RSA NetWitness Platform

Event Source Log Configuration Guide

Indegy Security Suite

Last Modified: Tuesday, December 10, 2019

Event Source Product Information:

Vendor: Indegy
Event Source: Indegy Security Suite
Versions: 3.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: cef
Collection Method: Syslog
Event Source Class.Subclass: Security.Analysis

Indegy protects industrial networks from cyber threats, malicious insiders and human error, by providing visibility and control. The RSA Partnership of Indegy and RSA NetWitness provides RSA Customers with a seamless solution to collect, analyze and report on all activity helping to reduce the time it takes to identify security related issues within the network infrastructure

To configure the Indegy event source, you must:

I. Set up a Syslog Server on Indegy Security Suite

II. Configure a Policy

III. Configure RSA NetWitness Platform for Syslog Collection

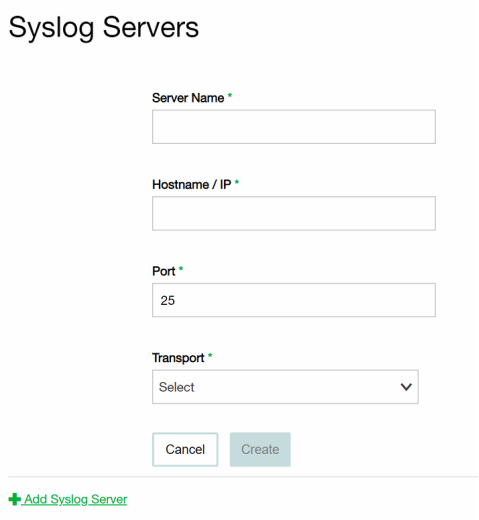
Set up a Syslog Server on Indegy Security Suite

To enable collection of log events on an external server, you need to set up a Syslog Server in the system. If you do not want to set up a Syslog Server, then the event logs will only be saved on the Indegy Core Platform.

To set up a Syslog server:

1. Under **Local Settings**, navigate to **User Management > Syslog Servers**.
2. Click + **Add Syslog Server**.

   The Syslog Server configuration window is displayed.



3. Fill in the details for your Syslog server.

Field	Description
Server Name	Enter the name of a Syslog Server to be used for logging system events
Hostname/IP	Enter a host name or an IP address of the Syslog server
Port	Enter the port number on the Syslog server to which the events will be sent. Default value is **514**.
Transport	Select a transport method from the drop-down menu: either TCP or UDP.
Send Test Email	Click if you would like to send a test message to verify that the configuration was successful, and check if the message has arrived.

4. Click **Save**.

Repeat the previous procedure if you need to set up additional Syslog servers.

Configure a Policy to Log Events

Policies are used to define specific types of events that are suspicious, unauthorized, anomalous or otherwise noteworthy that take place in the network. When an event occurs that meets all the Policy Definition conditions for a Policy, an Event is generated in the Indegy system. The Event is logged in the system and notifications are sent out in accordance with the Policy Actions configured for the Policy.

The system features a set of predefined policies (out-of-the-box). In addition, the system offers the ability to edit the predefined policies or define new custom policies.

Policy Configuration

Each Policy consist of a series of conditions that define a specific type of behavior in the network. This includes considerations such as the activity, the assets involved and the timing of the event. Only an event that conforms to all the parameters set in the Policy will trigger an Event for that Policy. Each Policy has a designated Policy Actions configuration which defines the severity, notification methods, and logging of the Event

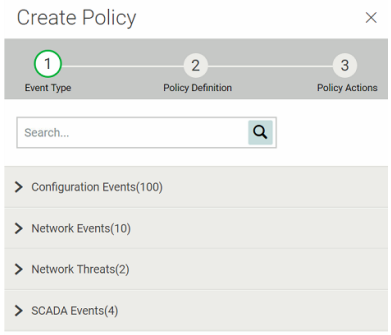
Creating Policies

You can create custom Policies based on the specific considerations of your ICS network. You can determine precisely what type of events should be brought to the attention of your staff and how the notifications are delivered. You have complete flexibility in determining how specific or broad a definition you would like to give to each Policy.

To create a new policy:

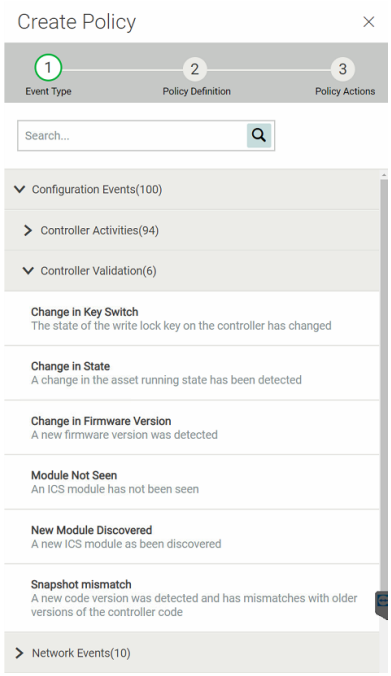
1. On the **Policies** screen, click **Create Policy**.

   The New Policy wizard opens.



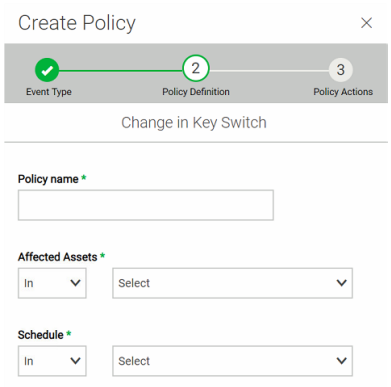
2. Click on a policy category to show the sub-categories and Policy Types.

A list of all sub-categories and Types included in that category are displayed.



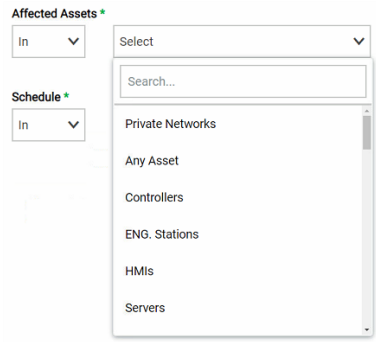
3. Select a Policy Type.
4. Click **Next**.

   A series of parameters for defining the Policy are displayed. This includes all relevant Policy conditions for the selected Policy Type.



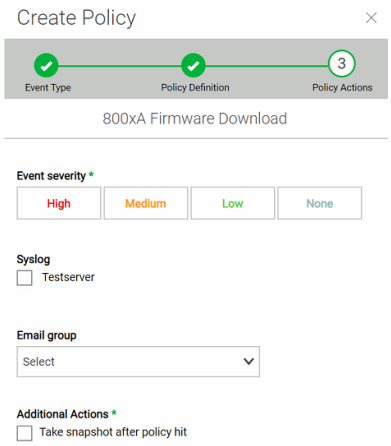
5. Name the policy by entering text in the **Policy Name** field.
6. For each parameter that is shown:
   - Where relevant, select **In** (default) to whitelist the selected element or **Not in** to blacklist the selected element.
   - Click on **Select**, and then choose the desired element from the drop-down list that

is displayed. The following screen shows an example.



7. After you have filled in all fields, click **Next**.

   A series of Policy Action parameters are shown (that is, the actions taken by the system when a Policy hit occurs).



8. Fill in available fields.

Section	Description
Event Severity	Select the desired severity level for this policy: High, Medium, Low, or None
Syslog	If you would like to send Event logs to one or more Syslog servers, select the checkbox next to each server to which you would like to send the Event logs
Email group	If you would like to send email notifications of events, select from the drop-down list the Email Group to be notified.

9. After you have filled in all fields, click **Create**.

The new Policy is created and automatically activated. The Policy is shown in the lists on the Policies screen.

Configure RSA NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is **cef**.

Configure Syslog Collection

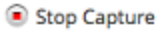
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **System**.
3. Depending on the icon you see, do one of the following:

- If you see 

, click the icon to start capturing Syslog.
- If you see 

, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

   The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.
5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

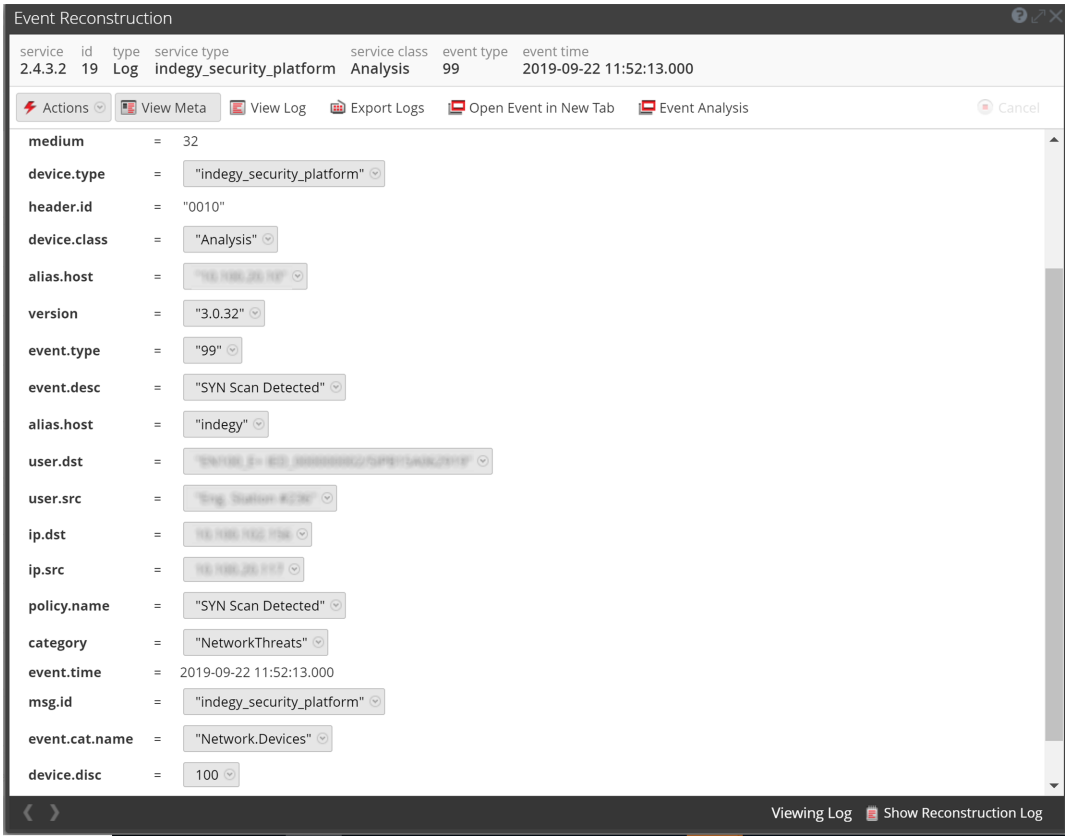
   The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

After you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Example Indegy Event in RSA NetWitness Platform

The following is an example of an event from the Indegy Suite, as displayed in RSA NetWitness Investigator event reconstruction:



Trademarks

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