

Quest® InTrust 11.4.2

Preparing for Auditing Microsoft Exchange Server



© 2020 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (<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, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

InTrust Preparing for Auditing Microsoft Exchange Server

Updated - September 2020

Version - 11.4.2

Contents

Processing Exchange-Related Logs	4
Collecting CA for Exchange Log Data	6
Collecting Exchange Tracking Log Data	7
Further Reading	9
About us	10
Contacting Quest	10
Technical support resources	10

Processing Exchange-Related Logs

Using InTrust, you can collect and report on audit data related to Microsoft Exchange Server.

The following Exchange Server versions are supported:

- 2019
- 2016
- 2013 Service Pack 1
- 2013
- 2010
- 2007

The following logs are supported:

Log	Extent of Support	Details
CA for Exchange log	InTrust supports auditing and SSRS reporting workflow for this type of log out of the box.	This log is written by Change Auditor for Exchange.
Exchange Tracking log	Minor additional InTrust configuration is required, as described in Collecting Exchange Tracking Log Data , and no SSRS reports are provided for this type of log.	There are several types of Tracking log: <ul style="list-style-type: none">• MSGTRK Transport service events.• MSGTRKMA Approvals and rejections used by moderated transport.• MSGTRKMD Information about messages delivered to mailboxes by the Mailbox Transport Delivery service.• MSGTRKMS Information about messages sent from mailboxes by the Mailbox Transport Submission service.

Log

Extent of Support

Details

InTrust can currently gather only MSGTRK logs.

Collecting CA for Exchange Log Data

The CA for Exchange log is made available by Change Auditor for Exchange agents on Exchange servers. InTrust provides a preconfigured workflow for collecting this type of log and reporting on the data.

To work with CA for Exchange log data

1. In InTrust Manager, locate the predefined Exchange-related tasks:
 - Auditing Exchange Servers: Daily Gathering
 - Auditing Exchange Servers: Ad-Hoc Reporting for the Last 24 Hours
 - Auditing Exchange Servers: Daily Reporting
 - Auditing Exchange Servers: Weekly Reporting
2. Make copies of the tasks that best fit your needs. In your new tasks, adjust the settings of the jobs as necessary. For example, you may want to change the set of reports or report delivery method.
3. Configure and enable the schedules of the tasks.
4. Commit your changes.

Collecting Exchange Tracking Log Data

InTrust does not provide a ready-made set of configuration objects for gathering and reporting on Exchange Tracking log data. However, the core components for creating this workflow are available, and only a few configuration steps are required.

To work with Tracking log data

1. In InTrust Manager, create a data source that will represent the Tracking log:
 - a. Right-click **Quest InTrust Manager | Configuration | Data Sources** and select **New Data Source**.
 - b. On the Select Data Source Type step of the New Data Source Wizard, select **Microsoft Exchange Events**.
 - c. Specify the name and optionally a description of the data source and complete the wizard.
2. Adjust the predefined site that contains Exchange servers:
 - a. Open the properties of the **Quest InTrust Manager | Configuration | Sites | Microsoft Windows Network | Auditing Exchange Servers: Exchange Servers** site.
 - b. On the **Objectstab**, specify your Exchange servers.
3. Create a gathering policy that will configure how the Tracking log is handled:
 - a. Right-click **Quest InTrust Manager | Configuration | Gathering | Gathering Policies | Microsoft Windows Network** and select **New Policy**.
 - b. On the Data Sources step of the Add Data Source Wizard specify the data source you have created.
 - c. Follow the remaining steps and configure the data source options as necessary.

4. Set up a task that will specify what to do with Tracking log data:
 - a. Create the task. For that, right-click **Quest InTrust Manager | Workflow| Tasks** and select **New Task** and complete the steps.
 - b. Right-click the newly-created task and select **New Job**.
 - c. On the Job Type step of the New Job Wizard, select **Gathering**.
 - d. On the Select Policy step, select the gathering policy you have created.
 - e. On the Select Site step, select **Auditing Exchange Servers: Exchange Servers**.
 - f. On the Data Stores step, make sure you gather to a repository.
 - g. Complete the steps.
5. Enable the schedule for your task if you haven't already done so.
6. Commit your changes.

The procedure above implements a minimal workflow required to get the Tracking log data into a data store. You can make further improvements to it as necessary: tweak gathering and filtering settings, enable notifications, configure data consolidation and cleanup, and so on.

To analyze the resulting Tracking log data, use Repository Viewer.

Further Reading

If you need more information about InTrust workflows and configuration, refer to the following topics:

- For details about tasks and jobs, see the [Auditing Guide](#).
- For details about SSRS-based reporting, see [Leveraging Microsoft SQL Server Reporting Services Integration for Advanced Reporting](#).
- For details about analyzing gathered events in InTrust repositories, see [Searching for Events in Repository Viewer](#), [Reporting on Events Using Repository Viewer](#) and the IT Security Search User Guide (available at <https://support.quest.com/it-security-search/technical-documents>).

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.

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