

RSA NetWitness Platform

Event Source Log Configuration Guide



Cisco Adaptive Security Appliance

Last Modified: Monday, May 16, 2022

Event Source Product Information:

Vendor: [Cisco](#)

Event Source: Adaptive Security Appliance

Versions: 7.x, 8.x, 9.x, 11.13

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 11.0 and later

Event Source Log Parser: ciscoasa

Collection Method: Syslog

Event Source Class.Subclass: Security.Firewall

To configure Syslog collection for the Cisco Adaptive Security Appliance you must:

- I. Configure Syslog Output on Cisco Adaptive Security Appliance
- II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Cisco Adaptive Security Appliance

To configure Cisco ASA to generate syslog events:

1. Connect to the ASA 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 Log Decoder or Remote Log Collector.

5. Press CTRL+Z to exit config mode.

6. Type the following command to save the configuration changes:

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

Configure RSA NetWitness Platform for Syslog Collection

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 **ciscoasa**.

Configure Syslog Collection

Note: Syslog collection must be configured only for the first time when you set up an event source which uses Syslog to send its output to NetWitness.

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

Log Decoder Configuration Steps for Syslog Collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the **Services** grid, choose 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.

Remote Log Collector Configuration Steps for Syslog Collection:

1. In the **NetWitness** menu, go to **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 will appear.
5. Choose either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Choose the **New Type** in the **Event Categories** panel and click **+** in the **Sources** panel toolbar.
The **Add Source** dialog will appear.
7. Enter **514** for the port, and choose **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.

© 2022 RSA Security LLC or its affiliates. All Rights Reserved.

November 2020

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.