

Quest® Change Auditor 7.0
SCOM Management Pack



© 2019 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.

Change Auditor SCOM Management Pack
Updated - August 2019
Software Version - 7.0

Contents

SCOM Management Pack Overview	4
Configuration Requirements	4
Prepare the SCOM installation to receive Change Auditor events	4
Prepare Change Auditor to send alerts to the SCOM agent	5
Knowledge Authoring — Purpose	5
Knowledge Authoring — Features	5
Knowledge Authoring — Configuration	6
SCOM 2012/2012 R2/2016 Management Pack Design	7
Change Auditor Target	7
Change Auditor Installation Object Discovery	7
Alert Views	8
About us	9
Our brand, our vision. Together.	9
Contacting Quest	9
Technical support resources	9

SCOM Management Pack Overview

Quest has designed and implemented management packs to integrate with System Center Operations Manager (SCOM) 2012, 2012 R2, and 2016.

i | **NOTE:** SCOM 2007 is no longer supported.

The SCOM management packs:

- Monitor an approved list of Change Auditor events.
- Display instances of these events within the SCOM Operations Console.
- Provide views that can quickly present information about and from the Change Auditor coordinators.

This guide provides information about:

- [Configuration Requirements](#)
- [Knowledge Authoring — Purpose](#)
- [Knowledge Authoring — Features](#)
- [Knowledge Authoring — Configuration](#)

Configuration Requirements

To integrate Change Auditor with SCOM, you need to:

- [Prepare the SCOM installation to receive Change Auditor events](#)
- [Prepare Change Auditor to send alerts to the SCOM agent](#)

Prepare the SCOM installation to receive Change Auditor events

To prepare the SCOM installation to receive events:

- 1 Install a SCOM agent on the server hosting the coordinator.

The agent monitors the server for the WMI events that are sent by triggered alerts.

- 2 Import the Change Auditor Management Pack into SCOM.

The management pack for SCOM 2012, 2012 R2 and 2016. (ChangeAuditor.mp) is located in the following directory within the Change Auditor installation package: <Change Auditor Installation Files Directory>/Integration/SCOM.

i | **NOTE:** Importing the management pack into SCOM may fail if the transaction log for the SCOM database “OperationsManager” is full. This can occur if the database size is set too small and the Autogrowth options are turned off for the database file and the log file.

Importing the management pack creates the rules required to receive the WMI events from the Change Auditor coordinator. The rules are automatically transferred to the SCOM agent.

i | **NOTE:** The list of rules in the SCOM management pack is based on the events in the latest version of Change Auditor. Deprecated events are not available in SCOM.

Prepare Change Auditor to send alerts to the SCOM agent

After you have deployed the SCOM agent and installed the Change Auditor management pack, you need to configure Change Auditor to send events to SCOM. This configuration is required on a per-search basis by creating alerts and enabling the WMI option.

To create an alert, using the Change Auditor client:

- 1 Select the **Searches** tab and choose the required search.
- 2 In the Search Properties panel, select the **Alert** tab.
- 3 Enable alerts on the search by checking the **Alert Enabled** option.
- 4 Enable the WMI setting by checking the option next to **Send Alert To**.
- 5 Save the search.

To create an alert using the web client:

- 1 Log onto the Change Auditor Web Client as an Administrator.
- 2 Click on the **Searches** page on the navigational panel, which is denoted by a magnifying glass icon.
- 3 Select a search.
- 4 In the Search Properties panel, select the **Alert** tab.
- 5 Enable alerts for this search by checking the **Alert Enabled** option.
- 6 Enable the WMI setting by checking the option next to **Send Alert To**.
- 7 Save the search.

When the events are detected, they will display in the SCOM console.

i | **NOTE:** Only alerts that are found in the search with the WMI alerts enabled display in SCOM.

Knowledge Authoring — Purpose

The Management Pack monitors the performance and availability of Change Auditor. By detecting and alerting on critical events, it helps indicate and prevent possible security breaches of Active Directory and the information and resources it contains.

Knowledge Authoring — Features

The Management Pack monitors events from Windows Management Information (WMI) of any computer that is running a properly installed and registered instance of the Change Auditor coordinator. These events, coupled with extensive embedded expertise, enable you to proactively manage Active Directory and avoid costly security breaches.

This management pack alerts you to important events that may occur within Active Directory.

Knowledge Authoring — Configuration

No special configuration is required for this management pack. The Change Auditor components are set up so that the management pack rules automatically deploy to any computer that is running a properly installed and registered instance of the Change Auditor coordinator.

SCOM 2012/2012 R2/2016 Management Pack Design

This section provides the implementation and configuration specifics of the various components of the Change Auditor Management Pack for SCOM 2012, 2012 R2, and 2016.

- [Change Auditor Target](#)
- [Change Auditor Installation Object Discovery](#)
- [Alert Views](#)

Change Auditor Target

The following SCOM type is supported with the Change Auditor Management Pack:

- Quest Change Auditor Installation

This SCOM type identifies which agents are intended to run the Change Auditor rules.

To view a list of all the Change Auditor rules associated with this SCOM type, open the Rules folder of the Authoring pane in the SCOM Operations Console.

Change Auditor Installation Object Discovery

The following SCOM Object Discovery is supported with the Change Auditor Management Pack:

- Quest Change Auditor

This attribute locates the servers that are running Change Auditor coordinators.

The attribute reflects the existence of the following Registry Key, whose presence indicates a properly installed and registered instance of the Change Auditor coordinator:

SOFTWARE\Quest\ChangeAuditor\Coordinator\Path

Alert Views

The following Alert View is supported with the Change Auditor Management Pack:

- Quest Change Auditor

This view presents the list of Change Auditor alerts associated with the members of the Quest Change Auditor Installation type.

Name: Change Auditor Alerts

Description: All Change Auditor alerts

To display the Change Auditor Alert view, open the Change Auditor folder in the Monitoring pane of the SCOM Operations Console.

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.