Quest

Quest® Change Auditor for Defender® 7.1

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 Defender User Guide
Updated - December 2020
Software Version - 7.1

Contents

1

Change Auditor for Defender Overview

- Introduction
- Deployment requirements

Introduction

Defender enhances security by enabling two-factor authentication to network, web, and applications-based resources. It is designed to base all administration and identity management on an organization's existing investment in Active Directory and eliminate the costs and time involved in setting up and maintaining proprietary databases. In addition, Defender works with any OATH-compliant hardware token enabling organizations to select the most appropriate token for their users. By leveraging an organization's existing investment in Active Directory and supporting multiple token vendors, Defender enables organizations to increase security and achieve and sustain compliance in a cost-effective manner.

Specifically, Defender auditing:

- Captures critical changes to Defender's administration and usage to ensure it is always available. Detailed information is provided on who, what, when, and where change events. Original and current values for all changes are also provided.
- Alerts, audits, and reports on critical changes made by administrators in real time (including adding, deleting, or modifying user accounts, back-end configurations and security settings).
- Notifies organizations of changes to important items or patterns of changes.
- Reduces the risk of downtime and misconfiguration with reports that enable you to address system communication concerns.
- Enables continuous compliance and security auditing across your Microsoft enterprise.

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

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

NOTE: Defender auditing is only available if you have licensed Change Auditor for Active Directory. If you do not have a valid license you can use the features, however, associated events are not captured. To verify that it is licensed, right-click the coordinator icon in the system tray and select **Licensing.**

2

Getting Started

- Deployment requirements and notes
- Enable Defender auditing
- Make changes and run a report
- Troubleshooting

Deployment requirements and notes

Because Defender extends the Active Directory schema, once Defender auditing is enabled, agents installed on Domain Controllers detect any changes made to the Defender-specific attributes in Active Directory and generate events.

NOTE:

- Specific Defender templates or configuration is not required.
- After an agent upgrade from version 7.0.4 or earlier, you will need to update your configuration setup to enable Defender auditing where required.

Enable Defender auditing

Defender auditing is enabled and disabled on a configuration basis from through the configuration setup.

To enable Defender auditing:

1. Open the Administration Tasks tab and click **Configuration**.
2. Select **Agent** in the Configuration task list.
3. From the Agent Configuration page, click **Configurations** to see the available configuration definitions. From here you can edit a configuration to include Defender or create a new configuration.
4. Select the required agent configuration, select the **Defender** tab, and click the option to enabled auditing.

Make changes and run a report

1. To test that events are being captured, make some changes on a domain where Defender is deployed.

   For example:

   - Add a Defender security server to a domain
   - Change a Defender policy for a group or user
2. Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client** to review the events generated.
3. Open the Searches tab.
4. Expand the **Shared | Built-in | Defender** folder in the left pane.
5. Locate and double-click **All Defender events in the last 30 days** in the right pane.

   A new Search Results tab is added to the client displaying the events captured over the last seven days.
6. Select an event from the Search Results grid to display the event details for the selected event.

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

Troubleshooting

If you have enabled Defender auditing but you are not receiving any events, ensure that the required Domain Controllers have agents deployed to them. Defender events are recorded in the Active Directory subsystem.

3

Defender Searches/Reports

Defender built-in searches

You can run built-in searches to retrieve Defender activity captured by deployed agents enabling you to retrieve valuable information from a variety of perspectives.

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

To see a complete list of built-in reports, see the Change Auditor Built-in Reports Reference Guide.

This section provides procedures for running built-in Defender searches and provides a description of the details displayed on the Search Results page.

To run a built-in search:

1. Click on the **Searches** tab or select **View | Searches**.
2. Expand and select the appropriate folder in the explorer view (left pane) to display the list of search definitions stored in the selected folder. For example, selecting the **Shared | Built-in | Defender** will display all the built-in searches available for Defender.
3. In the right-hand pane, locate the search to be run 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**.
4. A new Search Results Page will be displayed populated with the audited events that met the search criteria defined in the selected search definition.

NOTE: To modify a built-in search, see the Change Auditor User Guide.

Search results

The Defender event information (including key information like who, what, when, where, why, and the event origin information) can be viewed on the Event Details pane in the client. The following table provides a description of the event details provided for Defender events.

Table 1. Event Details pane: Defender events

ChangeAuditor	Description
Severity	Displays “Low”, “Medium”, or “High” depending on the event.
Who	Specifies the name of the user who initiated the change.
When	Specifies the date and time when the change occurred.
Where	Displays the name of the workstation where the change occurred.
Source	Displays ‘Change Auditor’ which is the application from which the event was retrieved.
Origin	Displays the NetBIOS name and IP address of the workstation from which the event was generated.
What	Displays a description of the activity that occurred. **NOTE:** For lengthy descriptions, hover your cursor over the description field to view the entire event description.
Facility	Displays that it is Defender activity.

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.