RSA NetWitness Platform

Event Source Log Configuration Guide

Trend Micro ScanMail

Last Modified: Tuesday, July 28, 2020

Event Source Product Information:

Vendor: Trend Micro
Event Source: ScanMail Suite for Microsoft Exchange
Versions: ScanMail 8.0 Service Pack 1, 10.2, 14.x

Platforms: Microsoft Exchange 2000/2003/2007

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser:

- for version 14.x: CEF
- for previous versions: trendmicroscanmail

Collection Method:

- for version 14.x: CEF
- for previous versions: SNMP

Event Source Class.Subclass: Security.Application Firewall

To configure the Trend Micro ScanMail event source, you must:

- For version 14, see Configure CEF Log Collection
- For previous versions, see Configure ScanMail for SNMP Collection

Configure CEF Log Collection

You need to configure log forwarding on the Trend Micro ScanMail event source so that they can then be collected by the NetWitness Platform CEF parser.

To configure log forwarding for ScanMail:

1. On ScanMail, select **Enable log forwarding**.
2. In the **Setting for Log Receiving Unit** section, set the following parameters:
   - **IP Address:** this is IP address of the log receiving server. Enter the IP address of your NetWitness Platform Log Decoder.
   - **Transportation Type:** Protocol to be used to transport logs to the log receiving server. If you select **TCP**, you can also select **Enable SSL** to encrypt log content.
   - **Facility:** Machine process that created the syslog event. Select an appropriate level from the drop-down menu.
   - **Severity:** Severity level of the log. RSA suggests you select **Informational**.
3. In the **Setting for Log Forwarding** section, set the following parameters:
   - **Frequency:** Frequency for collecting and forwarding logs. Default value is every 5 minutes.
   - **Event Format:** Select **CEF** for the event log format.
   - **Log Type:** Type of logs you want ScanMail to forward. RSA suggests that you select both available types, **Detection Logs** and **Event Tracking Log**.
4. Click **Test Network Connection** to verify the connection with the NetWitness Log Decoder.
5. After you can connect successfully, click **Save** to save your configuration.

Configure ScanMail for SNMP Collection

For ScanMail version 8 and 10.2, you need to configure SNMP collection on RSA NetWitness Platform and on the event source.

- In NetWitness: Add the SNMP Event Source Type
- In NetWitness: Configure SNMP v3 Users
- On the event source: Configure Trend Micro ScanMail
- On the event source: Reset the Notification Settings

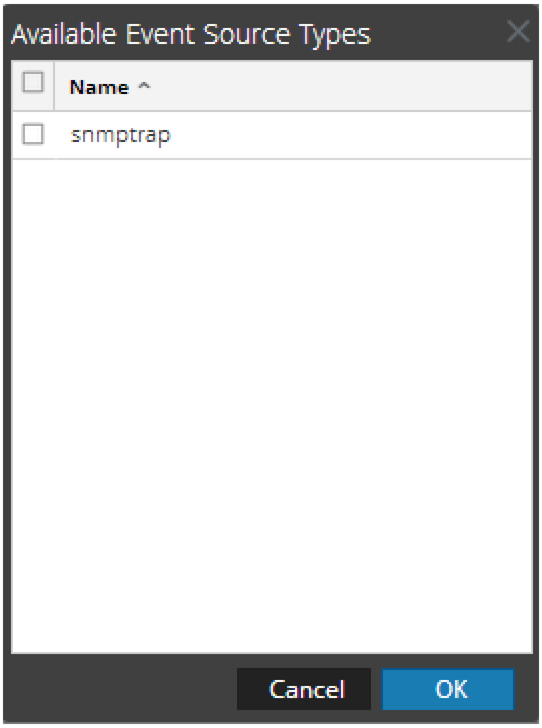
Add the SNMP Event Source Type

> **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 Platform** 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.

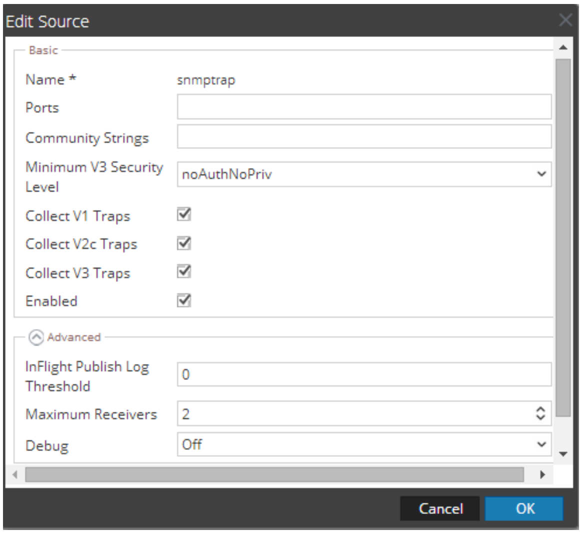
   The Sources panel is displayed with the existing sources, if any.
5. Click + to open the **Available Event Source Types** dialog.



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.


Edit Source

Basic

Name *	snmptrap
Ports	
Community Strings	
Minimum V3 Security Level	noAuthNoPriv
Collect V1 Traps	☑
Collect V2c Traps	☑
Collect V3 Traps	☑
Enabled	☑

Advanced

InFlight Publish Log Threshold	0
Maximum Receivers	2
Debug	Off

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

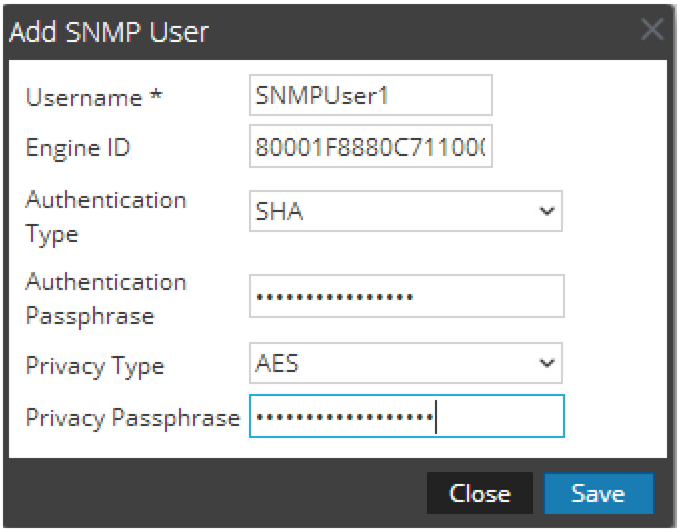
(Optional) Configure SNMP Users

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 Platform** 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.



Add SNMP User

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 *	User name (or more accurately in SNMP terminology, security name). RSA NetWitness Platform 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.

Configure Trend Micro ScanMail

To configure Trend Micro ScanMail:

Warning: Do not make any changes to the **Message** field in the Notification settings. If you change the **Message** field from the default Notification settings of any feature, see the Reset the Notification Settings instructions below.

1. Log on to the Trend Micro ScanMail web console with your Administrator credentials.
2. Follow these steps to set Notification settings:
   a. In the navigation pane, click **Administration > Notification Settings**.
   b. Under **SNMP** field, specify the IP address of the RSA NetWitness Platform Log Collector.
   c. In the **Community** field, type:
   ```
   public
   ```
   Note: This step is not necessary if the Community field is set to **public**.
   d. Click **Apply All**.
   e. Click **Save**.
3. Follow these steps to verify the Notification settings of **Security Risk Scan**:

   Note: In earlier versions of Trend Micro ScanMail, this section is labeled **Virus Scan**.

   a. In the navigation pane, click **Security Risk Scan**.
   b. Click the **Notification** tab.
   c. Under **Advanced Notification**, verify that **SNMP** is selected.
   d. Click **Show Details**.
   e. Confirm that the IP Address to your RSA NetWitness Platform Log Collector is correct.
   f. Confirm that the **Community** field is set to **public**.
   g. Click **Save**.
4. Follow these steps to verify the Notification settings of **Attachment Blocking**:

   a. In the navigation pane, click **Attachment Blocking**.
   b. Click the **Notification** tab.
   c. Under **Advanced Notification**, verify that **SNMP** is selected.
   d. Click **Show Details**.
   e. Confirm that the IP Address to your RSA NetWitness Platform Log Collector is correct.
   f. Confirm that the **Community** field is set to **public**.
   g. Click **Save**

5. Follow these steps to verify the Notification settings of **Content Filtering**:
   a. In the navigation pane, click **Content Filtering**. A list of content rules is displayed.
   b. Click on a rule.
   c. Click the **Notification** tab.
   d. Under **Advanced Notification**, click **Show Details** and confirm that:
      - **SNMP** is checked.
      - the IP Address of your RSA NetWitness Platform Log Collector is correct.
      - the **Community** field is set to **public**.
   e. Click **Save**.
   f. Repeat steps b to e for each content rule in the list.

6. Follow these steps to verify the Notification settings of **Web Reputation**:
   a. In the navigation pane, click **Web Reputation**.
   b. Click the **Notification** tab.
   c. Under **Advanced Notification**, verify that **SNMP** is selected.
   d. Click **Show Details**.
   e. Confirm that the IP Address of your RSA NetWitness Platform Log Collector is correct.
   f. Confirm that the **Community** field is set to **public**.
   g. Click **Save**.

7. Follow these steps to verify the Notification settings of **Manual Scans**:

a. In the navigation pane, click **Manual Scan**.

b. Under **Select the scan type**, click a scan type.

> **Note:** The scan type **Content Filtering** requires that you also select a rule.

c. Click the **Notification** tab

d. Under **Advanced Notification**, click **Show Details** and confirm that:

- **SNMP** is checked.
- the IP Address of your RSA NetWitness Platform Log Collector is correct.
- the **Community** field is set to **public**.

e. Click **Save**.

f. Repeat steps b to e for each scan type.

8. Follow these steps to verify the Notification settings of **Scheduled Scan**:

a. In the navigation pane, click **Scheduled Scan**.

b. Click on a scheduled scan.

c. Under **Select Scan Type**, click a scan type.

> **Note:** The scan type **Content Filtering** requires that you also select a rule.

d. Click the **Notification** tab

e. Under **Advanced Notification**, click **Show Details** and confirm that:

- **SNMP** is checked.
- the IP Address to your RSA NetWitness Platform Log Collector is correct.
- the **Community** field is set to **public**.

f. Click **Save**.

g. Repeat steps b to f for each scheduled scan.

9. Follow these steps to verify the Notification settings of **System Events**:

a. In the navigation pane, click **Alerts > System Events**.

b. Click a ScanMail Service, Event, or Exchange.

c. Under **Advanced Notifications**, confirm that:

    - **SNMP** is checked.
    - the IP Address to your RSA NetWitness Platform Log Collector is correct.
    - the **Community** field is set to **public**.

   d. Click **Save**.

   e. Repeat steps b to d for each ScanMail Service, Event, or Exchange.

10. Follows these steps to verify the Notification settings of **Outbreak Alerts**:

   a. In the navigation pane, click **Alerts** > **Outbreak Alert**.

   b. Apply the following steps to all conditions:

   c. Click a condition.

   d. Under **Advanced Notifications**, confirm that:

    - **SNMP** is checked.
    - the IP Address to your RSA NetWitness Platform Log Collector is correct.
    - the **Community** field is set to **public**.

   e. Click **Save**.

   f. Repeat steps b to e for each condition.

Reset the Notification Settings

If you change the **Message** field from the default settings of any feature, you must reset the Notification settings.

To reset the Message field to the default settings:

1. Under **Advanced Notification** of the selected feature, click **Reset**.
2. When prompted to verify the request, click **OK**.

   > **Warning:** If you reset the Notification settings of **System Events**, verify that all **ScanMail Services, Events**, and **Exchanges** are selected. Select items as necessary.

3. Click the **Notification** tab.

   > **Note:** Some features may require that you also select a rule, scan type, or condition to access the Notification settings.

4. Under **Advanced Notification**, select **SNMP**.
5. Click **Show Details**.
6. In the **IP Address** field, enter the IP address of your RSA NetWitness Platform Log Collector.
7. In the **Community** field, type the following:

   ```
   public
   ```
8. Click **Save**.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.