RSA NetWitness Logs

Event Source Log Configuration Guide

Cisco Secure IDS or IPS

Last Modified: Wednesday, October 4, 2017

Event Source Product Information:

Vendor: Cisco
Event Source: Secure Intrusion Prevention System (IPS)
Versions: 4.x, 5.0, 5.1, 6.0, 6.1, 6.2, 7.x

> **Note:** RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

Signature Engines: E1, E2, E3, E4

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: ciscoidsxml
Collection Method: SDEE
Event Source Class.Subclass: Security.IDS

Configure Secure Cisco IDS/IPS

To set up Cisco Secure IDS or IPS to work with RSA NetWitness Suite, perform the following tasks:

I. Configure Cisco Secure IDS/ IPS

II. Configure the Log Collector for SDEE Collection

Configure the Cisco Secure IDS/IPS event source

Configure RSA NetWitness Suite to access the sensor, apply an access list to the sensor.

On the Cisco Secure IDS/IPS event source, follow these steps:

1. Log on to the Cisco Secure IDS/IPS console, using administrative credentials.
2. Type the following commands:

   ```
   configure terminal
   service host
   network-settings
   ```

3. Use the access-list command to allow RSA NetWitness Suite to access the sensor. Type the following commands:

   ```
   access-list IP address of the RSA NetWitness Suite Log Collector
   ```

   For example, to allow a host access, type **access-list 1.2.3.4/32**, or to allow a network access, type **access-list 1.2.3.0/24**.

4. Exit the configuration mode, confirming to save changes when prompted

Configure the Log Collector for SDEE Collection

You should configure the Log Collector for SDEE collection.

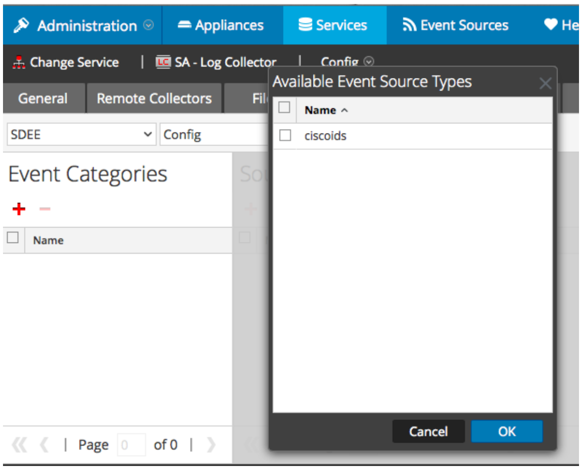
To configure the Log Collector for SDEE collection:

1. In the Security Analytics 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 **SDEE/Config** from the drop-down menu.

   The Event Categories panel displays the SDEE event sources that are configured, if any.

4. In the Event Categories panel toolbar, click +.

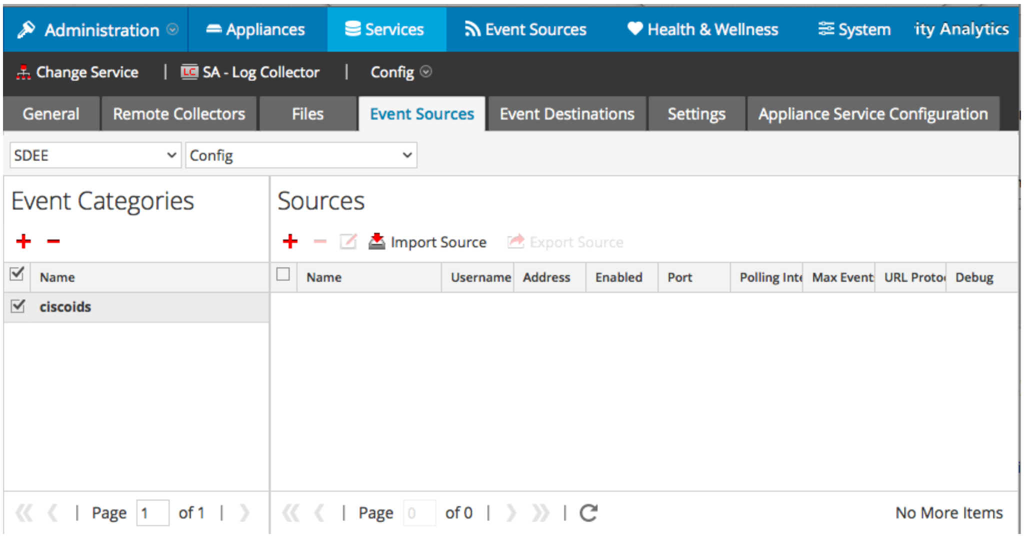
The Available Event Source Types dialog is displayed.



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

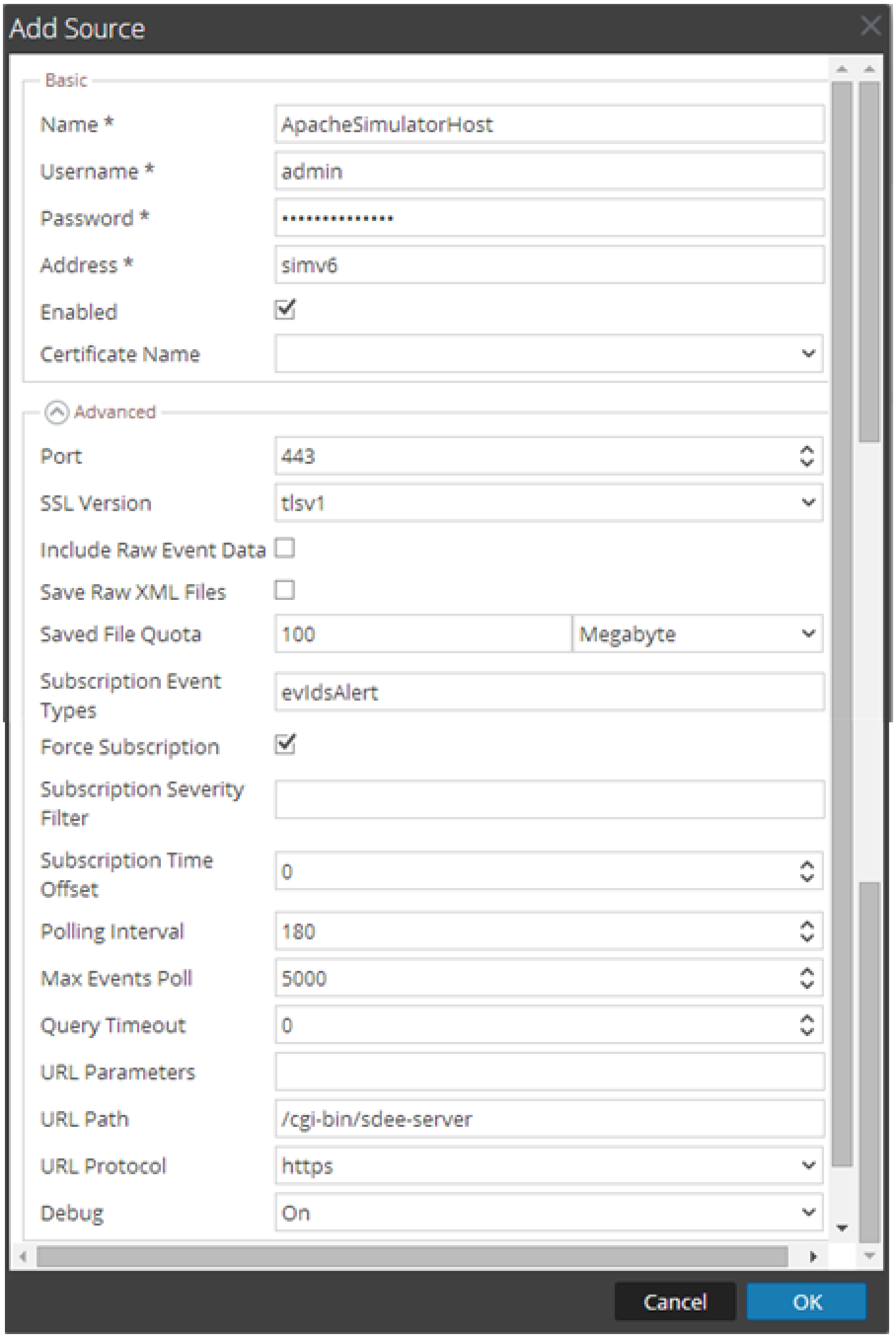
5. Select the correct type from the list, and click **OK**.

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.



Add Source

Basic

Name *	ApacheSimulatorHost
Username *	admin
Password *	•••••••••••••••
Address *	simv6
Enabled	☑
Certificate Name	

Advanced

Port	443
SSL Version	tlsv1
Include Raw Event Data	□
Save Raw XML Files	□
Saved File Quota	100 Megabyte
Subscription Event Types	evIdsAlert
Force Subscription	☑
Subscription Severity Filter	
Subscription Time Offset	0
Polling Interval	180
Max Events Poll	5000
Query Timeout	0
URL Parameters	
URL Path	/cgi-bin/sdee-server
URL Protocol	https
Debug	On

7. Add a Name, Username, Address, and Password, and modify any other parameters that require changes, and click **OK**.

Trademarks