Quest

Quest® Change Auditor for Active Directory 7.4
User Guide

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

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

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

Legend

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

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

Change Auditor for Active Directory User Guide
Updated - November 2023
Software Version - 7.4

Contents

1

Change Auditor for Active Directory Overview

Introduction

Quest Change Auditor for Active Directory drives the security and control of Microsoft Active Directory by tracking vital configuration changes in real-time. From GPO and schema to critical group and operational changes, Change Auditor for Active Directory tracks, audits, reports, and alerts on changes that impact your directory without the overhead costs of system-provided auditing.

In addition, Change Auditor for Active Directory allows you to lock down critical Active Directory, ADAM (AD LDS), and Group Policy Objects, to protect them from unauthorized or accidental modifications or deletions.

You can also track on Azure Active Directory changes. Change Auditor correlates activity across the on-premises and cloud environment making it easy to search all events regardless of where they occurred. For more information, see the Change Auditor for Office 365 and Azure Active Directory Auditing User Guide.

To ensure Active Directory compliance, you can automatically generate intelligent and in-depth reports, protecting you against policy violations and avoiding the risks and errors associated with day-to-day modifications. For fast troubleshooting, you always get the original and current values.

NOTE: Active Directory auditing and protection are 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.**

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

- For information on the core functionality available in Change Auditor regardless of the product license that has been applied, see the Change Auditor User Guide and the Change Auditor Installation Guide.
- For event details, see the Change Auditor for Active Directory Event Reference Guide.

Deployment Requirements

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

Client Components and Features

The following table lists the client components and features that require a valid Change Auditor for Active Directory license. You are not prevented you from using these features; however, associated events or protection are not captured and enforced unless the proper license is applied.

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

Table 1. Change Auditor for Active Directory components and features

Page	Component and Feature:
Administration Tasks Tab	Agent Configuration Page: • Event Logging - enable/disable event logging: ▪ Active Directory ▪ ADAM (AD LDS) **NOTE:** See Custom Active Directory Object Auditing for information about enabling event auditing. Auditing Task List: • Active Directory ▪ Attributes ▪ Member of Group • ADAM (AD LDS) ▪ Attributes **NOTE:** See Custom Active Directory Object Auditing, Custom Active Directory Attribute Auditing, Member of Group Auditing, or ADAM (AD LDS) Auditing for information about defining custom Active Directory auditing. Protection Task List: • Active Directory • ADAM (AD LDS) • Group Policy **NOTE:** See Active Directory Protection for more information about defining Active Directory object, ADAM object, and Group Policy object protection.
Event Details Pane	What Details: • Class (AD) • Object (AD) • Type (AD events associated with groups) • Policy (Group Policy) • Section (Group Policy) • Item (Group Policy) • SSL/TLS (AD) • Kerberos (AD) • Simple Bind (AD) • Port (AD) **Restore Value** tool bar button **NOTE:** See the Event Details Pane appendix for more information. **NOTE:** See Custom Active Directory Searches and Reports for more information.

Table 1. Change Auditor for Active Directory components and features

Page	Component and Feature:
Events	Facilities: • Configuration Monitoring • Connection Object • Custom AD Object Monitoring • Custom Computer Monitoring • Custom Group Monitoring • Custom User Monitoring • DNS Service • DNS Zone • Domain Configuration • Dynamic Access Control • Forest Configuration • FRS Service • Group Policy Item • Group Policy Object • IP Security • NETLOGON Service • NTDS Service • Organizational Unit (OU) • Replication Transport • Schema Configuration • Site Configuration • Site Link Bridge Configuration • Site Link Configuration • Subnets • SYSVOL
Overview Page	Count of Events by: • Subsystem | Active Directory | Attributes • Subsystem | Active Directory | Object • Subsystem | Active Directory | Object Class • Subsystem | Group Policy
Search Properties	What Tab: • Subsystem | Active Directory • Subsystem | ADAM (AD LDS) • Subsystem | Group Policy • Object Class **NOTE:** See Custom Active Directory Searches and Reports for information about using the What tab to create custom Active Directory search queries.

Table 1. Change Auditor for Active Directory components and features

Page	Component and Feature:
Searches Page	Built-in Reports: • All reports that include the events in the facilities listed above.
Alert Body Configuration Dialog - Event Details Tab	Variables (email tags): • AD_SAMACCOUNTNAME • AD_STATUS_CODE • AD_FAILURE_REASON • AD_USERMAIL • AD_USERPRINCIPALNAME • ADAM_CONFIGURATIONSET • ADAM_INSTANCENAME • ADAM_INSTANCEPORT • ADAM_PARTITIONNAME • GPO_POLICYCANONICAL • GPO_POLICYITEM • GPO_POLICYNAME • GPO_POLICYSECTION **NOTE:** See the Quest Change Auditor User Guide for a description of these email tags and how to configure alert email notifications.

2

Custom Active Directory Searches and Reports

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 allow you to define custom searches.

This section explains how to run the built-in All Active Directory Events and All Group Policy Events reports and how to create custom Active Directory searches using the What tab, including how to construct searches using wildcard expressions. For a description of the dialogs mentioned in this topic, see the online help.

Run the All Active Directory Events report

Running this report retrieves changes (all actions and results) to all Active Directory objects being audited.

1. From the Searches tab, expand the **Shared | Built-in | All Events** folder.
2. Locate and double-click **All Active Directory Events** in the right pane.

   This displays a new Search Results page displaying the Active Directory events captured over the last seven days.

Run the All Group Policy Events report

Running this report retrieves changes (all actions and results) to all Group Policy objects.

1. From the Searches tab, expand the **Shared | Built-in | All Events** folder.
2. Locate and double-click **All Group Policy Events** in the right pane.

   This displays a new Search Results page displaying the Group Policy events captured over the last seven days.

Create custom searches

The following scenarios explain how to use the What tab to create custom searches.

NOTE: You can use the other search properties tabs to define additional criteria:

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

To search for changes to a specific Active Directory container:

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

   Selecting the **Private** folder creates a search that only you can run and view, whereas selecting the **Shared** folder creates a search which can be run and viewed by all users.
3. Click **New** to enable the Search Properties tabs across the bottom of the Searches page.
4. On the Info tab, enter a name and description for the search.
5. On the What tab, expand **Add** and select **Subsystem | Active Directory.**

   NOTE: You can use **Add with Events | Subsystem | Active Directory** (instead of **Add | Subsystem | Active Directory**) to search for an entity that already has an event associated with it in the database.
6. On the Add Active Directory Container dialog, select one of the following options to define the scope of coverage:
   - **All Active Directory Objects** - select to include all objects. (Default when the Add tool bar button is used).
   - **This Object** - select to include the selected objects only. (Default when the Add With Events tool bar button is used).
   - **This Object and Child Objects Only** - select to include the selected objects and its direct child objects.
   - **This Object and All Child Objects** - select to include the selected objects and all subordinate objects (in all levels).
   - **Members of this group** - select this option to show changes made to users in a specified group. Nested groups are not supported.

   NOTE: You cannot exclude selections or use the *Like wildcard option when the scope is specified as Members of this group.
7. By default, **All Actions** is selected meaning that all the activity associated with the object generate an audited event. However, you can clear the **All Actions** option and select individual options. The options available are:
   - **All Actions** - select to include when any of the following actions occur (Default)
   - **Add Attribute** - select to include when an attribute is added
   - **Delete Attribute** - select to include when an attribute is deleted
   - **Modify Attribute** - select to include when an attribute is modified
   - **Rename Object** - select to include when an object is renamed

- **Add Object** - select to include when an object is added
- **Delete Object** - select to include when an object is deleted
- **Move Object** - select to include when an object is moved
- **Other** - select to include other types of activity against the selected object

8 By default, **All Transports** is selected indicating that all Active Directory events regardless of the transport protocol used are included in the search. However, you can clear the **All Transports** option and select individual options. The transport options available are:

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

NOTE: When you clear the **All Transports** check box and select both the **SSL/TLS** and **Kerberos** check boxes, only AD queries using both of these transport protocols will be included in the search results.

9 When a scope other than **All Active Directory Objects** is selected, the directory object picker is enabled allowing you to select the objects to include in the search definition.

Use either the Browse or Search page to search your environment to locate and select the Active Directory objects to include. Use the Options page to view or modify the search options to be used to retrieve directory objects.

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.

You can also select **Import Objects** to import a .csv (comma separated value) file containing a list of directory objects. Using this list, you can specify object names and optional values for the search criteria. You can use the * wildcard character to match any string of zero or more characters when specifying the Name values.

NOTE: For optimal performance, do not include more than 1000 objects in your import file.

The import will fail and an error message will be displayed if any errors are detected with the column names or specified values.

NOTE: Column names and values must be separated with a comma.

NOTE: If an optional column name is not specified, then the default All is used for the value for each object. The default All is also used if the optional column is specified, but the value is empty. Mandatory Name values cannot be empty.

COLUMNS	DESCRIPTION
Name (Required)	The name of the directory object to import. Name values must be specified in canonical name format. **NOTE:** The first column must be Name. **NOTE:** Wildcard characters are only supported for the Name values. Examples: Column: Name Values: • test.domain.ca/OU1/User1 • test.domain.ca/*/Group1 • test.domain.ca/OU1/*User*
Actions (Optional)	Possible values include: Add Attribute, Delete Attribute, Modify Attribute, Rename Object, Add Object, Delete Object, Move Object or Other. When specifying multiple values they must be separated by the Pipe character '|'. Examples: Columns: Name,Actions Values: • test.domain.ca/OU1/User1,Move Object|Modify Attribute • test.domain.ca/OU1/Group*,
Transports (Optional)	Possible values include SSL/TLS, Kerberos or Simple Bind. When specifying multiple values they must be separated by the Pipe character '|'. Examples: Columns: Name,Actions,Transports Values: • test.domain.ca/OU1/User1,Move Object|Modify Attribute,Kerberos • test.domain.ca/OU1/Group1,,Kerberos |SSL/TLS
Port (Optional)	The number of the required port. Examples: Columns: Name,Actions,Transports,Port Values: • test.domain.ca/OU1/*,Move Object|Modify Attribute,Kerberos,389 • test.domain.ca/OU1/Group1,Add Attribue,Kerberos, **NOTE:** When importing a file in the web client, the default value (All Ports) will be applied if port values are specified.

NOTE: Select the **Exclude the Above Selection(s)** check box to search for changes to all directory objects except those listed in the ‘what’ list.

NOTE: Select the **Runtime Prompt** check box on this dialog to prompt for a directory object every time the search is run.

10 Once you have added all the Active Directory objects to be included in the search, click **OK** to save your selection and close the dialog.

11 Once you have defined the search criteria, you can either save the search definition or run the search.

- To save the search definition without running it, click **Save**.
- To save and run the search, click **Run**.

When this search is run, Change Auditor searches for changes to the Active Directory objects specified on the What tab.

To construct an Active Directory object search using a wildcard expression:

1 Open the Searches page.

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

Selecting the **Private** folder will create a search that only you can run and view, whereas selecting the **Shared** folder will create a search which can be run and viewed by all Change Auditor users.

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

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

5 On the What tab, expand **Add** and select **Subsystem | Active Directory.**

6 On the Add Active Directory Container dialog, select the **This Object** scope.

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 By default, **All Actions** and **All Transports** are included. To change any of these settings, clear the corresponding check box and select the individual options.

8 Use the wildcard expression fields in the middle of the dialog to specify the expression to be used to search for Active Directory objects (Object Name column in Search Results grid).

- Select the comparison operator to be used: **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*** will find Active Directory objects that contain ‘admin’ anywhere in their name.
- Use **Add** to add the wildcard expression to the Selected Objects list box at the bottom of the dialog.

9 After entering the wildcard expression to be used, click **OK** to close the dialog and add the wildcard expression to the ‘what’ list.

10 Once you have defined the search criteria, you can either save the search definition or run the search.

- To save the search definition without running it, click **Save**.
- To save and run the search, click **Run**.

To search for changes to a specific Group Policy container:

1 Open the Searches page.

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

Selecting the **Private** folder will create a search that only you can run and view, whereas selecting the **Shared** folder will create a search which can be run and viewed by all Change Auditor users.

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

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

5 On the What tab, expand **Add** and select **Subsystem | Group Policy.**

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

6 On the Add Group Policy Container dialog, select one of the following options to define the scope of coverage:

- **All Objects** - select to include all objects (Default)
- **This Object** - select to include the selected object only

7 When the **This Object** scope option is selected, use either the Browse or Search page to search your environment to locate and select the Group Policy objects to include in the search.

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.

8 Use the Options page to view or modify the search options to be used to retrieve directory objects.

> **NOTE:** On the Add Group Policy Container, the Search page is initially displayed which contains **GroupPolicyContainer** in the Find field and an * wildcard character in the Canonical Name field. Simply click the **Search** button on this page to locate the Group Policy containers in your environment.

You can also select **Import Objects** to import a .csv (comma separated value) file containing a list of directory objects. Using this list, you can specify object names for the search criteria. You can use the * wildcard character to match any string of zero or more characters when specifying the Name values.

> **NOTE:** For optimal performance, do not include more than 1000 objects in your import file.

The import will fail and an error message will be displayed if any errors are detected.

COLUMNS	DESCRIPTION
Name (Required)	The name of the directory object to import. Name values must be specified in canonical name format. Examples: Column: Name Values: • test.domain.ca/System/Policies/{D72618D2-1413-4352-8EC9-FA4A33CBE99C} • test.domain.ca/System/Policies/*

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

> **NOTE:** Select the **Runtime Prompt** check box on this dialog to prompt for a Group Policy Object every time the search is run.

9 Once you have added all the Group Policy Objects to be included in the search, click **OK** to save your selection and close the dialog.

10 Once you have defined the search criteria, you can either save the search definition or run the search.

- To save the search definition without running it, click **Save**.
- To save and run the search, click **Run**.

When this search is run, Change Auditor searches for changes to the Group Policy Objects specified on the What tab.

To construct a Group Policy object search using a wildcard expression:

1 Open the Searches page.

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

Selecting the **Private** folder will create a search that only you can run and view, whereas selecting the **Shared** folder will create a search which can be run and viewed by all Change Auditor users.

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

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

5 On the What tab, expand **Add** and select **Subsystem | Group Policy.**

6 On the Add Group Policy Container dialog, select the **This Object** scope.

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 By default, **All Results** will be included. To change this setting, clear the **All Results** check box and select the individual results to be included.

8 Use the wildcard expression fields in the middle of the dialog to specify the expression to be used to search for Group Policy objects (Object and Canonical Name columns in Search Results grid).

- Select the comparison operator to be used: **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 Default* will find Group Policy objects whose name begins with the word 'Default'.
- Use the **Add** button to add the wildcard expression to the Selected Objects list box at the bottom of the dialog.

9 After entering the wildcard expression to be used, click **OK** to close the dialog and add the wildcard expression to the 'what' list.

10 Once you have defined the search criteria, you can either save the search definition or run the search.

- To save the search definition without running it, click **Save**.
- To save and run the search, click **Run**.

To search for changes to a specific object class (classSchema object):

1 Open the Searches page.

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

Selecting the **Private** folder will create a search that only you can run and view, whereas selecting the **Shared** folder will create a search which can be run and viewed by all Change Auditor users.

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

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

5 On the What tab, expand **Add** and select **Object Class.**

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

6 On the Add Object Class dialog select an object class and click **Add** to add it to the list box located across the bottom of the dialog. Repeat this step to add additional object classes.

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

> **NOTE:** Select the **Runtime Prompt** check box on this dialog to prompt for an object class every time the search is run.

7 Once you have made your selections, click **OK** to save your selection and close the dialog.

8 Once you have defined the search criteria, you can either save the search definition or run the search.

- To save the search definition without running it, click **Save**.
- To save and run the search, click **Run**.

When this search is run, Change Auditor searches for changes to the object classes specified on the What tab.

To search for changes to a specific ADAM (AD LDS) container:

1 Open the Searches page.

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

Selecting the **Private** folder will create a search that only you can run and view, whereas selecting the **Shared** folder will create a search which can be run and viewed by all Change Auditor users.

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

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

5 On the What tab, expand **Add** and select **Subsystem | ADAM (AD LDS).**

> **NOTE:** You can use **Add with Events | Subsystem | ADAM (AD LDS)** (instead of **Add | Subsystem | ADAM (AD LDS)**) to search for an entity that already has an event associated with it in the database.

6 On the Select the agent that hosts the ADAM/AD LDS instance dialog, use the Browse or Search page to locate and select the agent that hosts the ADAM (AD LDS) instance to be searched.

> **NOTE:** The Explorer View is displayed by default; however, this display will not include member servers. Therefore, if you have installed ADAM (AD LDS) on a workgroup server, select the **Grid View** option at the top of the dialog to select from a list of workgroup servers.

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

If credentials are required, a Credentials Required dialog is displayed allowing you to enter the credentials to be used to access the selected instance.

7 On the Add ADAM (AD LDS) Container dialog, select one of the following options to define the scope of coverage:

- **All ADAM (AD LDS) Objects** - select to include all objects. (Default when the Add tool bar button is used.)
- **This Object** - select to include the selected objects only. (Default when the Add With Events tool bar button is used).
- **This Object and Child Objects Only** - select to include the selected objects and its direct child objects.
- **This Object and All Child Objects** - select to include the selected objects and all subordinate objects (in all levels).
- **Members of this group** - select this option to show changes made to users in a specified group. Nested groups are not supported.

> **NOTE:** You cannot exclude selections or use the *Like wildcard option when the scope is specified as Members of this group.

8 By default, **All Actions** is selected meaning that all of the activity associated with the object will generate an audited event. However, you can clear the **All Actions** option and select individual options. The options available are:

- **All Actions** - select to include when any of the following actions occur (Default)
- **Add Attribute** - select to include when an attribute is added
- **Delete Attribute** - select to include when an attribute is deleted
- **Modify Attribute** - select to include when an attribute is modified
- **Rename Object** - select to include when an object is renamed
- **Add Object** - select to include when an object is added

- **Delete Object** - select to include when an object is deleted
- **Move Object** - select to include when an object is moved
- **Other** - select to include other types of activity against the selected object

9 By default, **All Transports** is selected indicating that all Active Directory events regardless of the transport protocol used will be included in the search. However, you can clear the **All Transports** option and select individual options. The transport options available are:

- **All Transports** - select to include LDAP operation or LDAP queries regardless of the transport protocol used (Default)
- **SSL/TLS** - select to include LDAP operation or LDAP queries that are secured using SSL or TLS technology
- **Kerberos**- select to include LDAP operation or LDAP queries that are signed using Kerberos-based encryption

NOTE: When you clear the **All Transports** check box and select both the **SSL/TLS** and **Kerberos** check boxes, only AD queries using both of these transport protocols will be included in the search results.

- **Port** - select to identify a specific port used for communication

10 When a scope other than **All ADAM (AD LDS) Objects** is selected, the directory object picker is activated allowing you to select the ADAM (AD LDS) containers to be included in the search definition.

Use either the Browse or Search page to search your environment to locate and select the ADAM (AD LDS) containers to be included.

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.

Use the Options page to view or modify the search options or ADAM instance to be used to retrieve directory objects.

Once you select a container to be included, click **Add** to add it to the list at the bottom of the dialog.

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

NOTE: Select the **Runtime Prompt** check box on this dialog to prompt for an ADAM (AD LDS) container every time the search is run.

11 Once you have added all the ADAM (AD LDS) containers to be included in the search, click **OK** to save your selection and close the dialog.

12 Once you have defined the search criteria, you can either save the search definition or run the search.

- To save the search definition without running it, click **Save**.
- To save and run the search, click **Run**.

When this search is run, Change Auditor searches for changes to the ADAM containers specified on the What tab.

3

Custom Active Directory Object Auditing

Introduction

By default, Change Auditor audits the Enterprise for all Active Directory events. To see a complete list of the Active Directory events that are audited by default, go to the Audit Events table (Administration Task->Auditing->Audit Events), and sort by license.

Using the Active Directory Auditing wizard, you can define additional custom object classes to be audited, as well as specify where you want to conduct the audit (for example, enterprise, or individual object).

This section provides a description of the Active Directory Auditing page and explains how to define custom Active Directory object auditing. For a description of the dialogs mentioned in this chapter, refer to the online help.

Active Directory Auditing page

The Active Directory Auditing page is used to define additional Active Directory custom events that you want to audit. The page is displayed when you select Active Directory from the Auditing task list in the navigation pane of the Administration Tasks tab. Custom Active Directory events will contain the word ‘custom’ in their facility name, for example “Custom User Monitoring”. By default user, group and computer object classes are selected on this page.

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, refer to the Change Auditor User Guide for more information on how to gain access.

NOTE: If you receive a message stating that the client is unable to acquire exclusive access to object monitoring, there is another user using the Active Directory Auditing page and therefore, all of the tool bar buttons will be deactivated preventing you from making any changes.

The Active Directory Auditing page contains an expandable view of the Active Directory objects selected for auditing. Initially, the list box will contain an entry for auditing all user, computer and group object classes in the entire enterprise.

To add an object to this list, use the **Add** tool bar button (or to add multiple objects, expand the **Add** tool bar button and select the **Select Multiple Objects** option). Once added, the following information will be displayed:

Object

Displays the distinguished name of object.

Status

Indicates whether the auditing for a selected object is enabled or disabled.

Scope

Displays the scope of coverage:

- Forest
- Object
- One Level
- SubTree

Object Class

This field is used for filtering data.

If the view is not already expanded, click the expansion box to the left of an object to expand the view to display the object classes and monitored attributed to be audited in the object.

Object Class

Displays the object class being audited (such as computer, user, and group.)

Monitored Attributes

Displays the number of schema attributes selected for auditing by Change Auditor for each object class listed.

NOTE: Attribute auditing is specified using the AD Attribute Auditing page.

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 the Change Auditor User Guide.

Custom Active Directory object auditing

Custom auditing allows you to specify custom Active Directory object classes and attributes to audit. A new event will be added for each object selected for auditing. Once set, these events are identified with “Custom” in the facility name.

By default, Change Auditor audits user, group and computer custom object classes. If you remove the custom objects from the Active Directory Auditing wizard you will no longer receive audit events for them. This will not affect ‘non-custom’ events and those will still be audited by Change Auditor.

To add an Active Directory object to the auditing list:

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **Active Directory** in the Auditing task list.

4 Click **Add** to open the Active Directory Auditing wizard, which steps you through the process of defining the objects and object classes to audit.

5 Select where to conduct the audit:

- Enterprise (Default)
- This object only
- This object and child objects only
- This object and all child objects

6 If you selected the **This Object**, **This Object and Child Objects Only**, or **This Object and All Child Objects** option, use the Browse or Search pages to locate the directory object or container to audit.

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 If you selected either the **This Object and Child Objects Only** or **This Object and All Child Objects** option, select **Next** to define the object classes to audit.

Use one of the following methods to move an object class to the Audited Object Class list (right-hand pane):

- Select one or more object classes in the UnAudited Object Class list and click **Add**.
- Select one or more object classes in the UnAudited Object Class list and 'drag and drop' the selected object classes into the Audited Object Class list.
- Double-click an object class in the UnAudited Object Class list.

You must select at least one object class for auditing.

8 After selecting the Active Directory objects (and object classes) to audit, click **Finish** to save your selection, close the wizard and return to the Active Directory Auditing page.

To add multiple Active Directory objects to the auditing list:

1 Open the Active Directory Auditing page.

2 Expand **Add** and select **Select Multiple Objects**.

3 Select where to conduct the audit:

- Enterprise (Default)
- This object only
- This object and child objects only
- This object and all child objects

4 If you selected the **This Object**, **This Object and Child Objects Only**, or **This Object and All Child Objects** option, use the Browse or Search pages to locate the directory object or container to audit.

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.

After selecting a directory object or container, click **Add** to add the selected object to the list box at the bottom of the page.

Repeat this step to add multiple Active Directory objects.

5 If you selected either the **This Object and Child Objects Only** or **This Object and All Child Objects** option, select **Next** to define the object classes to be audited.

Use one of the following methods to move an object class to the Audited Object Class list (right-hand pane):

- Select one or more object classes in the UnAudited Object Class list and then click **Add**.
- Select one or more object classes in the UnAudited Object Class list and 'drag and drop' the selected object classes into the Audited Object Class list.

- Double-click an object class in the UnAudited Object Class list.

You must select at least one object class for auditing.

NOTE: If you have selected multiple objects on the first page of the wizard, the object classes selected on this second page will apply to all of these objects.

6 After selecting the Active Directory objects (and object classes) to audit, click **Finish** to save your selection, close the wizard and return to the Active Directory Auditing page.

To modify an object in the auditing list:

1 On the Active Directory Auditing page, select the object to modify, and click **Edit**.

This opens the Active Directory Auditing wizard, where you can select a different Active Directory object or object classes for auditing.

2 Click **Finish** to save your selection, close the wizard and return to the Active Directory Auditing page.

To disable the auditing of an object in the auditing list:

Disabling a template allows you to temporarily disable the auditing of a directory object without having to remove it from the Active Directory auditing list.

1 On the Active Directory Auditing page, place your cursor in the **Status** cell for the required object, click the arrow control, and select **Disabled**.

The entry in the **Status** column for the object will change to 'Disabled'.

2 To re-enable the auditing of an object, use the **Enable** option in either the **Status** cell.

To delete an object from the auditing list:

1 On the Active Directory Auditing page, select the required object and click **Delete**.

2 Click **Yes** to confirm the deletion.

To delete an object class from the auditing list:

1 On the Active Directory Auditing page, select the required object class and click **Delete | Delete Object Class.**

2 Click **Yes** to confirm the deletion.

NOTE: You cannot delete the last object class in an object entry in the auditing list. In order to delete this last object class, you must delete the entire object from the auditing list.

Active Directory Auditing wizard

The Active Directory Auditing wizard opens when you select **Add** or **Add | Select Multiple Objects** on the Active Directory auditing page. This wizard steps you through the process of defining the custom Active Directory objects to audit.

The following table provides a description of the available fields and controls:

Table 2. Active Directory Auditing wizard

Create or modify Active Directory Auditing page: On the first page of the wizard, select the Active Directory object to audit.	
Scope	Select the appropriate option to specify the scope of coverage (**Enterprise** is selected by default): **Enterprise** - to audit the entire enterprise **This Object** - to audit an individual object **This Object and Child Objects Only** - to audit an object and its direct child objects **This Object and All Child Objects** - to audit an object and all of its subordinate objects (all levels) When an option other than **Enterprise** is selected, the Browse and Search pages allow you to locate and select the Active Directory objects to audit.
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the Active Directory objects to audit. 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. If you used the **Add | Select Multiple Objects** option, once you have selected an object, click **Add** to add it to the list.
Search page	Use the controls at the top of the Search page to locate an Active Directory object. If you used the **Add | Select Multiple Object** option, once you have selected an account, click **Add** to add it to the list.
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 in the online help or Quest Change Auditor User Guide.	
Select Object Classes Page: From here you can select at least one object class for auditing. **NOTE:** This page is only displayed if the **This Object and Child Objects Only** or **This Object and All Child Objects** scope option is selected on the first page of the wizard.	
UnAudited Object Class list	The list box located in the left displays the object classes that are currently not being selected to audit by this template.
Audited Object Class list	The list box located in the right contains the object classes that are currently selected for auditing.

Table 2. Active Directory Auditing wizard

Add	Select one or more object classes from the UnAudited Object Class list and click **Add** to select them for auditing. The selected object classes will be moved to the Audited Object Class list. **NOTE:** You can also double-click an object class to move it into the Audited Object Class list or 'drag and drop' it into the Audited Object Class list.
Remove	Select one or more object classes from the Audited Object Class list and click **Remove** to remove them from auditing. The selected object classes will then be moved back to the UnAudited Object Class list. **NOTE:** You can also double-click an object class to move it back into the UnAudited Object Class list or 'drag and drop' it into the UnAudited Object Class list.

Active Directory event logging

In addition to real-time event auditing, you can enable event logging to capture Active Directory events locally in a Windows event log. This event log can then be collected using InTrust® to satisfy long-term storage requirements.

For Active Directory events, event logging is disabled by default. When enabled, all Active Directory activity is sent to the InTrust for AD event log. See the Quest Change Auditor for Active Directory Event Reference Guide for a list of the events that can be sent to this event log.

To enable Active Directory event logging:

1. Open the Administration Tasks tab.
2. Click **Configuration**.
3. Select **Agent** in the Configuration task list to display the Agent Configuration page.
4. Click **Event Logging**.
5. On the Event Logging dialog, select **Active Directory**.
6. Click **OK** to save your selection and close the dialog.

4

Custom Active Directory Attribute Auditing

Introduction

Using custom attribute auditing, you can specify individual schema attributes to audit and assign a severity to the audited attributes. A new event will be added for each attribute selected for auditing. Once set, these events are identified with “Custom” in the facility name.

NOTE: Starting with Change Auditor 5.6, the attributes that can be set using the User Properties dialog in Active Directory Users and Computers (ADUC) are audited by default. If you have added custom attribute auditing for any of these attributes, you will receive two events when changes to these user attributes are made:

- A Custom User Monitoring event for the built-in user attribute event.
- A Custom AD Object Monitoring event for the custom attribute event (user attribute specified on Active Directory Attribute Auditing page).

To eliminate duplicate events, you can remove the user attribute from the Active Directory Attribute Auditing page which will prevent the custom attribute event from being generated.

NOTE: Change Auditor does not audit ‘constructed’ attributes, which are built from other normal attributes. To audit the changes made to these attributes, you need to audit the normal attributes associated with a constructed attribute.

NOTE: To use custom attribute auditing, you must be logged in to Change Auditor with an account with Enterprise Admin privileges.

Active Directory Attribute Auditing page

The Active Directory Attribute auditing page displays when you select **Active Directory | Attributes** from the Auditing task list in the navigation pane of the Administration Tasks page. From here you can specify individual schema attributes to audit and assign the severity.

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, see the Quest Change Auditor User Guide for information on how to gain access.

This page consists of the following information/controls:

Attributes list

The list box located across the top of this page lists the object classes that can be selected to define attribute auditing. It contains the object classes selected on the Attributes Auditing page.

In addition to the name of the object class, the assigned severity and number of custom attributes selected for auditing within each object class are also displayed.

NOTE: The default set of attributes (added, moved, removed and renamed) are always being audited, but they are not included in the Monitored Attributes count on this page. This count only includes the custom attributes selected for auditing.

Selecting an entry in this list, will populate the list boxes across the bottom of the dialog with the applicable attributes.

Unmonitored Attribute list

The list box located in the lower left-hand pane of this page displays the attributes that are currently NOT being audited by Change Auditor for the schema class selected in the Attributes list.

Monitored Attribute list

The list box located in the lower right-hand pane contains the attributes that are currently selected for auditing by Change Auditor for the schema class selected in the Attributes list.

In addition to the attribute, the assigned severity is also displayed. To change the severity level assigned to an attribute, place your cursor in the **Severity** cell and use the drop-down arrow to select the severity you want to assign to the selected attribute.

Add

Select one or more attributes from the Unmonitored Attribute list and click **Add** to select them for auditing. The selected attributes are moved to the Monitored Attribute list box.

NOTE: You can also double-click an attribute to select it for auditing or ‘drag and drop’ it into the Monitored Attribute list.

Remove

Select one or more attributes from the Monitored Attribute list and click **Remove** to remove them from auditing. The selected attributes are moved back to the Unmonitored Attribute list box.

NOTE: You can also double-click an attribute to remove it from auditing or ‘drag and drop’ it back into the Unmonitored Attribute list.

Custom Active Directory attribute auditing

To define custom attribute auditing:

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **Attributes** under Active Directory in the Auditing task list.
4. Select an object class from the list located across the top of this page. (This list box contains the default object classes and the object classes selected on the Active Directory Auditing page.)

   Selecting an entry in this list will populate the lists across the bottom of the dialog with the applicable attributes.

   If your current installation includes a foreign forest, the Select Foreign Forest dialog opens where you can select the required forest.
5. In the Unmonitored Attribute list, located in the lower left pane of this page, select one or more attributes and click **Add** to select them for auditing.

   You can also double-click an attribute to select it for auditing or ‘drag and drop’ it into the Monitored Attribute list.
6. To change the severity level assigned to an attribute, in the right-hand list box, place your cursor in the **Severity** cell and use the drop-down arrow to select the severity you want to assign to the selected attribute.
7. To remove an attribute from auditing, select the attribute from the right-pane and click **Remove**. This moves the selected attribute back into the Unmonitored Attribute list.

   You can also double-click an attribute to remove it from auditing or ‘drag and drop’ it back into the Unmonitored Attribute list.
8. Once you have selected at least one attribute for auditing, the associated Monitored Attributes column in the list box across the top of this page will display the number of attributes selected for auditing. This value will also be displayed in the **Monitor Attributes** column back on the Active Directory Auditing page.

5

Member of Group Auditing

Introduction

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

IMPORTANT: By default, Change Auditor monitors the user object class at the enterprise level. To limit the scope of users who will be audited, delete the user object class from the Active Directory Auditing page. Then use the Member of Group Auditing page to define the users to be audited.

The Group Membership Expansion pane on the Coordinator Configuration page (Administration Tasks tab) allows you to define and schedule the expansion of nested membership of the Active Directory groups defined on the Member of Group Auditing page. See the Quest Change Auditor User Guide for more information on defining group membership expansion behavior.

This section provides a description of the Member of Group Auditing page and explains how to add groups to the Member of Group Auditing list displayed on this page.

Member of Group Auditing page

The Member of Group Auditing page is displayed when you select **Member of Group** from the Auditing task list in the navigation pane of the Administration Tasks page. Member of Group auditing allows you to meet your auditing requirements by specifying the users to be audited based on their group membership.

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, refer to the Quest Change Auditor User Guide for more information on how to gain access.

This page list the groups whose users are to be audited based on their group membership. To add a group to this list, use the Add tool bar button. Once added, the following information is displayed:

Group

Displays the name of the group.

Display Name

If applicable, this column shows the display name assigned to the groups 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 groups 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 the Quest Change Auditor User Guide.

Member of Group auditing list

To add a group to the Member of Group Auditing list:

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **Active Directory** under the Auditing task list.

   Ensure that the user object class is removed from auditing and not listed on this page. If it is still listed, select it and click **Delete** to remove it.
4. Once the user object class has been removed, select **Member of Group** in the Auditing task list.
5. Click **Add** to open the Member of Group Auditing wizard to locate and select the groups whose users are to be audited.
6. If required, use the Forest drop-down to select the forest where the objects are located. Foreign agent forests may require foreing forest credentials which you can enter on the Credentials Required dialog.
7. Use the Browse and Search pages to locate and select a group and click **Add** to add them.

   Repeat this step to add additional groups.
8. Click **Select** to save your selections, close the wizard and return to the Member of Group auditing page, where your selections will now be listed.

   NOTE: When entering foreign forests credentials in the Credentials Required dialog, the "Save credential" will be forced to be enabled. This is due to the credentials being used for Group Membership Expansion of the foreign forest group. The credentials can be managed by clicking the Foreign Forest button on the Deployment tab.

To delete a group from the Member of Group Auditing list:

1. On the Member of Group auditing page, select the group to remove from auditing.
2. Click **Delete**.
3. Click **Yes** to confirm.

Member of Group Auditing wizard

The Member of Group Auditing wizard opens when you click **Add** on the Member of Group auditing page and allows you to locate and select Active Directory groups to audit. The following table provides a description of the available fields and controls.

Table 3. Member of Group Auditing wizard

Select Groups to Audit page: On this page select the groups to be audited.	
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the groups to audit. Once you have selected a group, click **Add** to move the group to the list at the bottom of the page.

Table 3. Member of Group Auditing wizard

Search page	Use the controls at the top of the Search page to search your environment to locate the groups to audit. Once you have selected a group, click **Add** to move the group to the list 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 in the online help or Change Auditor User Guide.

Selection list	The groups selected for auditing are displayed in the list box located across the bottom of this page. Use the buttons located above this list box as described below: • **Add** - Select a group in the Browse or Search page to add it to the selection list. • **Remove** - Select an entry in the selection list to remove it.

6

Active Directory Federation Services Auditing

Introduction

Change Auditor allows you to monitor sign-ins and configuration changes made through Active Directory Federation Services.

NOTE: A Change Auditor Logon Activity license is required to capture the sign-in events. A Change Auditor for Active Directory license is required to capture the configuration changes events.

To capture these events, you must:

- Create an Active Directory Federation Services template.
- Add this template to an agent configuration.
- Assign the agent configuration to agents.

This chapter includes a description of the Active Directory Federation Services auditing pages in the Administration Tasks tab, the procedure for creating and working with Active Directory Federation Services auditing templates.

Active Directory Federation Services Auditing page

The Active Directory Federation Services Auditing page is displayed when **Active Directory Federation Services** is selected from the Auditing task list in the navigation pane of the Administration Tasks page. From this page you can start the Active Directory Federation Services Auditing wizard to monitor sign-in activity and configuration changes. You can also edit existing templates, disable/enable templates and remove templates that are no longer being used.

The auditing page contains an expandable view of all the templates that have been previously defined. To add a new template to the list, use the **Add** tool bar button.

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, see the Change Auditor User Guide for more information about how to gain access.

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.

Sign-Ins

Displays whether the auditing of sign-in activity is enabled or disabled.

Configuration changes

Displays whether the auditing of configuration changes is enabled or disabled.

Active Directory Federation Services auditing templates

To create an auditing template:

1. Open the Administration Tasks page.
2. Click **Auditing**.
3. Select **Active Directory Federation Services** in the Auditing task list.
4. Click **Add** to open the Active Directory Federation Services Auditing wizard.
5. Enter a name for the auditing template.
6. Select the activity to audit. The options include sign-ins and configuration changes.
7. Click **Finish** or **Finish and Assign to Agent Configuration** to assign the template to an agent configuration.
8. On the Configuration Setup dialog, use one of the following methods to assign this template to an agent configuration:
   - Select the newly created 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 the newly created template.
- Select a configuration, then select the newly created template, right-click and select **Assign**.
- Select a configuration, then select the newly created template, click in the corresponding Assigned cell and click **Yes**.

9 If this configuration is not assigned to any agents, you will need to assign it to agents on each computer where Active Directory Federation Services is deployed.

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

1 On the Active Directory Federation Services Auditing page, select the required template and click **Edit**. This opens the Active Directory Federation Services Auditing wizard where you can modify the current settings.

2 Click **Finish** to save your changes and return to the Active Directory Federation Services Auditing page.

To disable and enable an auditing template:

Disabling a template temporarily stops auditing without having to remove the auditing template.

1 On the Active Directory Federation Services Auditing page, place your cursor in the Status cell for the auditing template to disable, click the arrow control, and select **Disabled**.

-OR-

Right-click the template to disable and select **Disable**.

The entry in the Status column for the template changes to 'Disabled'.

2 To enable the auditing template, select **Enable** in the Status cell.

To delete an auditing template:

1 On the Active Directory Federation Services Auditing page, select the required template and click **Delete | Delete Template**.

2 Click **Yes** to confirm.

Active Directory Federation Services Auditing Wizard

The Active Directory Federation Services Auditing wizard opens when you select **Add** on the Active Directory Federation Services Auditing auditing page. The following table provides a description of the available fields and controls:

Table 4. Active Directory Federation Services Auditing **wizard**

Select Active Directory Federation Services Auditing processes to audit: On the first page of the wizard, enter a name for the template.	
Template Name	Enter a descriptive name for the auditing template.
Activity	Select the activity to audit. You can choose to audit sign-ins and configuration changes.

7

ADAM (AD LDS) Auditing

Introduction

Change Auditor allows you to monitor Active Directory Application Mode (ADAM) and Active Directory Lightweight Directory Services (AD LDS) events. AD LDS provides directory services for directory-enabled applications without a risk compromising your Active Directory database.

NOTE: The File and Printer Sharing feature must be enabled under the Windows Firewall before you can set up ADAM auditing or protection.

NOTE: There are some special installation considerations for auditing ADAM (AD LDS) on workgroup servers. Refer to the Installing Change Auditor to Monitor ADAM (AD LDS) on Workgroup Servers appendix in the Change Auditor Installation Guide for more information.

To audit ADAM (AD LDS), you must first define the ADAM instances, the directory objects or containers, the object classes and optionally the individual attributes through the following pages on the Administration Tasks tab:

- Use the ADAM (AD LDS) Auditing page to create a list of ADAM instances, directory objects or containers, and object classes to monitor.
- Use the ADAM (AD LDS) Attribute Auditing page to select the individual schema attributes to monitor for the selected object classes.

This section provides a description of the ADAM (AD LDS) Auditing page and ADAM (AD LDS) Attribute Auditing page. It explains how to define custom ADAM (AD LDS) object and attribute auditing. For a description of the dialogs mentioned in this section, please refer to the online help.

ADAM (AD LDS) Auditing page

The ADAM (AD LDS) Auditing page contains a list of ADAM (AD LDS) instances and the associated object classes selected for auditing. This page displays when you select **ADAM (AD LDS)** from the Auditing task list in the navigation pane of the Administration Tasks tab.

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, refer to the Change Auditor User Guide for more information on how to gain access.

The ADAM (AD LDS) Auditing page contains an expandable view of the ADAM (AD LDS) instances selected for auditing. The view groups the information by agent, which can be expanded to view the object classes and monitored attributes. To add an instance to this list, click **Add**. Once added, the following information will be displayed:

Agents

Displays the name of the agent where the ADAM (AD LDS) instance resides. If there are many instances that have replicated partitions, the name of each agent hosting an instance will be displayed.

Object

Displays the distinguished name of the ADAM (AD LDS) instance.

Configuration Set ID

Displays the unique identifier of the configuration set shared between all ADAM (AD LDS) instances that are replicating their application partitions.

Status

Indicates whether the auditing for the ADAM instance is enabled or disabled.

Scope

Displays the scope of coverage:

- Enterprise
- Object
- One Level
- Subtree

Object Class

This field is used for filtering data.

If the view is not already expanded, click the expansion box to the left of the Instance Agent name to expand the view to display the following details:

Object Class

Displays the object class selected for auditing (such as container, user, and group).

Monitored Attributes

Displays the number of schema attributes selected for auditing by Change Auditor for each object class 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 the Quest Change Auditor User Guide.

NOTE: If credentials are needed in order to connect to the selected ADAM (AD LDS) instance, a credentials required dialog will be displayed prompting you to enter the appropriate credentials.

The page consists of the following information/controls:

Attributes list

The list box located across the top of this page lists the object classes that can be selected to define attribute auditing. More specifically, this list box contains the object classes selected on the ADAM (AD LDS) Auditing page.

In addition to the name of the object class, the following information is also displayed:

- the assigned severity
- number of custom attributes selected for auditing
- the names of the different schema classes available for auditing
- the name of the agent where the associated ADAM (AD LDS) instances resides. If there are many instances that have replicated partitions, the name of each agent hosting an instance will be displayed.
- Displays the unique identifier of the configuration set shared between all ADAM (AD LDS) instances that are replicating their application partitions.

Selecting an entry in this list, will populate the list boxes across the bottom of the dialog with the applicable attributes.

Unmonitored Attribute list

The list box located in the lower left-hand pane displays the attributes that are currently not being audited for the schema class selected in the Attributes list.

Monitored Attribute list

The list box located in the lower right-hand pane contains the attributes that are currently selected for auditing for the schema class selected in the Attributes list.

In addition to the attribute, the assigned severity is also displayed. To change the severity level assigned to an attribute, place your cursor in the **Severity** cell and use the drop-down arrow to select the severity you want to assign to the selected attribute.

Add

Select one or more attributes from the Unmonitored Attribute list and click **Add** to select them for auditing. The selected attributes will be moved to the Monitored Attribute list box.

NOTE: You can also double-click an attribute to select it for auditing or ‘drag and drop’ it into the Monitored Attribute list.

Remove

Select one or more attributes from the Monitored Attribute list and click **Remove** to remove them from auditing. The selected attribute will then be moved back to the Unmonitored Attribute list box.

NOTE: You can also double-click an attribute to remove it from auditing or ‘drag and drop’ it back into the Unmonitored Attribute list.

Enable ADAM (AD LDS) auditing

To enable ADAM (AD LDS) auditing:

1. Open the Administration Tasks page.
2. Click **Auditing**.
3. Select **ADAM (AD LDS)** in the Auditing task list.
4. Click **Add** to open the ADAM (AD LDS) Auditing wizard.
5. Select an ADAM (AD LDS) instance from the displayed list. This list includes the ADAM (AD LDS) instances found in your environment. Only instances running on computers with a Change Auditor agent installed display in this list.
6. On the second page of the wizard, use the Browse or Search pages to locate and select a directory object or container to audit.
7. On the Select Object Class page, use one of the following methods to move an object class from the UnAudited Object Class list to the Audited Object Class list:
   - Select one or more object classes in the UnAudited Object Class list and click **Add**.
   - Select one or more object classes in the UnAudited Object Class list and 'drag and drop' the selected object classes into the Audited Object Class list.
   - Double-click an object class in the UnAudited Object Class list.
8. After selecting one or more object classes, click **Finish** to save your selection and close the wizard.

   Change Auditor will then audit for events such as object created, deleted, moved, renamed and modified for the objects selected. However, to audit individual ADAM (AD LDS) attributes for these objects, you must specify the attributes to be audited using the ADAM (AD LDS) Attribute Auditing page.
9. On the Administration Tasks tab, select **ADAM (AD LDS) | Attributes** in the Auditing task list to open the ADAM (AD LDS) Attribute Auditing page.
10. Select an object class from the list box located across the top of this page. (This list contains the object classes selected on the ADAM (AD LDS) Auditing page.) Selecting an entry in this list will populate the list boxes across the bottom of the page with the applicable attributes.
11. In the Unmonitored Attribute list, located in the lower left-hand pane of this page, select one or more attributes and click **Add** to select them for auditing. The selected attributes will be moved to the Monitored Attribute list.

    You can also double-click an attribute to select it for auditing or 'drag and drop' it into the Monitored Attribute list.
12. To change the severity level assigned to an attribute, in the Monitored Attribute list, place your cursor in the **Severity** cell, click the arrow control and select the severity you want to assign to the selected attribute.
13. To remove an attribute from auditing, select the attribute in the Monitored Attribute list and click **Remove**. The selected attribute will then be moved back into the Unmonitored Attribute list.

    You can also double-click an attribute to remove it from auditing or 'drag and drop' it into the Unmonitored Attribute list.
14. Once you have selected at least one attribute for auditing, the associated Monitored Attribute column in the list box displays the number of attributes selected for auditing. This value will also be displayed in the Monitored Attribute column back on the ADAM (AD LDS) Auditing page.

ADAM (AD LDS) Auditing wizard

The ADAM (AD LDS) Auditing wizard opens when you click **Add** on the ADAM (AD LDS) Auditing page. This wizard steps you through the process of defining the ADAM (AD LDS) instance, directory objects or containers, and object classes to audit.

The following table provides a description of the available fields and controls:

Table 5. ADAM (AD LDS) Auditing wizard

Select an ADAM instance page: The first page of the wizard displays a list of available ADAM (AD LDS) instances found in your environment. This list only includes instances found on computers that are running a Change Auditor agent.	
ADAM (AD LDS) Instances	This list includes the following information about each ADAM (AD LDS) instance discovered in your environment: • **Agent** - displays the name of the agent where each of the ADAM (AD LDS) instances reside. • **Instance Name** - displays the name of the ADAM (AD LDS) instances displayed. • **Instance Port** - displays the port number assigned to each of the ADAM (AD LDS) instances displayed. From this list, select the ADAM (AD LDS) instance to be audited. **NOTE:** If you have multiple ADAM (AD LDS) instances with replicating application partitions, there is no need to configure an auditing template for each instance. Change Auditor will automatically send the auditing configuration to each machine that is hosting an instance. You must have an agent installed on each instance host.
Select directory object or container page: On this page select where to conduct the audit (such as enterprise or individual objects) and what to audit (such as directory object or container).	
Scope	Select the scope of coverage from the following options (**This Object and All Child Objects** is selected by default): • **Enterprise** - to audit the entire enterprise • **This Object** - to audit an individual object • **This Object and Child Objects Only** - to audit an object and its direct child objects • **This Object and All Child Objects** - to audit an object and all of its subordinate objects (all levels)
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the directory objects or containers to audit.
Search page	Use the controls at the top of the Search page to search your environment to locate the directory objects or containers to audit.
Options page	Use the Options page to modify the search options or ADAM instance to use to retrieve directory objects.
NOTE: For more information on using the Browse, Search or Options pages, refer to Directory Object Picker in the online help or the Quest Change Auditor User Guide.	
Select object class to audit page: On this page, select at least one object class to audit.	
UnAudited Object Class list	The list box on the left contains a list of all the unaudited object classes available for auditing. Select one or more unaudited object classes and click **Add** to move them to the Audited Object Class list box. At least one object class must be selected to continue.
Audited Object Class list	The list box to the right contains a list of all the object classes selected for auditing. Select one or more audited object classes and click **Remove** to remove them from auditing.

Table 5. ADAM (AD LDS) Auditing wizard

Add	Select one or more object classes from the UnAudited Object Class list to select them for auditing. **NOTE:** You can also double-click an object class to move it into the Audited Object Class list or 'drag and drop' it into the Audited Object Class list.
Remove	Select one or more object classes from the Audited Object Class list to remove them from auditing. The selected object classes will then be moved back to the UnAudited Object Class list. **NOTE:** You can also double-click an object class to move it back into the UnAudited Object Class list or 'drag and drop' it into the UnAudited Object Class list.

ADAM (AD LDS) event logging

In addition to real-time event auditing, you can enable event logging to capture ADAM (AD LDS) events locally in a Windows event log. This event log can then be collected using InTrust to satisfy long-term storage requirements.

For ADAM (AD LDS) events, event logging is disabled by default. When enabled, all ADAM activity is sent to the InTrust for ADAM event log. See the Change Auditor for Active Directory Event Reference Guide for a list of the events that can be sent to this event log.

To enable ADAM (AD LDS) event logging:

1. Open the Administration Tasks tab.
2. Click **Configuration**.
3. Select **Agent** in the Configuration task list to display the Agent Configuration page.
4. Click **Event Logging**.
5. On the Event Logging dialog, select **ADAM (AD LDS)**.
6. Click **OK** to save your selection and close the dialog.

8

Active Directory Database Auditing

Introduction

Change Auditor allows you to monitor the Active Directory database (NTDS.dit) file for possible unauthorized access attempts.

Extraction of this file could lead to parsing of usernames and passwords resulting in a security breach. The ability to audit changes to this file reduces the risk of the user account information from being accessed and tampered with by unwanted processes or users.

To capture Active Directory database events, you must:

- Create an Active Directory Database template.
- Add this template to an agent configuration.
- Assign the agent configuration to agents.

This chapter includes a description of the Active Directory Database auditing pages in the Administration Tasks tab, the procedure for creating and working with Active Directory Database auditing templates.

Active Directory Database Auditing page

The Active Directory Database Auditing page is displayed when **Active Directory Database** is selected from the Auditing task list in the navigation pane of the Administration Tasks page. From this page you can start the Active Directory Auditing wizard to monitor your Active Directory database for unauthorized access. You can also edit existing templates, disable/enable templates and remove templates that are no longer being used.

NOTE: By default, Change Auditor captures events regardless of the result of the operation mentioned in the event. However, you can specify which events to capture based on an event's result:

- All Results (default)
- Success Only
- Success and Failed Only
- Success and Protected Only

See the Change Auditor User Guide for more information about defining the events to be captured based on result.

The Active Directory Database Auditing page contains an expandable view of all the templates that have been previously defined. To add a new template to the list, use the **Add** tool bar button.

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, see the Change Auditor User Guide for more information about how to gain access.

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.

Exempt Process Filter

Displays a list of processes which bypass Active Directory database auditing.

Active Directory Database auditing templates

To create an auditing template:

1. Open the Administration Tasks page.
2. Click **Auditing**.
3. Select **Active Directory Database** in the Auditing task list.
4. Click **Add** to open the Active Directory Auditing wizard.
5. Enter a name for the Active Directory Database auditing template.
6. (Optional) Select the processes to exclude from auditing (for example, changes made by the processes specified on this page will be excluded from auditing).

7 Select one or more processes from the process list and click **Add** to move these processes to the exclusion list. By default, all processes (except lsass.exe) will be audited.

> **NOTE:** You can also view processes on a different server or enter a process not listed in the process list.

8 Click **Finish** or **Finish and Assign to Agent Configuration** to assign the template to an agent configuration.

9 On the Configuration Setup dialog, use one of the following methods to assign this template to an agent configuration:

- Select the newly created 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 the newly created template.
- Select a configuration, then select the newly created template, right-click and select **Assign**.
- Select a configuration, then select the newly created template, click in the corresponding Assigned cell and click **Yes**.

10 If this configuration is not assigned to any agents, you will need to assign it to agents installed on your Domain Controllers to apply the Active Directory database auditing.

> **NOTE:**
> - Agents should be installed on all Domain Controllers to ensure auditing has complete coverage.
> - The auditing should be applied on all Domain Controllers to ensure complete coverage.

- On the Agent Configuration page, select one or more agents from the agent list and click **Assign.**
- On the Agent Assignment dialog, select the configuration definition to be assigned to the selected agents and click **OK**.
- 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 Active Directory Database auditing template:

1 On the Active Directory Database Auditing page, select the required template and click **Edit**. This opens the Active Directory Database auditing wizard where you can modify the current settings.

2 Click **Finish** to save your changes and return to the Active Directory Database Auditing page.

To disable and enable an Active Directory Database auditing template:

Disabling a template temporarily stops auditing without having to remove the auditing template.

1 On the Active Directory Database auditing page, place your cursor in the Status cell for the auditing template to disable, click the arrow control, and select **Disabled**.

-OR-

Right-click the template to disable and select **Disable**.

The entry in the Status column for the template changes to 'Disabled'.

2 To enable the auditing template, select **Enable** in the Status cell.

To delete an Active Directory Database auditing template:

1 On the Active Directory Database Auditing page, select the required template and click **Delete | Delete Template**.

2 Click **Yes** to confirm.

Active Directory Database Auditing Wizard

The Active Directory Database Auditing wizard opens when you select **Add** on the Active Directory Database auditing page. This wizard steps you through the process of defining the Active Directory database processes to audit.
The following table provides a description of the available fields and controls:

Table 6. Active Directory Database Auditing wizard

Select Active Directory Database processes to audit: On the first page of the wizard, enter a name for the template and select the Active Directory database processes that are exempt from auditing.	
Template Name	Enter a descriptive name for the auditing template.
(Optional) Select processes exempt from auditing: Select the processes to exclude from auditing (for example, changes made by the processes specified on this page will be excluded from auditing).	
Add	Select one or more processes from the process list and click **Add** to move these processes to the exclusion list. By default, all processes (except lsass.exe) will be audited. You can also view processes on a different server or enter a process not listed in the process list.
Remove	The list box across the bottom of the page displays the objects that are exempt from auditing. Click **Remove** to remove a process from the exemption list.

9

Active Roles Integration

Active Roles uses a proxy account (service account) to connect and change Active Directory objects and group policies. Change Auditor for Active Directory can deploy to an Active Roles server which signals it to retrieve and send the name of the user that was logged in to the Active Roles console to Change Auditor for Active Directory. This additional information is then displayed in the Change Auditor for Active Directory client for events initiated using Active Roles.

NOTE: Change Auditor for Active Directory audits changes made through Active Roles workflow that are initiated by the Active Roles service account.

NOTE: As of Active Roles version 7.3.3, you can monitor a single server from multiple installations of Change Auditor. To ensure that the Active Roles server EventSource is created and registered in the Change Auditor database, you need to deploy the Active Roles integration script from each Change Auditor installation. See Deploying Change Auditor for Active Directory/Active Roles integration scripts.

This section covers the following topics for Active Roles integrations:

- Requirements
- Deploying Change Auditor for Active Directory/Active Roles integration scripts
- Client components added to Change Auditor for Active Directory
- Removing deployed Change Auditor for Active Directory/Active Roles integration scripts
- Troubleshooting Tips

Requirements

Refer to the Release Notes for the list of minimum system requirements.

Deploying Change Auditor for Active Directory/Active Roles integration scripts

For Active Roles to retrieve the name of the user that was logged in to the Active Roles console and forward this information to Change Auditor for Active Directory, you must first deploy the integration scripts to an Active Roles server.

NOTE: If the Active Roles scripting module has been deployed in a previous Change Auditor version, see the following knowledge base article which details the process to move to the updated version of these scripting modules that are available in Change Auditor 6.x and 7.x:

https://support.quest.com/change-auditor/kb?k=119136

NOTE: The Quest certificate used to sign the deployed scripts is added to the current user trusted publishers certificate stored on the Active Roles server.

To deploy Change Auditor for Active Directory/Active Roles integration scripts:

1. Open the Deployment page.
2. Select a server where Active Roles is installed.
3. Expand **Advanced Options** and select one of the following options:
   - **ActiveRoles Integration | Deploy Scripts Only**
   - **ActiveRoles Integration | Deploy Scripts and Excluded Account**
4. If you select the **Deploy Scripts Only** option, Change Auditor for Active Directory copies and runs the Active Roles integration PowerShell script on the Active Roles server which triggers Active Roles to retrieve the initiator information for all users and pass this information onto Change Auditor for Active Directory.
5. If you select the **Deploy Scripts and Excluded Accounts** option, the Select Active Directory Objects dialog is displayed. Use either the Browse or Search page to locate and select a user or computer to exclude. Change Auditor for Active Directory then deploys the integration script that signals Active Roles to retrieve the initiator information for all accounts except for those specified for exclusion.
6. Once successfully deployed, **Success** is displayed in the Deployment Results cell for the server.

   NOTE: If errors are encountered during the deployment process, corresponding error messages are displayed in the Deployment Results cell. Fix the errors reported and then redeploy the scripts.

Client components added to Change Auditor for Active Directory

After you have deployed the integration script, the initiator information retrieved from Active Roles can be viewed on the Search Results page in Change Auditor for Active Directory. Use the following to display additional information:

- A field on the Event Details pane that displays the additional information retrieved from Active Roles.
- A built-in report that retrieves all Active Directory changes, including changes initiated by Active Roles. Running this report also displays the **Initiator UserName** and **EventSource** columns in the search results.
- Columns on the Layout tab that allow you to add the event source and initiator information to other search definitions.
- Option on the Who tab that allows you to create a custom search to search for events initiated by a specific user, including events initiated by Active Roles.
- Email tags to include the additional information in alert email notifications.

Event Details pane

A Source field in the Event Details pane displays the name of the application from which the change event was generated (Change Auditor for Active Directory, Active Roles, or GPOADmin). For change events generated by Active Roles or GPOADmin, the name of the user account that initiated the change is displayed in parentheses.

NOTE: If the Source field displays ‘ActiveRoles’ (instead of ‘ActiveRoles Server’) you are not using the latest integration scripts. To take advantage of the additional events and initiator account information captured using the integration scripts, ensure that you are running Active Roles 6.9 (or higher) with Change Auditor for Active Directory 6.0 (or higher).

All Active Directory events including Active Roles/GPOADmin initiator built-in report

A built-in report is available which retrieves events for all Active Directory changes, including events initiated by Active Roles or GPOADmin. The search definition for this report also includes the initiator information (**Initiator UserName** and **EventSource** columns) in the search results.

To run the built-in Active Roles search:

1. Open the Searches page.
2. To display the available built-in searches, expand and select the **Shared | Built-in | All Events** folder.
3. Locate the **All Active Directory Events Including ActiveRoles/GPOAdmin Initiator** search and select the search definition and click **Run.**

   A new Search Results page is displayed populated with the audited events that met the search criteria, including the **Initiator UserName** and **EventSource** information.

Layout tab

The Change Auditor for Active Directory database includes columns to record Active Roles and GPOADmin information. The columns are not displayed by default on a Search Results page for most searches. However, using the Layout tab you can add the following information for all searches:

- **EventSource** — for all events, the name of the application from which the event was generated (Change Auditor for Active Directory, Active Roles, or GPOADmin).
- **Initiator Mail** — for all generated by Active Roles or GPOADmin, the email address of the user that initiated the change.
- **Initiator SID** — for events generated by Active Roles or GPOADmin, the SID of the user that initiated the change.
- **Initiator UserName** — for events generated by Active Roles or GPOADmin, the name of the user that initiated the change.

To add a column to the search results:

1. Open the Layout tab.
2. Locate the columns (**EventSource**, **Initiator Mail**, **Initiator SID**, or **Initiator UserName**) in the Unselected Columns table.
3. Select the columns to add and use the right arrow button to move them to the Selected Columns table.

   The column is added to the bottom of the list or beneath the highlighted column in the Selected Columns table.

   You can also ‘drag’ a column to the Selected Columns table.
4. The Selected Columns table also displays the order the columns are presented. To rearrange columns, use the up and down arrow buttons located to the right of the Selected Columns table.

   You can also ‘drag’ columns within this table to define the order.

Who tab

When using the Who tab to retrieve change events initiated by a specific user, changes initiated by Active Roles are not automatically included in the search. A check box is available on the Who tab which instructs Change Auditor for Active Directory to retrieve all change events initiated by the specified user, including those made through Active Roles and GPOADmin.

To include Active Roles initiated events:

1 Open the Searches page

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

3 Click **New** to enable the Search Properties tabs.

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

5 On the Select one or more Directory Objects dialog, use either the Browse or Search page to locate the user, computer, or group to include.

Once you have located the directory object, select it and click **Add** to add it to your selection list.

Repeat this step to include each additional directory object.

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

7 Back on the Who tab, select the **Include Event Source Initiator** check box.

NOTE: Including the event source initiator, may have a noticeable effect on the search performance, depending on the size of the database and the number of results returned in the search.

When this search runs, Change Auditor for Active Directory retrieves all events made by the specified user account, including events initiated by Active Roles.

In addition, when the **Include Event Source Initiator** option is selected the **Initiator UserName** column is added to the Search Results grid for this search. For events initiated by Active Roles, this column contains the user account that was logged in to the Active Roles console.

Email tags

Change Auditor for Active Directory/Active Roles integration email tags are available which can be added to the event details of alert email notifications. These new email tags are:

- %EVENTSOURCE% - indicates the application where the change event came from: Change Auditor for Active Directory, Active Roles, or GPOADmin.
- %INITIATORMAIL% - for events generated by Active Roles or GPOADmin, the email address of the user that initiated the event.
- %INITIATORSID% - for events generated by Active Roles or GPOADmin, the SID of the user that initiated the event.
- %INITIATORUSERNAME% - for events generated by Active Roles or GPOADmin, the name of the user that initiated the event.

See the Change Auditor User Guide for more information about how to configure and enable email notifications and customize email content.

Removing deployed Change Auditor for Active Directory/Active Roles integration scripts

You can use the Active Roles console to manually remove previously deployed integration scripts.

To remove integration scripts:

1 Open **Configuration | Policies | Administration**.

2 Right-click **Change Auditor Integration Policy**, select **Policy Scope**.

3 Remove **Active Directory** in the object list.

4 Delete **Change Auditor Integration Policy**.

5 Right-click **Change Auditor Integration Deprovision Policy**, select **Policy Scope**.

6 Remove **Active Directory** in the object list.

7 Delete **Change Auditor Integration Deprovision Policy**.

If you are using...	
Active Roles 6.9 Active Roles 7.0 Active Roles 7.1	• Navigate to **Configuration | Script Modules** and delete **Quest Change Auditor Integration Script.**

Troubleshooting Tips

Not receiving events from Active Roles

To diagnose problems with receiving events from Active Roles, check the 'Active Roles Admin Service' event log on the Active Roles server.

Initiator information missing in events

Some events do not provide the initiator account information. This could be caused by the following:

- Manually created objects

  Computer objects that are manually created do not capture the initiator account information of the user that initiated the change.

- Protected and unprotected objects

  If an object is protected and unprotected through the Active Roles console, the initiator account will be missing from Change Auditor for Active Directory.

  The Protect/Unprotect operation in Active Roles is not a direct Active Directory attribute operation. When you protect/unprotect an object, you actually add an Access Template link to the security descriptor in Active Directory. Because of this, the initiator account information is not captured for events related to protect/unprotect events.

- In some scenarios, the following events do not capture the initiator account information when made through the Active Roles console:
  - User password changed
  - User password changed by non-owner
  - User must change password at next logon option changed

10

Quest GPOADmin Integration

GPOADmin uses a proxy account (service account) to connect and change Active Directory objects and group policies. In past releases, Change Auditor for Active Directory only captured the service account name in the event details for changes initiated through GPOADmin. GPOADmin now integrates with Change Auditor for Active Directory and allows the name of the user who initiated the GPOADmin operation and comments to display in the Change Auditor for Active Directory client.

NOTE: GPOADmin only sends initiator and comment information to Change Auditor for Active Directory for the following operations:

- GPO deployment
- Working copy check-in
- Working copy check-out

This appendix covers the following topics for GPOADmin integrations:

Requirements

Refer to the Release Notes for the list of minimum system requirements.

GPOADmin and Change Auditor integration process

Some GPOADmin events recorded by Change Auditor have the initiator name in the event. The initiator is the name of the account logged in to the GPOADmin client performing actions in GPOADmin. However, the initiator name is not always populated due to how the GPO is processed in Active Directory.

The following is a high-level overview of typical Change Auditor events recorded when modifying a GPO using GPOADmin:

1. A user logged in to GPOADmin to modify a GPO setting.

   Change Auditor records the following events:

   An event for the creation of a new GPO (the working copy GPO). The “who” in the event shows the GPOADmin service account and the initiator and the name of the user who was logged in to GPOADmin.

   A rename event for the new GPO.

   A permission change for the new GPO, granting the user logged in to GPOADmin rights to the working copy GPO.

Modification events performed on the working copy GPO. The who of these events show the user logged in to GPOADmin and the initiator blank as the initiator and the who are the same.

2 Once the GPO is checked in, there are number of events recorded with the “who” being the GPOADmin service account and the initiator blank. This is because importing the settings from the working copy to the live copy is performed in Sysvol, outside of GPOADmin. It is the same processes that are performed if the GPO was edited in GPMC. GPOADmin has no knowledge of what is being performed with these Active Directory operations and cannot communicate to Change Auditor who the initiator is as they happened outside of all the GPOADmin processes.

3 Approval is requested in GPOADmin. The approver approves and deploys the GPO.

This generates Change Auditor events where the “who” is the GPOADmin service account and the initiator is the name of the approver.

Events where the initiator is the name of the approver and the action logged was that the version of the GPO attribute was changed, are the events that show when the GPO was deployed and who performed the deployment.

4 GPOADmin provides the initiator name to Change Auditor using Change Auditor APIs.

You will see a considerable amount Change Auditor GPO events generated when performing actions in GPOADmin. This is due to how GPOADmin processes GPOs and how they are deployed to the live environment.

NOTE: Enabling GPO protection in Change Auditor will prevent modifications to workflow disabled GPOs in GPOADmin.

Client components added to Change Auditor for Active Directory

You can view initiator information retrieved from GPOADmin on the Search Results page in the Change Auditor for Active Directory client. You can use the following to display this additional information:

- A field on the Event Details pane that displays the additional information retrieved from GPOADmin.
- A built-in report that retrieves all Active Directory changes, including those initiated by GPOADmin. Running this report also displays the **Initiator UserName** and **EventSource** columns in the search results.
- Columns on the Layout tab that allow you to add the event source and initiator information to other search definitions.
- Option on the Who tab that allows you to create a custom search to search for events initiated by a specific user, including those initiated by GPOADmin.
- Email tags to include the additional information in alert email notifications.

Event Details pane

A Source field is available in the Event Details pane that displays the name of the application from which the change event was generated (such as, Change Auditor for Active Directory, Active Roles, or GPOADmin). In addition, for change events generated by GPOADmin or Active Roles, the name of the user account that initiated the change is displayed in parenthesis.

All Active Directory events including Active Roles/GPOADmin initiator built-in report

A built-in report is available that retrieves events for all Active Directory changes, including those initiated by GPOADmin and Active Roles. The search definition for this report also includes the initiator information (**Initiator UserName** and **EventSource** columns) in the search results.

To execute the built-in GPOADmin search:

1. Open the Searches page.
2. Expand and select the **Shared | Built-in | All Events** folder to display the built-in searches available.
3. Locate the **All Active Directory Events Including ActiveRoles/GPOADmin Initiator** search and use one of the following methods to run the selected search:
   - Double-click a search definition
   - Right-click a search definition and select **Run**
   - Select the search definition and click **Run**

   A new Search Results page appears populated with the audited events that met the search criteria, including the **Initiator UserName** and **EventSource** information.

Layout tab

Columns are added to the database to record the information retrieved from GPOADmin or Active Roles. These columns are not displayed by default on a Search Results page for most searches. However, using the Layout tab you can add the following information to all searches:

- **EventSource** - for all events, the name of the application from which the event was generated (i.e., Change Auditor for Active Directory, Active Roles, or GPOADmin).
- **Initiator Mail** - for events generated by GPOADmin or Active Roles, the email address of the user that initiated the change.
- **Initiator SID** - for events generated by GPOADmin or Active Roles, the SID of the user that initiated the change.
- **Initiator UserName** - for events generated by GPOADmin or Active Roles, the name of the user that initiated the change.

To add new columns to the search results:

1. Open the Layout tab.
2. Locate the new columns (**EventSource**, **Initiator Mail**, **Initiator SID**, and/or **Initiator UserName**) in the Unselected Columns table.
3. Select the columns to add and use the right arrow button to move them to the Selected Columns table.

   The column will be added to the bottom of the list or beneath the highlighted column in the Selected Columns table.

   You can also drag a column to the Selected Columns table.
4. The Selected Columns table also displays the order the columns will be presented. To rearrange the columns, use the up and down arrow buttons located to the right of the Selected Columns table.

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

Who tab

When using the Who tab to retrieve change events initiated by a specific user, changes initiated by GPOADmin will not automatically be included in the search. A check is available in the Who tab which instructs Change Auditor for

Active Directory to retrieve all change events initiated by the specified user, including those made through GPOADmin.

To include GPOADmin initiated events:

1. Open the Searches page.
2. In the explorer view (left pane), expand and select the folder where you want to save your search (e.g., Shared or Private).
3. Click **New** to enable the Search Properties tabs.
4. On the Who tab, click **Add** to add an active user, computer or group to the 'who' list.
5. On the Select one or more Directory Objects dialog, use either the Browse or Search page to search your environment to locate the user, computer or group to be included.

   Once you have located the directory object to be included, select it and click **Add**.

   Repeat this step to include each additional directory object.
6. After selecting one or more directory objects, click **Select** to save your selection and close the dialog.
7. Back on the Who tab, select the **Include Event Source Initiator** check box.

   NOTE: Including the event source initiator, may have a noticeable effect on the search performance, depending on the size of the database and the number of results returned in the search.

   When this search is run, Change Auditor for Active Directory retrieves all events made by the specified user account, including those initiated by GPOADmin.

   In addition, when this check box is selected the **Initiator UserName** column is added to the Search Results grid for this search. For events initiated by GPOADmin, this column contains the user account that was logged into the GPOADmin console.

Email tags

The following email tags are available which can be added to the event details of alert email notifications:

- %EVENTSOURCE% - indicates the application where the change event came from: Change Auditor for Active Directory, Active Roles, or GPOADmin.
- %INITIATORMAIL% - for events generated by GPOADmin or Active Roles, the email address of the user that initiated the event.
- %INITIATORSID% - for events generated by GPOADmin or Active Roles, the SID of the user that initiated the event.
- %INITIATORUSERNAME% - for events generated by GPOADmin or Active Roles, the name of the user that initiated the event.

See the Change Auditor User Guide for more information on how to configure and enable email notifications and customize email content.

Troubleshooting tips

If GPO events initiated by GPOADmin do not appear in the Change Auditor for Active Directory client as expected, check the following:

- GPOADmin/Change Auditor for Active Directory integration is through the SDK. Once configured, Change Auditor for Active Directory agents receive the configured settings in the next configuration polling interval (default every 15 minutes). Before the configuration is received by a Change Auditor for Active Directory agent, GPOADmin initiator and comment information will not be available for GPO events.

To make sure Change Auditor for Active Directory has the latest GPOADmin configuration, manually refresh the agent configuration (**Refresh Configuration** on Agent Configuration Page on the Administration Tasks tab).

NOTE: This delay is only applicable when you first install GPOADmin/Change Auditor for Active Directory or when the service account in GPOADmin has changed.

- Verify that the GPO is not being protected by Change Auditor for Active Directory's Group Policy Object Protection feature. When configured, Change Auditor for Active Directory prevents all changes to GPOs, regardless of the tool that is used to make the change (including GPOADmin).
- GPOADmin only sends initiator and comment information to Change Auditor for Active Directory for GPO deployment, working copy check in, and working copy check out operations.
- It may be necessary to restart the GPOADmin service before correct initiator information can be retrieve by Change Auditor for Active Directory. Before restarting the GPOADmin service, check the Change Auditor for Active Directory coordinator's status to ensure that the coordinator has been initialized and is running.

11

Active Directory Protection

Introduction

Enabling Active Directory protection allows you to lock down critical objects and attributes to prevent accidental or unauthorized creations, modifications, or deletions. This allows you to protect the environment from harmful changes that could open security holes or cause resources to become unavailable. Once enabled, if an unauthorized user attempts to modify or delete a protected object, Change Auditor prevents the operation and captures an event.

Protection can be defined for any Active Directory, Group Policy, or ADAM (AD LDS) object that you consider critical such as Organizational Units, Group Policy Object, and service accounts.

This chapter provides a description of the Active Directory Object Protection, Group Policy Object Protection, and ADAM (ADLS) Object Protection features. Including a description of the protection pages on the Administration Tasks tab, the procedures for creating protection templates, and a description of the protection wizards used to define object protection.

NOTE: Protection Notes and Recommendations:

1. Reserve protection for locking only critical objects.
2. Do not protect regular user accounts as it could prevent users from actions such as changing their passwords.
3. Certain applications and services need to make harmless changes to the Configuration and Schema NCs through the LocalSystem account. Therefore, Quest recommends that you do not protect the following applications and services:
   - Active Directory Knowledge Consistency Checker (KCC)
   - Quest Directory Analyzer
   - Microsoft Operations Manager (MOM)
   - Microsoft Licensing Computer
   - Microsoft Message Queuing Service (MSMQ)
   - Terminal Services Licensing Computer
   - HP OpenView's Active Directory SPI
   - Microsoft Exchange

   If you protect a User object and prevent it from being deleted or modified, you are protecting all the user attributes and the forward links. You are not protecting any back linked attributes as back links are maintained by the system to ensure referential integrity only.

   If you modify the user's memberOf attribute and add the user to a group, although you get an error or warning message, the user gets added to any group that is not protected.

   To prevent anyone from being added to a Group, you would protect the Group object and prevent it from being modified. By locking the Group object, you are locking its member attribute. Hence its membership cannot be modified.
4. Before you can set up ADAM auditing or protection, you must enable the File and Printer Sharing feature under the Windows Firewall.
5. If you have Quest GPOADmin integrated with your Change Auditor deployment, the GPOADmin service account is exempt from protection.
6. A protected GPO can only be changed by override accounts that are excluded from protection.

Active Directory object protection

When configured, Change Auditor prevents changes from occurring to a protected object regardless of who attempts to change the object and the tool or method used. Attempts to change or delete a protected object fail and an event is generated. These 'failed' events are identified in the client by displaying 'Protected' in the **Result** column on the Search Results page and **Result** field in an event's detail pane.

NOTE: By default, Change Auditor captures events regardless of the result of the operation mentioned in the event. However, you can specify which events to capture based on an event's result:

- All Results (default)
- Success Only
- Success and Failed Only
- Success and Protected Only

See the Change Auditor User Guide for more information about defining the events to be captured based on result.

Active Directory protection page

This page displays when you select **Active Directory** from the Protection task list in the navigation pane of the Administration Tasks tab. From here, you can start the Active Directory Protection wizard to define critical Active Directory objects to protect from unauthorized modifications. You can also edit existing templates, disable and enable templates, and remove templates that are no longer being used.

The Active Directory protection page contains an expandable view of all previously defined Active Directory protection templates. To add new template, use the **Add** button.

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, see the Change Auditor User Guide for more information about how to gain access.

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/disable the template, place your cursor in this **Status** cell, click the arrow control and select the appropriate option from the drop-down menu.

Override Accounts

Indicates whether the override accounts listed are excluded from protection or included in protection. This setting corresponds to the option used at the top of the last page of the Active Directory Protection wizard:

- Excluded from Protection - indicates that you selected the **Allow** option to allow only the selected accounts to change the protected objects.
- Included in Protection - indicates that you selected the **Deny** option to allow all accounts to change the protected objects except for those selected.

Objects

This field is used for filtering data.

Override Account Filter

This field is used for filtering data.

Attributes

This field is used for filtering data.

NOTE: This field is only displayed when your Active Directory and Group Policy protection templates are stored in SQL, which is the default location for storing these templates.

Click the expansion box to the left of the template name to expand this view and display the following details for each template:

Object Canonical

Displays the canonical name of the object being protected.

Status

Indicates whether protection for the object is enabled or disabled.

Object Class

Displays the type of object being protected (for example, computer, group, user, and so on)

Operations

Displays the type of operations to be denied for the selected object:

- Create
- Delete
- Modify Attribute
- Move

Scope

Displays the scope of coverage for the protected object:

- This object only
- This object and child objects only
- This object and all child objects

Override Account

If applicable, this section of the grid displays the user and group accounts that are allowed (or not allowed) to change the protected objects.

NOTE: This field is not displayed when there are no override accounts specified in the Active Directory Protection wizard.

Attribute Protection

Displays the attribute setting specified in the wizard:

- Protect All
- Protect Only
- Protect Except

For **Protect Only** and **Protect Except**, click the expansion box to the left of the field to display the individual attributes included in the protection template.

Administration Account

If applicable, this section displays the user or group accounts that have been selected on the last page of the wizard to manage this protection template.

NOTE: This field is displayed only when there is at least one account specified on the last page of the protection wizard and your protection templates are being stored in SQL.

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 the Change Auditor User Guide.

Active Directory protection templates

The Active Directory protection templates are global settings and apply to all agents.

NOTE:

- If you are planning to use multiple Active Directory Protection templates, see the Change Auditor Technical Insight Guide for more information about how multiple protection templates are evaluated.
- Agents should be installed on all Domain Controllers to ensure that protection is fully covered. For example, if a user is restricted from making changes and accesses a Domain Controller that does not have an agent installed, they are allowed to make changes.
- To use protection templates, you must be logged in to Change Auditor with an account with Enterprise Admin privileges.
- You can also open the protection wizard from the event details pane. Simply open the Search Results tab, select an event, and click the Protect Object button.
- If Active Directory integrated DNS is deployed, you can access the ForestDNSZones or DomainDNSZones partitions by right-clicking on the top-level domain object in the directory object picker.

To create an Active Directory Protection template:

1. Open the Administration Tasks tab.
2. Click **Protection**.
3. Select **Active Directory** in the Protection task list.
4. Click **Add** to open the Active Directory Protection wizard to specify the Active Directory objects to protect.
5. Enter a name for the protection template.
6. Use the Browse or Search pages to locate and select the object to protect.

   NOTE: You can select a root domain object to prevent users from linking GPOs. However, if you do so, the gPLink attribute will be added by default and you will not be able to add other Active Directory objects or additional attributes to protect.

7. Click **Add** to add the object. Repeat this step as required to add more objects.

   You can 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.

If you have many objects to protect, you can create a .csv file containing the object and protection details, then import them into the template.

NOTE: CSV File Details

The file must follow this format:

<Canonical Name>, <Protection Scope>, <Protected Operation 1><Protected Operation 2>

<Protected Operation n>, <Foreign Agent Forest FQDN>

Valid protection scope values include:

- This object only
- This object and child objects only
- This object and all child objects

Valid protected operations include:

- Create
- Modify
- Delete
- Move

Foreign Agent Forest FQDN is not required for objects in the local forest of the coordinator. If left blank, the local forest is assumed.

The import supports the list separator defined for the locale of the operating system.

Example of CSV file entry for local forest object: Forest1.com/users/TestUser1, This object only, Create Delete Modify

Example of CSV file entry for foreign forest object: Forest2.com/users/TestUser2, This object only, Create Delete Modify, Forest2.com

After you have the file created, select **Import**, browse to the file, and click **Open**.

If any objects cannot be found, you can copy the results (ctrl+c) from the list into the clipboard so that you can use the information to locate any issues and make the necessary adjustments.

8 By default, the create, modify attributes, and delete operations are selected; however, you can change this by using the drop-down arrow in the **Operations** cell in the list box and selecting or clearing the different operations.

9 By default, the scope of coverage is for **This object only**; however, you can change this by using the drop-down arrow in the **Scope** cell in the list box and selecting one of the other two options:

- This object and child objects only
- This object and all child objects

10 By default, all attributes for the object will be protected. However, if you want to protect individual attributes instead, click **Next** and select one of the following options to activate the attributes list:

- Only Selected
- All EXCEPT Selected

From the attributes list box on the left, select the individual attributes to include in this protection template, click **Add**, and click **Next**.

If you have selected to protect the userAccountControl attribute, you can select to protect specific attribute flags on the (Optional) Select Attribute Flags to Protect of the wizard. By default, all flags are selected. Clear the **ALL** checkbox to select specific flags and click **Next**.

11 To specify users or groups that can change the protected object, click **Next**.

Use the Browse or Search pages to locate and select the user, group, or Managed Service Accounts to exclude from protection. Click **Add** to add the required accounts.

12 On the next page of the wizard, you can specify users or groups to manage this protection template.

NOTE: **Allow** is selected by default indicating that the selected users or groups can change the protected objects. However, you can select the **Deny** option and select individual users or groups that are not allowed to change the protected objects. When using the **Deny** option, you are allowing all users and groups to change the protected objects except for those selected on this page.

NOTE: This page only appears when your Active Directory and Group Policy protection templates are stored in SQL, which is the default location for storing these templates.

IMPORTANT: By default members of the Change Auditor Administrators group are authorized to access the Administration Tasks tab and perform administration tasks, including defining Active Directory and Group Policy protection; however, after you enter a user or group account on this page you are relinquishing your rights to modify the selected protection template to the users or groups specified on the last page of this protection wizard.

NOTE: If the users or groups specified are not members of the Change Auditor Administrators group, you must add them to the AD Protection Role for them to view the Administration Tasks tab to access Active Directory and Group Policy protection templates. For more information about adding members to the AD Protection role using the Application User Interface Authorization page (in the Configuration task list of the Administration Tasks tab), see the Change Auditor User Guide.

13 On the next page of the wizard, you can schedule when to enforce the protection. You can either select to always run the protection or run only during specific times. To enable the protection only during specific times, select **Protection is scheduled**, and define when it should be enabled (hour blocks on a weekly basis). The times selected are the local agent time where the template is applied.

NOTE: If you have denied specific users or groups the ability to change the protected objects and you have enabled a protection schedule, those users or groups are denied access only during this time. Anytime outside of when the schedule is set to enabled, these denied accounts can access the protected object.

When the schedule is disabled, all options are disabled with it, including any denied access to the specified users. The scheduling options override all other protection settings.

14 On the next page of the wizard, you can control when the protection is enabled based on the location. Location refers to the computer that is attempting to access the protected resource.

- **Protect access from all locations**: Protection is always enabled regardless of the location.
- **Protect access only from select locations**: Protection is only enabled for the specified locations.
- **Disable protection only for select locations**: Protection is disabled for the selected locations. Enabled everywhere else.
- **Protect access from all unknown locations**: All Active Directory requests from locations that cannot be determined by the Change Auditor agent will be protected.

NOTE: If you have denied specific users or groups access to protected objects, but you have specified locations that can access the protected object, the denied user or group will be able to access the protected objects from these locations.

The location options override all other protection settings.

15 Click **Finish** to save the protection template, close the wizard and return to the Active Directory Protection page.

To modify a protection template:

IMPORTANT: If the current user who is creating the protection template is not in the authorized accounts list, a warning message displays prompting the user to continue or stop with the creation of the protection template.

If you are in the authorized accounts list at template creation time, you may find yourself locked out later if someone else in the authorized accounts list decides to edit the template and remove you.

1. On the Active Directory Protection page, select the required template and click **Edit**.

   This opens the Active Directory Protection wizard where you can modify the current list of objects, and the attribute selection, the override accounts selected, and the administration accounts authorized to manage this protection template.

   NOTE: You can select a root domain object to prevent users from linking GPOs. However, if you do so, the gPLink attribute will be added by default and you will not be able to add other Active Directory objects or additional attributes to protect.

2. Click **Finish** to save your changes and return to the Active Directory Protection page.

To disable a protection template:

Disabling a template temporarily stops protection for the specified objects without having to remove the protection template.

1. On the Active Directory protection page, either:

   - Place your cursor in the **Status** cell for the protection template to disable, click the arrow control, and select **Disabled**
   - Right-click the template to disable and select **Disable**

   The entry in the **Status** column for the template changes to 'Disabled'.

2. To re-enable the protection template, select **Enable** in the **Status** cell.

To disable an object's protection within a protection template:

1. On the Active Directory Protection page, either:

   - Place your cursor in the **Status** cell for the required object, click the arrow control, and select **Disabled**.
   - Right-click the object and click **Disable.**

   The entry in the **Status** column for the object changes to 'Disabled'.

2. To re-enable an object's protection, select **Enable** in the **Status** cell.

NOTE: If you disable all the objects in a protection template, the template itself becomes disabled. Similarly, when you re-enable an object in the protection template, the template is automatically re-enabled.

To delete a protection template:

1. On the Active Directory Protection page, select the required template and click **Delete | Delete Template**.
2. Click **Yes** to confirm.

To delete an object from a protection template:

1. On the Active Directory Protection page, select the required object and click **Delete | Delete Object**.
2. Click **Yes** to confirm.

To delete an override account from a protection template:

NOTE: When you delete the last object in a protect template, the entire protection template is deleted.

1. On the Active Directory Protection page, select the required account and click **Delete | Delete Override Account**.
2. Click **Yes** to confirm.

To delete an administration account from a protection template:

1. On the Active Directory Protection page, select the required account and click **Delete | Delete Administration Account**.
2. Click **Yes** to confirm.

Active Directory Protection wizard

The Active Directory Protection wizard opens when you click **Add** or **Edit** on the Active Directory Protection page. Using this wizard you can define the Active Directory objects and attributes to protect from unauthorized modifications.

NOTE: You can also open the protection wizard from the event details pane. Simply open the Search Results tab, select an event, and click the Protect Object button.

NOTE: Agents should be installed on all Domain Controllers to ensure that protection is fully covered. For example, if a user is restricted from making changes and accesses a Domain Controller that does not have an agent installed, they are allowed to make changes.

The following table provides a description of the available fields and controls:

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 7. Active Directory Protection wizard

Select Active Directory objects to protect page: On the first page of the wizard, enter a name for the template and select the Active Directory objects to protect.

Table 7. Active Directory Protection wizard

Template Name	Enter a descriptive name for the protection template.
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the Active Directory objects to protect. 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. After you have selected an object, click **Add** to add it to the list. **NOTE:** If you have many objects that you want to protect, you can create a .csv file containing the object and protection details, then import them into the template. After you have the file created, select **Import**, browse to the file, and click **Open**. If any objects cannot be found, you can copy the results (ctrl+c) from the list into the clipboard so that you can use the information to locate any issues and make the necessary adjustments. **CSV File Details** The file must follow this format: <Canonical Name>, <Protection Scope>, <Protected Operation 1><Protected Operation 2> <Protected Operation n> Valid protection scope values include: • This object only • This object and child objects only • This object and all child objects Valid protected operations include: • Create • Modify • Delete • Move The import supports the list separator defined for the locale of the operating system.
Search page	Use the controls at the top of the Search page to search your environment to locate an Active Directory object to protect. After you have selected an object, click **Add** to add it to the list.
Options page	Use the Options page to modify the search options used to retrieve directory objects.
NOTE: For more information about using the Browse, Search or Options pages, see Directory Object Picker in the online help or Change Auditor User Guide.	
Object list **NOTE:** You can select a root domain object to prevent users from linking GPOs. However, if you do so, the gPLink attribute will be added by default and you will not be able to add other Active Directory objects or additional attributes to protect.	The list box across the bottom of the page displays the object(s) selected for protection. Use the buttons located above this list box to add and remove objects. • **Add** - Select an object in the Browse or Search page and add it to the Object list. • **Remove** - Select an entry in the Object list and remove it from the template.

Table 7. Active Directory Protection wizard

Operations	By default, the create, modify attributes and delete operations are selected. To change this use the drop-down arrow in the **Operations** cell and select/clear operations. • Create • Modify Attribute • Delete • Move
Scope	By default, the scope of coverage is set to **This object only**. To change this setting, use the drop-down menu in the **Scope** cell to select a different scope. • This object only • This object and child objects only • This object and all child objects For example, if you protect an OU and set an option with child objects, then all objects under the OU are also protected. If you protect a group, nested groups are not protected.
(Optional) Select Attributes to Protect page: By default all attributes for the selected objects are protected. However, you can protect individual attributes or to exclude individual attributes from protection.	
All Attributes	Select this option to protect all attributes for the selected object.
Only Selected	Select this option to protect individual attributes. Selecting this option will activate the list boxes on this page allowing you to select the individual attributes to be protected.
All EXCEPT Selected	Select this option to protect all attributes EXCEPT those selected. Selecting this option will activate the list boxes on this page allowing you to select the individual attributes that are not to be protected.
Attributes list	The list box to the left displays all the available attributes which may be selected for inclusion in the protection template. **NOTE:** This list box is not enabled when **All Attributes** is selected.
Add	Use the **Add** button to move the attributes selected in the Attributes list over to the Selected Attributes list.
Remove	Use the **Remove** button to move the attributes selected in the Selected Attributes list back over to the Attributes list.
Selected Attributes list	The list box to the right displays the attributes to be included in the protection template. **NOTE:** This list box is not enabled when the **All Attributes** option is selected.
(Optional) Select Attribute Flags to Protect page: If you have selected to protect the userAccountControl attribute, you can select to protect specific attribute flags on this page. By default, all flags are selected. Clear the **ALL** checkbox to select specific flags and click **Next**.	
Attributes Flags list	The list displays all the available attributes flags which may be selected for inclusion in the protection template. **NOTE:** This list box is not enabled when **ALL** is selected.
(Optional) Select Accounts Allowed (NOT Allowed) to Access Protected Objects page: By default all users and groups are prevented from changing the Active Directory objects selected for protection. However, you can specify users or groups that are allowed (not allowed) to change the protected objects. **NOTE:** Management actions performed by excluded accounts are audited but not prevented.	

Table 7. Active Directory Protection wizard

Allow	The **Allow** option is selected by default indicating that the users and groups selected on this page will be the only accounts allowed to change the protected objects. Use the Browse or Search page to select the user or group accounts.
Deny	Select the **Deny** option if you would like to allow all users and groups to change the protected objects EXCEPT for those selected on this page. Use the Browse or Search page to select the user or group accounts.
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the users or groups that are allowed (not allowed) to change the protected objects. After you have selected an account, click **Add** to add it to the list.
Search page	Use the controls at the top of the Search page to search your environment to locate the users or groups that are allowed (not allowed) to change the protected objects. After you have selected an account, click **Add** to add it to the list.
Options page	Use the Options page to modify the search options used to retrieve directory objects.
NOTE: For more information about using the Browse, Search or Options pages, see Directory Object Picker in the online help or Change Auditor User Guide.	
Override Accounts list	The list box across the bottom of the page displays the user and group accounts that are allowed (not allowed) to change the protected objects selected on the previous page of the wizard. Use the buttons located above this list box to add and remove accounts. • **Add — Select** an account in the Browse or Search page and add it to the Override Accounts list. • **Remove — Select** an account in the Override Accounts list and remove it.
(Optional) Schedule when protection is enabled	You can either select to always run the protection or run it only during specific times. To enable the protection only during specific times, select the Protection scheduled option, and define when it should be enabled (hour blocks on a weekly basis). The times selected are the local agent time where the template is applied. **NOTE:** If you have denied specific users or groups the ability to change the protected objects and you have enabled a protection schedule, those users or groups are denied access only during this time. Anytime outside of when the schedule is set to enabled, these denied accounts are able to access the protected object. When the schedule is disabled, all options are disabled with it, including any denied access to the specified users. The scheduling options override all other protection settings.

Table 7. Active Directory Protection wizard

(Optional) Enable or disable protection for specific location	Control when the protection is enabled based on the location. Location refers to the computer that is attempting to access the resource that is protected. Select from the following options: • Protect access from all locations: Protection is always enabled regardless of the location. • Protect access only from select locations: Protection is only enabled for the locations specified in the list box. • Allow access only from select locations: Protection is disabled for the select locations. Enabled everywhere else. **NOTE: Protect access from all unknown locations:** All requests from locations that cannot be determined by the Change Auditor agent will be protected. If you have denied specific users or groups access to protected objects, but you have specified locations that can access the protected object, the denied user or group will be able to access the protected objects from these locations. The location options override all other protection settings.
(Optional) Select Accounts Authorized to Manage This Protection Template page	
By default members of the Change Auditor Administrators group are authorized to access the Administration Tasks tab and perform administration tasks, including defining Active Directory and Group Policy protection; however, after you enter a user or group account here you are relinquishing your rights to modify the selected protection template to the users or groups specified on this page of the protection wizard. **NOTE:** This page only appears when your Active Directory and Group Policy protection templates are stored in SQL, which is the default location for storing these templates.	
Browse page	Displays the hierarchical view of the containers in your environment allowing you to locate and select the users or groups that will be authorized to manage this protection template. After you have selected an account, click **Add** to add it to the list.
Search page	Use the controls at the top of the Search page to search your environment to locate the users or groups that will be authorized to manage this protection template. After you have selected an account, click **Add** to add it to the list.
Options page	Use the Options page to modify the search options used to retrieve directory objects.
NOTE: For more information about using the Browse, Search or Options pages, see Directory Object Picker in the online help or Change Auditor User Guide.	
Administration Accounts list	The list box across the bottom of the page displays the user and group accounts authorized to manage this protection template. **NOTE:** By adding accounts to this list, you are relinquishing your rights to modify this protection template. Only those accounts specified on this page have access to modify this protection template. Use the buttons located above this list box to add and remove accounts. • **Add — Select** an account in the Browse or Search page and add it to the list. • **Remove — Select** an account in the Administration Accounts list and remove it.

Group Policy Object protection

You can prevent all changes to Group Policy Objects, regardless of the tool that is used to make the change. Protection includes both portions of the Group Policy data: the Group Policy Object (GPO) in Active Directory and the actual configuration data stored in the SYSVOL share on domain controllers.

IMPORTANT: A protected GPO can only be changed by override accounts that are excluded from protection.

NOTE: When an attempt is made to use the Windows Group Policy Editor to change a protected GPO, an access-denied error displays indicating that the change was not saved. However, when the error is dismissed the unsaved change will still be shown in the Editor as if it had been saved because the Group Policy Editor will not automatically refresh. To show the true (unchanged) state of the GPO, you must close and re-open the editor.

Group Policy protection page

The Group Policy protection page displays when you select **Group Policy** from the Protection task list in the navigation pane of the Administration Tasks tab. From here, you can start the Group Policy Protection wizard to define critical group policy objects to protect from unauthorized modifications. You can also edit existing templates, disable and enable templates, and remove templates that are no longer being used.

The Group Policy Protection page contains an expandable view of all previously defined Group Policy Protection

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, see the Change Auditor User Guide for more information about how to gain access.

templates. To add a Group Policy container to the protection list, use the **Add** button. Once added, the following information is provided for each template:

Template

Displays the name assigned to the template when it was created.

Objects

This cell is used for filtering data.

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.

Override Accounts

Indicates whether the override accounts listed are excluded from protection or included in protection. This setting corresponds to the option used at the top of the last page of the Group Policy Protection wizard:

- Excluded from Protection — indicates that you selected the **Allow** option to allow only the selected accounts to change the protected objects.
- Included in Protection - indicates that you selected the **Deny** option to allow all accounts to change the protected objects except for those selected.

Override Account Filter

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 for each template:

Policy Name

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 the Change Auditor User Guide.

Displays the name of the group policy being protected.

Group Policy Object

Displays the group policy object being protected.

Status

Indicates whether protection for the object is enabled or disabled.

Operations

Displays the type of operations to protect:

- Create
- Modify Attribute
- Delete
- Link

Override Account

If applicable, this section displays the user and group accounts that are allowed (or not allowed) to change the protected objects.

NOTE: This field is not displayed when there are no override accounts specified in the protection wizard.

Administration Account

If applicable, this section displays the user or group accounts that have been selected on the last page of the wizard to manage this protection template.

NOTE: This field is displayed only when there is at least one account specified on the last page of the protection wizard and your protection templates are being stored in SQL.

Group Policy protection templates

The Group Policy protection templates are global settings and apply to all agents.

NOTE: If you are planning to use multiple Group Policy Protection templates, see the Change Auditor Technical Insight Guide for more information about how multiple protection templates are evaluated.

NOTE: You can also open the protection wizard from the event details pane. Simply open the Search Results tab, select an event, and click the Protect Object button.

To create a Group Policy Protection template:

1. Open the Administration Tasks tab.
2. Click **Protection**.
3. Select **Group Policy** in the Protection task list.
4. Click **Add** to open the Group Policy Protection wizard and specify the GPOs to protect.
5. Enter a name for the template.

6 Use the Browse or Search pages to locate and select the group policy container to protect.

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.

Click **Add** to add the selected container to the list. Repeat this step to add additional group policy containers.

> **NOTE:** The Search page is initially displayed which contains **GroupPolicyContainer** in the Find field and an * wildcard character in the Name field. Click **Search** to locate the Group Policy containers in your environment.

7 By default, the create, modify attributes, and delete operations are selected; however, you can change this by using the drop-down arrow in the **Operations** cell in the list box and selecting or clearing the different operations.

When the **Link** operation is selected, the GPO is protected from any attempts to link to or unlink from any Active Directory container in the forest. If Enterprise protection is selected, all GPOs in the forest are protected from linking and unlinking attempts.

8 If required, enable the **Do not enforce protection for GPOADmin working copy group policies** option.

- When enabled, GPOADmin working copies selected for the protection template (or in the AD forest if Enterprise is selected), are ignored by the template.

> **NOTE:** Name-matching is used to identify GPOADmin temporary working copies based on a name prefix "[GPOADmin Working Copy] - ". The service account for the GPOADmin service should also be excluded from protection as an allowed account when the option to exclude GPOADmin working copies is selected.

9 If you have trusted administrators whose accounts must be permitted to change the protected group policy object, click **Next**.

Use the Browse or Search pages to locate and select the user or group accounts to exclude from this protection template.

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.

Use **Add** to add the accounts to the list at the bottom of the page.

> **NOTE:** The **Allow** option is selected by default indicating that the selected users or groups will be allowed to change the protected objects. However, you can select the **Deny** option at the top of this page and select individual users or groups that are NOT allowed to change the protected objects. When using the **Deny** option, you are allowing all users and groups to change the protected objects except for those selected on this page.

10 On the last page of the wizard, you can specify users or groups who are authorized to manage this protection template.

> **NOTE:** This page only appears when your Active Directory and Group Policy protection templates are stored in SQL, which is the default location for storing these templates.

> **IMPORTANT:** By default members of the ChangeAuditor Administrators group are authorized to access the Administration Tasks tab and perform administration tasks, including defining Active Directory and Group Policy protection; however, after you enter a user or group account on this page you are relinquishing your rights to modify the selected protection template to the users and groups specified on the last page of this protection wizard.

> **NOTE:** If the users and groups specified on this page are NOT members of the ChangeAuditor Administrators group, you need to add them to the AD Protection Role in order for them to view the Administration Tasks tab to access Active Directory and Group Policy protection templates. For more information about adding members to the AD Protection role using the Application User Interface Authorization page (in the Configuration task list of the Administration Tasks tab), see the Change Auditor User Guide.

11 Click **Finish** to save the template, close the wizard and return to the Group Policy Protection page.

IMPORTANT: If the current user who is creating the protection template is not in the authorized accounts list, a warning message is displayed prompting the user to continue or stop with the creation of the protection template. If you are in the authorized accounts list at template creation time, you may find yourself locked out later if someone else in the authorized accounts list decides to edit the template and remove you.

To modify a protection template:

1 On the Group Policy protection page, select the template to modify and click **Edit** to open the Group Policy Protection wizard where you can modify the current list of objects and the authorized accounts.

2 Click **Finish** to save your changes and return to the Group Policy protection page.

To disable a protection template:

Disabling a template allows you to temporarily stop protection for the specified objects without having to remove the protection template.

1 On the Group Policy protection page, place your cursor in the **Status** cell of the template and click the arrow control and select **Disabled**.

The entry in the **Status** column for the template changes to 'Disabled'.

2 To re-enable the protection template, use the **Enable** option in the **Status** cell.

To disable an object's protection within a protection template:

1 On the Group Policy Protection page, place your cursor in the **Status** cell for the object, click the arrow control, and select **Disabled**.

The entry in the **Status** column for the object changes to 'Disabled'.

2 To re-enable an object's protection, use the **Enable** option in the **Status** cell.

NOTE: If you disable all the objects in a protection template, the template itself becomes disabled. Similarly, when you re-enable an object in the protection template, the template will automatically be re-enabled.

To delete a protection template:

1 On the Group Policy Protection page, select the template and click **Delete | Delete Template**.

2 Click **Yes** to confirm.

To delete an object from a protection template:

1 On the Group Policy Protection page, select the object to delete and click **Delete | Delete Object**.

2 Click **Yes** to confirm.

To delete an override account from a protection template:

NOTE: When you delete the last object in a protect template, the entire protection template will be deleted.

1 On the Group Policy Protection page, select the account and click **Delete | Delete Override Account**.

2 Click **Yes** to confirm.

To delete an administration account from a protection template:

1 On the Group Policy Protection page, select the account and click **Delete | Delete Administration Account**.

2 Click **Yes** to confirm.

Group Policy Protection wizard

The Group Policy Protection wizard opens when you click **Add** or **Edit** on the Group Policy Protection page. From here, you can define the Group Policy Objects to protect from unauthorized modifications.

NOTE: You can also open the protection wizard from the event details pane. Simply open the Search Results tab, select an event, and click the Protect Object button.

The following table provides a description of the available fields and controls:

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 8. Group Policy Protection wizard

Create or modify a Group Policy Protection Template page: On the first page of the wizard, enter a name for the template and select the Group Policy objects to be protected.	
Template Name	Enter a descriptive name for the template.
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the group policy container to be protected. Once you have selected a container, click **Add** to add it to the list. 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.

Table 8. Group Policy Protection wizard

Search page	The Search page initially contains **GroupPolicyContainer** in the Find field and an * wildcard character in the Name field. Click **Search** to locate the Group Policy containers in your environment. You can use the controls at the top of the page to search your environment for a group policy container to protect. • In the **Find** field, either enter or use the drop-down menu to select the type of object to locate. You can enter multiple classes, separated by either a comma or semicolon. When you type in an entry, either click the **Enter** key or use **Search** to display the objects. • In the **Name** field, specify a search expression to use to locate a particular object. Usually, this field contains 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'. ▪ Enter a string preceded by the equal sign (=Admins) to return only exact matches. For example, entering '=Admin' returns only those objects containing the name 'Admin'. By default, ANR searches 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* returns objects that start with the letter 'n' ▪ *n returns objects that end in the letter 'n' ▪ *n* returns objects that contain the letter 'n' within their Display Name. Once you have selected a container, click **Add** to add it to the list at the bottom of the page.
Options page	Use this page to modify the search options used to retrieve directory objects.

NOTE: For more information about using the Browse, Search or Options pages, see Directory Object Picker in the online help or Change Auditor User Guide.

Table 8. Group Policy Protection wizard

Policy list	The list box across the bottom of the page displays the group policy containers selected for protection. Use the buttons located above this list box to add and remove containers. • **Add — Select** a container in the Browse or Search page to add it to the Policy list. • **Remove — Select** an entry in the Policy list to remove it from the template.
Operations	By default, the create, modify attributes, and delete operations are selected. To change this use the drop-down arrow in the **Operations** cell and select and clear operations. When the **Link** operation is selected, the GPO is protected from any attempts to link to or unlink from any Active Directory container in the forest. If Enterprise protection is selected, all GPOs in the forest are protected from linking and unlinking attempts.
Do not enforce protection for GPOADmin working copy group policies option	When enabled, GPOADmin working copies selected for the protection template (or in the AD forest if Enterprise is selected), are ignored by the template. Name-matching is used to identify GPOADmin temporary working copies based on a name prefix "[GPOADmin Working Copy] - ". The service account for the GPOADmin service should also be excluded from protection as an allowed account when the option to exclude GPOADmin working copies is selected.
(Optional) Select Accounts Allowed (Not Allowed) to Access Protected Objects page: By default all users and groups are prevented from changing the Group Policy containers selected for protection. However, you can use this page to specify individual users or groups that are allowed (not allowed) to change the protected objects. **NOTE:** Management actions performed by excluded accounts are audited but not prevented.	
Allow	**Allow** is selected by default indicating that the users and groups selected on this page will be the only accounts allowed to change the protected objects. Use the Browse or Search page to select the user or group accounts.
Deny	Select the **Deny** option if you want to allow all users and groups to change the protected objects except for those selected on this page. Use the Browse or Search page to select the user or group accounts.
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the users or groups that will be allowed (not allowed) to change the protected objects. 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. After you have selected an account, click **Add** to add it to the list.
Search page	Use the controls at the top of the Search page to search your environment to locate the users or groups that will be allowed (not allowed) to change the protected objects. After you have selected an account, click **Add** to add it to the list.
Options page	Use the Options page to modify the search options used to retrieve directory objects.
NOTE: For more information about using the Browse, Search or Options pages, see Directory Object Picker in the online help or *Change Auditor User Guide*.	
Override Accounts list	The list box across the bottom of the page displays the user and group accounts allowed (not allowed) to make changes to the protected objects selected on the previous page of the wizard. Use the buttons located above this list box to add and remove accounts. • **Add** - Select an account in the Browse or Search page to add it to the Override Accounts list. • **Remove** - Select an account in the Override Accounts list to remove it.

Table 8. Group Policy Protection wizard

(Optional) Select Accounts Authorized to Manage This Protection Template page: By default members of the ChangeAuditor Administrators group are authorized to access the Administration Tasks tab and perform administration tasks, including defining Active Directory and Group Policy protection; however, once you enter a user or group account on this page you will be relinquishing your rights to modify the selected protection template to the users/groups specified on this page of the protection wizard.

NOTE: This page only appears when your Active Directory and Group Policy protection templates are stored in SQL, which is the default location for storing these templates.

Browse page	Displays the hierarchical view of the containers in your environment allowing you to locate and select the users or groups that will be authorized to manage this protection template. Once you have selected an account, click **Add** to add it to the list.
Search page	Use the controls at the top of the Search page to search your environment to locate the users or groups that will be authorized to manage this protection template. Once you have selected an account, click **Add** to add it to the list.
Options page	Use the Options page to modify the search options used to retrieve directory objects.
NOTE: For more information about using the Browse, Search or Options pages, see Directory Object Picker in the online help or Change Auditor User Guide.	
Administration Accounts list	The list box across the bottom of the page displays the user and group accounts authorized to manage this protection template. **NOTE:** By adding accounts to this authorized accounts list, you are relinquishing your rights to modify this protection template. Only those accounts specified on this page will have access to modify this protection template. Use the buttons located above this list box to add and remove accounts. • **Add** - Select an account in the Browse or Search page and add it to the Administration Accounts list. • **Remove** - Select an account in the Administration Accounts list to remove it.

ADAM (AD LDS) object protection

When configured, you can prevent changes to objects in specified ADAM (AD LDS) instances.

ADAM (AD LDS) protection page

The ADAM (AD LDS) protection page displays when you select **ADAM (AD LDS)** from the Protection task list in the navigation pane of the Administration Tasks tab. From here, you can start the ADAM (AD LDS) Protection wizard to define critical objects to protect from unauthorized modifications. You can also edit existing templates, disable and enable templates, and remove templates that are not longer being used.

The ADAM (AD LDS) Protection page contains an expandable view of all previously defined ADAM (AD LDS)

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, see the Change Auditor User Guide for more information about how to gain access.

protection templates. To add new ADAM (AD LDS) protection template, use the **Add** 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/disable the template, place your cursor in this **Status** cell, click the arrow control and select the appropriate option from the drop-down menu.

Override Accounts

Indicates whether the override accounts listed are excluded from protection or included in protection. This setting corresponds to the option used at the top of the last page of the ADAM Protection wizard:

- Excluded from Protection - indicates you selected the **Allow** option to allow only the selected accounts to change the protected objects.
- Included in Protection - indicates you selected the **Deny** option to allow all accounts to change the protected objects except for those selected.

Objects

This field is used for filtering data.

Override Account Filter

This field is used for filtering data.

Attributes

This field is used for filtering data.

Click the expansion box to the left of the template to expand this view and display the following details for each template:

Object Canonical

Displays the canonical name of the object being protected.

Status

Indicates whether protection for the object is enabled or disabled.

Agents

Displays the name of the agent where the associated ADAM (AD LDS) instances reside. If there are many instances that have replicated partitions, the name of each agent hosting an instance is displayed.

Configuration Set ID

Displays the unique identifier of the configuration set shared between all ADAM (AD LDS) instances that are replicating their application partitions.

Object Class

Displays the type of object being protected (such as computer, group, or user).

Operations

Displays the type of operations to be denied for the selected object:

- Create
- Delete
- Modify Attribute
- Move

Scope

Displays the scope of coverage for the protected object:

- This object only
- This object and child objects only
- This object and all child objects

Attribute Protection

Displays the attribute setting specified in the wizard:

- Protect All
- Protect Only
- Protect Except

For **Protect Only** and **Protect Except**, click the expansion box to the left of the field to display the individual attributes included in the protection template.

Override Account

If applicable, this section displays the user and group accounts that are allowed (or not allowed) to change the protected objects.

NOTE: This field is not displayed when there are no override accounts specified in the protection wizard.

ADAM (AD LDS) protection templates

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 the Change Auditor User Guide.

The ADAM (AD LDS) protection templates defined are global settings and apply to all ADAM instances associated with a Change Auditor agent.

NOTE: If you are planning to use multiple ADAM (AD LDS) Protection templates, see the Change Auditor Technical Insight Guide for more information about how multiple protection templates are evaluated.

NOTE: You can also open the protection wizard from the event details pane. Simply open the Search Results tab, select an event, and click the Protect Object button.

To create an ADAM Protection template:

1. Open the Administration Tasks tab.
2. Click **Protection**.
3. Select **ADAM (AD LDS)** in the Protection task list to open the ADAM (AD LDS) protection page.
4. Click **Add** to open the ADAM (AD LDS) Protection wizard to specify the objects to protect.
5. On the first page of the wizard, select the ADAM (AD LDS) instance from which to choose protected objects. The list displays the ADAM (AD LDS) instances in your environment. It only shows instances running on computers with a Change Auditor agent installed.

   NOTE: If credentials are needed to connect to the selected ADAM (AD LDS) instance, a credentials required dialog is displayed prompting you to enter the appropriate credentials.

6. On the next page of the wizard, enter a name for the template.

   Use the Browse or Search pages to locate and select the object to protect. Click **Add** to add the selected object to the list. Repeat this step to add additional objects.

By default, the create, modify attributes, and delete operations are selected; however, you can change this by using the drop-down arrow in the **Denied Operations** cell in the list box and selecting or clearing the different operations.

By default, the scope of coverage is for **This object only**; however, you can change this by using the drop-down arrow in the Scope cell of the list box and selecting one of the other two options:

- This object and child objects only
- This object and all child objects

7 On the next page of the wizard, select the attributes to be protected. By default, all attributes for the object will be protected. However, if you want to protect individual attributes instead, select one of the following options to activate the attributes list:

- Only Selected
- All EXCEPT Selected

From the attributes list box on the left, select the individual attributes to be included in this protection template and click **Add** to move them to the Selected Attributes list.

8 If you want to specify individual users or groups that are to be allowed to make changes to the protected object, click **Next** to display the Select Accounts Allowed (Not Allowed) to Access Protected Objects page.

Use the Browse or Search pages to locate and select the user or group accounts to exclude from this protection template. Click **Add** to add the accounts.

9 Click **Finish** to save the protection template, close the wizard and return to the ADAM (AD LDS) Protection

> **NOTE:** The **Allow** option is selected by default indicating that the selected users or groups will be allowed to change the protected objects. However, you can select the **Deny** option at the top of this page and select individual users or groups that are NOT allowed to change the protected objects. When using the **Deny** option, you are allowing all users and groups to change the protected objects except for those selected on this page.

page.

To modify a protection template:

1 On the ADAM (AD LDS) protection page, select the template and click **Edit**.

The ADAM (AD LDS) Protection wizard opens where you can modify the current list of objects, and the attribute selection and the override accounts selected.

2 Click **Finish** to save your changes and return to the ADAM (AD LDS) protection page.

To disable a protection template:

Disabling a template allows you to temporarily stop protection for the specified objects without having to remove the protection template.

1 On the ADAM (AD LDS) protection page, place your cursor in the **Status** cell for the protection 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 protection template, use the **Enable** option in the **Status** cell.

To disable an object’s protection within a protection template:

1 On the ADAM (AD LDS) protection page, place your cursor in the **Status** cell for the object to be disabled, click the arrow control and select **Disabled**

The entry in the **Status** column for the object changes to ‘Disabled’.

2 To re-enable an object’s protection, use the **Enable** option in the **Status** cell.

> **NOTE:** If you disable all the objects in a protection template, the template itself will become disabled. Similarly, when you re-enable an object in the protection template, the template will automatically be re-enabled.

To delete a protection template:

1 On the ADAM (AD LDS) protection page, select the template and click **Delete | Delete Template**.

- Right-click the template and click **Delete.**

2 Click **Yes** to confirm.

To delete an object from a protection template:

1 On the ADAM (AD LDS) Protection page, select the object and click **Delete | Delete Object**.

ADAM Protection Wizard

NOTE: When you delete the last object in a protect template, the entire protection template will be deleted.

The ADAM (AD LDS) Protection wizard displays when you click **Add** or **Edit** on the ADAM (AD LDS) protection page. From the wizard, you can define the ADAM objects and attributes to protect from unauthorized modifications.

NOTE: You can also open the protection wizard from the event details pane. Simply open the Search Results tab, select an event, and click the Protect Object button.

The following table provides a description of the available fields and controls:

Table 9. ADAM (AD LDS) Protection wizard

Select ADAM (AD LDS) instance page: The first page of the wizard displays a list of ADAM (AD LDS) instances running a Change Auditor agent in your environment.	
ADAM (AD LDS) Instances	This list includes the following information about each ADAM (AD LDS) instance listed: • Agent - this column displays the name of the agent where each ADAM (AD LDS) instance resides. • Instance Name - this column displays the name of the ADAM (AD LDS) instances displayed. • Instance Port - this column displays the port number assigned to each of the ADAM (AD LDS) instances displayed. Select an instance from this list. When prompted, enter the user credentials to be used to access the selected instance. **NOTE:** If you have multiple ADAM (AD LDS) instances with replicating application partitions, there is no need to configure a protection template for each instance. Change Auditor will automatically send the protection configuration to each machine that is hosting an instance. You must have an agent installed on each instance host.
Select ADAM (AD LDS) Objects to Protect page: On this page, enter a name for the template and select the objects to be protected.	
Template Name	Enter a descriptive name for the protection template.
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the Active Directory object(s) to be protected. After you have selected an object, click **Add** to add it to the list.
Search page	Use the controls at the top of the Search page to search your environment to locate an Active Directory object to be protected. After you have selected an object, click **Add** to add it to the list.
Options page	Use the Options page to modify the search options or ADAM instance used to retrieve directory objects.
NOTE: For more information about using the Browse, Search or Options pages, see Directory Object Picker in the online help or *Change Auditor User Guide.*	

Table 9. ADAM (AD LDS) Protection wizard

Object list	The list box across the bottom of the page displays the objects selected for protection. Use the buttons located above this list box to add and remove objects. • **Add** - Select an object in the Browse or Search page and add it to the Object list. • **Remove** - Select an entry in the Object list and remove it from the template.
Denied Operations	By default, the create, modify attributes and delete operations are selected. To change this setting, use the drop-down arrow in the **Denied Operations** cell and select or clear operations.
Scope	By default, the scope of coverage is set to **This object only**. To change this setting, use the drop-down menu in the **Scope** cell to select a different scope. • This object only • This object and child objects only • This object and all child objects **NOTE:** Child objects do not refer to nested groups when protecting a group object.
(Optional) Select Attributes to Protect page: By default all attributes for the selected objects will be protected. However, you can use this page to protect individual attributes or to exclude individual attributes from protection.	
All Attributes	This option is selected by default indicating that all attributes will be protected from unauthorized access.
Only Selected	Select this option to protect individual attributes. Selecting this option will activate the list boxes on this page allowing you to select the individual attributes to be protected.
All EXCEPT Selected	Select this option to protect all attributes EXCEPT those selected. Selecting this option will activate the list boxes on this page allowing you to select the individual attributes that are not to be protected.
Attributes list	The list box to the left displays all of the available attributes which may be selected for inclusion in the protection template. **NOTE:** This list box is not enabled when the **All Attributes** option is selected.
Add	Use to move the attributes selected in the Attributes list over to the Selected Attributes list.
Remove	Use to move the attributes selected in the Selected Attributes list back over to the Attributes list.
Selected Attributes list	The list box to the right displays the attributes to be included in the protection template. **NOTE:** This list box is not enabled when **All Attributes** are selected.
(Optional) Select Accounts Allowed (Not Allowed) to Access Protected Objects page By default all users and groups are prevented from changing the ADAM (AD LDS) objects selected for protection. However, you can specify individual users or groups that are allowed (not allowed) to change the protected objects. **NOTE:** Management actions performed by excluded accounts are audited but not prevented.	
Allow (Default)	Indicates that the users and groups selected on this page ate the only accounts allowed to change the protected objects. Use the Browse or Search page to select the user or group accounts.
Deny	Select this if you want to allow all users and groups to change the protected objects except for those selected on this page. Use the Browse or Search page to select the user or group accounts.
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the users or groups that will be allowed (not allowed) to change the protected objects. After you have selected an account, click **Add** to add it to the list.

Table 9. ADAM (AD LDS) Protection wizard

Search page	Use the controls at the top of the Search page to locate the users or groups that will be allowed (not allowed) to change the protected objects. After you have selected an account, click **Add** to add it to the list.
Options page	Use to modify the search options used to retrieve directory objects.
NOTE: For more information about using the Browse, Search or Options pages, see Directory Object Picker in the online help or *Change Auditor User Guide*.	
Override Accounts list	The list box across the bottom of the page displays the user and group account(s) that will be allowed (not allowed) to make changes to the protected objects selected on the previous page of the wizard. Use the buttons located above this list box to add and remove accounts. • **Add** - Select an account in the Browse or Search page to add it to the Override Accounts list. • **Remove** - Select an entry in the Override Accounts list to remove it.

Active Directory Database protection

When configured, Change Auditor prevents 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.

This section includes a description of the Active Directory Database protection pages in the Administration Tasks tab, the procedure for creating an Active Directory Database protection template and description of the protection wizard used to define Active Directory Database protection template.

Active Directory Database protection page

This page displays when you select **Active Directory Database** from the Protection task list in the navigation pane of the Administration Tasks tab. From here, you can start the Active Directory Database protection wizard to define your Active Directory Database protection template to protect your Active Directory database from unauthorized access. You can also edit existing templates, disable and enable templates, and remove templates that are no longer being used.

The Active Directory Database protection page contains an expandable view of all previously defined Active Directory Database protection templates. To add new template, use the **Add** button.

NOTE: Authorization to use the administration tasks on the Administrations Tasks tab is defined using the Application User Interface page under the Configuration task list. If you are denied access to the tasks on this page, see the Change Auditor User Guide for more information about how to gain access.

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.

Exempt Process Filter

Displays a list of processes which bypass Active Directory database protection.

Active Directory Database protection templates

To create an Active Directory Database protection template:

1. Open the **Administration Tasks** tab.
2. Click **Protection**.
3. Select **Active Directory Database** in the Protection task list.
4. Click **Add** to open the Active Directory Database Protection wizard.
5. Enter a name for the Active Directory database protection template.
6. (Optional) Select processes to exclude from protection (for example, changes made by the processes specified on this page will be excluded from protection).
7. Select one or more processes from the process list and click **Add** to move these processes to the exclusion list. By default, all processes (except lsass.exe) will be protected from accessing the Active Directory database.

   NOTE: You can also view processes on a different server or enter a process not listed in the process list.

8. Click **Finish** or **Finish and Assign to Agent Configuration** to assign the template to an Agent Configuration immediately.
9. On the Configuration Setup dialog, use one of the following methods to assign this template to an agent configuration:
   - Select the newly created 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 the newly created template.
   - Select a configuration, then select the newly created template, right-click and select **Assign**.
   - Select a configuration, then select the newly created template, click in the corresponding Assigned cell and click **Yes**.
10. If this configuration is not assigned to any agents, you will need to assign it to agents installed on your Domain Controllers to apply the Active Directory database protection.

    NOTE:
    - Agents should be installed on all Domain Controllers to ensure auditing has complete coverage.
    - The auditing should be applied on all Domain Controllers to ensure complete coverage.

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

    NOTE: Active Directory database protection templates will not record audit events when access to the Active Directory database file is protected unless an Active Directory database auditing template is also assigned to the Change Auditor agent. See Active Directory Database Auditing for additional information.

To modify an Active Directory Database protection template:

1. On the Active Directory Database Protection page, select the required template and click **Edit**. This opens the Active Directory Database Protection wizard where you can modify the current settings.
2. Click **Finish** to save your changes and return to the Active Directory Database Protection page.

To disable an Active Directory Database protection template:

Disabling a template temporarily stops protection without having to remove the protection template.

1. On the Active Directory Database protection page, place your cursor in the Status cell for the auditing template to disable, click the arrow control, and select **Disabled**.

   -OR-

   Right-click the template to disable and select **Disable**.

   The entry in the Status column for the template changes to 'Disabled'.
2. To enable the protection template, select **Enable** in the Status cell.

To delete an Active Directory Database protection template:

1. On the Active Directory Database Protection page, select the required template and click **Delete | Delete Template**.
2. Click **Yes** to confirm.

Active Directory Database Protection wizard

The Active Directory Database Protection wizard opens when you click **Add** or **Edit** on the Active Directory Database Protection page. Using this wizard you can define the Active Directory Database processes to protect from unauthorized modifications.

NOTE: You can also open the protection wizard from the event details pane. Simply open the Search Results tab, select an event, and click the Protect Object button.

The following table provides a description of the available fields and controls:

Table 10. Active Directory Database Protection wizard

Select Active Directory Database processes to protect: On the first page of the wizard, enter a name for the template and select the Active Directory database processes that are exempt from protection.	
Template Name	Enter a descriptive name for the protection template.
(Optional) Select processes exempt from protection: Select processes to exclude from protection (for example, changes made by the processes specified on this page will be excluded from protection).	
Add	Select one or more processes from the process list and click **Add** to move these processes to the exclusion list. By default, all processes (except lsass.exe) will be audited. You can also view processes on a different server or enter a process not listed in the process list.
Remove	The list box across the bottom of the page displays the objects that are exempt from auditing. Click **Remove** to remove a process from the exemption list.

Setting extra security on protected objects

NOTE: The Security feature is only available if you have selected to save your Active Directory and Group Policy protection templates in Active Directory instead of SQL (using the Protection tab in the Coordinator Configuration tool). See the Change Auditor User Guide or online help for more information about the Coordinator Configuration tool.

By default, Change Auditor settings are accessible by all domain administrators. In some environments, there are many individuals assigned domain administrator privileges. You can use the Security feature to provide an extra layer of security for your protected objects. You can delegate the right to manage protected objects to trusted administrators, limiting the number of administrators that can change settings.

When you change the security settings on a protected object through the Active Directory Protection page (or Group Policy Protection page) in Change Auditor, you are not changing the permissions assigned to the object. You are changing the access rights on who can change the Change Auditor settings.

If you do not want to use the default global catalog to apply the ACLs to the protected object, click Connect To and enter the domain controller to use.

To set extra security on a protection template:

1. On the Active Directory Protection page (or Group Policy Protection page), right-click the protection template and click **Security**.

   The Access Control editor is displayed for the selected object.

2. Select the permissions then click **OK**.

   NOTE: Selecting access rights is similar to selecting access rights in Active Directory Users and Computers.

Each entry for the objects listed in the Protection template has it's individual security settings.

To set individual settings:

1. On the Active Directory Protection page (or Group Policy Protection page), click the **+** icon next to the protection template.
2. Right-click the entry in the template that want to set the security on and select **Security**.
3. Select the permissions and click **OK**.

   NOTE: Selecting access rights is similar to selecting access rights in Active Directory Users and Computers.

12

Event Details Pane

This section describes the Event Details pane for Active Directory and Group Policy events and the Restore Value feature that is available for some Active Directory events. It also describes the additional details added to this pane for Group Policy events.

Active Directory event details

The following table provides a description of the 'What' details that are provided on the Events Details pane for an Active Directory event.

Table 11. Event Details pane: Active Directory events

What field	Description
What	Provides a brief description of the change that occurred.
Subsystem	Displays 'Active Directory'.
Action	Displays the action that was taken against the Active Directory object, such as Add Attribute, Add Object, Delete Attribute, Delete Object, Modify Attribute, Move Object.
Facility	Displays the event class facility to which the event belongs.
Class	Displays the object class that was modified, such as group, user, computer, nTDSConnection, crossRefContainer.
Attr	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, such as Global (Security), Domain Local (Security).
Object	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	Indicates the port used for authentication.
From | To	Displays the old value that was assigned to the object and the new value that is now assigned. **NOTE:** The From | To information does not apply to permission and access control list (ACL) type changes and is replaced with the Changes table. This information is also not available for occurrence type events, such as when an object is created or deleted.
Changes	For permission type changes, the Changes table replaces the To | From information. This table provides details about the changes made, such as operation, type, account, permission, scope, and condition.

Restore Value feature

For simple Active Directory attribute changes (such as Add Attribute, Modify Attribute, Delete Attribute), the Event Details pane features an option to restore changed values. When applicable, **Restore Value** is displayed at the top

of the Event Details pane, allowing you to restore a changed value without needing to leave the client or use additional tools.

NOTE: The Restore Value feature honors the logged on user's domain rights. If the logged on user does not have sufficient rights to perform the restore, a dialog is displayed allowing the user to enter elevated credentials. If a user does not have sufficient privileges, Change Auditor displays a failure message noting either an access denial or a login failure.

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

To restore a changed value:

1. At the top of the Search Results page, select an event (such as Modify Attribute, Add Attribute, Delete Attribute) to display the related Event Details pane.
2. At the top of the Event Details pane, click **Restore Value**.
3. One of the following prompts is displayed:
   - If you do not have domain rights to access the selected server, the Credentials Required dialog is displayed allowing you to enter the credentials to be used to access the server.
   - A confirmation dialog is displayed explaining that you are about to restore the value of an attribute. Click **Yes** to perform the restore or **No** to cancel the restore operation.
   - A confirmation dialog is displayed explaining that the restore operation is not restoring the most recent value for an attribute. Click **Yes** to perform the restore or **No** to cancel the restore operation.
4. When a value is successfully restored, a success confirmation dialog is displayed and a Change Auditor event is generated reflecting the change that was made.
5. Events generated by a restore operation contain the 'Restored by Change Auditor' comment. To view a comment for an event, select the event in the grid at the top of the Search Results page and **Comments**.

Additional notes

The Restore Value feature cannot be used to restore deleted objects.

- If the affected object has been deleted from the server, a message is displayed stating that the server cannot process the restore request because the object no longer exists on the server.
- If the affected object has been marked for deletion but the change has not been fully replicated throughout the system, a similar message is displayed stating that the server is unable to process the request.

Group Policy event details

The following table provides a description of the ‘What’ details that are provided on the Events Details pane for a Group Policy event.

Table 12. Event Details pane: Group Policy events

What field	Description
What	Provides a brief description of the change that occurred.
Subsystem	Displays ‘Group Policy’.
Action	Displays the action that was taken against the Group Policy object or item, such as Add Attribute, Delete Attribute, Modify Attribute.
Facility	Displays the event class facility to which the event belongs: • Group Policy Item • Group Policy Object
Policy	Displays the name of the group policy that was modified.
Section	Displays what section of the group policy was modified.
Item	For events associated with Group Policy items, displays the group policy item that was modified.
From | To	Displays the old value that was assigned to the group policy object and the new value that is now assigned.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.