

RSA NetWitness Logs

Event Source Log Configuration Guide



Trend Micro Server Protect

Last Modified: Thursday, July 20, 2017

Event Source Product Information:

Vendor: [Trend Micro](#)

Event Source: Server Protect

Version: 5.8

Platforms: EMC Celerra and Windows Servers

Additional Download: trendmicro_log_format.txt

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: trendmicrosp

Collection Method: SNMP

Event Source Class.Subclass: Security.Antivirus

To configure Trend Micro Server Protect, you must complete these tasks:

- Configure Trend Micro Server Protect
- Configure SNMP Event Sources on RSA NetWitness Suite

Configure Trend Micro Server Protect to send SNMP

To configure Trend Micro Server Protect:

1. Log on to the Trend Micro Server Protect console with administrative credentials.
2. From the navigation pane, click **Set Notification**.
3. Click **Standard Alert**.
4. Ensure that every alert type is selected, and follow these steps:
 - a. Click **Configure Message** for each alert type.
 - b. For each alert type, replace the default string with the ones available in the **trendmicro_log_format.txt** additional file. You can download the Trend Micro Server Protect additional file from RSA Link here:
<https://community.rsa.com/docs/DOC-58056>.
 - c. Click **OK**.
5. To set the alert method, follow these steps:
 - a. Click **Set Alert Method**.
 - b. Select **SNMP Trap**.


Configure SNMP Event Sources on NetWitness Suite

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

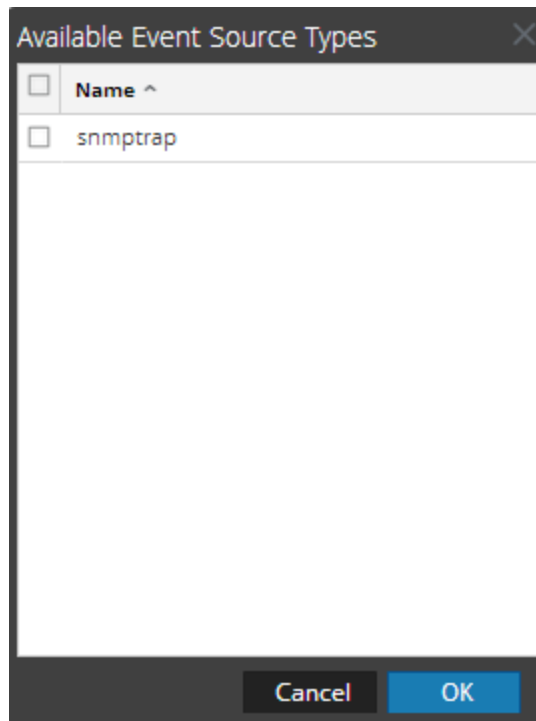
Note: If you have previously added the `snmptrap` type, you cannot add it again. You can edit it, or manage users.

Add the SNMP Event Source Type:

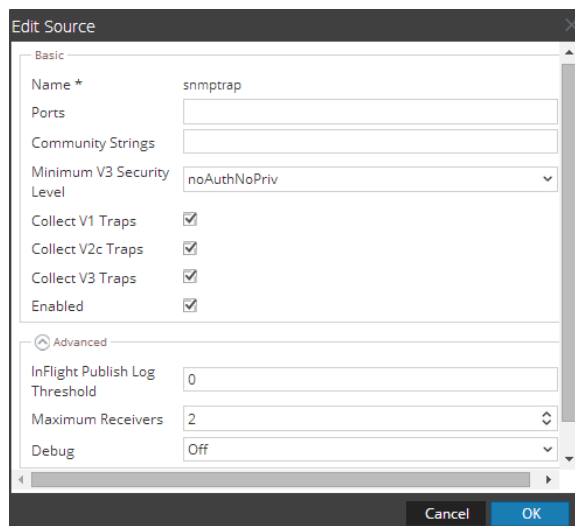
1. In the **RSA NetWitness Suite** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

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

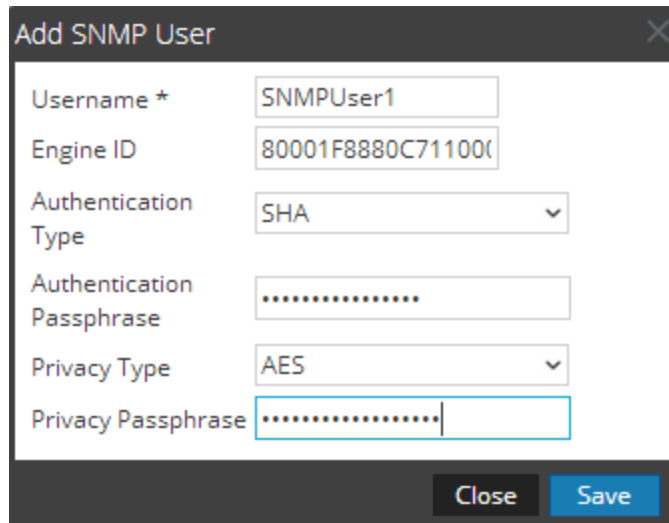
If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

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.



The image shows a dialog box titled "Add SNMP User" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Username ***: A text input field containing "SNMPUser1".
- Engine ID**: A text input field containing "80001F8880C71100".
- Authentication Type**: A dropdown menu with "SHA" selected.
- Authentication Passphrase**: A text input field filled with dots.
- Privacy Type**: A dropdown menu with "AES" selected.
- Privacy Passphrase**: A text input field filled with dots.
- At the bottom right, there are two buttons: "Close" and "Save".

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	Optional if you do not have the Authentication Type set. Authentication passphrase.
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	Optional if you do not have the Privacy Type set. Privacy passphrase.
Close	Closes the dialog without adding the SNMP v3 user or saving modifications to the parameters.
Save	Adds the SNMP v3 user parameters or saves modifications to the parameters.

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.