



# Quest<sup>®</sup> Change Auditor for Defender<sup>®</sup> 6.9 **User Guide**



© 2017 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.  
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.

# Contents

<b>Change Auditor for Defender Overview</b> .....	<b>2</b>
<b>Getting Started</b> .....	<b>4</b>
<b>Defender Searches/Reports</b> .....	<b>6</b>
<b>About us</b> .....	<b>9</b>

---

# 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.

**i** | **NOTE:** Defender auditing is only available when you have Defender installed and the Change Auditor for Defender license applied. Contact your Sales Representative for more information about obtaining a license.

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 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 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.

---

# Getting Started

- [Deployment requirements and notes](#)
- [Make changes and run a report](#)
- [Troubleshooting](#)

# Deployment requirements and notes

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

**i** | **NOTE:** Specific Defender templates or configuration is not required.

## 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 or remove a Defender license
- Add a Defender security server to a domain
- Change a Defender policy for a group or user

- 2 Launch the Change Auditor client (**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.

**i** | **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 applied the Defender license 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.

---

# Defender Searches/Reports

- [Defender built-in searches](#)
- [Search results](#)



# 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.

**i** | **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'.

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

The following built-in searches retrieve Defender events from monitored Change Auditor agents:

- All Defender events in last 30 days
- Defender – Member added to access node in last 30 days
- Defender – Member removed from access node in last 30 days
- Defender access node added in last 30 days
- Defender access node removed in last 30 days
- Defender password events in last 30 days
- Defender policy added in last 30 days
- Defender policy change events in last 30 days
- Defender policy removed in last 30 days
- Defender RADIUS payload added in last 30 days
- Defender RADIUS payload change events in last 30 days
- Defender RADIUS payload removed in last 30 days
- Defender security server added in last 30 days
- Defender security server assigned to access node in last 30 days
- Defender security server removed in last 30 days
- Defender security server unassigned from access node in last 30 days
- Defender temporary response events in last 30 days
- Defender token added in last 30 days
- Defender token assigned in last 30 days
- Defender token PIN events in last 30 days
- Defender token removed in last 30 days
- Defender token unassigned in last 30 days

## **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.

**i** | **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**

<b>ChangeAuditor</b>	<b>Description</b>
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. <b>NOTE:</b> For lengthy descriptions, hover your cursor over the description field to view the entire event description.
Facility	Displays that it is Defender activity.

## We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

## Our brand, our vision. Together.

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

## Contacting Quest

For sales or other inquiries, visit [www.quest.com/contact](http://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.