

# RSA NetWitness Logs

## Event Source Log Configuration Guide



## Riverbed Cascade Profiler

Last Modified: Wednesday, May 03, 2017

### Event Source Product Information:

**Vendor:** [Riverbed](#)

**Event Source:** Cascade Profiler (formerly known as Mazu Profiler)

**Note:** Support includes Riverbed Cascade Express, which is a combination of Cascade Profiler, Cascade Gateway, and Cascade Sensor.

**Versions:** 5.5.2, 6.0, 7.0, and 9.5.1

### RSA Product Information:

**Supported On:** NetWitness Suite 10.0 and later

**Event Source Log Parser:** mazuprofiler

**Collection Method:** SNMP

**Event Source Class.Subclass:** Security.IPS

Mazu Profiler has been rebranded as Riverbed Cascade Profiler. This includes Riverbed Cascade Express, which is a combination of three products: Riverbed Cascade Profiler, Riverbed Cascade Gateway, and Riverbed Cascade Sensor.

To configure SNMP collection for this event source, perform the following tasks:

- I. Configure Riverbed Cascade for SNMP Collection
- II. Configure SNMP Event Sources on RSA NetWitness Suite

## Configure Riverbed Cascade for SNMP Collection

---

Depending on your event source, perform one of the following tasks:

- Configure Riverbed Cascade Profiler, or
- Configure Mazu Profiler

### Configure Riverbed Cascade Profiler

**To configure Riverbed Cascade Profiler:**

1. Log on to the Riverbed Cascade Profiler web administration page with administrative credentials.
2. From the menu, select **Behavior Analysis > Notifications**.
3. Click the **Recipients** tab.
4. To add RSA NetWitness Suite as the default recipient, under the **Actions** column, click **Edit**. In the Edit Recipients window, follow these steps:

**Note:** To use RSA NetWitness Suite as a new recipient instead of the default, see the Riverbed Profiler documentation for creating new recipients, and complete the steps as follows.

- a. (Optional) In the **Recipient Label** field, enter a desired name.
- b. In the Email Recipient section, leave the default settings.

- c. In the SNMP Trap Recipient section, set the field values as follows:

Field	Action
<b>Destination IP 1</b>	Enter the IP address of RSA NetWitness Log Collector.
<b>Port 1</b>	Type <b>162</b> .
<b>SNMP Version</b>	Select <b>v1</b> .
<b>SNMP Community (read)</b>	Type <b>public</b> .

- d. Click **OK**.

## Configure Mazu Profiler

### To configure Mazu Profiler:

1. Log on to the Mazu Profiler web administration page with administrator credentials.
2. From the menu, select **Settings > Notifications**.
3. Click on the **Basic** tab and type the following values in the SNMP section:
  - IP Address: the IP address of RSA NetWitness Log Collector
  - Port: **162**
  - Type: **V1**
4. Click **Apply**.

## Configure SNMP Event Sources on RSA NetWitness Suite

---


To configure SNMP event sources on RSA NetWitness Suite, perform the following tasks:

- I. Add the SNMP Event Source Type
- II. Configure SNMP v3 Users

### Add the SNMP Event Source Type

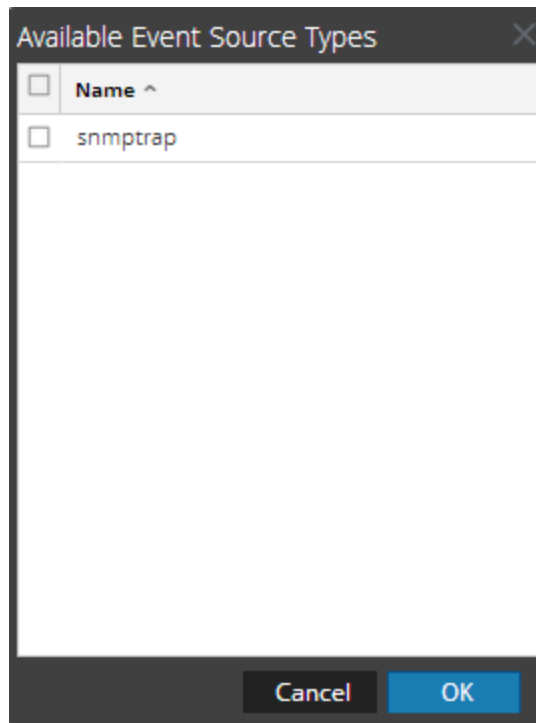
**Note:** If you have previously added the `snmptrap` type, you cannot add it again. You can edit it, or manage users.

#### Add the SNMP Event Source Type:

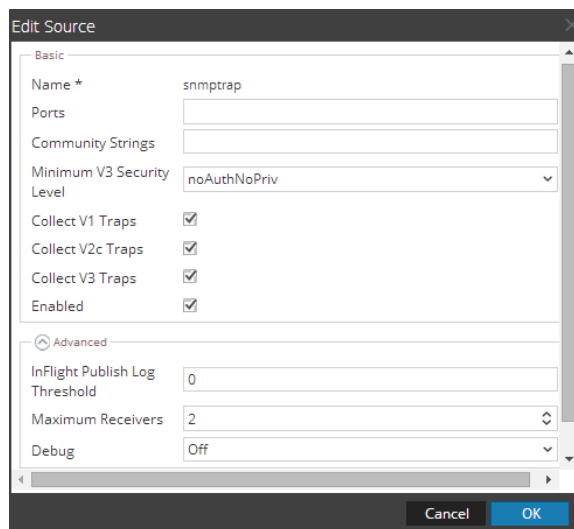
1. In the **RSA NetWitness Suite** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

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

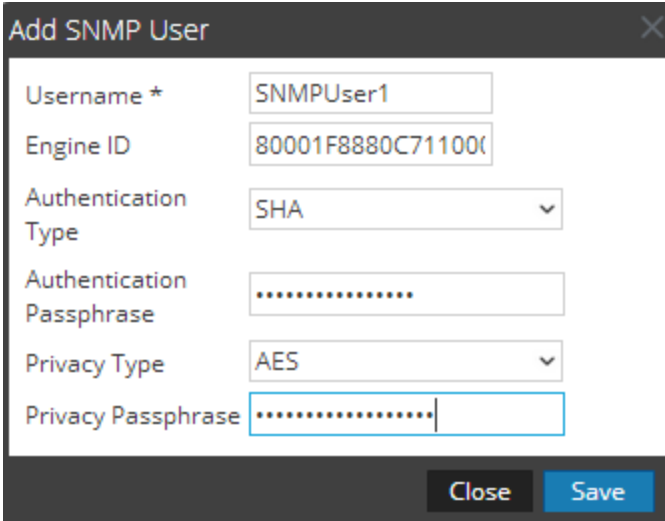
If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

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