cursors Event	Change Auditor for SQL Server
SQL Database Event	Change Auditor for SQL Server
SQL Data Level Database Changes	Change Auditor for SQL Server
SQL Deprecation Event	Change Auditor for SQL Server
SQL Errors and Warnings Event	Change Auditor for SQL Server
SQL Full Text Event	Change Auditor for SQL Server
SQL Locks Event	Change Auditor for SQL Server
SQL Object Event	Change Auditor for SQL Server
SQL OLEDB Event	Change Auditor for SQL Server
SQL Performance Event	Change Auditor for SQL Server
SQL Progress Report Event	Change Auditor for SQL Server
SQL Query Notifications Event	Change Auditor for SQL Server
SQL Scan Event	Change Auditor for SQL Server
SQL Security Audit Event	Change Auditor for SQL Server
SQL Server Event	Change Auditor for SQL Server
SQL Session Event	Change Auditor for SQL Server
SQL Stored Procedures Event	Change Auditor for SQL Server
SQL Transactions Event	Change Auditor for SQL Server
SQL TSQL Event	Change Auditor for SQL Server
SQL User-Configurable Event	Change Auditor for SQL Server
Subnets	Change Auditor for Active Directory
SYSVOL	Change Auditor for Active Directory
Search criteria (What tab)	
Subsystem | Active Directory	Change Auditor for Active Directory
Subsystem | AD Query	Change Auditor for Active Directory Queries
Subsystem | ADAM (AD LDS)	Change Auditor for Active Directory
Subsystem | Exchange	Change Auditor for Exchange
Subsystem | Office 365	Change Auditor for Exchange Change Auditor for SharePoint
Subsystem | File System	Change Auditor for Windows File Servers

Table 4. Change Auditor product specific features

Change Auditor feature/functionality	Change Auditor product license required
Subsystem | Group Policy	Change Auditor for Active Directory
Subsystem | Logon Activity	Change Auditor for Logon Activity
Subsystem | SharePoint	Change Auditor for SharePoint
Subsystem | SQL	Change Auditor for SQL Server
Object Class	Change Auditor for Active Directory
Administration Task tab	
Auditing task list | Forest	
Active Directory	Change Auditor for Active Directory
Active Directory | Attributes	Change Auditor for Active Directory
Active Directory | Member of Group	Change Auditor for Active Directory
Active Directory | Excluded AD Query	Change Auditor for Active Directory Queries
ADAM (AD LDS)	Change Auditor for Active Directory
ADAM (AD LDS) | Attributes	Change Auditor for Active Directory
Auditing task list | Applications	
Exchange Mailbox	Change Auditor for Exchange
Office 365	Change Auditor for Exchange Change Auditor for SharePoint
SQL	Change Auditor for SQL Server
SharePoint	Change Auditor for SharePoint
Auditing task list | Server	
File System	Change Auditor for Windows File Servers
Auditing task list | NAS	
EMC	Change Auditor for EMC
NetApp	Change Auditor for NetApp
FluidFS	Change Auditor for Fluid File System
Protection task list | Forest	
Active Directory	Change Auditor for Active Directory
ADAM (AD LDS)	Change Auditor for Active Directory
Group Policy	Change Auditor for Active Directory
Protection task list | Application	
Exchange Mailbox	Change Auditor for Exchange
Protection task list | Server	
File System	Change Auditor for Windows File Servers

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.