Quest

Quest® InTrust 11.4.2

Integration into SIEM Solutions Through Event Forwarding

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 Integration into SIEM Solutions Through Event Forwarding
Updated - September 2020
Version - 11.4.2

Contents

Integration into SIEM Solutions Through Syslog Forwarding

Events that arrive in a repository can be passed on to SIEM systems that know how to receive, store and index them for analysis. This is known as audit data forwarding and is configured on a per-repository basis.

Turning Forwarding On and Off

Forwarding has a dedicated group of settings in the properties of a repository. Use the **Enable forwarding** option to turn it on and off for the repository you are working with, and click **Apply** to confirm your changes.

From the moment you turn forwarding on, events that arrive in the repository during real-time collection will be forwarded. Events that were already in the repository will be ignored. A status line in the forwarding properties shows you statistical information about the forwarding activities for the repository (see also How Event Forwarding Statistics Can Help You).

NOTES:

- Forwarding does not work for events that are gathered to repositories by InTrust gathering jobs as part of the workflow described in the Auditing Guide.
- If you want to forward events from a repository, make sure the repository name is no longer than 127 characters. Rename the repository if necessary.
- When you turn forwarding off, the effect is immediate. If the forwarding queue is not empty at the time this happens, it will remain like that while forwarding stays disabled. When the events in the queue become older than the retention period, they will be cleared.
- When you turn forwarding back on, any existing events in the forwarding queue are sent first; this mean your forwarding may begin with old events.
- In forwarded events, the **When** field contains GMT timestamps. Therefore, when you view the forwarded events on the receiving end (for example, in Splunk), the timestamps will be different from the results in Repository Viewer (which converts the value of **When** to local time automatically).

For details about repository options, see Managing Repositories.

CAUTION: Do not forward events to an InTrust server that listens for Syslog messages, because the messages will arrive with incorrect timestamps.

The following options control how forwarding is performed:

- **Destination host**
  The host that listens for forwarded messages.
- **Transport**
  Which transport you want to use:
  - UDP (can be faster, but reception is not verified)
  - TCP (can be slower, but verifies reception)
  - TLS-secured TCP (the most secure option, but works only in environments using TLS)
- **Port**
  The port that the destination host uses for listening.
- **Message encoding**
  The Splunk JSON and Syslog RFC 5424 formats use UTF-8. For other formats, you can select the encoding.
- **Message filtering**
  If you need only a subset of the repository data, you can specify filters, which are really Repository Viewer searches. If you want to add or modify a filter, open Repository Viewer and make your changes. Your filter will be available the next time you configure forwarding. For details about working with searches, see Searching for Events in Repository Viewer. Using searches as filters has some important implications; see Event Filtering for details.
- **Message format**
  The format in which data is expected on the receiving end; see Data Conversion Formats for details. This setting has no effect on data that arrives from Syslog devices; such data is forwarded unchanged. Only collected Windows event log data is converted to the specified format.

Data Conversion Formats

SIEM appliances expect data in a specific format. For forwarding to be useful, InTrust must convert the contents of the repository to that format before passing them on.

The following output formats are supported:

- Dell SecureWorks
  This is synonymous with the Snare format, transferred over Syslog.
- IBM QRadar
- Tibco LogLogic
- Splunk JSON
  The JSON is transferred over Syslog.
- Syslog RFC 5424
  This message format is supported by multiple SIEM systems alongside their proprietary formats.

NOTE: When InTrust forwards data in RFC 5424 format, it includes IANA private enterprise number 3973 (registered to Quest Software Inc.) in the messages.

See the following topics for details about setting up integration with specific systems:

- Example: Set Up Forwarding to SecureWorks
- Example: Set Up Forwarding to Splunk

You can add support for other formats by providing custom format definition scripts.

To specify a different format, select the **Custom Format** item in the **Message format** drop-down list, click **Edit**, and use the editor that opens.

Note the following specifics:

1. Your custom formatting code must implement the **Transform()** function. This function will be used as the entry point by the event forwarding engine. It takes an event object and its sequential number as arguments, and it returns a string.
2. The custom message format will be applied only to the repository you are working with, and will not be replicated to other repositories.
3. Switching from the custom format to the predefined format resets the custom format script to its default state. Back up your custom format script in a file.
4. A custom format script has significantly lower performance than an equivalent built-in predefined formatter. For example, the default format script, provided as the template for custom format scripts, forwards events at only about 1/30th the rate of the predefined Dell SecureWorks formatter.

For more details about formatting custom messages, study the default formatting script provided in the built-in editor. This is a valid script that replicates the functionality of the predefined SecureWorks forwarding component in InTrust. To change the message format, either edit the **Format** variable or write your own custom script using this default script as an example. In the **Format** string, event field names enclosed in percent signs (**%**) will be replaced by their values.

For details about event objects and the InTrust object model in general, see Customization Kit.

Recommended Event Forwarding Scenario

For best results, consider using a dedicated repository for event forwarding. You can create the repository in advance in the Storage view of InTrust Deployment Manager. Alternatively, you can select to create a new repository when you create your new forwarding-oriented collection in the Collections view.

To make sure your repository doesn't waste disk space, set up daily cleanup for it. Cleanup is configured in the repository properties in the Storage view.

Event Filtering

You can select one or more filters for forwarding your repository contents. InTrust will forward events that match any of the filters you select. Remember that each filter you add broadens the scope instead of narrowing it.

To manage the set of filters, click the button next to the list of current filters. In the filter browser that opens, select the check boxes next to the filters you need. Avoid selecting more than just a few filters, because that can adversely affect performance. A better approach is to create a dedicated Repository Viewer search with the right options.

Also note the following details:

- Searches that are currently used for event filtering are marked with special icons to help prevent accidental modification. In addition, if you try to edit such a search, you are prompted to confirm this. Deleting a filtering search (or a search folder that contains it) is disallowed. Scheduling reports on filtering searches is also disallowed.
- If you want to create a forwarding filter from a regular search or from another filter, it is convenient to right-click the search and select **Make a Copy**. This way, you avoid the risk of making unwanted changes to the original search.
- Repository Viewer searches support grouping and sorting, but these settings have no meaning for message forwarding and will be ignored.
- If you edit a search that is already used as a filter, your changes will affect the filtering. Consider making dedicated searches for filtering purposes.
- If a filtering search is deleted, forwarding configuration becomes invalid for the repositories that used it, and forwarding stops for these repositories. This is a deliberate design choice to prevent incomplete data from being forwarded. The deleted filter is listed as invalid for the repositories. To resolve this situation:
    - In the list of repositories, look for repositories that are marked with an exclamation mark icon.
    - For each affected repository, remove the invalid filter from the filter list. If necessary, you can still view the location that the search used to be at. For that, open the filter browser.
- If you use predefined searches as a filters, note that changes made to them in Repository Viewer are not applied.
- Be careful when specifying the time range for the searches that will be used as filters. If you set the wrong type of range, this can effectively turn off message forwarding. For example, if you set a time range based on the “Last” keyword, no matches will ever occur. You should not specify a time range for a filtering search.

Choosing Event Filters

Generally, you don't want to forward all the data that you collect. If you are targeting a SIEM system, you are likely to concentrate on specific activities to reduce costs and level of noise and make threat hunting and security analysis as efficient as possible.

For these exact purposes, InTrust provides a set of Repository Viewer searches designed to work as event forwarding filters (they are in fact better used as filters). They are available in the **Threat Hunting | Windows | Native OS Logs Telemetry** search folder. These filters accommodate knowledge from important sources such as the following:

- MITRE recommendations
  https://github.com/MalwareArchaeology/ATTACK
- NSA recommendations
  https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Events
- Ultimate Windows Security website
  https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/

You can combine these filters as you see fit or select all of them to fully cover your infrastructure security while still retaining focus.

NOTE: Some of these filters rely on logs that may not be readily available on your systems, such as WMI or Task Scheduler logs. If you use any of such filters, make sure the necessary audit data is collected. For details about selecting what to collect, see Collecting Events in Real Time.

Example: Set Up Forwarding to SecureWorks

Suppose SecureWorks is already in place in your environment and is used for tracking the operation of Syslog-enabled systems. For Windows network auditing, you use InTrust and Change Auditor. You would like to extend the scope of your SecureWorks coverage to include suspicious user activity in the Windows network.

Make Sure You Have the Data

To capture suspicious administrative activity, you would need to look at the following:

- User session events provided by InTrust
  These events provide a deep insight into user logons, logoffs and sessions.
- Change Auditor for Active Directory log
  This log provides fine-grained information about all changes to Active Directory.

Confirm that these data sources are used by the collections that work with your repository.

Configure the Forwarding

You need to enable forwarding for the repository that you have chosen for this purpose. Go to the properties of the repository and, on the **Forwarding** tab, select **Enable forwarding** and specify where the messages should go.

After you have completed the collection setup, confirm that the forwarding is really working. Wait a few minutes for the new settings to take effect. After that, log on to some of the computers that InTrust is watching, and try to make Active Directory changes. Then check on the SecureWorks appliance whether it has registered your activity.

Example: Set Up Forwarding to Splunk

Suppose Splunk is deployed in your environment for analyzing Windows security events. You would like to use InTrust as the forwarding mechanism. The data you need goes to a repository that is set aside specifically for forwarding purposes. The repository has only Windows Security log data.

IMPORTANT: When Splunk parses messages that contain escape sequences, it may truncate the values of discovered fields. The truncation occurs at these escape sequences. As a result, the field values that Splunk displays can differ from the original data. This doesn't affect searching.

Get Splunk Ready

You need to perform some preparatory procedures in Splunk. An example of the configuration is described below, but it may differ for your Splunk deployment.

Step 1: Define a Source Type

To make sure that event fields are recognized correctly, make a specialized source type for incoming InTrust data. If you want to use the Splunk UI for this, configure the options as follows (the last three options are set up in the **Advanced** group):

Option	Value
Category	Structured
Indexed extractions	json
NO_BINARY_CHECK	true
SHOULD_LINEMERGE	false
pulldown_type	1

If you want to skip configuration through the Splunk UI, include the following snippet in the ***<Splunk_installation_folder>*\etc\apps\search\local\props.conf** file:

```
[InTrust]
DATETIME_CONFIG =
INDEXED_EXTRACTIONS = json
NO_BINARY_CHECK = true
SHOULD_LINEMERGE = false
category = Structured
pulldown_type = 1
```

Step 2: Configure a Network Input

In Splunk, add a new TCP or UDP network input and apply your new source type to it. Configure the network input as necessary, but make sure you set up the following:

1. The protocol must match the one specified in your forwarding configuration: either TCP or UDP.
2. Specify the source type you defined earlier; in this example, it is **InTrust**.

Make a note of the port number where Splunk will listen for forwarded traffic. You are going to need it for InTrust forwarding configuration.

If you want to skip configuration through the Splunk UI, include a snippet like the following in the ***<Splunk_installation_folder>*\etc\apps\search\local\inputs.conf** file:

```
[tcp://514]
connection_host = ip
index = main
sourcetype = InTrust
```

If you are forwarding events over UDP, the first line in the snippet above should be `[udp://514]`.

For details about the various ways that you can add network inputs in Splunk, see the "Get data from TCP and UDP ports" article in the documentation of your version of Splunk.

Step 3 (Conditional): Restart Splunk

If you made your changes by editing configuration files, restart Splunk to apply them; use either the **splunk stop** and **splunk start** commands or the **Restart** action in the Splunk UI. For details, see the Splunk documentation.

Configure the Forwarding

To send data to Splunk, enable forwarding for the repository with the necessary data. Go to the properties of the repository and, on the **Forwarding** tab, select **Enable forwarding** and specify where the data should go.

Select **Splunk JSON** as the message format, and specify the correct Splunk host name and the port where the forwarded data is expected.

After you have completed the collection setup, confirm that the forwarding is really working. Wait a few minutes for the new settings to take effect. After that, log on to some of the computers that InTrust is watching, and try to make Active Directory changes. Then open Splunk and check whether your activity has registered.

Example: Mirroring InTrust Real-Time Alerts in SIEM

InTrust real-time alerts, which are produced by real-time monitoring rules, cannot be directly transferred to a SIEM system. However, InTrust provides a way to get real-time alert data in event log form, which is compliant with SIEM technology. What you need to do is make your rules use **Event Log Recipient** as their notification destination, as described in Configuring Notification Groups and Recipients.

After you have set up event log-based notification as instructed in that topic, take the following steps in InTrust Deployment Manager:

1. Create a collection that includes all of your InTrust servers, because generally there is no telling which server processes which rules (unless you have a strict convention about this).
2. Select only the **InTrust Server Log** data source for the collection.
3. Enable event forwarding for the repository you use for the collection.
4. Apply the **InTrust Alerts | Alert triggered** forwarding filter. This filter skips everything except event ID 17408, which is the rule match event.

When you are done, your SIEM solution will receive the equivalent of InTrust real-time alerts, with all the benefits of InTrust event correlation and none of the event log noise.

How Event Forwarding Statistics Can Help You

The event forwarding engine provides the following performance counters on the InTrust server where it runs:

- Forwarded Events
- Forwarded Events/sec
- Processed Events
- Processed Events/sec
- Forwarded Bytes
- Forwarded Bytes/sec

By analyzing these counters in the Performance Monitor, you can diagnose event forwarding problems and tailor your forwarded event traffic to your available bandwidth. See the following examples:

What the counters show	What it might mean
There are roughly as many forwarded events as processed events.	You are forwarding everything, which may not be what you really want. You could reduce SIEM costs by using forwarding filters.
The rate of forwarded bytes per second is very high for the bandwidth you have available.	You can save bandwidth by using forwarding filters.
There seems to be zero forwarding activity according to the counters.	Your current forwarding filters may be too restrictive. Try reconfiguring them.

Fine-Tuning Forwarding with Organization Parameters

InTrust provides several organization parameters as a way to tweak the operation of the event forwarding system. These parameters are organization-wide and affect all InTrust servers in the organization.

For details about where to change the parameters, see Organization Parameter Editor.

Organization parameter	Details
FORWARDING_MAX_SESSION_DURATION_SECONDS	This is the time-to-live of a TCP connection in seconds. By default, there is no limit. The value of this parameter cannot be lower than one-tenth the system TcpTimedWaitDelay value, which is defined manually (as DWORD) in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters** registry key and is assumed to be 120 seconds by default. Therefore, you should not set the value of FORWARDING_MAX_SESSION_DURATION_SECONDS lower than 12.
FORWARDING_SESSION_KEEP_ALIVE_SECONDS	This is the interval in seconds for sending keep-alive packets over an idle TCP connection.
FORWARDING_MESSAGE_FRAMING	Whether to perform non-transparent (**0**) or octet-counting (**1**) message transfer, as detailed in RFC 6578.
FORWARDING_RETENTION_EXPIRATION_PERIOD_SECONDS	How old (in seconds) data must be to be marked for deletion. When data reaches this age, you get a warning in InTrust Deployment Manager. The default value is 86400 (24 hours).
FORWARDING_RETENTION_ENFORCEMENT_PERIOD_SECONDS	How long (in seconds) old data must still be available after it is marked for deletion. When this time elapses, the data is actually deleted. The default value is 86400 (24 hours).

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