RSA NetWitness Logs

Event Source Log Configuration Guide

Trend Micro InterScan Messaging Security Suite

Last Modified: Tuesday, April 25, 2017

Event Source Product Information:

Vendor: Trend Micro
Event Source: InterScan Messaging Security Suite
Versions: 7.1, 9.1 (Syslog only)
Additional Download: sftpagent.conf.trendmicroimss

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: trendmicroimss
Collection Method:

- For version 7.1: File, SNMP
- For version 9.1: Syslog

Event Source Class.Subclass: Security.Application Firewall

For this event source, collection method depends on your version:

- For version 9.1, you can configure Syslog
- For version 7.1, you can configure SNMP or File collection.

To configure Syslog (for Trend Micro IMSS version 9.1):

I. Configure Syslog Output on Trend Micro IMSS version 9.1

II. Configure Syslog on RSA NetWitness Suite

To configure SNMP collection (for Trend Micro IMSS version 7.1):

I. Configure SNMP on Trend Micro IMSS Version 7.1

II. Configure Syslog on RSA NetWitness Suite

To configure File collection (for Trend Micro IMSS version 7.1), see Configure File Collection on NetWitness Suite.

Configure Syslog Output on Trend Micro IMSS version 9.1

The following procedure describes how to configure Syslog output on Trend Micro IMSS.

To configure Trend Micro IMSS:

1. Go to **Logs > Syslog Settings**.
2. Click **Add**.

   The Add Syslog Server screen appears.
3. In the Syslog Server Setting section, select a facility level: **local0**

   Note: The facility level specifies the source of a message. This lets the configuration file specify that messages from different facilities are to be handled differently
4. In the **Syslog Type** section, select syslog types from the following:
   - Message tracking
   - Policy events
   - System events
   - MTA events

- Sender filtering
- Content scanning
- Administration

5. In the **Syslog Server** section, specify the following:
   - the IP address of the NetWitness Log Decoder,
   - port number **514**,
   - and supported protocol to TCP
6. Click **Add Syslog Server**.

   The new syslog server appears in the syslog server list within the Syslog Server section.
7. You can continue to add more servers, edit the existing servers, and delete servers from the syslog server list.
8. Click **Save**.

The details about each facility level, such as the syslog type and server, are shown on the Syslog Settings screen. A green check mark appears for each facility level, indicating that the associated syslog server has been enabled. To disable a facility level, click the green check mark.

Configure Syslog on 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 **trendmicroimss**.

Configure Syslog Collection

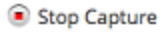
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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 

, click the icon to start capturing Syslog.
- If you see 

, 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.

Configure SNMP on Trend Micro IMSS Version 7.1

To configure Trend Micro InterScan Messaging Security Suite through SNMP traps:

1. Log on to the InterScan Messaging Security Suite web interface with administrative credentials.
2. Select **Administration** > **Notifications**.
3. Select the **Events** tab.
4. Ensure that all **SNMP** options are selected.
5. Click **Save**.
6. Select the **Delivery Settings** tab.
7. In the **SNMP Trap** section, complete the fields as follows.

Field	Action
Server name	Enter your enVision IP address
Community	Type **public**

8. Click **Save**.

Configure SNMP Event Sources on NetWitness Suite

If you are using version 7.1 of Trend Micro IMSS, configure SNMP Event Sources by performing the following tasks in RSA NetWitness Suite:

I. Add the SNMP Event Source Type

II. Configure SNMP Users

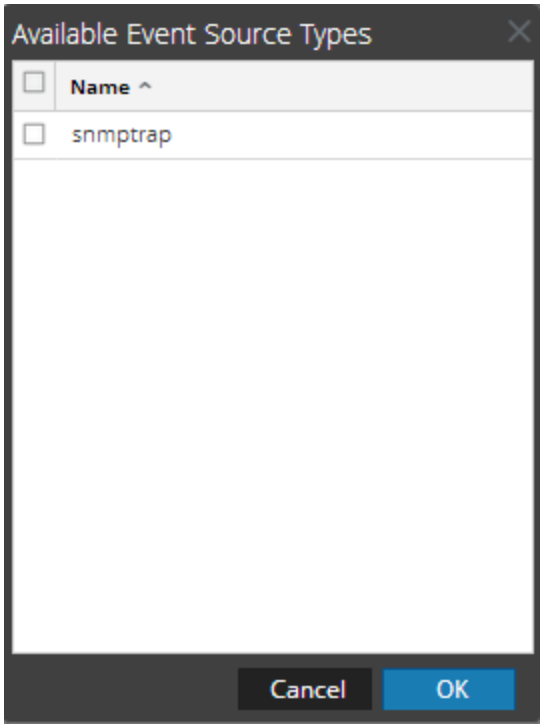
Add the SNMP Event Source Type

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

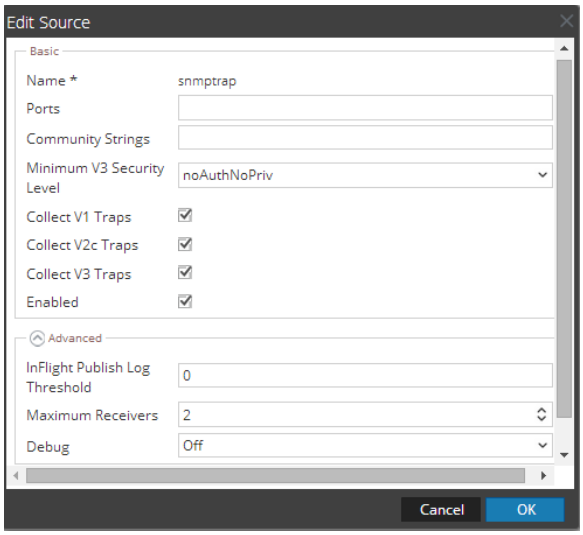
Add the SNMP Event Source Type:

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.

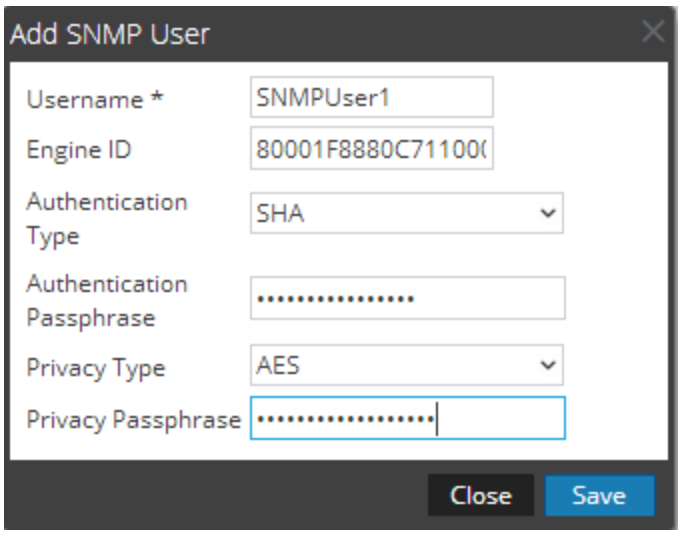
(Optional) Configure SNMP Users

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.



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.

Configure File Collection on NetWitness Suite

If you are using version 7.1 of Trend Micro IMSS, configure File collection by performing the following tasks in RSA NetWitness Suite:

I. Set up the SFTP Agent

II. Configure the Log Collector for File Collection

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see Install and Update SFTP Agent
- To set up the SFTP agent on Linux, see Configure SA SFTP Agent shell script

Configure the Log Collector for File Collection

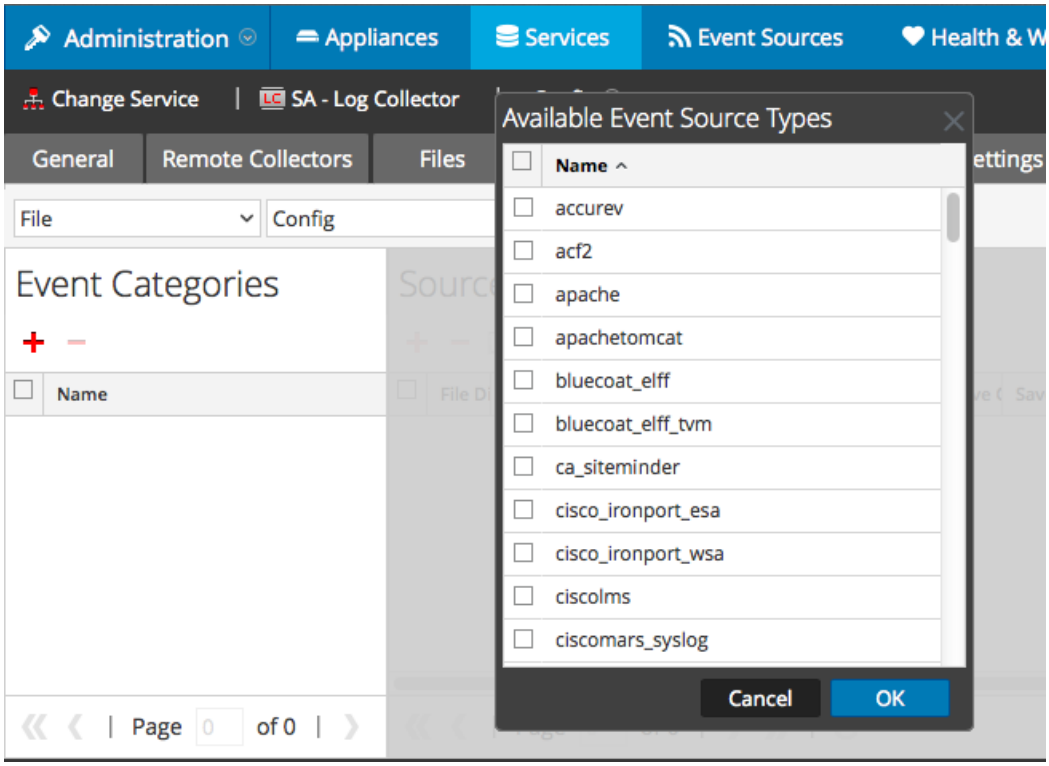
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

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

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

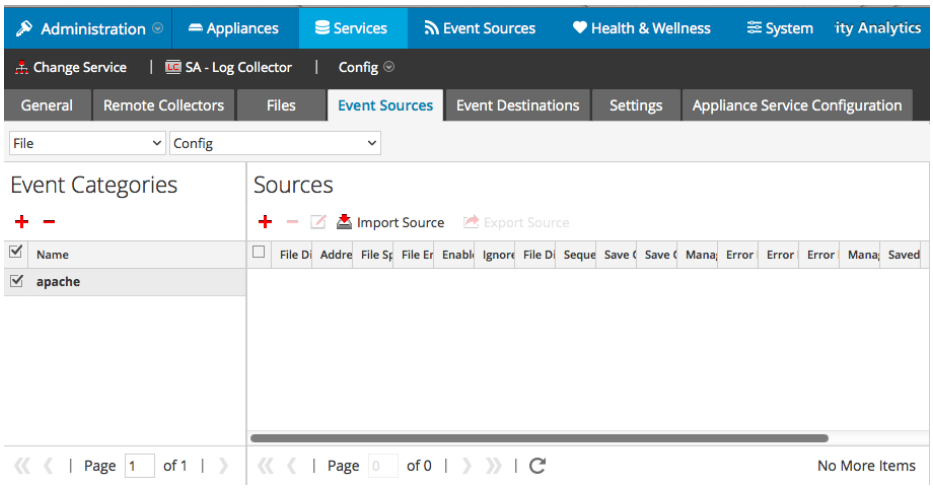
   The Available Event Source Types dialog is displayed.



5. Select the correct type from the list, and click **OK**.

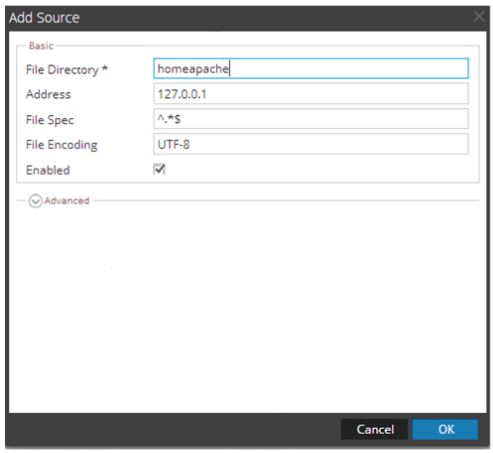
   Select **trendmicroimss** from the **Available Event Source Types** dialog.

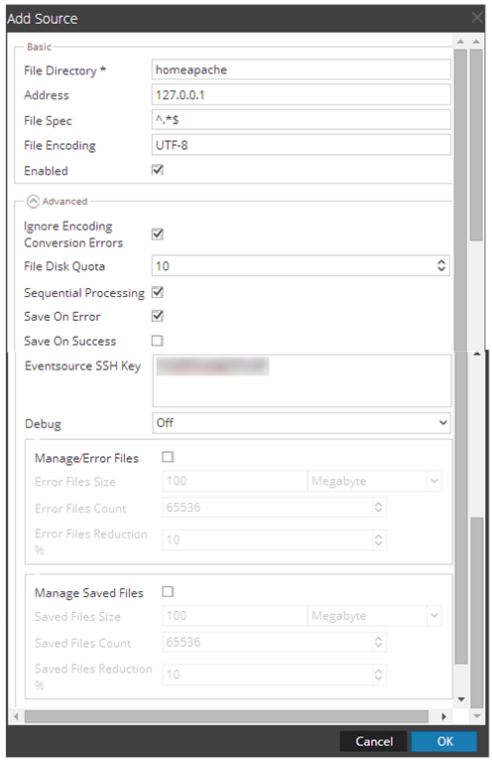
   The newly added event source type is displayed in the Event Categories panel.



6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

The Add Source dialog is displayed.





7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.
8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Trademarks