

RSA NetWitness Platform

Event Source Log Configuration Guide



ThreatQuotient Threat Intelligence Platform

Last Modified: Thursday, February 13, 2020

Event Source Product Information:

Vendor: [ThreatQuotient](#)

Event Source: Threat Intelligence Platform

Versions: 4.0

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Feed Format: csv

Collection Method: HTTP

Feed Collection Frequency: Hourly, Daily, or Weekly

About ThreatQuotient

ThreatQuotient delivers an open and extensible threat intelligence platform (TIP) with Threat Management and Operation characteristics. It provides defenders the context, customization, prioritization and collaboration needed for increased security effectiveness and efficient threat operations and management.

ThreatQ accelerates the transformation of threat data into actionable threat intelligence by giving defenders control through a self-tuning threat library, an adaptive workbench and an open exchange API to ensure that intelligence is accurate, relevant and timely to the business. With ThreatQ, customers can dramatically reduce the time to define and detect, increase productivity, and make the most of the existing defense infrastructure



ThreatQ Architecture Diagram

ThreatQ Configuration

This section provides instructions for configuring the ThreatQuotient Threat Intelligence Platform with RSA NetWitness.

Before You Start

This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components. All ThreatQuotient Threat Intelligence Platform components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

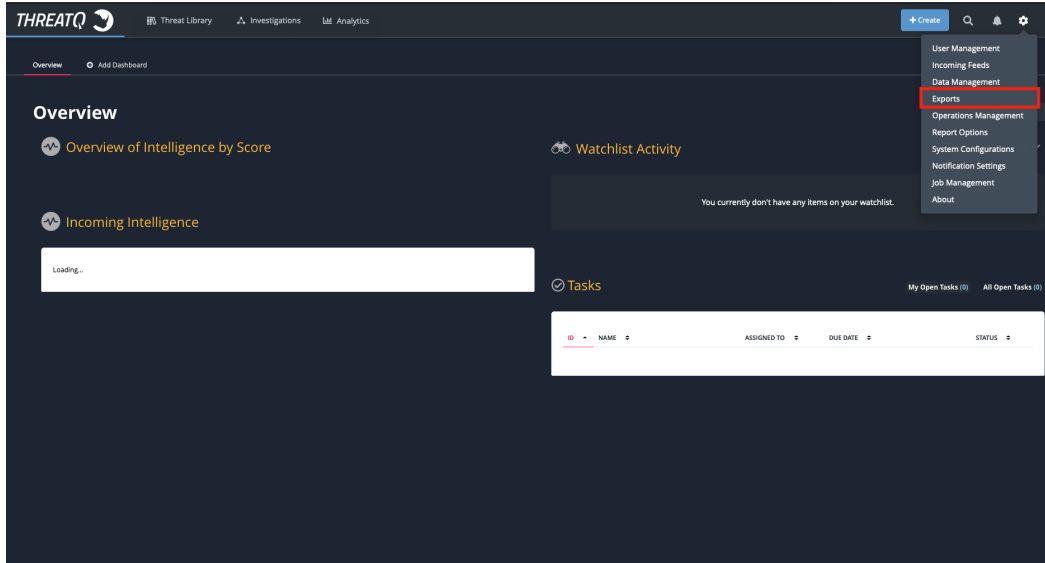
Intelligence Feed	File Function
Feed Contents	IP Address or Domain Name, ThreatQuotient Link, ThreatQuotient ID, Score, ThreatQuotient Status, and Detected Time.

Configure ThreatQuotient

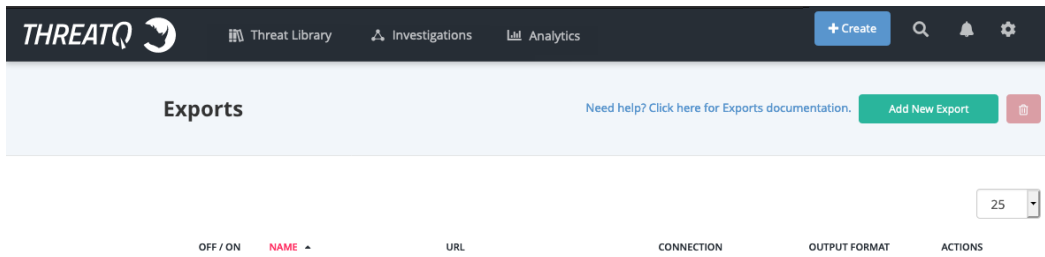
The ThreatQuotient Threat Intelligence Platform allows threat data to be exported in a variety of different ways. This is accomplished by using the **Exports** feature.

To configure the feed for NetWitness Platform, perform these steps:

1. Log into the ThreatQ Platform and navigate to the Exports page as below:



2. From the **Exports** page, click the green **Add New Export** button.

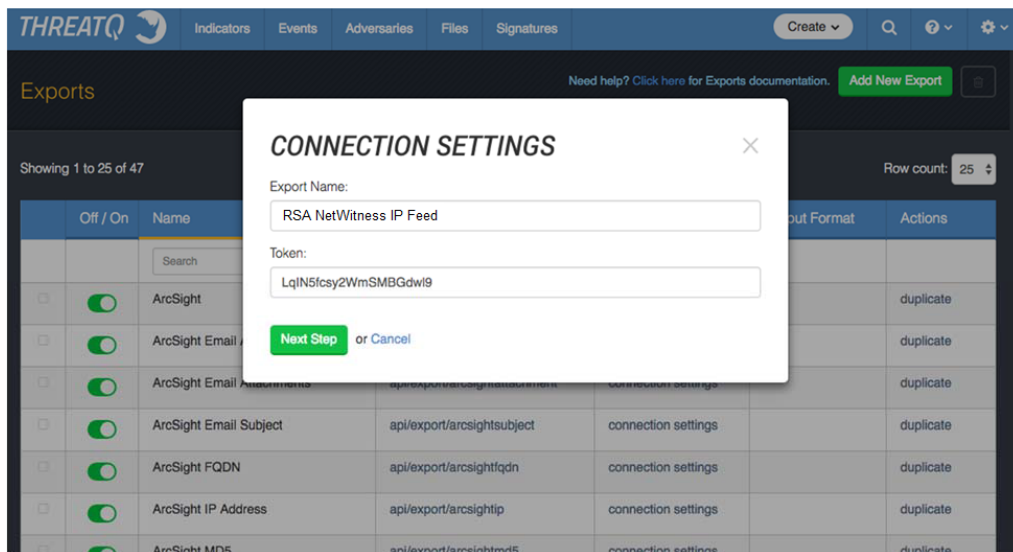


After you click the button, a wizard is launched that takes you through the steps to configure the NetWitness Export.

3. Define Export Name and Token.

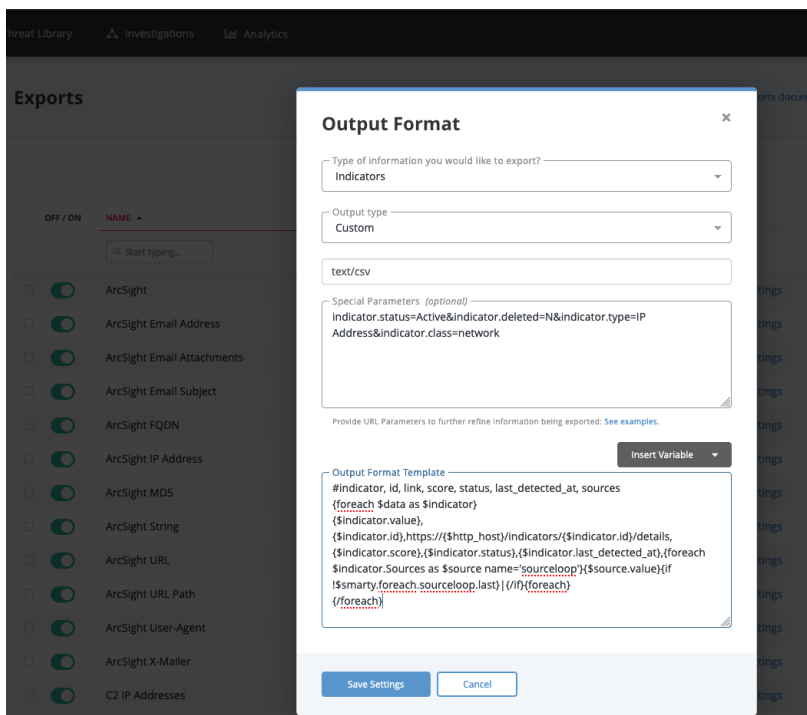
Select a name and token. The name should be short and descriptive, for example, “RSA NetWitness IP Feed.” The token is used to authorize a connection to view the data in this feed. This is randomly generated, and should not be changed.

- a. Enter a name. The name should be short and descriptive, for example, “RSA NetWitness IP Feed.”
- b. The token is used to authorize a connection to view the data in this feed. This is randomly generated, and should not be changed.



4. Click **Next Step** to proceed.
5. Configure Output Format.

The Output Format page allows you to describe the feed in detail. Here, we set the type of information to “Indicators”, the Output Type to “text/csv”, the special parameters and output format shown below.

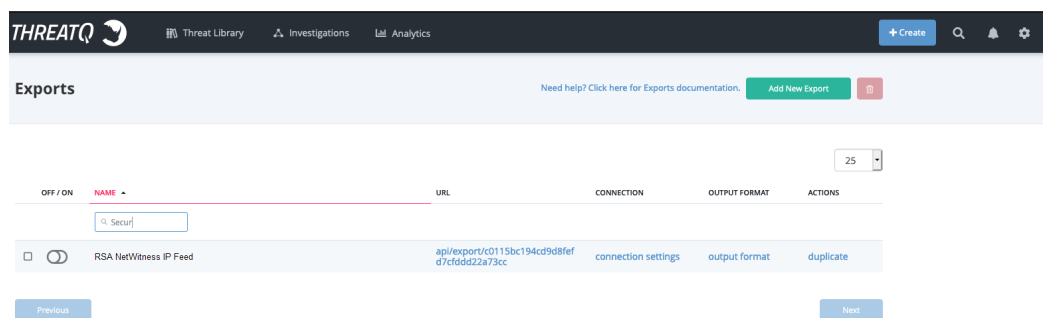


6. Click **Save Settings**.

The new export is saved, and you can then find this export by using the search bar on the Exports page.

7. Enable and Get Connection Information.

After the Export has been saved, you need to go get its URL and enable the feed. To do that, just search for it on the Exports page.



8. To enable the feed, click the Off/On toggle. Record the URL, as it is needed during the RSA NetWitness configuration.

Note: If you click on the URL, the system downloads the feed into a CSV, however, it will only take the top 10 indicators. To get the full list of indicators, right click the URL, and select “Copy Link Address”.

The configuration of the ThreatQuotient IP Feed is now complete. You can repeat the steps above for any type of indicator (for example FQDNs).

RSA NetWitness Custom Feed Configuration

Depending on your deployment and if you have elected to add an RSA NetWitness Log Decoder and/or Packet Decoder follow the steps below for your integration.

For reference, this procedure is available in the RSA NetWitness Online Documentation here: [Create a Custom Feed](#).

To create a custom feed:

1. From the main NetWitness menu, go to **Configure > CUSTOM FEEDS**.

The Custom Feeds view is displayed.

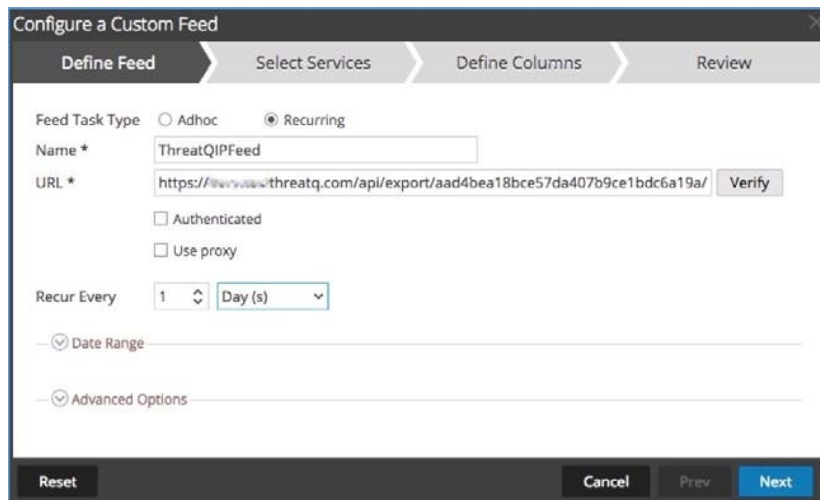
2. In the toolbar, click .

The Setup Feed dialog is displayed.

3. To select the feed type, click **Custom Feed** and **Next**.

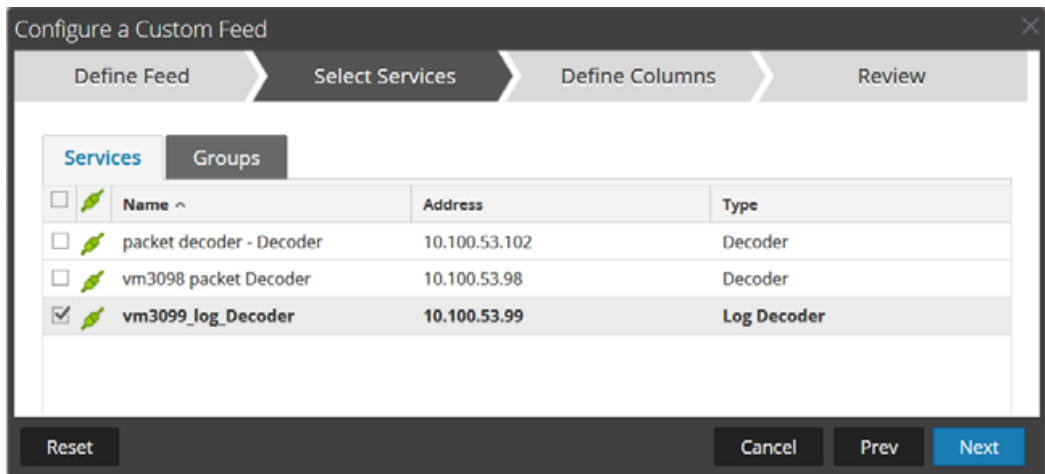
The Configure a Custom Feed wizard is displayed, with the Define Feed form open.

4. Select **Adhoc** if you are uploading the file once or **Recurring** if you plan to automate the feed. Enter the URL of the Feed provider and select how often to pull the feed by setting the **Recur Every** option and select **Next**.



The screenshot shows the 'Configure a Custom Feed' dialog box with the 'Define Feed' tab selected. The 'Feed Task Type' is set to 'Recurring'. The 'Name' field contains 'ThreatQIPFeed'. The 'URL' field contains 'https://www.threatq.com/api/export/aad4bea18bce57da407b9ce1bdc6a19a/'. There are checkboxes for 'Authenticated' and 'Use proxy'. The 'Recur Every' field is set to '1' with a dropdown menu for 'Day(s)'. There are sections for 'Date Range' and 'Advanced Options'. At the bottom, there are buttons for 'Reset', 'Cancel', 'Prev', and 'Next'.

5. Select the services on which to deploy the feed, by selecting one or more groups from the **Groups** tab.

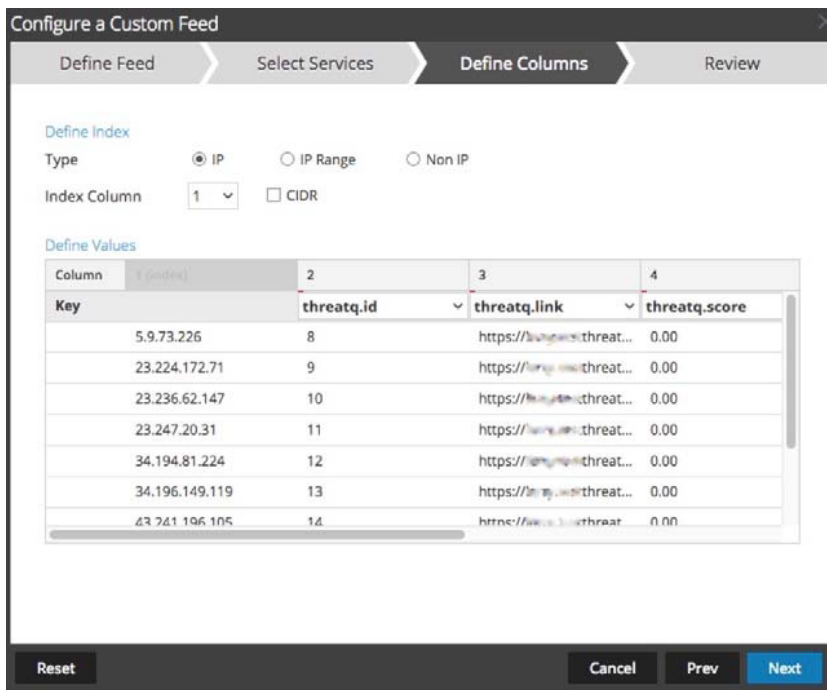


Note: Netwitness installations having only a Log Decoder or a Packet Decoder display one or the other, not both. Deploying the Feed to both Log and Packet Decoders enable matching of IP event sources such as **ip.dst**, **ip-src**, **ipv6-src**, **ipv6-dst**.

6. Click **Next**.

The Define Columns dialog is displayed.

7. Define the **Type** as **IP** and **Index Column 1** (IP Address Field). Set the header of each column as needed and click **Next**.

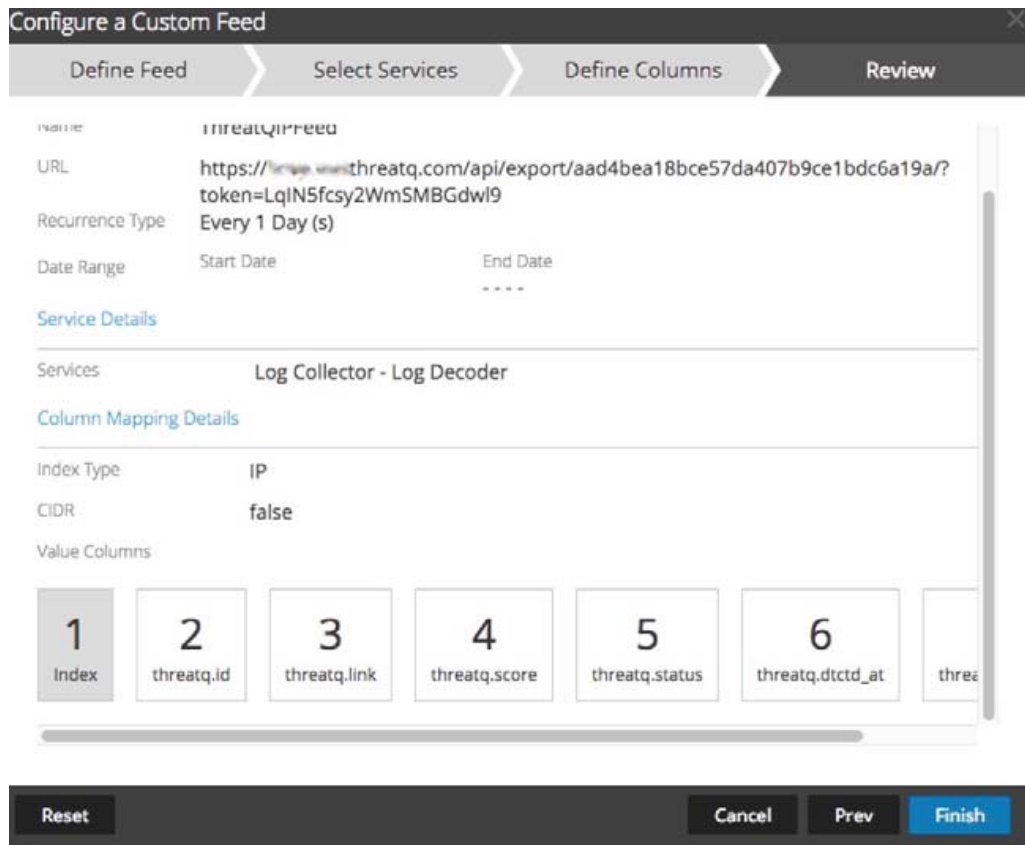


Important: This example used in this document is IP based. Use Type **Non IP** for DNS threat intelligence Callback Key(s), for **alias**host or **domain.dst** keys.

8. Select **Finish** to complete the setup of the Feed Integration.

Note that anytime before you click **Finish**, you can:

- Click **Cancel** to close the wizard without saving your feed definition.
- Click **Reset** to clear the data in the wizard.
- Click **Next** to display the next form (if not viewing the last form).
- Click **Prev** to display the previous form (if not viewing the first form)



9. Initially, the status appears as **Waiting** and the Progress indicator is yellow until RSA NetWitness completes the transfer of the Feed. After transfer is completed, the Status displays **Completed** and the Progress indicator turns green. Depending on the size of the feed, it may take some time for RSA NetWitness to download all Threat Intel from your provider.

Feeds					
Name	Trigger	Created	Last Run Time	Status	Progress
<input type="checkbox"/> RecordedFutureSALogs	Starting at 2015-Nov-04 14:34, every day	2015-11-04 09:34:26		Waiting	<div style="width: 10%; background-color: yellow;"></div>

The configuration of ThreatQ and Netwitness is complete. If there are any matches to the ThreatQ intelligence, they appear within the RSA Netwitness Investigator as part of the matched event.

2017-05-15T14:55:55 Log Network.Denied Connections 201 bytes

- ↔ 5.9.73.226 -> 192.168.150.77
- ↔ sessionid : 547889
- 📄 device.ip : 10.10.0.1
- 📄 medium : 32
- 📄 device.type : ciscoasa
- 📄 device.class : Firewall
- 📄 header.id : 0012
- ↔ alias.host : integration-server
- 📄 level : 4
- 📄 threatq.id : 8
- 📄 threatq.link : https://.../threatq.com/indicators/8/details
- 📄 threatq.score : 0.00
- 📄 threatq.status : Active
- 📄 threatq.sources : Bambenek Consulting - C2 IP
- 📄 ip.dstport : 443
- 📄 ec.activity : Deny
- 📄 ec.theme : Communication
- 📄 ec.subject : NetworkComm
- 📄 event.desc : denied by access-group
- 📄 msg.id : 106023:01
- 📄 event.cat.name : Network.Denied Connections
- 📄 parse.error : EVENTTIME
- 📄 did : nwappliance23082
- 📄 rid : 547847

Hide Additional Meta View Details

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.