

# RSA NetWitness Logs

## Event Source Log Configuration Guide



## Trend Micro OfficeScan and Control Manager

Last Modified: Thursday, November 30, 2017

### Event Source Product Information:

**Vendor:** [Trend Micro](#)

**Event Source:** OfficeScan and Control Manager

**Versions:**

- OfficeScan Corporate Edition 7.0, 8.0, 10.0, 10.5, 10.6, 11.x
- Control Manager 3.5, 5.0, 5.5, 6.x

**Note:** RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

**Additional Download:** ControlManager3\_5.sql

### RSA Product Information:

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

**Event Source Log Parser:** trendmicro

**Collection Method:** Syslog, SNMP

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

These instructions cover both Trend Micro OfficeScan and Trend Micro Control Manager.

I. Depending on your event source, perform the following procedure:

- Configure Trend Micro OfficeScan, or
- Configure Trend Micro Control Manager

II. Configure SNMP Event Sources on RSA NetWitness Suite

III. Configure RSA NetWitness Suite for Syslog Collection

## Configure Trend Micro OfficeScan

---

To configure Trend Micro OfficeScan:

1. Configure the OfficeScan event source
2. Configure RSA NetWitness Suite for SNMP Collection

The configuration for Trend Micro OfficeScan depends on your version:

- Configure OfficeScan 11.x
- Configure OfficeScan 10.0
- Configure OfficeScan 7.0 or 8.0

**Note:** If you want to use Trend Micro OfficeScan 10.0 or later with Trend Micro Control Manager, you must use Trend Micro Control Manager 5.0 or later.

### To configure Trend Micro OfficeScan 11.x:

1. Log on to the OfficeScan Administration web interface.
2. Select **Administration > Notifications > General Settings**.
3. In the **SNMP Trap** section, do the following:
  - a. In the **Server IP** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
  - b. In the **Community Name** field, type **public**.
  - c. Click **Save**.
4. Select **Administration > Notifications > Administrator**.
5. On the **SNMP Trap** tab, ensure **Enable notification via SNMP trap** is selected, and click **Save**.

**Warning:** Do not change the **Message** field.

6. Select **Administration > Notifications > Outbreak**
7. On the **SNMP Trap** tab, ensure **Enable notification via SNMP trap** is selected, and click **Save**.

**Warning:** Do not change the **Message** field.

**To configure Trend Micro OfficeScan 10.0:**

1. Log on to the OfficeScan Administration web interface.
2. Select **Notifications > Administrator Notifications > General Settings**.
3. In the **SNMP Trap** section, do the following:
  - a. In the **Server IP** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
  - b. In the **Community Name** field, type **public**.
  - c. Click **Save**.
4. Select **Notifications > Administrator Notifications > Standard Notifications**.
5. On the **SNMP Trap** tab, ensure **Enable notification via SNMP trap** is selected, and click **Save**.

**Warning:** Do not change the **Message** field.

6. Select **Notifications > Administrator Notifications > Outbreak Notifications**
7. On the **SNMP Trap** tab, ensure **Enable notification via SNMP trap** is selected, and click **Save**.

**Warning:** Do not change the **Message** field.

**To configure Trend Micro OfficeScan 7.0 or 8.0:**

1. Log on to the OfficeScan Administration web interface.
2. Select **Server Administration**.
3. Follow these steps to configure the standard alert notification:
  - a. Click **Standard Alert > SNMP Trap**.
  - b. Select **Enable notification via SNMP Trap**.
  - c. Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

**Note:** Do not alter the community trap or message.

- d. Click **Apply**.
4. Follow these steps to configure the outbreak alert notification:

- a. Click **Outbreak Alert > SNMP Trap**.
- b. Select **Enable notification via SNMP Trap**.
- c. Select **Outbreak threshold**.
- d. Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

**Note:** Do not alter the community trap or message.

- e. Click **Apply**.

## Configure Trend Micro Control Manager

---

To configure Trend Micro Control Manager, depending on your version:

- Configure Control Manager version 5.0 and later
  1. Configure the Control Manager event source (version 5.0 and higher)
  2. Configure SNMP Event Sources on NetWitness Suite
  3. Configure NetWitness Suite for Syslog Collection
- Configure Control Manager version 3.5
  1. Configure the Control Manager event source (version 3.5)
  2. Configure SNMP Event Sources on NetWitness Suite

**Note:** RSA NetWitness Suite collects from SNMP traps for Control Manager version 3.5, and from SNMP traps and Syslog for versions 5.0 and later.

### Configure Trend Micro Control Manager 5.0 and later

Use the following procedure to configure Control Manager version 5.0 and later.

1. Log on to the Trend Micro Control Manager web console with your Administrator credentials.
2. Depending on your version, do one of the following actions:
  - For 6.0, select **Administration > Event Center > General Event Settings**.
  - For 5.0, select **Administration > Settings > Event Center Settings**.
3. In the **SNMP Trap Settings** section, set the settings as follows:
  - a. In the **Community name** field, type **public**.
  - b. In the **Server IP Address** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
4. In the **SysLog Settings** section, set the settings as follows:
  - a. In the **Server IP Address** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

- b. In the **Server Port** field, ensure that the default is **514**.
    - c. In the **Facility** drop-down list, select **Local0**.
  5. Click **Save**.
  6. Depending on your version, do one of the following:
    - For 6.0, select **Administration > Event Center > Event Notifications**.
    - For 5.0, select **Administration > Event Center**.
  7. For each event category, expand the category, and select **Event**.
  8. Click **Save**.
  9. For each event category, expand the category, and set the Notification Methods settings as follows:
    - a. Click **Recipients**.
    - b. In the **Notification Methods** section, ensure that only **Syslog** or **SNMP Trap Notification** is selected.
- Note:** If both **Syslog** and **SNMP Trap Notification** are available, select only **Syslog**.
- c. Click **Save**.

## Configure Trend Micro Control Manager 3.5

Use the following procedure to configure Control Manager version 3.5.

1. Copy the **ControlManager3\_5.sql** file to the **C:\Program Files\Microsoft SQL Server\80\Tools\Binn** directory on the Control Manager server.
2. Open a command shell on the Control Manager server, and change directories to the **C:\Program Files\Microsoft SQL Server\80\Tools\Binn** directory.
3. Using the OSQL utility with database admin permissions, run the following script:

```
osql -Usa -iControlManager3_5.sql
```
4. With administrative credentials, log on to Trend Micro Control Manager.
5. From the top menu, select **Administration**.
6. From the left menu, select **Event Center**.
7. Select **Select All Events**, and click **Save**.

8. From the left menu, select **System Settings**.
9. In the **Notification settings** section, set the values as follows:
  - SNMP trap notification Community name: **public**
  - SNMP trap notification Server IP address: *server-IP-Address*  
where *server-IP-Address* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
10. Click **Save**.



## Configure SNMP Event Sources on NetWitness Suite

---


To configure SNMP Event Sources, perform the following tasks in RSA NetWitness Suite:

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

### Add the SNMP Event Source Type

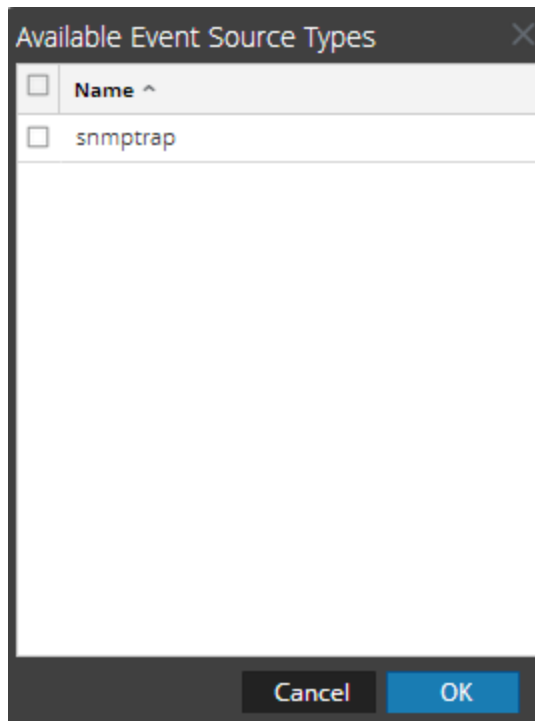
**Note:** If you have previously added the `snmptrap` type, you cannot add it again. You can edit it, or manage users.

#### Add the SNMP Event Source Type:

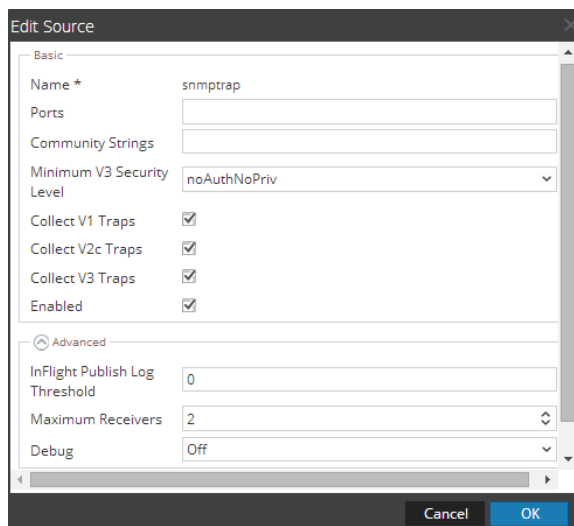
1. In the **RSA NetWitness Suite** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

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

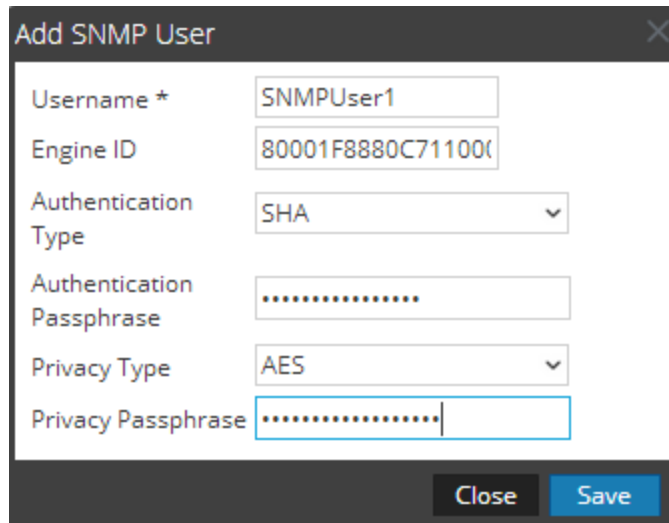
If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

### 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 \***: Text input field containing "SNMPUser1".
- Engine ID**: Text input field containing "80001F8880C71100(".
- Authentication Type**: Dropdown menu with "SHA" selected.
- Authentication Passphrase**: Password input field with masked characters (dots).
- Privacy Type**: Dropdown menu with "AES" selected.
- Privacy Passphrase**: Password input field with masked characters (dots).

At the bottom right of the dialog 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
<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>

## Configure RSA NetWitness Suite

---

Perform the following steps in RSA NetWitness Suite:

- Ensure the required parser is enabled
- Configure Syslog Collection

### Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Suite Live.

**Ensure that the parser for your event source is enabled:**

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

**Note:** The required parser is **trendmicro**.



### Configure Syslog Collection

**Note:** You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

**To configure the Log Decoder for Syslog collection:**

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > System**.
3. Depending on the icon you see, do one of the following:

- If you see  **Start Capture**, click the icon to start capturing Syslog.
- If you see  **Stop Capture**, you do not need to do anything; this Log Decoder is already capturing Syslog.

### To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click **+**.

The Available Event Source Types dialog is displayed.
5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

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.