Quest®

Quest® InTrust 11.3

Preparing for Auditing Microsoft Forefront Threat Management

Gateway and ISA Server

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

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 Forefront Threat Management Gateway and ISA Server
Updated - May 2017
Version - 11.3

Contents

Overview of Microsoft TMG and ISA Server Log Auditing

Using InTrust, you can collect and report on audit data from Microsoft Forefront Threat Management Gateway and ISA Server.

The following versions are supported:

- Forefront Threat Management Gateway 2010
- ISA Server 2006
- ISA Server 2004
- ISA Server 2000

For specifics about product version support, see System Requirements.

InTrust allows you to gather event data recorded by Microsoft Internet Security and Acceleration Server (ISAS) to the following audit trails:

- Microsoft Forefront Threat Management Gateway Server Web Proxy Log
- Microsoft Forefront Threat Management Gateway Server Firewall Log
- Microsoft ISA Server Web Proxy Log
- Microsoft ISA Server Firewall Log
- Windows Application Log (events generated by ISAS)
- Windows Security Log (events generated by ISAS)

NOTE: When you collect data for Microsoft Forefront Threat Management Gateway Server, the names of data sources that are displayed in InTrust Repository Viewer and InTrust reports are "Microsoft ISA Server Web Proxy Log" and "Microsoft ISA Server Firewall Log" by design.

InTrust collects Web Proxy and Firewall logs written into the files of the following formats:

- W3C Extended File Format: contains both data and directives describing the version, date, and logged fields. Because the fields are described in the file, unselected fields are not logged. The tab character is used as delimiter. Date and time are in GMT. Logs in this format are collected only from ISA, not from Threat Management Gateway.
- ISA Server file format: contains only data with no directives. All fields are always logged; unselected fields are logged as dash to indicate they are empty. The comma character is used as delimiter. The date and time fields are in local time.

Also, InTrust can collect Web Proxy and Firewall logs data stored in the MSDE database format. When you select to save the logs to an MSDE database, logs are saved in databases named **ISALOG_*yyyymmdd*_*xxx*_*nnn*** where:

- **yyyymmdd** stands for the date the log database refers to (year, month, and day)
- **xxx** represents the type that the log database refers to:
  - **FWS** represents the Firewall log
  - **WEB** represents the Web Proxy log

- **nnn** is a number that distinguishes between log databases that refer to the same day

For each log database, two files are created: **ISALOG_*yyyymmdd_xxx_nnn*.mdf** and **ISALOG_*yyyymmdd_xxx_nnn*.ldf**.

By default, the log information for MSDE logs and for the log files is stored in the ISALogs folder, under the ISA Server installation folder. If you change the location, the actual log folder may be different on every server.

Configuring TMG and ISA Server Logging

To configure logging, for example, of Microsoft ISA Server 2006, carry out the following:

1. In the console tree of ISA Server Management, click **Monitoring**:
    - For ISA Server Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2006**, expand **Arrays**, expand **Array_Name**, and then click **Monitoring**.
    - For ISA Server Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2006**, expand **Server_Name**, and then click **Monitoring**.
2. In the details pane, click the **Logging** tab.
3. On the **Tasks** tab, select the appropriate task:
    - Configure Firewall Logging
    - Configure Web Proxy Logging
4. In the Properties dialog box, specify the logging options you need.

NOTE: To generate the most comprehensive reports, you can configure logging options so as to include all events in log. However, in this case you should consider the log size growth and plan for the log cleanup frequency. Use ISA Server logging options and InTrust gathering options to configure log retention period as you need.

Gathering Microsoft TMG and ISA Server Events with InTrust

1. In InTrust Manager, select **Configuration | Sites | Microsoft Windows Network**, and select the **All TMG and ISA Servers** site.
2. To automatically install agents on the site computers, select **Install Agents** from site's shortcut menu. Agentless gathering peculiarities are described later.
3. Select the **TMG and ISAS Daily Collection** task, or configure a new task you need, with a gathering job involving the necessary gathering policy and site. In the task properties, select the Schedule enabled option.
4. Select the **TMG and ISAS Weekly Reporting** task, or configure a new reporting task you need, and enable its schedule in a similar way.

Gathering Data Using Agents

To minimize impact on the network when communicating data from target computer to InTrust server, agents are recommended for data gathering.

The following rights and permissions must be assigned to the InTrust agent account if the agent is not running under the **LocalSystem** account:

1. **Read** permission to the TMG or ISA server (or server array) configuration.
2. **Read** permission to the **HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation** registry key.
3. **Read** and **List Folder Contents** permissions to log file folders; the **Delete** permission must also be granted if the **Clear log files after gathering** option is turned on for the data source.

> **CAUTION: To collect TMG logs in SQL Server Express format, make sure that the InTrust agent runs under an account that has read access to the log database.**

Gathering Data Without Agents

You can configure InTrust to collect ISA Server 2000 logs without agents.

> **CAUTION: To collect audit data from TMG, ISA Server 2004 and ISA Server 2006, agents are required.**
>
> **However, TMG logs in SQL Server Express format can also be gathered without agents if you do the following:**
>
> - **Allow RPC connections to the Threat Management Gateway server.**
> - **Make the SQL Server instance named "MSFW" on the Threat Management Gateway remotely available.**
> - **Install the Microsoft TMG Management Console on the InTrust server.**

- To work without agents, Microsoft ISA Administrative Components must be installed on the InTrust server.
- On the processed computer, you can use Remote Registry Service, or Microsoft ISA Administrative Components.
- The account under which the gathering service will access site computers (specified explicitly in the site's settings, or inherited from InTrust server or task) requires the following:
    a. **Access this computer from the network** right must be granted.
    b. **Deny** access to this computer from network right must be disabled.
    c. Membership in the local **Administrators** group.
    d. Read permission to the **HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation** registry key.
    e. Read permission to the **HKLM\SYSTEM\CurrentControlSet\Control\NIs\Language** registry key.
    f. **Read** and **List Folder Contents** permissions to log file folders; the **Delete** permission must also be granted if the **Clear log files after gathering** option is enabled for the data source.

Resolution of IP Addresses

If specified by InTrust settings, IP addresses found in the log are resolved to host names, and InTrust saves them both (IP addresses and host names) into the log, appending them to original fields. This can significantly slow down gathering process; that is why this option is disabled by default. If necessary, you can enable this option in the following way:

1. In InTrust Manager, select **Configuration | Data Sources**.
2. On the right pane, select the ISA Server log you need, for example, Web Proxy Log.
3. From its shortcut menu, select **Properties**, on the **Settings** tab select **Resolve IP addresses to** and specify whether to resolve them into NetBIOS names or DNS names.

InTrust Knowledge Pack for Microsoft ISAS/Proxy Server

The Knowledge Pack for Microsoft ISAS/Proxy Server offers a set of predefined InTrust objects that will help you configure the gathering and monitoring of event data from your Microsoft TMG/ISA/Proxy Servers. The following objects are included:

- Gathering policies:
  - TMG and ISAS: Security
    Collects all TMG and ISAS security events to both a repository and a database.
  - TMG and ISAS: Health
    Collects all TMG and ISAS health events both to a repository and a database.
  - TMG and ISAS: Usage: Proxy
    Collects TMG and ISAS Web Proxy log both to a repository and a database.
  - TMG and ISAS: Usage: Firewall
    Collects TMG and ISAS Firewall log both to a repository and a database.
- Import policies:
  - TMG and ISAS: Security
    Imports all TMG and ISAS security events to a database.
  - TMG and ISAS: Health
    Imports all TMG and ISAS health events to a database.
  - TMG and ISAS: Usage: Proxy
    Imports events from TMG and ISAS Web Proxy log to a database.
  - TMG and ISAS: Usage: Firewall
    Imports events from TMG and ISAS Firewall log to a database.
- Jobs:
  - TMG and ISAS Security events collection
    Collection of all the TMG and ISAS security events to the default repository and the default database.
  - Weekly TMG and ISAS Web Proxy Reporting
    Weekly reporting of TMG and ISAS Web Proxy usage.
  - Weekly TMG and ISAS Firewall Reporting
    Weekly reporting of TMG and ISAS Firewall usage.
- Tasks:
  - TMG and ISAS Daily collection
    Daily collection of all the TMG and ISAS security events to the default repository and the default database.
  - TMG and ISAS Weekly Reporting
    Weekly reporting of TMG and ISAS Statistics and the most critical events.
- “All TMG and ISA servers” site

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 https://www.quest.com/company/contact-us.aspx or call +1-949-754-8000.

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