Quest

Quest® Change Auditor 7.6.3
User Guide

© 2026 Quest Software Inc

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc

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

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

Quest Software Inc
Attn: LEGAL Dept.
10801 N. Mopac Expressway
Building 3, Suite 400
Austin, TX 78759

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 User Guide
Updated - August 2026
Software Version - 7.6.3

Contents

Change Auditor Overview 9
Available Change Auditor auditing modules 9

Agent Deployment 13
Deployment page 13
Filter the fields on the Deployment page 13
Filter the computers on the Deployment page 15
Using group Managed Service Accounts (gMSA) 15
Deploy agents 16
Connect to a different foreign forest/update credentials 17
Change the agent installation location and system tray option 18
Enable auto deployment 19
Refresh or clear Deployment page information 20

Change Auditor Client Overview 21
Starting the Change Auditor client 21
Accessing Change Auditor news and updates 22
Managing connection profiles 22
Connection wizard 23
Client components 25
Customize table content 26
Sort data 26
Resize or move columns 26
Add or remove columns 28
Group data 28
Filter data 28
Using custom filters 29
Directory object picker 30
Browsing for a directory object 30
Searching for a directory object 31

Overview Page 33
Overview 33
My Favorite Search 33
Define a favorite search 33
Overview panes 34
Top Agent Activity 34
Recent Event Activity 35
Count of Events By 36
Agent Status 36
Coordinator Status 36
Event Details pane 37

Searches 38

Introduction . . . 38
Searches page . . . 38
Explorer view . . . 38
Searches list . . . 39
Search Properties tabs . . . 40
View a list of available searches . . . 41
Run searches . . . 41
Run a quick search . . . 42

Search Results and Event Details . . . 43
Introduction . . . 43
Search Results page . . . 44
Search Results grid . . . 44
Search Properties tabs . . . 45
Event Details pane . . . 46
View search results . . . 49
Display results in different formats . . . 49
Preview search results . . . 49
Compare results side-by-side . . . 50
View event details or search properties . . . 50
Copy event details . . . 51
Email event details . . . 51
Add comments . . . 52
View user context and run related searches . . . 52
Protect critical objects, mailboxes, files and folders . . . 53
Add search properties to existing event queries . . . 54

Custom Searches and Search Properties . . . 55
Introduction . . . 55
Create a custom search . . . 55
Search Properties tabs . . . 56
Info tab . . . 58
Who tab . . . 59
What tab . . . 61
Where tab . . . 66
When tab . . . 68
Origin tab . . . 69
Alert tab . . . 70
Report tab . . . 70
Layout tab . . . 71
SQL tab . . . 73
XML tab . . . 73

Enable Alert Notifications . . . 74
Introduction . . . 74
Alert tab (Search Properties tabs) . . . 74
Enable alerts . . . 75

Disable alerts . . . 78
Alert History page . . . 79
View alert history . . . 80
View event details or alert properties . . . 80

Administration Tasks . . . 82
Administration Tasks tab . . . 82
Administration Task lists . . . 82
Export/import Administration Task settings . . . 86

Agent Configurations . . . 89
Introduction . . . 89
Agent Configuration page . . . 91
Define agent configurations . . . 93
Assign agent configurations to server agents . . . 95
Enable event logging . . . 96

Coordinator Configuration . . . 98
Coordinator Configuration page . . . 98
Configure email alert notifications/reports . . . 99
Manually create a Microsoft Entra web application for sending Microsoft 365 mail . . . 102
Customize alert email content . . . 103
Shared Folder Configuration . . . 104
Group Membership Expansion . . . 104
Add groups to Group Membership Expansion list . . . 105
Agent Heartbeat Check . . . 106
Disconnect client after 30 minutes of inactivity . . . 106
Scheduled Task Handling . . . 106

Purging and Archiving your Change Auditor Database . . . 108
Introduction . . . 109
Planning your jobs . . . 109
Purge and Archive page . . . 111
Create and maintain jobs . . . 112
Purge and Archive wizard . . . 113
Purge selected records . . . 116
- Who tab . . . 116
- What tab . . . 117
- Where tab . . . 118
- Origin tab . . . 119

Working with Private Alerts and Reports . . . 121
Introduction . . . 121
Private Alerts and Reports page . . . 121
Disable private alerts and reports . . . 122
Move and delete private searches . . . 123

Generate and Schedule Reports 124
Schedule reports for distribution 124
Create global report template 124
Define report content and layout 125
Enable and schedule reporting 126
Launch Report Designer 129
Publish reports 130
Print or save a page's contents 130

SQL Reporting Services Configuration 132
Introduction 132
SQL Reporting Services Page 132
SQL Reporting Services Templates 133
SQL Reporting Services Wizard 134

Change Auditor User Interface Authorization 137
Introduction 137
Application User Interface Authorization page 138
Add task definition 139
Add role definition 139
Add application group 140
Remove a task definition 141

Client Authentication 142
Introduction 142
Client Authentication Page 142
Changing authentication methods 143

Certificate authentication for client coordinator communication 144
Introduction 144
Installation settings 144
Deployment 145
Coordinator configuration 145
Windows client configuration 146

Integrating with On Demand Audit 147
Managing a Quest On Demand Audit integration 147
Creating an On Demand Audit configuration 147
Working with an On Demand Audit configuration 148

Enable/Disable Event Auditing 150
Introduction 150
Audit Events page 150
Enable/disable event auditing 151
Modify event's severity level or event class description 152
Define events to be captured based on results 152
View event information 153

Account Exclusion **154**
Introduction 154
Excluded Accounts Auditing page 154
Excluded Accounts templates 155
Excluded Accounts wizard 157

Registry Auditing **160**
Introduction 160
Registry Auditing page 161
Registry Auditing templates 162
Registry Auditing wizard 164

Service Auditing **167**
Introduction 167
Services Auditing page 167
Service Auditing templates 168
Service Auditing wizard 170

Agent Statistics and Logs **172**
Introduction 172
Agent Statistics page 172
Agent Statistics grid 172
Resource Properties pane 175
Agent system tray icon 179
Change Auditor Agent Status dialog 181
View agent status/statistics 182
Manage Change Auditor agents 183
Agent Log page 184
View and save agent trace logs 186

Coordinator Statistics and Logs **187**
Introduction 187
Coordinator Statistics page 187
Coordinator system tray icon 189
Change Auditor Coordinator Status dialog 190
Coordinator Configuration tool 191
View coordinator status and statistics 194
Manage Change Auditor coordinators 195
Coordinator Log page 196
View and save coordinator trace logs 197

Change Auditor Commands **198**
Menu commands 198
Tool bar buttons 201
Right-click commands 208

Change Auditor Email Tags **216**

About us 223
Our brand, our vision. Together. 223
Contacting Quest 223
Technical support resources 223

1

Change Auditor Overview

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

- Audit critical changes across your enterprise including Active Directory, Microsoft Entra ID, Microsoft 365 Exchange Online\SharePoint Online\OneDrive for Business, Exchange, Windows File Servers, NetApp, EMC, SQL Server, and SharePoint.
- Collect user login and log out activity for regulatory compliance and user activity tracking.
- Automate ongoing compliance with tracking and reporting for compliance initiatives such as SOX, PCI-DSS, HIPAA, FISMA, GLBA, and more.
- Speed troubleshooting through real-time insight into changes with a comprehensive audit library including built-in audit alerts, reports, and powerful searches.
- Proactively protect (lock down) critical Active Directory objects, Exchange mailboxes, and Windows files and folders from harmful changes that could open security holes or cause resources to become unavailable.
- Modular approach allows separate product deployment and management for key environments including Active Directory, Exchange, Windows File Servers, NetApp, EMC, SQL Server, Active Directory Queries, SharePoint, and Logon Activity,.
- Track, audit, report, and alert on critical changes made using Safeguard Authentication Services and Quest Defender.

Available Change Auditor auditing modules

Continually being in-the-know helps you to prove compliance, drive security, and improve uptime while proactively auditing changes to configurations and permissions. You can automatically generate intelligent, in-depth reports, protecting you against policy violations and avoiding the risks and errors associated with day-to-day modifications.

Quest provides the following products to help you track, audit, report, and receive alerts on vital changes and activity:

Table 1.

Available auditing	Benefits
Quest Change Auditor for Active Directory	Drives the security and control of Active Directory by tracking vital configuration changes to users, groups, nested groups, GPOs, computers, services, registry, local users and groups and DNS — without the overhead costs of system provided auditing. You can also 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 Entra ID. 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.
Quest Change Auditor for Exchange	Simplifies auditing the activities taking place in your entire Exchange environment. You can audit over 300 Exchange events covering owner and nonowner mailbox changes, server configurations and permissions, and more. 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 Microsoft 365 Exchange Online configuration and permission changes.
Quest Change Auditor for Windows File Servers	Enables administrators to achieve the comprehensive auditing coverage of system provided tools without the mass of cumbersome data that system provided event logs generate. You can audit activity related to files and folders, shares, and changes to permissions. Change Auditor provides an access control model that allows administrators to protect business-critical files and folders on the file server.
Quest Change Auditor for EMC	Eliminates the time and complexity of system provided auditing by providing EMC Celerra/VNX file and folder changes in real time and translating events into plain English.
Quest Change Auditor for NetApp	Eliminates the time and complexity of system provided auditing by providing NetApp file and folder changes in real time and translating events into plain English.
Quest Change Auditor for SQL Server	Provides database auditing to secure SQL database assets with extensive, customizable auditing and reporting for all critical SQL changes including broker, database, object, performance, and transaction events, plus errors and warnings. Helps tighten enterprise-wide change and control policies by tracking user and administrator activity such as database additions and deletions, granting and removing SQL access. SQL Data Level auditing allows you to audit changes to databases and tables.
Quest Change Auditor for Active Directory Queries	Monitors directory access across all domain controllers in the environment and aggregates that information in a central database identifying LDAP-enabled applications and how they use Active Directory. The LDAP access data can then be used during Active Directory forest migration and restructuring projects.

Table 1.

Available auditing	Benefits
Quest Change Auditor for SharePoint	Provides centralized auditing, including configuration, event collection and reporting, for Microsoft SharePoint 2016 and 2019 servers and farms. It provides built-in queries and reports that focus on auditing the following areas: • Access to content in SharePoint sites • Modifications of content (creation, modification, and deletion) • Changes to permissions and security settings You can also audit Microsoft 365 SharePoint Online and OneDrive for Business changes.
Quest Change Auditor for Logon Activity	Change Auditor for Logon Activity has removed the dependency on InTrust and the Change Auditor Data Gateway Service to capture user logon activity. This auditing module consists of two licenses (one for server agents and another for workstation agents) and may be used to collect logon activity events for regulatory compliance and user activity tracking. • The Change Auditor for Logon Activity User license enables server agents to audit authentication activity, domain controller authentication activity (Kerberos), and user logon session activity (the actual time spent on a server). • The Change Auditor for Logon Activity Workstation license enables workstation agents to audit authentication activity and user logon session activity (the actual time spent on a workstation).
Quest Change Auditor for Authentication Services	Authentication Services enables organizations to extend the security and compliance of Active Directory to Unix, Linux, and Mac platforms and enterprise applications. Using Change Auditor for Authentication Services, users of Authentication Services can audit on critical changes to: • Unix/Linux/Mac-related data for Active Directory users, groups, computers, NIS objects, and Authentication Services personalities • Unix/Linux/Mac settings in Group Policy Objects **NOTE:** Authentication Services auditing is only available if you have licensed Change Auditor for Active Directory. If you do not have a valid license you can use the features, however, associated events are not captured.
Quest Change Auditor for Defender	Enhances security by enabling two-factor authentication to network, Web, and applications-based resources. Defender was designed to base all administration and identity management on an organization's existing investment in Active Directory and eliminates the costs and time involved in setting up and maintaining proprietary databases. Change Auditor for Defender tracks changes to user accounts enabled with Defender tokens in Active Directory. Because Defender extends the Active Directory schema, once the Change Auditor for Defender auditing is enabled, agents installed on Domain Controllers detect any changes made to the Defender-specific attributes in Active Directory and generate events. No audit template is needed. **NOTE:** Defender auditing is only available if you have licensed Change Auditor for Active Directory. If you do not have a valid license you can use the features, however, associated events are not captured. To verify that it is licensed, right-click the coordinator icon in the system tray and select Licensing.

NOTE: The Change Auditor User Guide explains the core functionality available in Change Auditor regardless of the product license that has been applied. In addition, there are separate user guides available for each module that describe the additional functionality added to Change Auditor when the different auditing modules are licensed.

2

Agent Deployment

- Deployment page
- Using group Managed Service Accounts (gMSA)
- Deploy agents
- Connect to a different foreign forest/update credentials
- Change the agent installation location and system tray option
- Enable auto deployment
- Refresh or clear Deployment page information

Deployment page

The Deployment page displays all the servers and workstations discovered in your Active Directory environment. From here, you specify the servers and workstations (if the Change Auditor for Logon Activity Workstation license is applied) to host a Change Auditor agent.

The first time you open Change Auditor, the Deployment tab is available for you to deploy agents. After agents are deployed, use the **View | Deployment** menu to open the page**.**

NOTE: The Deployment page does 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 Change Auditor Installation Guide for information about manually installing agents to workgroup servers or non-Active Directory workstations.

Filter the fields on the Deployment page

The Deployment page may contain the following for each server and workstation discovered in your Active Directory forest. To display fields other than the defaults, click the Field Chooser located to the far left of the column headings and select the columns to display.

Table 1. Deployment page: Field descriptions

Column	Default	Description
Agent Status	Yes	Displays the current deployment status: • Active • Inactive • Pending • Copying Files • Executing Installer • Uninstalled
Coordinator	No	Displays the computer name of the coordinator to which the agent is connected.

Table 1. Deployment page: Field descriptions

Column	Default	Description
Creds	Yes	Indicates whether user credentials have been entered for the selected domain. To enter the credentials to use to install agents on a domain, click **Credentials**.
Deployment Result	Yes	Indicates the status of the last deployment task: • Success - agent was successfully deployed • Valid Creds - user credentials have been verified; you can schedule a deployment task • Access Denied - user credentials are not valid; use the **Credentials** command to enter the proper user credentials for installing an agent on the selected domain • The target version is already installed - no action required. **NOTE:** You can select **Clear Results** to clear the entry in this column for the selected server.
DN	No	Displays the distinguished name of a server. (The 'path' to the server in the Active Directory schema.)
DNS Name	No	Displays the DNS name of a server.
Domain	Yes	Displays the name of the domain where a server is located.
Exchange Server	No	Indicates whether Exchange is installed on a server.
Foreign Forest	No	Indicates whether an agent is connected to a coordinator in a foreign forest.
Forest	No	Displays the name of the forest where the agent resides.
GC	No	Indicates whether the server is a Global Catalog server.
Installation	No	Displays the installation name assigned to the coordinator to which the agent is connected.
IP Address	No	Displays the IP address of a server.
Name	Yes	Displays the NetBIOS name of a server.
Operating System	No	Displays what version of the operating system is running on a server.
Read-Only DC	No	Displays the Read-Only DCs.
Site	No	Displays the name of the site where a server resides.
Type	No	Displays the type of server: • Server - member servers joined to the domain • Domain Controller - domain controllers joined to the domain • Read-Only - domain controller servers that are read-only • Global Catalog - domain controller servers designated as Global Catalog servers • Workstation - workstations that are joined to the domain **NOTE:** Non-member objects are not included in the Deployment tab because you cannot use this tab to deploy agents to objects which are not a member of the local forest. See the Change Auditor Installation Guide for information about deploying agents to workgroup servers or non-Active Directory workstations.
Version	Yes	Displays the version number of the Change Auditor agent currently installed on a server.

Table 1. Deployment page: Field descriptions

Column	Default	Description
When	No	Displays the date and time for a scheduled deployment task. That is, the date and time entered on the Install or Update dialog (or Uninstall dialog) when the **When** option is selected. **NOTE:** Based on the client's current local date and time. The format used to display this date and time is determined by the local machine's regional and language setting.
Workstation	No	Indicates whether the agent is a workstation agent used for capturing user logon activity when the Change Auditor for Logon Activity Workstation auditing module is licensed.

Filter the computers on the Deployment page

In addition to selecting the fields, you can define what type of computers to display.

The following table describes how to use these controls to filter the content displayed on the Deployment page.

Table 2. Deployment page: Filter controls

Control	Description
Type	Use the left-most control to specify the type of Active Directory objects to be included in the display: • **All** - select to display all domain controllers, member servers and workstations in the forest, domain or site • **DCs** - select to display all domain controllers in the forest, domain or site • **Read-Only DCs** - select to display the Read-Only domain controllers in the forest • **Servers** - select to display the servers in the forest, domain or site • **Workstations** - select to display the workstations in the forest, domain or site **NOTE:** Non-member objects are not included in the Deployment tab because you cannot use this tab to deploy agents to objects which are not a member of the local forest. **NOTE:** See the Change Auditor Installation Guide for information about deploying agents to workgroup servers or non-Active Directory workstations.
Active Directory view	By default, the Deployment page provides a forest view of the servers found. However, you can use the right-most controls to limit your view to an individual domain or site. Use the middle control to select the Active Directory view (forest, domain, or site) then use the right-most control to select an individual forest, domain, or site for which servers and workstations are to be displayed.

Using group Managed Service Accounts (gMSA)

NOTE: By default, all services run as LocalSystem. Using gMSA accounts as the service account is not supported.

When using a group Managed Service Account for your agent deployment:

- The account must end with '$' and the password must be blank.

- The domain should be entered in the Fully Qualified Domain Name format.
- The local Administrator group must be added to the group policy debug programs. (Found under Local Computer Policy | Windows Settings | Security Settings | Local Policies | User Rights Assignments | Debug programs.)
- The Windows client must be run as the administrator. (Right-click and select Run as administrator.)
- The agent host must be correctly configured to successfully retrieve the managed password for the specified group Managed Service Account.
- The Coordinator Credential Configurator must be run as the administrator. (Right-click and select Run as administrator.)
- For manual installations, the agent installer must be run as the administrator. (Right-click and select Run as administrator.)
- For foreign domain agent deployments, the account name for the agent to connect to the coordinator should be specified with the Fully Qualified Domain Name (For example: domain.com\user.)
- For foreign domain agent deployments, a trust relationship with the foreign domain and the coordinator's domain is required.

For information on group Managed Service Account implementations and requirements, refer to Microsoft documentation.

Deploy agents

Agents deployed to servers (domain controllers and member servers) track changes in real time. When a change is made on a server, the agent captures the change information (audit event), batches and forwards the information to the coordinator, which then inserts the event details into the Change Auditor database.

NOTE:

- If the Change Auditor for Logon Activity Workstations auditing module is licensed, you must deploy agents to the workstations that you want to monitor.
- For information on deploying and installing agents in a foreign forest, see the Change Auditor Installation Guide.

To deploy agents:

1. Verify that the user account used to deploy agents is at least a **Domain Admin** in every domain that contains servers and workstations where agents are to be deployed.
2. Verify that the user account is also a member of the ChangeAuditor Administrators group in the specified Change Auditor installation.
3. Open the Change Auditor client. The Deployment page is displayed if agents have not yet been deployed. Otherwise, use **View | Deployment** to open the Deployment page.

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

   NOTE: The Deployment page may initially be empty until the current forest's server topology has been initially harvested. This page is automatically refreshed after this task has completed.

4. From this list, select an entry and select **Credentials | Set** to enter the proper user credentials for installing agents on the selected domain.

   NOTE: If you are using a group Managed Service Account, see Using group Managed Service Accounts (gMSA) for additional requirements.

   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 reenter the proper credentials for installing agents.

6 By default, the Change Auditor agent folders (Agent, Systray) is 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 and 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 be initiated. Click **OK** to initiate or schedule the deployment task.

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

   NOTE: To cancel a pending deployment task, select the server and 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 is displayed in the lower right-hand corner of your screen.

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

   After the deployment, you will see a previous version of an agent in the Version cell if you installed the agent on an unsupported platform. See the Change Auditor Installation Guide for more details.

Connect to a different foreign forest/update credentials

Once an agent is installed, you can select to use a different coordinator in another forest or update the credentials.

IMPORTANT: The agent must be restarted once a change has been made.

To update foreign agent credentials from the Change Auditor client

1 Select the **Deployment** tab.

2 Select one or more deployed foreign agent servers or workstations and click **Foreign Agent Credentials**.

   NOTE:
   - Multiple agents in the same foreign forest can be selected, scheduled and (when scheduled to do so) processed concurrently.
   - Agents in different foreign forests must be selected and scheduled separately but (when scheduled to do so) can be processed concurrently.

3 Select one of the following options to initiate or schedule the task and click **OK**:

   - Now (default)
   - When (If you select this option, enter the date and time when you want the task to initiate.)

4 Enter the Active Directory credential information to locate the Change Auditor Installation and allow the agent to connect to the coordinator in the remote forest.

- Coordinator Forest Root (example.com): Enter the coordinator forest root domain name and an account to be used by the agent to connect to the coordinator.
- Account Name (example.com\user): Enter the name of the account that can find and connect to a coordinator in the Active Directory forest.
- Account Password: Enter the password associated with the specified account.
- Account Type: Select the account type of the specified account.

NOTE: If you are using a group Managed Service Account, see Using group Managed Service Accounts (gMSA) for additional requirements.

5 Click **OK** to initiate or schedule the credential update task.

NOTE: You can alternatively update the forest and credentials using the Coordinator Credential Configurator which is accessed by:

- Right-clicking the agent SysTray and selecting Coordinator Credential Configurator, or
- Running the CoordinatorCredentialConfigurator.exe file in the agent installation folder on the agent server. (By default, this is located under %ProgramFiles%\Quest\ChangeAuditor\Agent.)

If User Account Control is enabled, you may need to authorize the Coordinator Credential Configurator to use the required elevated permissions by right-clicking on the tool and selecting 'Run as administrator' option.

Change the agent installation location and system tray option

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

NOTE: The other option available under **Advanced Options** is discussed in the Active Roles Integration section in the Change Auditor for Active Directory User Guide.

To change the agent installation location and system tray option:

1 On the Deployment page, select one or more agents from the server/workstation list, and click **Advanced Options**.

2 To change the installation folder, check the **Specify Agent Installation Location** check box and enter the location to use for the agent installation folder.

NOTE: The location entered is used for all servers and workstations with agents selected on the Deployment page.

3 Select the appropriate option to specify the action to take if the path entered cannot be created on a server or workstation:

- Use the default location and continue (Default)
- Fail the installation/upgrade for that agent

4 By default, the system share (ADMIN$) is used; however, you can use a different share by selecting the **Specify a Custom Share on the Remote Server** option and entering the share to use.

5 Use the **Launch ServiceStatusTray on startup** options to indicate whether you would like to run/install the Change Auditor agent system tray icon when the agent is started.

- **Yes** - launch the ServiceStatusTray on startup
- **No** - do not launch the ServiceStatusTray on startup
- **Do not change** - do not change the ServiceStatusTray launch option (default)

NOTE: The agent system tray icon (and the **LaunchServiceStatusTray on startup** setting) applies only to server agents. For more information about this icon, see Agent system tray icon.

6 Use the **Restart Agent on failure** options to indicate whether to restart an agent if it fails to start.

- **Yes** - restart agent on failure.
- **No** - do not restart agent on failure
- **Do not change** - do not change the restart agent option (default)

NOTE: When you select **Yes**, the agent is restarted if a main Change Auditor service goes offline due to a crash, failure or unknown exception; however, if the agent is gracefully shut down, the service will not be restarted.

7 Optionally, select **Save as Default** to save the current advanced deployment settings as the default for future agent deployments.

You can select **Restore to Default** to restore all the advanced deployment settings to the factory default or last saved defaults.

8 Click **OK** to save your selections and close the dialog. These deployment settings apply to all the agents selected on the Deployment page.

Enable auto deployment

Auto deployment allows you to automatically deploy an agent to any new domain servers that are added to your forest.

NOTE: Auto deployment does not apply to servers already in the topology that are promoted to domain controllers.

To enable auto deployment:

1 From the Deployment page, click **Auto Deploy**.

2 Select the **Enable Auto Deployment to New Servers** option.

If you enable **Do Not Deploy on Read-Only DCs (Not Recommended)**, when a read-only domain controller is added to the domain, the agent is not installed on it.

If **Do Not Deploy on Read-Only DCs (Not Recommended)** is disabled (default state), when a read-only domain controller is added to the domain, the agent is installed on it.

3 If required, select **Enable Auto Deployment to New Workstations** check boxes.

4 Select one of the following options to specify the servers to which agents are to be deployed:

- All New Servers/Workstations (default)
- Include New Servers/Workstations in Container(s)
- Exclude New Servers/Workstations in Container(s)
- Include Read-Only DCs (default)

5 When the **Include New Server/Workstations in Container(s)** or **Exclude New Server/Workstations in Container(s)** option is selected, click **Add** to locate and select individual containers.

6 Clicking **Add** displays the Select Active Directory Objects dialog. Use the Browse or Search page to locate and select a container. Once a container is selected, click **Add** to add it to the Selection list. Once you have added all the containers, click **Select** to save your selection and close the dialog.

The containers specified are displayed in the Containers list on the Auto Deploy to New Computers dialog.

7 By default, Change Auditor checks if new servers are added to the forest every 60 minutes and if found will automatically deploy an agent. However, you can use one of the following **Check for New Computers Added to Forest** options to change this interval:

- Every *nn* Minutes
- Every Day At <*time*>

8 Click **Set** to specify the credentials of a user with administrator rights on the selected domains. Click **OK** to save these user credentials and close the Logon Credentials dialog.

> **NOTE:** If you are using a group Managed Service Account, see Using group Managed Service Accounts (gMSA) for additional requirements.

9 Click **OK** to save your selections and close the Auto Deploy to New Computers dialog.

Refresh or clear Deployment page information

To force a topology harvest refresh:

1 On the Deployment page, click **Force Refresh**.

2 Change Auditor forces a topology harvest and display any new servers/workstations added since the last topology harvest.

> **NOTE:** The default harvest interval is every 3 hours.
>
> **NOTE:** Topology scan takes a long time when the environment contains a large number of workstations.

To refresh a coordinator's status:

1 On the Deployment page, select one or more servers from the list.

2 Click **Refresh Status**.

3 Change Auditor retrieves and displays the latest status for the selected agents, including the agent version and deployment results.

To clear the deployment results:

1 On the Deployment page, right-click a server or workstation from the list and click **Clear Result.**

2 This clears the current and any future entries in the **Deployment Result** cell for the selected server and workstation.

3

Change Auditor Client Overview

- Starting the Change Auditor client
- Managing connection profiles
- Client components
- Customize table content
- Filter data
- Directory object picker

Starting the Change Auditor client

To connect to the client, the following conditions must be met:

- The coordinator service is running and has a valid SCP listening port (no firewall implications).
- The current authenticated user running the client has the proper credentials to access the Change Auditor coordinator service. If this condition fails, the client displays the Coordinator Credentials Required dialog where you can enter the proper logon credentials.
- The current authenticated user is a member of either the ChangeAuditor Administrators or ChangeAuditor Operators AD group. If this condition fails, the Change Auditor logon screen displays an error and credential text boxes for entering the appropriate credentials.
- When using a direct database connection, the current authenticated user running the client has the proper SQL credentials to access the SQL database. If this condition fails, the client displays the Database Credentials Required dialog where you can enter new logon credentials.

To start the client

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

   You can connect to the 'default connection' profile or specify a different connection profile. A connection profile defines the connection method to connect to a coordinator in trusted or untrusted forests, or to the database directly without connecting with the coordinator. See Managing connection profiles for more information.

2. Select **Connect** to use the default connection profile.

   Alternatively, select a previously defined connection profile and click **Connect**.

   If you do not have the proper credentials required for access, the credentials dialogs display allowing you to enter the required credentials.

   Depending on how your system has been configured:

   - You may need to enter a user account and password or a smart card certificate and personal identification number.
   - Select the option to disconnect the client from the coordinator after 30 minutes of inactivity.

3. The first time the client opens, you are presented with the Start page which provides up-to-date product information.

4 Select the Deployment page to deploy agents. This page may initially be empty until the current forest's server topology is harvested. This page automatically refreshes when the topology harvest completes.

> **NOTE:** Topology scan takes a long time when the environment contains many workstations.

5 To see a real-time stream of events based on a 'favorite' search definition as well as other valuable summary information about the application, select the Overview page.

Accessing Change Auditor news and updates

The first time you open Change Auditor, you are presented with the Start page. Form here, you can view and access relevant information including news and updates, support and knowledge base content, online documentation (release notes and guide), links to the latest releases, and essential contact links.

If you do not want to see this page, clear the **Display this page each time I log in** option. The next time you log in to Change Auditor you will be directed automatically to the Overview page. However, we suggest you keep the Start page active as it contains the most up-to-date access to the supporting information you may require.

Managing connection profiles

You can manage Change Auditor in the same forest or in a different forest from a single client allowing you to connect to the coordinator service or the database in many ways.

You can define connection profiles to connect to a coordinator in trusted or untrusted forests, or to connect to the database directly without connecting with the coordinator.

To define a connection profile

1 On the Connection screen, click **Manage**.

2 On the Manage Connection Profiles dialog, click **Add** to open the Connection wizard, which steps you through the process of defining a new profile.

> **NOTE:** Previously defined connection profiles are listed allowing you to review the details of each connection profile and edit any user-defined profiles.

3 On the Change Auditor Environment page, select the connection method to use. The available methods include:

- **Forest —** connect to a coordinator in a trusted forest. Enter the DNS name of the forest.
- **Global Catalog —** connect to a coordinator in an untrusted forest. Enter the name or IP address of the global catalog.
- **Manual —** connect to a coordinator located in a different Active Directory forest than the client.

> **NOTE:** When you select to add or edit a manual connection, you will have the option to **Use WCF Certificate Authentication** and **Disable Certificate Revocation List Check**. When specifying the coordinator service properties, these check boxes must reflect the options for which the coordinator is configured. For details see, Certificate authentication for client coordinator communication.

- **Database Direct —** connect directly to the Change Auditor database, without going through the coordinator (use this method to connect to an archived 6.x database). With this option, you are

connected as an operator with read-only privileges; therefore, the Administration Tasks tab is not available.

NOTE: To access an archive database, the account that you use to log into the client must not have the 'Deny logon over the network' right set.

4 Depending on the connection method selected, enter the requested information on the Connect to Change Auditor Coordinator page:

- Forest - select the Service Connection Point (SCP) to use to connect to the coordinator.
- Global Catalog - select the SCP to use. To override the coordinator service DNS, you can enter the IP address and port number assigned to the coordinator.
- Manual - enter the fully-qualified domain name or IP address (IPv4 or IPv6) of the server where the coordinator resides and specify the port number assigned to the coordinator.

  NOTE: If the coordinator host cannot be resolved by DNS (for example, if the coordinator service is running under a service account instead of Local System) you must enter the IP address of the server where the coordinator resides.

- Database Direct - use the **Browse** button to select the SQL instance and Change Auditor database.

  NOTE: If the current authenticated user does not have the proper SQL credentials to access the database, the Database Credentials Required dialog appears allowing you to enter new credentials.

  NOTE: If the database is in a SQL AlwaysOn Availability Group, specify the availability group listener for the sql server name.

5 On the Connection Profile Summary page, review the connection profile details, name the profile and click **Test** to test the new connection profile. Click **Finish** to save the connection profile and close the Connection wizard.

6 On the Manage Connection Profile dialog, the new connection profile is added to the list. Click **Save** to save the new profile and close the Manage Connection Profile dialog.

7 To use this new connection profile, select it from the drop-down list on the Connection screen and click **Connect**.

8 If you do not have the proper credentials required for access, a dialog opens allowing you to enter new credentials.

Connection wizard

The Connection wizard steps you through the process of defining a new connection profile. It is started when you select **Add** at the bottom of the Manage Connection Profiles dialog.

Table 1. Connection wizard

Change Auditor Environment page: Select one of the following connection methods. Depending on the option selected, additional information is requested on this or subsequent pages. **NOTE:** If logon credentials are required for access, a dialog displays allowing you to enter the credentials.	
Forest	Select to locate a coordinator in a trusted forest. By default the local forest is displayed; however, you can enter the DNS name of a different trusted forest that has access to a DNS server and can be resolved. **NOTE:** You cannot enter an IP address in this field.
Global Catalog	Select to connect to a coordinator in an untrusted forest and enter the name or IP address of the global catalog to be used. **NOTE:** Use SQL authentication when connecting to an untrusted forest.

Table 1. Connection wizard

Manual	Select to specify the fully qualified domain name or the IP address of the server where the coordinator resides and the port number assigned to the coordinator. **NOTE:** When you select to add or edit a manual connection, you will have the option to **Use WCF Certificate Authentication** and **Disable Certificate Revocation List Check**. When specifying the coordinator service properties, these check boxes must reflect the options for which the coordinator is configured. For details see, Certificate authentication for client coordinator communication.
Database Direct	Select to connect directly to the Change Auditor database, without going through the coordinator. With this option, you are connected as an operator with read-only privileges; therefore, the Administration Tasks tab is not available. **NOTE:** If the database is in a SQL AlwaysOn Availability Group, you need to connect to the availability group listener. Ensure there are no existing open connections to the database if an upgrade will be performed. The upgrade will not proceed if there are other existing open connections to the database. **NOTE:** Use the **Database Direct** method to connect to an archived 6.x Change Auditor database. An extra page is displayed requesting the following information: • Change Auditor Server (\SQL Instance) - Enter or browse to select the server (name or IP address) and the SQL instance for the Change Auditor database. • Change Auditor Database - Enter the name of the Change Auditor database.
Connect to Change Auditor Coordinator page: This page is displayed after you have selected the connection method. The information required is based on the connection method. **NOTE:** When you select to add or edit a manual connection, you will also have the option to **Use WCF Certificate Authentication** and **Disable Certificate Revocation List Check**. When specifying the coordinator service properties, these check boxes must reflect the options for which the coordinator is configured. For details see, Because this is a significant change which may require the re-deployment of Change Auditor components, you are presented with a confirmation dialog. Select Yes to continue or No to return to the Client Authentication page..	
Service Connection Point	When the **Forest** or **Global Catalog** options are selected on the previous page, this list displays the Service Connection Points (SCPs) available for use. Select the SCP to use from this list.
Coordinator DNS/IP Address	If you selected the **Global Catalog** option and want to override the coordinator service DNS, enter the IP address (IPv4 or IPv6) of the server where the coordinator resides. If you selected the **Manual** option, enter the fully qualified domain name or IP address (IPv4 or IPv6) of the server where the coordinator resides. **NOTE:** If the coordinator host cannot be resolved by DNS (e.g., if the coordinator service is running under a service account instead of Local System) you must enter the IP address of the server where the coordinator resides.
Coordinator Port	If you selected the **Global Catalog** option and entered the IP address to override the coordinator server DNS, enter the port number assigned to the coordinator. If you selected the **Manual** option, enter the port number assigned to the coordinator. **NOTE:** You can obtain the port number assigned to a coordinator using the coordinator log file or Coordinator Status dialog (coordinator system tray icon).

Table 1. Connection wizard

Connection Profile Summary page: This page allows you to review the connection profile details, name your profile and test your new connection profile.	
Profile Summary	This displays the settings defined within the wizard. The content depends upon the connection method selected. The information displayed may include: • Connection method • Coordinator • Port • SPN • Change Auditor coordinator server/instance
Connection Profile Name	Enter a descriptive name to assign to the new connection profile.
Test	Use to test the connection as defined in the connection profile.

Client components

The client contains the following main components:

- **Title Bar** - is located across the top of the screen and displays the name of the forest and installation name to which you are currently connected.
- **Menu Bar** - is located directly below the title bar and displays the menus for accessing Change Auditor commands. See Change Auditor Commands for a description of the menu bar commands.
  - **File Menu** - use the File Menu commands to connect to or disconnect from a coordinator, print the currently displayed content, open client logs, or exit the client.
  - **Edit Menu** - use the Edit Menu commands to manage your searches and folders on the Searches page.
  - **Action Menu** - use the Action Menu commands to refresh or reset a page, autofit columns, display the XML or SQL tabs, enable/disable the auto connect feature or enable/disable the desktop notification messages.
  - **View Menu** - use the View Menu commands to display a different Change Auditor page.
  - **Help Menu** - use the Help menu commands to display the online help, retrieve general information about this release, send feedback about using the product or collect system logs for troubleshooting purposes.
- **Tabbed Pages** - are displayed below the menu bar and are used to navigate through Change Auditor. The pages that can be displayed, include:
  - The **Start** page to view and access relevant information regarding Change Auditor including news and updates, support and knowledge base content, online documentation (release notes and guide), links to the latest releases, and essential contact links.
  - The **Deployment** page to deploy, upgrade or uninstall agents from a single location.
  - The **Overview** page provides a real-time stream of events based on a 'favorite' search definition. It also contains statistics about the events and the status information for the agents and the coordinator.
  - The **Searches** page contains a list of all the searches available. From this page you can run a search, create a customized search, enable/disable alerting and reporting for a search query.
  - A new **Search Results** page is created whenever a search is run. These pages contain a list of the events returned as a result of the selected search. From this page, you can also view the details of an event or the search properties used to return the displayed events.

- The **Alert History** page is displayed when the **Alert | History** right-click command is selected for an alert-enabled search definition on the Searches page and includes details regarding the events that triggered the selected alert.
- A new **Report** page is created whenever the **Preview Report** tool bar button is used on the Report tab (Search Properties tabs) for a search query. The Report page displays a rendering of the events returned as a result of the selected search.
- A new **Log** page is created whenever one of the View Logs commands are selected and displays the event details recorded in the selected log.
- The **Agent Statistics** page displays status and statistics for all installed agents.
- The **Coordinator Statistics** page displays status for all installed coordinators.
- The **Administration Tasks** tab allows you to perform a variety of administration tasks. Use the navigation pane in the left-hand pane to select the administrative task to be performed. See Administration Tasks for an overview of the tasks that can be performed using the Administration Tasks tab and the product license required to perform these tasks.

Customize table content

The contents of the various data grids displayed in the client can be sorted, rearranged, and grouped.

- Sort data
- Resize or move columns
- Add or remove columns
- Group data

Sort data

An arrow in the column heading identifies the sort criteria and order, ascending or descending, being used to display information.

To change the sort criteria:

1. Click the column heading to use for the sort criteria.
2. The sort order is in ascending order, but can be changed to descending order by clicking the heading a second time.
3. To specify a secondary sort order, SHIFT + click in the heading of the column to use for the secondary sort order.

Resize or move columns

Columns can also be resized or moved within a data grid.

To resize a column:

1. Place your cursor on the boundary between column headings (your cursor changes to a double-arrow).
2. Click and hold the left mouse button dragging the column boundary to the desired size.

To change the order of the columns in the table:

1. Use the left mouse button to click the heading to move.
2. Drag that column heading to the desired location in the table (arrows indicate where you are placing the selected column).

Add or remove columns

Change Auditor displays a default set of columns. You can however display more data or hide a particular column.

To add or remove columns:

1. Click the button to the far left of the column headings.
2. The Field Chooser dialog opens which lists all the data (columns) available for display.
3. Select the columns to display and clear the columns you do not want displayed.

   NOTE: For each individual search, you can select the data to retrieve and display in the client using the Layout search properties tab. From this tab, you can also define column order, sort criteria and order, groupings and the format to use for displaying the retrieved data.

Group data

You can group data to create a collapsed view that can be expanded to view the detailed information that applies to that group.

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.

Filter data

Traditional search capabilities provide the first phase of details, but locating individual events typically requires more granular search capabilities and additional steps. Change Auditor provides advanced filtering options to modify the results of a search without changing the original search. With this capability, filtering can be performed on one or more columns of a result, ultimately reducing the need to build the same search multiple times with minor customizations.

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 these cells, and click **Click here to filter data.**

2 In the selected cell, enter the word or string to use 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.

To create a custom filter:

When you place your cursor in a data filtering cell, a drop-down arrow displays to the right of this cell. This drop-down displays all the items available for selection, including (Custom), (Blanks), and (NonBlanks). Selecting an item from this list displays entries based on the item selected.

1 To create a custom filter, place your cursor in the cell beneath the column to filter. Click the arrow control and select **(Custom)**. The Custom Filter dialog opens.

2 Select the appropriate option in the **Filter based on <All | Any> of the following conditions.**

- Select **All** if all the criteria entered has to be met in order to be included.
- Select **Any** if only one of the criteria entered has to be met in order to be included.

3 In the field to the right of the column heading, click the arrow control to select the comparison operation to be used (for example, Like, Equals, Contains, and so forth).

4 In the field to the right of the comparison operator, enter the pattern (character string or value) to be used to search for a match.

Use the * wildcard character to match any string of zero or more characters. For example, entering **LIKE *change*** in the Event column, will find events that contain the string ‘change’, such as changed, Change Auditor, etc.

5 To add additional criteria, click **Add**. This allows you to add a row to the custom filter to specify additional criteria for the selected column.

6 After you have created the custom filter, click **OK** to close the dialog and filter the data based on the criteria entered.

Using custom filters

The following procedures walk you through a few scenarios using custom filters.

To find events generated when a member is added to a group:

1 Run the **All Events** search.

2 On the Search Results page, place your cursor in the data filtering cell of the Event column, click the arrow control and select **(Custom)**.

3 Select **All**.

4 Specify the following criteria:

- **Contains | group**
- **Contains | added**
- **Does not contain | group policy**

5 Click **OK**.

To find delete object operations related to a forest container:

1 Run the **All Events** search.

2 On the Search Results page, place your cursor in the data filtering cell of the Action column, click the arrow control and select **(Custom)**.

3 Select **All**.

4 Specify the following criteria:

- **Contains | delete**
- **Contains | object**

5 Click **OK**.

6 On the Search Results page, place your cursor in the data filtering cell of the **Facility** column and enter: **forest**.

Directory object picker

Throughout the client, the directory object picker is used to locate and select Active Directory objects from the environment. This object picker is displayed in either a stand-alone dialog (such as the Select Active Directory Objects dialog) or as a page in a wizard. The client needs to be able to connect to a Global Catalog (GC) to display the object picker and query objects. The client contacts the coordinator to get the Global Catalog that should be used. The coordinator attempts to choose a GC in its local domain and site. If none is found, it chooses one in its domain, then in the local site, and lastly the entire forest. It is recommended to have the coordinator and the client reside in the same site and/or domain so that the directory object picker performs more efficiently.

The object picker consists of the following pages:

- **Browse** - use the Browse page to select a directory object from a hierarchical view of your environment

  NOTE: If Active Directory integrated DNS is deployed, you can access the ForestDNSZones or DomainDNSZones partitions by right-clicking on the top-level domain object.

- **Search** - use the Search page to search your environment to locate and select a directory object

  NOTE: Disabled objects on these two pages are represented by a red X icon.

- **Options** - use the Options page to view or modify search options used to retrieve directory objects

Browsing for a directory object

To browse for a directory object:

1 Open the Browse page.

2 In the **Forest** field, select the forest that contains the required directory objects.

NOTE: The Forest field is available in directory object picker in the following areas:

- Group membership expansion, Email Alerts Configuration, and shared folder configuration
- Purge and archive jobs
- Active Directory, AD Query, ADAM (AD LDS), Exchange, Group Policy, Local accounts, Registry, Service, and SQL Server searches
- Report and alert email configuration
- Windows File System and AD Query auditing wizard
- Active Directory auditing and protection wizard
- File System protection wizard

3 In the Find field, either enter or use the drop-down menu to select the type of directory object.

You can enter multiple classes, separated by either a comma or semi-colon. Note that when you type in an entry, you must use the **Enter** key or the **Apply Filter** button to display the objects.

> **NOTE:** Most of the time, this field will be automatically filled in with the appropriate entry. Thus, when this field is grayed out, this is a read-only field which cannot be changed.

4 In the explorer view (left pane), single-click on the expansion state box to the left of a container or double-click a container to expand the view to display subordinate objects.

Select a container in this pane to populate the object list (right pane) with the objects that belong to the selected container.

> **NOTE:** Right-clicking the root domain in the explorer view displays a drop-down menu listing any peer domains. To view a different domain's objects, select the desired domain from those listed.

Use the **F5** button to force a refresh of the contents of this pane.

5 In the object list, click the object to select it and use the **Add** button to add it to the Selected Objects list at the bottom of the dialog.

> **NOTE:** The Selected Objects list is used for both the Browse and Search pages and will contain the objects selected from either of these pages.

6 Once you have added objects to this list, use the **Select** button to save your selection and close the dialog. Or if the directory object picker is part of a wizard, click **Next** to save your selection and continue.

Searching for a directory object

To search your environment for a directory object:

1 Open the Search page and use the controls at the top of the page to search your environment to locate the desired objects.

2 In the **Find** field, either enter or use the drop-down menu to select the type of directory object to be located.

You can enter multiple classes, separated by either a comma or semi-colon. Note that when you type in an entry, either click the **Enter** key or use the **Search** button to display the objects.

3 In the **Name** field, specify a search expression to be used to search Active Directory to locate a particular

> **NOTE:** Most of the time, this field will be automatically filled in with the appropriate entry. Thus, when this field is grayed out, this is a read-only field which cannot be changed.

object. In most cases, this field will contain an asterisk (*) indicating to search for all objects of the type specified in the **Find** field.

Select the **ANR** check box to use Ambiguous Name Resolution (ANR) as the search algorithm, which allows you to enter limited input (partial data) to find multiple objects in your network.

When the **ANR** check box is checked, use one of the following methods to enter your search expression:

- Enter a partial string to return exact matches or a list of possible matches. For example, entering 'Admin' will return objects that contain the names 'Admin', 'Admins', 'Administrator', Administrators', etc.
- Enter a string preceded by the equal sign (=Admins) to return only exact matches. For example, entering '=Admin' will return only those objects containing the name 'Admin'.

By default, ANR will search the following attribute fields in Active Directory:

- First Name (GivenName)
- Last Name (Surname)
- Display Name (displayName)
- LegacyExchangeDN

- msExchMailNickname
- Relative Discontinued Name of the object (RDN)
- Office (physicalDeliveryOfficeName)
- Email address (proxyAddress)
- Security Account Manager account (sAMAccountName)

When the **ANR** check box is not checked, the search expression entered will be used to search only the Display Name of directory objects to locate a particular object.

To use this search mechanism, enter a string of characters and the wildcard (*) character as described below.

- n* will return objects that start with the letter 'n'
- *n will return objects that end in the letter 'n'
- *n* will return objects that contain the letter 'n' within their Display Name.

4 After entering a search expression, use the **Search** button to initiate the search and return the results of the search.

5 The object list displays the objects found as a result of your search. To select an object, click on the object to highlight it and use the **Add** button to add it to the Selected Objects list.

> **NOTE:** The Selected Objects list is used for both the Browse and Search pages and will contain the objects selected from either of these pages.

6 Once you have added objects to this list, use the **Select** button to save your selection and close the dialog. Or if the directory object picker is part of a wizard, click **Next** to save your selection and continue.

To view or modify the search options to use to retrieve directory objects:

1 Open the Options page and modify the options as required.

> **NOTE:** The settings on the Options page only apply to the current user and do not impact other users using a Change Auditor client.

2 The **Search Limit** field specifies the maximum number of records to return for an Active Directory object search. The default is 2000 records.

To change this limit, enter a value between 100 and 9999.

Or to allow an unlimited number of records to be returned, select the **No Search Limit** check box.

3 The **Page Size** field displays the maximum number of records to return per LDAP polling cycle.

> **TIP:** Care should be taken when modifying this value, because it could impact the performance of your searches.

4 Once you have made changes on the Options page, use the **Select** button to save your selection and close the dialog. If the directory object picker is part of a wizard, click **Next** to save your selection and continue.

4

Overview Page

- Overview
- My Favorite Search
- Define a favorite search
- Overview panes
- Event Details pane

Overview

Once agents are deployed, the Overview page initially displays when the client successfully connects to a coordinator. This page highlights application details based on your preference. For example, you can display Agent Status, Top Agent Activity, Recent Event Activity, Coordinator Status, Event Counts, or Alert History Counts.

You can view a real-time stream of events based on a ‘favorite’ search definition. By default, the top pane uses the Change Auditor Real-Time search definition and display all events (up to 10,000 records) generated in the last 20 minutes. You can, however, define a different ‘favorite’ search and the events captured from that search will then be displayed across the top of the Overview page.

The information on this page is captured when the client starts. To refresh all of the information displayed on the Overview page, select **Refresh**. Also, when you select a different pane for display, the latest information for the 'new' pane will be displayed.

My Favorite Search

The Overview top pane displays a real-time view of events generated based on a user-defined ‘favorite’ search. By default, the Change Auditor Real-Time search definition is used and all events captured for the last 20 minutes are displayed

As events are returned, they are added to the search results, providing you with a real-time view of what’s happening in your environment. By default, the events are sorted by date, with the latest event being added to the top of the list. You can, however, use the column controls to select a different sort criteria for the information displayed. For more information on customizing the content of this table, see Customize table content.

Double-clicking an event displays the Event Details pane across the bottom of the page, which contains additional details regarding the selected event. The layout and content for My Favorite Search is the same as that used on the Search Results page. For a description of the search results grid and the Event Details pane, please refer to Search Results grid and Event Details pane.

Define a favorite search

By default the Change Auditor Real-Time search (all events captured in the last 20 minutes) is used to capture the events displayed on the Overview page. You can, however, select a different ‘favorite’ search, which will then be used to populate the top pane on the Overview page.

To define a 'favorite' search:

1. Open the Searches page.
2. Select the search to use, right-click and select **Set As My Favorite**.
3. Open the Overview page, click **Refresh** to display the results of that search in the My Favorite Search pane at the top of the Overview page.

To modify the current 'favorite' search:

1. From the Overview page, click **My Favorite Search: *<search name>*** title at the top of the My Favorite Search grid.
2. The Searches page and corresponding search properties tab are displayed.
3. Use the search properties tabs to modify the search criteria. Click **Save** from one of the search properties tabs to save your changes.
4. Open the Overview pane, click **Refresh** to display the results of the modified search in the My Favorite Search pane.

Overview panes

You can customize the Overview panes across the bottom of the Overview page based on your preference to display a variety of overview information about Change Auditor. By default, the Top Agent Activity and Agent Status panes display across the bottom of the Overview page. However, each of these panes has an arrow button on its heading that you can use to display different overview information.

The following overview views are available:

- Top Agent Activity
- Recent Event Activity
- Count of Events By
- Agent Status
- Coordinator Status
- Alert History Counts

Within the overview panes, blue underlined numbers are hypertext links. Selecting a link displays the search results for the selected count.

Top Agent Activity

The Top Agent Activity pane displays the most active agents in your environment. That is, the agents that have forwarded the most events to the coordinator based on the date range selected. If this pane is not displayed, click the arrow on the heading of one of the lower panes and select **Top Agent Activity** to display this pane.

By default, the agent activity on all servers for the past month, excluding uninstalled agents, will be displayed. You can, however, use the controls located at the top of this pane to specify the types of agented objects to be included as well as the date range.

Type

By default all agented objects are included. However, you can use the drop-down menu located in the upper left corner of this overview pane to limit the types of objects to be included:

- **All** - view all agented servers and workstations (default)
- **DCs** - view only agented domain controller servers

- **Servers** - view only agented servers that are joined to the domain
- **Workstations** - view only agented workstations that are joined to the domain
- **Others** - view only non-member objects, such as ADAM workgroup servers or workstation agents manually installed on non-Active Directory machines

Show Uninstalled Agents

Select this check box to include all uninstalled agents in the count. Uninstalled agents are not included by default.

Time interval

By default, data will be collected for the last month. However, you can use the controls in the upper right corner of this overview pane to specify a different time interval for collecting this data.

Where: <*nn*> is a positive numeric value and <*interval*> is one of the following:

- Hours
- Days
- Weeks
- Months (default)
- Years

Recent Event Activity

The Recent Event Activity pane allows you to display recent activity for selected events. Click the arrow on the heading of one of the Overview panes and select **Recent Event Activity** to display this pane. By default, the activity for the following events are displayed in this pane:

- Quest Change Auditor Agent restarted
- Quest Change Auditor Agent started
- Quest Change Auditor Agent stopped
- User account locked
- User member-of added
- User member-of removed
- User password changed

Use the controls at the top of this pane to define the content to be included in this Overview pane.

Select Events

Click **Select Events** to select different event classes to be displayed. Clicking this button displays the Select an Event Class dialog. Select the event classes to display and click **Add** to add them to the selection list.

NOTE: A maximum of 10 event classes can be selected. When you have reached this limit, the **Add** button is disabled preventing you from adding any additional event classes.

Use these buttons/controls to define the format used to display the information. By default, the data appears in a data grid format.

- Use this to display the data in a bar graph. Select the **Show Legend** check box to include a legend for the bar graph.

  NOTE: The bar graph button and **Show Legend** check box only appear when there is activity to report in this pane.

- Use this to redisplay the data using the data grid format.

Last <*nn*> Days

The default or selected events will be listed along with the number of events that occurred each day over the specified time interval. By default, the data will be collected for the last seven days. However, you can use the control in the upper right corner of this pane to display from one to seven days of data.

Count of Events By

The event counts pane displays a table listing the total number of events captured, sorted by the selected category. Click the arrow on the heading of one of the Overview panes, select **Count of Events By** and then select one of the following categories to display this pane:

- **Event Class**
- **Facility**
- **Location**
- **Severity**
- **Result**
- **Subsystem**

The count by event panes include the total number of events found in the Change Auditor database based on the category selected. The counts on these panes are hypertext links, which when selected display a Search Results page showing the events associated with the selected count. However, the Search Results page only displays the associated events generated in the last year. If you want to see all of the events associated with the selected count, edit the date range to include the 'last *nn* years' in the When tab on the Search Results page.

Agent Status

The Agent Status pane displays a gauge depicting the current status of agents. Click the arrow on the heading of one of the Overview panes and select **Agent Status** and then select one of the following options to display this pane:

- **Enterprise View** - displays all agented member servers installed in the enterprise
- **Workstation View** - displays all agented workstations that are installed on Active Directory machines in the enterprise
- **Other View** - displays all agented non-member objects, such as ADAM workgroup servers or workstation agents manually installed on non-Active Directory machines in the enterprise
- **<*DomainName*>** - displays all agented machines, including servers, workstations and non-member workgroup computers, installed on the selected domain

Show Uninstalled Agents

By default, only active and inactive agents are included. However, you can select this check box to include the agents that are set as 'uninstalled'.

Double-clicking the gauge displays the Agent Statistics page which provides a global view of all agents, including their current status.

Coordinator Status

The Coordinator Status pane displays a gauge depicting the current status of all the coordinators installed in the entire enterprise or in a selected domain. Click the arrow on the heading of one of the lower panes and select **Coordinator Status** and then select one of the following options to display this pane:

- **Enterprise View** - displays all coordinators installed in the enterprise

- **<*DomainName*>** - displays all coordinators installed in the selected domain

Show Uninstalled Coordinators

Coordinators set as ‘uninstalled’ are not included by default. However, you can select this check box to include the coordinators that are set as ‘uninstalled’.

Double-clicking the gauge displays the Coordinator Statistics page which provides a global view of all coordinators, including their current status.

Alert History Counts

The Alert History pane displays the number of alerts that were successfully sent or failed to send or the number of alerts triggered for a search query. Click the arrow on the heading of one of the lower panes, select **Alert History Counts** and then select one of the following options to display this pane:

- **Counts** - displays the number of alerts that were successfully sent and the number of alerts that failed to send
- **Counts By Query** - displays the number of alerts triggered by search query

Event Details pane

The Event Details pane is displayed when you select **Event Details** or when you double-click an event in the My Favorite Search grid. This pane provides additional details about the event selected in the My Favorite Search grid at the top of the page. The information displayed is the same as that displayed in the Event Details pane at the bottom of a Search Results page. Refer to Event Details pane for a description of the details that this pane may contain.

5

Searches

- Introduction
- Searches page
- View a list of available searches
- Run searches
- Run a quick search

Introduction

Once Change Auditor captures an event, it provides several ways to generate reports. All event information is displayed in the client and the built-in reports provide views for the most common and complex requests. You can view configuration changes from a variety of perspectives. For example, you can view all changes at a particular site; changes made during a specific time frame; or changes performed by a particular administrator. You can also run detailed searches based on user-defined criteria to fit the needs of your organization.

This section provides a description of the Searches page and steps on how to run a built-in search. For information on how to create and run a custom search see Custom Searches and Search Properties.

Searches page

The Searches page displays all search definitions, both private and shared, and the built-in reports. This page consists of the following panes:

- Explorer view
- Searches list
- Search Properties tabs

Explorer view

The left pane of the Searches page displays a hierarchical view of the folders used to manage your search definitions and the built-in reports. This view initially displays the following folders:

Quick Search

Allows you to define a search that is to run as soon as the definition is finished. Unlike other custom searches, this search definition will not be saved unless you click **Save As** on one of the Search Properties tabs.

Private

Used to store your personal custom searches. Only you can see these searches.

NOTE: A foreign security principal in foreign forests is required for some private searches to function properly.

To store foreign user created searches in Change Auditor:
1. Create a trust between the foreign domain and the domain where Change Auditor is installed.
2. Add the foreign user to any group in the Change Auditor domain. This will cause Windows to create a foreign security principal object in the Change Auditor domain.

Shared

Contains the predefined search definitions provided with Change Auditor and can also be used to store public custom searches. All users can see these searches.

Built-In

Contains all predefined reports.

Searches list

The right pane of the Searches page displays a list of the search definitions or built-in reports contained in the folder selected in the explorer view.

The following information is displayed for each search definition:

Table 1. Searches list: Field descriptions

Field	Description
Type	Displays the type of entry: Private Search, Shared Search, Private Alert, Shared Alert or Report.
Alert	Indicates whether an alert has been enabled for the search query. Valid entries for this field are: • **Enabled:** Alerting is enabled for the search query and that at least one transport method is enabled. • **Disabled**: Alerting is disabled for the search query; however at least one transport method is still enabled.
Report	Indicates whether reporting had been enabled for the search query. Valid entries for this field are: • **Enabled**: Reporting is enabled for the search query and a report will be sent to the specified recipients as defined on the Report tab. • **Disabled:** Previously enabled reporting has now been disabled for the search query.
Name	Displays the name assigned to the search definition.

Table 1. Searches list: Field descriptions

Field	Description
Alert To	Displays the email address of any recipients specified to receive an alert email notification. In addition to an email address or distribution list address, you will see the following parameterized values when the corresponding option has been selected on the Alert Custom Email dialog: • %WHO% - Indicates that an alert is to be sent to the user who initiated the change that triggered the alert. • %OWNER% - Indicates that an alert is to be sent to the changed user account, the Exchange Mailbox owner or whose mailbox was accessed by another user and their action triggered an alert. • %MANAGEDBY% - For events associated with users or groups that are being managed by another account, indicates that an alert is to be sent to the managing user's email.
Alert Cc	Displays the email address of any 'carbon copy' recipients specified to receive an alert email notification.
Alert Bcc	Displays the email address of any 'blind carbon copy' recipients specified to receive an alert email notification.
Report To	Displays the email address of any recipients and shared folder specified to receive a report as defined on the Report tab.
Report Cc	Displays the email address of any 'carbon copy' recipients specified to receive a report email.
Report Bcc	Displays the email address of any 'blind carbon copy' recipients specified to receive a report email.

Double-clicking a search definition will run the selected search and display the results in a new Search Results page.

Search Properties tabs

Located across the bottom of the page, the Search Properties tabbed pages define the criteria or properties which make up the selected search.

NOTE: If the Search Properties tabs are not displayed across the bottom of the Search page, click **Show Properties** at the top of the page.

The Search Properties tabs displayed are:

- Info: Allows you to enter a name and description for the search
- Who: Allows you to search for events generated by a specific user, computer, group, or service account.
- What: Allows you to search for events based on subsystem, event class, object class, severity, or results.
- Where: Allows you to search for events captured by a specific agent, domain, site, or server type.
- 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.
- Alert: Allows you to enable alerts and define how and where to dispatch alerts.
- Report: Allows you to enable reporting, specify the report layout template to be used or choose to design your own report layout, and define when and where to send the report.
- Layout: Allows you to define the data (columns) to be retrieved from the database and the sort order for displaying the retrieved data. The layout defined on this tab applies to both the search results displayed in the client and in the report, if reporting is enabled on the Report tab.

- SQL: Displays the SQL script used to create the selected search definition.

  NOTE: This tab is hidden by default. Use **Action | Show SQL Tab** to display this tab.

- XML: Displays the XML representation of the search criteria.

  NOTE: This tab is hidden by default. Use **Action | Show XML Tab** to display this tab.

For a detailed description of the Info, Who, What, Where, Origin and Layout tabs and how to use them to create a custom search, see Custom Searches and Search Properties. For more information about the Alert tab, see Enable Alert Notifications. For more information about the Report tab, see Generate and Schedule Reports.

View a list of available searches

All search definitions, private or shared, custom or built-in, are listed on the Searches page.

To view the search definitions available to all Change Auditor users:

1. Open the Searches page.
2. In the explorer view (left pane), double-click the **Shared** folder to expand the folder and display a hierarchy of folders.
3. Select a subordinate folder under the **Shared** folder.

   The right pane displays a list of the search definitions that are stored in the selected folder.
4. Double-clicking a search in the right-hand pane runs the search and opens a new Search Results page.
5. Right-clicking a search displays a context menu containing actions that can be taken against the selected search.

To view the search definitions that are only available to you:

1. Open the Searches page.
2. Select the **Private** folder (or a subordinate folder created under the **Private** folder) in the explorer view.

   The right pane displays a list of the search definitions that are stored in the selected folder.

To view the list of built-in reports (those provided with Change Auditor):

1. Open the Searches page.
2. Expand the **Built-in** folder in the explorer view.
3. Select a folder under the **Built-in** folder to view the list of search definitions that are stored in the selected folder.

   The right pane displays a list of the search definitions that are stored in the selected folder.

Run searches

To run a previously saved search or built-in report:

1. Open the **Searches** page.
2. Expand and select the appropriate folder in the explorer view to display the list of search definitions stored in the selected folder.

3 Use one of the following methods to run a search:

- Double-click the search definition.
- Right-click the search definition and select **Run.**
- Select the search definition and click **Run**.

4 A new Search Results page will be displayed populated with the events that met the search criteria defined in the selected search definition.

Run a quick search

Quick search allows you to run a search immediately without saving the search definition. To save the search definition, you can select **Save As** before you run the search.

To run a quick search:

1 Open the Searches page.

2 Select the **Quick Search** node in the explorer view to display the Quick Search entry in the Searches list

3 You can either run the default quick search which will retrieve all events that were generated since the beginning of the week or define the search criteria to be used.

- To run the default search, double-click the **Quick Search** entry in the Searches list or click **Run**.
- To define the search criteria, select the **Quick Search** definition to enable the Search Properties tabs. On the Search Properties tabs, enter the search criteria to use. Once finished entering the search criteria, click **Run** from one of the Search Properties tabs.

4 A new search results tab, titled **Quick Search**, will be displayed populated with the events that met the search criteria defined.

6

Search Results and Event Details

- Introduction
- Search Results page
- View search results
- Preview search results
- Compare results side-by-side
- View event details or search properties
- Copy event details
- Email event details
- Copy event details
- Add comments
- View user context and run related searches
- Protect critical objects, mailboxes, files and folders
- Add search properties to existing event queries

Introduction

Audit events are the changes captured by agents, reported to a coordinator, and then written to the database. These events can be retrieved and viewed through searches. When you run a search, Change Auditor searches the events in the database for the desired results. The results are then displayed in the Search Results page.

The terms ‘searches’ and ‘reports’ are used in conjunction to acquire the desired output. You run a 'search' and the results returned is a ‘report’.

Auditing and centralizing the collection of events is only one part of the total control and output required for enterprise security and compliance. It is equally important to be able to retrieve the real-time data and sort through it quickly and efficiently.

This section provides a description of the Search Results page and the Event Details pane. It also provides instructions for performing related tasks when viewing the search results. For a description of the other dialogs mentioned in this chapter, refer to the online help.

Search Results page

A new results page is created whenever a search is run. When a search is run, this page displays detailed information about the events found as a result of the search. This page consists of the following panes:

- Search Results grid
- Search Properties tabs or Event Details pane

Search Results grid

The Search Results grid displays the events captured as a result of running a search from the Searches page. The top area of the grid displays the following information:

Run on

Displays the date and time when the search was run.

NOTE: Based on the client's current local date and time. The format used to display this date and time is determined by the local machine's regional and language setting.

Run Time

Displays the amount of time it took to run the search.

Records

Displays the total number of records returned.

Refresh

Use the **Refresh** button to redisplay the latest information.

Cancel

When a large number of records are being captured for display, the **Refresh** button will become a **Cancel** button allowing you to cancel the search.

By default, the grid contains the following information about the events returned when a search is run. (You can specify the columns, sort order and grouping for a search, as well as the display format by using the Layout search properties tab.)

Table 1. Search Results grid: Event information displayed by default

Column	Description
Action	Displays what change was made to the object.
AD Failure Reason	Displays the reason for the Active Directory failed event.
AD Failure Status Code	Displays the failure code for the Active Directory failed event.
Coordinator ID	The coordinator that processed the event.
Domain	Displays the name of the domain to which the agented server belongs.
Event	Displays the type of change that occurred.
Facility	Defines the event class facility to which the change event belongs.

Table 1. Search Results grid: Event information displayed by default

Column	Description
Result	Indicates whether the operation mentioned in the event was successfully completed. Valid states are: • Success - Indicates the operation occurred as stated in the event. • Protected - Indicates that the operation was prevented from occurring because the object is protected by the Change Auditor object locking feature. • Failed - indicates that the operation was prevented from occurring due to a factor/setting outside of Change Auditor's control. • None - indicates that the operation occurred as stated, but no results were captured for the event. For example, this state is used for most of the internal Change Auditor events.
Server	Displays the name of the server where the change occurred.
Severity	Displays the severity assigned to a configuration change event: • High • Medium • Low
Site	Displays the name of the site where the agented server resides.
Subsystem	Defines the subsystem, or area of auditing, where the change event occurred.
Time Detected	Displays the date and time when the agent captured the event. **NOTE:** Based on the client's current local date and time. The format used to display this date and time is determined by the local machine's regional and language setting. **NOTE:** For Microsoft Entra sign in events the time detected in the search results references the sign-in time.
User	Displays the name of the user who initiated the change.

Search Properties tabs

From a Search Results page, use the **Search Properties** tool bar button to display the Search Properties tabs across the bottom of the screen. This view consists of tabbed pages defining the criteria or properties which make up the selected search.

For a detailed description of the Info, Who, What, Where, Origin and Layout tabs and how to use them to create a custom search, refer to Custom Searches and Search Properties. For more information about the Alert tab, see Enable Alert Notifications and the Report tab, see Generate and Schedule Reports.

Event Details pane

Use the **Event Details** button on a Search Results page, Overview page, or Alert History page to display the Event Details pane. You can also double-click an event in the search results grid to display the Event Details pane for the selected event.

The following details about the selected event selected are available:

NOTE: All dates and times are based on the client's current local date and time. The format used to display the date and time is determined by the local computer's regional and language setting.

Table 2. Event Detail pane: Field descriptions

Field	Description
Severity	The severity level assigned to the search is displayed in the upper left-hand corner.
Who	This field specifies the name of the user who initiated the change. If available, the display name of the user account is also displayed in parenthesis.
When	This field specifies the date and time when the change occurred.
Where	This field displays the name of the server where the change occurred.
Source	This field displays the source of the event: • Change Auditor • Active Roles • GPOADmin **NOTE:** When the event is generated from Active Roles or GPOADmin, the name of the user account that initiated the event is displayed in parenthesis. **NOTE:** If the **Source** field displays 'ActiveRoles' (instead of 'ActiveRoles Server') you are not using the latest integration scripts. If you want to take advantage of the additional events and initiator account information captured using the new integration scripts, ensure you are running Active Roles 6.9 (or higher) with Change Auditor for Active Directory 6.5 (or higher).
Origin	This field displays the NetBIOS name and IP address of the workstation or server from which the event was generated.
What	Displays a brief description of the change that occurred. There are three basic types of events generated that determine the 'what' information that will be displayed: • Occurrence events (such as an object is created or deleted) • Change events • Delta events (such as DACL/SACL changes) Depending on the type of event, additional details may be displayed at the bottom of this pane.
Result	Indicates whether the operation mentioned in the event was successfully completed. Valid states are: • Success (Green) - Indicates that the operation occurred as stated in the event. • Protected (Yellow) - Indicates that the operation was prevented from occurring because the object is being protected by the Change Auditor object locking feature • Failed (Red) - Indicates that the operation was prevented from occurring due to a factor/setting outside of Change Auditor's control. • None (Green) - Indicates that the operation occurred as stated, but no results were captured for the event. For example, this state is used for most of the internal Change Auditor events.
Subsystem	The first field defines the subsystem, or area of monitoring, where the change event occurred (for example, Active Directory, Service, or Group Policy).
Action	This field defines the action associated with the selected event.
Facility	This field defines the event class facility to which the change event belongs.

Table 2. Event Detail pane: Field descriptions

Field	Description
Class	For Active Directory and Exchange events, this field displays the object class that was modified, such as user, group, computer, nTDSConnection, CrossRefContainer.
Attribute	If an attribute has been added, deleted or modified, this field displays the name of the attribute.
Type	For Active Directory events associated with groups, this field displays the type of group that was modified (for example, Global (Security), Domain Local (Security)). For AD Query events, this field displays the type of query: • LDAP • GC
Object	For Active Directory and Exchange events, this field displays the name of the object that was modified.
Authentication	Indicates whether the LDAP operation is secured using the SSL (Secure Socket Layer)/ TLS (Transport Layer Security) technology, simple bind authentication, or signed using Kerberos-based encryption. **NOTE:** If changes are initiated within LSASS and not through the LDAP protocol itself, this field will not be captured.
Port	For Active Directory, AD Query, and Exchange events, this field indicates the port used for authentication.
Scope	For AD Query events, this field displays the scope of coverage: • This object only • This object and all children
Results	For AD Query events, this field displays the number of results returned as a result of the query.
Occurrences	For AD Query events, this field displays the number of times the AD query occurred during the specified interval.
Since	For AD Query events, this field displays the date and time when the AD query was first initiated.
Elapsed	For AD Query events, this field displays how long the AD query took to run. Zero (0) indicates that it took less than a millisecond to complete.
Filter	For AD Query events, this text box displays the filter string used in the AD query.
Attributes	For AD Query events, this text box displays the attributes that were queried.
Path	For File System events (including EMC and NetApp), this field displays the full path of the file or folder where the modification occurred.
Process	For File System events, this field is populated with the full path of the application responsible for the file change.
Service	For Service events, this field displays the name of the services that were modified.
Key	For Registry events, this field displays the name of the registry key that was modified.
Value	For Registry events, this field displays the registry value that was modified.
Policy	For Group Policy events, this field displays the name of the group policy that was modified.
Section	For Group Policy events, this field displays what section of the group policy was modified.
Item	For Group Policy events, this field displays the group policy item that was modified.
Account	For Local Account events, this field displays the local account that was modified.
From	This text box lists the old value that was assigned to the object.
To	This text box lists the new value that is now assigned to the object. **NOTE:** The To and From information does not apply to permission/ACL (Access Control List) type changes and is replaced with the Changes section. This information is also not available for occurrence type events, e.g., when an object is created or deleted.
Farm	For SharePoint events, this field displays the name of the SharePoint farm to which the modified component belongs.

Table 2. Event Detail pane: Field descriptions

Field	Description
URL	For SharePoint events, this field displays the name of the SharePoint site to which the modified component belongs.
Target	For SharePoint events, this field displays the URL of the SharePoint item that was modified.
Mailbox	For Microsoft 365 Exchange Online mailbox events, this field displays the account name of the online mailbox where the change occurred.
Folder	For Microsoft 365 Exchange Online mailbox events, this field displays the folder name where the change occurred.
Cmdlet	For Microsoft 365 Exchange Online administration events, this field displays the name of the administrative cmdlet what was run.
Object	For Microsoft 365 Exchange Online administration events, this field displays the name of the object within the administrative cmdlet that was modified.
Logon Start	For Logon Session events, this attribute displays the date and time when the user initially logged onto the computer.
Logon End	For Logon Session events, if applicable this attribute displays the date and time when the user logged out of the computer.
Duration	For Logon Session events, depending on the event this attribute displays how long the user session lasted or how long the user was actually logged onto the computer.
Session Start	For Logon Session events, this attribute displays the date and time when the current user session began.
Session End	For Logon Session events, if applicable this attribute displays the date and time when the current user session ended.

View search results

To view the results of a search:

1. From the Searches page, run a search.
2. For each search that is run, a new search results page is automatically created and opened, allowing you to view the event records returned.
3. When multiple search results are active, select the heading tab at the top of a search page to view the selected search results.
4. Use the column controls to sort, rearrange, or group the data displayed. See Customize table content for more information on using the column controls to customize the content of this page.
5. Change Auditor also provides advanced filtering options that allow you to modify the results of a search without changing the original search. Click in the **Click here to filter data** cell to enter the criteria to be used to filter the data displayed. See Filter data for more information on using Change Auditor's filtering feature.

Display results in different formats

When a grouping is created (for example, a single column heading is dragged up into the heading area to group the data), three icons are added to the heading area which can be used to display the data in a different format. The following icons/formats are available:

Data Grid: Select the data grid icon to redisplay the data in the grid format (default format).

Pie Chart: Select the pie chart icon to display a pie chart showing the correlated data. Move your cursor over the pieces in the pie chart to display the label and number of items that make up that piece of the pie.

Bar Graph: Select the bar graph icon to display a bar graph showing the correlated data. Move your cursor over the bars in the graph to display the label and number of items that make up that bar.

NOTE: The Pie Chart and Bar Graph displays are only available when a single level grouping has been applied to the data grid. Also, when the search results are too numerous to chart, a message will display stating that there are too many items to display them all.

Preview search results

The criteria definition is in-line with the results which enables you to preview and modify the results without closing and opening multiple dialogs.

To modify search criteria and preview the results:

1. Open the Search Results page for a search where you want to preview changes based on new search criteria.
2. Click **Search Properties** to display the Search Properties tabs across the bottom of the page.
3. Modify the search criteria and then click **Preview Changes** from one of the Search Properties tabs.

4 The results of the modified search appears at the top of the open Search Results page. An asterisk is appended to the name in the tab denoting that the search properties have been modified and these changes have not yet been saved.

5 Once you achieve the desired results, you can use **Save** or **Save As** on one of the Search Properties tabs to save the modifications made to the search criteria.

Compare results side-by-side

You can run two searches side-by-side simultaneously. When multiple pages are open, you can split the current screen to display two or more pages at the same time. For example, you can view multiple search results pages in the client allowing you to compare the results against each other.

NOTE: For optimal viewing, this feature should be used in a dual monitor configuration.

To compare results side-by-side:

1 Run the searches to be compared. On the Search Results pages, we recommend that you hide the Event Details pane and Search Properties tabs so that when the screen spits, you will have more space for viewing events.

2 Right-click the heading tab of one of these Search Results pages and select one of the following commands:

- **New Horizontal Tab Group** - to view two or more panes down the screen.
- **New Vertical Tab Group** - to view two or more panes across the screen.

3 This splits the screen (either horizontally or vertically depending on the command selected) displaying multiple pages in the single view.

4 To move a page from one pane to another, right-click the heading tab of the page to be moved and select **Move to Next Tab Group**. This will move the selected page to the other pane displayed. To move this page back, right-click the heading tab and select **Move to Previous Tab Group**.

5 To close the split screen and return to a single pane, use **Action | Reset Display**.

View event details or search properties

From the Search Results page, you can view the search properties used to generate the displayed events or you can access more detailed information about an event. You can easily switch between the Search Properties tabs and Event Details pane at any time.

To display event details for an event:

1 Open a Search Results tab and select an event from the Search Results grid.

2 If neither the Search Properties tabs or Event Details pane are being displayed (or the Search Properties tabs are displayed), use one of the following methods to display the event details:

- double-click the event entry in the results grid
- click the **Event Details** tool bar button
- right-click the event and select **Event Details**

3 To hide the Event Details pane, use hide button in the upper right corner of the Event Details pane.

To display search properties for an event:

1 Open a Search Results tab and select an event from the Search Results grid.

2 If neither the Search Properties tabs or Event Details pane are being displayed (or the Event Details pane is displayed), use one of the following methods to display the search properties:

- click the **Show Properties** tool bar button
- right-click the event and select **Show Properties**

3 To hide the Search Properties tabs, use the hide button in the upper right corner of the Search Properties pane.

Copy event details

To copy an event's details:

1 Open a Search Results tab and select an event from the Search Results grid.

2 Use one of the following methods to copy the contents to the clipboard:

- Right-click the event and select **Copy**.
- From the Events Details pane, click the **Copy** tool bar button.

> **NOTE:** You can also hold down the **Shift** key while clicking the **Copy** button to copy additional event details to the clipboard. This additional information may be requested by the Quest Support staff for troubleshooting purposes.

3 Open the application (for example, Notepad) where you want to paste the content, right-click and select **Paste**.

Email event details

To email an event's details:

1 Open a Search Results tab and select an event from the Search Results grid.

2 Use one of the following methods to email the selected event's details:

- Right-click the event in the Search Results grid and select **Email**.
- From the Event Details pane, click the **Email** tool bar button.

> **NOTE:** You can also hold down the **Shift** key while clicking the **Email** button to email additional event details. This additional information may be requested from the Quest Support staff for troubleshooting purposes.

3 This creates a new email containing the contents of the Event Details pane. Enter the recipient's email address (in the To and CC fields) and edit the subject line if desired.

4 Click **Send.**

5 If applicable, the Internet Connection wizard will be displayed allowing you to create a new Internet account, which includes the following information:

- display name as you would like it to appear in the From field of the outgoing message
- your email address
- your incoming mail server
- your outgoing mail (SMTP) server

Add comments

To append comments to an event which can then be later specified as search criteria to retrieve all the events that contain a specific comment or keyword.

To add comments to an event:

1. Open a Search Results tab and select an event from the Search Results grid.
2. Use one of the following methods to add or append comments to the selected event:
   - Right-click the event and select **Comments**.
   - From the Event Details pane, click the **Comments** tool bar button.
3. This will display the Comments dialog. In the New Comments text box at the bottom of this dialog, enter the comments to be associated with the selected event.
4. Click **OK** to close the dialog and return to the Search Results tab.

To view comments:

1. Open a Search Results tab and select an event from the Search Results grid.
2. Use one of the following methods to view or append comments to the selected event:
   - Right-click the event and select **Comments**.
   - From the Event Details pane, click the **Comments** tool bar button.
3. This will display the Comments dialog where previously entered comments are displayed in the top pane.
4. To append a new comment to those that already exist, use the text box at the bottom of the screen to enter your new comment.
5. Click **OK** to close the dialog and return to the Search Results tab.

View user context and run related searches

From the Event Details pane you can view additional details about the user who initiated the change, view resource details about the computer where the change occurred, or run related searches based on the who, where, what, when or origin of the event selected in the Search Results grid.

Expand **Related Search** on the Event Details pane to display the options available, which are based in the selected event:

- **Who**: Select this to run a query for all change events generated by this user during the same date interval as that specified in the When tab of the selected event.
- **View Contact Card**: For events with a user object, select this to view contact information and group membership for this user.
- **Where**: Select this to run a query for all change events captured by this agent during the same date interval as that specified in the When tab of the selected event.
- **View Resources**: Select this to display the Resource Properties pane for this server, which includes: Machine Info, Processors, Drives, Shares, Services, and if applicable Exchange Mailboxes.

  See Resource Properties pane for more details about the resource details provided.
- **What**: Select this to run a query for change events captured for this event class during the same date interval as that specified in the When tab of the selected event.
- **When**: Select this to run a query for change events that occurred on this date.

- **Origin**: Select this to run a query for change events that originated from this workstation or server during the same date interval as that specified in the When tab of the selected event.
- **Object**: Select this to run a query for change events generated against this object during the same date interval as that specified in the When tab of the selected event.

  NOTE: When selecting an object that contains a path, the related search will only return related events where the full paths are the same.

  NOTE: This last option is the object from the original event, such as a file or folder, directory object, registry key, etc.

To view the contact information and group membership for a user:

1. At the top of the Search Results page, select an event to display the related Event Details pane.
2. At the top of the Event Details pane, click the arrow to the right of the **Related Search** tool bar button and select **View Contact Card**.
3. The contact information appears for the user who initiated the change in the selected audit event. In addition, the Member Of pane on this dialog lists the groups to which this user belongs.
4. Click **OK** to close this dialog.

To run a query for events generated by the same user:

1. At the top of a Search Results page, select an event to display the related Event Details pane.
2. At the top of the Event Details pane, click the arrow to the right of the **Related Search** tool bar button.
3. Click the first entry in the context menu, which is the name of the user who initiated the change in the selected audit event.
4. A new Search Results page appears populated with all change events generated by this user during the same date interval as that specified in the When tab of the selected event.

   Note that the user's name is used as the Search Name (name on tab) for this new query.

To view resource properties about the server where the change occurred:

1. At the top of the Search Results page, select an event to display the related Event Details pane.
2. At the top of the Event Details pane, click the arrow to the right of the **Related Search** tool bar button.
3. Select **View Resources.**
4. The Resource Properties pane appears which contains additional details about the server where the change occurred. See Resource Properties pane for more information about the content of the tabbed pages on this pane.

Protect critical objects, mailboxes, files and folders

When viewing events, administrators can create protection templates to protect against unauthorized modifications to the following:

- Active Directory objects
- ADAM (AD LDS) objects
- Group Policy Objects
- Exchange mailboxes
- File System files and folders

To protect an object, mailbox, file, or folder:

1. Open a Search Results tab and select an event from the Search Results grid.
2. From the Event Details pane, click the **Protect Object** tool bar button.
3. This opens the required Object Protection Wizard for the selected object.

Add search properties to existing event queries

After selecting a specific event from the results of a search, you can further refine your search criteria. Expand **Add to Search** to display the available options for refining your current search. These options are produced from the details of the selected event and may differ between event types.

Choosing a criteria from this list will add it to your current search. You can then preview the refined results before saving the search. Once saved, the new search criteria will be permanent.

7

Custom Searches and Search Properties

- Introduction
- Create a custom search
- Search Properties tabs

Introduction

You can create custom search definitions to search for the configuration changes that need to be tracked in your environment. The search properties tabs across the bottom of the Searches page allows you to define new custom searches.

This section provides steps on how to create custom searches and to preview search results. It also provides a description of the Search Properties tabs and how to use these tabs to customize your searches. For a description of the other dialogs mentioned, see to the online help.

A new column has been added as of Change Auditor 7.0 that allows you to display extra information through the search Layout tab:

Table 1. Available columns

Layout Tab	Search Column Name	Description
Origin - AD Site Name	Origin AD Site	The Active Directory site of the computer from which the event originated.

Create a custom search

The following procedure provides the 'general' steps involved in creating a custom search.

NOTE: Selecting the **Private** folder creates a search that only you can run and view. Selecting the **Shared** folder creates a search that all users can run and view.

To define a new 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.
3. Click **New** at the top of the Searches page.
4. On the Search Properties tabs, enter the search criteria to use:
   - Info — enter a name and description for the search
   - Who — allows you to search for events generated by a specific user, computer, group, or service account.

- What — allows you to search for events based on subsystem, event class, object class, severity, or result
- Where — allows you to search for events captured by a specific agent, domain or site
- When — allows you to search for events that occurred during a specified date and time range
- Origin — allows you to search for events that originated from a specific workstation or server

NOTE: When you specify criteria on more than one search properties tab (for example, Who, What and Where tabs), Change Auditor first evaluates each individual tab's criteria and then chains the individual tab's criteria together using the 'AND' operator, returning only those events that meet all the specified search properties.

5 To be notified when an event is captured as a result of this custom search, open the Alert tab to enable and define how and where to dispatch alerts when the selected search criteria is met. See Enable Alert Notifications for more information about setting up alert notifications.

6 Once you have defined the search criteria to use, you can either save the search definition or run the search.

- To save and run the search, click **Run** from one of the Search Properties tabs.
- To save the search definition without running it, click **Save** from one of the Search Properties tabs.
- To create a search using a different name than was initially entered, click **Save As | Save As** from one of the Search Properties tabs.
- To save the search definition as the new default for new searches, click **Save As | Save As Default** from one of the Search Properties tabs.

Search Properties tabs

To define custom search criteria, use the Search Properties tabs, which are displayed across the bottom of the Searches page. The Search Properties tab pane consists of the following tabs:

- Info tab
- Who tab
- What tab
- Where tab
- When tab
- Origin tab
- Alert tab (Search Properties tabs)
- Report tab (Search Properties tabs)
- Layout tab
- SQL tab
- XML tab

To display and enable the Search Properties tabs:

1 From the Searches page:

- Click **Show Properties**
- Right-click a folder (left pane) or search definition (right pane) and select **Show Properties**

- Select a folder (left pane) or search definition (right pane) and click **New | New Search**

NOTE: You can also display the Search Properties tabs from a Search Results tab, using **Search Properties**.

2 Use the “X” hide button in the upper right corner of the Search Properties tab pane to hide this pane.

Info tab

From the Info tab, you can view or enter the name and description of a search definition. You can also define the maximum number of records to be retrieve and display, or enable a refresh interval that defines how often the client is to retrieve and redisplay updated information.

The Info tab contains the following information and controls:

Table 2. Info tab: Field and control descriptions

Field and Control	Description
Search Name	Displays the name of the selected search. When creating a search, place your cursor in this text box and enter a descriptive name for the search.
Search Description	Displays the description of the selected search. To add a description to a new search, place your cursor in this text box to enter a brief description of the search.
Search Limit	Specifies the maximum number of records to retrieve and display. By default, the maximum of 50,000 records are returned from the database during a single request. Select this check box and use the arrow controls to change the search limit for the selected search. **NOTE:** Clearing this check box removes the search limitation, which may increase both client memory and wait time if expected search results are over 100,000. Therefore, Quest recommends that you leave this check box checked and use the defined search limit.
Refresh Interval	Specifies how often the client is to retrieve and redisplay updated information. Select this check box and use the arrow controls to enable and set the refresh interval for the selected search. When this option is checked, an extra field, **Next Refresh**, is added to the heading area of the Search Results grid. **NOTE:** This option is not checked by default for new searches, only for the default favorite search (Change Auditor Real-Time) used in the Overview page. The default interval for the default favorite search is five minutes.

To name a new search:

1 Place your cursor in the **Search Name** text box and enter a descriptive name for the search.

> **NOTE:** If you do not enter a new name for your search, it is named ‘New Search’.

2 Place your cursor in the **Search Description** text box and enter a brief description of the search.

3 After entering the search name and optional description, proceed to the other Search Properties tabs to enter the search criteria.

To change the maximum number of records to retrieve:

The **Search Limit** field specifies the maximum number of records to retrieve and display for the selected search. By default, a maximum of 50,000 records are returned from the database during a single request.

1 To restrict the search results to a specific number of records, ensure that the **Search Limit** check box is checked.

2 Set the value to the maximum number of events to return.

> **NOTE:** Clearing this check box removes the search limitation, which may increase both client memory and wait time if expected search results are over 100,000. Quest recommends that you leave this check box checked and use the defined search limit.

To set a refresh interval:

The **Refresh Interval** field specifies how often to retrieve and redisplay updated information.

1 Select the **Refresh Interval** check box to enable this feature and activate the field to the right of this field.

> **NOTE:** This option is not checked by default for new searches, only for the default favorite search (Change Auditor Real-Time) used in the Overview page. The default interval for the default favorite search is five minutes.

2 Enter or use the arrow controls to set the refresh interval (how many minutes between refreshes) for the selected search.

When this option is checked, an extra field, **Next Refresh**, is added to the heading area of the search results grid whenever this search is run.

Who tab

The Who tab allows you to view or define the users, computers, groups, or service accounts to include in (or exclude from) the search definition. You can also select to include or exclude administrators. When multiple 'who' criteria is specified, Change Auditor uses the 'OR' operator to evaluate change events, returning events for activity performed by any of the users, computers, or groups listed.

> **NOTE:** You can add a group to a search to find all events by the members of that group. Change Auditor must expand and store the membership of the group before all expected events are returned when the search is run. When the search is saved, Change Auditor expands the group if it has not already been expanded. This may take several minutes, depending on your environment. See Group Membership Expansion for the options available regarding group expansion.

> **NOTE:** Activity performed by an account specified in an Excluded Accounts template is not captured by the agents to which this template is assigned. Change Auditor does not return any audit events for these excluded accounts even if you specify them in your 'who' search criteria. For more information about excluding accounts, see Account Exclusion.

The Who tab contains the following information and controls:

Table 3. Who tab: Field and control descriptions

Field and Control	Description
Runtime Prompt	Select this check box to prompt for the 'who' criteria when this search runs. That is, when you select **Run**, the Select Active Directory Object dialog is displayed allowing you to locate and select the users, computers, groups, or service accounts to search. **NOTE:** • When this check box is checked, the Add toolbar buttons are deactivated. • You cannot enable alerting for search definitions that use the Runtime Prompt option.
Exclude the Following Selection(s)	Select this check box to specify the users, computers, or groups to exclude from the search. That is, Change Auditor is to search all users, computers, and groups except those listed.

Table 3. Who tab: Field and control descriptions

Field and Control	Description
Include Event Source Initiator	Select this check box if you want to include Active Roles or GPOADmin events in the search. Selecting this check box instructs Change Auditor to retrieve all change events made by the specified user account, including those initiated by Active Roles and GPOADmin. **NOTE:** An extra column (Initiator UserName) is added to the Search Results grid that contains the user information of who made the change through Active Roles or GPOADmin.
Who list	Contains the individual users, computers, groups, or service accounts to include in the search (or excluded from the search if the **Exclude the Following Selection(s)** option is checked). By default, all users, computers, and groups are included in a new search definition and therefore, this list is empty.

To search for events generated by a specific user, computer, group, or service account:

NOTE: By default, each new search searches for change events generated by all users, computers, gruops, and service accounts; therefore, the list box on the Who tab will be empty.

1. On the Who tab, click **Add** to add an active user, computer, group, or service account to the 'who' list.

   On the Select Active Directory Object dialog, use either the Browse or Search page to search your environment to locate and select the user, computer, group, or service account to include.

   If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.

2. Click **Add** to add it to your selection list.

   Repeat to include each additional directory object.

3. After selecting one or more directory objects, click **Select** to save your selection and close the dialog.

   NOTE: You can use **Add with Events** (instead of **Add**) to select a user, computer, or group that already has an audit event associated with it in the database. The accounts available for selection are based on the 'when' clause (When tab) and the search limit (Info tab) specified for the current search.

   Use this to search for events that are tied to users who have been removed from Active Directory.

4. Optionally, select **Add | Administrator,** select **Yes** or **No** to include or exclude users with the Administrator right, and click **OK**.

5. When this search runs, Change Auditor searches for change events generated by only the selections listed on the Who tab.

   TIP: If you are running Active Roles or GPOADmin and want to include events generated by Active Roles or GPOADmin in the search, select the **Include Event Source Initiator** check box. For more information, see the Active Roles Integration or GPOADmin Integration sections in the Change Auditor Installation Guide.

To use a wildcard expression to specify a user or group:

1. On the Who tab, expand **Add** and select the **Add Wildcard Expression** option.
2. On the Add Who dialog, enter the wildcard expression to use to search for a user (domain\user name) or group (domain\group name):
   - Select the comparison operator to use: **Like** or **Not Like**.
   - In the field to the right, enter the pattern (character string and * wildcard character) to be used to search for a match. Use the * wildcard character to match any string of zero or more characters.

     For example, **LIKE *admin*** finds all users with the character string 'admin' anywhere in the name.

- By default, the wildcard expression is used to search for a user. To search for a group, select the **Group** option.

  NOTE: When using the **Group** option, the Group Membership Expansion option on the Coordinator Configuration page (on the Administration Tasks tab) must be set to **Expand all groups**.

3. After entering the wildcard expression to use, click **OK** to close the dialog and add the wildcard expression to the 'who' list.
4. When this search runs, Change Auditor searches for change events generated by the users (or users that are members of the groups) whose name matches the specified wildcard expression.

What tab

Use the What tab to define 'what' entities to inlcude (or exclude) in the search. More specifically, using this tab you can create a search for events based on:

- Subsystem
- Event Class
- Object Class
- Severity
- Result

When criteria is specified on the What tab, Change Auditor retrieves only those events that match the criteria listed on the What tab. When multiple 'what' criteria is specified on this tab, Change Auditor uses the 'AND' operator to evaluate an event and returns only those events that meet all the specified criteria. However, when multiple subsystems (for example, Active Directory, ADAM and Exchange) are specified, Change Auditor uses the 'OR' operator to evaluate these entities, returning events that meet any of the specified subsystem criteria. This also applies when multiple event classes are specified. That is, when multiple event classes are specified, Change Auditor uses the 'OR' operator and returns any of the specified events.

NOTE: By default, all events are included in a new search definition and therefore the list box on the What tab will be empty.

Once criteria is added, the criteria list box contains an expandable view displaying the following information for all the criteria defined for the search definition:

Entity

Lists the entity (subsystem, event class, object class, severity, or result) selected. Expanding the **Entity** entry displays the specific criteria and any options or restrictions, defined as part of the search criteria.

Exclude

Indicates whether the criteria is included in (False) or excluded from (True) the search definition.

Action(s)

When applicable, this column displays the actions (all, add attribute, delete attribute, modify attribute, rename object, add object, delete object, or other) included in the search definition.

NOTE: Only displayed when the entity is Active Directory, ADAM, Exchange, File System, Group Policy, Local Account, or Registry.

Transport(s)

When applicable, this column displays the transports (all, SSL/TLS, Kerberos, Simple Bind) included in the search definition.

NOTE: Only displayed when the entity is Active Directory, ADAM, Exchange, or AD Query.

Port

When applicable, this column displays the port included in the search definition.

Click the expansion box to the left of the Entity field to expand this view to display the following details:

Object

Displays the object selected for auditing.

Restriction

If applicable, this field displays the additional restrictions specified for the search definition.

NOTE: Only displayed when the entity is an Event Class.

Scope

Indicates the scope specified (All Object, This Object, This Object and Child Objects Only, This Object, All Child Objects, and Members of this group).

NOTE: Only displayed when the entity is Active Directory, ADAM, Exchange, File System, Group Policy, Local Account, or Registry.

Examples of custom searches based on ‘what’ criteria

NOTE: Only the ‘what’ criteria that does not require a specific license is covered in this section. For more information about ‘what’ criteria that requires a specific license, refer to the appropriate Change Auditor User Guide:

- **Object Class** - Change Auditor for Active Directory User Guide
- **Subsystem | Active Directory** - Change Auditor for Active Directory User Guide
- **Subsystem | AD Query** - Change Auditor for Active Directory Query User Guide
- **Subsystem | ADAM (AD LDS)** - Change Auditor for Active Directory User Guide
- **Subsystem | Microsoft Entra** - Microsoft 365 and Microsoft Entra ID Auditing User Guide
- **Subsystem | Exchange** - Change Auditor for Exchange User Guide
- **Subsystem | File System** - Change Auditor for Windows File Servers User Guide, Change Auditor for EMC User Guide or Change Auditor for NetApp User Guide
- **Subsystem | Group Policy** - Change Auditor for Active Directory User Guide
- **Subsystem | Logon Activity** - Change Auditor for Logon Activity User Guide
- **Subsystem | Microsoft 365** - Microsoft 365 and Microsoft Entra ID Auditing User Guide
- **Subsystem | SharePoint** - Change Auditor for SharePoint User Guide
- **Subsystem | SQL** - Change Auditor for SQL Server User Guide

To search for events based on an event class or facility:

1 On the What tab, click **Add**. (Or expand the **Add** button and select **Event Class**.)

NOTE: You can use the **Add with Events | Event Class** command (instead of **Add | Event Class**) to select an entity that already has an event in the database.

2 On the Add Facilities or Event Classes dialog, select a single event, click **Add**, and select **Add This Event** or **Add All Events in Facility**.

> **NOTE:** When multiple events are selected, Change Auditor uses the 'OR' operator to evaluate the change events, returning any of the events specified.

3 Depending on the event class entry selected in the data grid, an extra Restriction pane may display across the middle of this dialog.

For some event classes, use the restriction pane to specify 'from' and/or 'to' value restrictions. To define a restriction, select the appropriate check box and enter the value.

For other event classes (such as DNS Zone, Distribution and Security groups), use the restriction pane to apply filter options for filtering by individual parameter values (for example, auditing of static DNS entries).

To do this, select the **Filter by parameter** check box and then select from the available parameter values that are enabled (for example, for the DNS Entry Type parameter, you can select **Static** and/or **Automatically expiring**).

4 Once you have defined the restrictions, use either **Add** or **Update Restriction**:

- If the event has not been added to the Selections list box, click **Add** to add the event to the selection list.
- If the event was previously added to the Selections list box, click **Update Restriction** to update the restrictions for the event.

> **NOTE:** You can also use the **Shift** and **Ctrl** keys to add multiple event classes to the selection list. However, the restrictions pane and the **Add | Add All Events in Facility** command are not available when multiple event classes are selected.

> **NOTE:** Select the **Exclude the Above Selection(s)** check box if you want to search for all event classes and facilities except those listed in the 'what' list.

> **NOTE:** Select the Runtime Prompt check box to prompt for the facility or event class criteria every time the search runs. When this check box is checked, the data grid and buttons on this dialog are disabled.
>
> You cannot enable alerting for search definitions that use the Runtime Prompt option.

5 Once you have made your selections, click **OK**.

The search criteria listed on the What tab now defines what will be searched for when this search is run.

To search for changes to local users or groups:

1 On the What tab, expand **Add** and select **Subsystem | Local Account**.

> **NOTE:** You can use the **Add with Events | Subsystem | Local Account** command (instead of **Add | Subsystem | Local Account**) to select an entity that already has an event in the database.

2 On the Add Local Account dialog, select one of the following options to define the scope of coverage:

- **All Objects** - select this option to include all objects
- **This Object** - select this option to include individual objects

3 If you selected **This Object**, the data grid, which displays a list of all the users and groups in the local SAM databases on the selected Member Server, and associated buttons are enabled.

4 To add an account, select the account in the data grid and click **Add** to add it to the selection list at the bottom of the dialog. Repeat to add more accounts.

5 To replace an account in the selection list, select the 'new' account in the data grid, select the 'old' account in the selection list and click **Update**. The entry in the selection list is replaced with the 'new' account.

6 To select a local account on a different computer, click **Browse** to the right of the **Account** field. On the Select Active Directory Object dialog, use the Browse or Search pages to locate and select another computer.

If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.

7 Click **Select** to save your selection and close the dialog.

On the Add Local Account dialog, the local user and group accounts available on the specified computer are displayed in the data grid.

> **NOTE:** Select the **Exclude the Above Selection(s)** check box if you want to search for events generated by all local accounts except those listed in the 'what' list.

> **NOTE:** Select the Runtime Prompt check box to prompt for a local account every time the search runs. When this check box is checked, the data grid and buttons on this dialog are disabled.
>
> You cannot enable alerting for search definitions that use the Runtime Prompt option.

8 Once you have selected the local accounts to include in the search, click **OK**.

When this search is run, Change Auditor searches for events generated by the local accounts listed on the What tab.

To search for changes to registry keys:

> **NOTE:** Registry auditing is only available when you have applied custom Registry Auditing templates that define the registry changes to be audited. See Registry Auditing for more information about capturing registry events.

1 On the What tab, expand **Add** and select **Subsystem | Registry**.

> **NOTE:** You can use **Add with Events | Subsystem | Registry** (instead of **Add | Subsystem | Registry**) to select an entity that already has an event in the database.

2 On the Add Registry Key dialog, select one of the following options to define which system registry keys to include in your search definition:

- **All Registry Keys** — include all registry keys
- **This Object** — include only the selected objects
- **This Object and Child Objects Only** — include the selected objects and its direct child objects
- **This Object and All Child Objects** — include the selected objects and all subordinate objects (in all levels)

3 By default, **All Actions** is selected meaning that all the registry actions listed are included in the search definition. However, you can clear the **All Actions** option and select individual actions for auditing.

Select one or more of the following options:

- **All Actions** — include all the actions. When this option is selected, all the other options are disabled. (Default)
- **Add Value** — include when a new value is added to the selected registry key.
- **Delete Value** — include when a registry key value is removed.
- **Modify Value** — include when a registry key value is modified.
- **Add Key** — include when a new registry key is added.
- **Delete Key** — include when a registry key is removed.

4 When a scope option other than **All Registry Keys** is selected, the registry key hierarchy is enabled allowing you to locate and select an individual registry key.

Expand the hierarchy to locate and select a registry key. Then click **Add** to add it to the selection list box at the bottom of the dialog. Repeat to add more registry keys.

> **NOTE:** If you selected **Add With Events**, the registry key hierarchy pane is replaced with a data grid listing the registry keys that have an event associated with it in the database.

5 To replace a registry key in the selection list, select the 'new' registry key in the hierarchy, select the 'old' key in the selection list and click **Update**. The entry in the selection list is replaced with the 'new' registry key.

6 To select a registry key on a different computer, click **Browse** to the right of the **Path** field. On the Select a Directory Object dialog, use the Browse or Search pages to locate and select another computer.

If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.

7 Click **Select** to save your selection and close the dialog.

On the Add Registry Key dialog, the system registry keys associated with the specified computer will then be displayed in the hierarchy view.

NOTE: Select the **Exclude the Above Selection(s)** check box if you want to search for events in all registry keys except those listed in the 'what' list.

NOTE: Select the Runtime Prompt check box to prompt for a registry key every time the search runs. When this check box is checked, the data grid and buttons on this dialog are disabled.

You cannot enable alerting for search definitions that use the Runtime Prompt option.

8 Once you have selected the registry keys to include in the search, click **OK**.

When this search runs, Change Auditor searches for the selected events (actions) in the registry keys listed on the What tab.

To search for changes to services:

NOTE: Service auditing is only available when you have applied custom Service Auditing templates that define the services to audit. See Service Auditing for more information about capturing service events.

1 On the What tab, expand **Add** and select **Subsystem | Service**.

NOTE: You can use **Add with Events | Subsystem | Service** (instead of **Add | Subsystem | Service**) to select an entity that already has an event in the database.

2 On the Add Service dialog, select one or more services from the list at the top of the dialog and click **Add** to move them to the selection list box at the bottom of the page.

You can also click **Add All** to include all the listed services in the search definition.

3 To select services on a different computer, click **Browse** to the right of the **You are viewing services on** field. On the Select a Directory Object dialog, use the Browse or Search pages to locate and select another computer.

If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.

4 Click **Select** to save your selection and close the dialog.

On the Add Services dialog, the services found on the specified computer will then be displayed.

NOTE: Select the **Exclude the Above Selection(s)** check box if you want to search for events to all services except those listed in the 'what' list.

NOTE: Select the Runtime Prompt check box to prompt for a service every time the search runs. When this check box is checked, the data grid and buttons on this dialog are disabled.

You cannot enable alerting for search definitions that use the Runtime Prompt option.

5 Once you have selected the services to include in the search, click **OK**.

When this search is run, Change Auditor searches for change events to the services listed on the What tab.

TTo search for events based on severity:

1 On the What tab, expand **Add** and select **Severity**.

> **NOTE:** You can use **Add with Events | Severity** (instead of **Add | Severity**) to select a severity that already has an event associated with it in the database.

2 On the Add Severities dialog, select one or more severity levels and click **Add** to add them to the selection list box at the bottom of the dialog.

> **NOTE:** Select the **Exclude the Above Selection(s)** check box if you want to search for all events except those assigned a severity level that is listed in the 'what' list.

> **NOTE:** Select the **Runtime Prompt** check box on this dialog to prompt for a severity every time the search is run. When this check box is checked, the data grid and buttons on this dialog are disabled.

3 Once you have defined the severity levels to include in the search, click **OK**.

When this search is run, Change Auditor searches for events with the severity levels included on the What tab.

To search for events based on result:

1 On the What tab, expand **Add** and select **Result**.

> **NOTE:** You can use **Add with Events | Result** (instead of **Add | Result**) to select an entity that already has an event associated with it in the database.

2 On the Add Results dialog, select one or more results (none, success, protected or failed) and use **Add** to add them to the selected list box at the bottom of the dialog.

> **NOTE:** Select the **Exclude The Above Selection(s)** check box if you want to search for all events except those with the selected result.

> **NOTE:** Select the **Runtime Prompt** check box on this dialog to prompt for a result every time the search is run. When this check box is checked, the data grid and buttons on this dialog are disabled.

3 Once you have defined the results to include in the search, click **OK**.

When this search is run, Change Auditor searches for events with the results included on the What tab.

Where tab

The Where tab allows you to specify which agents to include (or exclude) in the search definition. You can select individual agents, all agents in a specific domain, or a given site. When multiple 'where' criteria is added to this tab, Change Auditor uses the 'OR' operator to evaluate change events, returning events captured by any of the specified agents, domains, or sites.

The Where tab contains the following information and controls:

Table 4. Where tab: Field and control descriptions

Field and Control	Description
Runtime Prompt	Select this check box to prompt for the 'where' criteria whenever the search is run. That is, when **Run** is selected, the Select Active Directory Objects dialog is displayed allowing you to locate and select the agents, domains, or sites to include in the search definition. **NOTE:** When this check box is checked, **Add** is deactivated. **NOTE:** You cannot enable alerting for search definitions that use the Runtime Prompt option.
Exclude the Following Selection(s)	Select this check box to specify the agents, domains, or sites to exclude from the search. That is, Change Auditor is to return events generated from all agents except those listed in the Where list.
Where list	By default, all agents are included in a new search and therefore this list box is initially empty. Once criteria is selected, this list box contains the agents, domains, sites, and server type (if specified) to include in the search (or exclude from the search if the **Exclude the Following Selection(s)** option is checked).

To search for events captured by a specific agent, domain or site:

NOTE: By default, all agents are included in a new search, therefore the list box on the Where tab is empty.

1. Open the Where tab and click **Add**.
2. Use the Browse or Search pages to locate and select an individual agent, a domain, or a site.

   NOTE: You can also select the Grid View option to select an agent from a list rather than using the Explorer View to locate it within your environment.

   If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.
3. Click **Add** to add your selection to the selection list box at the bottom of the page.

   NOTE: You can use **Add With Events** (instead of **Add**) to select an agent, domain, or site which already has an event associated with it in the database.
4. Once you have selected the agents, domains and sites to include in the search, click **OK**.

   The agents, domains and sites listed on the Where tab now defines where the search will be conducted when this search is run.

To use a wildcard expression to specify a domain, site or agent:

1. On the Where tab, expand **Add** and select **Add Wildcard Expression**.
2. Enter the wildcard expression to use to search for an agent (NetBIOS name), domain, or site:
   - Select the comparison operator to use: **Like** or **Not Like**.
   - In the field to the right, enter the pattern (character string and * wildcard character) to be used to search for a match. Use the * wildcard character to match any string of zero or more characters.

     For example, **LIKE *local** finds all agents with a NetBIOS name that ends in 'local'.
   - By default, the wildcard expression is used to search for an agent. To search for a domain or site, select the **Domain** or **Site** option.
3. After entering the wildcard expression to use, click **OK** to close the dialog and add the wildcard expression to the 'where' list.

4 When this search runs, Change Auditor searches for change events generated on the domains, sites, or agents whose name matches the specified wildcard expression.

To filter based on server type:

1 On the Where tab, expand **Add** and select **Add Server Types**.

2 Select to include Domain Controllers, Member Servers, Workstation Servers, Exchange Servers as required.

3 Click **OK** to close the dialog and add the server type to the 'Where' list.

When this search runs, Change Auditor searches for events generated on the specified domains, sites, or agents for the specified server type.

When tab

The When tab allows you to limit the returned results of the search by date and time. By default, a new search is set to include the change events captured this week. The When tab contains the following information and controls:

NOTE: All dates and times are based on the client's current local date and time. The format used to display the date and time is determined by the local computer's regional and language setting.

Table 5. When tab: Field and control descriptions

Field and Control	Description
Runtime Prompt	Select this check box to prompt for the date and time interval whenever the search is run. That is, when **Run** is selected, the When dialog is displayed allowing you to specify the date and time range to be used in your search. **NOTE:** When this check box is checked, **Add** is deactivated. **NOTE:** You cannot enable alerting for search definitions that use the Runtime Prompt option.
Date Interval	
Check one of the following options to change the default setting and define a different date range to limit your search.	
From/To	Select this check box and enter the date range. • **From**: Enter the start date for your date range; or click the arrow control to display a calendar from which to select the start date. Only events that occurred on or after this date are included in the search. • **To**: Enter the end date for your date range; or click the arrow control to display a calendar from which to select the end date. Only events that occurred before or on this date are included in the search.
Last	Select this check box and the appropriate relative date and value (that is, number of minutes, hours, days, weeks, months, quarters, or years). **NOTE:** Relative dates are calculated based on the actual date and time when the search is started.

Table 5. When tab: Field and control descriptions

Field and Control	Description
This	Select this check box and click the arrow control to select the appropriate date and time interval: • **This Day**: Start parameter is TODAY at midnight local time; end parameter is the current date and time. • **This Week**: Start parameter is midnight local time on the day specified in the First Day of Week parameter (Regional and Location setting) on the local machine (for example, SUNDAY); end parameter is the current date and time. (Default for new searches.) • **This Month**: Start parameter is the first day of the current month at midnight local time; end parameter is the current date and time.
Time Interval	
Use this pane to specify a time range to further limit your search.	
From	Use the arrow controls to select or enter the starting time for your time range. Only events that occurred at or after this time are included in the search.
To	Use the arrow controls to select or enter the ending time for your time range. Only events that occurred before or at this time are included in the search.
Reset	Use to clear the time interval settings.

To search for events generated during a specific date and time range:

NOTE: By default, new searches include the events captured this week (Sunday at midnight, local time, through the current date and time).

1. Open the When tab.
2. In the Date Interval pane, check one of the following options to specify a date range to limit your search:
   - **From/To** - select this option and enter the date range to use.
   - **Last** - select this option and the appropriate relative date and value (that is, number of minutes, hours, days, weeks, months, quarters, or years).
   - **This** - select this option and click the arrow control to select the appropriate time interval (that is, Day, Week, or Month).
3. In the Time Interval pane, optionally specify a time range to further limit your search.

Origin tab

The Origin tab allows you to search for events based on the workstation or server where the event originated. When multiple ‘origin’ criteria is specified on this tab, Change Auditor uses the ‘OR’ operator to evaluate change events, returning events that originated from any of the specified workstations or servers.

The Origin tab contains the following information and controls:

Table 6. Origin tab: Field and control descriptions

Field and Control	Description
Runtime Prompt	Select this check box to prompt for the originating workstation or server whenever the search is run. That is, when **Run** is selected, the Add Origin dialog is displayed allowing you to enter the wildcard expression to locate a specific workstation or server. **NOTE:** When this check box is checked, **Add** is deactivated. **NOTE:** You cannot enable alerting for search definitions that use the Runtime Prompt option.
Exclude the Following Selection(s)	Select this check box to specify the workstations or servers to exclude from the search. That is, Change Auditor will return events originating from all workstations and servers except those listed in the Origin list.
Origin list	By default, all events regardless of where they originated are included in a new search and therefore this list box is initially empty. Once criteria is selected, this list box contains the wildcard expression used to locate the workstations and servers to include in the search (or excluded from the search if the **Exclude the Following Selection(s)** option is checked).

To search for events based on where they originated:

NOTE: By default, all events regardless of the workstation or server from which it originated are included in the search.

1. Open the Origin tab.
2. Click **Add**.
3. Enter the wildcard expression to use to search for a workstation or server, based on its NetBIOS name or IP address:
   - Select the comparison operator to use: **Like** or **Not Like**.
   - In the field to the right, enter the pattern (character string and * wildcard character) to be used to search for a match. Use the * wildcard character to match any string of zero or more characters.
4. After entering the wildcard expression to use, click **OK** to close the dialog and add the wildcard expression to the 'origin' list.
5. When this search is run, Change Auditor searches for change events originating on workstations and servers whose name or IP address matches the specified wildcard expression.

NOTE: You can use **Add with Events** (instead of **Add**) to select a workstation or server that already has an event associated with it in the database. The workstations and servers available for selection are based on the 'when' clause (When tab) and the search limit (Info tab) specified for the current search.

Alert tab

The Alert tab allows you to enable alerting and define how and where to dispatch alerts. See Alert tab (Search Properties tabs) for a detailed description of the contents of this tab.

Report tab

The Report tab allows you to enable reporting and define when and where to send a report. Reports can be sent to email addresses and shared folders. See Report tab (Search Properties tabs) for a detailed description of the contents of this tab.

Layout tab

NOTE: In previous versions of Change Auditor, this tab was referred to as the Advanced tab.

Using the Layout tab, you can define the data (columns) to be retrieved from the database and displayed for the selected search. You can also define the column order, sort criteria and order, groupings and the format to use for displaying the retrieved data. The layout defined on this tab is used for both displaying the search results in the client and for the report layout when reporting is enabled on the Report tab.

The Layout tab contains the following information and controls:

Table 7. Layout tab: Table and Control descriptions

Table	Description
Unselected Columns	Displays the event details that can be retrieved from the database.
Selected Columns	Displays the event details that are being retrieved from the database. It also displays the order in which the columns will be presented, that is, the top entry will be the left-most column in the search results grid/report. To add and remove columns from this table, use the buttons to the left of the table: • Right arrow adds the column selected in the Unselected Columns table to the Selected Columns table. • Left arrow removes the column selected in the Selected Columns table, moving it back to the Unselected Columns table. To rearrange or sort the columns for display, use the buttons to the right of the table: • Up arrow moves the selected column up in the list. • Down arrow moves the selected column down in the list. • Right arrow adds the selected column to the Sort Criteria table. This column is placed after the column selected in the Sort Criteria table. • Left arrow removes the column selected in the Sort Criteria table from the sort criteria. • Arrow in a square resets the Selected Columns table back to the factory defaults.
Sort Criteria	Defines the criteria to use to sort the search results, including: • **Order By** — specifies the columns to use to sort the data. The primary sort criteria is listed first. • **Direction** — specifies whether to present the data in descending or ascending order • **Group By** — indicates whether to also use the column to group the data To rearrange the sort criteria, use the buttons to the right of the table: • Up arrow moves the selected column up in the list. • Down arrow moves the selected column down in the list. • Arrow in a square resets the Sort Criteria and Display Results tables back to the factory defaults.
Search Results	Specifies the format to use dto display the search results on the Search Results page. When a grouping is defined, select one of the following options: • In a Grid (default) • As a Pie Chart • As a Bar Graph **NOTE:** These options are only available when a single level of grouping is defined (that is, only one column contains a **Yes** in the **Group By** column of the Sort Criteria table). **NOTE:** The options in this table apply only to the search results in the client; they do not apply to reports.

To customize what is displayed for the selected search:

1 Open the Layout tab.

2 Review the columns listed in the Selected Columns table (second table from the left) to determine if it contains the information you want to display for the selected search.

3 To add a column, select the column from the Unselected Columns table and click the right arrow button (located between the first two tables) to move it to the Selected Columns table.

You can also 'drag' a column to the Selected Columns table.

4 To remove a column from display, select the column from the Selected Columns table and click the left arrow button (located between the first two tables) to move it back to the Unselected Columns table.

You can also 'drag' a column back to the Unselected Columns table.

5 The Selected Columns table also displays the order the columns will be presented. To rearrange the columns, in the Selected Columns table select the column to be moved and click the up or down arrow button (located to the right of the Selected Columns table) to move the selected column to the desired location. The top entry will be the left-most column in your display or report.

You can also 'drag' columns in this table to define the order.

NOTE: To reset the column selection and arrangements in the Selected Columns table back to the factory defaults, click the restore button located next to the lower right-hand corner of this table.

6 The Sort Criteria table (third table) defines the order to use to sort the search results. To define the sort criteria for your search results, select a column in the Selected Columns table and click the right arrow button (located to the right of the Selected Columns table) to move it to the Sort Criteria table.

To specify secondary sort criteria, add the additional column to the Sort Criteria table. Use the arrow controls to the right of the Sort Criteria table to define the primary (first column in list) and subsequent sort criteria.

You can also 'drag' columns between the Selected Columns and Sort Criteria tables and within the Sort Criteria table to define the sort criteria.

7 To change the direction, ascending or descending, select a column in the Sort Criteria table, click in the **Direction** cell, and select either ascending (ASC) or descending (DESC) from the drop-down menu.

8 In addition, you can use the **Group By** column to define groupings. To group the selected search's results, select the column to use for the grouping, click in the **Group By** cell and select **Yes** from the drop-down menu.

9 When a single level of grouping is defined (only one column contains a **Yes** in the **Group By** column of the Sort Criteria table), you can select one of the following options in the Display Results table to define the display format to use for the selected search:

- In a Grid (default)
- As a Pie Chart
- As a Bar Graph

NOTE: The settings in the Search Results table do not apply to reports.

NOTE: To reset the settings in the Sort Criteria table and Search Results table back to the default settings, click the restore button located next to the lower right-hand corner of the Sort Criteria table.

10 Click one of the following commands to save your selections:

- Save
- Save As | Save As
- Save As | Save As Default

NOTE: You can also use **Preview Changes** to rerun the query to preview the changes you have made without saving them.

SQL tab

The SQL tab displays the SQL query built to run the selected search. This information is only available after a search has been created.

NOTE: The SQL tab is hidden by default. To display the SQL tab, select **Action | Show SQL Tab**.

To copy the SQL query:

1 Select the text and click **Copy**.

NOTE: To copy the entire SQL query, click before the first word in the query, use the scroll bar to scroll to the end of the query text, and Shift + click after the last word in the query to select all the query statements.

2 Open the application (for example, Notepad) where you want to paste the content, right-click and select **Paste**.

XML tab

The XML tab displays the XML representation of the search criteria. This same information can be exported by right-clicking a search in the Searches list on the Searches page and selecting **Export**.

NOTE: The XML tab is hidden by default. To display the XML tab, use the **Action | Show XML Tab** menu command.

To copy the XML code:

1 Select the required text and click **Copy**.

NOTE: To copy the entire XML code, click before the first character in the XML file, use the scroll bar to scroll to the end of the text, and Shift + click after the last word in the file to select all the XML statements in the file.

2 Open the application (for example, Notepad) where you want to paste the content, right-click and select **Paste**.

8

Enable Alert Notifications

- Introduction
- Alert tab (Search Properties tabs)
- Enable alerts
- Disable alerts
- Alert History page
- View alert history

Introduction

Change Auditor can generate alerts when certain kinds of configuration changes occur. These alerts appear in the client and are then dispatched to designated recipients through email, SNMP or WMI events.

NOTE: You cannot enable alerting for search definitions that use the Runtime Prompt option.

NOTE: Email, SNMP and/or WMI must be configured to receive alerts before any alert notifications will be sent.

Smart Alert Technology provides intelligent event correlation by notifying you when event patterns cause potential security risks. You can customize the Smart Alerts to match your security policies. For example, if a privileged account is attempting to log on with a bad password at multiple computers within a predetermined time period, a proactive alert can be generated.

This section provides a description of the Alert tab and instructions on how to enable and disable alert notifications. It also provides a description of the Alert History page and instructions for viewing and deleting the alert history. For a description of the other dialogs mentioned in this chapter, refer to the online help.

Alert tab (Search Properties tabs)

The Alert tab displays the current alert configuration for the selected search definition. From the Alert tab, you can enable/disable an alert notification for the selected search definition, define how and where to dispatch the alert (through email, SNMP, or WMI), and modify the alert configuration settings.

Use the controls on the Alert tab as described below.

Table 1. Alert tab: Field/Control descriptions

Field/Control	Description
Alert Enabled	Select the **Alert Enabled** check box to enable an alert for the current search definition. This option will became available only after one of the transport methods are selected in the **Send Alert To** setting on this tab.
Alert Configuration pane	

Table 1. Alert tab: Field/Control descriptions

Field/Control	Description
Send Alert To	Select all of the transport options that are to be applied to this search definition: • **SNMP** - Select this option to dispatch alerts for this search definition via SNMP traps. • **WMI** - Select this option to dispatch alerts for this search definition via WMI (Windows Management Instrumentation) events. • **Email** - Select this option to dispatch alerts for this search definition via email. Selecting this option will display the Alert Custom Email dialog allowing you to specify the email address of the persons who are to receive the email notification.
History Search Limit	By default, up to 50,000 events can be included in the alert history. Use the arrow controls to increase or decrease this value to define the maximum number of events to be included in the alert history. **NOTE:** The **History Search Limit** setting is a global setting and changes made to this setting will be applied to ALL alerts.
Configure Email	For email alerts, click **Configure Email** to change the details about the alert email to be sent, including the To address, the Reply To address, and the Subject Line. In addition, from the Alert Custom Email dialog you can access the Alert Body Configuration dialog to configure the body of the email alert. **NOTE:** If email is not configured, a message box appears stating that the Coordinator email configuration has not been configured. Open the Administration Tasks tab and use the Coordinator Configuration page to enable email notification and configure mail.
Events Per Email	For email alerts, a maximum of 100 events will be included in a single alert email by default. Use the arrow controls to increase or decrease this value to define the maximum number of events to be included in an email.
Time zone	For email alerts, use this field to specify the time zone to be used for the time stamp in the name of the report attachment. By default, the time zone of the computer where the Change Auditor client resides is used.
Smart Alert pane	
Smart Alert Enabled	Select this check box to specify under what conditions an alert is to be sent. This feature is only available for email and SNMP notifications.
Send Alert When <*nn*> Events Occur Within <*nn*> <*interval*>	Select this option to specify the number of events that must occur within a specified time interval before generating/dispatching the alert. Where: <*interval*> is one of the following: minutes, hours or days
On A Single Object	Select this check box to specify that the event must occur for the same object the specified number of times before the alert will be triggered. When this check box is cleared (default), the event can occur on any object the specified number of times to trigger the alert. **NOTE:** Smart alerts on a single object are only supported for Active Directory and File System subsystems.

Enable alerts

Using the Searches page, you can enable/disable alert notifications for individual search definitions and dispatch them through email, SNMP or WMI.

NOTE: The right-click commands available for enabling/disabling alert notifications are available when multiple search definitions are selected. However, you can only enable/disable alert notifications using the Alert tab when a single search definition is selected.

To enable email alerts for individual search definitions:

NOTE: To dispatch configuration change alerts through email you must first enable email notification and define the email server to be used on the Coordinator Configuration page. See Click Test Mail to test the configuration. in the Coordinator Configuration chapter.

1 Open the Searches page.

2 Expand the **Private** or **Shared** folders in the explorer view to locate the search to which an alert is to be associated. Select the search from the Search list in the right-hand pane.

3 Use one of the following methods to enable an alert:

- Right-click the search and select the **Alert | Enable Transport | Email** command.
- Open the Alert tab and select the **Email** check box and then the **Alert Enabled** check box. (If the Search Properties tabs are not being displayed, right-click the search definition and select **Show Properties**).

NOTE: If email is not configured, a message box will display stating that the coordinator email configuration has not been configured. Open the Administration Tasks tab and use the Coordinator Configuration page to configure email alerts.

4 Using either of these methods displays the Alert Custom Email dialog allowing you to enter the email address of the persons who are to receive the alert notification.

Enter the email address or click the browse button to specify the users who are to receive the alert notification. Selecting the browse button displays one of the following dialogs:

- The Select Active Directory Objects dialog (directory object picker) where you can use the Browse or Search page to locate Active Directory users. This dialog is displayed when no Exchange host is specified in the Email Alerts Configuration pane of the Coordinator Configuration page.
- The Search Users dialog allowing you to locate and select an Exchange user (Exchange tab) or an Active Directory user (Active Directory tab). This dialog is displayed when an Exchange host is defined in the Email Alerts Configuration pane of the Coordinator Configuration page.

NOTE: You can enter an individual email address or distribution list address in the **To, Cc** or **Bcc** fields. You can also send the alert notification to additional recipients by selecting the appropriate check box, as described below:

- **Add Who** - Select this check box to send an alert to the user who initiated the change that triggered the alert.
- **Add Users** - When selected, alerts for user object changes are sent to the user; alerts for mailbox objects are sent to the mailbox owner.
- **Add Managers** - When selected, alerts for user object changes are sent to the user manager (if set); alerts for group objects are sent to the managed-by user (if set). Alerts for mailbox objects are sent to the owner's manager (if set).

Once a check box is selected, select the corresponding option to add it to the **To**, **Cc** or **Bcc** field.

By default, the values entered on the Email Alerts Configuration pane of the Coordinator Configuration page will be used for the following fields/settings:

- Reply To address
- Subject line
- email format (Plain Text or HTML)
- body of the email alert

If you do not want to use these default settings for the current search query, you can modify them on the Alert Custom Email dialog. To modify the body of the email alert, click **Configure Body**.

Once you have finished specifying the recipient email addresses, click **OK** to save your selections and close the dialog.

5 In addition, you can change the following alert configuration settings using the Alert tab (Search Properties tabs):

- By default, up to 50,000 events will be included in the alert history. Use the **History Search Limit** setting to change this value. (This setting is a global setting and changes made to this setting will be applied to ALL alerts.)
- By default, a maximum of 100 events will be included in a single alert email. Use the **Events Per Email** setting to change this number.
- By default the time zone of the computer where the Change Auditor client resides is used for an alert's date/time stamps in the email. To change the time zone to be used for these date/time stamps, select the time zone from the drop-down list.
- If you want to specify under what conditions an alert is to be sent, select the **Smart Alert Enabled** check box and specify the number of events that must occur within a specified time interval before generating/dispatching the alert.

  By default, a smart alert is generated when the event occurs on any object the specified number of times. You can however, select the **On a Single Object** option to have the smart alert triggered when the event occurs on the same object the specified number of times.

NOTE: If using the Alert tab, be sure to click **Save** to save the alert definition.

6 When an alert is enabled, the following indicators are added to the Searches list:

- **Type** - the icon for the search (magnifying glass) changes to a check mark and the label changes from 'Search' to 'Alert' (e.g., Shared Alert)
- **Alert** - displays 'Enabled'
- **Alert To** - displays the email address of any users who are to receive the alert email
- **Alert Cc** - if specified, displays the email address of any users who are to receive a copy of the alert email
- **Alert Bcc** - if specified, displays the email address of any users who are to receive a blind copy of the alert email

To enable SNMP alerts for individual search definitions:

NOTE: In order to generate SNMP alerts, SNMP must be installed and the trap receiver must be started.

1 Open the Searches page.

2 Expand the **Private** and **Shared** folders in the explorer view to locate the search to which an alert is to be associated. Select the search from the Search list in the right-hand pane.

3 Use one of the following methods to enable an alert:

- Right-click the search and select **Alert | Enable Transport | Email**.
- Open the Alert tab at the bottom of the page, select the **Email** check box, then the **Alert Enabled** check box. (If the Search Properties tabs are not being displayed, right-click the alert definition and select **Show Properties**).

4 In addition, you can change the following alert configuration settings using the Alert tab (Search Properties tabs):

- By default, up to 50,000 events will be included in the alert history. Use the **History Search Limit** setting to change this value. (This setting is a global setting and changes made to this setting will be applied to ALL alerts.)

NOTE: If using the Alert tab, be sure to click **Save** to save the alert definition.

5 When an alert is enabled, the following indicators are added to the Searches list:

- **Type** - the icon for the search (magnifying glass) changes to a check mark and the label changes from 'Search' to 'Alert' (e.g., Shared Alert)
- **Alert** - displays 'Enabled'

To enable WMI alerts for individual search definitions:

NOTE: In order to generate WMI alerts, WMI must be installed and started. A WMI event consumer must also be running on the coordinator server.

1. Open the Searches page.
2. Expand the **Private** and **Shared** folders in the explorer view to locate the search to which an alert is to be associated. Select the search from the Search list in the right-hand pane.
3. Use one of the following methods to enable an alert:
   - Right-click the search and select the **Alert | Enable Transport | WMI** command.
   - On the Alert tab, select the **WMI** check box and then the **Alert Enabled** check box. (If the Search Properties tabs are not being displayed, right-click the alert definition and select the **Show Properties** menu command).
4. In addition, you can change the following alert configuration setting using the Alert tab (Search Properties tabs):
   - By default, up to 50,000 events will be included in the alert history. Use the **History Search Limit** setting to change this value. (This setting is a global setting and changes made to this setting will be applied to ALL alerts.)

   NOTE: If using the Alert tab, be sure to click **Save** to save the alert definition.
5. When an alert is enabled, the following indicators are added to the Searches list:
   - **Type** - the icon for the search (magnifying glass) changes to a check mark and the label changes from 'Search' to 'Alert' (e.g., Shared Alert)
   - **Alert** - displays 'Enabled'

Disable alerts

NOTE: The right-click commands available for enabling/disabling alert notifications are available when multiple search definitions are selected. However, you can only enable/disable alert notifications using the Alert tab when a single search definition is selected.

To disable alerts:

1. Open the Searches page.
2. Expand the **Private** and **Shared** folders in the explorer view to locate the alert-enabled search to be disabled. Select the alert from the Search list box in the right-hand pane.
3. Use one of the following methods to disable an alert:
   - Right-click the alert and select **Alert | Disable Alert**. A message box is displayed asking you to confirm that you want to disable the alert. Click **Yes**.
   - Open the Alert tab, clear the **Alert Enabled** check box. (If the Search Properties tabs are not being displayed, right-click the alert definition and select the **Show Properties** menu command.)

   NOTE: If using the Alert tab, click the **Save** button to apply the change.
4. When the alert is disabled, the **Alert** column displays 'Disabled'.

In addition to disabling an alert, you can also disable the alerting transports for an alert-enabled search.

To disable email alerts for individual search definition:

1 Open the Searches page.

2 Expand the **Private** and **Shared** folders in the explorer view to locate the alert-enabled search to be disabled. Select the alert from the Search list in the right-hand pane.

3 Use one of the following methods to disable an alert:

- Right-click the alert and select **Alert | Disable Transport | Email**. A message box will be displayed asking you to confirm that you want to disable the alert. Click **Yes**.
- Open the Alert tab, clear the **Email** check box and the **Alert Enabled** check box. (If the Search Properties tabs are not being displayed, right-click the alert definition and select the **Show Properties** menu command.)

NOTE: If using the Alert tab, click **Save** to apply the change.

If this is the only transport or when all transports are disabled, the definition returns to a 'Search' type.

To disable SNMP alerts for individual search definition:

1 Open the Searches page.

2 Expand the **Private** and **Shared** folders in the explorer view to locate the alert-enabled search to be disabled. Select the alert from the Search list in the right-hand pane.

3 Use one of the following methods to disable an alert:

- Right-click the alert and select **Alert | Disable Transport | SNMP**. A message box will be displayed asking you to confirm that you want to disable the alert. Click **Yes**.
- Open the Alert tab, clear the **SNMP** check box and the **Alert Enabled** check box. (If the Search Properties tabs are not being displayed, right-click the alert definition and select **Show Properties**.)

NOTE: If using the Alert tab, click **Save** to apply the change.

If this is the only transport or when all transports are disabled, the definition returns to a 'Search' type.

To disable WMI alerts for individual search definition:

1 Open the Searches page.

2 Expand the **Private** and **Shared** folders in the explorer view to locate the alert-enabled search to be disabled. Select the alert from the Search list in the right-hand pane.

3 Use one of the following methods to disable an alert:

- Right-click the alert and select **Alert | Disable Transport | WMI**. A message box will be displayed asking you to confirm that you want to disable the alert. Click **Yes**.
- Open the Alert tab, clear the **WMI** check box and the **Alert Enabled** check box. (If the Search Properties tabs are not being displayed, right-click the alert definition and select the **Show Properties** menu command.)

NOTE: If using the Alert tab, click **Save** to apply the change.

If this is the only transport or when all transports are disabled, the definition returns to a 'Search' type.

Alert History page

The Alert History page is accessed by selecting an alert enabled search, right-clicking and selecting **Alert | History**. This page displays details regarding the events that triggered the selected alert, including the time the

alert was triggered, if the alert was successfully sent, a description of the event that triggered the alert and, if applicable, an error message stating the alert was not sent.

NOTE: Regardless of the alert state (enabled or disabled) the alert history for an alert-enabled search is always available until it is removed using **Alert | Delete History**.

The data grid on this page contains the following information for each event that triggered an alert:

Table 2. Alert History page: Field descriptions

Column	Description
Time Alerted	Displays the time the alert occurred.
Alert Type	Displays 'Email, SNMP, or WMI' for the type of alert that was generated.
Alerted	Indicates whether the alert was successfully sent: Yes or No.
Description	Displays a description of the events that caused this alert to be triggered.
Message	Displays an error message if the alert was not successfully sent.

View alert history

For each enabled alert, two additional context menu commands become available whenever you right-click an alert-enabled search definition on the Searches page: **Alert | History** and **Alert | Delete History**.

NOTE: The **Alert | History** and **Alert | Delete History** right-click commands are available for any search that has ever had an alert enabled in the current product version, regardless of its current state. These commands are not available for disabled alerts, only after the alert history has been deleted using **Alert | Delete History**.

To view the alerts triggered for a search:

1 On the Searches page, select an alert-enabled search definition, right-click, expand the **Alert** command and select **History**.

This opens a new Alert History page, which displays details regarding the alerts triggered for the selected search.

To delete alert history:

1 On the Searches page, select an alert-enabled search, right-click, expand the **Alert** command and select e **Delete History**.

This clears the alert history for the selected alert.

NOTE: Change Auditor deletes alerts in batches of 1000, so the alert history will not be immediately cleared; however, refreshing the screen will show the number of alerts decreasing.

View event details or alert properties

From an Alert History page, you can view the alert properties (Alert tab) used to generate the displayed alerts or access more detailed information about an individual alert. Using the tool bar buttons at the top of an Alert History page, you can easily switch between the Alert tab and Event Details pane.

To display event details for an alert:

1 Open an Alert History page and select an alert from the grid.

2 If neither the Alert tab or Event Details pane are being displayed (or the Alert tab is displayed), use one of the following methods to display the event details:

- double-click the alert entry in the results grid
- click the **Event Details** tool bar button
- right-click the alert and select **Event Details**

3 To hide the Event Details pane, use the hide button in the upper right corner of the Event Details pane.

To display the alert properties for an alert:

1 Open an Alert History page and select an alert from the grid.

2 If neither the Alert tab or Event Details pane are being displayed (or the Event Details pane is displayed), use one of the following methods to display the search properties:

- click the **Alert Properties** tool bar button
- right-click the alert and select **Alert Properties**

3 To hide the Alert tab, use the hide button in the upper right corner.

9

Administration Tasks

- Administration Tasks tab
- Administration Task lists
- Export/import Administration Task settings

Administration Tasks tab

The Administration Tasks tab allows you to perform various administration tasks based on the Change Auditor licenses that are applied. Use the **View | Administration** menu command to display the Administration Tasks tab, which consists of a navigation pane to the left and information pages to the right.

NOTE: Authorization to use the administration tasks on the Administration Tasks tab is defined using the Application User Interface page. Members of the ChangeAuditor Administrators security group have full administrative privileges with access to all aspects of the client. Members of the ChangeAuditor Operators security group only have limited access to the client and therefore, do not have access the Administration Tasks tab. For more information about assigning users and groups authorization to this tab, see Change Auditor User Interface Authorization.

The Administration Tasks tab navigation pane is divided into different task lists: Configuration, Auditing, and Protection. Click a task button from the bottom of the navigation pane to display a task list. Then select a task from the displayed task list to display the appropriate information page, from which you can perform the corresponding administrative task.

Administration Task lists

The following table lists the navigation pane's task lists and a description of the administrative tasks that you can perform. Many of the tasks listed require a specific license, which is indicated by the following codes in the last column of the table:

- Any - does not require a specific license; available with any license
- CAAD - Change Auditor for Active Directory
- CAEX - Change Auditor for Exchange
- CAFS - Change Auditor for Windows File Servers
- CASQL - Change Auditor for SQL Server
- CAAD-Q - Change Auditor for Active Directory Queries
- CAEMC - Change Auditor for EMC
- CANA - Change Auditor for NetApp

- CASP - Change Auditor for SharePoint

NOTE: You are not prevented from performing any of the administration tasks on the Administration Tasks tab; however, associated events are not captured and associated protection does not occur unless the proper license is applied.

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

For more information on how to perform an administrative task or a description of the page that is displayed, refer to the appropriate Change Auditor user guide.

Table 1. Administration Task tab: Task descriptions

Task List/Task	Description	License
Configuration: The following tasks are available in the Configuration task list**:**		
Agent	Define and assign agent configurations. For more information, see Agent Configurations.	Any
Coordinator	Enable email alert notifications/reports, configure email server to be used for alerting/reporting, configure the ability to send reports to a shared folder, define group membership expansion, modify agent heartbeat check interval, and select which coordinators will process scheduled reports, purge, and archive jobs. For more information, see Coordinator Configuration.	Any
Purge and Archive Jobs	Define and schedule purge jobs for deleting events from the production database. Define and schedule archive jobs to create a yearly archive database for older events that are no longer required to be represented in your reports. For more information, see Purging and Archiving your Change Auditor Database.	Any
Private Alerts and Reports	View and manage all private search queries where alerting and/or reporting has been enabled. Move and delete private searches as needed. For more information, see Working with Private Alerts and Reports and Move and delete private searches.	Any
SQL Reporting Services	Define SQL Reporting Services (SRS) templates that define all the necessary Report Server information (URL and credentials) and Change Auditor data source information for publishing reports. These templates can then be made available to users who choose to publish Change Auditor reports to SRS. For more information, see SQL Reporting Services Configuration.	Any
Report Layouts	Define report layout templates which contain the header/footer information to be used in reports. For more information, see Generate and Schedule Reports.	Any
Application User Interface	Define who is authorized to use the various Change Auditor client features. In addition, you can define who is authorized to view the Active Directory and Group Policy protection tasks in Change Auditor. For more information, see Change Auditor User Interface Authorization.	Any
Client Authentication	Specify the authentication method that all clients will use to access Change Auditor. There are two methods available - Windows Forms or Active Directory Client Certificate authentication. For more information, see Client Authentication.	Any

Table 1. Administration Task tab: Task descriptions

Task List/Task	Description	License
Event Subscriptions	Configure and manage a Splunk integration. You can add, edit, delete, and view event subscriptions. For more information see the Change Auditor SIEM Integration Guide.	Any
Auditing: The Auditing task list is divided into separate lists that identify configuration tasks, forest-level tasks that are globally applied, tasks that define auditing for different applications, server-level tasks that must be assigned to an agent configuration, and tasks that define NAS device auditing.		
Configuration: Use the tasks under this heading to configure the audit events to be captured by Change Auditor and to define accounts that are to be included and excluded from auditing.		
Audit Events	Enable/disable event auditing and modify an event's severity level or description. For more information, see Enable/Disable Event Auditing.	Any
Excluded Accounts	Create Excluded Accounts templates to define individual accounts that are to be excluded from Change Auditor auditing. For more information, see Account Exclusion.	Any
Forest: Use the tasks under this heading to define custom auditing definitions for your Active Directory forest.		
Active Directory	Define custom Active Directory object class auditing. For more information, see the Quest Change Auditor For Active Directory User Guide.	CAAD
Attributes	Define custom Active Directory attribute auditing. For more information, see the Quest Change Auditor for Active Directory User Guide.	CAAD
Member of Group	Define a Member of Group auditing list to specify the users to be audited based on their group membership. For more information, see the Quest Change Auditor for Active Directory User Guide.	CAAD
AD Query	Define the Active Directory containers that are to be included and excluded from AD query auditing. For more information, see the Quest Change Auditor for Active Directory Queries User Guide.	CAAD-Q
Active Directory Federation Services	Define Active Directory Federation Services auditing. For more information, see the Quest Change Auditor For Active Directory User Guide.	CALA
Active Directory Database	Define the Active Directory database auditing. For more information, see the Quest Change Auditor For Active Directory User Guide.	CAAD
ADAM (AD LDS)	Define custom ADAM (AD LDS) object auditing. For more information, see the Quest Change Auditor for Active Directory User Guide.	CAAD
Attributes	Define custom ADAM (AD LDS) attribute auditing. For more information, see the Quest Change Auditor for Active Directory User Guide.	CAAD
Applications: Use the tasks under this heading to define auditing for different types of applications within your environment.		
Exchange Mailbox	Define an Exchange Mailbox auditing list to specify which directory object's mailbox activities are to be audited by Change Auditor for Exchange. For more information, see the Quest Change Auditor for Exchange User Guide.	CAEX

Table 1. Administration Task tab: Task descriptions

Task List/Task	Description	License
Microsoft 365	Specify the Microsoft 365 service and Exchange Online mailboxes that are to be audited by Change Auditor for Exchange and Change Auditor for SharePoint. For more information, see the Microsoft 365 and Microsoft Entra ID Auditing User Guide.	CAEX CASP
SQL **SQL Server** **SQL Data Level**	Create SQL Auditing templates to define the SQL instances and operations that are to be audited. Create SQL Data Level Auditing templates to define the operations that are to be audited. For more information, see the Quest Change Auditor for SQL Server User Guide.	CASQL
SharePoint	Create SharePoint Auditing templates to define the SharePoint farm to be audited and the Change Auditor agent to be used to audit this farm. For more information, see the Quest Change Auditor for SharePoint User Guide.	CASP
Server: Use the tasks under this heading to create auditing templates that can then be assigned to agent configurations to enable custom server-level auditing.		
File System	Create File System Auditing templates to define the files/folders that are to be audited. For more information, see the Quest Change Auditor for Windows File Servers User Guide.	CAFS
Registry	Create Registry Auditing templates to define the registry keys and events that are to be audited. For more information, see Registry Auditing.	Any
Services	Create Service Auditing templates to specify the system services that are to be audited. For more information, see Service Auditing.	Any
NAS: Use the tasks under this heading to create auditing templates for NAS devices. For more information, see the Quest Change Auditor for NetApp User Guide and the Quest Change Auditor for EMC User Guide.		
EMC	Create a separate EMC Auditing template for each CIFS file access protocol to be audited by Change Auditor, defining the EMC file server (CIFS), auditing scope and Change Auditor agents that are to receive the EMC audit events.	CAEMC
NetApp	Create a separate NetApp Auditing template for each NetApp filer to be audited by Change Auditor, defining the location of the NetApp filer, the auditing scope, and the Change Auditor agents that are to receive the NetApp filer audit events.	CANA
Protection: The Protection task list is divided into separate task lists as well: one for forest-level tasks that are globally applied, one for tasks that define protection for applications, and another for server-level tasks that must be assigned to an agent configuration. To use Active Directory Protection templates, you must be logged in to Change Auditor with an account with Enterprise Admin privileges.		
Forest: Use the tasks under this heading to define global protection definitions for your Active Directory forest. For more information, see the Quest Change Auditor for Active Directory User Guide.		

Table 1. Administration Task tab: Task descriptions

Task List/Task	Description	License
Active Directory	Create Active Directory Protection templates to define critical Active Directory objects that are to be protected against unauthorized modifications. **NOTE:** If you have Quest GPOADmin integrated with your Change Auditor deployment, the GPOADmin service account is exempt from protection. **NOTE:** A protected GPO can only be changed by override accounts that are excluded from protection.	CAAD
ADAM (AD LDS)	Create ADAM (AD LDS) Protection templates to define critical ADAM objects that are to be protected against unauthorized modifications.	CAAD
Group Policy	Create Group Policy Protection templates to define critical Group Policy objects that are to be protected against unauthorized modifications.	CAAD
Active Directory Database	Create Active Directory Database Protection templates to prevent copying and other tampering attempts on the Active Directory database (NTDS.dit) file. Extraction of this file could lead to parsing of usernames and passwords resulting in a security breach.	CAAD
Applications: Use the task under this heading to define global protection for your Exchange Mailbox application. For more information, see the Quest Change Auditor for Exchange User Guide.		
Exchange Mailbox	Create Exchange Mailbox Protection templates to define critical Exchange Mailboxes that are to be protected against unauthorized modifications.	CAEX
Server Use the task under this heading to create protection templates that can then be assigned to agent configurations to enable server-level protection. For more information, see the Quest Change Auditor for Windows File Servers User Guide.		
File System	Create File System Protection templates to define critical files/folders that are to be protected against unauthorized modifications.	CAFS

Export/import Administration Task settings

Using the **Export** and **Import** commands on the **Action** menu, you can export/ import the settings defined on the various Administration Tasks tabs. Selecting one of these commands allows you to select the configuration, auditing and protection settings to be exported/imported.

To export Administration Task settings:

1 Open the Administration Tasks tab and click **Action | Export**.

2 Select the configuration, auditing and protection settings to be exported:

Table 2. Export dialog settings

Configuration	
NOTE: By default, all settings except for the Coordinator Configuration and Application User Interface settings are selected for export. When imported, these configuration settings overwrite any existing settings that may be present.	
Agent	Select to export all agent configurations including the settings and auditing and protection template assignments. When selected, the auditing and protection templates that must be assigned to agent configurations are selected by default, and cannot be cleared.
Coordinator	Select to export the coordinator configuration settings. This option is not selected by default.
Application User Interface	Select to export Change Auditor client feature authorizations. This option is not selected by default.
Report Layouts	Select to export any Report Layout templates.
Purge Jobs	Select to export any scheduled purge jobs.
Auditing	
Audit Events	Select to export the audit event settings, such as enabled/disabled events, event severity and descriptions.
Excluded Accounts	Select to export any Excluded Accounts templates. **NOTE:** When the **Agent** option is selected in the Configuration section of this dialog, this option is also selected and cannot be cleared. This is because this type of template must be assigned to an agent configuration in order to work properly.
Active Directory	Select to export any custom Active Directory auditing definitions.
Active Directory | Attributes	Select to export any custom Active Directory attribute auditing definitions.
Active Directory | Member Of Group	Select to export the contents of the Member of Group list.
Active Directory | AD Query	Select to export the contents of the AD Query list.
ADAM (AD LDS)	Select to export any ADAM (AD LDS) auditing definitions.
ADAM (AD LDS) | Attributes	Select to export any ADAM (AD LDS) attribute auditing definitions.
Microsoft 365	Select to export the Microsoft 365 Exchange Online mailbox auditing list.
Exchange Mailbox	Select to export the Exchange mailbox auditing list.
SQL	Select to export any SQL auditing templates. **NOTE:** When the **Agent** option is selected in the Configuration section of this dialog, this option is also selected and cannot be cleared. This is because this type of template must be assigned to an agent configuration in order to work properly.
SharePoint	Select to export any SharePoint auditing templates.

Table 2. Export dialog settings

File System	Select to export any File System auditing templates. **NOTE:** When the **Agent** option is selected in the Configuration section of this dialog, this option is also selected and cannot be cleared. This is because this type of template must be assigned to an agent configuration in order to work properly.
Registry	Select to export any Registry auditing templates. **NOTE:** When the **Agent** option is selected in the Configuration section of this dialog, this option is also selected and cannot be cleared. This is because this type of template must be assigned to an agent configuration in order to work properly.
Services	Select to export any Service auditing templates. **NOTE:** When the **Agent** option is selected in the Configuration section of this dialog, this option is also selected and cannot be cleared. This is because this type of template must be assigned to an agent configuration in order to work properly.
EMC	Select to export any EMC auditing templates.
NetApp	Select to export any NetApp auditing templates.
Protection	
Active Directory	Select to export any Active Directory protection templates.
ADAM (AD LDS)	Select to export any ADAM (AD LDS) protection templates.
Group Policy	Select to export any Group Policy protection templates.
Exchange Mailbox	Select to export any Exchange Mailbox protection templates.
File System	Select to export any File System protection templates. **NOTE:** When the **Agent** option is selected in the Configuration section of this dialog, this option is also selected and cannot be cleared. This is because this type of template must be assigned to an agent configuration in order to work properly.

3 Click **OK** to export the selected settings into an XML file.

4 On the Save Configuration dialog, select the location where the XML file is to be saved. By default, the name of the file is **Change Auditor Configuration**; however, you can change this in the **File name** field. Click **Save**.

NOTE: A similar dialog appears when you use the **Action | Import** menu command. From this dialog, you can then select the configuration, auditing and protection settings to be imported.

10

Agent Configurations

- Introduction
- Agent Configuration page
- Define agent configurations
- Assign agent configurations to server agents
- Enable event logging

Introduction

Change Auditor assigns the default configuration to each agent, including both server agents and workstation agents, during deployment.

TIP: Whenever you upgrade from a previous version of Change Auditor, the default configuration settings will be restored. Therefore, if you want to modify the default configuration settings, it is best to copy the default configuration and then save it using a different name.

NOTE: The values for the proxy server settings are not included when you copy a configuration.

The default configuration consists of the following settings:

System Settings:

- Polling Interval: 900 seconds
- Forwarding Interval: 5 seconds
- Kerberos Ticket Lifetime: 10 hours

  A Kerberos user ticket can be used to verify your identity and gain access to specific resources or services in your domain. A golden ticket is a forged Kerberos ticket. An attack using a golden ticket is extremely dangerous due to the forged identity, elevated access it allows, and because it can be reused over its lifetime (10 years by default).

  The setting determines the maximum ticket lifetime. When this value is exceeded, the “Kerberos user ticket that exceeds the maximum ticket lifetime detected” domain controller authentication event is generated which may indicate a possible golden ticket attack.
- Retry Interval: 300 seconds
- Maximum events per connection: 1,500
- Agent Load Threshold: Defines how many events can get backed up on an agent before it triggers warning level for agent load (Load Yellow).

  Default is 10000 events (Load Yellow)

  Valid range: 100 - 100000

  Suspend (Critical/Load Red) is when the database has reached 3GB of event data and only critical events will be written to the database until it is full (4GB).

- Allowed time for connection: 24 x 7

NOTE: These system settings apply to both server agents and workstation agents.

Proxy Server settings

- Proxy Server: Not set
- Port: 8080
- Requires authentication: Not set

File System settings:

- Discard duplicates that occur within: 10 seconds

NOTE: This setting only applies to file system auditing which is available with Change Auditor for Windows File Servers, Change Auditor for EMC and Change Auditor for NetApp.

AD Query settings:

- Discard query results less than: 0 records
- Discard queries taking less than: 20 milliseconds
- Discard duplicate queries occurring within: 15 minutes
- AD Query auditing enabled

NOTE: These settings only apply to Active Directory query auditing which is available with Change Auditor for Active Directory Queries.

Exchange settings:

- Discard duplicate folder opens that occur within: 0 seconds

NOTE: This setting only applies to Exchange auditing which is available with Change Auditor for Exchange.

You can define and assign different agent configurations to each deployed server agent from the Agent Configuration page on the Administration Tasks tab. However, workstation agents always use the default configuration; they cannot be assigned to a different agent configuration.

When the default configuration is modified, workstation agents will only receive these modifications when the polling interval determines there has been a change; clicking **Refresh Configuration** on the Agent Configuration page only pushes agent configuration changes out to server agents.

To enable custom auditing and protection, you must assign templates to an agent's configuration. The custom auditing and protection features that require custom templates to be assigned to an agent's configuration are:

- Excluded Accounts Auditing
- File System Auditing
- File System Protection
- Registry Auditing
- Service Auditing
- SQL Auditing

NOTE: The NetApp, EMC, SharePoint, and Microsoft 365 auditing templates define which agents are used to capture events; however, these templates do not use the agent configurations from the Agent Configuration page as described in this section. See the Quest Change Auditor for NetApp User Guide, Quest Change Auditor for EMC User Guide, Quest Change Auditor for SharePoint User Guide, Microsoft 365 and Microsoft Entra ID Auditing User Guide.

This section describes the Agent Configuration page and how to perform the tasks associated with defining and assigning configurations to agents. For a description of the other dialogs mentioned, see the online help.

For more information on Registry Auditing, Service Auditing and Account Exclusion refer to the appropriate sections in this document. For more information on File System Auditing and File System Protection, see the Quest Change Auditor for Windows File Servers User Guide. For more information on SQL Auditing, see the Quest Change Auditor for SQL Server User Guide.

Agent Configuration page

This page displays when **Agent** is selected from the Configuration task list in the navigation pane of the Administration Tasks tab. From here you can define and assign agent configurations.

NOTE: Workstation agents always use the default configuration and cannot be assigned to a different agent configuration; therefore, they are not included on the Agent Configuration page.

The following information is available for each deployed server agent. To display columns not on by default, use the **Field Chooser** button located to the far left of the column headings.

NOTE: All dates and times are based on the client's current local date and time. The format used to display the date and time is determined by the local computer's regional and language setting.

Table 1. Agent Configuration page: Field descriptions

Column	Default	Description
Active Directory	No	Indicates whether Active Directory auditing and/or protection has been defined.
ADAM (AD LDS)	No	Indicates whether ADAM (AD LDS) auditing and/or protection has been defined.
Agent	Yes	Displays the NetBIOS name of the server that hosts the Change Auditor agent.
Agent FQDN	No	Displays the fully qualified domain name (FQDN), consisting of the host and domain name including the top-level domain, of an agent.
Configuration	Yes	Displays the name of the agent configuration assigned to each agent listed.
Coordinator	No	Displays the computer name of the Change Auditor coordinator that an agent is connected through.
DB Size	No	Displays the size of an agent's database.
Domain	Yes	Displays the name of the domain where the server resides.
EMC	Yes	Indicates whether an agent has been assigned to an EMC auditing template to receive EMC events.
Events Last 24 Hours	No	Displays the number of events encountered on the agent during the past 24 hours from when the Agent Configuration page is initially opened during the current client session or when the page is refreshed using the **Refresh** button. The value in this field is a hypertext link and when selected launches a quick search to display the events generated in the last 24 hours.
Events Last Hour	No	Displays the number of events encountered on the agent in the last 60 minutes from when the Agent Configuration page is initially opened during the current client session or when the page is refreshed using the **Refresh** button. The value in the field is a hypertext link and when selected launches a quick search to display the events generated in the last 60 minutes.

Table 1. Agent Configuration page: Field descriptions

Column	Default	Description
Events Today	No	Displays the number of events encountered on the agent since 12:00 a.m. of the current day (based on the relative coordinator computer's time). The value in this field is a hypertext link and when selected launches a quick search to display today's events.
Events Total	No	Displays the number of events encountered since the agent was started. The value in this field is a hypertext link and when selected launches a quick search to display all events encountered since the agent was started.
Events Yesterday	No	Displays the number of events encountered between 12:00 a.m. yesterday and 12:00 a.m. of the current day (based on the relative coordinator computer's time). The value in this field is a hypertext link and when selected launches a quick search to display yesterday's events.
Exchange	No	For agents hosting Exchange, this column indicates whether Exchange Mailbox auditing and/or Exchange Mailbox protection has been defined.
Microsoft 365	Yes	Indicates whether an agent has been assigned to an Microsoft 365 auditing template to receive Exchange Online, SharePoint Online, and OneDrive for Business events.
Exchange Server	No	Indicates whether the server is an Exchange server.
Exclude Account	Yes	Indicates whether an Excluded Accounts Auditing template has been assigned to an agent's configuration.
File System	Yes	Indicates whether a File System Auditing or File System Protection template has been assigned to an agent's configuration.
Forest	No	Displays the name of the forest where the agent resides.
Group Policy	No	Indicates whether Group Policy protection has been defined.
Last Update	No	Displays the date and time when the agent configuration was last updated.
NetApp	Yes	Indicates whether an agent has been assigned to a NetApp Auditing template to receive NetApp filer events.
Registry	Yes	Indicates whether a Registry Auditing template has been assigned to an agent's configuration.
Service	Yes	Indicates whether a Service Auditing template has been assigned to an agent's configuration.
SharePoint	Yes	Indicates whether an agent has been assigned to a SharePoint Auditing template to capture SharePoint events.
SQL	Yes	Indicates whether a SQL Auditing template has been assigned to an agent's configuration.
SQL Data Level	Yes	Indicates whether a SQL Data Level Auditing template has been assigned to an agent's configuration.
Startup Time	No	Displays the date and time when the agent was last initialized.
Status	No	Displays the current status of the agent: • active • inactive • uninstalled
Type	No	Displays the agent platform: • Domain Controller • Global Catalog • Server

Table 1. Agent Configuration page: Field descriptions

Column	Default	Description
Unsent Events	No	Displays the number of events that have not yet been sent to the coordinator.
Uptime	No	Displays how long the agent has been running.
Version	No	Displays the version number of the Change Auditor agent currently deployed.

Define agent configurations

To define a new agent configuration:

1. Open the Administration Tasks tab and click **Configuration**.
2. Select **Agent** in the Configuration task list.
3. From the Agent Configuration page, click **Configurations**.

   The Configuration Setup dialog opens, which contains a list of configuration definitions available as well as the means for creating a new configuration.
4. Click **Add** to create a new definition or click **Copy** to duplicate the configuration selected in the Configurations list box.

   This adds a new configuration to the list, allowing you to name the new configuration, specify the system settings and assign auditing and protection templates to the configuration.
5. With the new/copied configuration highlighted in the Configuration list, enter the name for your new agent configuration.
6. Use the tabbed pages at the top of the dialog to modify the system settings, file system settings, AD Query settings, Exchange settings, Defender auditing, and Authentication Services auditing. The settings that can be modified on these tabs include:

   Table 2. Agent Configuration settings

Setting:	Default:	Valid range:
System Settings		
Polling Interval	900 seconds	60 - 9999 seconds
Forwarding Interval	5 seconds	5 - 999 seconds
Retry Interval	300 seconds	60 - 600 seconds
Kerberos Ticket Lifetime (hours)	10 hours	1 to 99999 hours
Max events per connection	1500 events	100 - 99999 events
Agent Load Threshold Defines how many events can get backed up on an agent before it triggers warning level for agent load (Load Yellow).	10000 events (Load Yellow) Suspend (Critical/Load Red) is when the database has reached 3GB of event data and only critical events will be written to the database until it is full (4GB).	100 - 100000 events
Allowed time for connection	Sunday - Saturday 12:00 am - 11:59 pm	N/A

Table 2. Agent Configuration settings

Setting:	Default:	Valid range:
Proxy Server Settings		
If your organization uses a proxy server to connect to the internet, these settings are required to audit Microsoft Entra ID and Microsoft 365 targets. Selecting **Validate Proxy Settings** uses the configured settings to access a website through the proxy server. This test uses the https://www.quest.com web site. **NOTE:** Clearing the value for 'Proxy Server' and selecting Apply resets all proxy settings to default values.		
Proxy Server	Not set	fully qualified domain name, down-level name, or IPv4 address
Port	8080	1- 65535
Requires Authentication If your proxy server requires authentication, click the option and enter the required credentials.	Not set	N/A
File System		
The settings on the File System tab only apply when Change Auditor for Windows File Servers, Change Auditor for EMC or Change Auditor for NetApp is licensed.		
Discard duplicates that occur within *nn* seconds	Enabled by default 10 seconds	1 - 600 seconds
Audit all configured, including duplicates (Not recommended)	Disabled by default	N/A
AD Query		
The settings on the AD Query tab only apply when Change Auditor for Active Directory Queries is licensed.		
Discard query results less than *nn* records	0 records	0 - 99999 records
Discard queries taking less than *nn* milliseconds	20 milliseconds	0 - 99999 milliseconds
Discard duplicate queries occurring within *nn* minutes	15 minutes	1 - 1440 minutes
AD Query auditing enabled	Enabled by default	N/A
Exchange		
The setting on the Exchange tab only applies when Change Auditor for Exchange is licensed. **NOTE:** These settings only apply to the Exchange subsystem events; they do not apply to the Microsoft 365 subsystem events.		
Discard duplicates that occur within *nn* seconds	0 seconds	0 - 600 seconds
Defender		
Defender auditing enabled	Disabled by default	N/A
Authentication Services		
Authentication Services auditing enabled	Disabled by default	N/A

For a detailed description of these settings, see the online help.

7 To add an auditing or protection template to the selected configuration, use the Auditing and Protection Templates pane. This pane displays the auditing and protection templates previously defined.

Use one of the following methods to assign a template to an agent configuration:

- Select a template and ‘drag and drop’ it onto a configuration in the Configuration list.

- Select a configuration from the Configuration list and 'drag and drop' it onto a template in the Auditing and Protection Templates pane.
- Select a configuration, then select a template, right-click and select **Assign**.
- Select a configuration, then select a template, click in the corresponding **Assigned** cell and click **Yes**.

Repeat this step to add additional templates to the selected configuration.

8 If the templates list is empty or you want to define a new template, click **Edit Templates**.

- On the Auditing and Protection Templates dialog, select the tab for the type of template to be added (e.g., Excluded Accounts) and click **Add Template**.
- The associated wizard will be displayed allowing you to define the auditing or protection to be applied. Refer to the appropriate chapters in this guide for details on completing each of these wizards.

9 Once you have defined the new template, click **OK** to close this dialog and return to the Configuration Setup dialog. Select this new template, right-click and select **Assign**.

10 Once you have named the configuration, selected the system settings and added auditing or protection templates, click **OK** to save your configuration and return to the Agent Configuration page.

Assign agent configurations to server agents

Once agent configurations are defined you can assign it to one or more installed server agents from the Agent Configuration page.

To assign a configuration to an agent from the Agent Configuration page:

1 On the Agent Configuration page, select one or more agents from the agent list and click **Assign**.

2 On the Agent Assignment dialog, select the configuration definition to be assigned to the selected agents and click **OK**.

On the Agent Configuration page, the agent configuration assignment will be updated in the **Configuration** column.

3 Select the agents assigned to the agent configuration and click **Refresh Configuration** to ensure that the assigned agents are using the latest agent configuration.

To reset ALL agent configurations back to the default configuration:

1 On the Agent Configuration page, click **Default All**.

2 A message is displayed confirming that you want to reset all agent configurations back to the factory default settings. Click **Yes**.

The agent configuration assignment will be updated in the **Configuration** column.

3 Select the agents assigned to the agent configuration and click **Refresh Configuration** to ensure that the assigned agents are using the latest agent configuration.

Enable event logging

Using the Agent Configuration page you can enable the event logging feature which writes Change Auditor events locally to a Windows event log. These event logs can then be collected using InTrust to satisfy long-term storage requirements.

NOTE: This is a global setting and applies to all agents. Keep the following in mind when defining custom auditing:

- Disabling Change Auditor events does NOT impact event logging.
- Excluding accounts from auditing does NOT impact event logging with the exception of Exchange. That is, if an Exchange Mailbox account is set to exclude ALL mailbox events, then these events will also be excluded from the event log.
- For Registry events, event logging is disabled by default. When enabled, only configured activities are sent to the event log "ChangeAuditor Service".
- For Service events, event logging is disabled by default. When enabled, only configured activities are sent to the event log "ChangeAuditor Service".
- For Active Directory events, event logging is disabled by default. When enabled, all Active Directory activity is sent to the event log "InTrust for AD".
- For Microsoft Entra events, event logging is disabled by default. When enabled, only configured activities are sent to the event log "Change Auditor for Microsoft Entra ID"
- For ADAM (AD LDS) events, event logging is disabled by default. When enabled, all ADAM activity is sent to the event log "InTrust for ADAM".
- For File System events, event logging is disabled by default. When enabled, only configured activities are sent to the event log "Quest File Access Audit".
- For Exchange mailbox events, event logging is disabled by default. When enabled, only configured Exchange Mailbox activities are sent to the event log "InTrust for Exchange". Microsoft 365 Exchange Online events are not logged to this event log.
- For SQL Server events, event logging is disabled by default. When enabled, only configured activities are sent to the event log "ChangeAuditor for SQL".
- For SQL Data Level events, event logging is disabled by default. When enabled, only configured activities are sent to the event log "ChangeAuditor for SQL" .
- For AD Query events, event logging is disabled by default. When enabled, all Active Directory queries, except those specified in the excluded AD Query list are sent to the event log "InTrust for AD". When enabling AD Query event logging, keep in mind that AD Query events could be of very high volume.
- For EMC events, event logging is disabled by default. When enabled, only configured activities are sent to the event log "ChangeAuditor for EMC ".
- For NetApp events, event logging is disabled by default. When enabled, only configured activities are sent to the event log "ChangeAuditor for NetApp".
- For SharePoint events, event logging is disabled by default. When enabled, only configured activities are sent to the event log "ChangeAuditor for SharePoint".

To enable event logging:

1. Open the Administration Tasks tab and select **Agent** (under the Configuration task list) to display the Agent Configuration page.
2. Click **Event Logging**.
3. Select the type of event logging to enable:
   - Active Directory
   - ADAM (AD LDS)

- Microsoft Entra
- Exchange
- File System
- SQL
- SQL Data Level
- EMC
- AD Query
- Registry
- Service
- Local Account
- Change Auditor
- NetApp
- SharePoint

NOTE: If an option is disabled, this indicates that you do not have the corresponding component licensed.

4 Click **OK** to save your selection and close the dialog.

11

Coordinator Configuration

- Coordinator Configuration page
- Configure email alert notifications/reports
- Manually create a Microsoft Entra web application for sending Microsoft 365 mail
- Customize alert email content
- Shared Folder Configuration
- Group Membership Expansion
- Add groups to Group Membership Expansion list
- Agent Heartbeat Check
- Disconnect client after 30 minutes of inactivity
- Scheduled Task Handling

Coordinator Configuration page

The Coordinator Configuration page is displayed when you select **Coordinator** from the Configuration task list in the navigation pane of the Administration Tasks tab.

This page consists of the following:

- **Configure email alert notifications/reports** - for enabling and configuring SMTP email and Microsoft 365 Mail for alerting and reporting
- **Shared Folder Configuration** - for enabling and configuring shared folders for reporting
- **Group Membership Expansion** - for defining the schedule for expanding nested membership of Active Directory groups that are referenced in searches (Who search criteria) or groups that are defined in the Member of Group auditing feature
- **Agent Heartbeat Check** - for specifying how long the coordinator service is to wait before an agent that is not sending updates will be marked as 'inactive'
- **Scheduled Task Handling** - for specifying which coordinators should handle purge, archive, and scheduled reports jobs.

This section provides a description of the panes listed above and instructions on how to use these panes to configure email alerting and group membership expansion. For a description of the other dialogs mentioned in this chapter, see the online help.

Configure email alert notifications/reports

To dispatch alerts and reports through email, SMTP or Microsoft 365 Mail, you need to enable notification and define the email settings.

NOTE: The settings set on this page are global settings and apply to all alert/report emails. For alerts you can override the reply to, alert subject, signature and body content for individual search queries using the settings on the Alert tab (Search Properties tabs). For reports, you can override the To and Reply addresses, specify carbon copy (Cc and Bcc) recipients, and modify the subject line for individual search queries using the Report tab (Search Properties tabs).

To enable and configure email notifications/reports:

1. Open the Administration Tasks page and click **Configuration** at the bottom of the navigation pane (left pane).
2. Select **Coordinator** in the Configuration task list to open the Coordinator Configuration page.
3. On the Email Alerts Configuration pane, specify the required information.

Table 1. Email Alerts Configuration pane options

Field/Control	Description
Disabled	Select to disable email notifications.
SMTP	Select this to enable SMTP email alert notifications and reporting. When this option is selected, you can specify a mail server and authentication options for the SMTP email configuration. • **Server Requires Authentication**: Select this check box if the specified email server requires authentication and enter the account information as described below. • **Enable SSL**: Select this check box to enable Secure Socket Layer (SSL) encryption protocol to create a secure connection for transmitting data from the email server. • **Requires Comma-Separated Addresses:** Select this option if your SMTP server requires comma separated addresses when multiple recipients are specified. • **Mail Server**: When SMTP is enabled for alerts and reporting, enter the name or IP address of the email server in this text box. To configure a specific SMTP port, append the email server (SMTP server name or IP address) with a colon and the required port. Change Auditor sends alerts/reports through a single SMTP (email) relay configuration even when multiple coordinators are configured. That is, all coordinators will use the same email server for sending alert notifications and reports. • **Account Name**: Enter the account name required to authenticate to the specified email server. Instead of entering the account name, you can use the browse button to the far right of the **Account Name** field to select the account to be used. Clicking this button displays the Select Active Directory Object dialog (Directory object picker). Use the Browse or Search pages to locate the user account to be used to authenticate to the email server. • **Password:** Enter the password associated with the account name entered above. Blank passwords are not allowed.

Table 1. Email Alerts Configuration pane options

Field/Control	Description
Microsoft 365 Mail	Select this to enable Microsoft 365 Mail alert notifications and reporting. When this option is selected, you can specify an Microsoft Entra Directory Name and web application for the email configuration. • **Microsoft Entra Directory Name**: The name of the Microsoft Entra directory for Microsoft 365 Mail. • **Application ID**: The Microsoft Entra web application ID. Select **Create New** to create a new application. (When creating a new web application, the account provided must hold the Global Administrator role in the specified Microsoft Entra directory.) • **Application Key**: The Microsoft Entra web application key. **NOTE:** Automatic web app creation is not supported for GCC High tenants. See Manually create a Microsoft Entra web application for sending Microsoft 365 mail for details.
From Address **NOTE:** Browsing for an email address is only supported for on-premises Active Directory and Exchange. **NOTE:** The From Address value must be an enabled mailbox in the specified Microsoft Entra directory when Microsoft 365 mail configuration is selected.	Enter the email address from which alert notifications and reports are to originate. You can use the browse button to select the user whose email address is to be used for alert notifications and email reports. Clicking this button displays one of the following dialogs: • The Select Active Directory Objects dialog (Directory object picker) allows you to locate and select an Active Directory user. Use the Browse or Search page to locate and select an Active Directory user. This dialog is displayed when no Exchange host is specified in the Coordinator Configuration page. • The Select Exchange Users dialog allows you to search for and select a mail-enabled object from the Exchange Global Access List (GAL). On the Exchange tab, enter a name or partial name, at least three characters long, and click the **Search** button to lookup mail-enabled objects in the GAL. On the Active Directory tab, use the Browse or Search page to locate and select an Active Directory user. This dialog is displayed when an Exchange host is defined in the Coordinator Configuration page.
Reply To	Enter the address where replies to alert/report emails are to be sent. You can use the browse button to select the user whose email address is to be used for alert notifications and email reports. Clicking this button displays one of the following dialogs: • The Select Active Directory Objects dialog (Directory object picker) allows you to locate and select an Active Directory user. Use the Browse or Search page to locate and select an Active Directory user. This dialog is displayed when no Exchange host is specified in the Coordinator Configuration page. • The Select Exchange Users dialog allows you to search for and select a mail-enabled object from the Exchange Global Access List (GAL). On the Exchange tab, enter a name or partial name, at least three characters long, and click **Search** to lookup mail-enabled objects in the GAL. On the Active Directory tab, use the Browse or Search page to locate and select an Active Directory user. This dialog is displayed when an Exchange host is defined in the Coordinator Configuration page.

Table 1. Email Alerts Configuration pane options

Field/Control	Description
Alert Subject **NOTE:** This does not apply to email reports.	Enter a customized subject line to replace the default text in the subject line for alert notifications. The default subject line contains the following information: Change Auditor *%Alert_Type%* from *%Alert_Coordinator_Name%*: *%Alert_Name%* Where: *%Alert_Type%* is either 'Alert' or 'Smart Alert' *%Alert_Coordinator_Name%* is the name of the coordinator generating the alert *%Alert_Name%* is the name of the alert that fired Click the browse button to select the variables to insert into the subject line or to reset it back to the default content. Expand the **Insert Variable** option to insert one or more of the following variables into the subject line: • ALERT_NAME • ALERT_TIME_SENT • ALERT_TYPE • ALERT_COORDINATOR_DOMAIN • ALERT_COORDINATOR_NAME • SMART_ALERT • SMART_ALERT_GROUPING • SMART_ALERT_OCCURRENCE • SMART_ALERT_PERIOD • SMART_ALERT_PERIOD_UNIT • BATCH_ID • EVENT_COUNT Select **Restore To Default** to reset the subject line back to the default content. That is, remove any variables that were inserted.
Send Plain Text Email	Select this option to have the email notification sent in plain text format. (Default)
Send HTML Email	Select this option to have the email notification sent in HTML format.

Table 1. Email Alerts Configuration pane options

Field/Control	Description
Configure Body	Click this button to define the content of the main body, the event details and the signature to be included in your alert emails. **NOTE:** The Alert Body Configuration settings do not apply to email reports. To define the content (columns) to be included in a report, use the Layout tab. In addition, you can use the Report Layouts page (Administration Tasks tab) to create customized report layout template(s) defining the header and footer information to be used in your reports.
Mailbox Search (optional) Entering the Exchange host information allows you to lookup email recipients from the Exchange GAL in addition to Active Directory. That is, when you click a browse button on the SMTP Configuration pane, Alert Custom Email dialog or Report tab to lookup an email recipient, the Select Exchange Users dialog appears which contains both an Exchange tab and an Active Directory tab. **NOTE:** Browsing for an email address is only supported for on-premises Active Directory and Exchange.	• **Exchange Host**: Enter the internet host name of the Exchange email server and the Exchange version associated with the specified Exchange host. • **Email:** Enter your full email address. • **My Host Requires Authentication**: Select this check box if the specified Exchange host requires authentication and enter the account name and password. • **Account Name**: Enter the user account name used to log into your email account. You can also use the browse button to select the account to be used. Clicking this button displays the Select Active Directory Object dialog (Directory object picker). Use the Browse or Search pages to locate the user account to be used to authenticate to the Exchange host. • Password: Enter the password associated with the account name entered above.

4 Click **Test Mail** to test the configuration.

5 Once the email server configuration is verified, click **Apply Changes** to save the configuration.

Now that alerting/reporting is enabled and configured, you can enable email alert notifications for individual search definitions using the Alert tab (Search Properties tabs) and/or reporting for individual search definitions using the Report tab (Search Properties tabs).

Manually create a Microsoft Entra web application for sending Microsoft 365 mail

See Microsoft documentation for details on integrating applications with Microsoft Entra ID and creating a web application.

NOTE: The Microsoft Entra web application:

- Should be a single-tenant application. A redirect URI is not required.
- Must have a Client Secret configured in the web application "Certificates and Secrets" page.

Ensure the following permission is assigned to the web application:

Microsoft Graph application permission:

- Mail.Send – Application - Send mail as any user

Once the required permission is applied, click **Grant admin consent for…** and confirm with **Yes**.

Customize alert email content

In addition to the customizable fields (Reply To, Alert Subject and Signature) on the Coordinator Configuration dialog, you can use the **Configure Body** button to define the content to be used in the main body of your alert emails as well as the event details to be included.

NOTE: When accessed through the Coordinator Configuration page, these settings will apply globally to all alert emails. However, if accessed through the Alert tab, these settings will apply to the selected alert only.

NOTE: The Alert Body Configuration settings do not apply to email reports. To define the content (columns) to be included in a report, use the Layout tab. In addition, you can use the Report Layouts page (Administration Tasks tab) to create customized report layout templates defining the header and footer information to be used in your reports.

To customize alert email content:

1. Click **Configure Body** to display the Alert Body Configuration dialog.
2. Select the appropriate option (at the bottom of the dialog) to edit either the **Plain Text** (default) or the **HTML** representation of the alert emails.
3. Use the **Main Body** tab to enter the text to be included and define the overall layout of the alert body.
   - Select the **Show Variables** check box to display the variables that can be added to the main body of your email.
   - To add a variable, double-click the variable from the Variable list at the bottom of the page. You can also drag and drop a variable from the Variable list into the main body text box.

   NOTE: The event details defined in the Event Details tab are placed in the Main Body pane using the following tag: %EVENT_DETAILS%. This tag should not be removed from the Main Body tab if you want to include the event details in the alert emails.
4. Use the **Event Details** tab to specify the event details to be included. That is, you can rearrange the entries, remove entries, or modify text, etc.
   - Select the **Show Variables** check box to display a list of the variable that can be added to the event details of your alert email.
   - To add a variable, double-click the variable from the Variable list at the bottom of the page. You can also drag and drop a variable from the Variable list into the Event Details text box.

   NOTE: Do not modify the blue text surrounded by percent signs (such as %USERNAME%). These are tags which represent actual data retrieved from the Change Auditor event that triggered the alert. See Change Auditor Email Tags for more information on these tags and the data retrieved by each.
5. Use the **Signature** tab to define the content of the signature line to be used in alert emails.
6. After you have entered the body content and defined the event details and signature line to be included, select the **Preview** tab to view a sample email using your defined format and content.
7. Once defined, click **OK** to save your settings and close the Alert Body Configuration dialog.

   NOTE: Click **Restore to Default** to revert back to the default email content and format.

Shared Folder Configuration

To allow users to send reports to a shared folder, you must specify credentials to use to write reports and a default shared folder.

To configure the ability to send reports to a shared folder:

1. Open the Administration Tasks page and click **Configuration**.
2. Select **Coordinator** in the Configuration task list to open the Coordinator Configuration page.
3. Under **Shared Folder Configuration**, select **Enable Shared Folder for Reporting**. Checking this option activates the remaining fields on this page to define the account credentials and folder to use.
4. Enter the credentials (account name and password) for the coordinator to use to write the reports to a shared folder. The credentials are used to write reports to the default shared folder as well as custom shared folders specified for individual reports.

   NOTE: If you are using a group Managed Service Account:
   - The account must end with '$' and the password must be blank.
   - The Windows client must be run as the administrator. (Right-click and select Run as administrator.)
   - The coordinator host must be correctly configured to retrieve the managed password for the specified group Managed Service Account.
   - The local Administrator group must be added to the group policy debug programs. (Found under Local Computer Policy | Windows Settings | Security Settings | Local Policies | User Rights Assignments | Debug programs.)

5. Select a shared folder to use as the default when users select to enable reporting for a search. Select **Test access** to ensure that the folder exists and the specified account has permissions to write to it.

   NOTE: If the default shared folder path is updated, it will be used for each report that uses it.

Group Membership Expansion

The middle pane of the Coordinator Configuration page contains options which allow you to define the schedule for expanding nested membership of Active Directory groups that are referenced in searches (Who search criteria) or groups that are defined in the Member of Group feature. Group membership will be recursively enumerated in order to determine nested group membership.

Use the following options to define group membership expansion behavior:

Table 2. Coordinator Configuration page: Group membership expansion options

Options	Description
Select the groups to expand	Select one of the following options to define how you want to expand groups: • **Expand all groups** - This expands all groups in the forest. Use this only if you are using SSIS and need the freedom to make requests for any group in the forest. • **Expand groups that are referenced in existing queries** - Change Auditor must expand all groups in queries in order to get their membership. With the membership, the events for the groups can be retrieved. This is always done and cannot be disabled. • **Expand groups that are referenced in existing queries and selected groups** (default) - In addition to the groups referenced in existing queries, you have the ability to select other groups. This would be useful when you have groups that need expansion for SSIS database requests, but you do not want to burden your production system with expanding all groups in the environment.
Group Membership Expansion list	The Group Membership Expansion list box is only available when the **Expand groups that are referenced in existing queries and selected groups** option is selected and displays a list of the groups to be expanded. Use **Add** to add groups to this list box and **Remove** to remove groups from the list box.
Add	Use to add groups to the group membership expansion list. Clicking this button will display the Select Active Directory Objects dialog allowing you to locate and select the groups to be added. See Directory object picker for a description of the Browse, Search and Options pages. Note that the **Find** field on this dialog will display **Group** and cannot be changed.
Remove	Use to remove the selected group from the group membership expansion list.
Select the refresh frequency	
Select from the following options to define how often you want to refresh the group membership expansion list.	
Refresh group membership every *nnn* minutes	By default, group membership will be refreshed every 360 minutes. Use the arrow controls to increase or decrease this value. Valid range: 10 - 43200
Number of groups to expand every 5-minute cycle	By default, 20 groups will be expanded every 5-minute cycle. Use the arrow controls to increase or decrease this value Valid range: 1 - 100000
Refresh the list of expanded groups every *nnn* minutes	By default, the group membership expansion list is refreshed every 180 minutes. Use the arrow controls to increase or decrease this value. Valid range: 10 - 43200
Defaults	Use to reset the fresh frequency settings back to the factory defaults.

Add groups to Group Membership Expansion list

By default, the **Expand groups that are referenced in existing queries and selected groups** option is selected on the Group Membership Expansion pane of the Coordinator Configuration page. With the option selected, you can add groups to the Group Membership Expansion list as described below:

1 Click **Add** to display the Select Active Directory Objects dialog.

2 Use either the Browse page or Search page to locate and select a group to be added to this list. Once a group is selected, click **Add** to add it to the selection list at the bottom of the dialog.

Repeat this step to add each additional group.

3 Once you have selected all the groups to be added, click **Select** to save your selection.

The specified groups will now be listed in the Group Membership Expansion list on the Coordinator Configuration page.

4 On the Coordinator Configuration page, click **Apply Changes** to apply your changes regarding group membership expansion.

Agent Heartbeat Check

The bottom pane on the Coordinator Configuration pane allows you to define how long the coordinator service will wait before an active agent that is not sending updates will be marked as 'inactive'.

Use the following options to define the Agent heartbeat check settings:

Table 3. Coordinator Configuration page: Agent heartbeat check options

Options	Description
Agent goes offline after being inactive for *nn* minutes	By default, the coordinator service will mark an agent as 'inactive' when it has not received any updates from the agent for 30 minutes. Use this setting to specify the period of time an agent must be inactive before the coordinator service marks it as 'inactive'. Valid range: 5 - 14400
Coordinator should try to restart agent service if an agent goes offline	Select this if you want to have the coordinator service try to restart an agent service before it marks it as inactive.

Disconnect client after 30 minutes of inactivity

Enabling this option makes all client disconnect from the coordinator after 30 minutes of inactivity. If this is not selected, the option to disconnect after 30 minutes of inactivity can be selected by users when they log on to the client.

Scheduled Task Handling

This option allows you to load balance as needed in a a multi-coordinator environment. Specifically, it allows you to specify which coordinators should handle purge, archive, and scheduled reports jobs. This is helpful in situations where some coordinators are busier than others due to closer agent load or they are further removed from the database.

By default, all coordinators are allowed to process scheduled jobs.

To specify coordinators to handle scheduled jobs:

1 Click **Select allowed coordinators**.

2 Check the coordinators that you want to used for scheduled jobs. All other coordinators will be blocked from processing these jobs.

12

Purging and Archiving your Change Auditor Database

- Introduction
- Planning your jobs
- Purge and Archive page
- Create and maintain jobs
- Purge and Archive wizard
- Purge selected records

Introduction

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

Using the purge options, you can define and schedule jobs that will eliminate events from the database based on the following criteria:

- All events older than a specific number of days.
- Selected events based on:
  - Who - purge events generated by a specific user, computer, group, or service account.
  - What - purge events based on subsystem, event class, object class, severity or results.
  - Where - purge events captured by a specific agent, domain or site.
  - Origin - purge events originating from a specific workstation or server.

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

Table 1. Archive and purge options

Job type	Description
Purge	This deletes events from the production database. You can create and run multiple purge jobs. When scheduling a purge job, you can choose a batch limit. This limit tells the job how many events to delete from the production database before pausing and running another job. Choosing too large of a batch limit may slow your purge jobs down. If you find that they are slow reduce the batch limit.
Archive	This moves events from the production database to an archive database (on the same database server). The archive process removes the events from the production database during the move. Archive events do not need to be purged separately. You can only create and run one “archive” job or one “purge and archive” job. When scheduling an archive job for the first time it may take a long time to complete (depending on how many years of data you are asking to be archived). Batch limit does not apply to an archive type job. When running an archive job, you need to pay attention to disk space growth on the SQL server.
Purge and archive	This deletes events (purge job) from the production database, then immediately performs an archive job to move the remaining records in the time period specified for the job from the production database to an archive database. You can only create and run one “purge and archive” job or one “archive” job. If you select a batch limit, it will only apply to the purging portion of the job. When the batch limit is reached, the job will immediately run again ensuring this job type runs to completion before the archive job begins.

Planning your jobs

Planning your jobs before scheduling them will help ensure they run as expected. Keep in mind, all jobs can take a significant time to run depending on the amount of data in your environment.

Scheduling a job

When scheduling your jobs, consider the following:

- Only one job can run at a time.
- Only one archive type job (archive only, purge/archive) can exist. However, multiple purge only jobs can be scheduled.
- Purge only jobs run until they reach the batch limit. When the batch limit is encountered the job pauses (runs again later) to give another job a chance to run. Archive type jobs will not pause to give other jobs the opportunity to run until they are complete.
- If you have multiple coordinators, only one coordinator will run the job.
- Use “purge and archive” job to ensure deletion of unwanted events completes before archiving begins.
- The first time the job is run it may be working with a large amount of data and therefore may take a significant amount of time to run.
- It is recommended to run jobs frequently so that they are working with less data and complete faster. Start with one job to see how long it takes to complete, then add more jobs as needed.
- If an archiving job is created to archive large amounts of data over multiple calendar years, it may take a significant amount of time to finish. If you have multiple calendar years of data to archive, select to archive the oldest calendar year first. When the first archive job finishes, update the job settings to archive the next calendar year and so on until all the data has been archived.
- Enable notification on the purge and archive internal events to monitor job performance.
- Starting with version 6.9, Change Auditor the Next Run of the reports, archive and purge jobs based on the master time zone. For new deployments, the maser time zone is set to the time zone of the server where the first coordinator is being installed. During an upgrade, the master time zone is set to UTC. You can manually change the master time zone, using the set-CAScheduleMaserTimeZone and get-CAScheduleMasterTimeZone commands. See the Change Audit PowerSell Command User Guide for details.It is recommended to set the master time zone to the time zone where the majority of the users are located.

  NOTE: Due to the fact that Daylight Saving Time changes on different dates worldwide, Change Auditors schedules will follow the time change of that specific time zone.

When multiple jobs types are scheduled to run close together the following behavior will occur:

- A list of jobs is created and ordered by next run time. If two jobs have the same run time the archive type will run first.

  NOTE: Because of this the “purge” jobs may not complete before the “archive” or “purge and archive” jobs run if you do not plan properly.

- Multiple “Purge” jobs will be run based on the next run time order.
- The “purge” job type runs until the batch limit is reached (batch limit is the total number of events to delete) and then pauses to give another “purge” job a chance to run.

During a job

During a purge and/or archive job, consider the following:

- Use internal events to monitor job performance.
- Monitor disk space on the SQL server while archiving is in progress. (No Shrink is performed)

Post job considerations

After the purge and/or archive job completes, consider the following:

- The physical database size is not changed. (Shrink operation is not performed). Once the archive database has been created, you should perform a database cleanup (shrink) on the production database as required to free up disk space.

For information on how to perform a database shrink, see https://msdn.microsoft.com/en-us/library/ms189035.aspx.

- Multiple archive databases may be created (1 database per archived year).
- Archive databases for previous years can be detached and moved to a backup storage if needed.

Purge and Archive page

The Purge and Archive page is displayed when **Purge and Archive** is selected from the Configuration task list in the navigation pane of the Administration Tasks page. From here you can specify the settings for the purge and archive jobs.

Before creating your jobs, ensure that you have reviewed Planning your jobs.

Once a job is defined, the page displays the following details:

Table 2. Purge and Archive page: Field descriptions

Column	Description
Job Name	Displays the name assigned to the job when it was created using the Purge and Archive wizard.
Last Run	Displays the date and time the job last ran. **NOTE:** Based on the client's current local date and time. The format used to display this date and time is determined by the local computer's regional and language setting.
Next Run	Displays the date and time the job is scheduled to run next. **NOTE:** Based on the client's current local date and time. The format used to display this date and time is determined by the local computer's regional and language setting.
Status	Indicates whether the job is enabled or disabled.
Schedule	Displays the schedule defined for running the job.

You will also see information regarding the status of reach job including:

- When the job was run.
- The duration of the job.
- The number of events processed.
- The coordinator involved in the process.
- Informational messages as to the status if the job:

  Immediately continuing job: Displays when the purge portion of a 'purge and archive' job continues.

  Archive database not found. Recreating archive database: Displays if an archive database has been moved or deleted.

  Starting job: Displays when the purge, archive, or purge and archive job is beginning.

  Successfully finished job: Displays when the purge and archive, purge, or archive job is finished.

  New archive database created: Displays when the new archive database has been created for the calendar year.

  Events archived: Displays the progression of the number of events being archived.

  Total events archived: Displays the total number of archived events when archiving is finished.

  Continue purge job: Displays when re-queued purge jobs run again.

Create and maintain jobs

In addition to viewing the details about previously defined jobs, use the Purge and Archive page to define and schedule new jobs, and edit, disable/enable or delete existing jobs.

CAUTION: Carefully review your current jobs before creating a new job or altering an existing job, as it is possible to create purge and archive conflicts.

NOTE: If you have specific purge jobs that you want to complete before a scheduled archive, ensure that you leave enough time between the purge only jobs and the archive job.

Before scheduling a job, ensure that you have reviewed the best practice information in Planning your jobs.

To schedule a purge and archive job:

1. Open the Administration Tasks tab and select **Configuration** | **Purge and Archive**.
2. Click **Add** to open the Purge and Archive wizard.
3. Enter a descriptive job name.
4. Select the data that you want to purge and/or archive. The default is to process events older than 90 days.

   NOTE: Jobs created in previous versions will have the process time converted from weeks/months/quarters/years to the appropriate number of days.

5. If required, select **Purge** and choose the records to be deleted from the production database.

   All events: Select this option to purge all events from the database that are older than the specified time.

   Only selected events: Select this option to purge only selected events, based on specific criteria, from the database that are older than the specified time.

   Use the criteria tabs to define the events to be deleted:

   Who - purge events generated by a specific user, computer, group, or service account.

   What - purge events based on subsystem, event class, object class, severity or results.

   Where - purge events captured by a specific agent, domain or site.

   Origin - purge events originating from a specific workstation or server.

   See Purge selected records for a description of the criteria options.

   NOTE: If you specify criteria on more than one tab, the criteria specified on ALL of the tabs must be met before an event is deleted from the database or archived.

6. Select **Archive events** if you want to create an archive database. A yearly archive database will be created beginning on the first day of the selected month. For example, if you select Jan, the database will contain events for 12 months beginning on January 1.

   If you have also selected to purge events based on specific criteria, any events that remain will be moved to the archive database.

   NOTE: A new archive database will be created for each year of events that you have in your production database.

   NOTE: This option is not available, if there is an existing archive job.

7. Click **Next**.
8. Select the job scheduling options to define when the events are to be deleted or archived.
9. Click **Finish** to save the job and exit the wizard.

To edit a scheduled purge and archive job:

1. On the Purge and Archive page, select the job to be edited.

2 Click **Edit** to open the Purge and Archive wizard.

3 Modify the current settings as necessary.

4 Click **Finish** to save your selections and exit the wizard.

To disable a scheduled purge and archive job:

1 On the Purge and Archive page, select the job to be disabled, right-click and select **Disable**.

When a job is disabled, that particular database cleanup job will not take place until it is re-enabled.

2 To enable a previously disabled job, select the job from the Purge and Archive page, right-click and select **Enable**.

To delete a scheduled purge and archive job:

1 On the Purge and Archive page, select one or more jobs from the list and click **Delete**.

2 When prompted, confirm that you want to delete the scheduled jobs.

Purge and Archive wizard

The wizard opens when you click **Add** on the Purge and Archive page under Administration Tasks. Use this wizard to define the records to be purged or archived, and the cleanup schedule.

NOTE: A red flashing icon indicates that you have not yet entered the required information. Hovering your cursor over this icon displays a tool tip explaining what needs to be entered

Before scheduling a job, ensure that you have reviewed the best practice information in Planning your jobs.

Using the Purge and Archive wizard:

1 Begin by entering a descriptive name for the job.

2 Select the data that you want to purge and/or archive. The default is to process events older than 90 days.

NOTE: Jobs created in previous versions will have the process time converted from weeks/months/quarters/years to the appropriate number of days.

3 Select whether you want to purge, archive, or both. If you have specific purge jobs that you want to complete before a scheduled archive, ensure that you leave enough time between the purge only jobs and the archive job.

Option	Notes
Purge events	If you select to purge events, specify the options that determine which events will be removed from the database. **All events:** Select this option to purge all events from the database that are older than the specified time. **Only selected events:** Select this option to purge only selected events, based on specific criteria, from the database that are older than the specified time. Use the criteria tabs to define the events to be deleted: • Who - purge events generated by a specific user, computer, group, or service account. • What - purge events based on subsystem, event class, object class, severity or results. • Where - purge events captured by a specific agent, domain or site. • Origin - purge events originating from a specific workstation or server. If you specify criteria on more than one tab, the criteria specified on ALL of the tabs must be met before an event is deleted from the database or archived. See Purge selected records for a description of the criteria tabs and options that appear to specify the records.
Archive events	When this option is selected, a yearly archive database will be created beginning on the first day of the selected month. For example, if you select Jan, the database will contain events for 12 months beginning on January 1.If you have also selected to purge events based on specific criteria, any events that remain will be moved to the archive database. **NOTE:** A new archive database will be created for each year of events that you have in your production database. If using SQL AlwaysOn and the Change Auditor database resides in an Availability Group, the archive database will be created on the current primary database node. On initial run of archive or purge/archive job, an archive database will be created on the same database server as your production Change Auditor database. The name of the archive database is as follows: Production database name appended with _Archive_ and the year of your oldest event and a selected month. Example: ChangeAuditor_Archive_2014 _August The *.mdf file will have the same name except that the date will be appended to the end. Example: ChangeAuditor_Archive_2014__August20150310163244.mdf If the archive database is moved or deleted a new archive database with the same name will be created (the *.mdf will differ because a new date is appended) the next time an archive or purge/archive job runs. **NOTE:** If an archive database is deleted or moved before the end of an archived year, then a new one will be created and will only contain events that were not previously archived to the deleted or moved database. **NOTE:** This option is not available, if there is an existing archive job.

4 Next, set the job schedule.

Option	Description
Occurs	Specifies if the job is to be run on a weekly or monthly schedule. The default is monthly. **NOTE:** When **Monthly** is selected, specify the monthly schedule to be used to run the job. For example, 1 for every month (default), 2 for every other month, 6 for every six months or twice a year, etc.
Batch Limit	Specifies the maximum number of events to be purged for each cycle. That is, the job task checks every five minutes to determine if it needs to run a job. When the job runs, by default it purges a maximum of 500,000 events in that five minute period. If there are more than 500,000 events to be purged, then five minutes later another 500,000 events are processed until all of the events are purged or archived.If there are 500,000 events or less in a job, then the job task checks again in the next five minutes and obeys the 'next run' time. **NOTE:** If SQL is slow or disk space is low, decrease this limit to 100000 or 50000. When this limit is decreased, the job will take longer to complete.
Every	When a **Monthly** schedule is selected, specifies on which day of the month the job is to be run: • First (default) • Last • Day # When a **Weekly** schedule is selected, specifies the weekly schedule to be used to run the job. For example, 1 for every week, 2 for every other week, 3 for every third week, and 4 for every fourth week.
On Days	When a **Weekly** schedule is selected, defines the days of the week when the job is to be run. The default is Monday through Friday.
Run Time	Defines the time of day when the job is to be performed. The default start time is 12:00:00 AM. **NOTE:** Based on the client's current local date and time. The format used to display this date and time is determined by the local machine's regional and language setting.
Last Run	This read-only field specifies the last time (date and time) the job ran. **NOTE:** Based on the client's current local date and time. The format used to display this date and time is determined by the local machine's regional and language setting.
Next Run	This read-only field specifies the next time (date and time) when the job is scheduled to run. **NOTE:** Based on the client's current local date and time. The format used to display this date and time is determined by the local machine's regional and language setting.

5 Select **Finish**.

Purge selected records

Use the criteria tabs in the Purge and Archive wizard to define what specific records are to be deleted from the database. These tabs are enabled when you choose the **Purge | Only selected events** option.

NOTE: If you specify criteria on more than one tab, the criteria specified on ALL of the tabs must be met before an event is deleted from the database or archived.

Who tab

Use the Who tab when you want to purge or archive events generated by specific users, computers, groups, or service accounts. By default (when the Who tab is empty), change events generated by all users, computers, groups, and service accounts will be deleted from the database or archived.

When multiple 'who' criteria is specified on this tab, Change Auditor uses the 'OR' operator to evaluate change events, purging or archiving events for activity performed by any of the users, computers, groups, or service accounts listed on this tab.

To purge events generated by a specific user, computer, group, or service account:

1. From the Purge and Archive wizard, select the **Purge** option, and then enable **Only selected events** to activate the criteria tabs.
2. Open the Who tab and click **Add**.
3. On the Select Active Directory Objects dialog, use the Browse or Search page to locate the user, computer, group, or service account to be included. Once you have located a directory object, select it and click **Add** to add it to the selection list at the bottom of the dialog.

   Repeat this step to include each additional directory object.
4. After selecting one or more directory objects, click **Select** to save your selection and close the dialog.

   NOTE: Use **Add with Events** (instead of **Add**) to select users, computers, groups, or service accounts that already have an event associated with it in the database. Use this to purge events tied to users who have been removed from Active Directory.

   Change Auditor now purges or archives events generated by the users, computers, groups, or service accounts listed on the Who tab.

   NOTE: To purge events NOT generated by the users, computers, groups, or service accounts listed on the Who tab, select the **Exclude The Following Selection(s)** check box at the top of the Who tab.

To use a wildcard expression to specify users or groups:

1. From the Purge and Archive wizard, select the **Purge** option, and then enable **Only selected events** to activate the criteria tabs.
2. Open the Who tab and expand **Add** and click **Add Wildcard Expression**.

   NOTE: If you used **Add With Events** instead, click **Add Wildcard Expression** on the Add Users, Computer, or Groups dialog.
3. On the Add Who dialog, enter the wildcard expression to be used to search for users (domain\user name) or groups (domain\group name).
   - Select the comparison operator to be used: **Like** or **Not Like**
   - Enter the pattern (character string and * wildcard character) to be used to search for a match. Use the * wildcard character to match any string of zero or more characters.
   - By default, the wildcard expression will be used to search for users. To search for groups, select the **Group** option.

> **NOTE:** When using the **Group** option, the Group Membership Expansion option on the Coordinator Configuration page (on the Administration Tasks tab) must be set to **Expand all groups**.

4 Click **OK** to close the dialog and add the wildcard expression to the Who tab.

Change Auditor now searches for and purges or archives change events generated by the users that are members of the groups whose name matches the specified wildcard expression.

What tab

Use the What tab to specify the what criteria to be used to determine whether an event is to be purged from the database. By default (when the What tab is empty), all events regardless of the subsystem, event class, object class, severity, or results will be purged or archived.

When multiple 'what' criteria is specified on this tab, Change Auditor uses the 'AND' operator to evaluate an event, purging only those events that meet all the specified criteria. However, when multiple subsystems (such as Active Directory, ADAM, and Exchange) are specified, Change Auditor uses the 'OR' operator to evaluate these entities, purging or archiving events that meet any of the specified subsystem criteria. This also applies when multiple event classes are specified. That is, when multiple event classes are specified, Change Auditor uses the 'OR' operator purging or archiving any of the specified events.

To purge events based on a specific entity:

1 From the Purge and Archive wizard, select **Purge**, and then enable **Only selected events** to activate the criteria tabs.

2 Open the What tab, expand **Add** (or **Add With Events**) and select the appropriate option. When you select an option, an additional dialog appears allowing you to enter specific criteria:

- **Subsystem | Active Directory** - Add Active Directory Container dialog
- **Subsystem | AD Query** - Add Active Directory Container dialog
- **Subsystem | ADAM (AD LDS)** - Select the agent that hosts the ADAM/LDS Instance dialog
- **Subsystem | Exchange** - Add Exchange Container dialog
- **Subsystem | Microsoft 365** - Microsoft 365 dialog
- **Subsystem | File System** - Add File System Path dialog
- **Subsystem | Group Policy** - Add Group Policy Container dialog
- **Subsystem | Local Account** - Add Local Account dialog
- **Subsystem | Logon Activity** - Add Logons dialog
- **Subsystem | Registry** - Add Registry Key dialog
- **Subsystem | Service** - Add Service dialog
- **Subsystem | SharePoint** - Add SharePoint Path dialog
- **Subsystem | SQL** - Add SQL Instance dialog
- **Event Class** - Add Facilities or Event Classes dialog
- **Object Class** - Add Object Classes dialog
- **Severity** - Add Severities dialog
- **Result** - Add Results dialog

3 Once you have selected or entered the specific criteria, click **Add** to add it to the selection list at the bottom of the dialog.

4 Click **OK** to save your selection and close the dialog.

Change Auditor now searches for and purges or archives change events that match the criteria listed on the What tab.

Where tab

Use the Where tab to purge events captured by specific agents, domains, or sites. By default (when the Where tab is empty), events captured by all agents will be purged or archived.

When multiple 'where' criteria is added to this tab, Change Auditor uses the 'OR' operator to evaluate events, purging or archiving events that were captured by any of the specified agents, domains or sites.

To purge events captured by a specific agent, domain or site:

1. From the Purge and Archive wizard, select **Purge**, and then enable **Only selected events** to activate the criteria tabs.
2. Open the Where tab and click **Add**.
3. On the Choose the Agents, Domains or Sites to Include dialog, use the Browse or Search pages to locate an individual agent, domain or site.

   NOTE: You can also select the Grid View option to select an agent from a list rather than using the Explorer View to locate it within your environment.

   Once you have located an agent, domain or site, select it and click **Add** to add it to the selection list at the bottom of the dialog.

   Repeat this step to include each additional agent, domain or site.
4. Click **OK** to save your selection and close the dialog.

   NOTE: Use **Add With Events** (instead of **Add**) to select agents, domains, or sites that already have an event associated with it in the database.

   Change Auditor now searches for and purges or archives change events captured by the agents, domains, or sites listed on the Where tab.

   NOTE: To purge or archive events NOT captured by the agents, domains, or sites listed on the Where tab, select the **Exclude The Following Selection(s)** check box at the top of the Where tab.

To use a wildcard expression to specify agents, domains, or sites:

1. From the Purge and Archive wizard, select **Purge**, and then enable **Only selected events** to activate the criteria tabs.
2. Open the Where tab, expand **Add** and click **Add Wildcard Expression**.

   NOTE: If you used **Add With Events** instead, click **Add Wildcard Expression** on the Add Agents, Domains, Sites dialog.
3. On the Add Where dialog, enter the wildcard expression to be used to search for agents (NetBIOS name, domains or sites.
   - Select the comparison operator to be used: **Like** or **Not Like**
   - Enter the pattern (character string and * wildcard character) to be used to search for a match. Use the * wildcard character to match any string of zero or more characters.
   - By default, the wildcard expression will be used to search for agents. To search for domains or sites, select the **Domain** or **Site** option.
4. Click **OK** to close the dialog and add the wildcard expression to the Where tab.

   Change Auditor now searches for and purges or archives change events captured by the agent(s), domains or sites whose name matches the specified wildcard expression.

To filter based on server type:

1. On the Where tab, expand **Add** and select **Add Server Types**.
2. Select to include Domain Controllers, Member Servers, Workstation Servers, Exchange Servers as required.
3. Click **OK** to close the dialog and add the server type to the 'Where' list.

   When this purge job runs, Change Auditor searches for and purges events generated on the specified domains, sites, or agents for the specified server type.

Origin tab

Use the Origin tab to purge events originating from a specific workstation or server. By default, (when the Origin tab is empty) events will be purged regardless of the workstation or server from which they originated.

When multiple 'origin' criteria is specified on this tab, Change Auditor uses the 'OR' operator to evaluate events, purging or archiving events originating from any of the specified workstations or servers.

To purge events based on where they originated:

1. From the Purge and Archive wizard, select **Purge**, and then enable **Only selected events** to activate the criteria tabs.
2. Open the Origin tab and click **Add**.
3. On the Add Origin dialog, enter the wildcard expression to be used to include workstations or servers, based on their NetBIOS name or IP address:
   - Select the comparison operator to be used: **Like** or **Not Like**
   - Enter the pattern (character string and * wildcard character) to be used to search for a match. Use the * wildcard character to match any string of zero or more characters.
4. Click **OK** to close the dialog and add the wildcard expression to the Origin tab.
5. Change Auditor now searches for and purges or archives change events originating from workstations/servers whose machine name (NetBIOS name or IP address) matches the specified wildcard expression.

   NOTE: To purge or archive events not originating from the workstations or servers listed on the Origin tab, select **Exclude The Following Selection(s)** box at the top of the Origin tab.

To select an originating workstation or server that has an event in the Change Auditor database:

1. From the Purge and Archive wizard, select **Purge**, and then enable **Only selected events** to activate the criteria tabs.
2. Open the Origin tab and click **Add With Events**.

   The Add Origin dialog appears populated with originating workstations/servers that have an event associated with it in the Change Auditor database.

   NOTE: Use **Add Wildcard Expression** to enter a wildcard expression to include workstations/servers from this list based on their NetBIOS name or IP address.
3. On the Add Origin dialog, select one or more originating workstations/servers from the list and click **Add** to add it to the selection list at the bottom of the page.
4. Click **OK** to close the dialog and add the selected workstations to the Origin tab.

   Change Auditor now searches for and purges or archives change events originating from the selected workstations/servers.

To put your archive database in a high availability group:

1. Once the database has been created, ensure that the database is using SQL AlwaysOn Availability Groups and the coordinator is connecting to the availability group listener.
2. Wait for the archive job to complete.
3. Add the database to the availability group.

13

Working with Private Alerts and Reports

- Introduction
- Private Alerts and Reports page
- Disable private alerts and reports
- Move and delete private searches

Introduction

Using the Private Alerts and Reports page on the Administration Tasks tab, administrators can disable alert notifications and scheduled reports that were created under a user's Private folder and move or delete the associated search. This feature allows administrators to clean up orphaned alerts and reports in all user's private folders.

NOTE: Authorization to use the administration tasks on the Administration Tasks tab is defined using the Application User Interface page. To disable private alerts/reports using the Private Alerts and Reports page, you must be assigned to a role that contains the **View Private Alerts and Reports**, **Disable Alert** and **Disable Report** operations. If you are denied access to the tasks on this page, see Change Auditor User Interface Authorization.

This section provides instructions on how to disable private alerts/reports and how to move or delete the associated searches from the Administration Tasks tab. For a description of the dialogs mentioned in this chapter, see the online help.

Private Alerts and Reports page

The Private Alerts and Reports page is displayed when Private Alerts and Reports is selected from the Configuration task list in the navigation pane of the Administration Tasks tab and displays a list of all private search queries where alerting and/or reporting has been enabled and configured. From this page, administrators with the proper permissions can disable valid alerts and reports from a user's private folder or move or delete the associated searches.

For each private alert/report found, the following information is displayed:

Name

Displays the name assigned to the search query when it was created.

Folder

Displays the full folder path where the search query was saved.

Owner

Displays the name of the owner who created the private alert/report.

Alert

Indicates whether an alert has been enabled for the search query. Valid entries for this field are:

- **Enabled** - which means that alerting is enabled for the search query and that at least one transport method is enabled.
- **Disabled** - which means that the alert is disabled for the search query; however at least one transport method is still enabled.

Report

Indicates whether reporting had been enabled for the search query. Valid entries for this field are:

- **Enabled** - which means reporting is enabled for the search query and a report will be sent to the specified recipients as defined on the Report tab.
- **Disabled** - which means previously enabled reporting has now been disabled for the search query.

Alert To

Displays the email address of any recipients specified to receive an alert email notification (SMTP).

Alert Cc

Displays the email address of any 'carbon copy' recipients specified to receive an alert email notification.

Alert Bcc

Displays the email address of any 'blind carbon copy' recipients specified to receive an alert email notification.

Report To

Displays the email address of any recipients or shared folder specified to receive a report as defined on the Report tab.

Report Cc

Displays the email address of any 'carbon copy' recipients specified to receive a report email.

Report Bcc

Displays the email address of any 'blind carbon copy' recipients specified to receive a report email.

Disable private alerts and reports

To disable a private alert or report:

1. Open the Administration Tasks tab and click **Configuration**.
2. Select **Private Alerts and Reports** from the task list.
3. On the Private Alerts and Reports page use one of the following methods to disable a private alert/report:
   - Select the alert/report to be disabled and click the appropriate tool bar button: **Disable Alert** or **Disable Report**.
   - Select the alert/report to be disabled, right-click and select the appropriate option: **Disable Alert** or **Disable Report**.

The disabled status also appears on the Searches page for the selected search query. The user can use the commands on the Searches page to re-enable alerting/reporting for a private search query.

Move and delete private searches

Administrators can delete or move another user's private search, move them to their private searches folder, or make them public by moving them to a shared searches folder.

To move a private search:

1. Open the Administration Tasks tab and click **Configuration**.
2. Select **Private Alerts and Reports** from the task list.
3. On the Private Alerts and Reports page, select the alert/report to be moved and click **Move**.
4. Select the destination folder and click **OK**.

To delete a private search:

1. Open the Administration Tasks tab and click **Configuration**.
2. Select **Private Alerts and Reports** from the task list.
3. On the Private Alerts and Reports page, select the alert/report to be deleted and click **Delete.**
4. Click **Yes** to confirm the removal.

14

Generate and Schedule Reports

- Schedule reports for distribution
- Launch Report Designer
- Publish reports
- Print or save a page's contents

Presenting audited information in a professional, concise, and effective way is as critical as gathering the data. You can schedule reports to be sent through email (using the same SMTP configuration defined for alerts), published to Microsoft SQL Server Reporting Services (SRS) or send to a shared folder.

Change Auditor's reporting allows you to specify who can see the report and define which data to include. For example, administrators could define reports that highlight how many times a particular event or category of events occurred in the last 30 days or provide a more detailed accounting to include who made the changes, how many times, and the before and after values associated with those changes.

This section provides a description of the Report Layouts page and Report tab, which are used to define the report layout and distribution.

Schedule reports for distribution

To enable, design, and schedule reports for distribution use the following components:

- Report Layouts page (Administration Tasks tab) to create global templates that define the header and footer information for reports. See Create global report template.
- Layout tab (Search Properties tabs) to specify the data (columns) to be retrieved from the database and displayed for the selected search. In addition, you can specify the column order, sort criteria and order, and data grouping to be used for displaying the retrieved data. The settings on this tab are also used to display the search results in the client. See Define report content and layout.
- Report tab (Search Properties tabs) to enable reporting for a selected search query, specify the global template to be used or choose to design a custom report using the report designer, and schedule the distribution of the report. See Enable and schedule reporting.

Create global report template

The report templates defined on the Report Layouts page on the Administration Tasks tab define the header and footer information to include the search results report. You can use the default report template or create a custom report template using the Report Layout page.

NOTE: Use the report templates on the Administration Tasks tab to define the header and footer information for a search results report. To design a custom report layout for an individual search, including content and data layout, click **Design Report** on the Report tab (Search Properties tab) to start the Report Designer.

Report Layouts page (Administration Tasks tab)

The Report Layouts page is displayed when **Report Layouts** is selected from the Configuration task list in the navigation pane of the Administration Tasks tab. From this page you can add, edit, or delete global report templates.

The Report Layouts page contains all the report templates that have been previously defined. Initially, this list contains the Default template, which is used for all search results reports unless changed on the Report tab of a search's Search Properties tabs.

To add a global report template:

1. Open the Administration Tasks tab and click **Configuration**.
2. Select **Report Layouts** in the Configuration task list to open the Report Layouts page.
3. Click **Add** to display the New Report Layout dialog. Enter a descriptive name for the new report template and click **OK**.

   The report designer is displayed.
4. Use the controls in the toolbar to the left of the report grid to define the header and footer information to include. For example:
   - To add a page header, click the **Page Header** button. Click the report grid and the header pane is added to the top of the page. Use the arrow controls or **Height** setting in the Properties pane to resize the header pane.
   - To add the report title to the page header pane, click the **Text** button. Move the pencil cursor in the heading pane where you want to place the report title and click. Open the System Variable tab in the Text Editor, locate the **ReportName** variable. Double-click the variable to add it to the text pane. Click **OK** to save your selection and close the Text Editor.
   - Back on the report grid, you can resize the {**ReportName}** text box to prevent the report titles from being truncated. You can also use the settings in the Properties pane to modify the font, size, color, and so forth.
   - To add a page footer (for example, page number), click the **Page Footer** button. Click the report grid and the page footer pane is added to the bottom of the page. Use the arrow controls or **Height** setting in the Properties pane to resize the footer pane.
   - To add the page number to the page footer pane, click the **Text** button. Move the pencil cursor in the footer pane where you want to place the page number and click. Open the System Variables tab in the Text Editor, locate the page number variable to use (for example, **PageNofM**). Double-click the variable to add it to the text pane. Click **OK** to save your selection and close the Text Editor.

   NOTE: This is an example of how to use the report designer to add a simple header and footer. However, there are many more capabilities with the report designer which uses StimulReport.Net components. For a detailed description and functionality of each component available for designing reports, click **F1** to view the Stimulsoft online help (www.stimulsoft.com).
5. The new report template is added to the Report Layouts page (Administration Tasks tab) and is available in the **Layout** drop-down menu on the Report tab (Search Properties tabs).

Define report content and layout

For each search, built-in or custom, the data displayed in both the client and in the associated report (when reporting is enabled) is predefined. However, you can use the Layout tab of the Search Properties tabs to customize the content (columns) to display for each individual search. See Layout tab in Custom Searches and Search Properties for a detailed description of the Layout tab.

Enable and schedule reporting

When reporting is enabled, a report containing the search results of an individual search, built-in, or custom, can be sent as an attachment through email to the designated recipients or written to a shared folder. Use the Report tab, which is one of the Search Properties tabs, to enable reporting for the selected search, define the format, and how and when to distribute the report.

To email reports, you need to enable SMTP for alerting and reporting and specify the Mail Server to use in the SMTP Configuration pane on the Coordinator Configuration page. The same SMTP configuration is used for both alert notifications and reporting. See Configure email alert notifications/reports for more information.

To send reports to a shared folder, you need to enable shared folders for reports and specify the credentials that will be used to write to a shared folder. See Shared Folder Configuration for details.

Change Auditor calculates the Next Run of the reports, archive, and purge jobs based on the master time zone. For new deployments, the maser time zone is set to the time zone of the server where the first coordinator is installed. During an upgrade, the master time zone is set to UTC. You can manually change the master time zone, using the set-CAScheduleMaserTimeZone and get-CAScheduleMasterTimeZone commands. See the Change Audit PowerSell Command User Guide for details. Quest recommends that you set the master time zone to the time zone where most the users are located.

NOTE: Because Daylight Saving Time changes on different dates worldwide, Change Auditors schedules follow the time change of that specific time zone.

Report tab (Search Properties tabs)

The Report tab displays the current report configuration for the selected search definition. From the Report tab you can perform the following tasks:

- Enable and disable reporting for the current search
- Specify the format for the report attachment (PDF, Html, Word, Text, Excel, CSV)
- Select the recipients who are to receive the report through email
- Select the shared folder where you want to write a report
- Define a schedule for sending the report
- Select the template for the report's headers and footers or design a custom report layout using the report designer

Use the controls on the Report tab as described in the following table:

NOTE: All dates and times are based on the client's current local date and time. The format used to display the date and time is determined by the local computer's regional and language setting.

Table 1. Report tab: Field and Control descriptions

Field and Control	Description
Report Enabled	Select to enable reporting for the current search definition. **NOTE:** This option becomes available only after a valid address is entered in the Report Configuration section of this tab. Use an e-mail address to send a report to mailbox and a network address to send a report to a shared folder.
Report Configuration	
Layout	Specifies the report template to use for the report's headers and footers. The **Default** report template is defined for you. To define more templates, use the Report Layouts page on the Administration Tasks tab. **NOTE:** This setting is disabled if you click **Design Report** to define a custom report layout for the selected search.

Table 1. Report tab: Field and Control descriptions

Field and Control	Description
Report	Specifies if the report is generated and sent on a weekly (default) or monthly schedule. **NOTE:** When **Monthly** is selected, specify the schedule to generate the report. For example, 1 for every month (default), 2 for every other month, 6 for every six months or twice a year.
Every	When a **Weekly** report is selected, specify the schedule to use to generate the report. For example, 1 for every week (default), 2 for every other week, 3 for every third week, and 4 for every fourth week.
On Days	When a **Weekly** report is selected, define the days of the week to generate the report. The default is Monday through Friday.
On Day of Month	When a **Monthly** report is selected, specifies on which day of month to generate the report: • First (default) • Last • Day #
Run Time	Specifies the time to generate the report.
Reset	Use to reset the settings back to the factory defaults.
Send to a mailbox	Use to select the options to share reports through email. Enter the email address of one or more persons who are to receive the report. You can also use the browse button to locate and select the users who are to receive the report. Selecting this button displays one of the following dialogs: • The Select Active Directory Objects dialog (directory object picker) where you can use the Browse or Search page to locate Active Directory users. This dialog is displayed when no Exchange host is specified in the SMTP Configuration pane of the Coordinator Configuration page. • The Search Users dialog allowing you to locate and select an Exchange user (Exchange tab) or an Active Directory user (Active Directory tab). This dialog is displayed when an Exchange host is defined in the SMTP Configuration pane of the Coordinator Configuration page. Click **Expand Properties** (right arrow) to the left of the **To** field to enter additional recipients and/or change the subject. When expanded, you can enter the following information: • **To**: Enter or use the browse button to specify the email address of users who are to receive the report. • **Reply**: Enter or use the browse button to specify the email address to which reply emails are to be sent. • **Cc**: Enter or use the browse button to specify the email address of users who are to receive a copy of the report email. • **Bcc**: Enter or use the browse button to specify the email address of users who are to receive a blind copy of the report email. Click **Collapse Properties** (down arrow) to hide these additional properties and show the other settings available on the Report Configuration pane. **NOTE:** You can enter an individual email address or distribution list in any of the email address fields. Separate multiple email addresses with a semicolon.

Table 1. Report tab: Field and Control descriptions

Field and Control	Description
Send to a shared folder	Use to select a shared folder to write reports to. You must enter a network path; a local address will not be accepted. The To field is automatically populated with the default shared folder path. However, you can specify a different path. The credentials from the Shared Folder Configuration are used to write reports to the shared folder. (The credentials are specified under the coordinator configuration Shared Folder Configuration option. See Shared Folder Configuration for details.) Ensure that the account has permissions to write to the shared folder. If you change the shared folder, the new path does not display in the search grid until you refresh the searches tree (click F5 while on the searches tree).
Do not send empty reports	When selected, a report will not be sent to email or a shard folder if it does not contain any results.
Send empty report email notification	Select this to receive an email notification for a report that ran but did not contain any results. **NOTE:** This is only available if you have selected the Send to a mailbox and the Do not send empty reports options
Attach	The report is sent as an email attachment. Select the appropriate **Attach** option to define the format to be used for the report: • PDF (default) • Html • Word • Text • Excel • CSV
Columns	Defines how the report content is to fill the page: • Fit to Page (default) • Fixed Width *nn.nn* Inches/Column **NOTE:** These settings are disabled if you click **Design Report** to define a custom report layout for the selected search.
Time Zone	Specifies the time zone to be used for the time stamp in the name of the report attachment. By default, the time zone of the computer where the Change Auditor client resides is used.
Last Run	This read-only field specifies the last time (date and time) the report ran.
Next Run	This read-only field specifies the next time (date and time) when the report is scheduled to run.

To enable/schedule reporting:

NOTE: To distribute reports through email (SMTP) or to a shared folder you must first enable the corresponding configuration on the Coordinator Configuration page of the Administration Tasks tab. See Click Test Mail to test the configuration. and Shared Folder Configuration.

1 Open the Searches page.

2 Expand the **Private** or **Shared** folders in the explorer view to locate the search to which reporting is to be enabled. Select the search from the Search list in the right pane.

3 Open the Report tab.

a To share a report through email, select **Send to a mailbox**, enter a valid email address in the **To** field and then select the **Report Enabled** check box.

b To send a report to a folder, select **Send to a shared folder**, enter a valid network path in the **To** field and then select the **Report Enabled** check box.

4 Specify the report configuration settings:

- Layout: Select the report template to be used.
- Report: Specify when the report is to be generated/sent (i.e., on a weekly or monthly schedule).
- Run Time: Specify the time (based on the client's current local date and time) at which the report is to be run.
- Attach: Select the report format to be used.
- Columns: Define how the report content is to fill the page.
- Time Zone: Select the time zone to be used for the time stamp in the name of the report attachment. By default, the time zone of the computer where the Change Auditor client resides is used.

NOTE: See Table 1 for a detailed description of the report configuration settings.

5 Click **Save**.

When reporting is enabled, the following details are added to the search entry in the Searches list:

- **Report** column displays 'Enabled'
- **Report To**, **Report Cc** and **Report Bcc** columns display the email address of specified recipients or a shared folder path.

To disable a scheduled report:

1 Open the Searches page.

2 Expand the **Private** or **Shared** folders in the explorer view to locate the search whose reporting is to be disabled. Select the search from the Search list in the right pane.

3 Use one of the following methods to disable reporting for the selected search:

- Right-click the search and select **Report | Disable Report**.
- Open the Report tab and clear the **Report Enabled** check box. Click **Save**.

Launch Report Designer

The report designer in Change Auditor uses StimulReport.Net components for designing reports. For a detailed description and functionality of each component available, click **F1** to view the Stimulsoft online help (www.stimulsoft.com).

To launch the report designer:

1 Open the Searches page, locate and select a search definition.

2 Open the Report tab for the selected search and click **Design Report**.

The report designer appears allowing you to create a custom report layout for the selected search.

NOTE: Once the report designer is launched, the **Layout** and **Columns** settings on the Report tab for the selected search are disabled. To re-enable these settings, click **Reset** at the bottom of the Report tab.

Publish reports

ChangeAuditor supports Microsoft's Microsoft SQL Server Reporting Services (SRS), providing a comprehensive, server-based solution that enables the creation, management and delivery of reports.

To publish reports to a SRS server:

1. Open the Searches page.
2. Expand the **Private** and **Shared** folders and select a folder in the explorer view to display the list of search/report definitions stored in the selected folder.
3. From the right-hand pane, right-click a search/report definition and select **Publish reports using SQL Reporting Services**. This displays the Create Report dialog allowing you to configure the SQL Server Reporting services to be used and to specify the report details. (To publish a series of reports (folder), select a folder in the explorer view.)
4. If not already configured, select the Configure button to specify the reporting services and Change Auditor shared data source to be used.
   - Enter the URL of the SRS server that is to host the ChangeAuditor reports For example: http://<SQL_Server>/<ReportServer>

     Where: <SQL_Server> is the name of the server hosting SRS and <ReportServer> is the name of the report server virtual directory. (In a default Reporting Services installation, the name of the virtual directory is reportserver.)

     NOTE: You can use the **Import SRS Settings** button on the Reporting Services Setup dialog to import a SQL Reporting Services template that was previously created to define the necessary SRS settings or enter the SRS settings as defined below.
   - Enter the user account, credentials and domain for a Windows account that has permissions to copy files to SRS.

     NOTE: This Windows account requires rights to create SRS reports and data sources on the server (a.k.a. Content Manager).
   - Enter the user account and credentials to be used to access the Change Auditor database (data source).
   - Click **Test** to verify the credentials entered above.
5. Once you have entered the requested information, Change Auditor will publish the reports to the specified server, which will then be available through SQL Server Reporting Services.

Print or save a page's contents

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 options. For each Change Auditor page, the data grid as it is displayed on the page is printed, except for the following pages:

- Searches page - The search properties specified for the selected search are printed. You must select a search from the searches list in the right page to enable the print options.
- Search Results page - The data grid, pie chart or bar graph as it is displayed on this page is printed.
- Coordinator Configuration page - The settings specified in the SMTP Configuration, Group Membership Expansion and Agent Heartbeat Check panes are printed.
- AD Attributes Auditing page - The attributes selected for auditing are printed.
- ADAM (AD LDS) Attributes Auditing page - The attributes selected for auditing are printed.
- Application User Interface page - Printing is not available for this page.

To print a page:

1 Open the page to be printed and click **Print**.

2 On the Print dialog, specify your print options and the printer to use.

> **NOTE:** You may want to use the **Print | Page Setup** option in the client or **Preferences** button on the Print dialog to change the page orientation to **Landscape** and decrease the page margins prior to printing the pages that contain grids.

3 Click **Print** to close the dialog and send the displayed page to the designated printer.

To preview a report prior to printing:

1 Open the page to be printed, expand **Print** and select **Print Preview**.

2 Use the controls at the top of the preview screen to print the report, display multiple or selected pages, zoom and close the preview screen.

To save a page to a file:

1 Open the page to be saved to a file, expand **Print** and select one of the following commands:

- **Print to File**
- **Print to PDF**

2 The Save As dialog appears allowing you to specify the file name and location. Also if you clicked the **Print to File** command, you can specify the type of file to be saved (.xls, .xlsx or .csv).

15

SQL Reporting Services Configuration

- Introduction
- SQL Reporting Services Page
- SQL Reporting Services Templates
- SQL Reporting Services Wizard

Introduction

You can define SQL Reporting Services (SRS) templates that define all the necessary Report Server information (URL and credentials) and Change Auditor data source information for publishing reports. These templates can then be made available to users who choose to publish reports to SRS. That is, when an authorized user attempts to publish a report to SRS using the **Publish reports to SQL Reporting Services** right-click command on the Searches page, they can use the **Import SRS Settings** button on the Reporting Services Setup dialog to import the settings defined in a SQL Reporting Services template to publish their reports.

This section provides instructions for creating SQL Reporting Services templates, as well as a description of the SQL Reporting Services page and SQL Reporting Services wizard. For a description of the other dialogs mentioned in this chapter, refer to the online help.

NOTE: SQL Server Reporting Services (SSRS) is not supported by Azure SQL Managed Instance.

SQL Reporting Services Page

The SQL Reporting Services page is displayed when **SQL Reporting Services** in the Configuration task list is selected in the navigation pane of the Administration Tasks tab. From this page you can launch the SQL Reporting Services wizard to define the reporting services and data source information needed to publish reports to SRS. You can also edit existing templates, disable/enable templates and remove templates that are no longer being used.

The SQL Reporting Services page contains an expandable view of all the SQL Reporting Services templates that have been previously defined. To add a new template to this list, use the **Add** tool bar button. Once added, the following information is provided for each template:

Template

Displays the name assigned to the template when it was created.

Status

Indicates whether the template is enabled or disabled.

URL

This field is used for filtering data.

Authorized Accounts

This field is used for filtering data.

Click the expansion box to the left of the Template name to expand this view and display the following details:

NOTE: The cells directly under the main heading rows are used for filtering data. That is, as you enter characters into these cells, the client will redisplay the templates that meet the search criteria (i.e., comparison operator and characters entered).

URL

Displays the Report Server URL specified in the wizard.

Database

Displays the Data Source name of the database as specified in the wizard.

Authorized Account

Displays the accounts that are authorized to use this SQL Reporting Services template.

SQL Reporting Services Templates

To create a SQL Reporting Services template:

1. Open the Administration Tasks tab and select **Configuration**.
2. Select **SQL Reporting Services** in the Configuration task list to open the SQL Reporting Services page.
3. Use **Add** to start the SQL Reporting Services wizard to define the report server and data source information.
4. On the first page of the wizard:
   - Enter a name for the template.
   - Enter the URL of the SRS server that is to host the Change Auditor reports

     For example: http://<*SQL_Server*>/<*ReportServer*>

     where: <*SQL_Server*> is the name of the server hosting SRS and <*ReportServer*> is the name of the report server virtual directory. (In a default Reporting Services installation, the name of the virtual directory is **reportserver**.)
   - Enter the user account, credentials and domain for a Windows account the has permissions to copy files to SRS.

     NOTE: This Windows account requires rights to create SRS reports and data sources on the server (a.k.a. Content Manager).
   - Enter the user account and credentials to be used to access the Change Auditor database (data source).
   - Click **Test** to verify the credentials entered above.

5 On the second page of the wizard, select the user or group accounts that are authorized to use this template to publish Change Auditor reports to SRS.

> **NOTE:** The user and group accounts entered on this page are the ONLY accounts that are allowed to import the settings in this template to publish Change Auditor reports to SRS. For example, the first time an authorized user selects the **Import SRS Settings** button on the Reporting Services Setup dialog, the Change Auditor Administrators will not be able to import the settings in this template to publish reports to SRS unless they are also added as an authorized account on this page.

Use the Browse or Search pages to locate and select the accounts to be included in the template. Use the **Add** button to add these accounts to the list box at the bottom of the page.

6 Select **Finish** to create the template and return to the SQL Reporting Services page.

Now when an authorized user attempts to publish a report to SRS using the **Publish reports to SQL Reporting Services** right-click command on the Searches page, they can use the **Import SRS Settings** button on the Reporting Services Setup dialog to import the settings defined in this template to publish their reports.

To modify a template:

1 On the SQL Reporting Services page, select the template to be modified and select **Edit**.

2 This displays the SQL Reporting Services wizard, where you can modify the report server and data source settings and authorized accounts included in the template.

3 Click **Finish**.

To disable a template:

The disable feature allows you to temporarily disable the use of a template without having to remove it from Change Auditor.

1 On the SQL Reporting Services page, use one of the following methods to disable a template:

- Click in the **Status** cell for the template to disable and select **Disabled**
- Right-click the template to disable and select **Disable**

The entry in the **Status** column for the template will change to 'Disabled'.

2 To re-enable a template, use the **Enable** option in either the **Status** cell or right-click menu.

To delete a template:

1 On the SQL Reporting Services Auditing page, select the template to delete and select **Delete | Delete Template**

2 A dialog will be displayed confirming that you want to delete the selected template. Select **Yes**.

SQL Reporting Services Wizard

The SQL Reporting Services wizard is displayed when you select **Add** on the SQL Reporting Services page. Using this wizard you can define the reporting services and data source information to be included in the template, as well the user and group accounts authorized to use this template to publish reports to SRS.

The following table provides a description of the fields and controls in the SQL Reporting Services wizard.

> **NOTE:** A red flashing icon indicates that you have not yet entered the required information. A green check mark indicates that the required information has been specified and you are ready to proceed.

Table 1. SQL Reporting Services wizard

Create or modify a SQL Reporting Services Template page: Use this page to enter a name for the template and credentials to be used to access the SQL Reporting Services server and Change Auditor shared data source.

Template Name	Enter a descriptive name for the SQL Reporting Services template being created.
SQL Server Reporting Services **NOTE:** SQL Reporting Services must be configured with anonymous access disabled. **NOTE:** The account entered in this section requires rights to create SRS reports and data sources on the server (a.k.a. Content Manager).	
Report Server URL	Enter the URL for the SQL Reporting Services (SRS) server that will be hosting the Change Auditor reports. For example: http://<*SQL_Server*>/<*ReportServer*> where <*SQL_Server*> is the name of the server hosting SRS and <*ReportServer*> is the name of the report server virtual directory.
User	Enter a user name for a Windows account that has credentials to copy files to a SQL Reporting Service.
Password	Enter the password associated with the user name entered above.
Domain	Enter the domain for the Windows account to be used to access SRS.
Change Auditor Shared Data Source **NOTE:** The account specified in this section is used to create and read data from the Change Auditor data source.	
Data Source Name	Enter the name of the Change Auditor data source.
Authentication	Select the appropriate authentication method for connecting to the Change Auditor data source: • **Windows Authentication** - Select this option to use Windows authentication for connecting to the Change Auditor data source. • **SQL Server Authentication** - Select this option to use SQL Server authentication for connecting to the Change Auditor data source.
User	Enter a user name for the account to be used to access the Change Auditor data source.
Password	Enter the password associated with the user name entered above.
Domain	Enter the domain for the user account to be used to access the Change Auditor data source. This only applies to Windows Authentication.
Test	Use the **Test** button at the bottom of the dialog to verify the credentials entered in the SQL Server Reporting Services section at the top of the dialog.
Select Accounts Authorized to Use This SQL Reporting Services Service Template page When you enter a user or group account on this page, you are defining which users/groups are allowed to use this template to publish reports to SRS. That is, only users who are listed on this page (or users in any groups listed on this page) will be able to use the Import SRS Settings button on the Reporting Services Setup dialog to select this SRS template.	
Browse Page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the user or group account(s) to be included in this template. Once you have selected an account, use **Add** to add it to the list box at the bottom of the page.

Table 1. SQL Reporting Services wizard

Search Page	Use the controls at the top of the Search page to search your environment to locate the desired user or group account. Once you have selected an account, use **Add** to add it to the list box at the bottom of the page.
Options Page	Use the Options page to modify the search options or global catalog used to retrieve directory objects.
Account List	The list box located across the bottom of this page, displays the accounts that are authorized to import the SRS settings in this template to publish Change Auditor reports to SRS. Use the buttons located above this list box to add and remove objects.
Add	Select a user or group in the Browse or Search page and select **Add** to add it to the list.
Remove	Select an entry from the list and then select **Remove** to remove it.

16

Change Auditor User Interface Authorization

- Introduction
- Application User Interface Authorization page
- Add task definition
- Add role definition
- Add application group

Introduction

Role-based access control allows you to assign users/groups to roles based on their job functions and grant these roles permissions to perform related tasks. Role-based access control is broken down into the following entities to define 'who can do what':

- Operation: a single action that users need to be granted rights to perform
- Task: a collection of logically related operations
- Role: a logical group of users and the tasks they are allowed to perform

Authorization for using the different features is defined using the Application User Interface Authorization page. From the Administration tab, you can add new task and role definitions or delete user-defined roles and tasks that are no longer required.

By default, the following roles and tasks are defined; therefore, no action is required on your part to start using the client:

- AD Protection Role - has access to view Active Directory and Group Policy protection
- Administrator Role - has full administrator privileges with access to all aspects of the client, web client and deployment of agents
- Operator Role - has only operator privileges with limited access to the client (e.g. these users can define and run searches, but they cannot access the Administration, Statistics or Deployment pages) and access to perform all tasks except the administration functions in the web client
- Web Client Shared Overviews Role - has view access to the web client shared overviews; while restricting access to only what has been shared
- AD Protection Task - grants access to Active Directory and Group Policy protection tasks
- Administrator Task - grants full administrator access
- Operator Task - grants operator access only
- Restore Value Task - allow use of the Restore Value button in the Event Details pane.
- Web Client Shared Overviews Task - grants view access to web client's shared overviews

During installation, you added user accounts to the Change Auditor security groups (ChangeAuditor Administrators - <*InstallationName*> and ChangeAuditor Operators - <*InstallationName*>). These security groups

are automatically added as members of the appropriate role (Administrator Role and Operator Role). If applicable, during the web client installation, you may have also added user accounts to the ChangeAuditor Web Shared Overview Users security group. This additional security group is added as a member to the Web Client Shared Overviews role.

NOTE: The Administrator, Operator and Web Client Shared Overviews roles and tasks cannot be removed, renamed or edited.

Using the AD Protection role and task, administrators can specify who is authorized to view protection definitions for Active Directory and Group Policy objects. Using the Restore Value task, administrators can enable and disable the ability to restore values when viewing events in the Event Details pane. See the Quest Change Auditor for Active Directory User Guide for information on restricting access to specific domains and organizational units and restoring values.

This section provides a description of the Application User Interface Authorization page. It also provides instructions for adding task definitions, role definitions and application groups to define who can use the different features available in the Change Auditor client. For a description of the other dialogs mentioned in this chapter, refer to the online help.

Application User Interface Authorization page

The Application User Interface Authorization page is displayed when **Application User Interface** is selected from the Configuration task list in the navigation pane of the Administration Tasks tab.

From this page, you can define who is authorized to perform the different operations available in the Change Auditor client, including performing the administrative tasks listed on the Administration Tasks tab and defining search criteria.

The Application User Interface Authorization page contains an expandable view of the role and task definitions which define role-based access. To add a role or task, use the appropriate **Add** tool bar command: **Add | Add Role Definition** or **Add | Add Task Definition**.

Once added, the following information is provided for each definition:

Name

Displays the name assigned to the role or task definition when it was created.

Type

Indicates the type of definition:

- Role
- Task

Description

Displays the description entered when the role or task definition was created.

Click the expansion box to the left of a Role Definition to expand this view and display the following details:

Member

Displays the user and group accounts that are assigned as members of the selected role.

Type

Indicates the type of account in the selected role:

- Group

- User
- Application Group

Description

Displays the description from the Members tab of the Authorization Role dialog when the role was created.

NOTE: The cells directly under the main heading rows are used for filtering data. That is, as you enter characters into these cells, the client will redisplay the roles or tasks that meet the search criteria (i.e., comparison operator and characters entered). For more details about using the data filtering function provided throughout the Change Auditor client, see Filter data.

Add task definition

A task is a collection of operations and sometimes lower-level tasks that can be performed.

1. Open the Administration Tasks tab and click **Configuration**.
2. Select **Application User Interface** in the Configuration task list to open the Application User Interface Authorization page.
3. Expand **Add** and click **Add Task Definition**.
4. On the Task page of the Authorizations: Task dialog, enter the following information:
   - Name: Enter a name for the task
   - Description: Enter a brief description of the task
5. Open the Definition tab and add the operations and lower-level tasks that can be performed:
   - To add a lower-level task, click **Add Task** and select a task from the Authorizations: Task Definitions dialog.
   - To add an operation, click **Add Operation** and select one or more operations from the Authorizations: Operations dialog.
6. Click **OK** to save your new task definition and close the Authorizations: Task dialog.

   This task will now be included in the task list on the Authorizations: Task Definitions dialog and can be included in a role definition.

   Task definitions are also listed on the Application User Interface Authorization page.

Add role definition

A role definition defines who is authorized to perform specific tasks and/or individual operations in the client. A role usually corresponds to a job function or responsibility and consists of a collection of tasks that a user must be authorized to perform to do their job function.

1. Open the Application User Interface Authorization page.
2. Select **Add | Add Role Definition**.
3. On the Authorizations: Role dialog, enter the following on the Role tab:
   - Name: Enter a name for the role
   - Description: Enter a brief description of the role
4. Open the Definition tab to add a role, task or operation to this role:
   - To add a role, click **Add Role** and select a role from the Authorizations: Role Definitions dialog.
   - To add a task, click **Add Task** and select a task from the Authorizations: Task Definitions dialog.

- To add an operation, click **Add Operation** and select one or more operations from the Authorizations: Operations dialog.

5 Open the Members tab to add a user, group or application group to this role.

- To add an application group, click **Add Application Group**n and select an application group from the Authorizations: Application Groups dialog.
- To add a user or group, click **Add User or Group**, which will display the Select one or more Directory Objects dialog. Use the Browse page or Search page to locate and select the user and/or group accounts to add.

NOTE: If a user or group account is added to multiple access roles, the account will have the authority to perform the operations defined in the more authoritative role.

6 Click **OK** to save your new role definition and close the Authorizations: Role dialog.

Role definitions are displayed on the Application User Interface Authorization page.

Add application group

Application groups allow you an alternate way of assigning users to roles. An application group is a feature of Windows Authorization Manager (AzMan) where you can define a group of users without having to go through your domain administrator to add a new group to Active Directory.

1 Open the Application User Interface Authorization page.

2 Expand **Add** and click **Add Application Group**.

3 On the Group tab of the Authorizations: Application Group dialog, enter the following information:

- Name: Enter a name for the application group
- Description: Enter a brief description for the application group

Select one of the following methods which is to be used to define a group of users:

- Basic (default)
- LDAP Query

NOTE: Basic groups are a lot like Active Directory groups; however you can define both included and excluded members. LDAP query groups allow you to define an LDAP query to dynamically create a group of users who are similar. Refer to the Windows Authorization Manager documentation for more information on basic and LDAP query groups.

4 Open the Members tab and add the users and groups that are to be members of this application group.

- To add an application group, click **Add Application Group** and select an application group from the Authorizations: Application Groups dialog.
- To add a user or group, click **Add User or Group**, which will display the Select Active Directory Objects dialog. Use the Browse page or Search page to locate and select the user(s) and/or group(s) to be added.

5 Optionally, open the Non-Members tab and add the users and groups that are to be excluded from this application group.

- To add an application group, click **Add Application Group** and select an application group from the Authorizations: Application Groups dialog.
- To add a user or group, click **Add User or Group**, which will display the Select Active Directory Objects dialog. Use the Browse page or Search page to locate and select the user(s) and/or groups to add.

6 Click **OK** to save your new role definition and close the Authorizations: Role dialog.

7 When the selected members now try to define Active Directory protection they will be restricted to defining protection for the selected domain or organizational unit.

Remove a task definition

Authorization for operations can be removed when no longer required.

1 Open the Administration Tasks tab and click **Configuration**.

2 Select **Application User Interface** in the Configuration task list to open the Application User Interface Authorization page.

3 Right-click the required task in the list.

4 Select **Edit**.

5 Select the **Definition** tab.

6 Highlight the required operation and click **Remove**.

17

Client Authentication

- Introduction
- Client Authentication Page

Introduction

Change Auditor has the following authentication methods:

- Windows Forms Authentication (enabled by default)

  When users log in, the current Windows logon user security context is used to authenticate with the coordinator. Typically, user account and password are not required.

- Active Directory Client Certificate Authentication

  When users log in, they must specify a smart card or certificate. User account and password are not required.

This section provides information on when to use each method and how to change the type of authentication. For information on an alternate method of authentication between the client and the coordinator in environments where NTLM authentication is denied, see Certificate authentication for client coordinator communication.

Client Authentication Page

The Client Authentication page is displayed when **Client Authentication** is selected from the Configuration task list in the navigation pane of the Administration Tasks tab.

From this page, you can define the authentication method required to access a particular Change Auditor installation.

Windows Forms Authentication

When this option is enabled, Change Auditor uses the standard login entry form where users specify login Windows credentials in both the clients. Credentials are securely verified with Active Directory to authenticate user access to Change Auditor. The current Windows logon user security context is used to authenticate with the coordinator. Typically, user account and password are not required.

Active Directory Client Certificate Authentication

When this option is enabled, authentication is performed using smart cards or certificates associated with Active Directory users. This permits users to log into clients using Smart Card-based authentication technologies.

NOTE: If you are having issues using the web client, ensure that Active Directory Client Certificate Authentication is set to enabled in IIS configuration at the server level. Also verify that your IIS server certificates are correctly configured.

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

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

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

Changing authentication methods

If you move from the default Windows Forms Authentication to Active Directory Client Certificate Authentication:

- A coordinator is required on each IIS server where the Change Auditor web client is installed. Installing the coordinator on the same computer as the IIS web server allows Change Auditor to securely and reliably authenticate the user account by its certificate without transmitting any credentials on the network.

  For more information see the Installation Guide and follow the Change Auditor Coordinator Setup wizard to install a new coordinator.
- Each web client will need to be configured to use the coordinator that is on the local IIS server. The web client will use this particular coordinator for accessing your Change Auditor installation. If a web client is already installed and using a different coordinator, it will need to be uninstalled, and re-installed to use the local coordinator. A reinstall is also necessary to change the web server configuration to allow Active Directory Client Certificate Authentication.
- Before you install the web client, ensure that your system meets the following minimum requirements:
  - IIS web server is configured with appropriate certificates to support Smart Cards.
  - Web site exists and is configured to use the HTTS protocol.
  - Active Directory Client Certificate mapping authentication is enabled in IIS on a server level.
  - Change Auditor coordinator is installed locally on the computer where you plan to install the web client.

If you move from Active Directory Client Certificate Authentication to Windows Forms Authentication, you will need to:

- Uninstall and re-install the web client. A re-install is necessary to change the web server configuration to allow Windows Forms Authentication.

To change the authentication method

1. Open the Administration Tasks tab and click **Configuration**.
2. Select **Client Authentication** in the Configuration task list to open the Client Authentication page.
3. Select the required method and click **Apply**.

   Because this is a significant change which may require the re-deployment of Change Auditor components, you are presented with a confirmation dialog. Select **Yes** to continue or **No** to return to the Client Authentication page.

18

Certificate authentication for client coordinator communication

- Introduction
- Installation settings
- Deployment
- Windows client configuration

Introduction

The following section provides information on configuring and maintaining certificate authentication between the client and coordinator in environments where NTLM restrictions are in place.

NOTE:

- When using certificate authentication for client / coordinator authentication, the option to use Active Directory Client Certificate Authentication for the client in the Client Authentication page is not available.
- For information on connecting to a coordinator with certificate authentication using PowerShell refer to the Connect-CAClient, Find-CASuitableCoordinator, and Install-CALicenses commands in the Change Auditor PowerShell User Guide.

Installation settings

The default Change Auditor installation includes the following configuration:

- Windows authentication for the connection between the Windows client and the coordinator.
- Coordinator and agent services run with the local system computer account.

In environments with stringent security requirements, administrators can:

- Restrict NTLM in their Active Directory domains by enabling and changing one or more of the following group policy settings:
  - Network security: Restrict NTLM: Incoming NTLM traffic.
  - Network security: Restrict NTLM: NTLM authentication in this domain.
  - Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers.
- Configure the coordinator to run with an alternate service account.

When these security options are in place, the default Windows authentication cannot be used for client - coordinator communication; instead certificate authentication can be used.

Deployment

Certificates are required for both the coordinators and the clients that connect to them. In a default deployment, administrators can use:

- Domain Certificate Services with default templates for user and computer certificates that manage deployment details such as certificate properties, deployment requests, and the certificate stores and folders.
- Manual certificate deployment and manually-created self-signed certificates are also supported for evaluation or other low-security purposes.

When using certificate authentication, the following must be in place:

- Each server that hosts a coordinator must have a valid, trusted certificate with at least the “Server authentication” and “Client authentication” purposes located in the Local Machine\Personal certificate store. The certificate must include the private key. The trust chain of the certificate must evaluate to a trusted root CA certificate in the “Trusted Root Certification Authorities” Certificates folder of the coordinator host and all client hosts. Peer (“Trusted People”) trusts are not supported.
- Each client must have a valid, trusted certificate with at least the “Client authentication” purpose located in the User\Personal certificate store. The certificate must include the private key. The trust chain of the certificate must evaluate to a trusted root CA certificate in the “Trusted Root Certificate Authorities” Certificates folder of the client host and all coordinator hosts. Peer trusts are not supported. Active Directory or IIS certificate identity mapping of client certificates is not required, and is not used by Change Auditor if provided.
- When self-signed certificates are used, Certificate Revocation List checking must be disabled as described in Coordinator configuration.

Coordinator configuration

To configure certificate authentication on a coordinator:

1. Ensure a valid Server authentication certificate is deployed on the host server.
2. Install the Change Auditor coordinator as described in the Change Auditor Installation Guide.

> **NOTE:** When specifying the Coordinator SQL Server information, connections using Windows authentication may fail if NTLM restrictions are in place and the SQL server specified is not excepted from the restrictions. In this case the use of SQL authentication is recommended.

3. Stop the coordinator, if it is running.
4. In the Coordinator installation folder (located by default in Program files\Quest\ChangeAuditor\Service). Make a backup copy of the ChangeAuditor.Service.exe.config file, then open the file using a text editor such as Notepad.exe.
5. Under the <configuration> <appSettings file=””> nodes, locate the <add key="WcfAuth" value="Windows" /> node and change the value from “Windows” to “Certificate”.

   If you are using self-signed certificates (without Certificate Revocation List information), locate the <add key="DisableCrlCheck" value="false" /> node and change the value from “false” to “true”.

   By default a suitable service certificate is selected from the Local Machine\Personal certificate store automatically. If an alternate certificate in the Local Machine\Personal certificate store is required, locate the <add key="ServiceCertificate" value="" /> node and change the value from “” (empty string) to the thumbprint string copied from a certificate found in the certlm.msc Certificate Manager for Local Machine applet in the User\Personal certificate store. Ensure that the certificate is trusted, is not expired, has a private key and at least the “Server Authentication” (“Ensures the identity of a remote computer”) purpose.
6. Save the changes to the file and restart the coordinator.

Windows client configuration

NOTE:

- Before starting, ensure that a valid client authentication certificate is deployed to the client host computer if any coordinator is configured for certificate authentication.

You can manage the connection profile for coordinators configured for certificate authentication by selecting **Manage** on the Connection screen. The following information and options are available:

- The Connection Profiles displays **Yes** in the **Certificate Auth** column if the coordinator is configured for certificate authentication; and **No** if configured for the default Windows authentication. From here, you can also see the current certificate subject field and expiration date.
- When the **Override automatic client certificate selection for the current user** option is enabled, users can specify an alternate certificate from the Current User's Personal certificate store.
- When you select to add or edit a manual connection, you will have the option to **Use WCF Certificate Authentication** and **Disable Certificate Revocation List Check**. When specifying the coordinator service properties, these check boxes must reflect the options for which the coordinator is configured.

  NOTE: These options do not apply to the Forest, Global Catalog and Database Direct connection methods.

- When using a connection profile for the first time, or one for which credentials have not been saved with the "Remember Me" option, the user is prompted for the credentials of a domain user with the Change Auditor security group membership appropriate to the user's role (such as Operator or Administrator).

19

Integrating with On Demand Audit

- Managing a Quest On Demand Audit integration
- Creating an On Demand Audit configuration
- Working with an On Demand Audit configuration

Managing a Quest On Demand Audit integration

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

On Demand Audit can provide a single view of activity across hybrid Microsoft environments. By sending Change Auditor Active Directory, Group Policy, Logon Activity, and File System Activity event data, you can gain visibility to on premises changes.

Historical data sent to On Demand Audit is as follows:

- Trial On Demand Audit subscription: 24 hours.
- Full On Demand Audit subscription: All events in Change Auditor. (Any events collected prior to Change Auditor 7.0.0 will not be included.)

By integrating Change Auditor with Quest On Demand Audit, you will gain access to:

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

Creating an On Demand Audit configuration

An On Demand Audit subscription is required before you can configure the connection to Change Auditor.

NOTE: If you do not currently have a subscription, you can select to register for a free 30 day trial. Once you have registered, you can sign in and configure the connection between Change Auditor and On Demand Audit.

NOTE: To create the configuration, you must use the email from the account that created the On Demand subscription or have been delegated the appropriate permissions from your On Demand administrator.

To delegate the required permissions, the On Demand Audit administrator must add the required accounts to the Auditing Administrator role through the On Demand Access page.

NOTE: Once a configuration is in place, all coordinators which belong to the Change Auditor Installation will be registered with On Demand Audit.

To create a configuration with On Demand Audit, Change Auditor clients and coordinators must be able to access specific URLs. See the Quest On Demand Audit User Guide for details.

To send events to On Demand Audit, Change Auditor coordinators must be able to access specific URLs. See the Quest On Demand Audit User Guide for details.

IMPORTANT: If the only coordinator in the Installation is removed for any reason the On Demand Audit subscription will become unavailable. Once a new coordinator is deployed, set all deprecated coordinators to "Uninstalled" status in the Change Auditor client under View | Statistics | Coordinator. Once complete, recreate the On Demand Audit subscription under View | Administration | Configuration | On Demand Audit. Event forwarding will continue from the last forwarded event.

To create a configuration

1. From the **Administration Tasks**, select **Configuration | On Demand Audit**.
2. Select **Sign in and Configure** to create the connection.
3. Enter your Quest account credentials to sign in to On Demand Audit.
4. Choose the required organization if prompted and click **Select Organization**.

   By default, the current installation is used for the configuration name. If required, you can enter a different name for the configuration. This is the configuration name used in On Demand Audit; it does not change the Change Auditor installation name.
5. Click **Finish**.

   On Demand Audit will now create the subscription and Change Auditor will begin to send events.

Working with an On Demand Audit configuration

You can view the On Demand Audit configuration details in Change Auditor; however, the configuration is managed (paused, started, or removed) through On Demand Audit. See the On Demand Audit User Guide for details.

To view existing details of the subscription created by the configuration:

1. From the **Administration Tasks**, select **Configuration | On Demand Audit**.
2. Click **Refresh** to update the information.

   The following subscription information is displayed.

Table 1. Subscription properties

Property	Description
ActiveBatchSize	The current batch size. (The current number of events to include in a single notification message.) The batch size is automatically adjusted based on network throughput and system performance. Its value never exceeds the specified batch size.
AllowedCoordinators	List of coordinators permitted to send events.
BatchSize	Batch size. (The maximum number of events that the active batch size can increase to.)
BatchesSent	Number of batches sent.
Enabled	Whether the subscription is enabled.
EventsSent	Number of events sent.
LastCoordinator	The coordinator that is sending events. If the subscription is disabled, this is the last coordinator that sent events.
LastEventResponse	The last event response. Provides the response in JSON format from the event receiver.
LastEventTimeUTC	When the last event was sent.
NotificationInterval	How often how often (in milliseconds) notifications are sent.
StartTimeUTC	Starting point in time for events being sent.
Subscription Id	The subscription ID.
Subsystems	Subsystems that contain the event data being sent.
Webhook Subscription Id	The webhook subscription ID.

To pause, start, or remove a configuration

1 From the **Administration Tasks**, select **Configuration | On Demand Audit**.

2 Click the link to access On Demand Audit.

20

Enable/Disable Event Auditing

- Introduction
- Audit Events page
- Enable/disable event auditing
- Modify event's severity level or event class description
- Define events to be captured based on results
- View event information

Introduction

You can enable/disable the auditing of individual events so that Change Auditor is auditing only those events that are vital to your organization's operation. In addition, you can modify the severity level (high, medium, or low) and description assigned to each event. The severity level is used when processing events and to help you in determining the potential level of risk associated with each configuration change event.

This section provides a description of the Audit Event page (Administration Tasks tab) which is used to enable/disable event auditing and modify an event's severity level or description. In addition, it provides information on how to set up Change Auditor to capture events based on the results of the operation performed in the event.

Audit Events page

The Audit Events page is displayed when **Audit Events** is selected from the Auditing task list in the navigation pane of the Administration Tasks tab, and lists all of the events available for auditing. It also displays the facility and subsystem to which the event belongs, the severity assigned to each event, if the event is enabled or disabled and the type of license that is required.

NOTE: Changes made on this page are global and will apply to all Change Auditor agents.

The Audit Events page contains an alphabetical list of all the Change Auditor events, including the following information:

Table 1. Audit Events page: Field descriptions

Column	Description
Severity	Indicates the severity level assigned to each event: • Low • Medium • High When your cursor is placed in this cell, a drop-down arrow is added allowing you to change an event's severity setting.
Facility Name	Displays the name of the facility to which each event belongs.

Table 1. Audit Events page: Field descriptions

Column	Description
Event Class	Displays a descriptive title for each event.
Status	Indicates whether the event is enabled or disabled. When your cursor is placed in this cell, a drop-down arrow is added allowing you to either enable or disable the event.
License Type	Displays the type of Change Auditor license required for each event: • Any License • Active Directory • AD Query • EMC • Exchange • File System • Logon Activity • NetApp • SharePoint • SQL
Results	Displays the result criteria used to capture change events. That is, you can use the options in this column to specify if an event is to be captured based on the results of the operation mentioned in the event. • All Results (default) • Success Only • Success and Failed Only • Success and Protected Only For example, if you only want to capture successful events where the operation occurred as stated in the event, you would set this to **Success Only**. Then, if the change was prevented from occurring as stated in the event (because the object was protected by Change Auditor or the operation was prevented due to a factor/setting outside of Change Auditor's control) the associated event would not be captured.
Subsystem	Displays the name of the subsystem to which each event belongs.

Enable/disable event auditing

You can enable or disable events to best suit your organization. To view or modify the current event auditing settings, use the Audit Events page, which is accessible through the Administration Tasks tab.

NOTE: If event logging is enabled, enabling or disabling events in Change Auditor does not impact this setting and events will continue to be sent to the appropriate Windows event log.

To disable/enable individual events:

1. Open the Administration Tasks tab and click **Auditing**.
2. Select **Audit Events** (under the Configuration heading in the Auditing task list) to display the Audit Events page.
3. To disable an event, select one or more enabled events and click **Disable**. (Use the **Shift** or **Ctrl** keys to select multiple events.)

4 To enable an event,select one or more disabled events and click **Enable**. (Use the **Shift** or **Ctrl** keys to select multiple events.)

NOTE: You can also disable or enable an event using the **Disable/Enable** tool bar button at the top of the Event Details pane on a Search Results page.

Modify event's severity level or event class description

Each event has been assigned a severity level and a description, which can also be changed based on your organization's operation. To view or modify the current event auditing settings, use the Audit Events page, which is accessible through the Administration Tasks tab.

To modify an event's severity level:

1 Open the Audit Events page.

2 Select one or more events and click the appropriate Severity (**High, Medium** or **Low**) tool bar button. Use the **Shift** or **Ctrl** keys to select multiple events.

3 To reset an event's severity to the factory default, select one or more events and click **Default**.

To modify an event class description:

1 Open the Audit Events page.

2 Select the event from the list and click **Edit**.

This displays the Rename dialog listing the existing description and allowing you to enter a new description for the selected event.

3 In the New field, enter the new description for the selected event and click **OK**.

Define events to be captured based on results

The Results column on the Audit Events page allows you to specify if an individual event is to be captured by Change Auditor based on the results of the operation performed in the event. That is, you can specify to capture an individual event based on the following results:

- All Results - capture event regardless of the result returned.
- Success Only - capture event only if the operation occurred as stated in the event.
- Success and Failed Only - capture event if the operation occurred as stated in the event or if it was prevented due to a factor/setting outside of Change Auditor's control.
- Success and Protected Only - capture event if the operation occurred as stated in the event or if it was prevented because the object was protected using Change Auditor's protection feature.

To change the results criteria for capturing an event:

1 Open the Audit Events page.

2 Locate the event to modify.

3 Place your cursor in the **Results** cell for that event, click the arrow control and select one of the following options:

- All Results (default)
- Success Only
- Success and Failed Only
- Success and Protected Only

4 Change Auditor will now only capture and return the event if the operation mentioned if the event meets the results criteria selected.

View event information

Change Auditor provides access to the associated Event Reference Guide which contains detailed descriptions for each event, including how Change Auditor detected the configuration change event, what the changed parameter controls, and the consequence of such a change.

To view the event reference guide:

1 Open the Audit Events page.

2 Select an event from the list and click **Knowledge Base**.

21

Account Exclusion

- Introduction
- Excluded Accounts Auditing page
- Excluded Accounts templates
- Excluded Accounts wizard

Introduction

Account exclusion allows you to define a list of trusted accounts to exclude from auditing. This enables you to exclude events generated by accounts that make a large number of changes or by accounts which are trusted.

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

1. Create an Excluded Accounts template which specifies the user and/or computer accounts that are to be excluded from the auditing process. For more information on creating a template, refer to Excluded Accounts templates.
2. Add this template to an agent configuration. For more information on how to add a template to an agent configuration, refer to Define agent configurations.
3. Assign the agent configuration to Change Auditor agents. For more information on how to assign an agent configuration to an agent, refer to Assign agent configurations to server agents.

This section provides instructions for creating Excluded Accounts templates, as well as a description of the Excluded Accounts page and Excluded Accounts wizard. For a description of the other dialogs mentioned, refer to the online help.

Excluded Accounts Auditing page

The Excluded Accounts Auditing page is displayed when **Excluded Accounts** is selected from the Auditing task in the navigation pane of the Administration Tasks tab. From this page you can launch the Excluded Accounts wizard to create a new template. You can also edit existing templates, disable/enable templates, and remove templates that are no longer being used.

The Excluded Accounts Auditing page contains an expandable view of all the Excluded Accounts templates that have been defined. To add a new template to this list, use the **Add** tool bar button. Once added, the following information is provided for each Excluded Accounts template:

Template

Displays the name assigned to the template when it was created.

Status

Indicates whether the template is enabled or disabled. To enable/disable the template, place your cursor in this **Status** cell, click the arrow control and select the appropriate option from the drop-down menu.

Account

This field is used for filtering data.

Operations

If specified, displays the event classes and/or facilities specified on the first page of the wizard that are to be excluded for the account.

Click the expansion box to the left of the Template Name to expand this view and display the following details about the template:

Type

Displays the type of account (i.e., user, computer or group) selected for exclusion as specified on the second page of the wizard.

Account

Displays the name of the account selected for exclusion.

Display Name

If available, displays the display name assigned to the excluded accounts listed.

NOTE: The cells directly under the main heading rows are used for filtering data. That is, as you enter characters into these cells, the client will redisplay the templates that meet the search criteria (i.e., comparison operator and characters entered). For more details about using the data filtering function provided throughout the client, see Filter data.

Excluded Accounts templates

To exclude accounts from auditing, you must first create an Excluded Accounts template which specifies the user or computer accounts that are to be excluded. You can then add this template to an agent configuration, which then needs to be assigned to the appropriate agents.

To create an Excluded Accounts template:

1. Open the Administration Tasks tab and click **Auditing**.
2. Select **Excluded Accounts (**under the Configuration heading in the Auditing task list) to open the Excluded Accounts Auditing page.
3. Click **Add** to start the Excluded Accounts wizard which will step you through the process of creating an Excluded Accounts template.
4. On the first page of the wizard, enter the following information:
   - **Template Name** - Enter a name for the template.
   - Optionally select the facilities/event classes to be excluded.
     - To add individual event classes, select one or more events from the displayed list and click **Add | Add This Event**.
     - To add all the events in a facility, select an event from the facility and click **Add | Add All Events in Facility**.

   After providing a name and optionally selecting the facilities/event classes to be excluded, click **Next**.
5. On the second page of the wizard, select the accounts that are to be excluded from auditing.

   Use the Browse or Search pages to locate and select the account to be excluded. Click **Add** to add the selected account to the list box at the bottom of the page.

If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.

Repeat this step to add additional accounts to the exclusion list.

6 (Optional) To specify a wildcard search expression to dynamically exclude additional user accounts from auditing, click **Next**.

On the Select Accounts to Exclude using Wildcards page, add the accounts to be excluded from auditing. In the text box, enter the wildcard expression (string of characters and/or wildcard character) to be used to search the Domain(NetBIOS)\NT 4 account name for matching users:

- Use an asterisk (*) to substitute zero or more alphanumeric characters.
- Use a question mark (?) to substitute a single alphanumeric character.

Click **Add** to add the string to the Account list.

NOTE: This page should be used to exclude multiple users that match the wildcard search expression. Explicitly named user accounts must be specified on the previous page of the wizard.

7 After specifying the accounts to be excluded, click **Finish** to create the template without assigning it to an agent configuration.

Clicking **Finish** creates the template, closes the wizard and returns to the Excluded Accounts Auditing page, where the newly created template will now be listed.

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

This displays the Configuration Setup dialog, allowing you to select the agent configuration to which the template is to be assigned.

NOTE: Back on the Excluded Accounts Auditing page, you can also use the Assign tool bar button to assign the selected template to an agent configuration. Clicking this button will display the Configuration Setup dialog allowing you to select the agent configuration to which this template is to be assigned.

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

NOTE: If you do not refresh the agent's configuration, the agent 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.

To modify an Excluded Accounts template:

1 On the Excluded Accounts Auditing page, select the template to be modified and click **Edit**.

2 This displays the Excluded Accounts wizard, where you can modify the current list of accounts included in the template.

3 Click **Finish** or expand the **Finish** button and click **Finish and Assign to Agent Configuration**.

To disable an Excluded Accounts template:

Disabling allows you to temporarily stop excluding the specified accounts without having to remove the auditing template.

1 On the Auditing page, use one of the following methods to disable an auditing template:

- Place your cursor in the **Status** cell for the template to be disabled, click the arrow control and select **Disabled**.
- Right-click the template to be disabled and select **Disable**.

The entry in the **Status** column for the template will change to 'Disabled'.

2 To re-enable the auditing template, use the **Enable** option in either the **Status** cell or right-click menu.

To delete an Excluded Accounts template:

1 On the Auditing page, select the template to be deleted and click **Delete | Delete Template**.

2 A dialog will be displayed confirming that you want to delete the selected template. Click **Yes**.

To delete an account from an Excluded Accounts template:

1 On the Excluded Accounts Auditing page, select the account to be deleted and click **Delete | Delete Excluded Account**,

2 A dialog will be displayed confirming that you want to delete the account from the template. Click **Yes**.

NOTE: If the account is the last one in the template, deleting this account will also delete the template.

Excluded Accounts wizard

The Excluded Accounts wizard is displayed when you click **Add** on the Excluded Accounts Auditing page. This wizard steps you through the process of creating a new Excluded Accounts template, identifying the user, computer or group accounts to be included in the template. You will also use this wizard to modify a previously defined Excluded Accounts template.

The following table provides a description of the fields and controls in the Excluded Accounts wizard:

NOTE: A red flashing icon indicates that you have not yet entered the required information. Hovering your cursor over this icon displays a tool tip explaining what needs to be entered.

Table 1. Excluded Accounts wizard

Create or modify an Excluded Accounts Auditing Template page On the first page of the wizard, enter a name for the template and optionally select the event classes/facilities to be excluded.	
Template Name	Enter a descriptive name for the Excluded Accounts template being created.
Facility/Event Class data grid	The data grid located across the middle of the page displays all of the event classes available for auditing in Change Auditor. By default, all event classes/facilities will be excluded for the selected accounts. To exclude individual event classes and/or facilities, use this grid to select the event classes and/or facilities to be excluded and use **Add** to add them to the Exclusion list box at the bottom of the page. **NOTE:** The Change Auditor Internal Auditing facility or events CANNOT be excluded.

Table 1. Excluded Accounts wizard

Exclusion list	The list box located at the bottom of this page displays the individual event classes or facilities selected for exclusion. Use the buttons above this list box to add or remove entries from this list. • **Add | Add This Event** - Click this option to add the selected events to the list box. This option is selected by default when more than one event is selected in the data grid. • **Add | Add All Events in Facility** - Click this option to add all of the events in the selected facility to the list box. This option is only available when a single event is selected in the data grid. • **Remove** - Select an entry in the list box and click the **Remove** button to remove it from the template. **NOTE:** If you want to exclude all event classes/facilities for the selected account, this list box will be empty.
Select Accounts to Exclude page (a.k.a. Directory object picker)	
Use this page to select the individual accounts to be excluded from auditing.	
Browse page	Displays a hierarchical view of the directory objects in your environment allowing you to locate and select the accounts to excluded from auditing. If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog. Once you have selected an account, click **Add** to add it to the list box at the bottom of the page.
Search page	Use the controls at the top of the Search page to search your environment to locate the desired account. Once you have selected an account, click **Add** to add it to the list box at the bottom of the page.
Options page	Use the Options page to modify the search options used to retrieve directory objects.
NOTE: For more information on using the Browse, Search or Options pages, refer to Directory object picker.	
Account list	The list box located across the bottom of this page, displays the accounts selected for exclusion. Use the buttons located above this list box to add and remove objects. • **Add** - Select an account in the Browse or Search page and click **Add** to add it to the list. • **Remove** - Select an entry from the list and then click **Remove** to remove it.
(Optional) Select Accounts to Exclude using Wildcards page	
Use this page to optionally add additional user accounts (Domain(NetBIOS)\NT 4 account) that match a wildcard search expression to the excluded accounts list.	
NOTE: This page should be used to exclude multiple users that match the wildcard search expression. Explicitly named user accounts must be specified on the previous page of the wizard.	

Table 1. Excluded Accounts wizard

Search expression	In the text box, enter the string of characters and/or wildcard character to be used to search for additional user accounts that are to be excluded from auditing. Valid wildcards are: • Use an asterisk (*) to substitute zero or more characters. • Use a question mark (?) to substitute a single character. Click **Add** to add the string to the Account list.
Account list	The list at the bottom of the page displays the wildcard search expressions to be used to search for additional user accounts that are to be excluded from auditing. Use the buttons to the left of the text box to add, remove and modify a search expression. • **Add** - Click **Add** to add the search expression in the text box to the Account list. • **Remove** - Select an entry in the Account list and click **Remove** to remove it from the list. • **Modify** - Select an entry in the Account list, make the necessary changes to the search expression (which is displayed in the text box) then click the **Modify** button to replace it in the Account list. **NOTE:** If you click **Add** after modifying a search expression, an additional entry will be added instead of replacing the original search expression.

22

Registry Auditing

- Introduction
- Registry Auditing page
- Registry Auditing templates
- Registry Auditing wizard

Introduction

The ability to audit registry settings improves operational efficiency dramatically. For example, some applications, such as virus scanning software, modify registry keys when an update is installed. By capturing these change events proactively, administrators can determine whether or not specific machines received an update.

Furthermore, other applications may warrant the tracking of modifications to certain registry settings to ensure that they have not been tampered with. Change Auditor's registry auditing feature allows you to audit changes to a specific key or to a folder and its sub folders.

To capture registry events, you must define the registry keys to be audited and the events to be captured:

1. Create a Registry Auditing template which specifies the registry keys and events to be audited. For more information on creating a Registry Auditing template, refer to Registry Auditing templates.
2. Add this template to an agent configuration. For more information on adding a Registry Auditing template to an agent configuration, refer to Define agent configurations.
3. Assign the agent configuration to agents. For more information on assigning an agent configuration to an agent, refer to Assign agent configurations to server agents.

NOTE: Event logging is disabled by default; and when enabled, only configured activities will be captured in the Windows event log.

This section provides instructions for creating Registry Auditing templates, as well as a description of the Registry Auditing page and Registry Auditing wizard. For a description of the other dialogs mentioned in this chapter, refer to the online help.

Registry Auditing page

The Registry Auditing page is displayed when **Registry** is selected from the Auditing task list in the navigation pane of the Administration Tasks page. From this page you can launch the Registry Auditing wizard to specify a registry key to be audited. You can also edit existing templates, disable/enable templates and remove templates that are no longer being used.

The Registry Auditing page contains an expandable view of all the Registry Auditing templates that have been previously defined. To add a new template to the list, use the **Add** tool bar button. Once added, the following information is provided for the template:

Template

Displays the name assigned to the template when it was created.

Status

Indicates whether the template is enabled or disabled. To enable/disable the template, place your cursor in this **Status** cell, click the arrow control and select the appropriate option from the drop-down menu.

Registry Keys

This field is used for filtering data.

Click the expansion box to the left of the Template name to expand this view and display additional details about an auditing template.

Registry Key

Displays the name of the file path for the registry key in the HKEY_LOCAL_MACHINE hive which was selected for auditing on the Key page of the wizard.

Status

Indicates whether auditing of the registry key is enabled or disabled. To enable/disable the auditing of the registry key, place your cursor in this **Status** cell, click the arrow control and select the appropriate option from the drop-down menu.

Scope

Displays the scope selected for this template on the Key page of the wizard:

- This object only
- This object and child objects only
- This object and all child objects

Value

If applicable, this column displays the specific value selected for auditing (only applies to **This object and child objects only** scope).

Operations

Displays the events selected for auditing on the Events page of the wizard. Hover your mouse over this cell to view all of the events included in the template.

Exclude

Displays the names of the sub keys to be excluded from auditing as specified on the Exclusions tab of the wizard.

NOTE: The cells directly under the main heading rows are used for filtering data. That is, as you enter characters into these cells, the client will redisplay the templates that meet the search criteria (i.e., comparison operator and characters entered). For more details about using the data filtering function provided throughout the Change Auditor client, see Filter data.

Registry Auditing templates

To enable custom registry auditing you must create a Registry Auditing template which specifies the registry keys and events to audit. You can then assign this template to an agent configuration, which then needs to be assigned to the appropriate agents.

To create a Registry Auditing template:

1. Open the Administration Tasks tab and click **Auditing**.
2. Select **Registry** (under the Server heading in the Auditing task list) to open the Registry Auditing page.
3. Click **Add** to start the Registry Auditing wizard which will step you through the process of creating a Registry Auditing template.
4. Enter a name for the template.
5. Enter or use one of the Browse options to locate and select the registry key in the HKEY_LOCAL_MACHINE hive to be audited.
   - Selecting the **Browse | Local Registry** option displays the Select registry key dialog allowing you to select a registry key from the local server.
   - Selecting the **Browse | Remote Registry** option displays the Select Active Directory Object dialog allowing you to select the server whose registry you would like to browse. Use the Browse or Search pages to locate and select the server. On the Select registry key dialog select the registry key to be audited.

   Once you have selected the registry key to be audited, click **Add** to add it to the selection list.

   Repeat this step to add additional registry keys to the template.
6. For each registry key listed, select the key in the list and perform steps 8 - 11 to specify the scope, events, values and optionally any sub keys that are to be excluded.
7. In the **Scope** cell, use the drop-down menu to select the scope of coverage:
   - This object only
   - This object and child objects only
   - This object and all child objects (default)
8. On the Events tab select the key and value events that are to be included in the audit.

   NOTE: Selecting the **Key Events** or **Value Events** check box at the top of the events list on the Events tab will select all of the events listed under the heading. Similarly, clearing the check boxes will clear all of the selected events.
9. If you selected the **This object and child objects only** option in the **Scope** cell, you can also specify a specific value for the selected key. To audit a specific value, open the Value tab and enter the value in the text box provided.
10. (Optional) On the Exclusions tab, add the names of any sub keys to be excluded from auditing. Use one of the Browse options to locate and select a sub key under the selected registry key to be excluded from auditing:
    - Selecting **Browse | Local Registry** displays the Select registry key dialog allowing you to select a sub key from the local server.

- Selecting **Browse | Remote Registry** displays the Select Active Directory Object dialog allowing you to select the server whose registry you would like to browse. Use the browse or search pages to locate and select the server. From the Select registry key dialog, select the sub key to be excluded.

NOTE: If you select a sub key that does not belong to the selected registry key, the wizard will not allow you to continue. A red flashing icon is displayed indicating that you have selected a sub key outside of the selected registry key.

You can also enter the name of the sub key to be excluded or use a file mask to select a group of sub keys. A file mask can contain any combination of the following:

- Fixed characters such as letters, numbers and other characters allowed in sub key names.
- Asterisk (*) wildcard character to substitute zero or more characters.
- Question mark (?) wildcard character to substitute a single character.

Once you have specified a sub key for exclusion, click **Add** to add it to the Exclusions list at the bottom of the page.

Repeat this step to add additional sub keys to the Exclusions list.

11 To create the template without assigning it to an agent configuration, click **Finish**.

Clicking **Finish** creates the template, closes the wizard and returns to the Registry Auditing page, where the newly created template will now be listed.

12 To create the template and assign it to an agent configuration, expand **Finish** and click **Finish and Assign to Agent Configuration**.

This will display the Configuration Setup dialog allowing you to select the agent configuration to which this template is to be assigned.

NOTE: On the Auditing page, you can also use the **Assign** tool bar button to assign the selected template to an agent configuration. Clicking this button will display the Configuration Setup dialog allowing you to select the agent configuration to which this template is to be assigned.

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

NOTE: If you do not refresh the agent's configuration, the agent 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.

To modify a Registry Auditing template:

1 On the Registry Auditing page, select the registry key whose properties are to be modified, and click **Edit**.

2 This displays the Registry Auditing wizard, where you can modify the following properties:

- Registry key
- Scope
- Events (Events tab)
- Value (Value tab)
- Excluded sub keys (Exclusions tab)

3 Once you have made your modifications, click **Finish** or expand **Finish** and click **Finish and Assign to Agent Configuration**.

To disable a Registry Auditing template:

Disabling allows you to temporarily stop auditing the specified registry key without having to remove the auditing template or individual registry key from an active template.

1 On the Auditing page, place your cursor in the **Status** cell for the template to be disabled, click the arrow control and select **Disabled**.

The entry in the **Status** column for the template will change to 'Disabled'.

2 To re-enable the auditing template, use the **Enable** option in either the **Status** cell or right-click menu.

To disable the auditing of a registry key in an auditing template:

1 On the Registry Auditing page, place your cursor in the **Status** cell for the registry key to be disabled, click the arrow control and select **Disabled** from the drop-down menu

The entry in the **Status** column for the registry key will change to 'Disabled'.

2 To re-enable the auditing of a registry key, use the **Enable** option in either the **Status** cell or right-click menu.

To delete a Registry Auditing template:

1 On the Auditing page, select the template to delete and click **Delete | Delete Template**.

2 A dialog will be displayed confirming that you want to delete the selected template. Click **Yes**.

To delete a registry key from an auditing template:

1 On the Registry Auditing page, select the registry key to delete and click **Delete | Delete Registry Key**

2 A dialog will be displayed confirming that you want to delete the registry key from the template. Click **Yes**.

> **NOTE:** If the registry key is the last one in the template, deleting this registry key will also delete the template.

Registry Auditing wizard

The Registry Auditing wizard displays when you click **Add** on the Registry Auditing page. From this wizard, select the registry key to be audited as well as the events to be audited.

The following table provides a description of the fields and controls in the Registry Auditing wizard.

> **NOTE:** A red flashing icon indicates that you have not yet entered the required information. Hovering your cursor over this icon displays a tool tip explaining what needs to be entered. A green check mark indicates that the required information has been specified and you are ready to proceed.

Table 1. Registry Auditing wizard

Create or modify a Registry Auditing Template page	
Use the first page of the wizard to enter a name for the template and select the registry keys to audit.	
Template Name	Enter a descriptive name for the Registry Auditing template being created.
Registry key in the HKEY_LOCAL_MACHINE hive	Enter or use one of the browse options to select the registry key in the HKEY_LOCAL_MACHINE hive to be audited.

Table 1. Registry Auditing wizard

...	Expand the browse button to browse for and select a registry key: • **Local Registry** - select this option to browse and select a registry key from the local computer • **Remote Registry** - select this option to browse and select a registry key from a remote server. Selecting this option displays the Select Active Directory Object dialog allowing you to select the server whose registry you would like to browse. Use the browse or search pages to locate and select the server. **NOTE:** Make sure that the selected remote computer is on the network, has remote administration enabled and that both computers are running the remote registry service. If the remote computer does not allow remote admin access, a message will be displayed explaining that you need to select a different server.
Registry Keys list	The list box located across the middle of the page displays the registry keys to be included in the Registry Auditing template. Use the **Add** and **Remove** buttons to control the contents of this list: • **Add** - Use this to add the specified registry key to the template. • **Remove** - Select a registry key from the list and click the **Remove** button to remove the selected registry key from the template. Use the drop-down box in the **Scope** cell of the list box to specify the scope of coverage: • **This object only** - select this option to audit only this key, not its values or sub keys. • **This object and child objects only** - select this option to audit this key, its values and direct sub keys only. This is not recursive. • **This object and all child objects** - select this option to audit this key, all sub keys and all values. (Default) Select a key in this list to enable the corresponding Events, Value and Exclusions tabs at the bottom of this page.
Events tab	
Use the Events tab to select the type of events (e.g., registry key added, registry key deleted) that are to be audited for the selected registry key. The contents of this tab is based on the entry selected above in the Registry Keys list.	
Key Events	Select the Key events to audit. Select the **Key Events** check box to select all of the Key events listed or select individual events from the list.
Value Events	Select the Value events to audit. Select the **Value Events** check box to select all of the Value events listed or select individual events from the list.
Value tab	
If you selected the **This object and child objects only** option in the **Scope** cell, this additional tab will be displayed allowing you to enter a specific value to be audited for the selected key.	
Audit a specific value	Enter the value to be audited for the selected key.
Exclusions tab (Optional)	
Use the Exclusions tab to exclude sub keys in the selected registry key from being audited.	

Table 1. Registry Auditing wizard

Add the sub keys to exclude from auditing	To exclude a sub key in the selected registry key from being audited, expand the browse button and select one of the browse options to browse either the local or remote server for the sub key. You can also enter the name of the sub key to be excluded from auditing. Use a file mask to select a group of sub keys. A file mask can contain any combination of the following: • Fixed characters such as letters, numbers and other characters allowed in the name of sub keys. • Asterisk (*) wildcard character to substitute zero or more characters. • Question mark (?) wildcard character to substitute a single character. Once you have specified a sub key for exclusion, click the **Add** button to add it to the Excluded Keys list at the bottom of the page.
...	Expand the browse button and select one of the following options: • **Local Registry** - select this option to select a sub key from the local server. • **Remote Registry** - select this option to select a sub key from a remote registry. Selecting this option displays the Select Active Directory Object dialog allowing you to select the server whose registry you would like to browse. Use the browse or search pages to locate and select the server. **NOTE:** Make sure that the selected remote computer is on the network, has remote administration enabled and that both computers are running the remote registry service. If the remote computer does not allow remote admin access, a message will be displayed explaining that you need to select a different server.
Excluded Keys list	The list across the bottom of this page contains the sub keys that are to be excluded from auditing. Use the **Add** and **Remove** buttons to add and remove entries. • **Add** - Use the **Add** button to add the specified sub key to the Excluded Keys list. • **Remove** - Select an entry in the Excluded Keys list and click the **Remove** button to remove it.

23

Service Auditing

- Introduction
- Services Auditing page
- Service Auditing templates
- Service Auditing wizard

Introduction

Windows services are the backbone of applications and require frequent administrator actions. Changes can be simple, such as changing a startup type or service account password. But, even the simple changes can cause major issues. In fact, in this case it would render an application useless to its users. Change Auditor provides service auditing capabilities, including the ability to track who starts and stops a service.

To capture service events, you must first define the services to audit:

1. Create a Service Auditing template to specify the system services to audit or exclude from auditing. For more information about creating a template, see Service Auditing templates.
2. Add this template to an agent configuration. For more information about how to add a template to an agent configuration, see Define agent configurations.
3. Assign the agent configuration to Change Auditor agents. For more information about how to assign an agent configuration to an agent, see Assign agent configurations to server agents.

NOTE: Event logging is disabled by default; and when enabled, only configured activities are captured in the Windows event log.

This section provides instructions for creating Service Auditing templates, as well as a description of the Service Auditing page and Service Auditing wizard. For a description of the other dialogs mentioned in this chapter, refer to the online help.

Services Auditing page

The Services Auditing page is displayed when **Services** is selected from the Auditing task list in the navigation pane of the Administration Tasks tab. From this page, you can start the Service Auditing wizard to define the system services to include in the auditing template. You can also edit existing templates, disable and enable templates and remove templates that are no longer being used.

The Service Auditing page contains an expandable view of all the Service Auditing templates that have been previously defined. To add a new template to this list, use the **Add** tool bar button. Once added, the following information is provided for each template:

Template

Displays the name assigned to the template when it was created.

Status

Indicates whether the template is enabled or disabled. To enable and disable the template, place your cursor in this **Status** cell, click the arrow control, and select the appropriate option from the drop-down menu.

Exclude

Displays the option selected to determine which services are included or excluded from auditing:

- Audit ALL
- Audit all EXCEPT
- Audit ONLY

Services

This field is used for filtering data.

When individual services have been included in a Service Auditing template, click the expansion box to the left of the Template name to expand this view and display the following details:

Service

Displays the name of the services included in the template.

Status

Indicates whether auditing of the service is enabled or disabled. To enable and disable the auditing of the service, place your cursor in this **Status** cell, click the arrow control, and select the appropriate option from the drop-down menu.

Display Name

Displays the display name for the listed services.

NOTE: The cells directly under the main heading rows are used for filtering data. That is, as you enter characters into these cells, the client redisplays the templates that meet the search criteria (that is, comparison operator and characters entered). For more details about using the data filtering function provided throughout the client, see Filter data.

Service Auditing templates

To enable service auditing, create a Service Auditing template to specify the system services to audit or to exclude from auditing. You can then assign this template to an agent configuration, which then needs to be assigned to the appropriate Change Auditor agents.

To create a Service Auditing template:

1. Open the Administration Tasks tab and click **Auditing**.
2. Select **Services** (under the Server heading in the Auditing task list) to open the Services Auditing page.

3 Click **Add** to start the Service Auditing wizard which allows you to define the system services to be included in the template.

4 Enter a name for the template.

5 Select one of the following options to define whether this template is to include or exclude system services for auditing:

- Audit ALL services (default)
- Audit ALL services except the following
- Audit ONLY the following services

6 If you selected either the **Audit ALL services except the following** or the **Audit ONLY the following services** option, the data grid is activated allowing you to select the services to be included or excluded depending on the option selected.

From the services listed:

- Select one or more services and click **Add** to move them to the list box.
- Select **Add All** to move all the services,

OR

- Select **Enter a service not listed above** to enter an unlisted service.

7 To view the services on a different server, click the browse button to the far right of **You are viewing services on**.

Clicking the browse button displays the Select a Directory Object dialog, where you can use either the **Browse** or **Search** pages to locate and select a different server. After selecting the server, click **Select** to close the dialog and display the services found on the selected server.

8 To create the template without assigning it to an agent configuration, click **Finish**.

Clicking **Finish** creates the template, close the wizard and return to the Services Auditing page, where the newly created template is listed.

9 To create the template and assign it to an agent configuration, expand **Finish** and click **Finish and Assign to Agent Configuration**.This displays the Configuration Setup dialog allowing you to select the agent configuration to which this template is to be assigned.

NOTE: Back on the Auditing page, you can also use the Assign button to assign the selected template to an agent configuration. Clicking this button displays the Configuration Setup dialog allowing you to select the agent configuration to which this template is to be assigned.

10 On the Agent Configuration page, select the agents assigned to use the modified agent configuration and click **Refresh Configuration** to ensure that the agents are using the latest configuration.

NOTE: If you do not refresh the agent's configuration, the agent automatically checks for a new agent configuration based on the polling interval setting (on the System Settings tab of the Configuration Setup dialog). The default is every 15 minutes.

To modify a template:

1 On the Services Auditing page, select the template to modify and click **Edit**.

This displays the Service Auditing wizard, where you can modify the current list of services included in the template.

2 Click **Finish** or expand **Finish** and click **Finish and Assign to Agent Configuration**.

To disable a template:

Disabling allows you to temporarily stop auditing the specified service without having to remove the auditing template or individual service from an active template.

1 On the Auditing page, place your cursor in the **Status** cell for the required template, click the arrow control, and select **Disabled**.

The entry in the **Status** column for the template changes to 'Disabled'.

2 To re-enable the auditing template, use the **Enable** option in either the **Status** cell or right-click menu.

To disable the auditing of a service in a template:

1 On the Services Auditing page, place your cursor in the **Status** cell for the required service, click the arrow control, and select **Disabled**

The entry in the **Status** column for the service changes to 'Disabled'.

2 To re-enable the auditing of a service, use the **Enable** option in either the **Status** cell or right-click menu.

To delete a template:

1 On the Auditing page, select the required template and click **Delete | Delete Template**.

2 A dialog displays confirming that you want to delete the selected template. Click **Yes**.

To delete a service from an auditing template:

1 On the Services Auditing page, select the required service and click **Delete | Delete Service**.

2 A dialog displays confirming that you want to delete the service from the template. Click **Yes**.

NOTE: If the service is the last one in the template, deleting this service will also delete the template.

Service Auditing wizard

The Service Auditing wizard is displayed when you click **Add** on the Services Auditing page. Using this wizard you can define the system services to be included in the template.

The following table provides a description of the fields and controls in the Service Auditing wizard.

NOTE: A red flashing icon indicates that you have not yet entered the required information. Hovering your cursor over this icon displays a tool tip explaining what needs to be entered.

Table 1. Service Auditing wizard

Create or modify a Service Auditing Template page Use this page to enter a name for the template and select the services that are to be audited.	
Template Name	Enter a descriptive name for the Service Auditing template being created.
Inclusion/Exclusion options	Select one of the following options to define whether this template is to include or exclude system services for auditing: • **Audit ALL services (default)** • **Audit ALL services except the following** • **Audit ONLY the following services**
Service data grid	If you selected either the **Audit ALL services except the following** or the **Audit ONLY the following services** option, the data grid will be activated allowing you to select the services to be included or excluded depending on the option selected. Select the services to be included in the template and click **Add** to add them to the list box at the bottom of the dialog.

Table 1. Service Auditing wizard

You are viewing services on	Displays the name of the server from which the service data grid was populated. Use the browse button to the right of this field to select a different server. The services found on the selected server will then be displayed.
Services list	The list box located across the bottom of the page displays the individual services to be included in the Services Auditing template. Use the buttons above this list box to add or remove services. • **Add** - Use the **Add** button to add the service(s) selected in the Services data grid to the list. • **Add All** - Use the **Add All** button to add all of the services listed in the Service data grid to the list. • **Remove** - Select a service entry in the list and click the **Remove** button to remove it from the template (move it back into the Services data grid). **NOTE:** If you want to audit all services, this list will be empty.

24

Agent Statistics and Logs

- Introduction
- Agent Statistics page
- Agent system tray icon
- View agent status/statistics
- Manage Change Auditor agents
- Agent Log page
- View and save agent trace logs

Introduction

In addition to the overview information provided in the Top Agent Activity pane and Agent Status pane on the Overview page, you have two additional means of obtaining agent status and statistics:

- The Agent Statistics page provides a global view of all installed (and if selected, uninstalled) Change Auditor agents, including the current status and other usage statistics for each agent.
- The Change Auditor Agent Status dialog, which is accessed using the Change Auditor agent system tray icon, provides the status and usage statistics for a single agent.

You can also view or retrieve agent trace logs from the Agent Statistics page or by using the agent system tray icon.

This section provides a description of the Agent Statistics page as well as the agent system tray component and explains how to use these features to maintain agents.

Agent Statistics page

Use the **View | Statistics | Agent** menu command (or **Ctrl+F11**) to display the Agent Statistics page, which provides a global view of all installed agents. This page contains the following components:

- Agent Statistics grid, located at the top of the page, consists of a list of agents and their current status and usage statistics.
- Resource Properties pane, located across the bottom of the page, displays additional information about the selected agent.

Agent Statistics grid

NOTE: When agents are connected or disconnected, an Agent Status message will be displayed in the lower right corner of your screen. You can use the **View Agent Statistics** link in this message box to display the Agent Statistics page.

The Agent Statistics grid may contain the following information for each agent. The default column identifies the fields that are displayed by default. To display different fields, click the **Field Chooser** button located to the far left of the column headings and select the columns to be displayed:

NOTE: All dates and times are based on the client's current local date and time. The format used to display the date and time is determined by the local computer's regional and language setting.

Table 1. Agent Statistics page: Field descriptions

Column	Default	Description
Active Directory	No	Indicates whether custom Active Directory auditing or protection has been defined.
ADAM	No	Indicates whether custom ADAM (AD LDS) auditing or protection has been defined.
Agent	Yes	Displays the NetBIOS name of the server that hosts a Change Auditor agent.
Agent FQDN	No	Displays the fully qualified domain name of the agent.
Architecture	No	Displays whether the agent is installed in a 32-bit (x86) or 64-bit (x64) environment.
Configuration	No	Displays the agent configuration assigned to the agent.
Coordinator	No	Displays the computer name of the Change Auditor coordinator(s) to which the agent is connected.
DB Size	Yes	Displays the size of the agent database.
Domain	Yes	Displays the name of the domain where the agent is located.
EMC	No	Indicates whether the agent is assigned to an EMC Auditing template to capture EMC events.
Events Last 24 Hours	No	Displays the number of events encountered on the agent during the past 24 hours from when the dialog is initially opened during the current client session. The value in this field is a hypertext link and when selected launches a quick search to display the events generated in the last 24 hours.
Events Last Hour	No	Displays the number of events encountered on the agent in the last 60 minutes from when the dialog is initially opened during the current client session. The value in this field is a hypertext link and when selected launches a quick search to display the events generated in the last 60 minutes.
Events Today	Yes	Displays the number of events encountered on the agent since 12:00 a.m. of the current day (based on the relative coordinator computer's time). The value in this field is a hypertext link and when selected launches a quick search to display the events generated today.
Events Total	Yes	Displays the number of events encountered since the agent was started. The value in this field is a hypertext link and when selected launches a quick search to display all events encountered since the agent was started.
Events Yesterday	No	Displays the number of events encountered between 12:00 a.m. yesterday and 12:00 a.m. of the current day (based on the relative coordinator computer's time). The value in this field is a hypertext link and when selected launches a quick search to display the events generated yesterday.
Exchange	No	For agents hosting Exchange, this column indicates whether Exchange Mailbox auditing or Exchange Mailbox protection has been defined.
Exchange Server	No	Indicates whether the server is an Exchange Server.

Table 1. Agent Statistics page: Field descriptions

Column	Default	Description
Exclude Account	No	Indicates whether an Excluded Accounts Auditing template has been assigned to the agent's configuration.
File System	No	Indicates whether a File System Auditing template or File System Protection template has been assigned to the agent's configuration.
Forest	No	Displays the name of the forest where the agent resides.
Group Policy	No	Indicates whether Group Policy protection has been defined.
IP Address	No	Displays the IP address of the agent.
Last Update	Yes	Displays the date and time when the agent configuration was last updated.
Load	Yes	Displays the load status of the agent service in regards to processing events. Valid entries are: • Normal - agent service is running and processing events as expected • Medium - agent service has more than 100 events waiting • Critical - agent service has reached a critical load and events may be missed • Unknown - agent service is inactive; therefore, the load is unknown
NetApp	No	Indicates whether an agent is assigned to a NetApp Auditing template to capture NetApp filer events.
Registry	No	Indicates whether a Registry Auditing template has been assigned to the agent's configuration.
Service	No	Displays whether a Service Auditing template has been assigned to the agent's configuration.
SharePoint	No	Indicates whether an agent is assigned to a SharePoint Auditing template to capture SharePoint events.
SQL	No	Indicates whether a SQL Auditing template has been assigned to the agent's configuration.
Startup Time	No	Displays the date and time when the agent was last initialized.
Status	Yes	Displays the current status of the agent: • active • inactive • uninstalled
Type	No	Displays the agent platform: • Domain Controller • Global Catalog • Server • Workstation
Uptime	Yes	Displays how long the agent has been running.
Version	No	Displays the version number of the agent currently deployed.
Workstation	No	Indicates whether this is a workstation agent.

In addition to selecting the fields to display, you can use the drop-down controls to define what servers/workstations are to be included on the Agent Statistics page.

The following table describes how to use these controls to filter the content displayed on the Agent Statistics page.

Table 2. Agent Statistics page: Filter controls

Control	Description
Type	Use the left-most control to specify the type of objects to be included in the display: • **All** - select to view all agented servers and workstations (default) • **DCs** - select to view agented domain controller servers • **Servers** - select to view agented servers regardless of domain membership • **Workstations** - select to view agented workstations (including workstations joined to the domain and workstation agents manually installed on non-Active Directory computers)
Active Directory view	By default, the Agent Statistics page provides a forest view of the servers found. However, you can use the right-most controls to limit your view to an individual domain or site. Use the middle control to select the Active Directory view (forest, domain or site) then use the right-most control to select an individual forest, domain or site for which servers are to be displayed.

Resource Properties pane

The Resource Properties pane located across the bottom of the Agent Statistics page contains additional information about the agent selected in the Agent Statistics grid.

To display the Resource Properties pane:

1 To display this pane, select an agent from the Agent Statistics grid and click **Show Properties.**

2 Use the hide button in the upper right-hand corner of the Resource Properties pane to hide this pane.

NOTE: The Resource Properties pane also appears when you select **Related Search | View Resources** on an Event Details pane. When accessed using the Event Details pane, the additional information is for the server referenced in the selected event.

The Resource Properties pane is divided into the following tabbed pages:

- Machine Info page
- Processors page
- Drives page
- Shares page
- Services page
- Exchange Mailboxes page

Machine Info page

The Machine Info page contains the following operating system and hardware-related information for the selected server.

Table 3. Resource Properties pane: Machine Info page field descriptions

Field	Description
TimeZone	The local machine's time zone.
Offset (Hours)	The amount of time the unitary computer system is offset from Coordinated Universal Time (UTC).

Table 3. Resource Properties pane: Machine Info page field descriptions

Field	Description
Operating System	
The left pane contains the following operating system details:	
OS	The operating system running on the machine.
Version	The operating system version running on the machine.
Installed	The date and time when the operating system was installed on the machine.
Last Restart	The date and time when the machine was last restarted.
Language	The language version of the operating system installed.
SKU	The unique identifying number (SKU) assigned to the machine.
Service Pack	The version number of the latest Service Pack installed on the system.
Windows	The Windows directory of the operating system.
Computer System	
The right pane contains the following computer system information:	
Computer	The full name assigned to the computer.
Host Name	The name of the local computer according to the domain name server (DNS).
Domain	The domain to which the agented server belongs.
Domain Role	The role assigned to the computer within a domain workgroup. Possible values include: • 0: Standalone Workstation • 1: Member Workstation • 2: Standalone Server • 3: Member Server • 4: Backup Domain Controller • 5: Primary Domain Controller
Model	The manufacturer's model number for the computer.
Roles	A list of the roles assigned to the system.
System Type	The type of system running on the Windows-based computer.
Physical Memory	The total amount of memory installed on the machine.

Processors page

The Processors page contains the following information about the processors on the selected server.

Table 4. Resource Properties pane: Processors page field descriptions

Field	Description
AddressWidth	The size (or width) of the address bus, which indicates the maximum amount of RAM a processor can address. Possible values include: • 32: 32-bit operating system • 64: 64-bit operating system
Architecture	The processor architecture used by the platform. Possible values include: • 0: x86 • 1: MIPS • 2: Alpha • 3: PowerPC • 5: ARM • 6: Itanium-based systems • 9: x64
Caption	A short description (one line string) for the object.
DataWidth	The size (or width) of the external data bus, which defines the rate at which data can be moved into or out of the processor. Possible values include: • 32: 32-bit operating system • 64: 64-bit operating system
ExtClock	The external clock frequency, in MHz.
Family	The processor family type.
L2CacheSize	The amount of cache memory available for the Level 2 processor cache.
L2CacheSpeed	The clock speed, in MHz, of the Level 2 processor cache.
L3CacheSize	The amount of cache memory available for the Level 3 processor cache.
L3CahceSpeed	The clock speed, in MHz, of the Level 3 processor cache.
Manufacturer	The name of the company that manufactured the processor.
MaxClockSpeed	The maximum clock speed, in MHz, for the processor.
Name	The label assigned to the processor.
NumberOfCores	The number of cores for the current instance of the processor.
NumberOfLogical Processors	The number of logical processors for the current instance of the processor.
OtherFamilyDescription	The processor family type.
ProcessorId	The processor identifier that describes the processor features.
ProcessorType	The primary function of the processor. Possible values include: • 1: Other • 2: Unknown • 3: Central Processor • 4: Math Processor • 5: DSP Processor • 6: Video Processor
Revision	The architecture-dependent system revision level.
Stepping	The revision level of the processor in the processor family.
UniqueId	The globally unique identifier for the processor.

Table 4. Resource Properties pane: Processors page field descriptions

Field	Description
Version	The architecture-dependent processor revision number.
VoltageCaps	The voltage capabilities of the processor. Possible values include: • 1: 5 volts • 2: 3.3 volts • 4: 2.9 volts

Drives page

The Drives page contains the following information about the drives that are configured on the selected server.

Table 5. Resource Properties pane: Drives page field descriptions

Field	Description
DeviceID	The unique identifier assigned to the disk drive.
InterfaceType	The interface type of the physical disk drive.
Manufacturer	The name of the company that manufactured the disk drive.
Model	The manufacturer's model number of the disk drive.
Partitions	The number of partitions contained on the physical disk drive.
Size	The size of the disk drive.

Shares page

The Shares page contains the following information about the shared resources that are configured for the selected server.

Table 6. Resource Properties pane: Shares page field descriptions

Field	Description
AllowMaximum	The maximum number of concurrent users that can connect to the shared resource.
Caption	A short comment that describes the shared resource.
Name	The alias assigned to the path set up as a shared resource.
Path	The fully qualified path to the shared resource.

Services page

The Services page contains the following information about the services installed on the selected server.

Table 7. Resource Properties pane: Services page field descriptions

Field	Description
Description	A comment that explains the purpose of the service.
DisplayName	The display name used by user interface programs to identify the service.
Name	The unique name assigned to the installed service.
PathName	The fully qualified path of the executable file for the service.
ProcessId	The process identifier of the service.

Table 7. Resource Properties pane: Services page field descriptions

Field	Description
ServiceType	The type of service provided to calling processes: • Kernel Driver • File System Driver • Adapter • Recognizer Driver • Own Process • Share Process • Interactive Process
StartMode	The start mode of a Windows base service: • Boot: Device driver started by the operating system loader. • System: Device driver started by the operating system initialization process. • Auto: Service that is to be started automatically by the Service Control Manager during system startup. • Manual: Service that is to be started by the Service Control Manager when a process calls the StartService method. • Disabled: Service that cannot be started.
StartName	The name of the account under which the service should run.
State	The current state of the service: • Stopped • Start Pending • Stop Pending • Running • Continue Pending • Pause Pending • Paused • Unknown

Exchange Mailboxes page

For Exchange Mailbox servers, the Exchange Mailboxes page displays a list of the Exchange mailbox databases on the selected server.

Agent system tray icon

An agent icon in the system tray allows you to enable, disable, or display the status of the agent installed on the current server.

NOTE: The agent system tray icon is only available for server agents.

Whenever an agent is not active, a status indicator will appear in the lower left corner of this icon to represent its current status:

- Red - inactive
- Yellow - initializing

You can load the agent system tray icon using one of the following methods:

- Click **Advanced Options** on the Deployment page to launch the Advanced Deployment Options dialog. From this dialog, select the **Yes** option for the **Launch ServiceStatusTray on startup** setting.

  NOTE: By default, the **Do not change** option is selected which indicates that you want to use the current setting for the agent system tray icon. That is, if you already have it set to launch on startup it will continue to operate that way. Similarly, it will not launch on startup if this is a clean install and you have not previously set it up to do so.

- Navigate to %ProgramFiles%\Quest\ChangeAuditor\Agent and double-click on the ServiceStatusTray.exe file.

By right-clicking on the agent system tray icon, a context menu is displayed which consists of the following commands:

Table 8. Agent system tray icon: Right-click commands

Command	Description
Agent Status	Displays the Change Auditor Agent Status dialog which assists you in determining if the agent is running, what version is installed, and how active the agent is. See Change Auditor Agent Status dialog for a full description of this status dialog.
Enable/Disable Agent	Starts or stops the agent service.
Find More Connections / Retry Connections	Looks for more coordinators in a forest than the agent automatically found. **NOTE:** An agent automatically connects to a coordinator in its own site. However, if a coordinator is not available in the site it will then search for a coordinator in the forest. When the agent is connected to a coordinator that is not currently running, use the **Retry Connections** command to reattempt to connect to a coordinator.
Refresh Configuration	Applies a new agent configuration to the selected agent. **NOTE:** This command only available when the coordinator to which the agent is connected is running.
Coordinator Credential Configurator	Use to enter the credentials of the agent that can be used to find and connect to a coordinator in an Active Directory forest. **NOTE:** This command is only available when you install a agent on a workgroup server.
View Agent Log	Opens the log viewer to review the events recorded in the Change Auditor agent log (ChangeAuditor.AgentLog.nptlog). For example: %ProgramFiles%\Quest\ChangeAuditor\Agent\Logs\ChangeAuditor.AgentLog.nptlog
Load on startup	Automatically loads the system tray application when the agent service starts.
About	Displays information about the agent including the installed version number and licensing information.
Exit	Closes the system tray application.

Change Auditor Agent Status dialog

The Change Auditor Agent Status dialog helps you determine if the agent is running and what version is installed on the domain controller. The other status information in the dialog is broken down into the following sections:

- **Agent Information** - displays the status, version number, the coordinator installation name to which the agent is connected, and the agent's database size
- **Events** - displays audit event activity
- **Coordinator Connection** - displays information regarding the connection between the agent and the coordinators

This dialog contains the following status information:

Table 9. Change Auditor Agent Status dialog: Status information

Field	Description
Agent Information	
Agent is	The current agent status: • Running - the agent service is running • Initializing - the agent service has started but is still initializing • Not Running - the agent service is not currently running • Failed - the agent service failed to initialize
Version	The current version of the agent installed on the server.
Installation Name	The installation name assigned to the coordinator to which the agent is connected.
DB Size (KB)	The size of the agent database, in kilobytes. This is dependent on the number of monitored Active Directory, registry and file system objects, and the number of events queued for transmission to the coordinator. If a coordinator is not available, this database may become large. When the events are successfully sent to a coordinator, the database space is re-used for subsequent events.
License	The licenses that are applied. Use the arrow controls to scroll through the licenses.
Events	
Contains indicators of internal Change Auditor activity and may be used by Quest Support should they need to diagnose agent problems.	
AD Events	If licensed (Change Auditor for Active Directory), this is the number of Active Directory related events processed by the agent. This field will be blank for agents running on member servers.
ADAM Events	If licensed (Change Auditor for Active Directory), this is the number of ADAM events processed by the agent.
Exchange Events	If licensed (Change Auditor for Exchange) and configured, this is the number of Exchange Mailbox events processed by the agent.
Local Security Events	If licensed (Change Auditor for Active Directory), this is the number of local user and group (SAM) events processed by the agent.
File System Events	If licensed (Change Auditor for Windows File Servers) and configured, this is the number of File System events processed by the agent.
Registry Events	If configured, this is the number of Registry events processed by the agent.
SQL Events	If licensed (Change Auditor for SQL Server) and configured, this is the number of SQL Server events processed by the agent.
NetApp Events	If licensed (Change Auditor for NetApp) and configured, this is the number of NetApp filer events processed by the agent.
EMC Events	If licensed (Change Auditor for EMC) and configured, this is the number of EMC events processed by the agent.
SharePoint Events	If licensed (Change Auditor for SharePoint) and configured, this is the number of SharePoint events processed by the agent.

Table 9. Change Auditor Agent Status dialog: Status information

Field	Description
Microsoft Entra Events	If licensed (Change Auditor for Active Directory) and configured, this is the number of Microsoft Entra events processed by the agent.
ADFS Events	If licensed (Change Auditor for Logon Activity) and configured, this is the number of ADFS events processed by the agent.
Logon Events	If licensed (Change Auditor for Logon Activity User), this is the number of user logon activity events processed by the agent.
Microsoft 365 Events	If configured (Change Auditor for Exchange and Change Auditor for SharePoint), this is the number of Exchange Online, SharePoint Online, and OneDrive for Business events processed by the agent.
Other Events	This is the number of events processed by the agent that do not 'fit' into the other event categories (such as Authentication Services events, Service events, etc.).
Excluded Events	If configured, this is the number of events excluded by the agent because they originated from a user or computer that was defined as an excluded account.
Coordinator Connection	
Connected	The computer name (and SCP port) of the coordinators to which this agent is currently connected. **NOTE:** For more details on agent connection behavior, see Installation Notes and Best Practices in the Quest Change Auditor Installation Guide.
All	The list of all available coordinators in the installation.
Last Conf Update	The time when the agent last downloaded the agent configuration information/settings.
Events Last Sent	The local time when the last event was sent. If no events have been detected by Change Auditor recently, this time may be fairly old.
Events Sent	The number of events that have been sent to a coordinator since the agent was last started.
Acknowledged	The number of events that a coordinator has acknowledged. Normally, this value will be the same as the **Events Sent**. However, it may be smaller if the coordinator is not running or if a large number of events are being processed by the coordinator which may be slowing it down. Events may also be lost due to communication problems, in which case the agent will try to re-send the events.
Events Waiting	The number of events in the agent database that are waiting to be forwarded to a coordinator. This value should be at or near zero when the server is idle, but can grow if it is busy. If the value never returns to zero, it may indicate that the agent is having difficulty communicating with the coordinator service. If this is the case, contact Technical Support for assistance.

View agent status/statistics

To view agent status/statistics (Overview page):

1. Open the Overview page and if the Top Agent Activity pane is not displayed, click the arrow on the heading of one of the overview panes and select **Top Agent Activity**.

   This pane displays the top most active agents in your environment, based on the data range specified.

2. By default, the agent activity on all servers for the past month, excluding uninstalled agents, is displayed. Use the controls at the top of this pane to specify the type of agented objects to be included as well as the date range.

3. The values in the Audited Events column are links, which when selected will open up a new Search Results tab to display the related details for these events.

4 If the Agent Status pane is not displayed, click the arrow on the heading of one of the overview panes and select one of the following commands:

   - **Agent Status | Enterprise View**
   - **Agent Status |** *<domain>*

5 By default, this pane will only include active and inactive (installed) agents in the pie chart. You can however, select the **Show Uninstalled Agents** check box to include agents that are set as 'uninstalled' in the pie chart.

6 Double-clicking the pie chart will display the Agent Statistics page.

To view agent status/statistics (Agent Statistics page):

1 Open the Agent Statistics page and click **Refresh** to retrieve updated information.

2 Click **Show Uninstalled Agents** to include uninstalled agents. Click **Hide Uninstalled Agents** to exclude uninstalled agents from the display.

   The values in the different event columns are links, which when selected will open up a new Search Results tab to display the related details for these events.

To view agent status/statistics on the current agent only (agent system tray icon):

NOTE: The agent system tray icon can be loaded using one of the following methods:

- Click **Advanced Options** on the Deployment page to display the Advanced Deployment Options dialog. From this dialog, select the appropriate **Launch ServiceStatusTray on startup** option (**Yes** or **Do not change**).
- Navigate to %ProgramFiles%\Quest\ChangeAuditor\Agent and double-click the ServiceStatusTray.exe file.

1 Right-click the system tray icon and select **Agent Status**.

   This opens the Change Auditor Agent Status dialog, which displays agent information (including if the agent is running), event activity for the agent and coordinator connection information.

2 Click **OK**.

Manage Change Auditor agents

NOTE: You can use the **Action | Agent Notifications** menu command to hide (or display) the desktop notifications that are displayed when these processes are performed.

To stop an agent (Agent Statistics page):

1 Open the Agent Statistics page.

2 Select the agent to stop and click **Stop Agent**.

   NOTE: The **Stop Agent** command is only available when an agent is 'Active'.

3 An information message is displayed, click **OK** to stop the agent.

4 In addition, a desktop notification is displayed in the lower right-hand corner of your screen explaining that the selected agent is being disconnected from a specific coordinator.

   Once disconnected, the agent's status will be changed to 'Inactive' on the Agent Statistics page.

5 If you so choose, click **Set Agent Uninstalled** to flag the selected agent as 'Uninstalled'.

6 Click **Show Uninstalled Agents** to include uninstalled agents in the Agent Statistics list. Click **Hide Uninstalled Agents** to exclude uninstalled agents from the display.

To stop an agent (agent system tray icon):

NOTE: The agent system tray icon is only available for server agents.

1. From the server where the agent is installed, right-click the agent system tray icon and select **Disable Agent**.
2. On the confirmation dialog, click **Yes** to stop the agent service.
3. A message displays explaining that the agent is being stopped.
4. In addition, a desktop notification displays in the lower right-hand corner of your screen explaining that the selected agent is being disconnected from a specific coordinator.

   Once disconnected, the agent system tray icon contains a red light indicating that the agent is inactive.

To start an agent (Agent Statistics page):

1. Open the Agent Statistics page.
2. Select a previously stopped agent and click **Start Agent**.

   NOTE: The **Start Agent** command is only available when an agent is 'Inactive'.

3. An information message displays explaining that it may take a few minutes to start the agent. Click **OK** to start the agent.
4. In addition, a desktop notification displays in the lower right-hand corner of your screen explaining that the selected agent is being connected to a specific coordinator.

   Once connected, the agent's status returns to 'Active' on the Agent Statistics page.

To start an agent (agent system tray icon):

NOTE: The agent system tray icon is only available for server agents.

1. From the server where the agent is installed, right-click the agent system tray icon and select **Enable Agent**.
2. A message displays explaining that the agent is being started.
3. In addition, a desktop notification displays in the lower right-hand corner of your screen explaining that the selected agent is being connected to a specific coordinator.

   Once connected, the agent system tray icon no longer contains a red or yellow button indicating that the agent is now active.

Agent Log page

A new log page is created whenever the **View Agent Log** command is selected and displays the event details recorded in the trace log for the selected agent.

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

- Windows Management Instrumentation (WMI) must be enabled in 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 10.

The data grid and event details pane on this page contains the following information for each log entry. The default column in the table below identifies the fields that are displayed in the data grid by default. To display different fields, click the **Field Chooser** button located to the far left of the column headings.

Table 10. Agent Log page: Field descriptions

Column	Default	Description
File	No	Specifies the name of the source file that logged the message.
Function	No	Displays the name of the function that logged the message.
ID	No	Displays the event ID used to identify the event.
Level	Yes	Indicates the severity of the event message: • Info - 'For your information'; does not require attention • Error - events that indicate a problem has occurred; requires attention • Warning - events that warn of potential problems; does not require immediate attention
Line	No	Specifies the line within the source file that logged the message.
Logger	No	Specifies the logger used to log events.
Message	Yes	Displays the event message that was posted to the log.
Thread	No	Specifies the thread within the source file that logged the message.
Timestamp	Yes	Displays the date and time when the entry was posted to the log. **NOTE:** Based on the client's current local date and time. The format used to display this date and time is determined by the local machine's regional and language setting.

Use the tool bar buttons at the top of the log page to scroll through the log and search for log entries.

Table 11. Agent Log page: Tool bar buttons

Refresh	Use to refresh and reload the log entries from the source file. **NOTE:** Not available when the log page is launched using the **View Agent Log** command.
Copy	Use to copy the selected content to the clip board. Use with the **Select All** button to copy and paste the contents of the entire log into another application.
Select All	Use to select the entire contents of the log. Use with the **Copy** button to copy and paste the contents of the log into another application.
Find:	Enter a specific string of characters or word to be located in the log and use the **Find** button to locate the text.
 Show Matched Entries Only (Ctrl+M)	Use to display only the entries that match the word/string of characters entered in the search text.
Match Case	Use to locate entries that match the case as it was entered in the search text.
Previous	Use to move to the previous entry that contains the search text.
Next	Use to move to the next entry that contains the search text.
Print	Use one of the **Print** options to print or save the contents of the log.

View and save agent trace logs

To view Change Auditor logs (Statistics page):

1. Open the Statistics page and select **Logs | Open Log**.
2. On the Open Log File dialog, use the controls at the top of the dialog to locate the Change Auditor log to view. Select the log file and click **Open**.

   This opens a new page in the client which displays the log entries for the selected log.
3. Whenever an entry is highlighted in the top pane, the corresponding details are displayed in the Event Details pane across the bottom of the screen.
4. Use the tool bar buttons to search the log for a specific entry, to copy and paste the contents of this log for use in another application, and print or save the contents of this log.

To save Change Auditor logs to a specific location (Agent Statistics page):

1. Open the Agent Statistics page.
2. Select one or more agents from the list and select **Logs | Get All Logs**.
3. On the Browse for Folder dialog, select the location to save the logs for the selected agents. Click **OK** to save your selection.

   NOTE: If necessary, select **Make New Folder** to create a new folder for these logs.

To view Agent logs (Agent Statistics page):

1. Open the Agent Statistics page.
2. Select one or more agents from the list and select **Logs | View Agent Log**.
3. This opens a new page in the client which displays the selected agent's log (ChangeAuditor.AgentLog.nptlog). If multiple agents are selected, multiple log pages are created.
4. Whenever an entry is highlighted in the top pane, the corresponding details are displayed in the Event Details pane across the bottom of the screen.

   In addition, when an error is highlighted in the top pane and there is a call stack available for that error, an Exception pane will also be displayed.
5. Use the tool bar buttons to search the log for a specific entry, to copy and paste the contents of this log for use in another application, and to print or save the contents of this log.

To view Agent logs (agent system tray icon):

NOTE: The agent system tray icon is only available for server agents.

1. On the server where the agent is installed, right-click the agent system tray icon and select **View Agent Logs**.
2. This opens the log viewer allowing you to review the events recorded in the selected agent's log (ChangeAuditor.AgentLog.nptlog).

25

Coordinator Statistics and Logs

- Introduction
- Coordinator Statistics page
- Coordinator system tray icon
- View coordinator status and statistics
- Manage Change Auditor coordinators
- Coordinator Log page
- View and save coordinator trace logs

Introduction

In addition to the overview information provided in the Coordinator Status pane on the Overview page, you can obtain coordinator status and statistics through the following options:

- The Coordinator Statistics page which provides a global view of all installed coordinators, including the current status and other usage statistics for each coordinator.
- The Change Auditor Coordinator Status dialog, which is accessed using the coordinator system tray icon, provides the status and usage statistics for a single coordinator.

You can also view or retrieve coordinator trace logs from the Coordinator Statistics page or by using the coordinator system tray icon.

This section provides a description of the Coordinator Statistics page as well as the Coordinator System tray component and explains how to use these features to maintain coordinators.

Coordinator Statistics page

Use the **View | Statistics | Coordinator** menu command to display the Coordinator Statistics page, which provides a global view of all installed coordinators, including the current status of the coordinators.

The Coordinator Statistics page may contain the following information for each coordinator. The following table identifies the fields that are displayed by default. To display different fields, click the **Field Chooser** button located to the far left of the column headings and select the required columns:

NOTE: All dates and times are based on the client's current local date and time. The format used to display the date and time is determined by the local computer's regional and language setting.

Table 1. Coordinator Statistics page: Field descriptions

Column	Default	Description
Agents Connected	Yes	Displays the number of agents to which this coordinator is connected.
Alerts Last 24 Hours	No	Displays the number of alerted event entries in the last 24 hours of the coordinator operation. The value in this field is a hypertext link and when selected displays the alerts generated in the last 24 hours.
Alerts Last Hour	No	Displays the number of alerted event entries in the last 60 minutes. The value in this field is a hypertext link and when selected displays the alerts generated in the last 60 minutes.
Alerts Today	Yes	Displays the number of alerted event entries since local midnight today. The value in this field is a hypertext link and when selected displays the alerts generated since local midnight today.
Alerts Total	No	Displays the number of alerted events found in the coordinator database. The value is this field is a hypertext link and when selected displays the alerts in the coordinator database.
Alerts Yesterday	No	Displays the number of alerted event entries from local midnight today to local midnight yesterday. The value in this field is a hypertext link and when selected displays the alerts generated yesterday.
Architecture	No	Displays whether the coordinator is installed in a 32-bit (x86) or 64-bit (x64) environment.
Client Port	Yes	Displays the port number assigned to the coordinator Service Connection Point (SCP).
Coordinator	Yes	Displays the computer name of the coordinator.
Coordinator FQDN	No	Displays the fully qualified domain name of the coordinator.
Coordinator ID	Yes	Displays the ID of the coordinator that processed the event.
DB Catalog	Yes	Displays the name assigned to the coordinator database during the coordinator installation.
DB Instance	No	Displays the name of the SQL instance that is being used for the coordinator database.
DB Size	Yes	Displays the size of the coordinator database, in kilobytes.
Domain	Yes	Displays the name of the domain where the coordinator is located.
Events Last 24 Hours	No	Displays the number of event entries received from all agents in the last 24 hours of coordinator operation. The value in this field is a hypertext link and when selected launches a quick search to display the events generated in the last 24 hours.
Events Last Hour	No	Displays the number of event entries received in the last 60 minutes of the coordinator operation. The value in this field is a hypertext link and when selected launches a quick search to display the events generated in the last 60 minutes.
Events Today	Yes	Displays the number of events encountered since 12:00 a.m. of the current day (based on the relative coordinator computer's time). The value in this field is a hypertext link and when selected launches a quick search to display the events generated today.
Events Total	No	Displays the number of entries found in the coordinator events database. The value in this field is a hypertext link and when selected launches a quick search to display all events encountered since the agent was started.

Table 1. Coordinator Statistics page: Field descriptions

Column	Default	Description
Events Yesterday	No	Displays the number of events encountered between 12:00 a.m. yesterday and 12:00 a.m. of the current day (based on the relative coordinator computer's time). The value in this field is a hypertext link and when selected launches a quick search to display the events generated yesterday.
Forest	No	Displays the name of the forest where the coordinator resides.
Startup Time	No	Displays the date and time when the coordinator was last initialized.
Status	Yes	Displays the current status of the coordinator: • running • initializing • stopped • failed
Uptime	Yes	Displays how long the coordinator has been running.
Version	Yes	Displays the current coordinator version installed on the server.

Coordinator system tray icon

During the coordinator installation process, Change Auditor automatically loads an icon in the system tray of each coordinator. This system tray icon allows you to enable/disable the coordinator, display the status of the coordinator installed on the current machine, and to change the database instance and service accounts used to access the database. Whenever a coordinator is not active, a status indicator will appear in the lower left corner of this icon to represent its current status:

- Red - inactive
- Yellow - initializing

By right-clicking on the coordinator icon in the system tray, a context menu is displayed which consists of the following commands:

Table 2. Coordinator system tray icon: Right-click commands

Command	Description
Coordinator Status	Displays the Coordinator Status dialog which assists you in determining if the coordinator is running, what version is installed and how active the coordinator is. See Change Auditor Coordinator Status dialog for a full description of this status dialog.
Enable/Disable Coordinator	Starts or stops the coordinator.
View Coordinator Log	Opens the log viewer to review the events recorded in the coordinator log (ChangeAuditor.ServiceLog.nptlog). For example: %ProgramFiles%\Quest\ChangeAuditor\Service\Logs\ChangeAuditor.ServiceLog.nptlog

Table 2. Coordinator system tray icon: Right-click commands

Command	Description
Coordinator Configuration	Starts the Coordinator Configuration Tool which allows you to: • modify the credentials used to access the coordinator database • specify a 'static' port to be used for communication with the coordinator • specify where the Active Directory/GPO protection templates are to be stored: SQL (default) or Active Directory • specify the authentication method to use to make Active Directory requests. See Coordinator Configuration tool for a description of how to use this utility.
Load On Startup	Automatically loads the system tray application when the coordinator starts.
About	Display information about Change Auditor including the installed version number and licensing information.
Exit	Closes the system tray application.

Change Auditor Coordinator Status dialog

The Change Auditor Coordinator Status dialog helps you determine if the coordinator is running and what version is installed on the server. The other status information on the dialog is broken down into the following sections:

- **Coordinator Information** - displays the status, version number, SCP port and installation name for the coordinator
- **Database Information** - displays the coordinator database server, name and size
- **Agent Connections to this Coordinator** - displays the total number of agents that are connected to the coordinator
- **Events and Alerts on this Coordinator** - displays status information regarding events, alerts, and search activities for this particular coordinator
- Agent Ports on this Coordinator - displays all ports used for communication.

The Change Auditor Coordinator Status dialog contains the following information:

Table 3. Change Auditor Coordinator Status dialog: Status information

Field	Description
Coordinator Information	
Coordinator Status	Displays the current status of the coordinator: • Running • Initializing • Stopped • Failed This value will normally be 'Running'. If the credentials supplied for the database access during the coordinator installation are incorrect or have expired, this field will display 'Not Running' indicating that the coordinator did not successfully start. If this happens, use the Database Configuration Utility to change the permissions trying to access the database.
Installation Name	Displays the installation name assigned to the coordinator during installation.
Version	Displays the current version of the coordinator installed on the server.
Database Information	
SQL Server	Displays the name of the server where the coordinator resides.
Database Catalog	Displays the name assigned to the coordinator database during the coordinator installation.

Table 3. Change Auditor Coordinator Status dialog: Status information

Field	Description
Database Size	Displays the size of the coordinator database, in megabytes.
Database Free Space	Displays the available free space in the coordinator database.
Agent Connections to This Coordinator	
Agents Connected (Total)	Displays the total number of agents connected to this coordinator.
Events and Alerts on This Coordinator	
Total Events	Displays the number of events this coordinator has received since it was last started.
Events in Receive Buffer	Displays the number of events that have not yet been processed by this coordinator and forwarded to the client.
Average Events Per Second	Displays the average number of events processed by this coordinator per second.
Agent Ports on This Coordinator	
Client SCP Port	Displays the port number assigned to the coordinator Service Connection Point (SCP).
Public SDK Port	Displays the port number assigned for external applications to access the coordinator.
Agent Port	Displays the port number assigned to the agents to communicate with the coordinator.

Coordinator Configuration tool

You can use the Coordinator Configuration tool to modify the credentials used by the coordinator when accessing the database. Right-clicking the coordinator system tray icon and selecting **Coordinator Configuration**, displays the Coordinator Configuration tool. From here, you can:

- modify the credentials to be used to access the Change Auditor database
- change the database instance
- specify static SCP listening ports to be used to communicate with the coordinator
- specify where the Active Directory and GPO protection templates are to be stored: SQL (default) or Active Directory
- specify the authentication method to use to make Active Directory requests.

This tool consists of the following tabbed pages:

- Security page
- Ports page
- Protection page
- LDAP Authentication page

Security page

From the Security page, you can change the database instance and service accounts used to access the database.

NOTE: If User Account Control (UAC) is enabled, a confirmation dialog appears where you can authorize the Coordinator Configuration tool to use the required elevated rights.

Use the fields/options to enter the credentials to be used to access the designated SQL Server/instance as described below:

SQL server and instance

Enter the name or IP address of the SQL instance to be used. (i.e., <*Server Name*>\<*Instance Name*>). You can also click **Browse** to locate and select the SQL server and instance.

NOTE: If your database is in a SQL AlwayOn Availability Group, specify the name of the availability group listener for the SQL Server name.

Name of database Catalog

This displays the name assigned to the Change Auditor database.

Connect using

Specify whether Windows authentication, Microsoft Entra authentication or SQL server authentication will be used when communicating with the SQL database instance. (The authentication method is set up when SQL is installed.)

NOTE: Microsoft Entra authentication is only supported for SQL Managed Instances.

Depending on the authentication option selected, enter the appropriate user credentials.

- **Windows Authentication** - this is selected by default and will use Windows authentication to access the database.

  If you are using a group Managed Service Account:

  - The account must end with '$' and the password must be blank.
  - The domain should be entered in the Fully Qualified Domain Name format.
  - The Coordinator Configuration Tool must be run as the administrator. (Right-click and select Run as administrator.)
  - The coordinator host must be correctly configured to retrieve the managed password for the specified group Managed Service Account.
  - The local Administrator group must be added to the group policy debug programs. (Found under Local Computer Policy | Windows Settings | Security Settings | Local Policies | User Rights Assignments | Debug programs.)

- **SQL Server Authentication** - select this to use SQL Server authentication to access the database.
- **Microsoft Entra Authentication** - select this to use Microsoft Entra authentication to access the database located on an Azure SQL Managed Instance.

  Azure SQL Managed Instance:

- For a private endpoint, specify the managed instance host name in the following format: MyHostName.dns_zone.database.windows.net

  For private endpoint with default port, port specification is not explicitly required. For example: MyHostName.b1b2a3d4e5f7.database.windows.net

  or

  MyHostName.b1b2a3d4e5f7.database.windows.net,1433

- For a public endpoint, specify the managed instance host name and port in the following format: MyHostName.public.dns_zone.database.windows.net,3342

  For public endpoint, port specification is required. For example: MyHostName.public.b1b2a3d4e5f7.database.windows.net,3342

  NOTE:

  - Azure SQL Managed Instance (PaaS) is supported using SQL authentication or Microsoft Entra Authentication with an encrypted connection. Windows authentication is not supported.

- For an Azure SQL Managed Instance (PaaS), SQL authentication or Microsoft Entra authentication with an encrypted connection must be used.
- Single User Mode is not supported during installation or upgrade when using Azure SQL Managed Instance. Ensure that all SQL connections to the Change Auditor database are closed before and during the upgrade.
- Azure SQL Managed Instance (HA) high availability is supported using the read-write listener endpoint.
- Performance may vary depending on network configuration, topology, and Azure SQL Managed Instance configuration.

Login ID

Enter the user name for the account to be used to access the SQL server instance.

Password

Enter the password associated with the user account entered above.

Domain

Enter the domain name for the Windows account used to access the designated SQL server instance. (Only valid for Windows Authentication.)

Encryption

Select the appropriate level of encryption for the data sent between the coordinator and SQL server.

- **Strict (SQL Server 2022)**: Select this option for SQL Server 2022 and Azure SQL Managed Instance or when the instance has **Force Strict Encryption** enabled.
- **Mandatory**: Select this option when the instance has **Force Encryption** enabled. It can also be used when no encryption is configured for the instance, but **Trust server certificate** is enabled. While this method is less secure than installing a trusted certificate, it does support an encrypted connection.
- **Optional**

Enabling **Trust server certificate**, when 'Optional' or 'Mandatory' encryption is selected, or if the server enforces encryption, means that SQL Server will not validate the server certificate on the client computer when encryption is enabled for network communication.

Under **Host name in the certificate**, you can provide an alternate, yet expected, Common Name (CN) or Subject Alternative Name (SAN) in the server certificate. You would use this option when the server name does not match the CN or SAN, for example, when using DNS aliases.

Leaving this option blank allows certificate validation to confirm that the CN or SAN matches the server name.

NOTE: Change Auditor supports TLS 1.3; however, TLS 1.2 remains a requirement since SQL Server 2022 satellite services require TLS 1.2 to be enabled.

Ports page

By default, Change Auditor dynamically assigns communication ports for each installed coordinator. However, using the Ports page of the Coordinator Configuration dialog, you can specify static SCP listening ports to be used to communicate with the coordinator.

If you upgraded from a 5.x installation where static ports were defined, these static ports are retained as part of the upgrade process. However, the **Agent Port** setting, which is used by 6.0 agents, is set to use a dynamic port. Check with your system administrator to determine whether this new connection should also be using a static port.

Enter the ports to use to communicate with the coordinator:

NOTE: A zero (0) indicates that a dynamic port is being used. If you have set a static port and wish to use a dynamic port, change the port number back to 0.

Client Port

Enter the static port number to be used by the client to communicate with the coordinator.

Public SDK Port

Enter the static port number to be used by external applications to access the coordinator.

Agent Port

Enter the static port number to be used for communication between a agent and a coordinator.

Protection page

By default, Change Auditor stores the Active Directory and GPO protection templates in SQL. However, you can use the Protection page of the Coordinator Configuration dialog to store the Active Directory and GPO protection templates in Active Directory instead of SQL.

When you select to store your Active Directory and Group Policy protection templates in Active Directory, you can use the Security feature on the Active Directory Protection page or Group Policy Protection page to provide an additional layer of security. The additional setting is intended when you require tighter security ACLs on your Active Directory and GPO objects and templates (for example, the Change Auditor SQL database may not be fully secured by ChangeAuditor Administrators). For more information about setting this additional security on protected objects, see the Change Auditor for Active Directory User Guide.

Specify the appropriate option for storing Active Directory/GPO protection and ADAM (AD LDS) protection:

Store Active Directory/GPO protection in:

Select one of the following options:

- SQL (default)
- AD

Store ADAM (AD LDS) protection in:

Select one of the following options:

- SQL (default)
- AD

LDAP Authentication page

From this page you can specify the authentication method to use to make Active Directory requests.

- Select Simple Authentication and Security Layer (SASL) to use Kerberos or NTLM.
- Select Secure Socket Layer (SSL) to use certificates.

IMPORTANT: If you choose SSL, please see the Change Auditor Install Guide for important guidelines.

NOTE: When making Active Directory requests, credentials and message content are encrypted for both authentication methods.

View coordinator status and statistics

To view coordinator status and statistics (Overview page):

1. Open the Overview page and if the Coordinator Status overview pane is not being displayed, click the arrow button on an overview pane and select one of the following commands:
   - **Coordinator Status | Enterprise View**
   - **Coordinator Status |** <*domain*>

   This displays a pie chart depicting the current status of all the coordinators installed in either the entire enterprise or in a selected domain.

2 By default, this pane only includes installed coordinators in the pie chart. You can however, select the **Show Uninstalled Coordinators** check box to include uninstalled coordinators in the pie chart.

3 Double-clicking the pie chart displays the Coordinator Statistics page.

To view coordinator status/statistics (Coordinator Statistics page):

1 Open the Coordinator Statistics page.

2 Click **Show Uninstalled Coordinators** to include coordinators set as 'uninstalled'. Click **Hide Uninstalled Coordinators** to exclude these coordinators from the display.

The values in the different event columns are links, which when selected will open up a new Search Results tab to display the related details for these events.

To view coordinator status/statistics on current coordinator only (coordinator system tray icon):

1 From the server where the coordinator is installed, right-click the coordinator system tray icon and select **Coordinator Status**.

2 This displays the Change Auditor Coordinator Status dialog with the status and statistics regarding the coordinator, database, agent connections and events and alerts.

3 Click **OK** to close this dialog.

Manage Change Auditor coordinators

NOTE: You can use **Action | Agent Notifications** to hide (or display) the desktop notifications that are displayed when these processes are performed.

To stop a coordinator:

1 From the server where the coordinator is installed, right-click the coordinator system tray icon and select **Disable Coordinator**.

2 On the confirmation dialog, click **Yes** to stop the coordinator service.

A message displays explaining that the coordinator is being stopped.

In addition, a desktop notification displays in the lower right-hand corner of your screen explaining that the selected coordinator is being disabled.

Once disabled, the coordinator system tray icon contains a red light indicating that the coordinator is disabled.

3 If you so choose, click **Set Coordinator Uninstalled** to flag the selected coordinator as 'Uninstalled'.

4 Click **Show Uninstalled Coordinators** to include uninstalled coordinators in the Coordinator Statistics list. Click **Hide Uninstalled Coordinators** to exclude uninstalled coordinators from the display.

To start a coordinator:

- From the server where the coordinator is installed, right-click the coordinator system tray icon and select **Enable Coordinator**.

  A message displays explaining that the coordinator is being started.

  In addition, a desktop notification is displayed in the lower right-hand corner of your screen explaining that the selected coordinator is being started.

  Once restarted, the coordinator system tray icon no longer contains a red or yellow button indicating that the coordinator is now active.

Coordinator Log page

Two new log pages are created whenever you select **View Coordinator Log**. These log pages contain the event details that were recorded in each of these trace logs for the selected coordinator:

- Service: CA4xCompat.exe.nptlog - this log includes the messages logged during agent to coordinator communications.
- Service: ChangeAuditor.ServiceLog.nptlog - this log includes the messages logged during client to coordinator communications.

The data grid and event details pane on this page contains the following information for each log entry. The default column in the table below identifies the fields that are displayed in the data grid by default. To display different fields, click the **Field Chooser** button located to the far left of the column headings.

Table 4. Coordinator Log page: Field descriptions

Column	Default	Description
File	No	Specifies the name of the source file that logged the message.
Function	No	Displays the name of the function that logged the message.
ID	No	Displays the event ID used to identify the event.
Level	Yes	Indicates the severity of the event message: • Info - 'For your information'; does not require attention • Error - events that indicate a problem has occurred; requires attention • Warning - events that warn of potential problems; does not require immediate attention
Line	No	Specifies the line within the source file that logged the message.
Logger	No	Specifies the logger used to log events.
Message	Yes	Displays the event message that was posted to the log.
Thread	No	Specifies the thread within the source file that logged the message.
Timestamp	Yes	Displays the date and time when the entry was posted to the log. **NOTE:** Based on the client's current local date and time. The format used to display this date and time is determined by the local machine's regional and language setting.

Use the tool bar buttons at the top of the log page to scroll through the log and search for log entries.

Table 5. Coordinator Log page: Tool bar buttons

Refresh	Use to refresh and reload the log entries from the source file. **NOTE:** Not available when the log page is launched using the **View Coordinator Log** command.
Copy	Use to copy the selected content to the clip board. Use with the **Select All** button to copy and paste the contents of the entire log into another application.
Select All	Use to select the entire contents of the log. Use with the **Copy** button to copy and paste the contents of the log into another application.
Find:	Enter a specific string of characters or word to be located in the log and use the **Find** button to locate the text.
 Show Matched Entries Only (Ctrl+M)	Use to display only the entries that match the word/string of characters entered in the search text.
Match Case	Use to locate entries that match the case as it was entered in the search text.

Table 5. Coordinator Log page: Tool bar buttons

Previous	Use to move to the previous entry that contains the search text.
Next	Use to move to the next entry that contains the search text.
Print	Use one of the **Print** options to print or save the contents of the log.

View and save coordinator trace logs

To view Change Auditor logs (Statistics page):

1. Open the Statistics page.
2. Click **Logs | Open Log**.
3. On the Open Log File dialog, use the controls at the top of the dialog to locate the Change Auditor log to be viewed. Select the log file and click **Open**.

   This opens a page in the client which displays the log entries for the selected log.

   Whenever an entry is highlighted in the top pane, the corresponding details will be displayed in the Event Details pane across the bottom of the screen.
4. Use the tool bar buttons to search the log for a specific entry, to copy and paste the contents of this log for use in another application, and print or save the contents of this log.

To save Change Auditor logs to a specific location (Coordinator Statistics page):

1. Open the Coordinator Statistics page.
2. Select a coordinator from the list and click **Logs | Get All Logs**.
3. On the Browse for Folder dialog, select the location where these logs are to be saved. Click **OK** to save your selection.

   NOTE: If necessary, click **Make New Folder** to create a new folder for these logs.

To view the coordinator log (Coordinator Statistics page):

1. Open the Coordinator Statistics page.
2. Select a coordinator from the list and click **Logs | View Coordinator Log**.

   This opens a page in the client which displays the log entries in the Change Auditor coordinator log (ChangeAuditor.ServiceLog.nptlog).

   Whenever an entry is highlighted in the top pane, the corresponding details will be displayed in the Event Details pane across the bottom of the screen.

   In addition, when an error is highlighted in the top pane and there is a call stack available for that error, an Exception pane will also be displayed.
3. Use the tool bar buttons to search the log for a specific entry, to copy and paste the contents of this log for use in another application, and to print or save the contents of this log.

To view the coordinator log (coordinator system tray icon):

1. From the server where the coordinator is installed, right-click the coordinator system tray icon and select **View Coordinator Log**.
2. This opens the log viewer, allowing you to review the entries recorded in the coordinator log (ChangeAuditor.ServiceLog.nptlog).

26

Change Auditor Commands

This appendix lists the commands available throughout the Change Auditor client. The tables in this appendix list the following commands that are available throughout the entire client:

- Menu commands
- Tool bar buttons
- Right-click commands

Menu commands

The Change Auditor commands are grouped under a menu on the menu bar. Some of these commands perform an action immediately; others display an additional dialog or open a wizard where you select options or specify additional information.

The following table provides a description of the commands available under each of the Change Auditor menus.

Table 1. Menu commands

Menu command	Shortcut key	Description
File Menu		
Connect	Ctrl+O	Use to display the Connection screen to select the connection profile to be used to connect to a Change Auditor coordinator. This command is only available when the client is disconnected from a coordinator.
Disconnect	Ctrl+D	Use to disconnect from the current coordinator.
Open Log		Use to view one of the log files. Selecting this command will display the Open Log dialog allowing you to select the log file to be viewed. Once selected, a new tabbed page will be created in the client displaying the entries logged in the selected log.
Open Client Log		Use to view the current client log. A new tabbed page will be created in the client displaying the entries logged to the current client log.
Print	Ctrl+P	Use to send the contents of the displayed page to the designated printer. When you select this command, the Print dialog will be displayed allowing you to specify various print options.
Print to File	Ctrl+Shift+F	Use to save the contents of the displayed page to either an Excel (.xls) or comma delimited (.csv) file. When you select this command, the Save As dialog will be displayed allowing you to specify the location, file name and type of file to be created.
Print to PDF	Ctrl+Shift+D	Use to save the contents of the displayed page to a PDF file. When you select this command, the Save As dialog will be displayed allowing you to specify the location and file name.
Print Preview	Ctrl+Shift+P	Use to preview the contents of the displayed page prior to printing it.

Table 1. Menu commands

Menu command	Shortcut key	Description
Page Setup	Ctrl+Shift+U	Use to define the page settings for printing. Selecting this command will display the Page Setup dialog allowing you to define the paper, page orientation and margins.
Exit	Ctrl+Q	Use to close the client.
Edit Menu		
Cut	Ctrl+X	Use to move the selected item (folder or search definition) to a different location in the explorer view (left pane) on the Searches page. Once cut, this item can then be pasted (or moved) to another location.
Copy	Ctrl+C	Use to copy the selected item (folder or search definition) to another location in the explorer view (left pane) on the Searches page. Once copied, a copy of this item can be pasted to another location.
Paste	Ctrl+V	Use to paste the contents of the clipboard (folder or search definition) to the selected location.
Delete		Use to remove the selected user-defined item (folder or search definition).
Move		Use to move the selected item (folder or search definition) to another location in the explorer view (left pane) on the Searches page. Selecting this command will display the Select the Destination Folder dialog allowing you to select the new location.
Action Menu		
Refresh	F5	Use to retrieve and redisplay current data.
Autofit Columns to Contents	Ctrl+F	Use to resize the columns based on the content, which will eliminate the scroll bars.
Reset Display		Use to close multiple client windows and return to a single client window.
Show XML Tab		Use to display the XML tab, which displays the XML representation of a selected search criteria, at the end of the Search Properties tabs. **NOTE:** This command is only available from the Searches page and a Search Results page.
Show SQL Tab		Use to display the SQL tab, which displays the SQL query built to run a selected search, at the end of the Search Properties tabs. **NOTE:** This command is only available from the Searches page and a Search Results page.
Auto Connect		Use to enable or disable the auto connect feature. When enabled, the Connection Profile dialog will not be displayed when the client is launched. Instead, the previously specified connection profile will automatically be used to connect to the coordinator.
Disconnect client after 30 minutes of inactivity		Use this to disconnect from the client after 30 minutes of inactivity. If this option is not checked, the connection to the coordinator remains open.
Agent Notifications		Use to hide (or display) the desktop notification that is displayed in the lower right-hand corner of the screen whenever an agent is connected or disconnected from the coordinator, or when the coordinator is stopped or started. **NOTE:** **Agent Notifications** is enabled by default.

Table 1. Menu commands

Menu command	Shortcut key	Description
Agent Auto Refresh		Use to enable or disable the refreshing of the currently displayed grid (on the Deployment, Overview or Agent Statistics page) when an agent either connects or disconnects. **NOTE:** **Agent Auto Refresh** is enabled by default.
Hide Unlicensed Components		Use to hide unlicensed components from the Administration Tasks tab and unlicensed events throughout the client. **NOTE:** This command is only available from the Administration Tasks tab. **NOTE:** This feature only applies to users who have never had a specific product license (e.g., Change Auditor for Exchange). Users who had a trial license that has expired, will not be able to hide components. This is so that you can continue to search for events that may have occurred during your trial period.
Export		Use to export the Administration settings, such as configurations and settings, and auditing and protection templates, into an XML file. Selecting this command displays an Export dialog allowing you to select the settings/templates to be exported. **NOTE:** This command is only available from the Administration Tasks tab.
Import		Use to import previously exported Administration settings. Selecting this command displays an Import dialog allowing you to select the settings/templates to be imported. **NOTE:** This command is only available from the Administration Tasks tab.
View Menu		
Deployment	Ctrl+F8	Use to display the Deployment page, from which you can deploy agents.
Overview	Ctrl+F9	Use to display the Overview page, which displays the results of your favorite search as well as an overview of the following information: • Top agent activity • Recent event activity • Count of events by event class, facility, location, severity, result or subsystem • Agent status for the entire enterprise or individual domain • Coordinator status for the entire enterprise or a single domain • Alert history counts
Searches	Ctrl+F10	Use to display the Searches page, from which you can run searches, define new searches and enable alerting.
Statistics | Agent	Ctrl+F11	Use to display the Agent Statistics page which provides a global view of all your agents, providing you with their current status and statistics.
Statistics | Coordinator	Shift+F11	Use to display the Coordinator Statistics page which provides coordinator status, database information and agent connection, event and alert data.
Administration	Ctrl+F12	Use to display the Administration Tasks tab which provides a single location where you can perform various administrative tasks related to configuring Change Auditor, customizing the auditing process and defining protection.

Table 1. Menu commands

Menu command	Shortcut key	Description
Close All Windows		Use to close all open windows.
List of open windows		The remainder of this menu lists all of the windows that are currently opened in the client. A check mark to the left of a window indicates the window that is currently active.
Help Menu		
About		Use to display the Quest Change Auditor dialog which displays the following information: • The **About** tab displays the current version, patent, trademark and copyright statements. • The **License** tab provides license compliance information. • The **Legal Notices** tab displays acknowledgments for third party components that are used in Change Auditor • The **Contact** tab provides contact information for technical support, product questions and sales.
Contents	F1	Use to display the contents and initial screen of the online help.

Tool bar buttons

The following table lists all of the commands available on the various tool bars in the client. It lists the commands/buttons in alphabetical order and provides a brief description of each command.

NOTE: When a tool bar button contains an arrow to the far right, this indicates that you can expand the button to select an additional command.

Table 2. Tool bar buttons

Tool bar button	Description	Change Auditor pages
Add	Depending on the page, use to add an entry to a search criteria list, add an object to an auditing list, define a new template, create a scheduled purge job, etc.	Most Administration Tasks pages
Add **Add Role Definition** **Add Task Definition** **Add Application Group**	Use the Add options as defined below: • **Add Role Definition** - use to define a new role defining who is authorized to perform the selected tasks and/or operations. • **Add Task Definition** - use to define a new task defining the operations that can be performed. • **Add Application Group** - use to define a new Authorization Manager Application Group.	Application User Interface page
Add **Subsystem** **Event Class** **Object Class** **Severity** **Results**	Use to add an entity (subsystem, event class, object class, severity or results) to the What search criteria list or purge criteria.	What tab

Table 2. Tool bar buttons

Tool bar button	Description	Change Auditor pages
Add with Events **Subsystem** **Event Class** **Object Class** **Severity** **Results**	Use to add an entity that already has an event associated with it in the coordinator database to the What search criteria list or purge criteria.	What tab
Add with Events	Use to add an entity that already has an event associated with it in the coordinator database to the search or purge criteria.	Who tab Where tab Origin tab
Add | Add Wildcard Expression	Use to specify a wildcard expression for the search criteria or purge criteria.	Who tab Where tab
Add | Add Server Types	Use to specify a server type for the search criteria or purge criteria.	Where tab
Add | Exclude	Use to exclude a mailbox from Exchange auditing.	Exchange Mailbox Auditing page
Add | Select Multiple Objects	Use to define custom Active Directory and ADAM auditing - defining the objects, classes and/or attributes to be audited by Change Auditor.	Active Directory Auditing page ADAM (AD LDS) Auditing page
Advanced Options | Advanced Options	Use to display the Advanced Deployment Options dialog where you can view or modify the following settings: • Specify Agent Installation Location • Specify a Custom Share on the Remove Server • Launch ServiceStatusTray of startup • Restart Agent on failure • Specify a Group Policy Backup	Deployment page
Advanced Options | ActiveRoles Integration **Deploy Scripts Only** **Deploy Scripts and Excluded Accounts**	Use the Active Roles integration options as described below: • **Deploy Scripts Only** - use to copy and run the Active Roles integration scripts on the Active Roles server. These scripts instruct Active Roles to capture the initiator information for all users and pass this information onto Change Auditor. • **Deploy Scripts and Excluded Accounts** - use to specify user and computer accounts that are to be excluded from this integration. Change Auditor then deploys the Active Roles integration scripts that signal Active Roles to retrieve the initiator information for all users except for those specified for exclusion. Refer to the Quest Change Auditor Installation Guide for more information on Active Roles integration.	Deployment page
Alert Properties	Use to display the Alert properties across the bottom of the Alert History page.	Alert History page
Apply Changes	Use to save your coordinator configuration settings.	Coordinator Configuration page

Table 2. Tool bar buttons

Tool bar button	Description	Change Auditor pages
Assign	Use to assign an agent configuration to the selected agents or to assign a template to an agent configuration.	Agent Configuration page Excluded Accounts Auditing page SQL Auditing page File System Auditing page Registry Auditing page Services Auditing page File System Protection page
Comments	Use to enter a comment for the selected event.	Event Details pane
Configurations	Use to display the Configuration Setup dialog to add, edit or delete agent configuration definitions.	Agent Configuration page
Connect To	Use this button to select the domain controller to be used to apply ACLs or to revert back to the client's default global catalog. **NOTE:** This button is available only when you have selected to save your Active Directory and Group Policy protection templates to Active Directory using the Protection tab of the Coordinator Configuration tool.	Active Directory Protection page Group Policy Protection page
Copy	Use to copy the displayed event details to the clipboard.	Log pages Event Details pane SQL tab XML tab
Credentials **Set** **Clear** **Test**	Use to set, clear or test the credentials to be used for installing agents on the selected domain.	Deployment page
Default	Use to reset the severity and enabled settings of the selected events back to the factory defaults.	Audit Events page
Default All	Use to reset all agent configurations back to the default configuration.	Agent Configuration page
Delete	Use to remove the selected entry from the list.	Application User Interface page Member of Group Auditing page AD Query Auditing page Exchange Mailbox Auditing page Purge Jobs page Report Layouts page Who tab Where tab Origin tab

Table 2. Tool bar buttons

Tool bar button	Description	Change Auditor pages
Delete | Delete Administration Account	Use to remove the selected administration account from an Active Directory, ADAM (AD LDS), or Group Policy protection template.	Active Directory Protection page ADAM (AD LDS) Protection page Group Policy Protection page
Delete | Delete Agent	Use to remove the selected agent from an EMC or NetApp auditing template.	EMC Auditing page NetApp Auditing page
Delete | Delete Excluded Account	Use to remove the selected account from an Excluded Accounts auditing template.	Excluded Accounts Auditing page
Delete | Delete File Path	Use to remove the selected file path from a File System auditing or protection template, an EMC auditing template or a NetApp auditing template.	File System Auditing page EMC Auditing page NetApp Auditing page
Delete | Delete Object	Use to remove the selected object from custom Active Directory or ADAM auditing; an Active Directory, ADAM (AD LDS) or Group Policy protection template.	Active Directory Auditing & Protection pages ADAM (AD LDS) Auditing & Protection pages Group Policy Protection page
Delete | Delete Object Class	Use to remove the selected object class from the Active Directory or ADAM (AD LDS) auditing list.	Active Directory Auditing page ADAM (AD LDS) Auditing page
Delete | Delete Override Account	Use to remove the selected override account from a protection template.	Protection pages
Delete | Delete Path	Use to remove the selected path from the auditing template.	SharePoint Auditing page
Delete | Delete Registry Key	Use to remove the selected registry key from a Registry auditing template.	Registry Auditing page
Delete | Delete Service	Use to remove the selected service from a Service auditing template.	Service Auditing page
Delete | Delete SQL Instance	Use to remove the selected SQL instance from a SQL auditing template.	SQL Auditing page
Delete | Delete Template	Use to remove the selected auditing or protection template.	Auditing pages Protection pages
Delete Criteria	Use to remove the selected entry from the What search criteria list.	What tab
Design Report	Use to launch the report designer to create a custom report layout for a selected search query.	Report tab
Disable	Use to disable the selected events.	Event Details pane Audit Events page
Disable Alert	Used to disable a private alert.	Private Alerts and Reports page
Disable Report	Used to disable a private report.	Private Alerts and Reports page

Table 2. Tool bar buttons

Tool bar button	Description	Change Auditor pages
Edit	Use to modify the selected item.	Most Administration Tasks pages, including: • Purge Jobs page • Report Layouts page • Application User Interface page • Auditing pages • Protection pages
Edit Event Class	Use to modify the selected entry in the What search criteria list.	What tab
Edit Logon	Use to modify the type of logons included in a logon search.	What tab
Email	Use to launch the configured email client to email the selected event details.	Event Details pane
Enable	Use to enable the selected events.	Audit Events page Event Details pane
Event Details	Use to display the Event Details pane across the bottom of the Overview pane, Search Results page, or Alert History page.	Overview page Search Results page Alert History page
Event Logging	Use to enable or disable event logging.	Agent Configuration page
Explorer View	Use to show the explorer view in the left-hand pane of the Searches page.	Searches page
Find	Use to search for text in the currently displayed trace log. Enter a word or string of characters to be located.	Log pages
Force Refresh	Use to force a topology harvest refresh to discover new servers added to the Active Directory forest and display them on the Deployment page. **NOTE:** Topology scan takes a long time when the environment contains a large number of workstations.	Deployment page
Grid View	Use to hide the explorer view and display only the Searches list on the Searches page.	Searches page
Hide Properties	Use to hide the Search Properties tabs across the bottom of the Searches page. Use to hide the Resource Properties pane across the bottom of the Agent Statistics page.	Searches page Agent Statistics page
Hide Uninstalled Agents	Use to remove uninstalled agents from the current Agent Statistics view.	Agent Statistics page
Hide Uninstalled Coordinators	Use to remove uninstalled coordinators from the current Coordinator Statistics view.	Coordinator Statistics page
High/Medium/Low	Use to change the severity level assigned to the selected events.	Audit Events page
Install or Upgrade	Use to install or upgrade an agent on the selected servers.	Deployment page
Knowledge Base	Use to display the associated Event Reference Guide.	Audit Events page Event Details pane

Table 2. Tool bar buttons

Tool bar button	Description	Change Auditor pages
Logs **Open Log** **Get All Logs** **View Agent Log** **View Coordinator Log**	Use the Log options as described below: • **Open Log** - use to retrieve a Change Auditor trace log file and display it in the client. • **Get All Logs** - use to retrieve any associated logs and save them to a specified location on the local machine. • **View Agent Log** - use to display the current Change Auditor agent trace log in the Change Auditor client. • **View Coordinator Log** - use to display the current coordinator trace log in the client.	Agent Configuration page Agent Statistics page Coordinator Statistics page Deployment page
Match Case	Use to locate log entries that match the case that was entered in the search text.	Log pages
New **New Folder** **New Search**	Use the New options as described below: • **New Folder** - use to create a new folder in the explorer view of the Searches page. • **New Search** - use to create a new search definition.	Searches page
New Servers	Use to enable or disable the automatic deployment of agents to new servers found in your Active Directory forest.	Deployment page
Next	Use to move to the next log entry that contains the search text.	Log pages
Overviews	Use to display the Overview panes across the bottom of the Overview page.	Overview page
Preview Changes	Use to run the search based on the changes made to the search query and display the results in the current Search Results page.	Search Properties tabs (Search Results page)
Preview Report	Use to display a query results report.	Report tab
Previous	Use to move to the previous log entry that contains the search text.	Log pages
Print **Print** **Print to File** **Print to PDF** **Print Preview** **Page Setup**	Use the print options to print or save the contents of the displayed page. • **Print** - use to send the contents of the active page to a designated printer. • **Print to File** - use to save the contents of the active page to either an Excel (.xls) or comma delimited (.csv) file. • **Print to PDF** - use to save the contents of the active page to a PDF file. • **Print Preview** - use to display the print layout of the active page prior to printing it. • **Page Setup** - use to define the page settings for printing.	All pages
Protect Object	Use to protect Active Directory objects, ADAM (AD LDS) objects, Group Policy Objects, Exchange mailboxes, File System files and folders against unauthorized modifications.	Event Details pane
Refresh	Use to retrieve and display the latest data available.	Overview page Log pages

Table 2. Tool bar buttons

Tool bar button	Description	Change Auditor pages
Refresh Configuration	Use to retrieve the current agent configuration assignments.	Agent Configuration page
Refresh Status	Use to refresh the deployment status of the selected servers.	Deployment page
Related Search	Use to view additional details about the user who initiated the change, view resource details about the machine where the change occurred, or run related searches based on the who, where, what, when or origin of an event.	Event Details pane
Restart Agent	Use to stop and then restart an agent. This button is only available when an agent is in an 'active' state.	Agent Statistics page
Restore Value	Use to restore the current value (To value) to its previous value (From value). **NOTE:** Applies to 6.x (and higher) events reporting Active Directory attribute changes only. **NOTE:** The Restore Value feature may not work for all events. Specifically, values cannot be restored for the following events: • User password changed • User password changed by non-owner • User account locked • User account unlocked • User must change password at next logon option changed	Event Details pane
Run	Use to run the selected search and display the events returned in a new Search Results page.	Searches page Search Properties tabs
Save	Use to save a newly created search or modifications made to a search definition.	Search Properties tabs
Save As **Save As** **Save As Default**	Use the Save As options as described below: • **Save As** - use to save the search definition using a different name and/or location. • **Save As Default** - use to save the search definition as the new default for creating new searches.	Search Properties tabs
Search Properties	Use to display the Search Properties tabs across the bottom of the page.	Search Results page
Select All	Use to select all the entries in the currently displayed trace log, which can then be copied for use in another application.	Log pages
Set Agent Uninstalled	Use to flag the selected agent as 'uninstalled'. **NOTE:** This button is only available when the selected agent is in an 'active' state.	Agent Statistics page
Set Coordinator Uninstalled	Use to flag the selected coordinator as 'uninstalled'. **NOTE:** This button is only available when the selected coordinator is in an 'active' state.	Coordinator Statistics page
Shared Mailboxes	Use to view automatically detected shared mailboxes or to define a shared mailbox on the Exchange Mailbox auditing page.	Exchange Mailbox Auditing page

Table 2. Tool bar buttons

Tool bar button	Description	Change Auditor pages
Show Matched Entries Only ( )	Use to display only the log entries that match the word/string of characters entered in the search text.	Log pages
Show Properties	Use to display the Search Properties tabs across the bottom of the Searches page. Use to display the Resource Properties pane across the bottom of the Agent Statistics page.	Searches page Agent Statistics page
Show Uninstalled Agents	Use to include uninstalled agents in the current Agent Statistics view.	Agent Statistics page
Show Uninstalled Coordinators	Use to include uninstalled coordinators in the current Coordinator Statistics view.	Coordinator Statistics page
Start Agent	Use to start a stopped agent. This button is only available when an agent is in an 'inactive' state.	Agent Statistics page
Stop Agent	Use to stop an agent. This button is only available when an agent is in an 'active' state.	Agent Statistics page
Test Mail	Use to generate a test email based on the configuration information entered in the Email Alerts Configuration pane.	Coordinator Configuration page
Test SNMP	Use to generate a test SNMP trap based on the configuration information entered in the Email Alerts Configuration pane.	Coordinator Configuration page
Uninstall	Use to uninstall the agent from the selected servers.	Deployment page

Right-click commands

The following table lists the commands which are available through right-click functionality. The commands are listed in alphabetical order with a reference to the pages from which they can be accessed.

Table 3. Right-click commands

Command	Present on the following pages
Add Application Group	Administration Tasks tab: • Application User Interface Authorization - Role • Application User Interface Authorization - Member
Add Task Definition	Administration Tasks tab: • Application User Interface Authorization - Role • Application User Interface Authorization - Member
Add Role Definition	Administration Tasks tab: • Application User Interface Authorization - Role • Application User Interface Authorization - Member

Table 3. Right-click commands

Command	Present on the following pages
Alert **Enable Transport** **Email** **SNMP** **WMI** **Disable Transport** **Email** **SNMP** **WMI** **Disable Alert** **History** **Delete History**	Searches page - Search definition (right pane) **NOTE:** The **History** and **Delete History** options are only displayed when alerting has been enabled for a search.
All Results	Administration Tasks tab: • Audit Events - event
Assign	Administration Tasks tab: • Agent Configuration
Assign to Configuration	Administration Tasks tab: • Excluded Accounts Auditing - template or account • File System Auditing - template or file path • File System Protection - template or file path • Registry Auditing - template or registry key • Services Auditing - template or service • SQL Auditing - template or instance • SQL Data Level Auditing - template
Audit	Exchange Mailbox Auditing page - excluded mailbox
Clear Result	Deployment page - agent
Collapse All	Searches page - folder (left pane)
Comments	Overview page - event (data grid) Search Results page - event (data grid)

Table 3. Right-click commands

Command	Present on the following pages
Copy	Administration Tasks tab: • Coordinator Configuration - text boxes • Excluded Accounts Auditing - template • File System Auditing - template • Registry Auditing - template • Report Layouts - template • Services Auditing - template • SQL Auditing - template • SQL Data Level Auditing - template Event Details pane (text boxes) Overview page - event (data grid) Search Properties tabs: • Report tab (text boxes) • Info tab (text boxes) Searches Results page - event (data grid) Searches page: • Folder (left pane) • Search definition (right pane)
Credentials **Set** **Clear** **Test**	Deployment page - agent
Cut	Administration Tasks tab: • Coordinator Configuration (text boxes) Search Properties tabs: • Report tab (text boxes) • Info tab (text boxes) Searches page: • Folder (left pane) • Search definition (right pane)

Table 3. Right-click commands

Command	Present on the following pages
Delete	Administration Tasks tab: • Active Directory Auditing - object • Active Directory Auditing - object class • Application User Interface Authorization - role • Coordinator Configuration - text boxes • EMC Auditing - template or file path • Exchange Mailbox Auditing - mailbox • Exchange Mailbox Protection - template or mailbox • Excluded Account Auditing - template or account • AD Query Auditing - container • File System Auditing - template or file path • File System Protection - template or file path • NetApp Auditing - template or file path • Purge Jobs - job • Registry Auditing - template or registry key • Report Layouts - template • Services Auditing - template or service • SharePoint Auditing - template or path • SQL Auditing - template or instance • SQL Data Level Auditing - template Search Properties tabs: • Report tab (text boxes) • Info tab (text boxes) Searches page: • Folder (left pane) • Search definition (right pane)

Table 3. Right-click commands

Command	Present on the following pages
Disable	Administration Tasks tab: • Active Directory Auditing - object • Active Directory Protection - template or object • Audit Events - event • EMC Auditing - template or file path • Exchange Mailbox Auditing - mailbox • Exchange Mailbox Protection - template or mailbox • Excluded Accounts Auditing - template • AD Query Auditing - container • File System Auditing - template or file path • File System Protection - template or file path • Group Policy Protection - template or object • NetApp Auditing - template or file path • Purge Jobs - job • Registry Auditing - template or registry key • Services Auditing - template or service • SharePoint Auditing - template or path • SQL Auditing - template or instance • SQL Data Level Auditing - template Overview page - event (data grid) Search Results page - event (data grid)
Disable Alert	Private Alerts and Reports page
Disable Report	Private Alerts and Reports page
Edit	Administration Tasks tab: • Active Directory Auditing - object or object class • Active Directory Protection - template, object or attribute protection • Application User Interface Authorization - role • EMC Auditing - template or file path • Exchange Mailbox Protection - template or mailbox • Excluded Accounts Auditing - template or account • File System Auditing - template or file path • File System Protection - template or file path • NetApp Auditing - template or file path • Purge Jobs - job • Registry Auditing - template or registry key • Report Layouts - template • Services Auditing - template or service • SharePoint Auditing - template or path • SQL Auditing - template or instance • SQL Data Level Auditing - template
Email	Overview page - event (data grid) Search Results page - event (data grid)

Table 3. Right-click commands

Command	Present on the following pages
Enable	Administration Tasks Tab: • Active Directory Auditing - object • Active Directory Protection - template or object • Audit Events - event • EMC Auditing - template or file path • Exchange Mailbox Auditing - mailbox • Exchange Mailbox Protection - template or mailbox • Excluded Accounts Auditing - template • AD Query Auditing - container • File System Auditing - template or file path • File System Protection - template or file path • NetApp Auditing - template or file path • Purge Jobs - job • Registry Auditing - template or registry key • Services Auditing - template or service • SharePoint Auditing - template or path • SQL Auditing - template or instance • SQL Data Level Auditing - template Overview page - event (data grid) Search Results page - event (data grid)
Event Details	Overview page - event (data grid) Search Results page - event (data grid)
Exclude	Exchange Mailbox Auditing page - audited mailbox
Expand All	Searches page - folder (left pane)
Export	Searches page: • Folder (left pane) • Search definition (right pane)
Hide Properties	Searches page: • Folder (left pane) • Search definition (right pane) Agent Statistics page - agent
High/Medium/Low	Administration Tasks tab: • Audit Events Auditing
Import Folder	Searches Page - folder (left pane)
Import Search	Searches Page - folder (left pane)
Install or Upgrade	Deployment page - agent
Knowledge Base	Administration Tasks Tab: • Audit Events Auditing Overview page - event (data grid) Search Results page - event (data grid)
Logs **Open Log** **Get All Logs** **View Agent Log** **View Coordinator Log**	Agent Statistics page - agent Coordinator Statistics page - coordinator Deployment page - agent

Table 3. Right-click commands

Command	Present on the following pages
Move	Searches page: • Folder (left pane) • Search definition (right pane)
New **New Folder** **New Search**	Searches Page: • Folder (left pane) • Search definition (right pane)
Overviews	Overview page - event (data grid)
Paste	Administration Tasks tab: • Coordinator Configuration (text boxes) Search Properties tabs: • Report tab (text boxes) • Info tab (text boxes) Searches page: • Folder (left pane) • Search definition (right pane)
Redo	Administration Tasks tab: • Coordinator Configuration (text boxes) Search Properties tabs: • Report tab (text boxes) • Info tab (text boxes)
Refresh Configuration	Administration Tasks tab: • Agents Configuration
Refresh Status	Deployment page - agent
Rename	Searches page - folder (left pane)
Report **Disable Report**	Searches page - search definition (right pane)
Restart Agent	Agent Statistics page - agent
Run	Searches page - Search definition (right pane)
Scope **Object** **One Level** **Subtree**	Exchange Mailbox Auditing page - audited mailbox
Search Properties	Search Results page - event (data grid)
Security	Active Directory Protection page - object Group Policy Protection page - object
Select All	Administration Tasks tab: • Coordinator Configuration - text boxes Event Details pane - text boxes Search Properties tabs: • Report tab (text boxes) • Info tab (text boxes)
Set Agent Uninstalled	Agent Statistics page - agent
Set As My Favorite	Searches page - Search definition (right pane)
Set Coordinator Uninstalled	Coordinator Statistics page - coordinator

Table 3. Right-click commands

Command	Present on the following pages
Show Properties	Searches page • Folder (left pane) • Search Definition (right pane) Agent Statistics page -agent
Start Agent	Agent Statistics page - agent
Stop Agent	Agent Statistics page - agent
Success Only	Administration Tasks tab: • Audit Events - event
Success and Protected Only	Administration Tasks tab: • Audit Events - event
Success and Failed Only	Administration Tasks tab: • Audit Events - event
Undo	Administration Tasks tab: • Coordinator Configuration - text boxes Search Properties tabs: • Report tab (text boxes) • Info tab (text boxes)
Uninstall	Deployment page - agent

27

Change Auditor Email Tags

The Alert Body Configuration dialog allows you to edit the plain text and the HTML representation of alert emails. It consists of the following tabbed pages:

- **Preview -** is for previewing a sample of what your customized email will look like.
- **Main Body** - to define the overall content and layout of the alert email body.
- **Event Details** - to define the details to be included for each event included in the alert email.
- **Signature** - to define the signature line to be included.

The text entered in the these tabs is sent when the alert triggers, with the exception of the variable tags (%xxx%). These tags are used to retrieve information from Change Auditor. The following tags are used and should not be modified.

Table 1. Tags valid in the Main Body tab

Email Tag:	Description:
%AD_MANAGEDBY%	The email address for the user assigned to manage the user referenced in an Active Directory user event.
%AD_USERMAIL%	The email address for the user referenced in an Active Directory user event.
%ALERT_COORDINATOR_DOMAIN%	The name of the domain where the coordinator that generated the alert resides.
%ALERT_COORDINATOR_NAME%	The name of the coordinator generating the alert.
%ALERT_NAME%	The name of the alert that fired.
%ALERT_TIME_SENT%	The date and time when the alert fired.
%ALERT_TYPE%	The type of alert: Smart Alert or Alert.
%BATCH_ID%	The batch ID for all alerts grouped into a single smart alert email.
%EVENT_COUNT%	The number of events grouped into a single smart alert email.
%SMART_ALERT%	Indicates whether this is a smart alert email.
%SMART_ALERT_GROUPING%	Indicates whether this is a smart alert email and on a single object.
%SMART_ALERT_OCCURRENCE%	For smart alerts, the occurrence value specified in ‘Send alert when <*nn*> Events occur within <*nn*> <*interval*>’.
%SMART_ALERT_PERIOD%	For smart alerts, the period of time specified in ‘Send alert when <*nn*> Events occur within <*nn*> <*interval*>’.
%SMART_ALERT_PERIOD_UNIT%	For smart alerts, the time interval (minutes, hours or days) specified in ‘Send alert when <*nn*> Events occur within <*nn*> <*interval*>’.

Table 2. Tags valid in the Event Details tab

Email Tag:	Description:
%AAD_ACTIVITYORIGIN%	For Microsoft Entra events, the origin of the activity.
%AAD_ACTIVITYSTATUSREASON%	For Microsoft Entra events, the status reason.
%AAD_ACTIVITYTYPE%	For Microsoft Entra events, the type of activity.
%AAD_CATEGORY%	For Microsoft Entra events, the associated category.

Table 2. Tags valid in the Event Details tab

Email Tag:	Description:
%AAD_CITY%	For Microsoft Entra events, the associated city.
%AAD_COUNTRY%	For Microsoft Entra events, the associated country.
%AAD_ONPREMISESSUBJECT%	For Microsoft Entra events, the associated Active Directory on premises subject.
%AAD_ONPREMISESTARGET%	For Microsoft Entra events, the associated Active Directory on premises target.
%AAD_ONPREMISESUSERNAME%	For Microsoft Entra events, the associated Active Directory on premises username.
%AAD_STATE%	For Microsoft Entra events, the associated state.
%AAD_SUBJECTDISPLAYNAME%	For Microsoft Entra events, the associated subject display name.
%AAD_SUBJECTSYNCTYPE%	For Microsoft Entra events, the associated subject synchronization type.
%AAD_TARGETDISPLAYNAME%	For Microsoft Entra events, the target display name.
%AAD_TARGETSYNCTYPE%	For Microsoft Entra events, the target synchronization type.
%AAD_TENANTDEFAULTDOMAIN%	For Microsoft Entra events, the tenant default domain.
%AAD_TENANTDISPLAYNAME%	For Microsoft Entra events, the tenant display name.
%ACTIONNAME%	The action associated with the event (e.g., Modify Attribute).
%AD_SAMACCOUNTNAME%	For Active Directory events, the logon name of the user who initiated the change event.
%AD_FAILURE_REASON%	For Active Directory events, the failure reason for failed events.
%AD_STATUS_CODE%	For Active Directory events, the status code for failed events.
%AD_USERPRINCIPALNAME%	For Active Directory events, the user principal name (UPN) of the user who initiated the change event.
%ADAM_CONFIGURATIONSET%	For ADAM (AD LDS) events, the name of the configuration set that holds the ADAM instance where the change occurred.
%ADAM_INSTANCENAME%	For ADAM (AD LDS) events, the name of the ADAM instance where the change occurred.
%ADAM_INSTANCEPORT%	For ADAM (AD LDS) events, the communications port used by the ADAM instance where the change occurred.
%ADAM_PARTITIONNAME%	For ADAM (AD LDS) events, the name of the directory partition where the change event occurred.
%ALERT_COORDINATOR_DOMAIN%	The name of the domain where the coordinator that generated the alert resides.
%ALERT_COORDINATOR_NAME%	The name of the coordinator generating the alert.
%ALERT_NAME%	The name of the alert that fired.
%ALERT_TIME_SENT%	The date and time when the alert fired.
%ALERT_TYPE%	The type of alert: Smart Alert or Alert.
%ATTRIBUTENAME%	For Active Directory and ADAM (AD LDS) events, the name of the schema attribute that was modified (e.g., displayName). For File System events, the name of the file or folder attribute that was modified.
%BATCH_ID%	The batch ID assigned to all alerts grouped into a single smart alert email.
%COMMENT%	Any comments for the event which were entered using the Comments feature on the Event Details pane.

Table 2. Tags valid in the Event Details tab

Email Tag:	Description:
%DOMAINCONTROLLER%	Indicates whether the agented server is a domain controller.
%DOMAINDN%	The distinguished name (DN) of the domain to which the agent that generated the alert belongs.
%DOMAINFQDN%	The fully qualified domain name (FQDN) of the domain to which the Change Auditor agent that generated the alert belongs.
%DOMAINNAME%	The name of the domain to which the agent that generated the alert belongs.
%EVENT_COUNT%	The number of events grouped into a smart alert email.
%EVENTCLASSNAME%	The event name.
%EVENTMESSAGE%	The actual event that triggered the alert.
%EVENTSOURCE%	Indicates the application where the change event came from: Change Auditor, Active Roles, or GPOADmin.
%EXCHANGE%	Indicates whether the agented server is an Exchange server.
%FACILITYNAME%	The name of the event class facility to which the event belongs (e.g., Domain Configuration).
%FORESTNAME%	The name of the forest where the agent that captured the event resides.
%FS_ATTRIBUTENAME%	For File System events, the name of the attribute that was modified.
%FS_FILENAME%	For File System events, the name of the file that was modified.
%FS_FILESERVER%	For File System events, the name of the server where the file or folder that was modified resides.
%FS_FILESYSTEMTYPEID%	For File System events, the type of object (File or Folder) that was modified.
%FS_FOLDERPATH%	For File System events, the full path of the file or folder where the modification occurred.
%FS_LOGONID%	For File System events, the logon ID of the user who made the change.
%FS_PRIMARYSID%	For File System events, the SID of the user who made the change.
%FS_PROCESSNAME%	For File System events, the full path of the application responsible for the change.
%FS_SHARENAME%	For File System events, the name of the local share that was modified.
%FS_TRANSACTIONID%	For File System Transaction Status Changed events, the identification number assigned to a transaction.
%FS_TRANSACTIONSTATUS%	For File System Transaction Status Changed events, the current status of the transaction.
%GLOBALCATALOG%	Indicates whether the agented server is a Global Catalog.
%GPO_POLICYCANONICAL%	For Group Policy events, the canonical name (CN) of the group policy that was modified.
%GPO_POLICYITEM%	For Group Policy events, the group policy item that was modified.
%GPO_POLICYNAME%	For Group Policy events, the name of the group policy that was modified.
%GPO_POLICYSECTION%	For Group Policy events, the section of the group policy that was modified.
%INITIATORMAIL%	For events generated by Active Roles or GPOAdmin, the email address of the user that initiated the change event.
%INITIATORSID%	For events generated by Active Roles or GPOAdmin, the SID of the user that initiated the change event.

Table 2. Tags valid in the Event Details tab

Email Tag:	Description:
%INITIATORUSERNAME%	For events generated by Active Roles or GPOADmin, the name of the user that initiated the change event.
%IPADDRESS%	The IP address of the Change Auditor agent that generated the alert.
%LDAP_ATTRIBUTES%	For AD Query events, the attributes that were queried.
%LDAP_ELAPSED%	For AD Query events, how long the AD query took to run.
%LDAP_FILTER%	For AD Query events, the filter string used in the AD query.
%LDAP_OCCURRENCES%	For AD Query events, the number of times the AD query occurred during the specified interval.
%LDAP_RESULTS%	For AD Query events, the number of results returned as a result of the query.
%LDAP_SCOPE%	For AD Query events, the scope of coverage: This object only or This object and all children.
%LDAP_SINCE%	For AD Query events, the date and time when the AD query was first initiated.
%LDAP_TYPE%	For AD Query events, the type of query: LDAP or GC.
%LOGON_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).
%LOGON_END%	For Logon Session events, the date and time when the user logged out of the computer.
%LOGON_SESSIONEND%	For Logon Session events, the date and time when the current user session ended.
%LOGON_SESSIONSTART%	For Logon Session events, the date and time when the current user session began.
%LOGON_START%	For Logon Session events, the date and time when the user initially logged onto the computer.
%LOGON_TYPE%	For Logon Activity events, the type of logon that occurred: • Domain Authentication • Interactive • Remote Interactive
%OBJECTCANONICAL%	For Active Directory and ADAM (AD LDS) events, the canonical name of the object that was modified. For Group Policy events, the canonical name of the group policy that was modified. For AD Query events, the LDAP object canonical name of the object that was queried.
%OBJECTCLASS%	For Active Directory and Exchange events, the object class that was modified (e.g., groupPolicyContainer). For ADAM (AD LDS) events, the object class that was modified (e.g., container, user, group). For AD Query events, the object class that was queried.
%OBJECTNAME%	For Active Directory and Exchange events, the name of the object that was modified. For ADAM (AD LDS) events, the distinguished name of the object that was modified. For Group Policy events, the name of the group policy that was modified. For AD Query events, the name of the object that was queried.

Table 2. Tags valid in the Event Details tab

Email Tag:	Description:
%ORGANIZATIONALUNIT%	For Active Directory and ADAM (AD LDS) events, the OU associated with the object that was modified. For Group Policy events, the name of the OU that is linked to the group policy that was modified. For AD Query events, the name of the OU associated with the LDAP query.
%OSVERSION%	Indicates the operating system version of the machine where the modification occurred.
%REGISTRYKEY%	For Registry events, the name of the registry key that was modified.
%REGISTRYVALUE%	For Registry events, the registry value that was modified.
%RESULTNAME%	Indicates the result of the operation mentioned in the event: • Success • Protected • Failed • None
%SAM_PRINCIPALNAME%	The logon name of the local account that initiated the change event.
%SAM_PRINCIPALTYPE%	The type of local account that initiated the change event.
%SERVERDN%	The distinguished name (DN) of the agented server that captured the event.
%SERVERFQDN%	The fully qualified domain name (FQDN) of the agented server that captured the event.
%SERVERNAME%	The name of the agented server where the change occurred.
%SERVEROU%	The name of the organizational unit where the agented server resides.
%SERVICE_DISPLAYNAME%	For Service events, the display name of the service that was modified.
%SERVICE_NAME%	For Service events, the name of the service that was modified.
%SEVERITYNAME%	The severity assigned to the change event: High, Medium or Low.
%SHAREPOINT_FARMNAME%	For SharePoint events, the name of the SharePoint farm where the modification occurred.
%SHAREPOINT_ITEMNAME%	For SharePoint events, the name of the SharePoint item (e.g. document, folder, list item) that was modified.
%SHAREPOINT_ITEMURL%	For SharePoint events, the URL of the SharePoint item that was modified.
%SHAREPOINT_LISTNAME%	For SharePoint events, the name of the SharePoint list that was modified.
%SHAREPOINT_LISTPATH%	For SharePoint events, the full path of the SharePoint list where the modification occurred.
%SHAREPOINT_WEBNAME%	For SharePoint events, the name of the web site where the modification occurred.
%SHAREPOINT_WEBURL%	For SharePoint events, the URL of the web site where the modification occurred.
%SIGNSEAL%	For Active Directory and AD Query events, indicates whether the LDAP operation or LDAP query is signed using Kerberos-based encryption.
%SITEDN%	The distinguished name (DN) of the site where the agented server resides.
%SITENAME%	The name of the site where the agented server resides.
%SMART_ALERT%	Indicates whether this is a smart alert email.

Table 2. Tags valid in the Event Details tab

Email Tag:	Description:
%SMART_ALERT_GROUPING%	Indicates whether this is a smart alert email and on a single object.
%SMART_ALERT_OCCURRENCE%	For smart alerts, the occurrence value specified in 'Send alert when <*nn*> Events occur within <*nn*> <*interval*>'.
%SMART_ALERT_PERIOD%	For smart alerts, the period of time specified in 'Send alert when <*nn*> Events occur within <*nn*> <*interval*>'.
%SMART_ALERT_PERIOD_UNIT%	For smart alerts, the time interval (minutes, hours or days) specified in 'Send alert when <*nn*> Events occur within <*nn*> <*interval*>'.
%SQL_APPLICATIONNAME%	For SQL events, the name of the client application that initiated the change event.
%SQL_CLIENTPROCESSID%	For SQL events, the identification number associated with the client process that initiated the change event.
%SQL_DATABASEID%	For SQL events, the identification number associated with the SQL database used by the process that initiated the change event.
%SQL_DATABASENAME%	For SQL events, the name of the SQL database used by the process that initiated the change event.
%SQL_EVENTCLASS%	For SQL events, the SQL Server operation (event class) that was performed.
%SQL_EVENTSUBCLASS%	For SQL events, the type of event subclass that was performed.
%SQL_HOSTNAME%	For SQL events, the name of the client workstation that initiated the session.
%SQL_INSTANCENAME%	For SQL events, the name of the SQL instance where the change event occurred.
%SQL_ISSYSTEM%	For SQL events, indicates whether a system session initiated the change.
%SQL_LINKEDSERVERNAME%	For SQL events, the name of the linked server.
%SQL_OBJECTID%	For SQL events, the object identifier associated with the SQL object that was changed.
%SQL_OBJECTID2%	For SQL events, the object identifier of related objects or entities, if available.
%SQL_OBJECTNAME%	For SQL events, the name of the SQL Server object that was changed.
%SQL_OBJECTTYPE%	For SQL events, the type of SQL Server object that was changed.
%SQL_OWNERID%	For SQL lock events, the type of object that owns a lock.
%SQL_OWNERNAME%	For SQL events, the database user name of the object owner.
%SQL_PARENTNAME%	For SQL events, the name of the schema in which the object that changed resides.
%SQL_PROVIDERNAME%	For SQL events, the name of the OLEDB provider.
%SQL_ROWCOUNTS%	For SQL events, the number of rows returned by the SQL query.
%SQL_SESSIONLOGINNAME%	For SQL events, the SQL Server login name used by the client to create the session.
%SQL_SPID%	For SQL events, the SQL Server Process ID associated with the process that initiated the change.
%SQL_SUCCESS%	For SQL events, indicates whether the event was successful.
%SQL_TEXTDATA%	For SQL events, the character string used in the SQL query.
%SSLTLS%	For Active Directory or AD Query events, indicates whether the LDAP operation or LDAP query is secured using SSL or TLS technology.
%SUBSYSTEMNAME%	The subsystem, or area of auditing, where the change event occurred (e.g., Active Directory, Service, Group Policy).

Table 2. Tags valid in the Event Details tab

Email Tag:	Description:
%TIMEBATCHED%	The UTC date and time when the batch of events were sent from the agent to coordinator.
%TIMEDETECTED%	The UTC date and time when the agent captured the event.
%TIMEOFDAY%	The UTC time (no date) when the event the agent captured the event.
%TIMERECEIVED%	The UTC date and time when the event was received by Change Auditor.
%TIMEZONE%	The name of the time zone used for the alert's date/time stamps in the email.
%TIMEZONETIMEDETECTED%	The date and time when the Change Auditor agent captured the event, based on the selected time zone.
%TIMEZONETIMERECEIVED%	The date and time when the event was received by Change Auditor, based on the selected time zone.
%USERADDRESS%	The machine name or IP address of the machine where the change originated.
%USERADDRESSIPV4%	The IPv4 IP address of the machine where the change originated.
%USERADDRESSIPV6%	The IPv6 IP address of the machine where the change originated.
%USERDISPLAY%	The display name of the user who initiated the change.
%USERMAIL%	The email address of the user that initiated the change.
%USERNAME%	The NT4 logon name (domain\name) of the user who initiated the change.
%USERSID%	The security identifier (SID) assigned to the user who initiated the change.
%VALUENEW%	The new value that is now assigned to the object.
%VALUEOLD%	The old value that was assigned to the object.

The event details defined in the Event Details tab are placed in the Main Body pane using the following tag:

%EVENT_DETAILS%

This tag should NOT be removed from the Main Body tab if you want to include the event details in the alert emails.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.