RSA NetWitness Logs

Event Source Log Configuration Guide

Secude Security Intelligence

Last Modified: Wednesday, October 18, 2017

Event Source Product Information:

Vendor: SECUDE
Event Source: Security Intelligence
Versions: 1.0
Additional Download: sftpagent.conf.secudesi

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: secudesi
Collection Method: File
Event Source Class.Subclass: Security.Analysis

To configure Secude Security Intelligence as an event source, perform the following tasks:

I. Set Up Security Intelligence Logging Directories for RSA NetWitness Suite

II. Set up the SFTP Agent

III. Configure the Log Collector for File Collection

Set Up Security Intelligence Logging Directories

Warning: You must install the latest SECUDE Security Intelligence installation packages, which include the RSA connector. The RSA connector is part of the installation package, and any patch or upgrade. Existing SECUDE Security Intelligence customers can download the latest version of the RSA connector as part of the Security Intelligence installation package through a download link that will be provided by the SECUDE sales team.

To configure logging directories:

1. Log on to the SAP System on the C-BUS Server.
2. For the transaction code, type **/SECUDE/CBUS**.
3. Click the **Applications** tab.
4. From the **Application Type** drop-down list, select **RSA**.
5. Select the application types on which you want to report, and click **Configuration** > **Detect Environment**.
6. Complete the fields as follows.

Field	Action
Path	Enter the path to the directory where you want Security Intelligence to store the logs.
Filename	Specify a file for Security Intelligence to create log messages.

Note: If you leave the path blank or set to **Initial**, SECUDE will write logs into the directory according to the directory parameter, **DIR_HOME**.

7. Click the **Applications** tab.

8. Click **Configuration** > **Deactivate Application Types**.

   A dialogue box opens, showing the list of supported application types to deactivate.

9. Ensure that each application type on which you want to report is ***not*** set to deactivated. RSA NetWitness Suite supports the following application types:

   - **CHANGEDOC**
   - **HEARTBEAT**
   - **SAL**
   - **SYSLOG**
   - **SYSPAR**
   - **TABLELOGS**
   - **TABLES**
   - **TRANSPORT**

   > **Warning:** For each "Application Type – RSA" pair, you need a time stamp initialization. For more information on how to configure time stamp initialization, see the *SECUDE Installation and Administration Guide*.

   > **Note:** You can add filters to select or clear certain parameters, depending on each application type. For more information on how to configure filters, see the *SECUDE Installation and Administration Guide*.

10. (Optional) Select which publishers publish logs. For more information on how to configure publishers, see the *SECUDE Installation and Administration Guide*.

11. Click **Configuration** > **Save**.

Set Up SFTP and Configure the Log Collector

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.

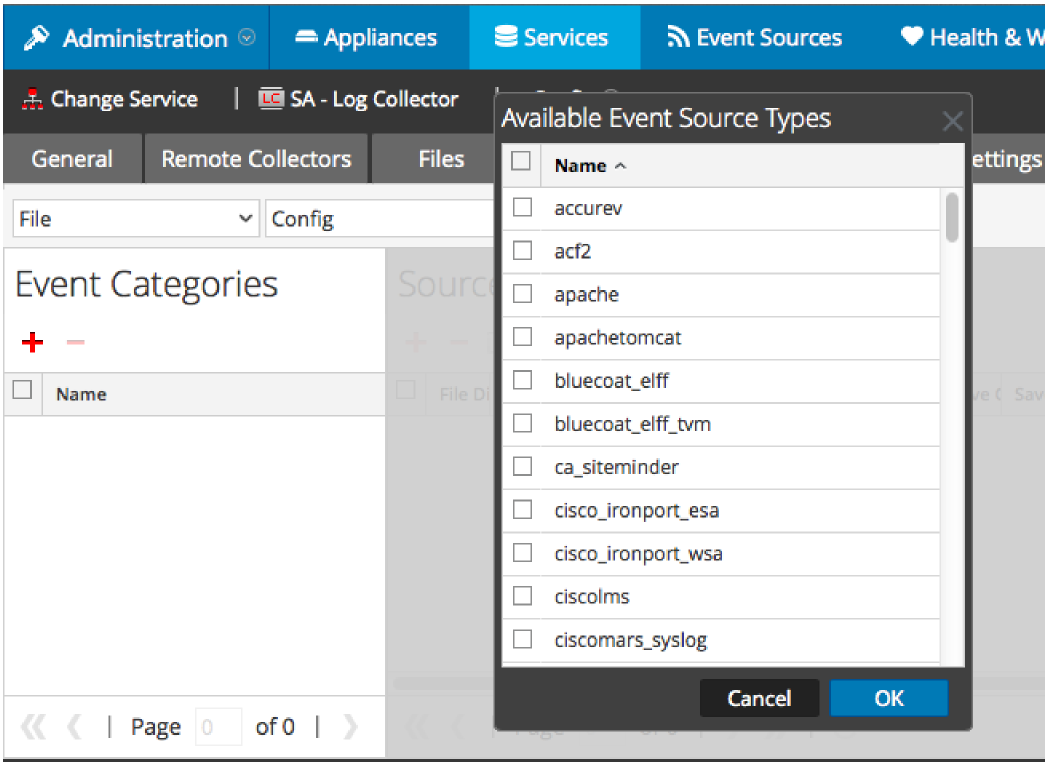
To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **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.

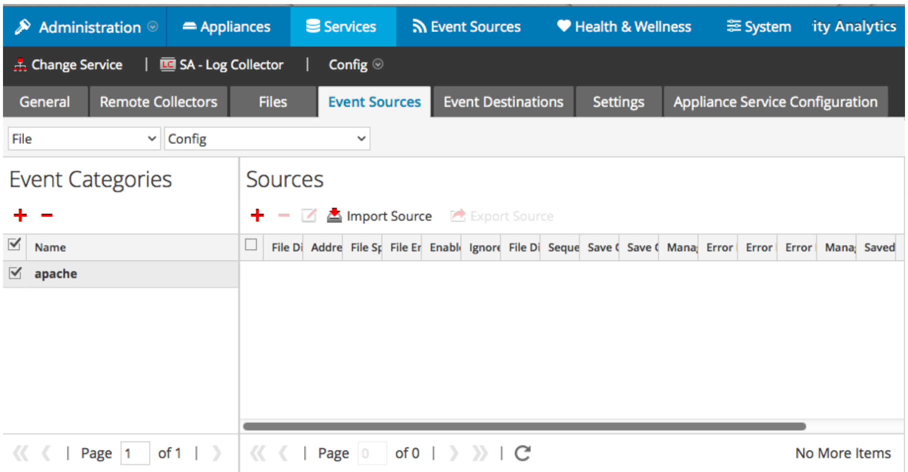


5. Select the correct type from the list, and click **OK**.

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

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

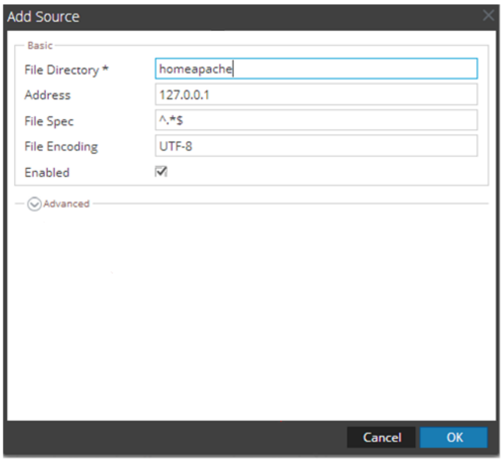
Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



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.



Add Source

Basic

File Directory *: homeapache

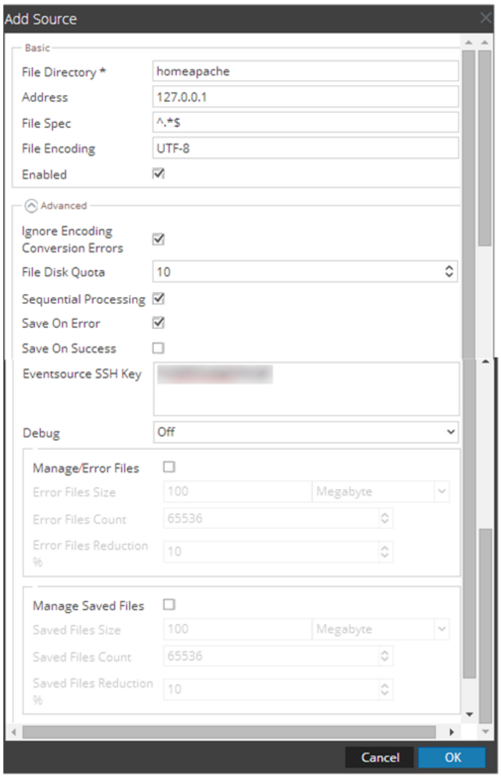
Address: 127.0.0.1

File Spec: ^.*$

File Encoding: UTF-8

Enabled: ☑

Advanced



Add Source

Basic

File Directory *: homeapache

Address: 127.0.0.1

File Spec: ^.*$

File Encoding: UTF-8

Enabled: ☑

Advanced

Ignore Encoding Conversion Errors: ☑

File Disk Quota: 10

Sequential Processing: ☑

Save On Error: ☑

Save On Success: □

Eventsource SSH Key: [redacted]

Debug: Off

Manage/Error Files: □

Error Files Size: 100 Megabyte

Error Files Count: 65536

Error Files Reduction %: 10

Manage Saved Files: □

Saved Files Size: 100 Megabyte

Saved Files Count: 65536

Saved Files Reduction %: 10

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.

Trademarks