

# RSA NetWitness Platform

## Event Source Log Configuration Guide



## Cisco IronPort Email Security Appliance

Last Modified: Friday, April 5, 2019

### Event Source Product Information:

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

**Event Source:** Email Security Appliance

**Versions:** 5.7.0, 7.1.3, 8.0.1, 8.5.x, 11.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:** ciscoiportesa

**Collection Method:** File, Syslog

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

You can use File or Syslog collection (or both). Follow the steps in the appropriate section to configure the Cisco IronPort Email Security Appliance for use with RSA NetWitness Platform.

## Configure File Collection

---

- I. Configure RSA NetWitness Log Collector for SCP Protocol
- II. Configure the Cisco IronPort ESA event source for File Collection
- III. Configure the RSA NetWitness Log Collector for File Collection

### Configure RSA NetWitness Log Collector for SCP Protocol

On 10.6.x Log Collectors, the SELinux environment prevents the SCP protocol from working with the default configuration. The following steps allow the SCP protocol to function.

#### Log Collector versions 10.6.2 and Later

The Log Collector configures SELinux to run **Enforcing** mode. This is required for the **plugin** collection protocol. If you have AWS Cloudtrail or Microsoft Azure event sources on a Log Collector, SELinux must remain in **Enforcing** mode.

The recommendation is to use a separate VLC for the File collection event sources using SCP. On this VLC, disable SELinux as mentioned below for Log Collector 10.6.0 and Later. This step **MUST** be performed whenever the Log Collector RPM is updated on this VLC.

#### Log Collector versions 10.6.0 and Later

By default, SELinux runs in Permissive mode. Disabling SELinux resolves the problem.

#### To configure RSA version 10.6.0 and Later Log Collectors:

1. Log into the Log Collector appliance.
2. Edit the `/etc/selinux/config` file. Change the line from:  

```
SELINUX=permissive
```

 or 

```
SELINUX=enforcing
```

 to:  

```
SELINUX=disabled
```
3. Save the file.
4. Reboot the system.

5. Confirm that SELinux is disabled by running the command `sestatus`. The command should return the following text:

```
SELinux status: disabled
```

## Configure Cisco IronPort ESA for File Collection

Perform the following steps on the Cisco IronPort ESA event source to configure file collection.

### To configure Cisco IronPort ESA for file collection:

1. Log on to the IronPort web interface.
2. To edit the settings of the Authentication Logs subscription, follow these steps:
  - a. From the top menu, click **System Administration > Log Subscriptions**.
  - b. In the Log Subscriptions window, click **authentication** to view the Authentication Logs subscription.
  - c. In the **Retrieval Method** section of the Edit Log Subscription window, select **SCP on Remote Server**.
  - d. Under **SCP on Remote Server**, complete the fields as follows.

Field	Action
<b>Protocol</b>	Select <b>SSH2</b> .
<b>SCP Host</b>	Enter the IP address of your RSA NetWitness Platform Log Collector.
<b>SCP Port</b>	Enter <b>22</b> .
<b>Directory</b>	Enter the following path:  /home/upload/eventsources/cisco_ironport_esa/CISCO_IRONPORT_ESA
<b>Username</b>	Enter <b>upload</b> .

- e. Click **Submit**.  
An SSH key is generated.
- f. Copy the generated SSH Key into RSA NetWitness Platform. See the details in the [Configure the Log Collector for File Collection](#) section.

**Note:** The entire SSH key must be on a single line and cannot include any spaces. If necessary, remove spaces.

3. To edit the settings of the IronPort Text Mail Logs subscription, follow these steps:
  - a. From the top menu, click **System Administration > Log Subscriptions**.
  - b. In the Log Subscriptions window, click **mail\_logs** to view the IronPort Text Mail Logs subscription.
  - c. In the **Retrieval Method** section of the Edit Log Subscription window, select **SCP on Remote Server**.
  - d. Under **SCP on Remote Server**, complete the fields as described in step 2.
  - e. Click **Submit**.

**Note:** The same SSH key as in step 2 is generated. You can ignore this SSH key.

4. To edit the settings of the CLI Audit Logs subscription, follow these steps:
  - a. From the top menu, click **System Administration > Log Subscription**.
  - b. In the Log Subscriptions window, click **cli\_logs** to view the CLI Audit Logs subscription.
  - c. In the **Retrieval Method** section of the Edit Log Subscription window, select **SCP on Remote Server**.
  - d. Under **SCP on Remote Server**, complete the fields as described in step 2.
  - e. Click **Submit**.

**Note:** The same SSH key as in step 2 is generated. You can ignore this SSH key.

5. Click **Commit Changes** to save all log settings.
6. In the Uncommitted Changes window, click **Commit Changes** to apply all log settings.

## Configure the Log Collector for File Collection

Perform the following steps to configure the Log Collector for File collection.

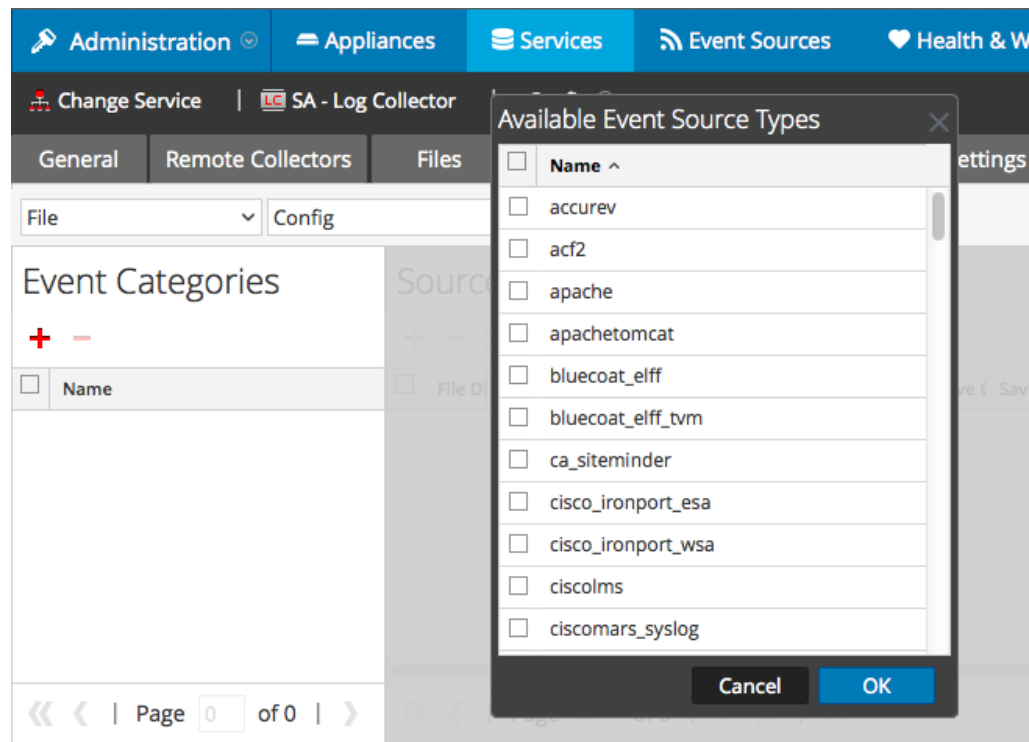
**To configure the Log Collector for file collection:**

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

The Event Categories panel displays the File 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 the correct type from the list, and click **OK**.

Select **cisco\_ironport\_esa** from the **Available Event Source Types** dialog.

6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.

7. Add a File Directory name, modify any other parameters that require changes, and

click **OK**.

8. To add the SSH key, click **Advanced** to display the advanced settings, and then copy your SSH key into the **Eventsource SSH Key** field.
9. **Stop and Restart File Collection.** After you add a new event source that uses file collection, you must stop and restart the RSA NetWitness Platform File Collection service. This is necessary to add the key to the new event source.

## Configure Syslog Collection

---

- I. Configure the Cisco IronPort ESA event source for Syslog Collection
- II. Configure the RSA NetWitness Platform For Syslog Collection

### Configure Cisco IronPort ESA for Syslog Collection

Perform the following steps on the Cisco IronPort ESA event source to configure Syslog collection.

#### To configure Cisco IronPort ESA for Syslog:

1. Log onto your Cisco IronPort UI.
2. Select **System Administration\Log Subscriptions**.
3. Click **Add Log Subscription**.
4. Configure the following values:
  - **Log Type:** Define a log subscription for both IronPort Text Mail Logs and System Logs (whichever you want to monitor)
  - **Log Name:** Type a descriptive log name
  - **File Name:** Use the default configuration value
  - **Maximum File Size:** Use the default configuration value
  - **Log Level:** Select **Information** (Default).
  - **Retrieval Method:** Select **Syslog Push**
  - **Hostname:** Type the the IP address of the RSA NetWitness Log Decoder or Remote Log Collector
  - **Protocol:** Select **UDP**
  - **Facility:** Use the default configuration value; this value depends on the configured Log Type
5. Save the subscription.

## 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 **ciscoiportesa**.

### 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 **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.

Copyright © 2019 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](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).