Quest® InTrust 11.3.1

Preparing for Auditing Microsoft Exchange Server

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 2017
Version - 11.3.1

Contents

Processing Exchange-Related Logs

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

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: • 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. 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 **Objects**tab, 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.

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

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