RSA NetWitness Logs

Event Source Log Configuration Guide

Airtight Management Console

Last Modified: Thursday, May 04, 2017

Event Source Product Information:

Vendor: AirTight
Event Source: Airtight Management Console
Versions: 7.0, 7.1 U4
Platforms: Linux / CentOS 6.7

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: airtightmc
Collection Method: Syslog
Event Source Class.Subclass: Security.Intrusion

Configure Airtight Management Console

This document contains the following sections:

I. About Airtight Management Console

II. Configure the Airtight Management Console Event Source

III. Configure RSA NetWitness Suite for Syslog Collection

About Airtight Management Console

Airtight Management Console is an end-to-end wireless intrusion prevention solution, It blocks wireless threats by automatically scanning, detecting and classifying all unauthorized access and rogue traffic to your network. Airtight Management Console Enterprise provides performance management and knowledge-based troubleshooting features that allow analysis and resolution of remote wireless network issues from a central location.

By integrating with RSA NetWitness Suite, SGE log activity can be used in an effective security log management solution for real-time alerting, correlated rules and events, and scheduled reporting.

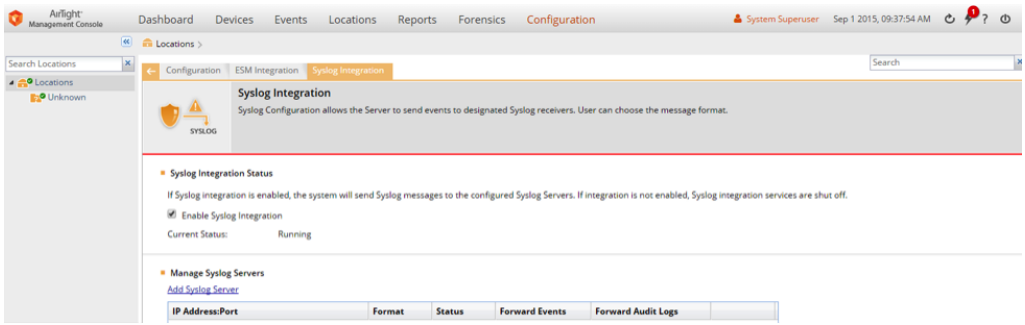
Configure the Airtight Management Console Event Source

The Airtight Management Console should be configured to send syslog events to RSA NetWitness Suite. For detailed description of the Airtight Management Console user interface, please refer to the *Airtight Management Console User Guide*.

To configure Airtight Management Console:

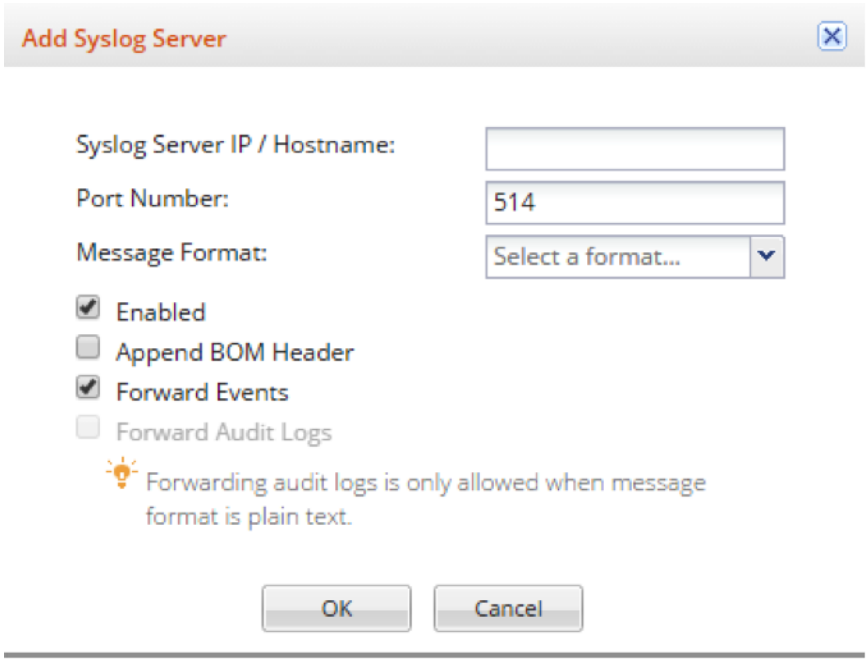
1. Log onto the Airtight Management Console UI as a user with administrator privileges.
2. Select **Configuration**
3. Select **ESM Integration**.
4. Select **Syslog**.

   The Syslog Configuration screen displays.



5. Examine the following parameters:
   - **Syslog Integration Status:** Ensure that this parameter is checked. When selected, the system sends messages to the configured Syslog Servers. Otherwise, Syslog integration services are shut-off and you cannot manage the Syslog Servers.
   - **Current Status:** Ensure that the status is **Running**. If the service is currently stopped, you must start it.
6. Under **Manage Syslog Servers**, click **Add**.

   The Syslog Configuration screen displays.



7. Fill in the screen as follows:
   - **Syslog Server (IP Address or Hostname)**: enter the IP address of your RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.

- **Port Number**: accept the default value, 514.
- **Message Format**: select Plain text.
- **Enabled**: ensure this parameter is selected.
- **Forward Events**: ensure this parameter is selected.

8. Click **Add** to complete the configuration.

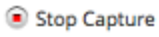
Configure RSA NetWitness Suite for Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **System**.
3. Depending on the icon you see, do one of the following:
   - If you see 

, click the icon to start capturing Syslog.
   - If you see 

, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

   The Event Categories panel displays the Syslog 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 either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Trademarks