NetWitness® Platform

Airtight Management Console Event Source Configuration Guide

NETWITNESS
Platform

Airtight Management Console

Last Modified: Monday, December 2, 2024

Event Source Product Information:

Vendor: AirTight

Event Source: Airtight Management Console

Versions: 7.0, 7.1 U4, 7.4

Platforms: Linux / CentOS 6.7

NetWitness Product Information:

Supported On: NetWitness Platform 12.3 and later

Event Source Log Parser: airtightmc

Collection Method: Syslog

Event Source Class.Subclass: Security.Intrusion

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Miscellaneous

November 2024

Contents

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 Platform 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 Platform, SGE log activity can be used in an effective security log management solution for real-time alerting, correlated rules and events, and scheduled reporting.

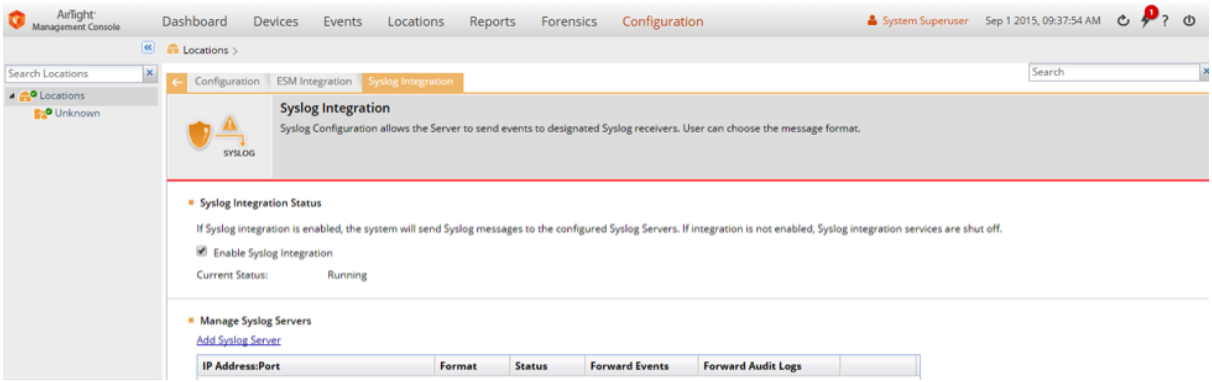
Configure the Airtight Management Console Event Source

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

To configure Airtight Management Console:

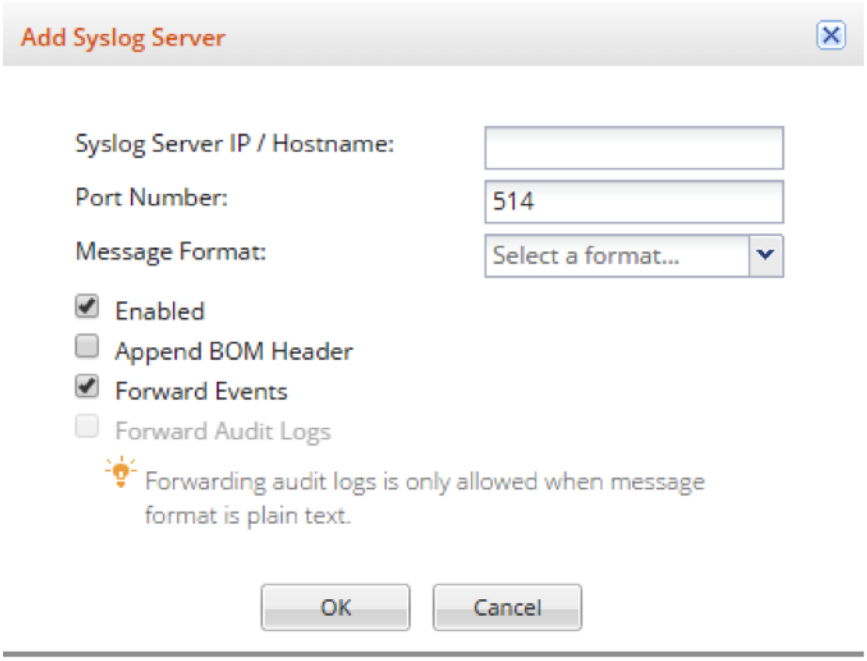
1. Log onto the Airtight Management Console UI as a user with administrator privileges.
2. Select **Configuration**
3. Select **ESM Integration**.
4. Select **Syslog**.

   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 Platform Log Decoder or RSA NetWitness Platform 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 Platform 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 only need to configure either the Log Decoder or the Remote Log Collector for Syslog, not both.

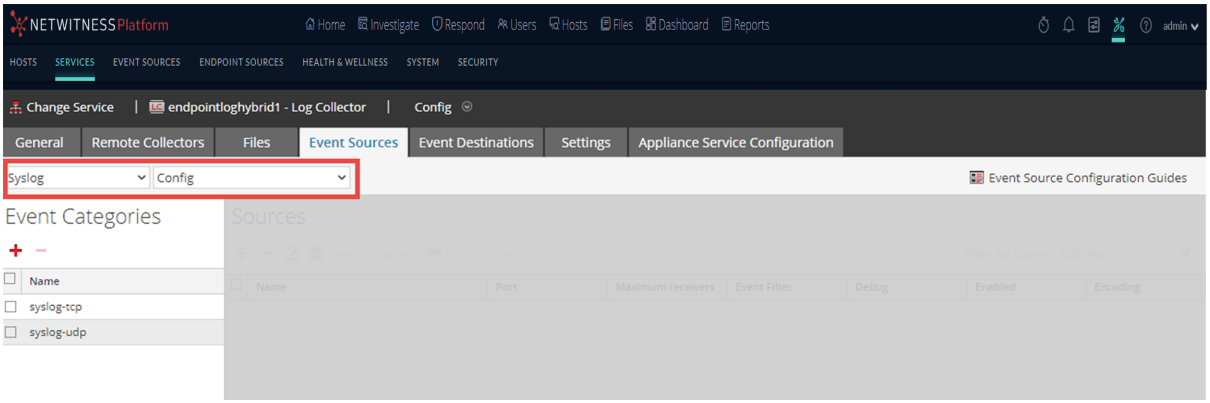
To configure Log Decoder for Syslog Collection

1. In the NetWitness Platform menu, select (Admin) > **Services**.
2. In the **Services** grid, choose 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 Start Capture , click the icon to start capturing Syslog.
   - If you see Stop Capture , you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure Remote Log Collector for Syslog Collection

1. In the NetWitness Platform menu, go to (Admin) > **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.

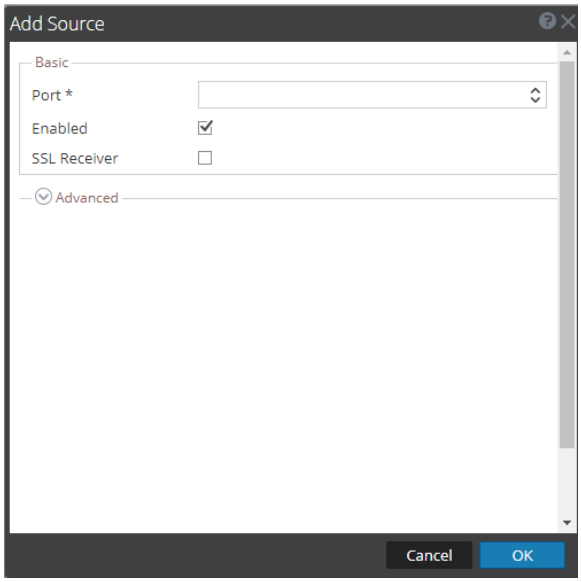


4. In the **Event Categories** panel toolbar, click +.

   The **Available Event Source Types** dialog will appear.
5. Choose either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.

6. Choose the **New Type** in the **Event Categories** panel and click + in the **Sources** panel toolbar.

   The **Add Source** dialog will appear.



7. Enter **514** for the port and choose **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

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

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

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.