

RSA NetWitness Logs

Event Source Log Configuration Guide



RSA Federated Identity Manager

Last Modified: Friday, April 14, 2017

Event Source Product Information:

Vendor: [RSA, The Security Division of EMC](#)

Event Source: Federated Identity Manager

Versions: 4.1

Additional Download: [sftpagent.conf.rsafim](#)

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: rsafim

Collection Method: File

Event Source Class.Subclass: Security.Access Control

To configure RSA FIM, you must complete the following tasks:

- 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 SA SFTP Agent shell script](#)

Configure the Log Collector for File Collection

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

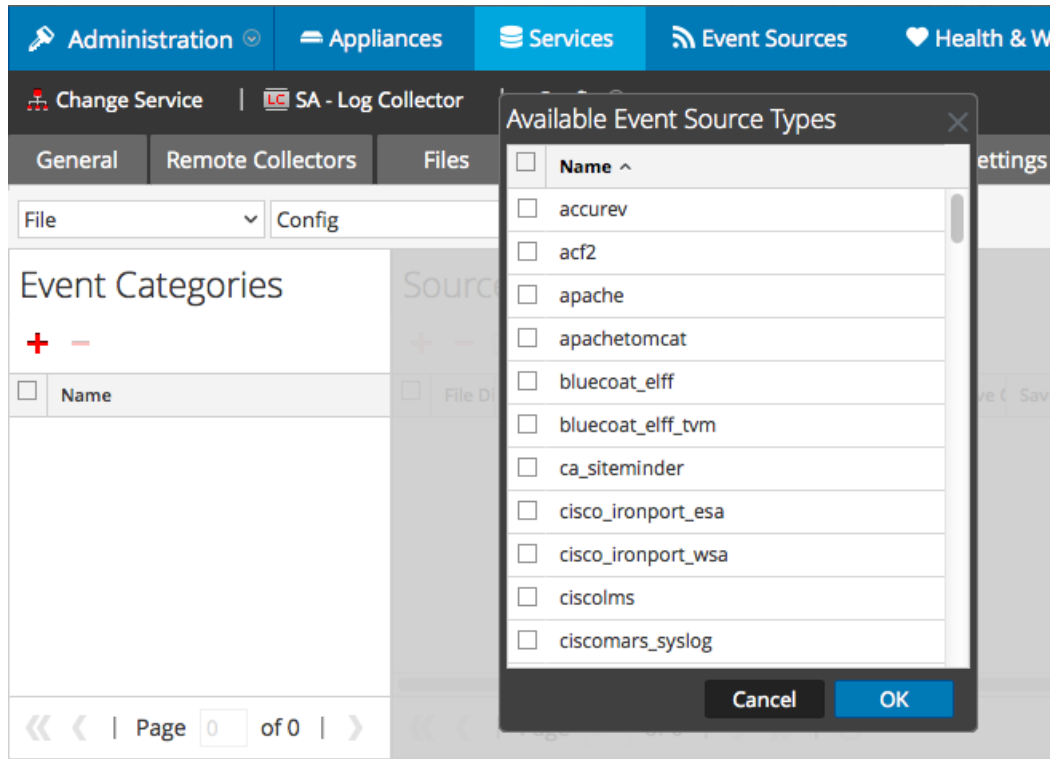
To configure the Log Collector for file collection:

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 **+**.

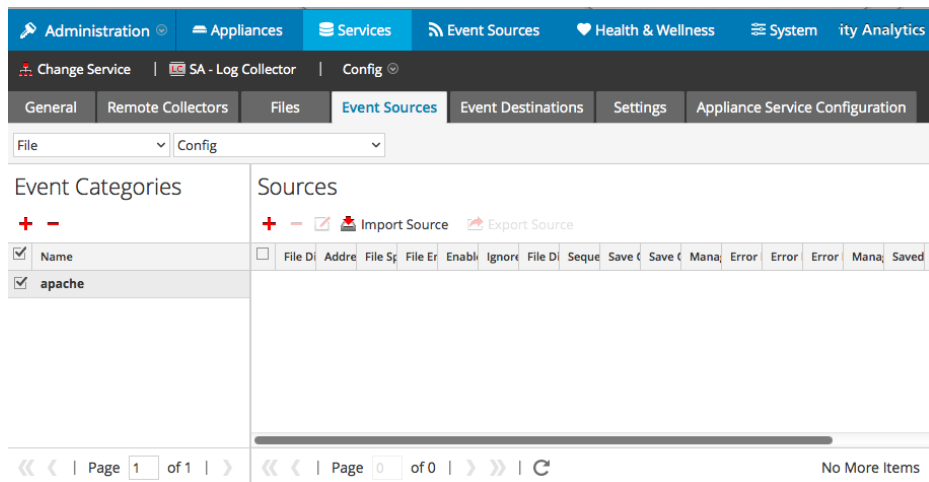
The Available Event Source Types dialog is displayed.



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

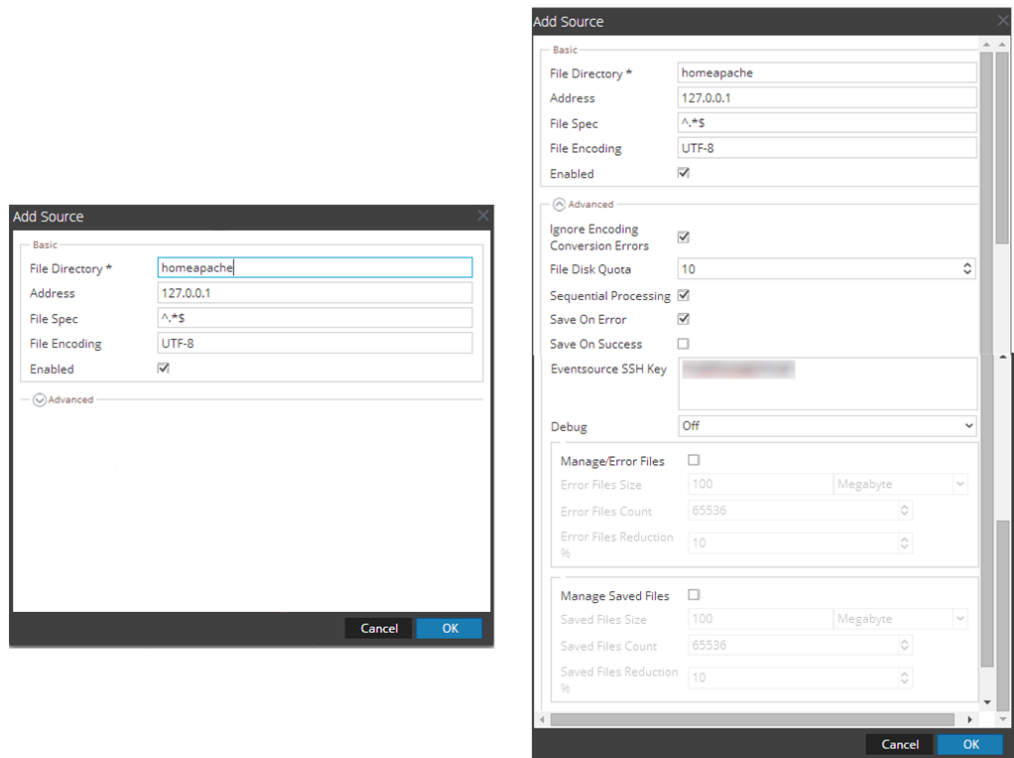
Select **rsafim** from the **Available Event Source Types** dialog.

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



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. 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 © 2017 EMC Corporation. All Rights Reserved.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.