

RSA NetWitness Logs

Event Source Log Configuration Guide



Trend Micro OSSEC

Last Modified: Monday, January 16, 2017

Event Source Product Information:

Vendor: [Trend Micro](#)

Event Source: OSSEC

Versions: 2.5.1, 2.6

Additional Download: [trendmicroossec.additional.downloads.zip](#)

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: trendmicroossec

Collection Method: Syslog

Event Source Class.Subclass: Security.Intrusion

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

- I. Configure NetWitness Suite for Syslog Collection
- II. Configure Syslog Output on Trend Micro OSSEC

Configure 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 **trendmicroossec**.



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.

Configure Trend Micro OSSEC

To configure Trend Micro OSSEC, you must complete these tasks:

1. [Configure Syslog](#)
2. [Configure OSSEC to send Active-Response Logs \(Optional\)](#)

Configure Syslog

To configure Trend Micro OSSEC to send messages through syslog:

1. On the OSSEC server, in the /ossec/etc directory, open the **ossec.conf** file and add the following lines:

```
<syslog_output>
    <server> <Platform_IP> </server>
</syslog_output>
```

where <Platform_IP> is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

2. To enable client syslog and to start OSSEC, run the following commands:

```
# /var/ossec/bin/ossec-control enable client-
syslog
# /var/ossec/bin/ossec-control start
```

Configure OSSEC to Send Active-Response Logs (Optional)

Note: Perform these tasks only if you want to collect Active-Response logs.

To configure OSSEC to send Active-Response Logs, you must complete these tasks:

1. [Download and edit the additional downloads on the OSSEC server](#)
2. [Linux: Configure OSSEC to send Active-Response Logs](#)
3. [Windows: Configure OSSEC to send Active-Response Logs](#)

Note: Whether you configure Active-Response logs on Linux or Windows depends on your environment. If you have both systems in your environment, you must configure both.

Download and edit the additional downloads on the OSSEC Server

To download and edit the additional downloads on the OSSEC server:

1. Navigate to the [Downloads](#) space on [RSA Link](#), and select the [Trend Micro OSSEC downloads page](#).
2. Download and unpack the **trendmicroossec.additional.downloads.zip** file.
3. Save the **local_decoder.xml** and the **local_rules.xml** files to the `/ossec/etc` directory.

Note: These files may already exist on your system. If they do, take the content out of the files that RSA provides and add it in. If these files do not exist, you must add them.

4. In the **local_rules.xml** file, you must edit the rule ID tag.

For information on editing the rule ID, see http://www.ossec.net/wiki/Know_How:RuleIDGrouping.

Note: You should choose a rule ID value between 100000 and 109999.

Linux: Configure OSSEC to send Active-Response logs

To configure OSSEC to send Active-Response logs on Linux:

1. Under the `/ossec/etc` directory, open the **ossec.conf** file, and add the following lines:

```
<localfile>

    <log_format>syslog</log_format>

    <location>complete path to the active-responses.log
    file</location>
```

```
</localfile>
```

For example, `/var/ossec/logs/active-responses.log`.

2. Restart OSSEC.
3. Ensure that all the active-response scripts reside at the default directory `ossec\active-response\bin` directory.

4. Ensure that each script has the following default log format as shown below:

```
echo "`date` $0 $1 $2 $3 $4 $5" >> ${PWD}/../logs/active-  
responses.log
```

Windows: Configure OSSEC to send Active-Response logs

To configure OSSEC to send Active-Response logs on Windows:

1. Under the ossec-agent directory, open the **ossec.conf** file and add the following lines:

```
<localfile>  
  
    <location>complete path to the active-responses.log  
    file</location>  
  
    <log_format>syslog</log_format>  
  
</localfile>
```

For example, C:\Program Files\ossec-agent\active-
response\active-responses.log.

2. To enable Active-Response, change the default value from *yes* to *no*:

```
<active-response>  
  
    <disabled>no</disabled>  
  
</active-response>
```

3. Ensure that all the active-response scripts reside at the default directory ossec/active-response/bin directory.
4. Ensure that each script has the following default log format as shown below:

```
ECHO %DATE% %TIME% %0 %1 %2 %3 %4 %5 %6 %7 %8 %9 >> active-  
response/active-responses.log
```

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.