Quest

Quest® Change Auditor for Logon Activity 7.0
User 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 for Logon Activity User Guide
Updated - May 2018
Software Version - 7.0

Contents

1

Change Auditor for Logon Activity Overview

Introduction

Increasing compliance regulations and security concerns make automated, reliable and complete tracking of user activity essential in organizations today. Change Auditor for Logon Activity captures, alerts, and reports on all user logon and log off activity, and promotes better security, auditing and compliance across your enterprise.

This guide has been prepared to assist you in becoming familiar with Change Auditor for Logon Activity. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

- For information on the core functionality available in Change Auditor, see The Change Auditor User Guide and the Change Auditor Installation Guide.
- For event details, see the Change Auditor for Logon Activity Event Reference Guide.

Benefits and features

Change Auditor for Logon Activity offers system-wide visibility, consolidated auditing reports, user activity analysis, automated collection of logon events and a centralized view. Calculated workstation session events deliver an overview of the session in a single event, including the total session length and the reason for logoffs.

More specifically, it provides the following features:

- Compliance-ready: Fulfills and simplifies collection of logon activity for major external regulations and internal security policies.
- Real-time alerts on the move: Sends critical alerts on access attempts (both successful and failed logons) via email and mobile devices to prompt immediate action, enabling you to respond faster to security threats even while you're off-site.
- Security awareness: Easily discerns user logon by type (interactive, remote, local or network) to help identify suspicious activity.
- Related searches: Provides instant, one-click access to all information on the event you're viewing and all related activity, eliminating guesswork and unknown security concerns.
- Best practice reporting: Provides system visibility with comprehensive reports for best practices, such as access reports, successful logons, failed logons, authorization comparison reports and reports grouped by users.

- Event timeline: Enables the viewing, highlighting and filtering of logon activity and related change events over time for better forensic analysis of events and trends.
- Web-based access with dashboard reporting: Searches from anywhere using a web browser, and creates targeted dashboard reports that provide upper management and auditors with access to the information they need without having to understand architecture or administration.

Change Auditor Logon Activity auditing consists of two licenses that allow you to collect logon and log off activity for both servers and workstations.

- The Change Auditor for Logon Activity User license enables server agents to capture the following events:
  - Authentication activity (interactive, remote interactive and network logons) including successful and failed logons performed on monitored servers
  - Domain Controller authentication activity (Kerberos), including successful and failed requests (available for Domain Controller agents only)
  - User logon session activity (the actual time spent on a server)
- The Change Auditor for Logon Activity Workstation license enables workstation agents to capture the following events:
  - Authentication activity (interactive, remote interactive and network logons), including successful and failed logons performed on monitored workstations
  - User logon session activity (the actual time spent on a workstation)

System requirements

For a successful deployment, ensure that your environment meets the minimum system requirements. For information on system requirements, see the Change Auditor Release Notes. For details on installing Change Auditor, see the Change Auditor Installation Guide.

NOTE: Starting with Change Auditor 6.5, the dependency on InTrust and the Change Auditor Data Gateway Service to capture logon activity is eliminated.

Client components and features

The following table lists the client components and features that require a valid Change Auditor for Logon Activity license. The product will not prevent you from using these features; however, associated events will not be captured unless the proper license is applied.

NOTE: To hide unlicensed Change Auditor features from the Administration Tasks tab (including unavailable audit events throughout the client), use the **Action | Hide Unlicensed Components** menu command. Note this command is only available when the Administration Tasks tab is the active page.

Table 1. Change Auditor for Logon Activity client components/features

Client Page	Feature
Event Details Pane	What Details: • Subsystem: Logon Activity • Logon Start (Logon Session events) • Logon End (Logon Session events) • Duration (Logon Session events) • Session Start (Logon Session events) • Session End (Logon Session events) **NOTE:** See Search Results for more information.
Events	Facilities: • Authentication Activity • Domain Controller Authentication (only available with Change Auditor for Logon Activity User auditing module for server agents) • Logon Session
Layout Tab/Search Results Page/Reports	Columns: • Subsystem: Logon Activity • Logon Type • Logon Start (Logon Session events) • Logon End (Logon Session events) • Logon Session Start (Logon Session events) • Logon Session End (Logon Session events) • Logon Duration (Logon Session events)
Search Properties	What Tab: • Subsystem | Logon Activity **NOTE:** See User Logon Activity Searches/Reports for information on creating custom logon activity search queries.
Searches Page	Built-in Reports: • All Failed Logons in the last 7 days • All Interactive Logons in the past 24 hours • All Kerberos Logons in the past 24 hours • All Logons in the past 24 hours • All Remote Interactive Logons in the past 24 hours • All User Sessions in the past 24 hours **NOTE:** See Built-in logon activity searches for a description of these search queries.
Alert Body Configuration dialog - Event Details tab	Variables (email tags): • LOGON_DURATION • LOGON_END • LOGON_SESSIONEND • LOGON_SESSIONSTART • LOGON_START • LOGON_TYPE **NOTE:** See the Change Auditor User Guide for a description of these email tags and how to configure alert email notifications.

This guide has been prepared to assist you in becoming familiar with Change Auditor for Logon Activity. This User Guide contains information about the additional features that are available when a valid Change Auditor for Logon Activity license has been applied. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product. For information on installing and configuring Change Auditor for Logon Activity, see the Change Auditor Installation Guide.

2

Getting Started

- Deployment requirements
- Run reports

Deployment requirements

Before you can begin to capture logon activity events, you must:

- Ensure you meet the minimum system requirements.
- Apply the Change Auditor for Logon Activity User license to monitor servers. (All DCs and Member Servers with an agent installed will be included.)
- Apply the Change Auditor for Logon Activity Workstation license and deploy workstation agents to the workstations to be monitored. See the Change Auditor Installation Guide for more information on deploying workstation agents.
- Deploy agents. Depending on your implementation, you can deploy server and/or workstation agents.

NOTE: See Appendix: Agent Comparison on page 20 for more information.

The recommended installation for domain workstations is through the Deployment tab. However, for non-domain workstations you must manually install the Change Auditor workstation agent. See Appendix: Workstation Agent Deployment on page 16 for recommendations on deploying agents necessary for auditing both domain workstations and non-domain workstations.

- Enable the following policies through the Group Policy Management Console:

  When Local Policies\Audit Policy is used:

  1. Enable the 'Audit Logon events' audit policy for all servers and workstations. (Set to audit Success and Failure)
     - Domain - Group Policy:
       - Default Domain Policy\Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit logon events
     - Default Domain Controller Policy:
       - Default Domain Controllers Policy\Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit logon events
       - Default Domain Controllers Policy\Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon
     - Workgroup - Local Group Policy:
       - Local Computer Policy\Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit logon events
  2. Wait 30-90 minutes for the policy to refresh.

  When Security Settings\Advanced Audit Policy Configuration is used:

1 Enable the ‘Audit Logon’ advanced audit policy for all servers and workstations. (Set to audit Success and Failure)

- Domain - Group Policy:
  - Default Domain Policy\Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon
- Default Domain Controller Policy:
  - Default Domain Controllers Policy\Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit logon events
  - Default Domain Controllers Policy\Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon
- Workgroup - Local Group Policy:
  - Local Computer Policy\Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Logon/Logoff\Audit Logon

2 Wait 30-90 minutes for the policy to refresh.

Additional notes

- Quest recommends that you deploy a server agent to all servers (domain controllers and member servers) to track configuration changes in real-time.
- For workstation events, the agent is stored locally to capture logon, logoff, and calculated session activity.
- If a computer is disconnected from the network, the agent continues to work and store the information locally. Once the computer connects to the network again, the events are sent to the database and integrated at the time they were captured.

NOTE: Logon activity is only available if you have applied the Change Auditor for Logon Activity User license to monitor servers and the Change Auditor for Logon Activity Workstation license to monitor workstations. To verify that it is licensed, right-click the coordinator icon in the system tray and select **Licensing.**

Run reports

Using reports, you can obtain valuable information. For example, you can:

- Group, sort, and filter the information to help answer key questions for security, HR, and auditors. You can run reports to see who is logging into your servers, gather remote user session information, and access related search information to see what activities specific users have been performing.
- Create simplified reports by user, computers, logon type, etc.
- Create private searches and alerts for specific events that need urgent attention. For example, “all server logons in the last 24 hours”.
- Create dashboards, viewable in the web client, to help facilitate user management. You can then, enable shared overviews to be used by the Helpdesk to see information such as account logons, session activity, and account lockouts.

To test that events are being captured:

1 Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client** to review the events generated.

2 Open the Searches tab.

3 Expand the **Shared | Built-in | Logon Activity** folder in the left pane.

4 Locate and double-click **All User Sessions in the past 24 hours** in the right pane.

A new Search Results tab is added to the client displaying the events captured over the last 24 hours.

5 Select an event from the Search Results grid to display the event details for the selected event.

> **NOTE:** If the Search Properties tabs are displayed across the bottom of the Search Results page, double-click an event to display the event details for the selected event.

3

User Logon Activity Searches/Reports

Introduction

You can run built-in searches to retrieve user logon activity captured by deployed Change Auditor server and workstation agents. In addition, you can create custom queries to search for specific user logon activities that need to be tracked in your environment.

This section provides procedures for running built-in user logon activity searches and for creating custom logon queries. It also provides a description of the new details displayed on the Search Results page for user logon activity events. For a description of the dialogs mentioned in this chapter, refer to the online help.

Built-in logon activity searches

The following built-in searches have been added to Change Auditor, which retrieve user logon activity events from monitored server and workstation agents:

All Failed Logons in the last 7 days

Returns failed user logon events collected in the last 7 days. This includes events generated when a user fails to authenticate through Kerberos, fails to log on interactively (locally or from a remote computer), or fails to perform a network logon from a remote computer.

All Interactive Logons in the Past 24 hours

Returns the interactive logon events that were collected in the past 24 hours. This includes interactive logons that were successful as well as those that failed.

All Kerberos Logons in the Past 24 hours

Returns the Kerberos authentication events that were collected in the past 24 hours. This includes the Kerberos authentication requests that were successful as well as those that failed.

All Logons in the Past 24 hours

Returns all of the authentication activity, domain controller authentication and logon session events that were collected in the past 24 hours. This includes logon activity that was successful as well as those that failed.

All Remote Interactive Logons in the Past 24 hours

Returns the remote interactive logon events that were collected in the past 24 hours. This includes the remote interactive logons that were successful as well as those that failed.

All User Sessions in the Past 24 hours

Returns the all user logon session events that were collected in the past 24 hours.

Run built-in search

To run the All Logons in Past 24 hours search:

Running the **All Logons in the Past 24 hours** search will retrieve the all user logon activities for monitored servers and workstations.

1. Open the Searches page.
2. Expand and select the **Shared | Built-in | Logon Activity** folder to display the built-in searches available.
3. In the right-hand pane, locate the **All Logons in the Past 24 hours** search and use one of the following methods to run the selected search:
   - Double-click a search definition
   - Right-click a search definition and click the **Run** menu command
   - Select the search definition and click the **Run** tool bar button at the top of the Searches page
4. A new Search Results page appears populated with the events that met the search criteria.

Create custom user logon activity searches

The following procedures explain how to user the What tab to create custom user logon activity event queries.

NOTE: If you wanted to, you can use the other search properties tabs to define additional criteria:

- Who - allows you to search for events generated by a specific user, computer or group
- Where - allows you to search for events captured by a specific agent or within a specific domain or site
- When - allows you to search for events that occurred within a specific date/time range
- Origin - allows you to search for events that originated from a specific workstation or server

To search for all network logon events captured this week:

This search will capture both successful and failed logon attempts from a remote computer on the network.

NOTE: The network logon events are disabled by default and must first be enabled in the client before they will be captured. Use the Audit Events page on the Administration Tasks tab to enable these events.

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

   Select the **Private** folder to create a search that only you can run and view. Select the **Shared** folder to create a search which can be run and viewed by all Change Auditor users.

3 Click **New**.

4 On the Info tab, enter a name and description for the search.

5 Open the What tab, expand **Add** and select **Subsystem | Logon Activity**.

6 On the Add Logons dialog, select **Network** from the list, click **Add** to add it to the selection list at the bottom of the dialog. Click **OK**.

7 Click **Run**to save and run the newly created search.

A new Search Results page is populated with the results of your search.

To search a specific user's logon activity over a specific time period:

This scenario uses the **Runtime Prompt** options to create a generic search definition where you can then specify the user and time interval each time you run the search.

1 Open the Searches page.

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

Select the **Private** folder to create a search that only you can run and view. Select the **Shared** folder to create a search which can be run and viewed by all Change Auditor users.

3 Click **New**.

4 Open the Info tab, enter a name and description for the search.

5 Open the Who tab and select **Runtime Prompt** to specify the user to be audited each time you run this search.

6 Open the What tab, expand **Add** and select **Subsystem | Logon Activity**. On the Add Logons dialog, select all of the entries in the Logon text box at the top of the dialog, click **Add**, then **OK** to save your selections and close the dialog.

7 Open the When tab and select **Runtime Prompt** to specify the time interval each time you run this search.

8 Select **Run** to save and run the search.

9 Since you selected the **Runtime Prompt** options on both the Who tab and When tab, you will be prompted to specify the user who's logon activity you want to audit and the time interval to be searched:

- On the Select Active Directory Objects dialog, use the Browse or Search pages to locate one or more users. Click **Add** to add the selected user to the list at the bottom of the page. Click **Select** to save your selection and close the dialog.
- On the When dialog enter the date range and/or time of day to be searched. Click **OK** to save your selection and close the dialog.

A new Search Results page will be displayed populated with the results of your search.

Search Results

The user logon activity event information can be viewed on the Search Results page in the Change Auditor client. The user logon activity details appear on the following Change Auditor components:

- Search Results Grid
- Event Details Pane

Search Results Grid

For logon activity events, a new **Logon Type** column is added to the Search Results grid. This column displays the type of logon that occurred:

- Domain Authentication
- Interactive
- Remote Interactive

In addition, the Search Results grid for Logon Session events displays the **Logon Start, Logon End, Logon Session Start**, **Logon Session End** and **Logon Duration** columns.

Event Details Pane

For user logon activity events, the **What** field combines various event data to form a detailed description of the event that occurred. In addition, for Logon Session events, the Event Details pane displays the following attributes about the session:

- Logon Start
- Logon End
- Duration
- Session Start
- Session End

The following table provides a description of the event details provided for user logon activity events.

Table 2. Event Details pane: User logon activity events

ChangeAuditor	Description
Severity	Displays ‘Medium’, which is the severity level assigned to all user logon activity events.
Who	Specifies the name of the user who initiated the change.
When	Specifies the date and time when the change occurred.
Where	Displays the name of the server where the change occurred.
Source	Displays ‘Change Auditor’ which is the application from which the event was retrieved.
Origin	Displays the NetBIOS name and IP address of the workstation or server from which the event was generated.
What	Displays a description of the user logon activity that occurred. This description consists of various fields to describe the user logon activity. **NOTE:** For lengthy descriptions, hover your cursor over the description field to view the entire event description.

Table 2. Event Details pane: User logon activity events

ChangeAuditor	Description
Result	Indicates whether the user logon activity was successfully completed. Displays one of the following: • Success • Failed
Subsystem	Defines the subsystem, or area of auditing, where the event occurred. Displays 'Logon Activity'.
Facility	Depending on the type of event, this field displays one of the following: • Authentication Activity • Domain Controller Authentication • Logon Session
Logon Start	For Logon Session events, the date and time when the user initially logged onto the computer.
Logon End	For Logon Session events, the date and time when the user logged out of the computer.
Duration	For Logon Session events, how long the user session lasted or how long the user was actually logged onto the computer (depends on the event).
Session Start	For Logon Session events, the date and time when the current user session began.
Session End	For Logon Session events, the date and time when the current user session ended.

4

Appendix: Workstation Agent Deployment

Change Auditor for Logon Activity workstation agents are required to capture logon activities when a Change Auditor for Logon Activity Workstation license is applied.

This section provides recommendations for deploying agents necessary for auditing both domain workstations and non-domain workstations. It also includes instructions on manually deploying workstation agents.

- Recommendations/deployment requirements
- Manual workstation agent deployment

Recommendations/deployment requirements

All workstation agents

- .NET framework 4.5.2 is the minimum requirement (available in Autorun.exe Redistributables).
- Quest highly recommends a phased approach to deploying workstation agents. A phased approach, where a maximum of 100 workstation agents are deployed at a time which will allow you to monitor the coordinator performance before deploying another batch of agents.

Deploying workstation agents (domain workstations)

- Recommended installation is from the Deployment tab.
- Alternately, workstation agents can be manually deployed. See Manual workstation agent deployment for more information on manually installing agents.

Deploying foreign workstation agents (non-domain workstations)

- A routable network path must exist between non-domain workstations, domain controllers and the coordinator servers. Name resolution of domain controller(s) and the coordinator servers is also required from the non-domain workstations, whether DNS server configuration, NetBIOS/WINS configuration or local hosts file entries are used.
- Required installation is to manually deploy the workstation agent. See Manual workstation agent deployment for more information.
- During installation, the workstation agent prompts for Active Directory domain and credential information to locate a coordinator and installation name.

- When the first foreign workstation agent is manually installed, a ChangeAuditor Agents - <*InstallationName*> security group is created. User accounts must be added to this security group in order to properly authenticate.
  - The Workstation Agent installer allows you to add the domain user account to the ChangeAuditor Agents – <*InstallationName*> security group, if appropriate LDAP and network protocol access is available.

  NOTE: In some cases, it might be necessary to pre-stage\create the ChangeAuditor Agents – <*InstallationName*> security group and manually add the configured workstation agent user account to the security group.

- The Coordinator Credential Configurator can also be used to change between coordinator domains at any time after the agent is installed, if desired.

  NOTE: The Coordinator Credential Configurator application can be launched using the CoordinatorCredentialConfigurator.exe file in the agent installation folder on the workstation. The default agent installation location is: %ProgramFiles%\Quest\ChangeAuditor\Agent

Manual workstation agent deployment

When installed manually, the Change Auditor Workstation Agent installer must be run as an account with the local administrator account privileges and with elevated User Account Control (UAC) permissions.

NOTE: Depending on the User Account Control (UAC) policies (refer to User Account Control (UAC) settings for more information), elevated UAC permissions may require launching the installer using one of the following methods:

- Shift + Right-click installer to select 'Run as a different user'.
- From the Windows Task Manager, select File | Run New Task, browse and select the Change Auditor Workstation Agent installer file, and select the 'Create this task with administrative privileges' option, then click **OK**.

To manually install a workstation agent:

1. Copy the appropriate agent installer package from the Change Auditor service installation directory (%ProgramFiles%\Quest\ChangeAuditor\Service) to the workstation to be monitored:
   - Quest Change Auditor Workstation Agent 6 (x64).msi
   - Quest Change Auditor Workstation Agent 6 (x86).msi
2. Run the installer file on the workstation to open the Quest Change Auditor Workstation Agent Setup wizard.
3. Review the following table for additional information about the information requested in this wizard. This table only covers unfamiliar information. It does not include all the wizard pages or field descriptions.

Table 3. Change Auditor Workstation Agent wizard

Active Directory Information screen On the Active Directory Information screen, enter the Active Directory information which will allow the agent to establish a coordinator connection.	
Name of Active Directory Root Domain (domain.com)	Enter the DNS name (domain.com) of the root domain of Active Directory.
Account Name (domain\user)	Enter the name of the user (domain\user) that can find and connect to a Change Auditor coordinator in the Active Directory forest.
Account Password	Enter the password associated with the user account entered above.

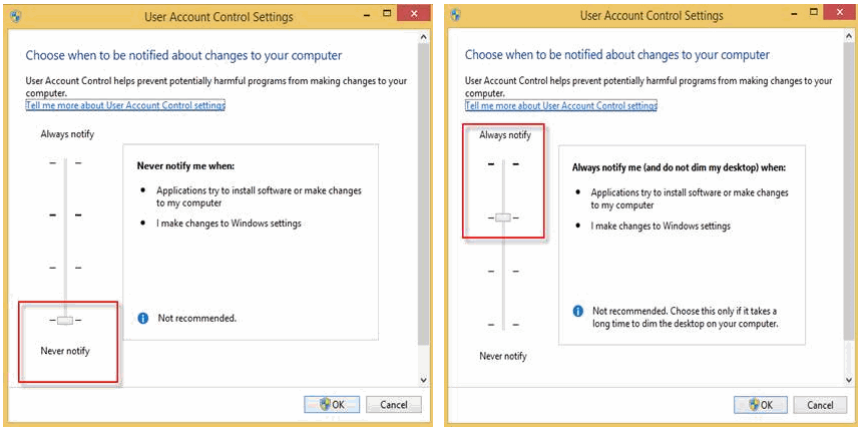
Table 3. Change Auditor Workstation Agent wizard

Add this user to the “ChangeAuditor Agents - <*InstallationName*>” security group	This check box is selected by default indicating that the user account specified above will be added to the ChangeAuditor Agents security group. **NOTE:** User accounts must be added to this security group in order to properly authenticate.
Installation Name screen The Installation Name screen will prompt you to enter the installation name to identify the database to which the coordinator is to be connected. A workstation agent must join an existing Change Auditor installation.	
ChangeAuditor Installation Name	Click **Next** to use the DEFAULT installation name. If you want to use a different Change Auditor installation, enter the installation name of an existing Change Auditor installation or click the **Browse** button to select an existing Change Auditor installation. Clicking the Browse button will display the Browse for ChangeAuditor Installation dialog allowing you to select from a list of existing installations.

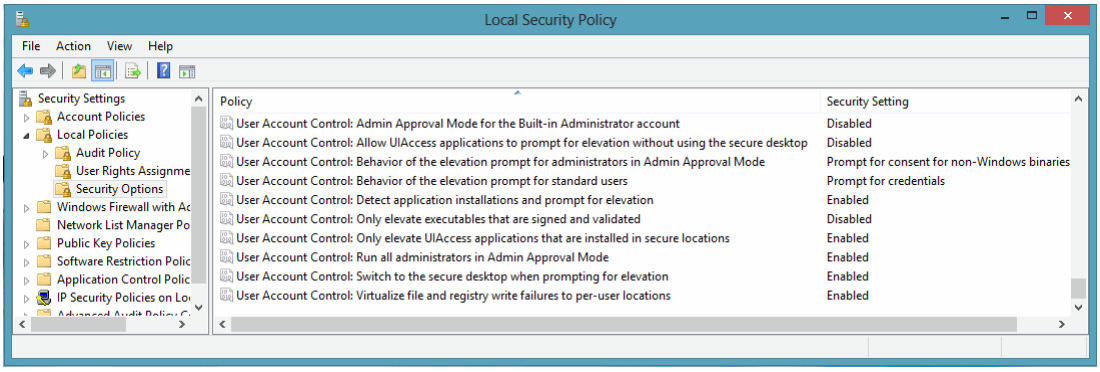
4 Repeat to install a workstation agent to all of the workstations to be monitored.

User Account Control (UAC) settings

- UAC policies typically use different settings for the ‘Administrator’ account and other accounts with Administrative privileges, so it may be easier to run the Change Auditor Workstation Agent installer with elevated UAC permissions if the Administrator account is used.
- General UAC elevation and prompt level configurations can be accessed via the Control Panel User Access Control configuration.



- More specific UAC policies can be configured in the Local Security Policy or a Group Policy Object (where appropriate) to determine whether all Administrators or the built-in Administrator account are run in Admin Approval Mode, the elevation prompt level, whether the secure desktop is used for prompting, whether elevation is possible without prompting, etc.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignme
Security Options
Windows Firewall with Ac
Network List Manager Po
Public Key Policies
Software Restriction Polic
Application Control Polic
IP Security Policies on Lo
Policy
Security Setting
User Account Control: Admin Approval Mode for the Built-in Administrator account
Disabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop
Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
Prompt for consent for non-Windows binaries
User Account Control: Behavior of the elevation prompt for standard users
Prompt for credentials
User Account Control: Detect application installations and prompt for elevation
Enabled
User Account Control: Only elevate executables that are signed and validated
Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations
Enabled
User Account Control: Run all administrators in Admin Approval Mode
Enabled
User Account Control: Switch to the secure desktop when prompting for elevation
Enabled
User Account Control: Virtualize file and registry write failures to per-user locations
Enabled

5

Appendix: Agent Comparison

There are a few Change Auditor client features that are not available for workstation agents. The following table displays the agent-related features that are available for server and workstation agents.

Table 4. Agent comparison

Page/Feature	Available for server agents?	Available for workstation agents?
Deployment Page		
The Deployment page will not display non-member objects, such as ADAM workgroup servers or non-Active Directory workstations, because agents cannot be deployed to non-member objects using the Deployment tab. See the Appendix: Workstation Agent Deployment for more information on manually installing agents to workgroup servers or non-Active Directory workstations.		
Included in topology harvest	Yes	Yes
Install or Upgrade (deploy agent)	Yes	Yes
Advanced Options | Specify Agent Installation Location	Yes	Yes
Advanced Options | Specify a Custom Share on the Remote Server	Yes	Yes
Advanced Options | Launch ServiceStatusTray on startup	Yes	No
Advanced Options | Restart Agent on failure	Yes	Yes
New Servers | Enable Auto Deployment on New Servers	Yes	No
Overview Page		
Agent Status Pane		
▪ Enterprise View (member objects)	Yes	No
▪ Workstation View (member objects)	No	Yes
▪ Other View (non-member objects)	Yes	Yes
▪ <*Domain*> (member and non-member objects)	Yes	Yes
Count of Events Pane		
▪ Location (member and non-member objects)	Yes	Yes
Top Agent Activity Pane		
▪ All (member and non-member objects)	Yes	Yes
▪ DCs (member objects)	Yes	No
▪ Servers (member objects)	Yes	No
▪ Workstations (member objects)	No	Yes
▪ Others (non-member objects)	Yes	Yes
Search Properties Tabs		
Where Tab	Yes	Yes
Origin Tab	Yes	Yes
Agent Statistics Page		
Included in Agent Statistics page	Yes	Yes
Start | Stop | Restart agent (member objects)	Yes	Yes

Table 4. Agent comparison

Page/Feature	Available for server agents?	Available for workstation agents?
Start | Stop | Restart agent (non-member objects)	No	No
Set Agent Uninstalled	Yes	Yes
Hide | Show Uninstalled agents	Yes	Yes
View agent logs	Yes	Yes (See Note below)
View resource properties	Yes	Yes
Administration Tasks Page - Agent Configuration		
Included in Agent Configuration page	Yes	No
Assign agent configurations	Yes	No (Uses Default Configuration)
Configuration Setup dialog | System Settings	Yes	Yes (From Default Configuration)
Configuration Setup dialog | File System settings (Change Auditor for Windows File Servers, Change Auditor for EMC or Change Auditor for NetApp)	Yes	No
Configuration Setup dialog | AD Query settings (Change Auditor for Active Directory Queries)	Yes	No
Configuration Setup dialog | Exchange settings (Change Auditor for Exchange)	Yes	No
Configuration Setup dialog | VMware settings	Yes	No
Agent system tray icon	**Yes**	**No**

NOTE: For workstation log management (such as Get Logs and View Agent Logs), the following must be enabled on the workstation:

- Windows Management Instrumentation (WMI) must be enabled in the firewall rule set (usually domain) on the workstation
- Network Discovery and File Sharing must be enabled
- Remote Registry Service must be set to ‘Start Automatically’. By default, this service is stopped and set to ‘Manual’ for Windows 7, 8/8.1, and 10.

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.