Quest

Quest® Change Auditor for Active Directory® Queries 7.6.3

User Guide

© 2026 Quest Software Inc.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

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

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

Change Auditor for Active Directory Queries User Guide
Updated - August 2026
Software Version - 7.6.3

Contents

Change Auditor for Active Directory Queries Overview 4
Introduction 4
Deployment requirements 4
Client components/features 5

Configure AD Query Auditing 7
Introduction 7
AD Query Auditing page 7
AD Query Auditing wizard 9
AD Query settings 10

Active Directory Query Searches/Reports 12
Introduction 12
Run AD Query reports 12
Create custom AD Query search 13

AD Query Event Details 16

About us 18
Our brand, our vision. Together. 18
Contacting Quest 18
Technical support resources 18

1

Change Auditor for Active Directory Queries Overview

- Introduction
- Deployment requirements
- Client components/features

Introduction

Many applications use Active Directory as an LDAP directory to provide user credentials, group membership information, and other application data. During a directory migration or restructuring project, such as a corporate acquisition, it is important to understand the ways that applications use the directory *before* migrating the directory structure, to avoid unnecessary application downtime. Obtaining this information from Windows audit logs is extremely difficult, as it requires setting SACLs and aggregating security audit logs from all domain controllers in the environment.

Change Auditor monitors directory access across all domain controllers in the environment and aggregates that information in a central database identifying LDAP-enabled applications and how they use Active Directory. The LDAP access data gathered by Change Auditor can then be used during Active Directory forest migration and restructuring projects.

NOTE: Active Directory query auditing is only available if you have licensed Change Auditor for Active Directory Queries. 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 Queries. 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.

Deployment requirements

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

Client components/features

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

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

Table 1. Change Auditor for Active Directory Queries client components/features

Client page	Feature
Administration Tasks tab	Agent Configuration page: • Configuration Setup Dialog - AD Query Events settings ▪ Discard query results less than *nn* records ▪ Discard queries taking less than *nn* milliseconds ▪ Discard duplicate queries occurring within *nn* minutes ▪ AD Query auditing enabled Audit Task list: • AD Query **NOTE:** See Configure AD Query Auditing for information on using these settings for Active Directory query auditing.
Event Details pane	What details: • Type • Scope • Results • SSL/TLS • Kerberos • Simple Bind • Port • Occurrences • Since • Elapsed • Filter • Attributes **NOTE:** See the AD Query Event Details appendix for a description of these fields.
Events	Facilities: • AD Query
Search Properties	What tab: • Subsystem | AD Query **NOTE:** See Active Directory Query Searches/Reports for information on using the What tab to create custom Active Directory query search queries.
Searches page	Built-in Reports: • All reports that include the event in the AD Query facility.

Table 1. Change Auditor for Active Directory Queries client components/features

Client page	Feature
Advanced tab/Search Results page	Columns: • LDAP Attributes • LDAP Elapsed • LDAP Filter • LDAP Occurrences • LDAP Results • LDAP Scope • LDAP Since • LDAP Type
Alert Body Configuration dialog - Event Details tab	Variables (email tags): • LDAP_ATTRIBUTES • LDAP_ELAPSED • LDAP_FILTER • LDAP_OCCURRENCES • LDAP_RESULTS • LDAP_SCOPE • LDAP_SINCE • LDAP_TYPE **NOTE:** See the *Change Auditor User Guide* for a description of these email tags and how to configure alert email notifications.

2

Configure AD Query Auditing

- Introduction
- AD Query Auditing page
- AD Query Auditing wizard
- AD Query settings

Introduction

Because the overhead of recording each Active Directory query read operation is likely to be high, you can optimize the process by summarizing similar operations from the same client, and only record the summary periodically. **Quest highly recommends that you perform the following steps to optimize the Active Directory query auditing/reporting process to reduce the number of events being generated**:

- Use the AD Query Auditing page to specify the containers to include and exclude from Active Directory query auditing.
- Use the AD Query settings to optimize the auditing process and define the interval to be used for recording Active Directory query operations.

This section provides instructions for specifying the containers to include and exclude from Active Directory query auditing, as well as a description of the AD Auditing page and AD Query Auditing wizard. It also explains the AD Query settings available on the Configuration Setup dialog which you can use to summarize Active Directory query activity and reduce the number of events generated. For a more detailed description of the dialogs mentioned in this chapter, refer to the online help.

AD Query Auditing page

The AD Query Auditing page displays when you select **AD Query** from the Auditing task list in the navigation pane of the Administration Tasks tab. From this page you can specify the Active Directory containers to include and exclude in Active Directory query auditing.

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:

- By default, all containers are included
- Due to the high volume of Active Directory queries performed against the Schema, RootDSE, and the Configurations containers, Quest recommends that you add these to the exclusion list.

Inclusion and exclusion rules

Only objects that are included (and not excluded) are monitored. For example:

- When an object is included and excluded at the same time, it will not be monitored.

- When an object is included and some of its child objects are excluded, only child objects that are not excluded will be monitored.
- When an object is excluded and some of its child objects are included, none of the child objects will be monitored.

AD Query Auditing page

The AD Query Auditing page contains an expandable view of Active Directory containers included and excluded from Active Directory query auditing.

Added containers display the following information:

Type

Displays the type of container.

Status

Indicates whether the container is temporarily included\excluded (enabled) or not included\excluded (disabled) from Active Directory query auditing.

Scope

Displays the scope of coverage:

- Object - excludes this object only
- Subtree - excludes this object and all child objects

Included Container

Displays the name of the container selected for inclusion.

Excluded Container

Displays the name of the container selected for exclusion.

To include a container to the AD Query audit list:

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **AD Query** (under the Forest heading in the Auditing task list) to open the AD Query Auditing page.
4. Click **Add** to open the AD Query Auditing wizard.
5. Select the scope:
   - **RootDSE** - select this to include the RootDSE object.
   - **This Object and All Child Objects** - select this to specify the containers to include. (Selecting a container will also include any child objects.)
6. If the **This Object and All Child Objects** option is selected, use the Browse and Search pages to locate and select a directory object. Click **Add** to add the selected directory object to the inclusion list.

   Repeat this step to add additional directory objects.
7. Click **Finish** to close the wizard and return to the AD Query Auditing page, where your selections will now be listed.

To exclude a container to the AD Query audit list:

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **AD Query** (under the Forest heading in the Auditing task list) to open the AD Query Auditing page.

4 Click **Add** to open the AD Query Auditing wizard.

5 Select the scope:

- **RootDSE** - select this option to exclude the RootDSE object. (Selecting this container will not exclude child objects.)
- **This Object and All Child Objects** - select this option to specify the containers to exclude. (Selecting a container will also exclude any child objects.)

6 If the **This Object and All Child Objects** option is selected, use the Browse and Search pages to locate and select a directory object. Click **Add** to add the selected directory object to the exclusion list.

Repeat this step to add additional directory objects.

7 Click **Finish** to close the wizard and return to the AD Query Auditing page, where your selections will now be listed.

To disable the inclusion or exclusion of a container:

The disable feature allows you to temporarily stop including or excluding an individual container from Active Directory query auditing without having to remove it from the AD Query Auditing list.

1 On the AD Query Auditing page, use one of the following methods to disable the exclusion of a container:

- Place your cursor in the **Status** cell for the container to be disabled, click the arrow control and select **Disabled**.
- Right-click the container to be disabled and select **Disable**.

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

2 To re-enable the exclusion or inclusion of the selected container, use the **Enable** option in either the **Status** cell or right-click menu.

To delete a container from the inclusion or exclusion list:

1 On the AD Query Auditing page, select the container to be deleted and click **Delete**.

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

AD Query Auditing wizard

The AD Query Auditing wizard is displayed when you click **Add** on the AD Query Auditing page. This wizard enables you to locate and select Active Directory containers to include and exclude from Active Directory query auditing.

Only objects that are included and not excluded are monitored. For example:

- When an object is included and excluded at the same time, it will not be monitored.
- When an object is included and some of its child objects are excluded, only child objects that are not excluded will be monitored.
- When an object is excluded and some of its child objects are included, none of the child objects will be monitored.

The following table provides a description of the fields and controls in the AD Query Auditing wizard.

Table 2. AD Query Auditing wizard

Add Objects to include from AD Queries page

Table 2. AD Query Auditing wizard

RootDSE	Select this option to include the RootDSE container.
This Object and All Child Objects	Select this option to specify the containers to include. When this option is selected, use the Browse and Search page to locate and select a container.
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the required containers. Once you have selected a container, click **Add** to move the entry to the list at the bottom of the page.
Search page	Use the controls at the top of the Search page to search your environment to locate the required containers. Once you have selected a container, click **Add** to move the entry 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.	
Included Containers List	The containers selected for inclusion for Active Directory query auditing are displayed in the list box located across the bottom of this page. Use the buttons located above this list box to add and remove containers. • **Add** - Select a container in the Browse or Search page and click **Add** to add it to the list. • **Remove** - Select an entry in the list and then click **Remove** to remove it.
Add Objects to exclude from AD Queries page	
RootDSE	Select this option to exclude the RootDSE container. **NOTE:** Selecting this option will NOT exclude any child objects.
This Object and All Child Objects	Select this option to specify the containers to exclude. When this option is selected, use the Browse and Search pages to locate and select a container.
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the containers to exclude from Active Directory query auditing. Once you have selected a container, click **Add** to move the entry to the list at the bottom of the page.
Search page	Use the controls at the top of the Search page to search your environment to locate the containers to exclude from Active Directory query auditing. Once you have selected a container, click **Add** to move the entry 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.	
Excluded Containers List	The containers selected for exclusion from Active Directory query auditing are displayed in the list box located across the bottom of this page. Use the buttons located above this list box to add and remove containers. • **Add** - Select a container in the Browse or Search page and click **Add** to add it to the list. • **Remove** - Select an entry in the list and then click e **Remove** to remove it.

AD Query settings

From the Agent Configuration page on the Administration Tasks tab you can define how to optimize the Active Directory query auditing process, summarizing similar operations from the same client.

Use the AD Query tab at the top of the Configuration Setup dialog to define the settings for summarizing similar operations from the same client and only record the summary in the Active Directory query event:

Discard query results less than *nn* records

This setting instructs Change Auditor to only generate an event if an Active Directory query returns more or equal to the number of results specified.

The default value is 0; therefore Change Auditor will generate an event even if the Active Directory query returns no results.

Discard queries taking less than *nn* milliseconds

This setting instructs Change Auditor to only generate an event if the Active Directory query takes longer than or equal to the specified number of milliseconds.

The default value is 20 milliseconds.

Discard duplicate queries occurring within *nn* minutes

This setting defines how long Active Directory query events are to be 'held' to determine if duplicates have occurred before they are forwarded to the Change Auditor client.

The default is 15 minutes meaning Change Auditor will gather Active Directory query events and hold them in a queue to determine if any duplicate queries have been generated during the specified interval. Change Auditor will then forward the AD Query event to the client specifying how many occurrences of that query were performed during the 15 minute interval.

AD Query auditing enabled

This check box is selected by default which enables AD Query auditing. Clearing this check box disables all AD Query auditing on the agents using the agent configuration selected in the left pane, which is often times desired for busy agents.

To set the AD Query settings:

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 **Configurations**.
5. On the Configuration Setup dialog, select an agent configuration from the left pane.
6. Open the AD Query tab and set the Active Directory query event settings as defined above.
7. Once you have set these settings, click **OK** to save your selections, close the dialog and return to the Agent Configuration page.
8. On the Agent Configuration page, select the agents assigned to the selected agent configuration and click **Refresh Configuration** to ensure the agent 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.

3

Active Directory Query Searches/Reports

- Introduction
- Run AD Query reports
- Create custom AD Query search

Introduction

You can search, report and alert on LDAP-enabled applications and how they use Active Directory. This section explains how to run the built-in AD Query reports and how to create a custom AD Query search using the What tab. For a description of the dialogs mentioned in this chapter refer to the online help.

Run AD Query reports

Running the **All AD Query Events** report will retrieve all the AD Query events captured for Active Directory® containers being audited.

To run the All AD Query Events report:

1. Launch the Change Auditor client and open the Searches tab.
2. In the explorer view (left pane), expand the **Shared | Built-in | All Events** folder.
3. Locate and double-click **All AD Query Events** in the right pane.
4. A new Search Results page appears displaying the AD Query events captured over the last seven days.

In addition to the **All AD Query Events** report, Change Auditor for Active Directory Queries ships with some additional Active Directory Query reports, which are located in the AD Query folder in the explorer view.

To run a more specific AD Query report:

1. Open the Searches tab.
2. In the explorer view, expand the **Shared | Built-in | AD Query** folder.
3. Locate and double-click one of the AD Query searches in the right-hand pane.
4. This will display a new Search Results page displaying the AD Query events that meet the search criteria defined in the selected search.

   NOTE: By default, the AD Query reports display additional LDAP details (such as, LDAP Occurrences, LDAP Results, etc.) in the Search Results page.

Create custom AD Query search

The following scenario explains how to use the What tab to create custom AD query searches.

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

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

To search Active Directory containers for AD queries:

1. Open the Searches page.
2. In the explorer view, 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**.
4. On the Info tab, enter a name and description for the search.
5. Open the What tab, expand **Add** and select **Subsystem | AD Query**. This opens the Add Active Directory Container dialog.
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 search all objects.
   - **This Object** - select to search the selected objects only.
   - **This Object and Child Objects Only** - select to search the selected object) and its direct child objects.
   - **This Object and All Child Objects** - select to search 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. When a scope other than **All Active Directory Objects** is selected, the directory object picker will be activated allowing you to select the objects to include in the search definition.

   Use the Browse or Search page to search your environment to locate and select the Active Directory containers to include.

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

   Use the Options page to view or modify the search options to be used to retrieve directory objects.
8. In addition, you can optionally enter one or more AD query parameters to be included in the search definition:
   - **Filter** - allows you to search for a filter string used in a query. This field uses the **Like** operator; therefore, you can enter a partial string of characters to have Change Auditor return any queries that use a filter string that contains the characters entered.

- **Attributes** - allows you to search for attributes that are being queried. This field uses the **Like** operator; therefore, you can enter a partial string of characters to have Change Auditor return any queries that query attributes that contain the characters entered.
- **Results >=** - allows you to search for queries that have returned a specific number of results. Enter (or use the arrow controls to specify) the number of results to be included in the search definition and Change Auditor will display the queries that have returned results equal to or greater than the number entered.
- **Elapsed (ms) >=** - allows you to search for queries that take a certain amount of time to complete. Enter (or use the arrow controls to specify) the number of milliseconds to be included in the search definition and Change Auditor will display the queries that took the specified number of milliseconds or longer to run.
- **Transports** - allows you to specify the type of transport protocols used to secure LDAP operation or LDAP queries. To include a specific transport, clear the **All Transports** check box.
  - **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.

  NOTE: For pre-5.5 LDAP Query events, this field is NULL in the database; therefore, 'All Transports' will be included regardless of this setting.

When you specify more than one AD query parameter, Change Auditor uses the 'OR' operator and will return AD Query events that meet any of the AD query parameters specified for the selected Active Directory container.

9 Once you have selected an Active Directory container (and any AD query parameters) to be included, click the **Add** button to add it to the Selection 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 Active Directory containers EXCEPT those listed in the 'what' list.

NOTE: Select the **Runtime Prompt** check box on this dialog to prompt for an Active Directory container every time the search is run.

10 Once you have selected the Active Directory container(s) to be included in the search, click the **OK** button 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**.

12 When this search is run, Change Auditor will search for AD Query events based on the search criteria specified on the What tab and display the results in a new search results page.

To search for an object that already has an audited AD Query event in the database:

1 Open the Searches page.

2 In the explorer view, 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 the **New** tool bar button at the top of the Searches page (or right-click a folder and select the **New | New Search** menu command).

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

5 Open the What tab, expand **Add with Events** and select **Subsystem | AD Query**.

6 On the Add Active Directory Container dialog, select an object from 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.

7 Click the **Add** button to add it to the selection list at the bottom of the page.

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

9 Once you have defined your search, 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 runs, Change Auditor searches for the AD Query events based on the search criteria specified on the What tab and display the results in a new search results page.

4

AD Query Event Details

This section provides a description of the ‘What’ details that are provided on the Events Details pane for an AD Query event.

Table 3. AD Query monitored event

Event	Description	Severity
AD Query Performed	Created when an AD query is performed on a container.	Low

Table 4. Event Details pane: AD Query events

What Fields	Description
What	Shows the container that was queried. For example, on LDAP bind operations, this displays the name (DN) being bound to; on LDAP search operations, this displays the baseObject of the search; and on LDAP compare operations, this displays the entry (DN) of the object being compared.
Subsystem	Displays ‘AD Query’
Action	Displays ‘Other’
Facility	Displays ‘AD Query’
Type	Displays the type of query: • LDAP • GC
Scope	Displays the scope of coverage: • This object only • This object and all children • Child objects only
Results	Displays the number of results returned as a result of the query.
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.
Occurrences	Displays the number of times the query occurred during the specified interval.
Since	Displays the date and time when the query was first initiated.
Elapsed	Displays how long the query took to run. Zero (0) indicates that it took less than a millisecond to complete.
Kerberos	Indicates whether the LDAP operation or AD query is 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.

Table 4. Event Details pane: AD Query events

What Fields	Description
Filter	Displays the filter string used in the query.
Attributes	Displays the attributes that were queried.

About us

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

Our brand, our vision. Together.

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

Contacting Quest

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

Technical support resources

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

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

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