Quest®

Quest® InTrust 11.3

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 - May 2017
Version - 11.3

Contents

Integration into SIEM Solutions Through Syslog Forwarding **4**
Turning Forwarding On and Off 4
Filtering Specifics 5
Data Conversion Formats 5
Basic Event Forwarding Scenario 6
Advanced Event Forwarding Scenario 6
Example: Set Up Forwarding to SecureWorks 6
Make Sure You Have the Data 7
Configure the Forwarding 7
Example: Set Up Forwarding to Splunk 7
Get Splunk Ready 7
Step 1: Define a Source Type 7
Step 2: Configure a Network Input 8
Step 3 (Conditional): Restart Splunk 8
Configure the Forwarding 8

About us **10**
Contacting Quest 10
Technical support resources 10

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
- Data Conversion Formats
- Basic Event Forwarding Scenario
- Advanced Event Forwarding Scenario
- Example: Set Up Forwarding to SecureWorks
- Example: Set Up Forwarding to Splunk

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.

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.
- **Port**
  The port that the destination host uses for listening.
- **Message encoding**
  By default, Western European is used.
- **Message filtering**
  If you need only a subset of the repository data, you can specify one of the available filters. These filters are really Repository Viewer search folders. 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 search folders, see Searching for Events in Repository Viewer. Using search folders as filters has some important implications; see Filtering Specifics below 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.

Filtering Specifics

- Repository Viewer search folders support grouping and sorting, but these settings have no meaning for message forwarding and will be ignored.
- If you edit a search folder that is already used as a filter, your changes will affect the filtering. Consider making dedicated search folders for filtering purposes.
- If a filtering search folder is deleted, filtering is turned off for the repository that used it.
- If you use predefined search folders as a filters, note that changes made to them in Repository Viewer are not applied.
- Be careful when specifying the time range for the search folders 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 folder.

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
  For details, see Example: Set Up Forwarding to SecureWorks.
- IBM QRadar
- Tibco LogLogic
- Splunk (JSON)
  For details, see 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.

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.

Basic Event Forwarding Scenario

This scenario applies if both of the following are true for the repository that you want to forward events from:

1. The InTrust server that manages the repository has at least 8 CPU cores.
2. The rate of incoming events is no more than 2,000 per second.

NOTE: If you use custom script-based format conversion, the rate of outgoing events will be considerably lower than with the predefined format.

In this case, all you need to do is enable event forwarding for your existing repository, as described in the Turning Forwarding On and Off topic.

InTrust logs its event forwarding activities and gives you errors if the forwarding queue overflows. If this happens, the event rate is too high, and there will be gaps in the continuity of forwarded events. In that case, you should use the recommendations from the Advanced Event Forwarding Scenario topic.

NOTE: The retention threshold for the event forwarding queue is 48 hours by default. Events that are older than the threshold value are dropped from the queue and cannot be forwarded.

Advanced Event Forwarding Scenario

In this scenario, you use a dedicated repository for event forwarding. Create a new collection specifically for the events you want to forward, and select to create a new repository for this collection.

As a final step, you can make sure that disk space is not wasted on the repository contents that you are not going to use. Set up automatic cleanup of the repository contents. For that, use the InTrust Manager console from an extended InTrust deployment to do the following:

1. Connect InTrust Manager to the organization where your repository resides.
2. Create a task and schedule it to run periodically; for example, every day.
3. Within the task, create a single repository cleanup job that clears everything from the repository used for the forwarding.
4. Commit your configuration changes.

For details about performing these steps, see the Auditing Guide.

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 with the necessary data. 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.

Get Splunk Ready

> **CAUTION: For the sake of speed, the Splunk forwarding component of InTrust uses the UDP protocol, so successful delivery of forwarded data is not guaranteed.**

You need to perform two procedures in Splunk (and maybe restart it), as described below.

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

Option	Value
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 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. It must use the UDP protocol.
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 UDP traffic. You are going to need it for InTrust forwarding configuration.

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

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

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 UDP 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.

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