

RSA NetWitness Platform

Event Source Log Configuration Guide



Cisco IronPort Web Security Appliance (WSA)

Last Modified: Tuesday, January 21, 2020

Event Source Product Information:

Vendor: [Cisco](#)

Event Source: Web Security Appliance (WSA)

Versions: 5.7.0, 6.3, 7.x, 8.x, 9.x, 10.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.

Additional Download: `ciscoportwsa_custom_fields.txt`

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: `ciscoportwsa`

Collection Method: File, Syslog (7.5.x and higher)

Event Source Class.Subclass: Host.Web Logs

Configure Cisco IronPort WSA

To configure Cisco IronPort WSA, you must complete one of the following tasks:

- Configure File Collection for Cisco IronPort WSA, or
- Configure Syslog for Cisco IronPort WSA

RSA supports log collection through File collection or syslog for Cisco IronPort WSA. Syslog is only supported on version 7.5.x and higher for this event source.

Note: RSA recommends that you only use File collection for Cisco IronPort WSA. Syslog messages greater than 1024 bytes are truncated, and thus the Log Decoder cannot parse them.

Configure File Collection for Cisco IronPort WSA

To configure File for Cisco IronPort WSA, you must complete the following tasks:

- I. Configure NetWitness Platform for File Collection
 - Optional (for Cisco IronPort WSA version 9.x): Configure NetWitness Platform for SCP
 - Configure the Log Collector for File collection
- II. Configure Logs on Cisco IronPort WSA

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:

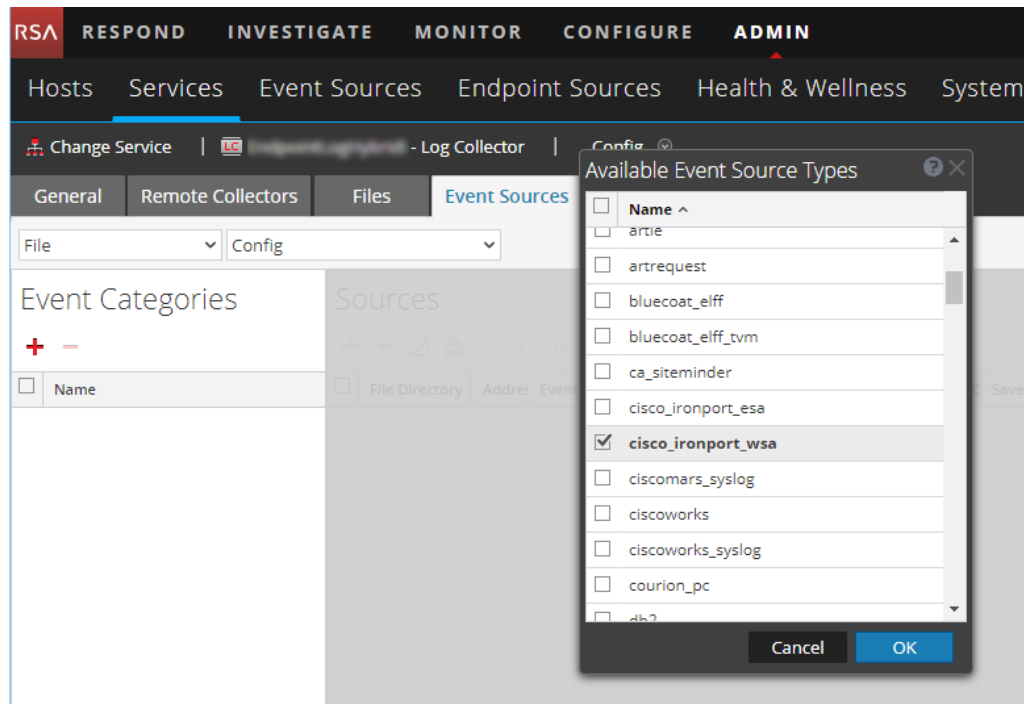
```
SELinux status: disabled
```

Configure 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 **ADMIN > 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 **cisco_ironport_wsa** from the **Available Event Source Types** dialog, and click **OK**.



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**.

Remember the value you enter in the **File Directory** field. You will need to enter the same value later for the **Directory** value when you configure the Cisco IronPort WSA event source. For example, if you enter **ciscoWSA** for **File Directory** in this dialog box, make sure to set your **Directory** parameter to

`/home/upload/eventsources/cisco_ironport_wsa/ciscoWSA.`

Note: The file directory gets created in the following location on the Log Collector: `/var/netwitness/logcollector/upload/cisco_ironport_wsa/ciscoWSA`. Make sure that the user upload has permissions to write data to the directory.

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.

Note: You need to perform the steps in [Configure Logs on Cisco IronPort WSA](#), generate the SSH key there, and then return to this step to enter the SSH key.

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 Logs on Cisco IronPort WSA

Note: All logs are optional, however, the RSA NetWitness Platform parses only the logs that are configured as follows. Logs can be accessed in either Apache or Squid format.

To configure Cisco IronPort WSA:

1. Log on to the IronPort web interface.
2. Select **System Administration > Log Subscriptions**.
3. To configure Access Logs in Apache format, complete these tasks:
 - a. Click **Add Log Subscription**.
 - b. For **Log Type**, select **Access Logs** and use the following settings.

Setting	Value
Rollover by Time	Custom Time Interval
Rollover every	5m
Log Style	Apache
Custom Fields	<ul style="list-style-type: none"> • For IronPort WSA 5.7.0 and 6.3: %k %p %u %XF • For IronPort WSA 7.x and higher: Copy the Apache custom field string from the ciscoportwsa_custom_fields.txt additional file. You can download the Cisco IronPort WSA additional file from RSA Link here: https://community.rsa.com/docs/DOC-45501 <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: Ensure the string is in <code>key= %string key= %string</code> format when you paste the string in the Custom Fields. Any difference in this format can lead to unknown messages.</p> </div>
Retrieval Method	SCP on Remote Server

Setting	Value
Max Time Interval	This field is optional. Recommended value is 180 Note: For sites that generate a lot of traffic, try lowering this value to 60 seconds to reduce the number of Events Per Second (EPS) generated.
Protocol	SSH2
SCP Host	IP address of the RSA NetWitness Platform Log Collector.
SCP Port	22
Directory	/home/upload/eventsources/cisco_ironport_wsa/ <i>userFolder</i> , where <i>userFolder</i> is the name you specify. Note that <i>userFolder</i> must match the File Directory name that you specified when you configured the Log Collector for file collection earlier.
Username	upload

- c. Click **Submit**.
- d. Copy the generated SSH Key into RSA NetWitness Platform. See the details in [Step 8](#) of the **Configure the Log Collector for File Collection** section.

Note: The entire key must be on a single line. Also, remove any spaces from the key. IronPort creates the same SSH Key for all log subscriptions. The key only needs to be saved once.

- e. Commit your changes.
4. To configure Access Logs in Squid format, complete these tasks:

Note: Access Logs in Squid format only works with Cisco IronPort WSA 7.x and higher.

- a. Click **Add Log Subscription**.
- b. For **Log Type**, select **Access Logs** and use the following settings.

Setting	Value
Rollover by Time	Custom Time Interval
Rollover every	5m

Setting	Value
Log Style	Squid
Custom Fields	Copy the Apache custom field string from the ciscoiportwsa_custom_fields.txt additional file. You can download the Cisco IronPort WSA additional file from RSA Link here: https://community.rsa.com/docs/DOC-45501
Retrieval Method	SCP on Remote Server
Max Time Interval	This field is optional. Recommended value is 180 <div style="border: 1px solid green; padding: 5px; margin-top: 5px;"> <p>Note: For sites that generate a lot of traffic, try lowering this value to 60 seconds to reduce the number of Events Per Second (EPS) generated.</p> </div>
Protocol	SSH2
SCP Host	IP address of the RSA NetWitness Platform Log Collector.
SCP Port	22
Directory	<code>/home/upload/eventsources/cisco_ironport_wsa/userFolder</code> , where userFolder is the name you specify. Note that userFolder must match the File Directory name that you specified when you configured the Log Collector for file collection earlier.
Username	upload

- c. Click **Submit**.
- d. Copy the generated SSH Key into RSA NetWitness Platform. See the details in [Step 8](#) of the **Configure the Log Collector for File Collection** section.

Note: The entire key must be on a single line. Also, remove any spaces from the key. IronPort creates the same SSH Key for all log subscriptions. The key only needs to be saved once.

- e. Commit your changes.
5. To configure W3C Logs, complete these tasks:

Note: W3C Logs are not supported for IronPort WSA 7.x or higher.

- a. Select **W3C Logs** and use the following settings:

Setting	Value
Selected Log Fields	<div style="border: 1px solid green; padding: 5px; margin-bottom: 10px;"> <p>Note: The Selected Log Fields must be in this exact order.</p> </div> <p>timestamp x- elapsed-time c-ip s-ip s-port x-resultcode-httpstatus sc-bytes cs-method cs-url cs-username x-hierarchy-origin cs-mime-type x-acltag x-result-code cs(User Agent) x-webcat-code-full sc-httpstatus cs(Referer) cs(Cookie) s-computename s-hostname sc-result-code cs-version cs-auth-group</p>
Retrieval Method	SCP on Remote Server
Max Time Interval	180
Protocol	SSH2
SCP Host	IP address of the RSA NetWitness Platform Log Collector.
SCP Port	22
Directory	/home/upload/eventsources/cisco_ironport_wsa/ <i>userFolder</i> , where <i>userFolder</i> is the name you specify. Note that <i>userFolder</i> must match the File Directory name that you specified when you

Setting	Value
	configured the Log Collector for file collection earlier.
Username	upload

- b. Click **Submit**. The generated SSH Key will be identical to the one initially generated.

Note: IronPort creates the same SSH Key for all log subscriptions. The key only needs to be saved the first time.

- 6. To configure CLI Audit Logs, complete these tasks:

- a. Select **CLI Audit Logs** and use the following settings:

Setting	Value
Retrieval Method	SCP on Remote Server
Max Time Interval	180
Protocol	SSH2
SCP Host	IP address of the RSA NetWitness Platform Log Collector.
SCP Port	22
Directory	/home/upload/eventsources/cisco_ironport_wsa/ <i>userFolder</i> , where <i>userFolder</i> is the name you specify. Note that <i>userFolder</i> must match the File Directory name that you specified when you configured the Log Collector for file collection earlier.
Username	upload

- b. Click **Submit**. The generated SSH Key will be identical to the one initially generated.

Note: IronPort creates the same SSH Key for all log subscriptions. The key only needs to be saved the first time.

- 7. To configure IDS Data Loss Logs, complete these tasks:

- a. Select **IDS Data Loss Logs** and use the following settings:

Setting	Value
Retrieval Method	SCP on Remote Server
Max Time Interval	180
Protocol	SSH2
SCP Host	IP address of the RSA NetWitness Platform Log Collector.
SCP Port	22
Directory	/home/upload/eventsources/cisco_ironport_wsa/ userFolder , where userFolder is the name you specify. Note that userFolder must match the File Directory name that you specify when you configure the Log Collector for file collection later.
Username	upload

- b. Click **Submit**. The generated SSH Key will be identical to the one initially generated.

Note: IronPort creates the same SSH Key for all log subscriptions. The key only needs to be saved the first time.

8. Click **Commit Changes**.
9. Click **Commit Changes**.

Configure Syslog Collection for Cisco IronPort WSA

Note: RSA recommends that you only use File collection for Cisco IronPort WSA. Syslog messages greater than 1024 bytes are truncated, and thus the Log Decoder cannot parse them.

To configure File for Cisco IronPort WSA, you must complete the following tasks:

- I. Configure Logs on Cisco IronPort WSA
- II. Configure Syslog on RSA NetWitness Platform

Configure Logs on Cisco IronPort WSA

1. Log on to Cisco IronPort WSA with administrator credentials.
2. Select **System Administration > Log Subscriptions**.
3. To configure Access Logs in Apache format, complete these tasks:
 - a. Click **Add Log Subscription**.
 - b. For **Log Type**, select **Access Logs** and use the following settings.
 - **Rollover by Time** = Custom Time Interval
 - **Rollover every** = 5m
 - **Log Style** = Apache
 - **Custom Fields** =

Copy the Apache custom field string from the **ciscoportwsa_custom_fields.txt** additional file. You can download the Cisco IronPort WSA additional file from RSA Link, in the Event Source Additional Downloads space here: <https://community.rsa.com/docs/DOC-45501>.

Note: Ensure the string is in `key= %string key= %string` format when you paste the string in the Custom Fields. Any difference in this format can lead to unknown messages.

- **Retrieval Method** = Syslog Push

Complete the following fields:

Field	Value
Hostname	Enter the IP address of your RSA NetWitness Platform Log Decoder or Remote Log Collector
Protocol	UDP
Facility	local0

- c. Click **Submit**.
 - d. Commit changes.
4. To configure Access Logs in Squid format, complete these tasks:
- a. Click **Add Log Subscription**.
 - b. For **Log Type**, select **Access Logs** and use the following settings.

- **Rollover by Time** = Custom Time Interval
- **Rollover every** = 5m
- **Log Style** = Squid
- **Custom Fields** =

Copy the Squid custom field string from the **ciscoportwsa_custom_fields.txt** additional file. You can download the Cisco IronPort WSA additional file from RSA SecurCare Online.

- **Retrieval Method** = Syslog Push

Complete the following fields:

Field	Value
Hostname	Enter the IP address of your RSA NetWitness Platform Log Decoder or RSA NetWitness PlatformRemote Log Collector
Protocol	UDP
Facility	local0

- c. Click **Submit**.
- d. Commit changes.

Configure RSA NetWitness Platform for Syslog

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 **ciscoiportwsa**.



Configure RSA NetWitness Platform 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 **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  **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 **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.

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.