Quest

Quest® Change Auditor for SharePoint® 7.6

User Guide

© 2025 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.
20 Enterprise, Suite 100
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 SharePoint User Guide
Updated - July 2025
Software Version - 7.6

Contents

Change Auditor for SharePoint Overview 4
Introduction 4
System overview 5
Deployment requirements 6
Enable SharePoint settings 6
Verify MySite permissions 7
Add and deploy Change Auditor SharePoint Solution 8
Create SharePoint Auditing template 9
Client components and features 9

Getting Started 12
Introduction 12
Verify deployment status of Change Auditor SharePoint Solution 12
Verify auditing template is applied 13
Make changes and run a report 13
Troubleshooting steps 14

SharePoint Auditing 16
Introduction 16
SharePoint Auditing page 16
SharePoint Auditing templates 17
SharePoint event logging 20

SharePoint Searches and Reports 21
Introduction 21
Create custom SharePoint searches 21

Manually Add and Deploy the Change Auditor SharePoint Solution 25

SharePoint Event Requirements 26

Upgrade Change Auditor for SharePoint 27
Step 1: Upgrade Change Auditor components 27
Step 2: Run SharePoint Solution Manager 27
Step 3: Edit existing SharePoint Auditing templates 28

About us 29
Our brand, our vision. Together. 29
Contacting Quest 29
Technical support resources 29

1

Change Auditor for SharePoint Overview

- Introduction
- System overview
- Deployment requirements
- Client components and features

Introduction

Auditing your SharePoint platform is critical to maintaining internal security controls and meeting external auditing regulation requirements. Change Auditor for SharePoint tracks operations across your SharePoint environment, providing comprehensive auditing and reporting that tells you 'who, what, when and where' changes are being made to SharePoint configuration, documents, lists and sites.

To enable SharePoint auditing, you must deploy the Change Auditor SharePoint component to the SharePoint farms, then create an auditing template for each farm to define the paths within the farm to audit, and the agent to capture the events.

IMPORTANT: Change Auditor processes all activities on all site collections within the audited SharePoint farm. When auditing a large SharePoint farm with a lot of activity, the agent may experience performance-related issues including slowness in loading the plugin and capturing events or the potential for missed events. Factors that can impact performance include the number of site collections in the farm and the volume of activity in the SharePoint environment. Quest recommends performing a test in the environment of the similar size and configuration to determine if your farm is suitable to be audited by Change Auditor.

Change Auditor also audits user and administration activity for SharePoint Online (and OneDrive for Business) that corresponds to the events in the Microsoft 365 Security & Compliance Center unified audit log. You can track, report, and create alerts on activities including:

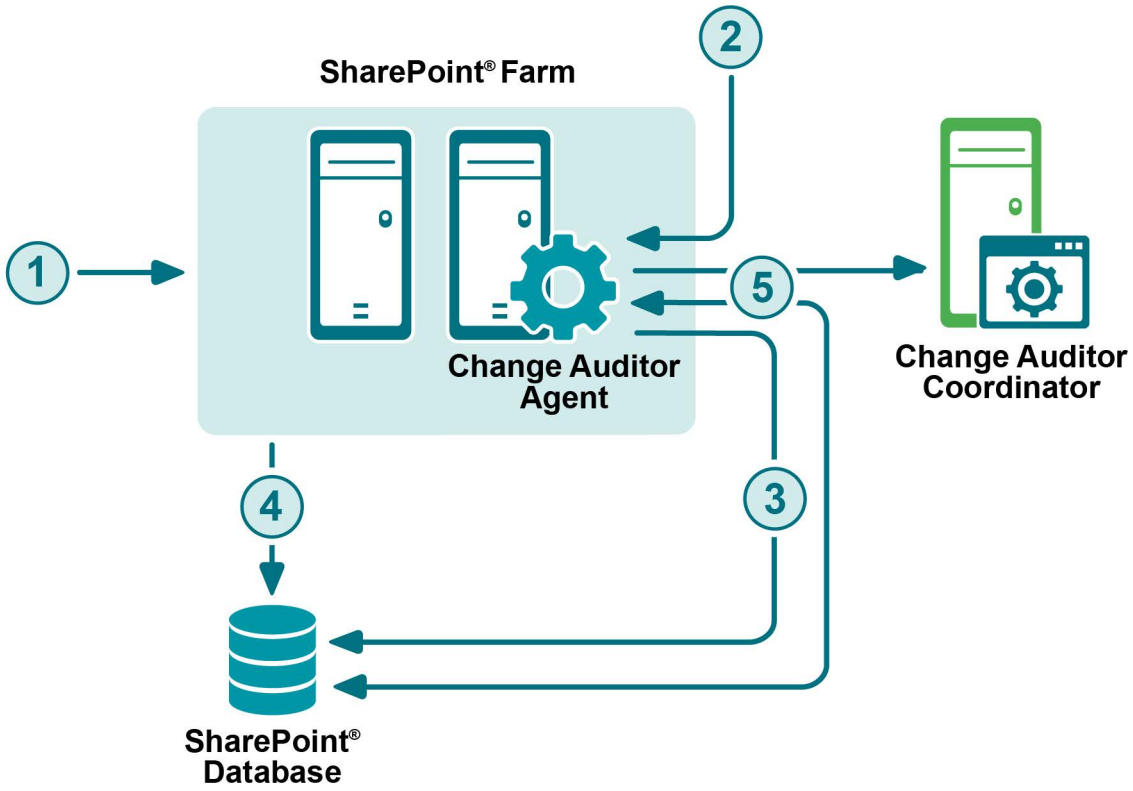
- When files and folders are accessed, created, deleted, uploaded, moved, renamed, and checked in and out of SharePoint Online and OneDrive for Business sites.

This guide has been prepared to assist you in becoming familiar with auditing Change Auditor for SharePoint. 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 SharePoint Event Reference Guide.
- For SharePoint Online and OneDrive for Business event details, see the Microsoft 365 and Microsoft Entra ID Auditing User Guide and Event Reference Guide.

System overview

The following diagram illustrates how SharePoint integrates with Change Auditor to provide this auditing capability.



1 The SharePoint Farm Administrator deploys the **SharePoint.Auditing.Monitor.wsp** solution, which writes event information from each server to the SharePoint database. Deployment is done by running the SharePoint Solution Manager utility.

2 The administrator installs an agent on one of the SharePoint Web Front End servers in the farm.

3 The agent enables the solution for the event information to be captured and written to the SharePoint database AuditData table.

4 System provided SharePoint auditing writes events in the AuditData table shortly after events occur.

5 The agent periodically queries the SharePoint AuditData table to collect the events and forwards them to the coordinator.

Deployment requirements

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

NOTE: This guide assumes SharePoint 2016/2019 is properly installed and configured. For detailed installation steps, see the appropriate guide from Microsoft.

After you have installed Change Auditor, complete the following to audit SharePoint events:

- Enable SharePoint settings
- Add and deploy Change Auditor SharePoint Solution
- Create SharePoint Auditing template

Enable SharePoint settings

To capture some of the SharePoint events, you must enable:

- System provided auditing
- Versioning
- MySite Site Collection
- MySite Web Application

NOTE:

- See SharePoint Event Requirements for a list of the events that need these additional settings enabled.
- Since SharePoint Foundation Server does not provide a graphical user interface, enable these auditing flags (system provided auditing and versioning) using PowerShell commands.

System provided auditing

For all SharePoint web applications (including each user site under MySite) to be audited, system provided auditing must be enabled.

To enable system provided auditing:

1. From a top-level site, or web application, select **Site Actions | Site Settings**.
2. Under the **Site Collection Administration** heading, click **Site collection audit settings**.
3. Under the **Documents and Items** section, select all the check boxes.
4. Under the **Lists, Libraries, and Sites** section, select the **Editing users and permissions** check box.

   NOTE: Log trimming is off by default. Enable log trimming to meet your policies. If the agent is offline or is otherwise unable to retrieve event information from the SharePoint database for a period longer than the trim period, events could be lost.

Versioning

To audit versioning within SharePoint, enable it for each individual Library and List Item pertaining to the Sites being audited.

NOTE: This procedure also applies to announcements, calendars, and tasks. The only difference is that the 'Tools' section and tabs are specific to the List Settings item.

To enable document versioning for shared documents for a top-level site:

1. Navigate to a Document Library.
2. Under **Library Tools**, select the **Library** tab.
3. Click the **Library Settings** icon, located to the right of the ribbon.
4. Click **Versions settings** under General Settings.
5. In the **Document Version History** section, change the selection of **No Versioning** to the desired level of versioning: **Create major versions** or **Create major and minor (draft) version.**

Verify MySite permissions

For proper auditing of sites within the MySite Site Collection or Web Application, the account Change Auditor uses to access the SharePoint database must be added as a Site Collection Administrator (primary or secondary) or to the User Web Policy for the MySite host.

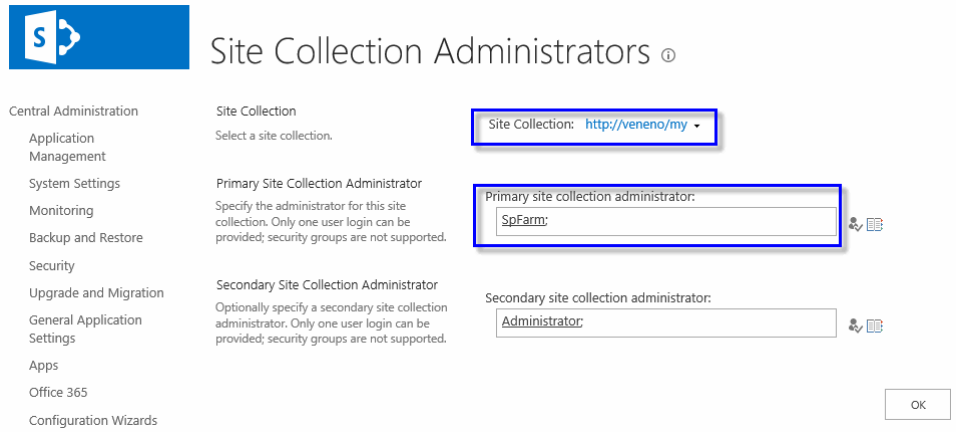
Depending on how your MySite host is initially set up, use the Central Administration Web Site to verify, and if necessary add, this account.

NOTE: This account must be added BEFORE you add a personal site to a SharePoint auditing template or you will encounter an 'access denied' error when you select a personal site in the SharePoint Auditing wizard.

MySite Site Collection

This refers to the default 'MySite' Site Collection that is automatically created during a SharePoint Single Server installation. Its location is under the default SharePoint-80 Web Application (//veneno in the following screen shot). By default, the SharePoint farm account is assigned as the Primary Site Collection Administrator. However, if this site collection is manually created, then the primary and secondary administrator can be specified.

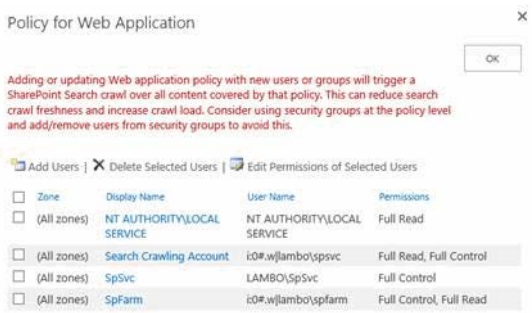
In this scenario, verify that the account Change Auditor is using is listed as either the Primary Site Collection Administrator or Secondary Site Collection Administrator for the MySite Site Collection.



MySite Web Application

This refers to the 'MySite' Web Application that is created manually after a SharePoint Multi-Server Farm installation. In this case, MySite is not tied to any other web application (i.e., is not underneath the default SharePoint Web Application) and therefore uses the User Policy permissions.

In this scenario, verify that the account Change Auditor is using is included in the User Web Policy for the MySite Web Application.



Add and deploy Change Auditor SharePoint Solution

To capture SharePoint events, add the Change Auditor SharePoint Solution (SharePoint.Auditing.Monitor.wsp) to the SharePoint Solution Store (which can be found on the Solution Manager page in the Central Administration site) and deploy it all SharePoint web applications of the SharePoint farms to audit.

Change Auditor provides the SharePoint Solution Manager utility to add the solution to the SharePoint Solution Store and deploy it globally to all SharePoint web applications. The Change Auditor SharePoint Solution must be deployed to all SharePoint web applications on **all** SharePoint farms that you want to audit.

NOTE:

- If you have multiple SharePoint farms in your environment, you must run this utility locally on the Central Administration server in each SharePoint farm.
- You can also do this manually using a Windows PowerShell cmdlet to add it to the store and then deploy it using the SharePoint Central Administration web site. See Manually Add and Deploy the Change Auditor SharePoint Solution.

To add and deploy the solution globally throughout a SharePoint farm:

1. On the local SharePoint farm server, run the SharePoint Solution Manager utility:
   - SharePoint 2016: **SharePointSolutionManagerCALauncher2016.exe**
   - SharePoint 2019: **SharePointSolutionManagerCALauncher2019.exe**

   These utilities can be found in the Plug-in for SharePoint folder under the agent installation folder. For example, the default location is:

   %ProgramFiles%\Quest\ChangeAuditor\Agent\Plug-in for SharePoint
2. On the SharePoint Solution Manager dialog, select both check boxes under the **Install** heading:
   - Add solution to SharePoint solution store
   - Deploy solution to all SharePoint web applications (requires IIS restart)

     NOTE: Since the deployment step requires an IIS restart, this is a separate step that can be run at a more convenient time when an IIS restart is less disruptive. Note that if you do not select this step, you must deploy the solution using the SharePoint Solution Manager utility or SharePoint's Central Administration web site BEFORE Change Auditor can start capturing events.

   Click **Run**.

3 A progress dialog is displayed. When completed, the Change Auditor SharePoint Solution status is updated at the top of the SharePoint Solution Manager dialog.

> **NOTE:** If the add and deploy solution process cannot be completed, an error message is displayed explaining why the process did not complete successfully. Click **Close** to exit the SharePoint Solution Manager utility.
>
> Once the issue is resolved, rerun the SharePoint Solution Manager utility to deploy the Change Auditor SharePoint Solution.

Click **Close** to close the SharePoint Solution Manager dialog.

4 A message is displayed explaining that the deployment status has changed and that the agent needs to be restarted. Click **Close** to close the message box.

5 Restart the agent to enable auditing of SharePoint events.

Create SharePoint Auditing template

Create a SharePoint Auditing template which specifies the SharePoint farm and the paths within the SharePoint farm to audit and the agent to receive events from the selected SharePoint farm.

> **NOTE:** If you have multiple SharePoint farms to be audited, create a separate SharePoint auditing template for each farm.

Client components and features

The following table lists the client components and features that require a valid Change Auditor for SharePoint 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 that this command is only available when the Administration Tasks tab is the active page.

Table 1. Change Auditor for SharePoint client components and features

Client page	Feature
Administration Tasks tab	Agent Configuration page • Event Logging - enable/disable SharePoint event logging Audit Task list: • SharePoint **NOTE:** See SharePoint Auditing for information about enabling event logging and creating templates to define SharePoint auditing.
Event Details pane	What details: • Farm • Site • Item URL

Table 1. Change Auditor for SharePoint client components and features

Client page	Feature
Events	Facilities: • SharePoint Document • SharePoint Document Library • SharePoint Farm • SharePoint Folder • SharePoint List • SharePoint List Item • SharePoint Permission • SharePoint Security Group • SharePoint Site • SharePoint Site Collection
Search Properties	What tab: • Subsystem | SharePoint **NOTE:** See SharePoint Searches and Reports for information on using the What tab to create custom SharePoint search queries.
Searches page	Built-in reports: • All SharePoint Events in the last 7 days • Document Content changes in the last 7 days • Document Story changes in the last 7 days • Document Version changes in the last 7 days • List Item changes in the last 7 days • Permission changes in the last 7 days • Permission Inheritance changes in the last 7 days • Site Collection Groups created and deleted in the last 7 days • Site Collection Groups Membership changes in the last 7 days • Site Collection Ownership changes in the last 7 days • Site Collections created and deleted in the last 7 days • Sites created and deleted in the last 7 days • Sites moved in the last 7 days

Table 1. Change Auditor for SharePoint client components and features

Client page	Feature
Advanced tab/Search Results page	Columns: • SharePoint FarmName • SharePoint ItemName • SharePoint ItemURL • SharePoint ListName • SharePoint ListPath • SharePoint WebName • SharePoint WebURL
Alert Body Configuration dialog - Event Details tab	Variables (email tags): • SHAREPOINT_FARMNAME • SHAREPOINT_ITEMNAME • SHAREPOINT_ITEMURL • SHAREPOINT_LISTNAME • SHAREPOINT_LISTPATH • SHAREPOINT_WEBNAME • SHAREPOINT_WEBURL **NOTE:** See the Change Auditor User Guide for a description of these email tags and how to configure alert email notifications.

2

Getting Started

- Introduction
- Verify deployment status of Change Auditor SharePoint Solution
- Verify auditing template is applied
- Make changes and run a report
- Troubleshooting steps

Introduction

You can search, report and alert on changes to SharePoint Server configuration, permissions, document stores and lists and receive real-time alerts whenever someone makes a critical change in your SharePoint environment.

This section provides a high-level view of the tasks to get you started using Change Auditor for SharePoint. It assumes you have successfully installed/licensed Change Auditor for SharePoint.

NOTE: SharePoint auditing is only available if you have licensed Change Auditor for SharePoint. 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.**

Verify deployment status of Change Auditor SharePoint Solution

You can verify the deployment status of the Change Auditor SharePoint Solution using either the SharePoint Central Administration web site or through the SharePoint Auditing template defined in the client.

To verify status using SharePoint Central Administration web site:

1. Select **Start | All Programs | Microsoft SharePoint 2016/2019 Products | SharePoint 2016/2019 Central Administration**.
2. On the Central Administration Home page, select **System Settings**.
3. On the System Settings page, under Farm Management, click **Manage farm solutions**.
4. Verify that the status associated with the Change Auditor SharePoint Solution (SharePoint.Auditing.Monitor.wsp) is set to 'Deployed'.
5. If the solution's status is 'Not Deployed', deploy the solution:
   - Click the **Sharepoint.Auditing.Monitor.wsp** entry.
   - On the Solution Properties page, click **Deploy Solution**.
   - On the Deploy Solution page, select the appropriate options as described below:
     - **Deploy When** - select one of the following options: **Now** or **At a specified time**

        - **Deploy To** - select to deploy globally to all web applications
    - Click **OK** to save your selections and close the Deploy Solution page.
6. Once the solution is deployed, restart the agent to enable auditing of SharePoint events.

To verify status using the SharePoint auditing template in Change Auditor:

1. Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client**.
2. Open the Administration Tasks tab (**View | Administration** menu command).
3. Click **Auditing**.
4. Select **SharePoint** (under the Applications heading in the Auditing task list) to open the SharePoint Auditing page.
5. Select the template from the list and click **Edit**.
6. Page through the screens of the SharePoint Auditing wizard using the **Next** button.
7. On the last page of the wizard, verify that the Change Auditor SharePoint Solution has been successfully added and deployed to the SharePoint farm selected for auditing.

   NOTE: The Change Auditor SharePoint Solution status is checked/refreshed once every hour; therefore, the status displayed may not reflect the most current status. Click **Refresh Change Auditor Solution Status** to force a refresh of the solution's status.
8. Click **Finish** to close the SharePoint Auditing wizard.

If the status indicates that the solution is not yet added and/or deployed, run the SharePoint Solution Manager utility to add and deploy it. See Add and deploy Change Auditor SharePoint Solution.

Verify auditing template is applied

Check to see if the agent assigned to the SharePoint auditing template is using the latest agent configuration.

To verify that the latest agent configuration is being used:

1. Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client**.
2. Open the Administration Tasks tab (**View | Administration**) menu command.
3. Click **Configuration**.
4. Select **Agent** in the Configuration task list to open the Agent Configuration page.
5. Select the agents assigned to the SharePoint auditing template (**Auditing** appears in the **SharePoint** column) and click **Refresh Configuration**.

   NOTE: If you do not refresh the agent's configuration, the agent automatically checks 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.

Make changes and run a report

1. To test SharePoint auditing, make some changes to the SharePoint farm specified in the template.

   For example:

   - add a document
   - add a folder
   - add an announcement

- add a task
- delete the document added above
- delete the task added above

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 | SharePoint** folder in the left pane.
5. Locate and double-click **All SharePoint Events in the last 7 days** in the right-hand pane.

   A new Search Results tab is added to the client displaying the SharePoint events that were captured.
6. Double-click an event from the Search Results grid to display the event details for the selected event.

Troubleshooting steps

If the SharePoint events do not appear as expected, check the following:

- Review the SharePointPluginCA.Log.nptlog for any errors and to verify that the SharePoint plug-in process is running.
- Verify that a SharePoint Web Front End server is assigned to audit the farm.
- If you are not getting some events (e.g., restore events, permission events, etc.) from a specific site, verify that system provided auditing is enabled for that SharePoint site. See System provided auditing.
- If you are not getting versioning events, verify that versioning is enabled for that type of object in SharePoint. See Versioning.
- Verify that the user account being used to access the SharePoint farm has the following permissions:
  - Local Administrator on the Change Auditor Agent\SharePoint Central Administration server
  - SharePoint Farm Administrator
  - The following mappings on the SQL Server that contains the SharePoint databases:
    - SharePoint_Config
      - SharePoint_Shell_Access
      - SPDataAccess
    - WSS_Content
      - SPDataAccess
    - SharePoint_AdminContent
      - SPDataAccess
- If you get an access denied error when attempting to add a personal site to the SharePoint Auditing wizard, verify that the account being used by the selected agent has been added to the User Web Policy for the site. See MySite Site Collection.
- Verify that you have included the correct SharePoint paths for auditing. (Paths listed across the middle of the first page of the SharePoint Auditing wizard.)
- Verify that you have not excluded the specified paths from auditing. (Paths listed at the bottom of the first page of the SharePoint Auditing wizard.)
- Verify that you have selected those types of events in the SharePoint auditing template. (Facilities and/or event classes specified in the SharePoint Auditing wizard.)
- Verify that the events selected for auditing are enabled. (Use the Audit Events page on the Administration Tasks tab.)

- Verify that the Change Auditor SharePoint Solution has been successfully deployed. See Verify deployment status of Change Auditor SharePoint Solution.
- Refresh the specified agent configuration on the Agent Configuration page to ensure the latest SharePoint auditing template is being used. See Verify auditing template is applied.

3

SharePoint Auditing

- Introduction
- SharePoint Auditing page
- SharePoint Auditing templates
- SharePoint event logging

Introduction

The SharePoint Auditing page on the Administration Tasks tab displays details about each SharePoint auditing template created and allows you to add new auditing templates or modify and delete templates.

NOTE: Each SharePoint farm to be audited requires its own SharePoint Auditing template.

This section provides instructions for creating SharePoint Auditing templates, and a description of the SharePoint Auditing page and SharePoint Auditing wizard. For a description of the dialogs mentioned, see the online help.

SharePoint Auditing page

The SharePoint Auditing page displays when **SharePoint** is selected from the Auditing task list in the navigation pane of the Administration Tasks tab. From this page, you can start the SharePoint Auditing wizard to specify the SharePoint farm and paths to audit. You can also edit existing templates and remove templates that are no longer being used.

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, see the Change Auditor User Guide for more information about how to gain access.

The SharePoint Auditing page contains an expandable view of all the SharePoint Auditing templates that have been defined. To add an template to this list, use the **Add** toolbar button. Once added, the following information is provided for each template:

Farm

Displays the name and GUID of the SharePoint farm specified in the wizard.

Status

Indicates whether the auditing template is enabled or disabled.

Operations

Displays the events selected for auditing on the second page of the wizard. Hover your mouse over this cell to view all the events included in the template.

Agent

Displays the name of the agent assigned to audit the SharePoint farm.

Paths

This field is used for filtering data.

Click the expansion box to the left of the Farm name to expand this view and display the following details for each template:

Title

NOTE: The cells directly under the main heading rows are used for filtering data. That is, as you enter characters into these cells, the client redisplays the templates that meet the search criteria (that is, comparison operator and characters entered). For more details about using the data filtering function provided throughout the client, see the Change Auditor User Guide.

Displays the name assigned to the SharePoint component being audited.

Status

Indicates whether auditing for the selected audit path is enabled or disabled.

Path

Displays the audit path of each SharePoint component to be audited.

Exclude

Displays the SharePoint paths that have been excluded from auditing as specified at the bottom of the first page of the wizard.

SharePoint Auditing templates

To enable SharePoint auditing, create a SharePoint auditing template for each SharePoint farm to audit. Each auditing template defines the SharePoint path within the farm to audit and the agent to capture events from the selected SharePoint farm.

NOTE: There can only be one SharePoint auditing template per SharePoint farm. You cannot proceed if you select a SharePoint farm that already has a template defined.

Be sure that all the SharePoint auditing templates contain a GUID in their Farm name (**Farm** field on SharePoint Auditing page) BEFORE you attempt to add any new templates.

To create a SharePoint Auditing template:

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **SharePoint**.
4. Click **Add** to open the SharePoint Auditing wizard to define the SharePoint farm and paths to audit and the agent to receive the events.
5. On the first page of the wizard, specify the SharePoint farm and paths to audit:
   - **SharePoint Farm**:

     If you are creating a template for a farm that has not been previously audited, use the drop-down arrow and select **Find a SharePoint farm**. On the Eligible Change Auditor Agents dialog, select the SharePoint Web Front End server to capture SharePoint events. Note: If you have multiple agents, select the Web Front End server. The first time an agent is selected, you are prompted to enter the credentials to connect to the SharePoint farm. Change Auditor then performs a SharePoint topology

search to locate the SharePoint farm residing on the selected agent (which may take several minutes). Once the topology is completed, the name of the farm (and GUID) is displayed in the **SharePoint Farm** field in the wizard.

If you are creating a template for a previously audited farm, use the drop-down arrow and select a <*SharePoint Farm (and GUID)*> from the list.

> **NOTE:** The **Next** button on this page is disabled if you select a SharePoint farm from the drop-down list that is assigned to a SharePoint Auditing template. You can only select a SharePoint farm whose auditing template has been deleted.

- Click **Add** and select the SharePoint paths to audit. Once you have selected the paths to audit, they are displayed in the **SharePoint Paths to audit** list.
- Optionally, select **Add optional SharePoint paths to exclude from auditing under** to select a path that has been added to the SharePoint paths to audit and click **Add** to locate and add any subsequent paths within the selected path to exclude from auditing.

6 On the second page of the wizard, select the operations (facilities or event classes) to audit. Select an entry from the list box at the top of the page, expand **Add** and click one of the following commands:

- Use **Add | Add This Event** to add individual events.
- Use the **Add | Add All Events in Facility** option to add all events in the selected facility.

Repeat this step to include more events or facilities. At least one event or facility must be specified.

> **NOTE:** If you want to audit all SharePoint events, they must all be added to this page of the wizard. In addition, the events that are disabled by default must be enabled using the Audit Events page on the Administration Tasks tab.

> **NOTE:** The following operations are audited by default when you create a template. Therefore, they are NOT included in the event class list on this page.
>
> - Site Created
> - Site Deleted
> - Site Moved
> - Site Collection Created
> - Site Collection Deleted

7 The third page of the wizard displays the information about the agent.

If you are creating a template for a farm that has not been previously audited (you used the **Find a SharePoint farm** option) you see a list of servers with Change Auditor agents. Select the required agent, and click **OK**.

If you are creating a template for a previously audited farm, select the required agent in the SharePoint farm and click **OK**. Click **Set Credentials** and enter the credentials to access the SharePoint farm. Click OK. A notification message is displayed indicating whether you have entered valid credentials.

8 On the last page of the wizard, verify that the Change Auditor SharePoint Solution has been successfully added and deployed to the SharePoint farm selected for auditing.

> **NOTE:** The Change Auditor SharePoint Solution status is checked and refreshed once every hour; therefore, the status displayed may not reflect the most current status. Click **Refresh Change Auditor Solution Status** to force a refresh of the solution's status.

9 To create the template, click **Finish**.

10 On the Administration Tasks tab, click **Configuration**, select **Agent** in the Configuration task list to open the Agent Configuration page.

11 Select the agent assigned to the SharePoint Auditing template and click **Refresh Configuration**.

12 Verify that **Auditing** is displayed in the **SharePoint** column.

> **NOTE:** If you do not refresh the agent's configuration, the agent automatically checks for a new agent configuration based on the polling interval setting (on the System Settings tab of the Configuration Setup dialog). The default is every 15 minutes.

To modify a template:

> **NOTE:** If you do not refresh the agent's configuration, the agent automatically checks for a new agent configuration based on the polling interval setting (on the System Settings tab of the Configuration Setup dialog). The default is every 15 minutes.

1. On the SharePoint Auditing page, select a template and click **Edit**.
2. The SharePoint Auditing wizard opens where you can modify the paths included and excluded in the template. For example:
   - On the first page of wizard, you can add a path to the auditing template. You can also add a SharePoint path that to exclude from auditing.
   - On the second page of the wizard, you can add or remove SharePoint events and facilities from the auditing template.
   - On the third page of the wizard, you can select the required agent in the SharePoint farm or change the user account used to access the SharePoint farm.
3. You can also use the last page of the wizard to verify the deployment status of the Change Auditor SharePoint Solution.
4. Once you have made the necessary modifications, click **Finish**.
5. On the Administration Tasks tab, click **Configuration**. Select **Agent** in the Configuration task list to open the Agent Configuration page.
6. Select the agent assigned to the SharePoint Auditing template and click **Refresh Configuration**.

> **NOTE:** If you do not refresh the agent's configuration, the agent automatically checks for a new agent configuration based on the polling interval setting (on the System Settings tab of the Configuration Setup dialog). The default is every 15 minutes.

To disable an auditing template:

The disable feature allows you to temporarily stop auditing the specified SharePoint farm or path without having to remove the template or individual path from a template.

1. On the Auditing page, place your cursor in the **Status** cell for the template, click the arrow control, and select **Disabled**.

   The entry in the **Status** column for the template changes to 'Disabled'.
2. To re-enable the auditing template, use the **Enable** option in either the **Status** cell or right-click menu.

To disable the auditing of a path in a template:

1. On the SharePoint Auditing page, click in the **Status** cell for the path and select **Disabled**.

   The entry in the **Status** column for the selected path changes to 'Disabled'.
2. To re-enable the auditing of a path, use the **Enable** option in either the **Status** cell or right-click menu.

To delete an auditing template:

1. On the Auditing page, select the template and click **Delete | Delete Template**.
2. A dialog is displayed confirming that you want to delete the selected template. Click **Yes**.

To delete a path from a template:

1. On the SharePoint Auditing page, select the path and click **Delete | Delete Path**.
2. A dialog is displayed confirming that you want to delete the selected path from the template. Select **Yes**.

> **NOTE:** If the selected path is the last one in the template, deleting it also deletes the template.

SharePoint event logging

In addition to real-time event auditing, you can enable event logging to capture SharePoint events locally in a Windows event log. This event log can then be collected using InTrust to satisfy long-term storage requirements.

For SharePoint events, event logging is disabled by default. When enabled, only configured activities are sent to the ChangeAuditor for SharePoint event log. See the Change Auditor for SharePoint Event Reference Guide for a list of the SharePoint events that can be sent to the event log.

To enable SharePoint event logging:

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 **Event Logging**.
5. On the Event Logging dialog, select **SharePoint**.
6. Click **OK** to save your selection and close the dialog.

   The SharePoint events configured in the SharePoint Auditing template will then be sent to the ChangeAuditor for SharePoint event log.

4

SharePoint Searches and Reports

- Introduction
- Create custom SharePoint searches

Introduction

You can search, report and alert on SharePoint activity, such as changes to SharePoint configurations, security, and documents. Using the search capabilities of Change Auditor, you can retrieve SharePoint events for multiple site collections and farms or for an individual SharePoint farm, site, path, or object.

This section explains how to create a custom SharePoint search using the What tab. For a description of the dialogs, see the online help.

Create custom SharePoint searches

The following scenarios explain how to use the What tab to create custom SharePoint searches.

NOTE: You can use the other Search Properties tabs to define extra 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

The Origin is not available for SharePoint events.

NOTE: Selecting the **Private** folder creates a search that only you can run and view, whereas selecting the **Shared** folder creates a search which can be run and viewed by all users.

To search all SharePoint paths:

1. Open the Searches page.
2. In the explorer view (left pane), expand and select the folder where you want to save your search.
3. Click **New** to enable the Search Properties tabs across the bottom of the Searches page.
4. On the Info tab, enter a name and description for the search.
5. Open the What tab, expand **Add** and select **Subsystem | SharePoint**.
6. On the Add SharePoint Path dialog, select **All SharePoint Paths.**
7. Click **OK** to save your selection and close the dialog.
8. 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**.

9 When this search runs, Change Auditor searches for the SharePoint events based on the search criteria specified on the What tab and display the results in a new search results page.

To search for changes to a SharePoint farm:

NOTE: This procedure also applies to searching for changes to the other SharePoint objects (such as web applications, sites, lists, and so on.).

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

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

5 Open the What tab, expand **Add** and select **Subsystem | SharePoint**.

6 On the Add SharePoint Path dialog, select **This Object.**

7 Selecting **This Object** enables the selection controls on this dialog, which includes a hierarchical display (left pane) and a wildcard expression pane (right pane).

The hierarchical pane displays your SharePoint farms, including the web applications, sites and lists discovered on each farm. Using this pane, you can search for events against an individual object.

The wildcard expression pane is populated as you select objects in the hierarchical pane. Using this pane, you can expand your search for events against all objects that match a specific wildcard expression.

Using this pane, select the SharePoint farm to include in the search.

- To search an individual SharePoint farm, select the farm to search in the hierarchical pane on the left.
- To search SharePoint farms using a wildcard expression, select the check box next to the **Farm Name** in the right pane. Select the operator (**Like** or **Not Like**) and enter the string of characters to use to find SharePoint farms.

8 Once you have selected the SharePoint farm to include in the search definition, click **Add** 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 SharePoint farms EXCEPT those listed in the 'what' list.

NOTE: Select the **Runtime Prompt** check box on this dialog to prompt for a SharePoint object every time the search is run.

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

10 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**.

11 When this search runs, Change Auditor searches for the SharePoint events based on the search criteria specified on the What tab and display the results in a new search results page.

To locate SharePoint events based on a wildcard expression:

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

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

5 Open the What tab, expand **Add** and select **Subsystem | SharePoint**.

6 On the Add SharePoint Path dialog, select **This Object.**

7 Use the right pane to specify the wildcard expression to be used to search for SharePoint events.

- Select the SharePoint components to include in your search: **Farm Name, Web Name, List Name, Item Name** and/or **Item URL**.
- For each SharePoint component selected, select the comparison operator to use: **Like** or **Not Like**
- For each SharePoint component selected, enter the pattern (character string and * wildcard character) to use to search for a match.

  NOTE: When multiple wildcard expressions are specified (such as when multiple check boxes are selected), they are 'ANDed' together and all of the expressions must be met to be considered a match.

  For example, to search all web application sites that begin with 'Admin' for documents that contain 'procedure' in their name:

  - Select (check) **Web Name** and specify: **Like Admin***
  - Select (check) **Item Name** and specify: **Like *procedure***

NOTE: You can also select objects in the hierarchical pane to pre-populate the fields in the wildcard expression pane. When you use this approach to pre-populate the fields, the check boxes associated with the objects do not need to be checked in order to include them in your wildcard expression. However, in order to convert or add a specific expression, you must select the corresponding check box in order to select the comparison operator and pattern to be matched.

For example, to search for all documents that begin with 'Sales' in a SharePoint farm:

- From the hierarchical pane, select/highlight the SharePoint farm to be searched (this will pre-populate the Farm Name field in the wildcard expression pane)
- From the wildcard expression pane, select **Item Name** check box and specify: **Like Sales***

8 After entering the wildcard expressions to use, click **Add** 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 SharePoint sites EXCEPT those listed in the 'what' list.

NOTE: Select the **Runtime Prompt** check box on this dialog to prompt for a SharePoint path every time the search is run.

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

10 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**.

11 When this search runs, Change Auditor searches for the SharePoint events based on the search criteria specified on the What tab and display the results in a new search results page.

To search for SharePoint paths that already have an event in the database:

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

3 Click **New** to enable the Search Properties tabs across the bottom of the Searches page.

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 | SharePoint**.

6 On the Add SharePoint Paths dialog, select a path from the list and click **Add** to add it to the selection list at the bottom of the page.

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

8 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**.

9 When this search runs, Change Auditor searches for the SharePoint events based on the search criteria specified on the What tab and display the results in a new search results page.

5

Manually Add and Deploy the Change Auditor SharePoint Solution

The procedure provided in this section explains how to manually add the Change Auditor SharePoint Solution to the SharePoint Solution Store and deploy the solution to web applications.

NOTE: If you have already run the SharePoint Solution Manager utility as described in Add and deploy Change Auditor SharePoint Solution, there is no need to manually add and deploy the solution.

To add and deploy the Change Auditor SharePoint Solution:

1. On the server that is running Microsoft SharePoint 2016/2019 Products, open a SharePoint PowerShell management shell (**Start | All Programs | Microsoft SharePoint 2016/2019 Products | SharePoint 2016/2019 Management Shell**).
2. At the command prompt, enter the following command:

   ```
   Add-SPSolution -LiteralPath "C:\Program Files\Quest\ChangeAuditor\Agent\Plug-in for SharePoint\SharePoint.Auditing.Monitor.wsp"
   ```

   Running this command adds the Change Auditor SharePoint Solution to the farm's solution store.

   You need to now deploy the solution.
3. Open the SharePoint Central Administration web site (**Start | All Programs | Microsoft SharePoint 2016/2019 Products | SharePoint 2016/2019 Administration**).
4. On the Central Administration Home page, select **System Settings**.
5. On the System Settings page, under Farm Management, click **Manage farm solutions**.
6. On the Solution Management page, locate and click **SharePoint.Auditing.Monitor.wsp**.
7. On the Solution Properties page, click **Deploy Solution**.
8. On the Deploy Solution page, select the appropriate options as described below:
   - **Deploy When** - select one of the following options: **Now** or **At a specified time**
   - **Deploy To** - select to deploy globally to all web applications or to an individual web application if you have specified a web application in the PowerShell cmdlet when you added the solution to the solution store

   Click **OK** to save your selections and close the Deploy Solution page.
9. Once successfully deployed, the **Status** column for the Change Auditor SharePoint Solution displays **Deployed** as shown below.
10. Once the solution is deployed, restart the agent to enable auditing of SharePoint events.

6

SharePoint Event Requirements

The following table lists the SharePoint events that require additional SharePoint settings enabled for

Table 2. SharePoint event requirements

Event	System Provided Auditing	Versioning
All document versions deleted	X	X
All list item versions deleted	X	X
All permission levels revoked	X	
Document library restored from recycle bin	X	
Document restored from recycle bin	X	
Document version deleted	X	X
Document viewed	X	
Folder restored from recycle bin	X	
List item restored from recycle bin	X	
List item version deleted	X	X
List restored from recycle bin	X	
Member added to security group	X	
Member removed from security group	X	
Permission inheritance broken	X	
Permission inheritance restored	X	
Permission level created	X	
Permission level deleted	X	
Permission level granted	X	
Permission level inheritance broken	X	
Permission level permissions modified	X	
Permission level revoked	X	
Security group created	X	
Security group deleted	X	
Site collection ownership granted	X	
Site collection ownership revoked	X	

7

Upgrade Change Auditor for SharePoint

Use this upgrade procedure if you have a previous version of Change Auditor for SharePoint installed and have existing SharePoint auditing templates defined.

- Step 1: Upgrade Change Auditor components
- Step 2: Run SharePoint Solution Manager
- Step 3: Edit existing SharePoint Auditing templates

Step 1: Upgrade Change Auditor components

If you have a previous version of Change Auditor installed, upgrade the Change Auditor components in the following order:

NOTE: For detailed instructions on upgrading Change Auditor, see the Change Auditor Installation Guide.

1. Change Auditor coordinator (and database schema)

   NOTE: If you are upgrading from Change Auditor for SharePoint 6.0, you will not require a new license for this product (or any of the other Change Auditor products).

2. Change Auditor client
3. Change Auditor agents

   NOTE: Deploy an agent on one of the SharePoint Web Front End servers in the SharePoint farm to be monitored.

Step 2: Run SharePoint Solution Manager

Users with existing SharePoint auditing in place must run the SharePoint Solution Manger on all SharePoint Central Administration servers.

NOTE: If any existing SharePoint auditing templates are edited after a 6.5 upgrade, the wizard checks the Solution Deployment .wsp file and alerts you if the SharePoint Solution Manager has not been run.

1. On the local SharePoint farm server, run the SharePoint Solution Manager utility:
   - SharePoint 2016: SharePointSolutionManagerCALauncher2016.exe

- SharePoint 2019: SharePointSolutionManagerCALauncher2019.exe

These utilities can be found in the Plug-in for SharePoint folder under the Change Auditor agent installation folder. For example, the default location is: %ProgramFiles%\Quest\ChangeAuditor\Agent\Plug-in for SharePoint.

Running the SharePoint Solution Manager scans the topology and displays the message 'Solution needs to be upgraded'.

2 Select both check boxes under the **Remove previous and Install** heading:

- Add solution to SharePoint solution store
- Deploy solution to all SharePoint web applications

Click **Run**.

3 A progress dialog appears. When completed, the Change Auditor SharePoint Solution status is updated at the top of the dialog. Click **Close**.

4 A message appears explaining that the old solution was removed and that the new solution was added and deployed.

5 Click **Close** to close the message box.

6 Restart the Change Auditor agent to enable auditing of SharePoint events.

Step 3: Edit existing SharePoint Auditing templates

Change Auditor for SharePoint 5.9 and later includes the GUID of the SharePoint farm server in the template name. Therefore if you are upgrading from a pre-5.9 version, you must open and edit each of your existing SharePoint auditing templates to capture this additional information.

NOTE: You must edit all exiting SharePoint templates before you can add any new ones. Ensure that all SharePoint templates contain a GUID in their Farm name (**Farm** field on SharePoint Auditing page) before adding new templates.

To edit an existing SharePoint Auditing template:

1 Open the Administration Tasks tab.

2 Click **Auditing**.

3 Select **SharePoint** (under the Applications heading in the Auditing task list) to open the SharePoint Auditing page.

4 Select the template to be edited and click **Edit**.

The wizard automatically appends the GUID associated with the selected SharePoint Farm to the name displayed in the **SharePoint Farm** field. In addition, the drop-down option to 'Find a new SharePoint Farm' is not available.

5 Click through the wizard pages. No changes are required.

6 On the last page of the wizard, click **Refresh Change Auditor Solution Status** and verify that the Change Auditor SharePoint Solution has been successfully added and deployed to the SharePoint farm.

7 Click **Finish** to save the updated template.

Once the existing SharePoint Auditing templates are updated, you can add new SharePoint Auditing templates to monitor other SharePoint farms.

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.