

RSA NetWitness Logs

Event Source Log Configuration Guide



BeyondTrust Powerbroker Endpoint Protection Platform

Last Modified: Wednesday, October 18, 2017

Event Source Product Information:

Vendor: [BeyondTrust](#)

Event Source: Powerbroker Endpoint Protection Platform (formerly branded as eEye Blink Endpoint Protection)

Versions: 4.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.

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: eeyeblink

Collection Method: SNMP

Event Source Class.Subclass: Security.Intrusion

To configure the BeyondTrust Powerbroker Endpoint Protection Platform event source, perform the following tasks:

- I. Configure SNMP Output on BeyondTrust Powerbroker Endpoint Protection Platform
- II. Configure RSA NetWitness Suite for SNMP Collection

Configure SNMP Output on BeyondTrust Powerbroker Endpoint Protection Platform

The following procedure describes how to configure SNMP output on your device.

To configure collection through SNMP for BeyondTrust Powerbroker Endpoint Protection Platform:

1. Log on to BeyondTrust Powerbroker Endpoint Protection Platform with your administrator credentials.
2. Click **Tools > Options**.
3. In the Options and Settings window, click the **Events** tab.
4. In the **SNMP Manager** field, complete the fields as follows

Field	Action
Enable	Type Yes .
Address	Enter the IP address of your RSA NetWitness Suite Log Collector.
SNMP Version	Make sure the version number is SNMPv1 .

5. Click **OK**.

Configure SNMP Event Sources on NetWitness Suite

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.


Note: The required parser is **eeyeblink**.

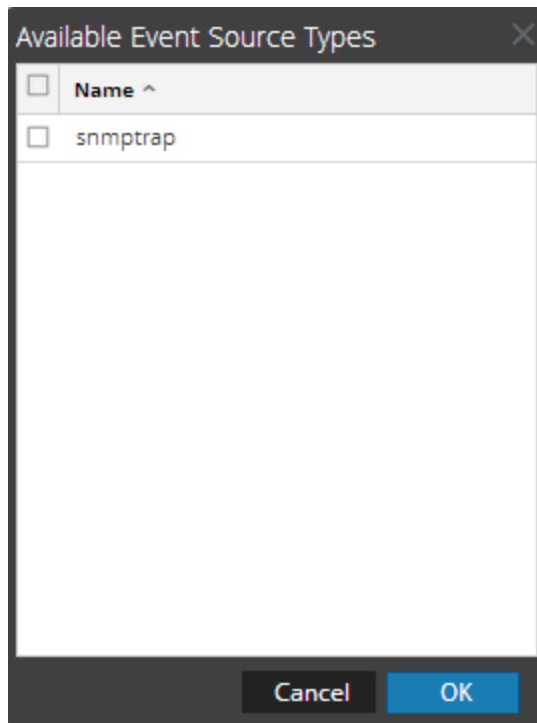
The first time that you configure an SNMP event source on RSA NetWitness Suite, you need to add the SNMP event source type and configure SNMP users.

Add the SNMP Event Source Type

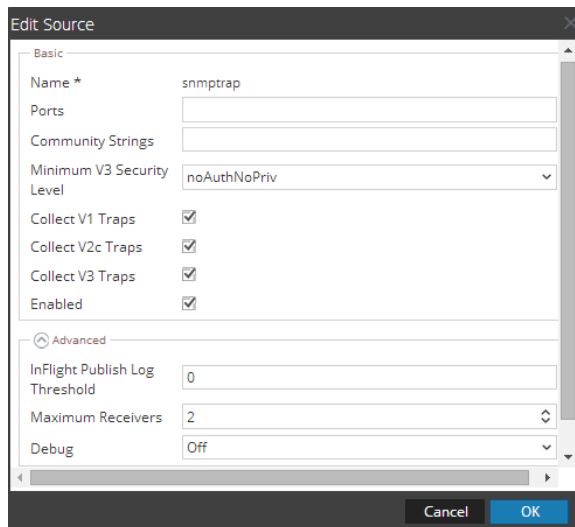
Note: If you have previously added the **snmptrap** type, you cannot add it again. You can edit it, or manage users.

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

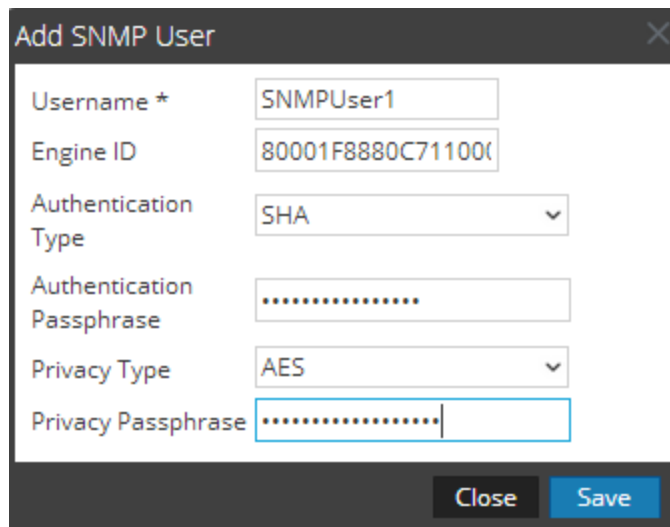
If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

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.



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>

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.