

Quest® Change Auditor for Exchange 7.3
User Guide



© 2022 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

Change Auditor for Exchange Overview	4
Introduction	4
Deployment requirements	4
Client components and features	5
Exchange Searches and Reports	7
Introduction	7
Run the All Exchange Events report	7
Create custom Exchange searches	8
Exchange Mailbox Auditing	12
Introduction	12
Exchange Mailbox Auditing page	13
Exchange Mailbox Auditing list	14
Exchange Auditing wizard	16
Exchange Settings and Event Logging (Agent Configuration Page)	18
Introduction	18
Exchange Folder Open Event setting	18
Exchange event logging	19
Exchange Mailbox Protection	20
Exchange mailbox protection introduction	20
Exchange Mailbox Protection page	20
Exchange Mailbox Protection templates	22
Exchange Protection wizard	23
Managing Shared Mailboxes	26
Shared Mailbox events	27
Disabled Exchange Events	29
About us	32
Our brand, our vision. Together.	32
Contacting Quest	32
Technical support resources	32

Change Auditor for Exchange Overview

- [Introduction](#)
- [Deployment requirements](#)
- [Client components and features](#)

Introduction

Change Auditor for Exchange proactively audits the activities taking place in your entire Exchange environment, then provides real-time, detailed alerts about vital changes that occur. It provides extensive, customizable auditing and reporting capabilities for all critical changes, including those made to administrative groups, mailbox policies, public and private information stores, ActiveSync mailbox policies, and distribution lists. Continually being in-the-know helps you to prove compliance, drive security, and improve uptime while proactively auditing changes to Exchange Server configurations and permissions.

The Exchange Mailbox auditing feature helps tighten enterprise-wide change and control policies by tracking user and administrator activity such as user account changes, delivery restriction changes, send on behalf updates, and more. With these types of real-time alerts and in-depth analysis and reporting capabilities, your Exchange infrastructure is protected from exposure to suspicious behavior or unauthorized access and kept in compliance with corporate and government standards.

In addition to Exchange Mailbox auditing, you can protect and lock down critical mailboxes from unauthorized or accidental access.

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

Change Auditor for Exchange also allows you to audit the activities taking place in the Office 365 Exchange Online organization. For details see the Change Auditor for Office 365 and Azure Active Directory Auditing User Guide.

This guide has been prepared to assist you in becoming familiar with Change Auditor for Exchange. 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 Exchange Event Reference Guide.

Deployment requirements

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

Client components and features

The following table lists the client components and features that require a valid Change Auditor for Exchange license. You are not prevented you from using these features; however, associated events or protection are not captured or enforced unless the proper license is applied.

i | **NOTE:** To hide unlicensed Change Auditor features from the Administration Tasks tab (including unavailable audit events throughout the client), select **Action | Hide Unlicensed Components**. This is only available when the Administration Tasks tab is the active page.

Table 1. Change Auditor for Exchange client components and features

Client Page	Feature
Administration Tasks Tab	<p>Agent Configuration:</p> <ul style="list-style-type: none"> Configuration Setup Dialog - Exchange Tab <ul style="list-style-type: none"> Discard duplicates that occur within <i>nn</i> seconds Event Logging - enable/disable Exchange event logging <p>NOTE: See Exchange Settings and Event Logging (Agent Configuration Page) for information about viewing and modifying the agent configuration setting and enabling event logging.</p> <p>Audit Task List:</p> <ul style="list-style-type: none"> Exchange Mailbox <p>NOTE: See Exchange Mailbox Auditing for information about including mailboxes for Exchange Mailbox auditing and Shared Mailbox auditing.</p> <p>Protection Task List:</p> <ul style="list-style-type: none"> Exchange Mailbox <p>NOTE: See Exchange Mailbox Protection for information about creating and maintaining Exchange Mailbox Protection templates.</p>
Event Details Pane	<p>What Details:</p> <ul style="list-style-type: none"> Class (Exchange) Object (Exchange) <p>NOTE: See Exchange Searches and Reports for details on additional information.</p>
Events	<p>Facilities:</p> <ul style="list-style-type: none"> Exchange ActiveSync Monitoring Exchange Administrative Group Exchange Distribution List Exchange Mailbox Monitoring Exchange Organization Exchange Permission Tracking Exchange User
Search Properties	<p>What Tab:</p> <ul style="list-style-type: none"> Subsystem Exchange <p>NOTE: See Exchange Searches and Reports for information about creating custom Exchange search queries.</p>

Table 1. Change Auditor for Exchange client components and features

Client Page	Feature
Searches Page	Built-in Reports: <ul style="list-style-type: none">• All reports that include the events in the Exchange facilities.
Alert Custom Email Dialog	<ul style="list-style-type: none">• Add Users - When selected, alerts for user object changes are sent to the user; alerts for mailbox objects are sent to the mailbox owner.• Add Managers - When selected, alerts for user object changes are sent to the user manager (if set); alerts for group objects are sent to the managed-by user (if set). Alerts for mailbox objects are sent to the owner's manager (if set).

Exchange Searches and Reports

- [Introduction](#)
- [Run the All Exchange Events report](#)
- [Create custom Exchange searches](#)

Introduction

Change Auditor delivers both preconfigured and customizable reports displaying events from Exchange servers in one centralized viewer. Change Auditor for Exchange provides two subsystems related to Exchange auditing:

- The **Exchange** subsystem is used for administration, searching and reporting on the Exchange events contained in the following facilities:
 - Exchange ActiveSync Monitoring
 - Exchange Administrative Group
 - Exchange Distribution List
 - Exchange Mailbox Monitoring
 - Exchange Organization
 - Exchange Permission Tracking
 - Exchange User
- The **Office 365** subsystem is used for administrators, searching and reporting on events contained in the following facilities:
 - Office 365 Exchange Online Administration
 - Office 365 Exchange Online Mailbox

i | **NOTE:** See the Office 365 and Azure Active Directory Auditing User Guide for details.

This section explains how to run a built-in Exchange report and how to create custom Exchange search queries using the What tab. For a description of the dialogs mentioned in this chapter, refer to the online help.

Run the All Exchange Events report

Running this report retrieves the Exchange events captured on all Exchange servers hosting a Change Auditor agent.

i | **NOTE:** This query uses the Exchange subsystem; therefore, it returns all Exchange events except for Office 365 Exchange Online events.

- 1 Open the client and the Searches tab.
- 2 In the explorer view (left pane), expand the **Shared | Built-in | All Events** folder.

- 3 Locate and double-click **All Exchange Events**.

This displays a new Search Results page displaying the Exchange events captured over the last seven days.

- i** | **NOTE:** To retrieve the Exchange events captured over the last 24 hours, use the **All Exchange Events in the last 24 hours** report under the **Shared | Built-In | Recommended Best Practice | Exchange** folder.

Create custom Exchange searches

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

- i** | **NOTE:** You can use the other search properties tabs to define more criteria:

- Who - allows you to search for events generated by a specific user
- Where - allows you to search for events captured by a specific agent
- When - allows you to search for events that occurred within a specific date/time range
- Origin - allows you to search for events that originated from a specific workstation or server

To search for changes to a specific Exchange container:

- 1 Open the Searches page.
- 2 In the explorer view (left pane), expand and select the folder where you want to save your search.
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 Change Auditor users.
- 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 On the What tab, expand **Add** and click **Subsystem | Exchange** to display the Add Exchange Container dialog.
i | **NOTE:** You can use **Add with Events | Subsystem | Exchange** to search for an entity that already has an event associated with it in the database.
- 6 On the Add Exchange Container dialog, select one of the following options to define the scope of coverage:
 - **All Exchange Objects** - select to include all objects. (Default when Add is used.)
 - **This Object** - select to include the selected objects only. (Default when Add With Events is used.)
 - **This Object and Child Objects Only** - select to include the selected objects and its direct child objects.
 - **This Object and All Child Objects** - select to include the selected objects and all subordinate objects (in all levels).
 - **Members of this group** - select this option to show changes made to users in a specified group. Nested groups are not supported.
i | **NOTE:** You cannot exclude selections or use the *Like wildcard option when the scope is specified as Members of this group.
- 7 By default, **All Actions** is selected meaning that all the activity associated with the object generates an audited event. However, you can clear the **All Actions** option and select individual options. The options available are:
 - **All Actions** - select to include when any of the following actions occur (Default)
 - **Add Attribute** - select to include when an attribute is added

- **Delete Attribute** - select to include when an attribute is deleted
- **Modify Attribute** - select to include when an attribute is modified
- **Rename Object** - select to include when an object is renamed
- **Add Object** - select to include when an object is added
- **Delete Object** - select to include when an object is deleted
- **Move Object** - select to include when an object is moved
- **Other** - select to include other types of activity against the selected object

8 By default, **All Transports** is selected indicating that all Exchange events regardless of the transport protocol used are included in the search. However, you can clear the **All Transports** option and select individual options. The transport options available are:

- **All Transports** - select to include Exchange events regardless of the transport protocol used (Default)
- **All Transports** - select to include LDAP operation or LDAP queries regardless of the transport protocol used (Default)
- **SSL/TLS** - select to include LDAP operation or LDAP queries that are secured using SSL or TLS technology
- **Kerberos** - select to include LDAP operation or LDAP queries that are signed using Kerberos-based encryption
- **Simple Bind** - select to include LDAP operation or LDAP queries that are secured using simple bind authentication (neither SSL/TLS or Kerberos used)
- **Port** - select to identify a specific port used for communication

i | **NOTE:** When you clear the **All Transports** check box and select both the **SSL/TLS** and **Kerberos** check boxes, only AD queries using both of these transport protocols will be included in the search results.

9 When a scope other than **All Exchange Objects** is selected, the directory object picker is enabled to select the objects to include in the search definition.

Use either the Browse or Search page to locate and select the Exchange containers to include.

If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.

Use the Options page to view or modify the search options to retrieve directory objects.

You can also select **Import Objects** to import a .csv (comma separated value) file containing a list of directory objects. Using this list, you can specify object names and optional values for the search criteria. You can use the * wildcard character to match any string of zero or more characters when specifying the Name values.

i | **NOTE:** For optimal performance, do not include more than 1000 objects in your import file.

The import will fail and an error message will be displayed if any errors are detected with the column names or specified values.

i | **NOTE:** Column names and values must be separated with a comma.

i | **NOTE:** If an optional column name is not specified, then the default All is used for the value for each object. The default All is also used if the optional column is specified, but the value is empty. Mandatory Name values cannot be empty.

COLUMNS	DESCRIPTION
Name (Required)	<p>The name of the directory object to import. Name values must be specified in canonical name format.</p> <p>NOTE: The first column must be Name.</p> <p>NOTE: Wildcard characters are only supported for the Name values.</p> <p>Examples:</p> <p>Column: Name</p> <p>Values:</p> <ul style="list-style-type: none"> • test.domain.ca/OU1/User1 • test.domain.ca/*/Group1 • test.domain.ca/OU1/*User*
Actions (Optional)	<p>Possible values include: Add Attribute, Delete Attribute, Modify Attribute, Rename Object, Add Object, Delete Object, Move Object or Other.</p> <p>When specifying multiple values they must be separated by the Pipe character ' '. Examples:</p> <p>Columns: Name,Actions</p> <p>Values:</p> <ul style="list-style-type: none"> • test.domain.ca/OU1/User1,Move Object Modify Attribute • test.domain.ca/OU1/Group*,
Transports (Optional)	<p>Possible values include SSL/TLS, Kerberos or Simple Bind.</p> <p>When specifying multiple values they must be separated by the Pipe character ' '. Examples:</p> <p>Columns: Name,Actions,Transports</p> <p>Values:</p> <ul style="list-style-type: none"> • test.domain.ca/OU1/User1,Move Object Modify Attribute,Kerberos • test.domain.ca/OU1/Group1,,Kerberos SSL/TLS
Port (Optional)	<p>The number of the required port.</p> <p>Examples:</p> <p>Columns: Name,Actions,Transports,Port</p> <p>Values:</p> <ul style="list-style-type: none"> • test.domain.ca/OU1/*,,Move Object Modify Attribute,Kerberos,389 • test.domain.ca/OU1/Group1,Add Attribute,Kerberos, <p>NOTE: When importing a file in the web client, the default value (All Ports) will be applied if port values are specified.</p>

- i** | **NOTE:** Select the **Exclude the Above Selection(s)** check box if you want to search for changes to all Exchange containers except those listed in the 'what' list.
- i** | **NOTE:** Select the **Runtime Prompt** check box on this dialog to prompt for an Exchange container every time the search is run.

10 After you have added all the Exchange containers to include in the search, click **OK** to save your selection and close the dialog.

- 11 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**.
- 12 When this search runs, Change Auditor searches for changes to the Exchange containers specified on the What tab.

To search for changes to an Exchange object using 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.

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 Change Auditor users.
- 3 Click **New** at the top of the Searches page to activate 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 On the What tab, expand **Add** and click **Subsystem | Exchange**.
- 6 On the Add Exchange Container dialog, select the **This Object** scope.

If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.
- 7 Use the wildcard expression fields in the middle of the dialog to specify the expression to use to search for Exchange objects (Object Name column in Search Results grid).
 - Select the comparison operator: **Like** or **Not Like**.
 - In the field to the right, enter the pattern (character string and * wildcard character) to use to search for a match.

Use the * wildcard character to match any zero or more characters. For example: **LIKE *admin*** finds Exchange objects that contain 'admin' anywhere in their name.
 - Click **Add** to add the wildcard expression to the Selected Objects list box at the bottom of the dialog.
- 8 After entering the wildcard expression to use, click **OK** to close the dialog and add the wildcard expression to the 'What' list.
- 9 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**.
- 10 When this search runs, Change Auditor searches for changes to the Exchange containers specified on the What tab.

Exchange Mailbox Auditing

- [Introduction](#)
- [Exchange Mailbox Auditing page](#)
- [Exchange Mailbox Auditing list](#)
- [Exchange Auditing wizard](#)

Introduction

Exchange mailbox auditing helps tighten enterprise-wide change and control policies by tracking user and administrator activity such as user account changes, delivery restriction changes, send on behalf updates, and more. With these real-time alerts and in-depth analysis and reporting capabilities, your Exchange infrastructure is always protected from exposure to suspicious behavior or unauthorized access and kept in compliance with corporate and government standards.

- i** **NOTE:** Agent processing of Exchange auditing and protection configurations may slow down initial user login access or cause timeouts if many user logins occur at the same time. To avoid this issue, Quest recommends that changes to mailbox auditing or protection configurations be performed during maintenance intervals or other periods of low user mailbox activity.
Before the system is returned to normal load, one user should log on to Outlook Web Access (OWA), Outlook (Outlook for Mac) clients. This triggers the agent to process the mailbox auditing and protection configuration changes when the fewest logins are occurring.
- i** **NOTE:** Starting the agent on Exchange 2013 and higher mailbox servers in large organizations during periods of heavy user mailbox activity, can also cause service interruptions to Outlook users while the clients reconnect. To avoid this, Quest recommends that the agent be scheduled for periods of reduced user activity.
If necessary, you can disable forcing Outlook reconnections on a server-by-server basis. Contact Quest Technical Support for additional information.
- i** **NOTE:** To eliminate auditing of automated tasks, the agent attempts to automatically exclude auditing of mailboxes accessed by Blackberry Enterprise Server (BES) or similar service accounts. These accounts have both 'Receive All' and 'Administer Information Store' rights on the mailbox database. If these explicit rights are granted to user accounts, those accounts are also excluded from mailbox auditing, which may not be wanted. If necessary, you can disable this automated exclusion on a server-by-server basis. Contact Quest Technical Support for additional information.

To enable mailbox auditing, you define a mailbox auditing list that contains the directory objects whose mailbox activities you want to audit. Change Auditor for Exchange generates shared mailbox events for shared mailbox, room and equipment resources, and for any other mailboxes that the user has identified as shared. See the [Managing Shared Mailboxes](#) appendix for more information.

In Change Auditor, some mailbox events are disabled by default due to the potentially high volume of events that can occur. To capture these events, enable them using the Audit Events page of the Administration Tasks tab.

i | **IMPORTANT:** When the Message read by non-owner event is enabled and a mailbox is moved from one mailbox store to another, Change Auditor generates an event for every email in the mailbox that is being moved. For example, if a user has 1,000 emails in their mailbox, you receive 1,000 Message read by non-owner events in Change Auditor.

To avoid generating these events, do not add the user account for the mailbox to be moved to the list on the Exchange Mailbox Auditing page on the Administration Tasks tab.

This section provides a description of the Exchange Mailbox Auditing page and explains how to create and maintain the Exchange Mailbox Auditing list. For a description of the dialogs mentioned in this chapter, refer to the online help.

Exchange Mailbox Auditing page

To enable mailbox auditing, you must first specify the mailbox activity to audit. To do this, you will use the Exchange Mailbox Auditing page, which displays when you select **Exchange Mailbox** from the Auditing task list in the navigation pane of the Administration Tasks tab.

i | **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 information about how to gain access.

i | **NOTE:** The directory objects listed on this page only apply to the events contained in the Exchange Mailbox Monitoring and Exchange ActiveSync Monitoring facilities. This list does not apply to any of the other Exchange facilities.

The Exchange Mailbox Auditing page contains a list of the directory objects whose mailboxes are to be audited. If a directory object is not listed on this page, its mailbox will not be audited. To add a directory object to this list, click **Add**. Once added, the following information is displayed:

Type

Displays the type of directory object selected for Exchange Mailbox auditing (such as User, Group, Container, DomainDNS, OrganizationalUnit, or BuiltinDomain)

Events

Indicates the type of events to audit:

- Non-owner
- Non-owner or Owner (only applies to individual user objects)

To change this setting, place your cursor in this cell, click the arrow control, and select the appropriate option from the list.

i | **NOTE:** 'By owner' events are disabled by default and need to be enabled to capture these events if the **Non-owner or Owner** option is selected.

Scope

Displays the scope of coverage:

- Object
- One Level
- Subtree

To change this setting, place your cursor in this cell and select the appropriate option from the list.

Exclude

Indicates whether mailboxes in the directory object are audited (Exclude = No) or excluded from auditing (Exclude = Yes).

To change this setting, place your cursor in this cell, click the arrow control, and select **Yes** to exclude the directory object or **No** to include the directory object in the auditing process.

Status

Indicates whether the audit entry for this directory object is enabled or disabled. Disabled entries have no effect on auditing. Disabled entries can be re-enabled later.

To change this setting, place your cursor in this cell, click the arrow control, and select **Enabled** to enable the audit object or **Disabled** to disable the audit object.

Exchange Mailbox

Displays the canonical name associated with the directory objects listed.

Name

Displays the name of the directory objects listed.

DisplayName

If applicable, this column shows the display name assigned to the directory object.

i **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 redisplay 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 Quest Change Auditor User Guide.

Exchange Mailbox Auditing list

The Exchange Mailbox Auditing list contains a list of the directory object's whose Exchange Mailbox is to be either included or excluded in the auditing process. Click **Add** to include a mailbox in the auditing process or use the **Add | Exclude** toolbar option to exclude a mailbox from the auditing process.

To include an Exchange Mailbox in the auditing process:

- 1 Open the Administration Tasks tab.
- 2 Click **Auditing**.
- 3 Select **Exchange Mailbox** (under Applications).
- 4 Click **Add** to display the Exchange Auditing Wizard.
- 5 Select one of the options at the top of the page: **Enterprise** or **This Object** (default).
- 6 If the **This Object** option is selected, use the Browse and Search pages to locate and select a directory object (for example, User, Group, Container, DomainDNS, OrganizationalUnit, or BuiltinDomain) and use the **Add** button to add the selected directory object to the Selected Object list at the bottom of the page.

If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.

Repeat this step to add more directory objects to the Exchange Mailbox Auditing list.

- 7 Click **Finish** to close this wizard and return to the Exchange Mailbox Auditing page, where your selections are listed with a **No** in the **Exclude** cell.

i | **NOTE:** From the Exchange Mailbox Auditing page, you can include a previously excluded mailbox by changing the setting in the **Exclude** cell. Use one of the following methods:

- Place your cursor in the **Exclude** cell of the mailbox to include, click the arrow control, and select **No**.
- Right-click the mailbox entry and click **Audit**.

- 8 By default, only Non-Owner events are selected for auditing.

For individual user mailboxes, you can change this to include 'By Owner' events as well. To do so, place your cursor in the **Events** cell, click the arrow control, and select the **Owner, Non-Owner** option from the list.

i | **IMPORTANT:** Selecting 'By Owner' auditing for many mailboxes can produce a large number of events. This adversely affects Change Auditor auditing and in severe cases the performance of the Exchange Server itself. In extreme cases, Outlook connections may be slowed or dropped. Select owner auditing for at most only a few critical mailboxes.

i | **NOTE:** 'By Owner' events are disabled by default. Therefore, you need to enable these events from the Audit Events page on the Administration Tasks tab before Change Auditor processes them.

i | **NOTE:** Auditing normal mailboxes where access permission is granted to many delegates (more than 10), can produce large numbers of non-owner events. This will adversely affect Change Auditor auditing and in severe cases, the performance of the Exchange Server itself. If these mailboxes must be audited, add them to the Shared Mailbox list (User Defined tab) to reduce unwanted non-owner events and to improve performance. See [Managing Shared Mailboxes](#) for more information.

- 9 The default scope of coverage is displayed in the **Scope** cell. You can change this by placing your cursor in the **Scope** cell, clicking the arrow control and selecting the appropriate option from the list:
 - Object - to audit an individual object
 - One Level - to audit an object and its direct child objects
 - Subtree - to audit an object and all its subordinate objects (all levels)

To exclude an Exchange Mailbox from the auditing process:

- 1 Open the Administration Tasks tab.
- 2 Click **Auditing**.
- 3 Select **Exchange Mailbox** (under Applications in the Auditing task list) to open the Exchange Mailbox Auditing page.
- 4 Expand **Add** and click **Exclude** to display the Exchange Auditing Wizard.
- 5 Select one of the options at the top of the page: **Enterprise** or **This Object** (default).
- 6 If the **This Object** option is selected, use the Browse and Search pages to locate and select a directory object (for example User, Group, Container, DomainDNS, OrganizationalUnit, or BuiltinDomain) and click **Add** to add the selected directory object to the Selected Object list at the bottom of the page.

If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.

Repeat this step to add more directory objects to the exclusion list.
- 7 Click **Finish** to close this wizard and return to the Exchange Mailbox Auditing page, where your selections are listed with a **Yes** in the **Exclude** cell.

i | **NOTE:** From the Exchange Mailbox Auditing page, you can exclude a previously included mailbox by changing the setting in the **Exclude** cell. Place your cursor in the **Exclude** cell of the mailbox to include, click the arrow control, and select **Yes**.

For example, if you wanted to audit all mailboxes in the Enterprise, except those belonging to the accounts in the ExchangeAdmin organizational unit, you would create two entries in the Exchange Mailbox Auditing list:

- Use **Add** to create an audit entry for the **Enterprise** with **Exclude = No**.
- Use **Add | Exclude** to create an audit entry for the **ExchangeAdmin OU** with **Exclude = Yes**.)

To disable an audit entry:

The disable feature allows you to temporarily disable the audit entry of a directory object without having to remove it from the Exchange Mailbox Auditing list.

- 1 On the Exchange Mailbox Auditing page, place your cursor in the **Status** cell for the Exchange mailbox whose auditing you want to disable, click the arrow control and select **Disabled**
The entry in the **Status** column for the object changes to 'Disabled'.
- 2 To re-enable the auditing of a directory object's mailbox, use the **Enable** option in either the **Status** cell or right-click menu.

To delete an Exchange mailbox from the auditing list:

- 1 On the Exchange Mailbox Auditing page, select the mailbox and click **Delete**.
- 2 A dialog is displayed confirming that you want to delete the Exchange mailbox from the auditing list. Click **Yes**.

Exchange Auditing wizard

The Exchange Auditing wizard is displayed when you select **Add** (or **Add | Exclude**) on the Exchange Mailbox Auditing page. This wizard allows you to locate and select directory objects (such as User, Group, Container, DomainDNS, OrganizationalUnit, or BuiltinDomain) to add to the Exchange Mailbox Auditing list. Depending on the commands used (**Add** vs. **Add | Exclude**) you will either be selecting directory objects whose Exchange mailboxes are to be included or excluded from the auditing process.

The following table provides a description of the fields and controls in the Exchange Mailbox Auditing wizard.

Table 2. Exchange Auditing wizard

Select an Exchange Mailbox(es) to Audit page: This page opens when you select **Add**. From here, you select the Exchange mailboxes to audit.

NOTE: To audit members of a group, select a security group (not a distribution group, even though distribution groups are included in the list).

Scope	<p>Select one of the following options to define the scope of coverage:</p> <ul style="list-style-type: none"> • Enterprise • This Object <p>When the This Object option is selected the Browse and Search pages are enabled allowing you to select a directory object (such as user, group, container, DomainDNS, OrganizationalUnit, or BuiltinDomain) whose mailbox is to be audited.</p>
Browse page	<p>Displays a hierarchical view of the containers in your environment allowing you to locate and select the directory objects whose Exchange mailbox you want to audit.</p> <p>If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.</p> <p>After you have selected an object, click Add to move the entry to the list at the bottom of the page.</p>

Table 2. Exchange Auditing wizard

Search page	<p>Use the controls at the top of the Search page to search your environment to locate the directory objects whose Exchange mailbox you want to audit.</p> <p>After you have selected an object, click Add to move the entry to the list at the bottom of the page.</p>
Options page	<p>Use this page to modify the search options used to retrieve directory objects.</p> <p>NOTE: For more information about using the Browse, Search or Options pages, see Directory Object Picker in the online help or Change Auditor User Guide.</p>
Selection List	<p>The directory objects selected for mailbox auditing are displayed in the list box located across the bottom of this page. Use the buttons located above this list box to add and remove objects.</p> <ul style="list-style-type: none">• Add - Select an object in the Browse or Search page and then click Add.• Remove - Select an entry in the selection list and then click Remove.
<p>Select An Exchange Mailbox(es) to Exclude From Auditing page: This page opens when you select Add Exclude. From here, you can select the directory objects whose mailboxes are to be excluded from auditing.</p> <p>NOTE: To exclude members of a group, you must select a security group (not a distribution group, even though distribution groups are included in the list).</p>	
Scope	<p>Select one of the following options to define the scope of coverage:</p> <ul style="list-style-type: none">• Enterprise• This Object <p>When the This Object option is selected the Browse and Search pages are enabled allowing you to select a directory object (for example, user, group, container, DomainDNS, OrganizationalUnit, or BuiltinDomain) whose mailbox is to be excluded from being audited.</p>
Browse page	<p>Displays a hierarchical view of the containers in your environment allowing you to locate and select the directory objects whose Exchange mailbox is to be excluded from being audited.</p> <p>If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.</p> <p>Once you have selected an object, click Add to move the entry to the list at the bottom of the page.</p>
Search page	<p>Use the controls at the top of the Search page to search your environment to locate the directory objects whose Exchange mailbox is to be excluded from being audited.</p> <p>Once you have selected an object, click Add to move the entry to the list at the bottom of the page.</p>
Options page	<p>Use this page to modify the search options used to retrieve directory objects.</p> <p>NOTE: For more information about using the Browse, Search or Options pages, see Directory Object Picker in the online help or Change Auditor User Guide.</p>
Excluded Objects List	<p>The directory objects selected for exclusion from Exchange mailbox auditing are displayed in the list box across the bottom of this page. Use the buttons located above this list box to add and remove objects.</p> <ul style="list-style-type: none">• Add - Select an object in the Browse or Search page and then click Add.• Remove - Select an entry in the Excluded Objects list and then click Remove.

Exchange Settings and Event Logging (Agent Configuration Page)

- [Introduction](#)
- [Exchange Folder Open Event setting](#)
- [Exchange event logging](#)

Introduction

From the Agent Configuration page on the Administration Tasks tab you can define how Change Auditor handles duplicate Exchange folder open events and enable and disable event logging for Exchange events.

i | **NOTE:** This setting and event logging apply to the Exchange subsystem and therefore do not apply to Office 365 Exchange Online events, which are part of the Office 365 subsystem.

This section explains how to modify the Exchange setting and enable event logging using the Agent Configuration page. For a description of the dialogs mentioned, see the online help. For more information about agent configurations, see the Change Auditor User Guide.

Exchange Folder Open Event setting

Use the Exchange tab at the top of the Configuration Setup dialog to define how Change Auditor handles duplicate folder open events.

Discard duplicates that occur within *nn* seconds

This setting defines how long to hold Exchange folder open events to determine if duplicates have occurred before they are forwarded to the client. This process is intended to eliminate the folder open events that Outlook or OWA Exchange users get when their inbox is automatically refreshed.

By default, this setting is set to zero indicating that it is turned off and duplicate folder opens are sent. However, you can use the arrow controls to enable this setting and specify the amount of time to hold folder open events to determine if duplicates have occurred. Valid range is 0 - 600 seconds.

To set the duplicate folder open event setting:

- 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 **Configurations**.
- 5 On the Configuration Setup dialog, select an agent configuration from the left-hand pane.
- 6 Open the Exchange tab and set the duplicate folder open event setting as defined above.

- 7 Once you have set this setting, click **OK** to save your selections, close the dialog and return to the Agent Configuration page.
- 8 On the Agent Configuration page, select the agents assigned to the selected configuration and click **Refresh Configuration** to ensure the agents are using the latest 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.
- 9 Exchange event logging

Exchange event logging

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

When event logging for Exchange is enabled in Change Auditor, the following types of Exchange events are sent to the InTrust for Exchange event log:

- ActiveSync events
- Exchange Mailbox events, including non-owner, owner, permission and protection events
 - NOTE:** Only configured Exchange Mailbox activities are sent to the event log.
- Public folder events
- Store mount events
- System events
- Exchange Administrative PowerShell events

See the Change Auditor for Exchange Event Reference Guide for a list of the events that can be sent to this event log.

To enable Exchange 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 **Exchange**.
- 6 Click **OK** to save your selection and close the dialog.

Exchange events, including activities associated with the Exchange Mailboxes included on the Exchange Mailbox Auditing list, will then to be sent to the event log.

Exchange Mailbox Protection

- [Exchange mailbox protection introduction](#)
- [Exchange Mailbox Protection page](#)
- [Exchange Mailbox Protection templates](#)
- [Exchange Protection wizard](#)

Exchange mailbox protection introduction

Using mailbox protection, you can prevent unwanted access on critical mailboxes through an Exchange Mailbox Protection template.

i NOTE:

- Protection is designed to protect a few high-value mailboxes.
- Protection prevents unauthorized users from accessing a protected mailbox through Outlook clients, OWA; it does not prevent access using ActiveSync or permission changes on the mailbox through the Exchange Administration tools.
- You can specify users and groups who *can* access protected mailboxes.
- After monitoring has been enabled or changed, it may take several minutes to complete the configuration process necessary to enable protection on the agent. Protecting a large number of mailboxes slows down the configuration process.
- Agent processing of Exchange auditing and protection configurations may slow down initial user logon access or cause timeouts if many user logins occur at the same time. To avoid this issue, Quest recommends that changes to mailbox auditing or protection configurations be performed during maintenance intervals or other periods of low user mailbox activity.

Before the system is returned to normal load, one user should log in to Outlook Web Access (OWA), and Outlook clients. This triggers the agent to process the Exchange Mailbox auditing and protection configuration changes when the fewest login are occurring.

This section provides instructions for creating Exchange Mailbox Protection templates, and a description of the Exchange Mailbox Protection page and Exchange Mailbox Protection wizard. For a description of the dialogs mentioned in this section, see the online help.

Exchange Mailbox Protection page

The Exchange Mailbox Protection page displays when you select **Exchange Mailbox** from the Protection task list in the navigation pane of the Administration Tasks tab. From this page you can start the Exchange Mailbox

Protection wizard to define the mailboxes to protect from unauthorized access. You can also edit existing templates, disable a template, and remove templates that are no longer being used.

i | **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, refer to the Change Auditor User Guide for more information on how to gain access.

The Exchange Mailbox Protection page contains an expandable view of all previously defined Exchange Mailbox Protection templates. To add a template to this list, click **Add**. Once added, the following information is provided for each template:

Template

Displays the name assigned to the template when it was created.

Status

Indicates whether the template is enabled or disabled. To enable/disable the template, place your cursor in this **Status** cell, click the arrow control and select the appropriate option from the drop-down menu.

Override Accounts

Indicates whether the override accounts listed are excluded from protection or included in protection. This setting corresponds to the option used at the top of the last page of the Exchange Protection wizard:

- Excluded from Protection - indicates that you selected the **Allow** option to allow only the selected accounts to access the protected objects.
- Included in Protection — indicates that you selected the **Deny** option to allow all accounts to access the protected objects EXCEPT for those selected.

Owner Override

Indicates whether the **Mailbox owner can bypass protection** check box was selected and mailbox owners are allowed to access their own mailboxes.

Mailboxes

This field is used for filtering data.

Override Account Filter

This field is used for filtering data.

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

Exchange Mailbox

Displays the canonical name of the Exchange Mailbox or directory object included in the protection template.

Status

Indicates whether the protection for the mailbox is enabled or disabled.

Name

If applicable, this column shows the display name assigned to the directory object.

Override Account

Displays any accounts that are allowed (or not allowed) to access the protected mailboxes, as specified on the last page of the wizard.

i | **NOTE:** This field is not displayed when there are no override accounts specified in the Exchange Protection wizard.

i | **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 will redisplay the templates that meet the search criteria (i.e., comparison operator and characters entered). For more details about using the data filtering function provided throughout the client, see the Change Auditor User Guide.

Exchange Mailbox Protection templates

To enable protection, you must first create one or more Exchange Mailbox Protection templates which specify whose mailboxes to lock down. Once Exchange Mailbox Protection templates are defined, they will apply to all Exchange servers that host a Change Auditor agent.

i | **NOTE:** If you are planning to use multiple Exchange Mailbox Protection templates, see the Change Auditor Technical Insight Guide for information on how multiple protection templates are evaluated.

i | **NOTE:** You can also open the protection wizard from the event details pane. Simply open the Search Results tab, select an event, and click the Protect Object button.

To create a protection template:

- 1 Open the Administration Tasks tab.
- 2 Click **Protection**.
- 3 Select **Exchange Mailbox** in the Protection task list to open the Exchange Mailbox Protection page.
- 4 Click **Add** to start the Exchange Protection wizard which steps you through the process of defining the mailboxes to protect.
- 5 Use the Browse and Search pages to locate and select a directory object (i.e., User, Group, Container, DomainDNS, OrganizationalUnit, or BuiltinDomain) and click **Add** to add the selected object to the Selected Object list. Repeat this step to add additional directory objects to the template.

If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.

- 6 On the next page of the wizard, use the Browse or Search page to optionally select user or group accounts which will be allowed to access the protected objects selected on the previous page.

If required, use the Forest drop-down box to select in which forest the objects reside. (Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.)

Click **Add** to add the selected user or group to the Account list.

i | **NOTE:** The **Allow** option is selected by default indicating that the selected users or groups are allowed to access the protected objects. However, you can select the **Deny** option to select individual users or groups that are not allowed to access the protected objects. When using the **Deny** option, you are allowing all users and groups to access the protected objects except for those selected on this page.

To allow mailbox owners to bypass protection and be able to access their own mailboxes, select the **Mailbox owner can bypass protection** check box at the top of this page.

- 7 Click **Finish** to create the template, close the wizard, and return to the Exchange Mailbox Protection page, where the newly created template is listed.

To modify a template:

- 1 On the Exchange Mailbox Protection page, select the template to modify and click **Edit**.
This displays the Exchange Mailbox Protection wizard, where you can modify the directory objects whose mailboxes to protect.
- 2 Click **Finish**.

To disable a template:

The disable feature allows you to temporarily stop protecting the specified mailboxes without having to remove the protection template or individual mailbox from an active template.

- 1 On the Exchange Mailbox Protection page, place your cursor in the **Status** cell for the template to be disabled, click the arrow control and select **Disabled**.
The entry in the **Status** column for the template will change to 'Disabled'.
- 2 To re-enable the protection template, use the **Enable** option in either the **Status** cell or right-click menu.

To disable the protection of a mailbox:

- 1 On the Exchange Mailbox Protection page, place your cursor in the **Status** cell for the mailbox whose protection is to be disabled, click the arrow control and select **Disabled**.
The entry in the **Status** column for the selected mailbox will change to 'Disabled'.
- 2 To re-enable protection for the mailbox, use the **Enable** option in either the **Status** cell or right-click menu.

To delete a template:

- 1 On the Exchange Mailbox Protection 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 an individual mailbox from a template:

- 1 On the Exchange Mailbox Protection page, select the mailbox and click **Delete | Delete Exchange Mailbox**.
- 2 A dialog is displayed confirming that you want to delete the selected mailbox from the template. Click **Yes**.

i | **NOTE:** If the mailbox is the last one in the template, deleting this mailbox will also delete the template.

Exchange Protection wizard

The Exchange Protection wizard displays when you click **Add** on the Exchange Mailbox Protection page. This wizard steps you through the process of defining the mailbox to protect from unauthorized access.

i | **NOTE:** You can also open the protection wizard from the event details pane. Simply open the Search Results tab, select an event, and click the Protect Object button.

The following table provides a description of the fields and controls in the Exchange Protection wizard:

i | **NOTE:** A red flashing icon indicates that you have not yet entered the required information. Hovering your cursor over this icon displays a tool tip explaining what needs to be entered.

Table 3. Exchange Protection wizard

Create or modify an Exchange Mailbox Protection Template page:

Use this page to enter a name for the template and select one or more Exchange mailboxes to be protected.

Table 3. Exchange Protection wizard

Template Name	Enter a descriptive name for the template being created.
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the directory objects whose mailbox is to be protected from unauthorized access. Once you have selected a directory object, click Add to add it to the list at the bottom of the page.
Search page	Use the controls at the top of the Search page to search your environment to locate the directory objects whose mailbox is to be protected. Once you have selected a directory object, click Add to add it to the list at the bottom of the page.
Options page	Use the Options page to modify the search options used to retrieve directory objects.
<p>NOTE: For more information about using the Browse, Search or Options pages, see to Directory Object Picker in the online help or Change Auditor User Guide.</p>	
Exchange Mailbox list	The Exchange mailboxes selected for protection are displayed in the list box at the bottom of the page. Use the buttons located above this list box to add and remove mailboxes. <ul style="list-style-type: none"> • Add - Select a directory object in the Browse or Search page and then click Add. • Remove - Select an entry in the Exchange Mailbox list and then click Remove. • Enterprise - Click Enterprise to protect all mailboxes in the Enterprise from unauthorized access.
<p>(Optional) Select Accounts Allowed (not Allowed) to Access Protected Objects page</p> <p>Use this page to optionally select user or group accounts that are allowed (not allowed) to access the selected protected mailboxes.</p>	
Allow	The Allow option is selected by default indicating that the users and group selected on this page will be the only accounts allowed to access the protected objects. Use the Browse or Search page to select the user or group accounts.
Deny	Select the Deny option to allow all users and groups to access the protected objects except for those selected on this page. Use the Browse or Search page to select the user or group accounts.
Mailbox owner can bypass protection	Select this check box to allow mailbox owners to bypass protection and access their own mailboxes even though they are not explicitly added to the Override Account list.
Browse page	Displays a hierarchical view of the containers in your environment allowing you to locate and select the users or groups that will be allowed (not allowed) to access the protected mailboxes. Once you have selected an account, click Add to add it to the list at the bottom of the page.
Search page	Use the controls at the top of the Search page to search your environment to locate the users or groups that will be allowed (not allowed) to access the protected mailboxes. Once you have selected an account, click Add to add it to the list at the bottom of the page.
Options page	Use the Options page to modify the search options used to retrieve directory objects.

Table 3. Exchange Protection wizard

NOTE: For more information on using the Browse, Search or Options pages, refer to Directory Object Picker in the online help or Change Auditor User Guide.

Override Account list	<p>The list box at the bottom of this page contains the user and group accounts selected above. Use the buttons located above this list box to add and remove accounts.</p> <ul style="list-style-type: none">• Add - Select an account in the Browse or Search page and then click Add.• Remove - Select an entry in the Override Account list and then click Remove.
-----------------------	---

Managing Shared Mailboxes

Change Auditor for Exchange generates shared mailbox events for shared mailbox, room and equipment resources, and for any other mailboxes identified as shared. Shared mailbox events are generated only when both of the following conditions exist:

- The affected mailbox is selected for auditing (i.e., added to the Exchange Mailbox Auditing list on the Administration Tasks tab).
- The mailbox is either located in an Exchange mailbox store or has been marked as a shared mailbox by the user.

i **NOTE:** As with individual mailboxes, if the shared mailbox is not added to the Exchange Mailbox Auditing list, the mailbox is not being audited and no events are generated.

If the mailbox is not a shared mailbox, room or equipment resource in an Exchange mailbox store and it has not been manually marked as a shared mailbox by the user, then normal mailbox owner or non-owner events will be generated for the affected mailboxes.

Many of the shared mailbox events are disabled by default. In order to generate these events, they must first be enabled using the Audit Events page on the Administration Tasks tab.

Use the [Exchange Mailbox Auditing page](#) on the Administration Tasks tab to ensure shared mailboxes are set up correctly for auditing. From this page, you can:

- View a list of shared mailboxes that have been automatically detected in the network. By default, this list is filtered to display only the shared mailboxes selected for auditing.
- Mark normal mailboxes as 'shared' by manually adding them to the shared mailbox list.

To view list of shared mailboxes in the auditing list:

Automatic shared mailbox detection locates shared mail, equipment and room mailboxes in the network.

- 1 Open the Administration Tasks tab.
- 2 Click **Auditing**.
- 3 Select **Exchange Mailboxes** under the Applications heading in the Auditing task list.
- 4 At the top of the Exchange Mailbox Auditing page, click **Shared Mailboxes**.
- 5 If not already displayed, open the **Auto Detected** page.

The Auto Detected page displays a read-only list of the shared mailboxes detected in the network.

The **Filter Shared Mailboxes Based on Exchange Auditing Scope** check box is selected by default and only shared mailboxes that are selected for auditing are displayed. To display all shared mailboxes detected in the network, clear this check box.

- 6 Click **Close** to return to the Exchange Mailbox Auditing page.

i **NOTE:** If you have not yet added the shared mailboxes to the Exchange Mailbox Auditing list, click **Add** on the Exchange Mailbox Auditing page to locate and add the mailboxes to audit.

To add mailboxes to shared mailbox list:

Any mailbox can be marked as a shared mailbox by manually adding it to the shared mailbox list.

- 1 Open the Administration Tasks tab.

- 2 Click **Auditing**.
 - 3 Select **Exchange Mailboxes** under the Applications heading in the Auditing task list.
 - 4 At the top of the Exchange Mailbox Auditing page, click **Shared Mailboxes**.
 - 5 Open the **User Defined** page on the Shared Mailboxes dialog.
 - 6 Click **Add**.
 - 7 On the Exchange Shared Mailboxes dialog, use the Browse and Search pages to locate and select a directory object (such as User, Group, Container, DomainDNS, OrganizationalUnit, or BuiltinDomain) and click **Add** to add the selected object to the Selected Object list.

If required, use the Forest drop-down box to select in which forest the objects reside. Foreign agent forests may require foreign forests credentials which can be entered on the Credentials Required dialog.

Repeat this step to add additional directory objects to the Exchange Shared Mailbox list.
 - 8 Click **Finish** to return to the Shared Mailboxes dialog, where your selections will now be listed on the User Defined page of this dialog.
 - 9 The default scope of coverage is displayed in the **Scope** cell. You can change this by placing your cursor in the **Scope** cell, clicking the arrow control and selecting the appropriate option from the list:
 - Object - to audit an individual object
 - One Level - to audit an object and its direct child objects
 - Subtree - to audit an object all of its subordinate objects (all levels)
 - 10 The **Status** field on this page indicates the type of events that are to be generated for the mailbox:
 - Enabled (default) - shared mailbox events are to be generated for the mailbox
 - Disabled - owner or non-owner events are to be generated for the mailbox

To change this setting, place your cursor in the **Status** cell, click the arrow control and select the appropriate option from the list.
 - 11 Click **Close** to save your selections, close the dialog, and return to the Exchange Mailbox Auditing page.
- i** | **NOTE:** If you have not yet added the 'marked' mailboxes to the Exchange Mailbox Auditing list, click **Add** on the Exchange Mailbox Auditing page to locate and add the mailboxes to audit.

Shared Mailbox events

The Exchange Mailbox Monitoring events that can be generated for shared mailboxes include:

- Appointment Copied in Shared Mailbox*
- Appointment Created in Shared Mailbox*
- Appointment Deleted in Shared Mailbox*
- Appointment Modified in Shared Mailbox*
- Appointment Moved in Shared Mailbox*
- Appointment Permanently Deleted in Shared Mailbox*
- Appointment Read in Shared Mailbox*
- Contact Copied in Shared Mailbox*
- Contact Created in Shared Mailbox*
- Contact Deleted in Shared Mailbox*
- Contact Modified in Shared Mailbox*
- Contact Moved in Shared Mailbox*

- Contact Permanently Deleted in Shared Mailbox*
- Contact Read in Shared Mailbox*
- Folder Copied in Shared Mailbox
- Folder Created in Shared Mailbox
- Folder Deleted in Shared Mailbox
- Folder Moved in Shared Mailbox
- Folder Permanently Deleted in Shared Mailbox
- Folder Renamed in Shared Mailbox
- Message Copied in Shared Mailbox*
- Message Created in Shared Mailbox*
- Message Deleted in Shared Mailbox*
- Message Marked Unread in Shared Mailbox*
- Message Modified in Shared Mailbox*
- Message Moved in Shared Mailbox*
- Message Permanently Deleted in Shared Mailbox*
- Message Read in Shared Mailbox*
- Object Copied in Shared Mailbox*
- Object Created in Shared Mailbox*
- Object Deleted in Shared Mailbox*
- Object Marked Unread in Shared Mailbox*
- Object Modified in Shared Mailbox*
- Object Moved in Shared Mailbox*
- Object Permanently Deleted in Shared Mailbox*
- Object Read in Shared Mailbox*
- Shared Mailbox Folder Permissions Changed
- Shared Mailbox Opened*
- Task Copied in Shared Mailbox*
- Task Created in Shared Mailbox*
- Task Deleted in Shared Mailbox*
- Task Modified in Shared Mailbox*
- Task Moved in Shared Mailbox*
- Task Permanently Deleted in Shared Mailbox*
- Task Read in Shared Mailbox*

i | **NOTE:** The events marked with an asterisk (*) are disabled by default. In order to generate any of these events, you must first enable them using the Audit Events page on the Administration Tasks tab.

Disabled Exchange Events

This section provides an alphabetical list of the Exchange Mailbox Monitoring and Exchange ActiveSync Monitoring events that are disabled by default. You must enable these events using the Audit Events page on the Administration Tasks tab before they can be audited.

Table 4. Disabled Exchange events

Event Class disabled by default	Facility
ActiveSync Autodiscover command executed	Exchange ActiveSync Monitoring
ActiveSync Ping command executed	Exchange ActiveSync Monitoring
Appointment Copied by Owner	Exchange Mailbox Monitoring
Appointment Copied in Shared Mailbox	Exchange Mailbox Monitoring
Appointment Created by Owner	Exchange Mailbox Monitoring
Appointment Created in Shared Mailbox	Exchange Mailbox Monitoring
Appointment Deleted by Owner	Exchange Mailbox Monitoring
Appointment Deleted in Shared Mailbox	Exchange Mailbox Monitoring
Appointment Modified by Owner	Exchange Mailbox Monitoring
Appointment Modified in Shared Mailbox	Exchange Mailbox Monitoring
Appointment Moved by Owner	Exchange Mailbox Monitoring
Appointment Moved in Shared Mailbox	Exchange Mailbox Monitoring
Appointment Permanently Deleted by Owner	Exchange Mailbox Monitoring
Appointment Permanently Deleted in Shared Mailbox	Exchange Mailbox Monitoring
Appointment Read by Non-Owner	Exchange Mailbox Monitoring
Appointment Read by Owner	Exchange Mailbox Monitoring
Appointment Read in Shared Mailbox	Exchange Mailbox Monitoring
Calendar Opened by Non-Owner	Exchange Mailbox Monitoring
Calendar Opened by Owner	Exchange Mailbox Monitoring
Contact Copied by Owner	Exchange Mailbox Monitoring
Contact Copied in Shared Mailbox	Exchange Mailbox Monitoring
Contact Created by Owner	Exchange Mailbox Monitoring
Contact Created in Shared Mailbox	Exchange Mailbox Monitoring
Contact Deleted by Owner	Exchange Mailbox Monitoring
Contact Deleted in Shared Mailbox	Exchange Mailbox Monitoring
Contact Modified by Owner	Exchange Mailbox Monitoring
Contact Modified in Shared Mailbox	Exchange Mailbox Monitoring
Contact Moved by Owner	Exchange Mailbox Monitoring
Contact Moved in Shared Mailbox	Exchange Mailbox Monitoring
Contact Permanently Deleted by Owner	Exchange Mailbox Monitoring
Contact Permanently Deleted in Shared Mailbox	Exchange Mailbox Monitoring
Contact Read by Owner	Exchange Mailbox Monitoring

Table 4. Disabled Exchange events

Event Class disabled by default	Facility
Contact Read in Shared Mailbox	Exchange Mailbox Monitoring
Contacts Opened by Owner	Exchange Mailbox Monitoring
Folder Copied by Owner	Exchange Mailbox Monitoring
Folder Created by Owner	Exchange Mailbox Monitoring
Folder Deleted by Owner	Exchange Mailbox Monitoring
Folder Moved by Owner	Exchange Mailbox Monitoring
Folder Permanently Deleted by Owner	Exchange Mailbox Monitoring
Folder Renamed by Owner	Exchange Mailbox Monitoring
Inbox Opened by Owner	Exchange Mailbox Monitoring
Mailbox Opened by Owner	Exchange Mailbox Monitoring
Message Copied by Owner	Exchange Mailbox Monitoring
Message Copied in Shared Mailbox	Exchange Mailbox Monitoring
Message Created by Owner	Exchange Mailbox Monitoring
Message Created in Shared Mailbox	Exchange Mailbox Monitoring
Message Deleted by Owner	Exchange Mailbox Monitoring
Message Deleted in Shared Mailbox	Exchange Mailbox Monitoring
Message Marked Unread by Owner	Exchange Mailbox Monitoring
Message Marked Unread in Shared Mailbox	Exchange Mailbox Monitoring
Message Modified by Owner	Exchange Mailbox Monitoring
Message Modified in Shared Mailbox	Exchange Mailbox Monitoring
Message Moved by Owner	Exchange Mailbox Monitoring
Message Moved in Shared Mailbox	Exchange Mailbox Monitoring
Message Permanently Deleted by Owner	Exchange Mailbox Monitoring
Message Permanently Deleted in Shared Mailbox	Exchange Mailbox Monitoring
Message Read by Owner	Exchange Mailbox Monitoring
Message Read in Shared Mailbox	Exchange Mailbox Monitoring
Object Copied by Owner	Exchange Mailbox Monitoring
Object Copied in Shared Mailbox	Exchange Mailbox Monitoring
Object Created by Owner	Exchange Mailbox Monitoring
Object Created in Shared Mailbox	Exchange Mailbox Monitoring
Object Deleted by Owner	Exchange Mailbox Monitoring
Object Deleted in Shared Mailbox	Exchange Mailbox Monitoring
Object Marked Unread by Owner	Exchange Mailbox Monitoring
Object Marked Unread in Shared Mailbox	Exchange Mailbox Monitoring
Object Modified by Owner	Exchange Mailbox Monitoring
Object Modified in Shared Mailbox	Exchange Mailbox Monitoring
Object Moved by Owner	Exchange Mailbox Monitoring
Object Moved in Shared Mailbox	Exchange Mailbox Monitoring
Object Permanently Deleted by Owner	Exchange Mailbox Monitoring
Object Permanently Deleted in Shared Mailbox	Exchange Mailbox Monitoring
Object Read by Owner	Exchange Mailbox Monitoring
Object Read in Shared Mailbox	Exchange Mailbox Monitoring

Table 4. Disabled Exchange events

Event Class disabled by default	Facility
Shared Mailbox Opened	Exchange Mailbox Monitoring
Task Copied by Owner	Exchange Mailbox Monitoring
Task Copied in Shared Mailbox	Exchange Mailbox Monitoring
Task Created by Owner	Exchange Mailbox Monitoring
Task Created in Shared Mailbox	Exchange Mailbox Monitoring
Task Deleted by Owner	Exchange Mailbox Monitoring
Task Deleted in Shared Mailbox	Exchange Mailbox Monitoring
Task Modified by Owner	Exchange Mailbox Monitoring
Task Modified in Shared Mailbox	Exchange Mailbox Monitoring
Task Moved by Owner	Exchange Mailbox Monitoring
Task Moved in Shared Mailbox	Exchange Mailbox Monitoring
Task Permanently Deleted by Owner	Exchange Mailbox Monitoring
Task Permanently Deleted in Shared Mailbox	Exchange Mailbox Monitoring
Task Read by Owner	Exchange Mailbox Monitoring
Task Read in Shared Mailbox	Exchange Mailbox Monitoring
Tasks Opened by Owner	Exchange Mailbox Monitoring

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Our brand, our vision. Together.

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

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.