

RSA NetWitness Logs

Event Source Log Configuration Guide



Blue Coat ProxyAV

Last Modified: Friday, May 05, 2017

Event Source Product Information:

Vendor: [Blue Coat Systems](#)

Event Source: ProxyAV

Versions: 3.3.1.2, 3.5.1.1

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: bluecoatproxyav

Collection Method: Syslog, SNMP

Event Source Class.Subclass: Security.Antivirus

Configure Blue Coat ProxyAV

ProxyAV appliances work in tandem with Blue Coat ProxySG appliances and support anti-malware engines. As an inline scanning device, the ProxyAV appliance analyzes file downloads from Web 2.0 sites, web mail, file sharing and other methods of content delivery.

To configure Blue Coat ProxyAV to work with RSA NetWitness Suite, you must complete the following tasks:

- I. [Configure ProxyAV for Syslog](#)
- II. [Configure ProxyAV for SNMP](#)

Note: Blue Coat ProxyAV logs some events in Syslog format, and others in SNMP traps, so you must configure both formats to send all events to the RSA NetWitness Suite platform.

Configure Blue Coat ProxyAV for Syslog

This section describes how to configure ProxyAV to send system logs, in Syslog format, to the RSA NetWitness Suite platform. To configure Syslog collection for the Blue Coat ProxyAV you must:



- I. Configure RSA NetWitness Suite for Syslog Collection
- II. Configure Syslog Output on Blue Coat ProxyAV

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  **Start Capture**, 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.

Configure Syslog Output on Blue Coat ProxyAV

To configure ProxyAV to send Syslog events to the RSA NetWitness Suite:

1. On the ProxyAV event source, open the Blue Coat ProxyAV Management Console.
2. From the left-hand navigation pane, click **Log Files**.

- In the Logging section, fill in the fields as follows.

Field	Details
Enable sending logging information to remote computer	Select this option.
Connection logs	Select this option.
Audit logs	Select this option.
Use syslog protocol	Select this option.
Address	Specify the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Port	Type 514 .
Protocol	Select UDP
Choose logging format.	From the drop-down list, select User Defined .
Include W3C headers	Leave this selection unchecked.
Delimiter	Select Comma
Log Format	Select User Defined .
Format String	Enter the following string (remove any newline characters): <code>cs-protocol sc-bytes cache date time time-taken c-dns c-ip c-username s-dns s-ip s-port s-sitename cs-bytes cs-method sc-mimetype sc-status cs(User-Agent) cs-uri cs-uri-stem cs-uri-query</code>

- Click **Save Changes**.

Configure ProxyAV for SNMP


This section describes how to configure ProxyAV to send virus details, in SNMP format, to the RSA NetWitness Suite platform. To configure SNMP collection for the Blue Coat ProxyAV you must:

- I. Configure SNMP Event Sources on the RSA NetWitness Suite platform:
 - i. Add the SNMP Event Source Type
 - ii. Configure SNMP v3 Users
- II. Configure SNMP Output on Blue Coat ProxyAV

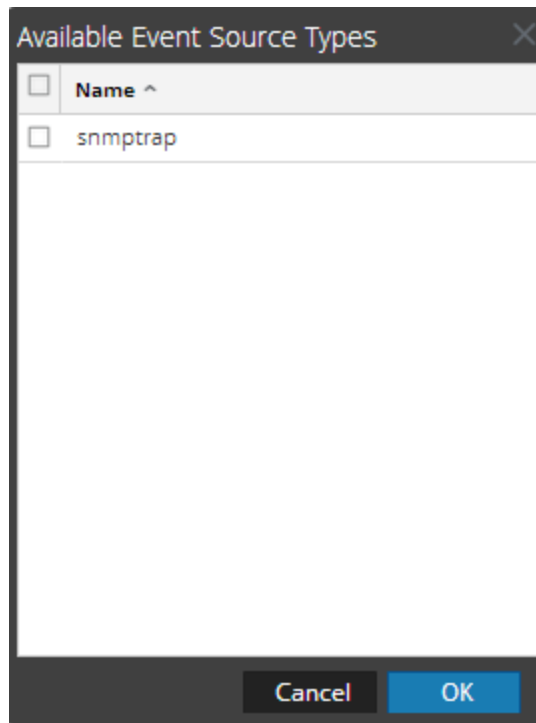
Add the SNMP Event Source Type

Note: If you have previously added the `snmptrap` type, you cannot add it again. You can edit it, or manage users.

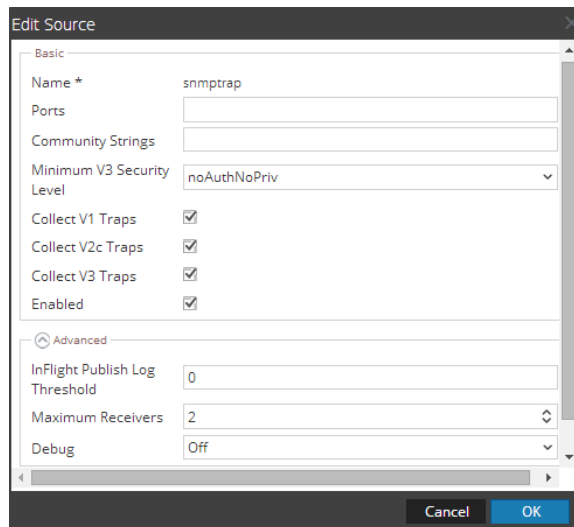
Add the SNMP Event Source Type:

1. In the **RSA NetWitness Suite** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

The Sources panel is displayed with the existing sources, if any.
5. Click **+** to open the **Available Event Source Types** dialog.



6. Select **snmptrap** from the Available Event Source Types dialog and click **OK**.
7. Select **snmptrap** in the Event Categories panel.
8. Select **snmptrap** in the Sources panel and then click the Edit icon to edit the parameters.




9. Update any of the parameters that you need to change.

(Optional) Configure SNMP Users

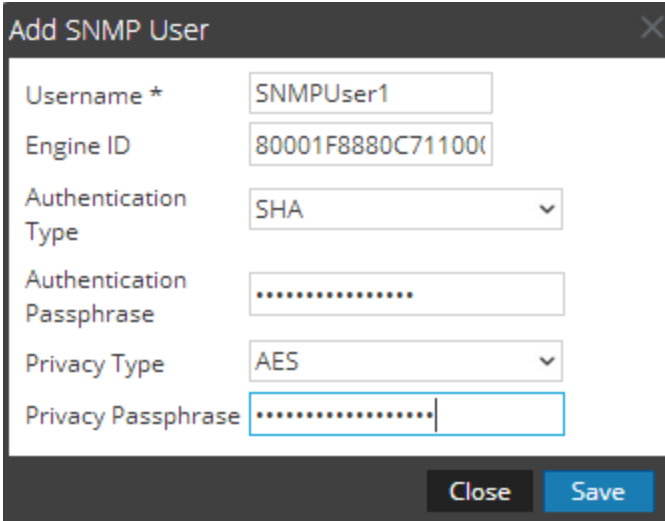
If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

Configure SNMP v3 Users

1. In the **RSA NetWitness Suite** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/SNMP v3 User Manager** from the drop-down menu.

The SNMP v3 User panel is displayed with the existing users, if any.

5. Click **+** to open the **Add SNMP User** dialog.



The screenshot shows the 'Add SNMP User' dialog box with the following fields and values:

Field	Value
Username *	SNMPUser1
Engine ID	80001F8880C71100
Authentication Type	SHA
Authentication Passphrase
Privacy Type	AES
Privacy Passphrase

6. Fill in the dialog with the necessary parameters. The available parameters are described below..

SNMP User Parameters

The following table describes the parameters that you need to enter when you create an SNMP v3 user.

Parameter	Description
Username *	<p>User name (or more accurately in SNMP terminology, security name). RSA NetWitness Suite uses this parameter and the Engine ID parameter to create a user entry in the SNMP engine of the collection service.</p> <p>The Username and Engine ID combination must be unique (for example, logcollector).</p>
Engine ID	<p>(Optional) Engine ID of the event source. For all event sources sending SNMP v3 traps to this collection service, you must add the username and engine id of the sending event source.</p> <p>For all event sources sending SNMPv3 informs, you must add just the username with a blank engine id.</p>
Authentication Type	<p>(Optional) Authentication protocol. Valid values are as follows:</p> <ul style="list-style-type: none"> • None (default) - only security level of noAuthNoPriv can be used for traps sent to this service • SHA - Secure Hash Algorithm • MD5 - Message Digest Algorithm
Authentication Passphrase	<p>Optional if you do not have the Authentication Type set. Authentication passphrase.</p>
Privacy Type	<p>(Optional) Privacy protocol. You can only set this parameter if Authentication Type parameter is set. Valid values are as follows:</p> <ul style="list-style-type: none"> • None (default) • AES - Advanced Encryption Standard • DES - Data Encryption Standard
Privacy Passphrase	<p>Optional if you do not have the Privacy Type set. Privacy passphrase.</p>
Close	<p>Closes the dialog without adding the SNMP v3 user or saving modifications to the parameters.</p>
Save	<p>Adds the SNMP v3 user parameters or saves modifications to the parameters.</p>

Configure SNMP Output on Blue Coat ProxyAV

To configure ProxyAV to send SNMP events to the RSA NetWitness Suite platform:

1. On the ProxyAV event source, open the Blue Coat ProxyAV Management Console.
2. From the left-hand navigation pane, click **Advanced**.
3. In the Logging section, fill in the fields as follows.

Field	Details
Enable SNMP	Select this option.
SysLocation SysContact	Fill in these fields with any values that you like.
Trap Community Verify Trap Community	Type public in both fields
Interface	Select Interface 0
Send Traps To	Specify the IP address of the RSA NetWitness Suite Log Collector.
Enable Authentication Traps	Select this option
Enable Diagnostics	Selecting this field is optional. Note, however, that selecting this field decreases performance.
SNMP Version	Select SNMPV2
Read Comment Verify Read Comment	Type public in both fields

4. Click **Save Changes**.

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.