

# RSA NetWitness Logs

Event Source Log Configuration Guide



## Cisco Firewall Service Module

Last Modified: Tuesday, May 09, 2017

### Event Source Product Information:

**Vendor:** [Cisco](#)

**Event Source:** Firewall Service Module (FWSM)

**Versions:** 4.1(5)

### RSA Product Information:

**Supported On:** NetWitness Suite 10.0 and later

**Event Source Log Parser:** ciscoasa

**Collection Method:** Syslog

**Event Source Class.Subclass:** Security.Firewall

# Configure Cisco Firewall Service Module

---

To configure Syslog collection for the Cisco Firewall Service Module you must:



- I. Configure RSA NetWitness Suite for Syslog Collection
- II. Configure Syslog Output on Cisco Firewall Service Module

## Configure RSA NetWitness Suite for 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 **Administration > 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  **Start Capture**, click the icon to start capturing Syslog.
  - If you see  **Stop Capture**, 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 **Administration > 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.

Once 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.

## Configure Syslog Output on Cisco Firewall Service Module

Cisco FWSM generates syslog events.

### To configure Cisco FWSM to generate syslog events:

1. Connect to the FWSM console through telnet or SSH.
2. To enter the enable mode, type:

```
enable
```

3. To enter the configure mode, type:

```
config terminal
```

4. Type the following lines:

```
no logging timestamp
logging trap debugging
logging host inside 1.2.3.4
```

where *1.2.3.4* is the IP address of the RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Collector.

5. Press CTRL+Z to exit config mode.
6. Type the following command to save the configuration changes:

```
copy running-config startup-config
```

Copyright © 2017 EMC Corporation. All Rights Reserved.

## **Trademarks**

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.