# **CA SiteMinder**

Last Modified: Tuesday, January 14, 2020

## **Event Source Product Information:**

Vendor: CA Event Source: SiteMinder Versions: r12 Additional Downloads: sftpagent.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.
- 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.

RSA RESPOND	INVESTIGATE	м	ONITOR	CONFIGUR	E ADI	MIN
Hosts Service	s Event Sou	rces	Endpoin	it Sources	Health	& Well
A Change Service		- 1	Log Collector	Config ©		
General Remote	Collectors Fil	es	Event Source	es Event De	stinations	Settin
File	Config		~			
Event Categorie	es So	Availat	ole Event Sou	urce Types	©×	
+ -			ame ^			
□ Name		ac ac	f2		— i I	
		🗆 ac	f2tvm		- 11	
		🗆 ap	ache		- 1	
		🗆 ap	achetomcat		- 11	
		⊔ ar □ ar	taccess		- 11	
		ar	tie		- 11	
		🗆 ar	trequest		- 1	
		D bl	uecoat_elff		- 11	
		L bi	uecoat_elff_tvm			
				Cancel	ОК	

5. 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.

<b>Note:</b> The image bel different, depending	ow uses <b>Apache</b> as on which Event Sou	s an example arce type you	only. Yo are conf	ur screen iguring.	will look	
RSA RESPOND INVESTI	GATE MONITOR CC	ONFIGURE AD	MIN	(	0 Q Č	admin 🏾 🕐
Hosts Services Even	t Sources Endpoint S	ources Health	n & Wellnes	s System	n Security	1
🚠 Change Service 🔰 🔟	- Log Collector	Config ©				
General Remote Collectors	Files Event Sources	Event Destinations	Settings	Appliance Se	rvice Configurat	tion
File 💙 Config	~			📰 Ever	nt Source Config	uration Guides
Event Categories	Sources					
+ -	🕂 🗕 🗹 📥 Import Source	🖄 Export Source				
Name Name	ame 🗆 File Directory		Event Filter	File Spec	File Encoding	Enabled
🗹 apache	apache_logs	127.0.0.1		^. <b>*\$</b>	UTF-8	true
<pre>《 (   Page 1 of 1   )</pre>	<pre>《《 《   Page 1 of 1</pre>	> ≫   C				items 1 - 1 of 1

 Select the new type in the Event Categories panel and click + in the Sources panel toolbar. The Add Source dialog is displayed.

		Add Source			
		Basic			
		File Directory *	homeapache		
		Address	127.0.0.1		
		File Spec	^.*\$		
		File Encoding	UTF-8		
		Enabled			
50		Advanced —			
.e		Ignore Encoding Conversion Error	.s		
ectory *	homeapache	File Disk Quota	10		
s	127.0.0.1	Sequential Proces	ssing 🗹		
c	^.*S	Save On Error	$\checkmark$		
ding	UTF-8	Save On Success			
	$\overline{\mathbf{v}}$	Eventsource SSH	Key		
d					
		Debug	Off		
		Manage/Error F	Files 🗆		
		Error Files Size		Megabyte	
		Error Files Cour	nt 65536	$\diamond$	
		Error Files Redu %		٥	
		Manage Saved	Files		
		cel OK Saved Files Size	a 100	Megabyte	
		Saved Files Cou	unt 65536	0	

**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.