

# RSA NetWitness Platform

## Event Source Log Configuration Guide



## CiscoWorks Common Services

Last Modified: Wednesday, January 22, 2020

### Event Source Product Information:

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

**Event Source:** CiscoWorks Common Services / Cisco Security Manager

**Supported Versions:** 2.3, 3.0, 3.3, 4.0

**Additional Downloads:** [sftpageant.conf.ciscoverks](#)

Link: [CiscoWorks Common Services Additional Downloads](#)

### RSA Product Information:

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

**Event Source Log Parser:** ciscoworks

**Collection Method:** File

**Event Source Class.Subclass:** Network.Configuration Management

## Configure CiscoWorks Common Services

---

You must complete these tasks to configure CiscoWorks Common Services for File collection:

- I. Set Up the SFTP Agent
- II. Configure the Log Collector for File Collection

### Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see [Install and Update SFTP Agent](#)
- To set up the SFTP agent on Linux, see [Configure SFTP Shell Script File Transfer](#)

### Configure the Log Collector for File Collection

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

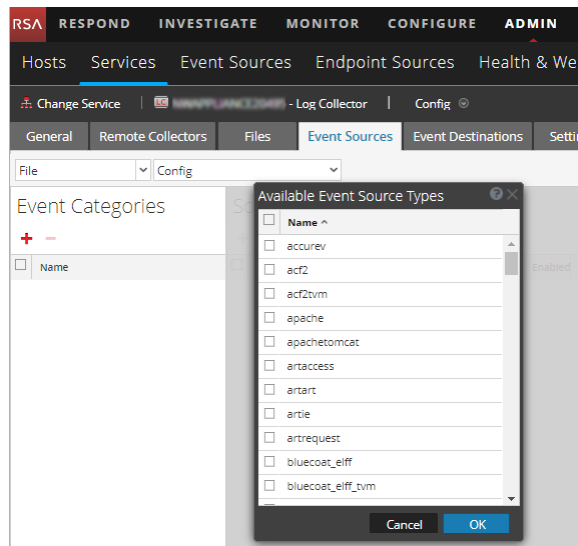
#### To configure the Log Collector for file collection:

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.

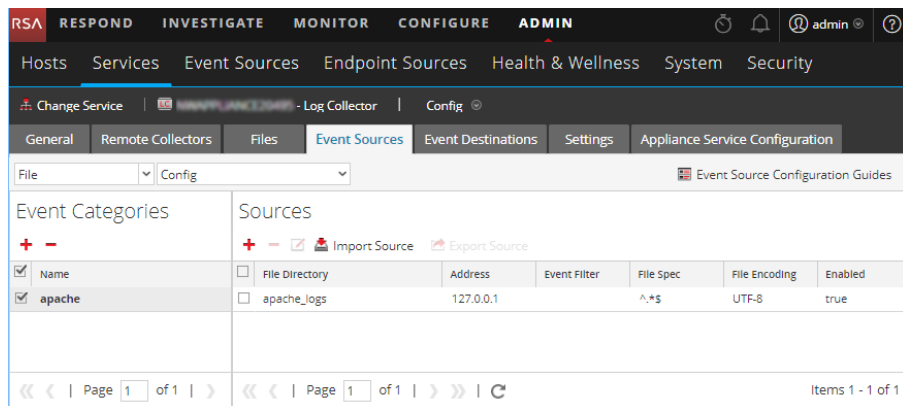


5. Select the correct type from the list, and click **OK**.

Select either **ciscoworks** or **ciscoworks\_syslog** from the **Available Event Source Types** dialog.

The newly added event source type is displayed in the Event Categories panel.

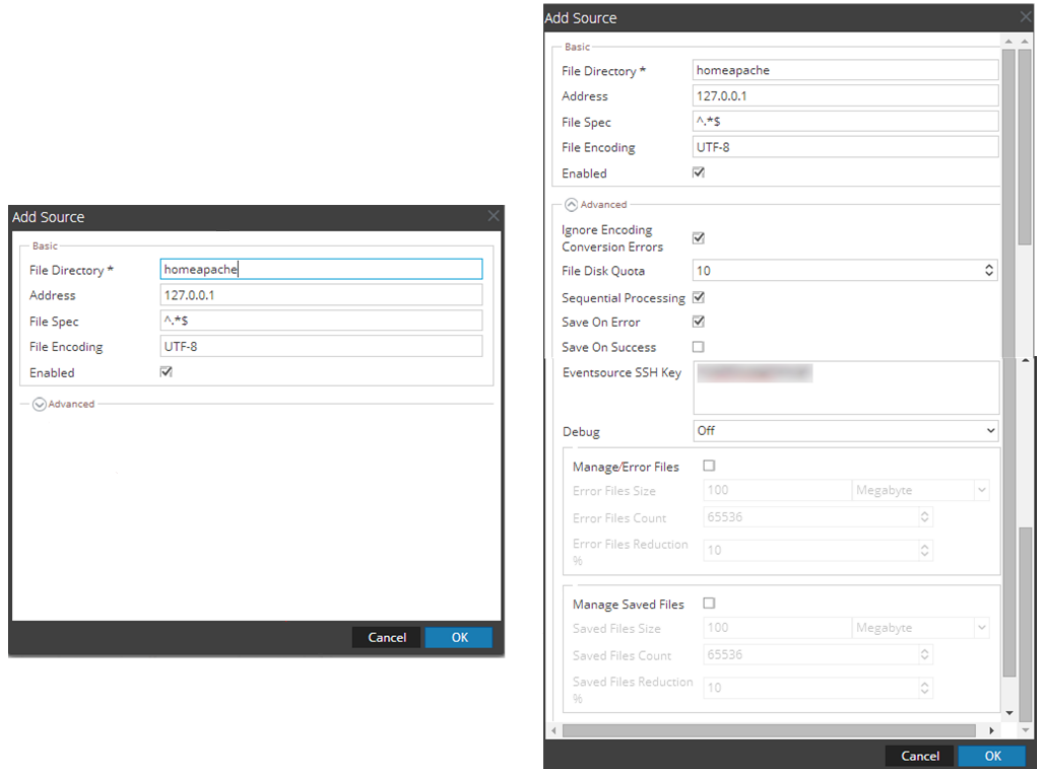
**Note:** The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



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

The Add Source dialog is displayed.

**Note:** Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.
8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

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