

CA SiteMinder

Last Modified: Tuesday, January 14, 2020

Event Source Product Information:

Vendor: [CA](#)

Event Source: SiteMinder

Versions: r12

Additional Downloads: [sftpageant.conf.casiteminder](#)

Link: [CA SiteMinder Additional Downloads](#)

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: casiteminder

Collection Method: File

Event Source Class.Subclass: Security.Access Control

CA Siteminder

This section describes how to:

- Configure CA SiteMinder to collect logs
- Set Up the SFTP Agent
- Set Up the File Service

Configure CA SiteMinder to Collect Logs

To configure CA SiteMinder:

1. Log on to the CA SiteMinder console with administrative credentials.
2. Click **Start > All Programs > Siteminder > Siteminder Policy Server Management Console**.
3. In the Policy Server Management Console window, follow these steps:
 - a. Select the **Data** tab.
 - b. From the **Database** drop-down list, select **Audit logs**.
 - c. From the **Storage** drop-down list, select **Text file**.

Note: RSA only supports logs collected in the text file format.

- d. In the **File Name** field, enter a location to store the log files.

Note: You will need this location when you set up the SFTP Agent.

- e. Click **OK**.

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.

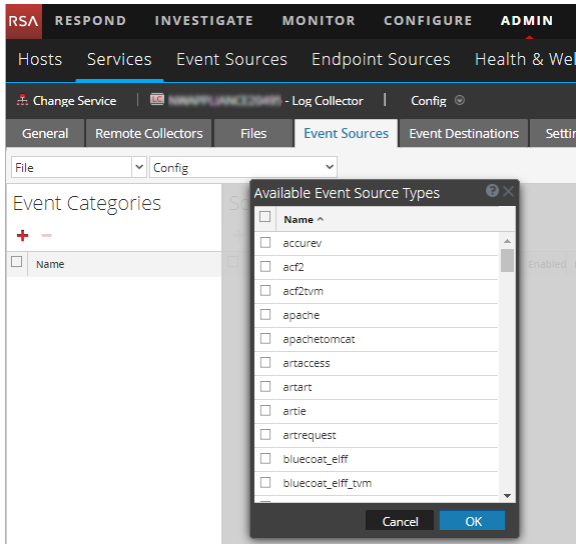
To configure the Log Collector for file collection:

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.

- In the Event Categories panel toolbar, click **+**.

The Available Event Source Types dialog is displayed.

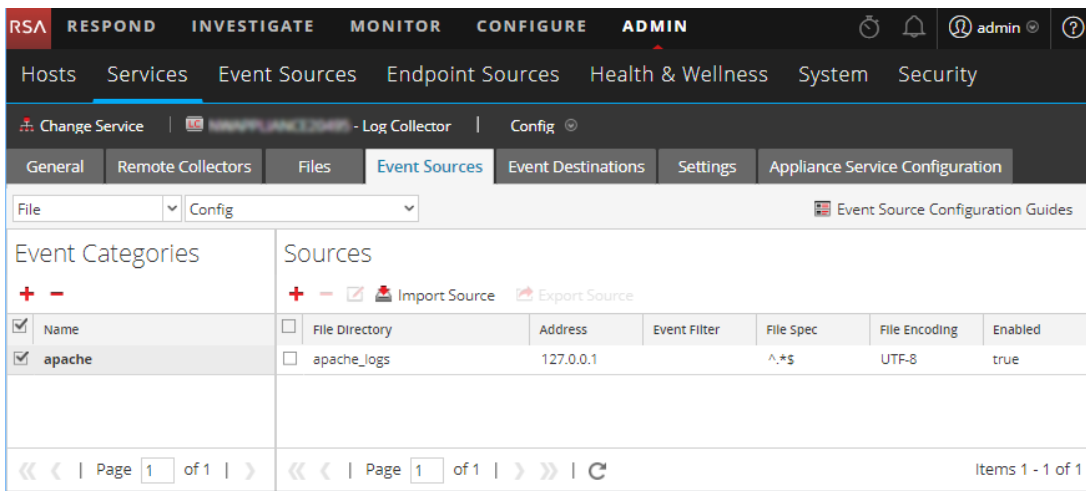


- Select the correct type from the list, and click **OK**.

Select **ca_siteminder** from the **Available Event Source Types** dialog.

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

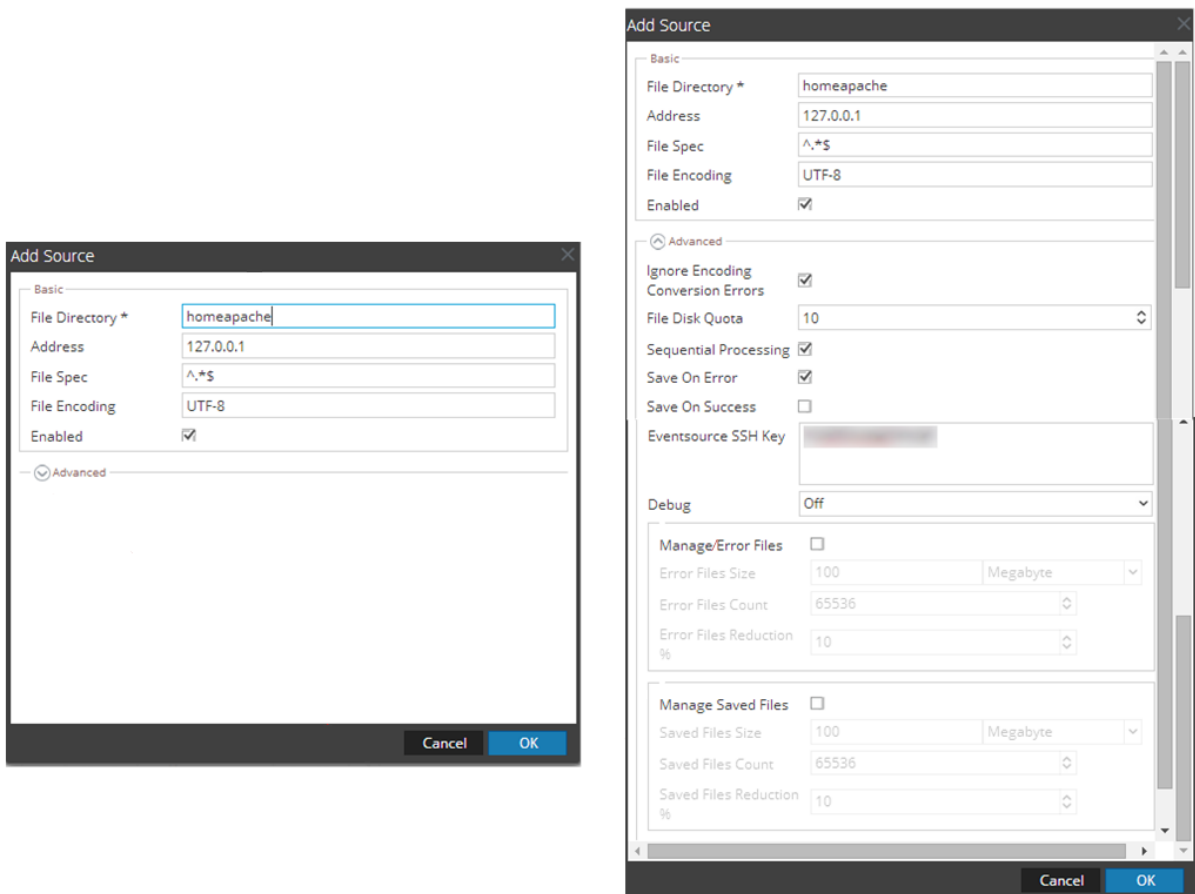
Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



- 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.