RSA NetWitness Logs

Event Source Log Configuration Guide

CA Integrated Threat Management

Last Modified: Friday, August 04, 2017

Event Source Product Information:

Vendor: CA

Event Source: Integrated Threat Management

Version: r8, 8.1

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: caitm

Collection Method: SNMP

Event Source Class.Subclass: Security.Antivirus

To configure CA Integrated Threat Management, you must complete these tasks:

- Configure CA Integrated Threat Management
- Configure SNMP Event Sources on RSA NetWitness Suite

Configure CA Integrated Threat Management to send SNMP

To configure CA Integrated Threat Management, you must complete these tasks:

I. Configure the CA Integrated Threat Management Alert Notification

II. Configure the CA Integrated Threat Management Alert Manager

Configure the CA Integrated Threat Management Alert Notification

To configure the Alert Notification:

1. Log on to CA Integrated Threat Management Agent web interface with administrator credentials.
2. On the **Settings** tab, click **Alert Notification**.
3. On the **Alert** tab, confirm the following settings:

Field	Setting
Report to:	**Local Alert Manager** is selected if the Alert Manager is running on the local host. **Forward to Machine** is selected if the Alert Manager is running on a remote host.
Report Criteria	Queue up: 1 Time out after: 1 Skip older than: 30

4. Click **Apply**.
5. On the **Alert Filer** tab, select **Notification by Level of Security**..
6. Select the following:

- Information
- Warning
- Critical

7. Click **Apply**.

Configure the CA Integrated Threat Management Alert Manager

To configure the Alert Manager:

1. Open the CA Alert Manager.
2. Click **My Computer** > **Configuration** > **eTrust ITM** > **SNMP**.
3. Right-click **SNMP**, and select **New Item**.
4. In the SNMP Recipients window, complete the fields as follows.

Field	Action
Manager Name:	Type **NetWitness**.
Send Via:	Type **IP**.
Address:	Enter the IP address of your RSA NetWitness Log Collector.

5. Click **OK**.

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.

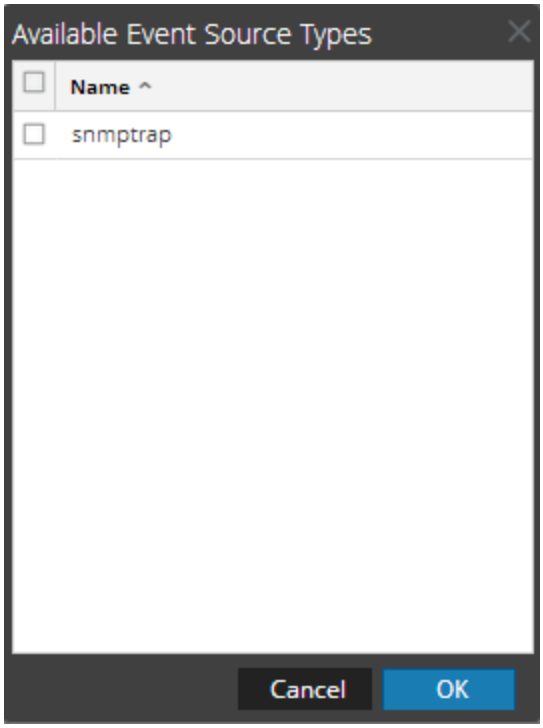
Add the SNMP Event Source Type

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

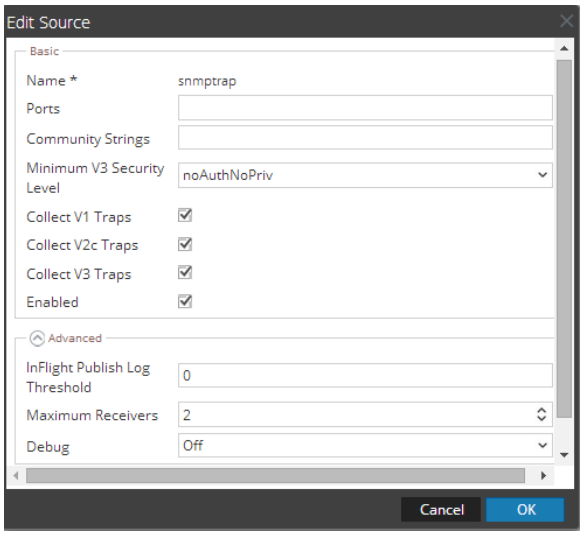
Add the SNMP Event Source Type:

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.

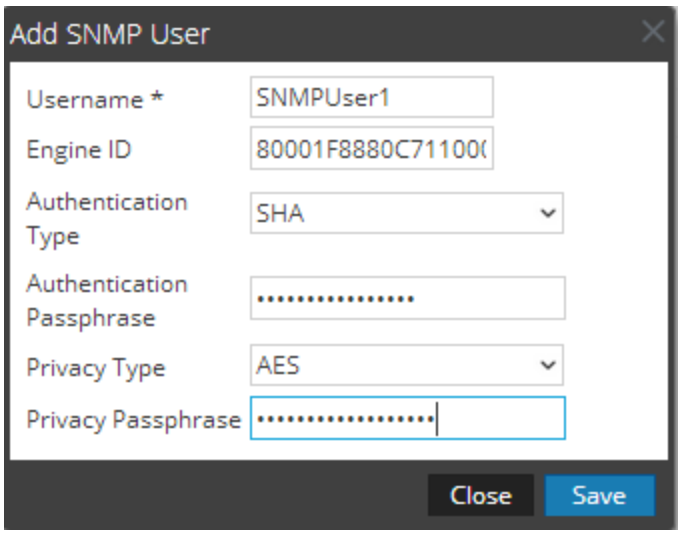
(Optional) Configure SNMP Users

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.



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 *	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. The **Username** and **Engine ID** combination must be unique (for example, **logcollector**).
Engine ID	(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. For all event sources sending SNMPv3 informs, you must add just the username with a blank engine id.
Authentication Type	(Optional) Authentication protocol. Valid values are as follows: • **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	(Optional) Privacy protocol. You can only set this parameter if Authentication Type parameter is set. Valid values are as follows: • **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.

Trademarks