

Quest® Change Auditor for Defender® 7.1
Event Reference Guide



© 2020 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 Software, 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

Introduction	4
Change Auditor for Defender Events	5
Defender	5
Built-in Reports	7
Defender built-in reports	7
About us	9
Our brand, our vision. Together.	9
Contacting Quest	9
Technical support resources	9

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 5.7 (or later) installed and Change Auditor for Active Directory licensed.

Because Defender extends the Active Directory schema, once Defender auditing is enabled, agents installed on Domain Controllers will detect any changes made to the Defender-specific attributes in Active Directory and generate events. No audit template is needed.

This document lists the events that can be captured by Change Auditor for Defender. Separate event reference guides are provided that list the core Change Auditor events (when any Change Auditor license is applied) and the events captured when the different auditing modules are licensed.

Change Auditor for Defender Events

This section lists the audited events captured by Change Auditor for Defender. They are listed in alphabetical order by facility.

- i** | **IMPORTANT:** When expecting large numbers of events, it may be necessary to increase the Max Events per Connection setting in the client (Agent Configuration on the Administration Tasks tab) to avoid an ever-increasing backlog of events waiting to be sent from the agent to the coordinator database.
- i** | **NOTE:** To view a complete list of all the Change Auditor for Defender events, open the Audit Events page on the Administration Tasks tab in the client. This page contains a list of all the events available for auditing by Change Auditor. It also displays the facility to which the event belongs, the severity assigned to each event, if the event is enabled or disabled, and the type of license that is required to capture each event.

Defender

Table 1. Defender events

Event	Description	Severity
Defender Access Node Added	Created when a new Defender access node is added in a domain.	Medium
Defender Access Node Removed	Created when a Defender access node is removed from a domain.	Medium
Defender License Added	Created when a Defender license is added.	Medium
Defender License Removed	Created when a Defender license is removed.	Medium
Defender License Usage Changed	Created when the Defender license usage value is changed.	Medium
Defender Password Changed	Created when a Defender password is changed for a user.	Medium
Defender Password Cleared	Created when a Defender password is cleared for a user.	Medium
Defender Password Expiry Cleared	Created when the Defender password expiry setting is cleared for a user.	Medium
Defender Password Set	Created when a Defender password was set for a user.	Medium
Defender Policy Added	Created when a new Defender policy is added in a domain.	Medium
Defender Policy Changed for Access Node	Created when a Defender policy for an access node is changed.	Medium
Defender Policy Changed for Group	Created when a Defender policy for a group is changed.	Medium
Defender Policy Changed for Security Server	Created when a Defender policy for a security server is changed.	Medium
Defender Policy Changed for User	Created when a Defender policy for a user is changed.	Medium
Defender Policy Removed	Created when a Defender policy is removed from a domain.	Medium
Defender RADIUS Payload Added	Created when a new Defender RADIUS payload is added in a domain.	Medium

Table 1. Defender events

Event	Description	Severity
Defender RADIUS Payload Changed for Access Node	Created when a Defender RADIUS payload for an access node is changed.	Medium
Defender RADIUS Payload Changed for Group	Created when a Defender RADIUS payload for a group is changed.	Medium
Defender RADIUS Payload Changed for Security Server	Created when a Defender RADIUS payload for a security server is changed.	Medium
Defender RADIUS Payload Changed for User	Created when a Defender RADIUS payload for a user is changed.	Medium
Defender RADIUS Payload Removed	Created when a Defender RADIUS payload is removed from a domain.	Medium
Defender Security Server Added	Created when a Defender security server is added in a domain.	Medium
Defender Security Server Assigned to Access Node	Created when a Defender security server is assigned to an access node.	Medium
Defender Security Server Removed	Created when a Defender security server is removed from a domain.	Medium
Defender Security Server Unassigned to Access Node	Created when a Defender security server is unassigned to an access node.	Medium
Defender Token Added	Created when a new Defender token is added in a domain.	Medium
Defender Token Assigned	Created when a Defender token is assigned to a user.	Medium
Defender Token License Added	Created when a Defender token license is added.	Medium
Defender Token License Removed	Created when a Defender token license is removed.	Medium
Defender Token License Usage Changed	Created when a Defender token license usage value is changed.	Medium
Defender Token PIN Changed	Created when a PIN is changed for a Defender token assigned to a user.	Medium
Defender Token PIN Cleared	Created when a PIN is cleared for a Defender token assigned to a user.	Medium
Defender Token PIN Expiry Cleared	Created when a PIN is set to not expired for a Defender token assigned to a user.	Medium
Defender Token PIN Expiry Set	Created when a PIN is set to expired for a Defender token assigned to a user.	Medium
Defender Token PIN Set	Created when a PIN is set for a Defender token assigned to a user.	Medium
Defender Token Removed	Created when a Defender token is removed from a domain.	Medium
Defender Token Temporary Response Cleared	Created when a temporary response is cleared for a Defender token assigned to a user.	Medium
Defender Token Temporary Response Expiration Changed	Created when a temporary response's expiration is changed for a Defender token assigned to a user	Medium
Defender Token Temporary Response Set	Created when a temporary response is set for a Defender token assigned to a user.	Medium
Defender Token Temporary Response Usage Changed	Created when a temporary response's usage is changed for a Defender token assigned to a user	Medium
Defender Token Unassigned	Created when a Defender token is unassigned to a user.	Medium
Member Added to Access Node	Created when a member is added to an access node.	Medium
Member Removed from Access Node	Created when a member is removed from an access node.	Medium
User Reset Count Changed	Created when the reset count for a user is changed.	Medium
User Violation Count Changed	Created when the violation count for a user is changed.	Medium

Built-in Reports

Change Auditor provides predefined reports which allow you to quickly retrieve valuable change 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'.

To execute a built-in search:

- 1 Click on the **Searches** tab or select the **View | Searches** menu command or **Ctrl+F10** to open the Searches page.
- 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 the **Run** menu command
 - Select the search definition and click the **Run** tool bar button at the top of the Searches page
- 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 or create a custom Defender search, see the Change Auditor User Guide.

Defender built-in reports

The following built-in reports are available with Change Auditor for Defender:

- 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 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 event 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

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. 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.