RSA Event Source Configuration Guide

Trend Micro ScanMail

Last Modified: Tuesday, August 12, 2014

Event Source (Device) Product Information	
Vendor	Trend Micro
Event Source (Device)	ScanMail Suite for Microsoft Exchange
Supported Versions	ScanMail 8.0 Service Pack 1, 10.2
Supported Platforms	Microsoft Exchange 2000/2003/2007
RSA Product Information	
Supported Version	RSA enVision 4.0 and 4.1
Event Source (Device) Type	trendmicrosanmail,142
Collection Method	SNMP
Event Source (Device) Class.Subclass	Security.Application Firewall
Content 2.0 Table	Application Firewall

This document contains the following information for the Trend Micro ScanMail event source:

Trend Micro ScanMail Configuration Instructions

SNMP traps are automatically supported through this update.

You must complete these tasks to configure Trend Micro ScanMail:

I. Configure RSA enVision

II. Configure Trend Micro ScanMail

Configure RSA enVision

To configure enVision:

1. Log on to enVision.
2. Click **Overview > System Configuration > Services > Universal Device Collection > Manage SNMP Traps**.
3. In the **Delete** column, select **Trend**.
4. Click **Apply**.
5. Follow these steps to restart the **NIC Trapd Service**:
    a. Click **Overview > System Configuration > Services > Manage Services**.
    b. In the **Start/Stop Service** column, select **NIC Trapd Service**.
    c. Click **Apply**.
    d. Click **Refresh** twice to stop the NIC Trapd Service.
    e. In the **Start/Stop Service** column, select **NIC Trapd Service**.
    f. Click **Apply** to start the NIC Trapd Service.

Configure Trend Micro ScanMail

To configure Trend Micro ScanMail:

Important: 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 theNotification Settings** instructions.

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, enter the IP Address of your enVision appliance.
   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 enVision appliance 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 of your enVision appliance 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 enVision appliance 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 enVision appliance 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 enVision appliance 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 enVision appliance 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 enVision appliance 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 enVision appliance 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**.

   Important: 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 enVision appliance.
7. In the **Community** field, type the following:

   public
8. Click **Save**.

Trend Micro ScanMail Release Notes (20140812-120845)

New and Updated Event Messages in Trend Micro ScanMail

For complete details on new and updated messages, see the Event Source Update Help.