

RSA NetWitness Platform

Event Source Log Configuration Guide



Trend Micro InterScan Web Security

Last Modified: Thursday, January 3, 2019

Event Source Product Information:

Vendor: [Trend Micro](#)

Event Source: InterScan Web Security

Version: 3.1, 5.6, 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 Downloads: nicsftpageant.conf.trendmicroiws1, nicsftpageant.conf.trendmicroiws2

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: trendmicroiws

Collection Method: File, ODBC (3.1 only), Syslog (5.6, 6.x)

Event Source Class.Subclass: Host.Web Logs

Depending on your version of Trend Micro InterScan Web Security, complete one of the following:

- Configure Trend Micro InterScan Web Security 5.6 or 6.x. You can configure Syslog or File collection for version 5.6 or 6.x:
 - Syslog collection: [Configure Trend Micro InterScan Web Security Syslog collection for version 5.6 or 6.x](#)
 - File collection: [Configure Trend Micro InterScan Web Security File collection](#)
- Configure Trend Micro InterScan Web Security 3.1. You can configure ODBC or File collection for version 3.1:
 - ODBC collection: [Configure Trend Micro InterScan Web Security ODBC collection for version 3.1](#)
 - File collection: [Configure Trend Micro InterScan Web Security File collection](#)

Configure Trend Micro InterScan Web Security Syslog collection for version 5.6 or 6.x

To configure Syslog collection, perform the following tasks:

- I. Configure Syslog Output on Trend Micro InterScan Web Security
- II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog for Trend Micro InterScan Web Security 5.6 or 6.x

To configure syslog collection for Trend Micro InterScan Web Security 5.6 or 6.x:

1. Log on to the Trend Micro InterScan Web Security web console with administrator credentials.
2. Click **Logs > Syslog Configuration > Add**.

3. Ensure that the **Enable Syslog** box is checked, and complete the following fields:

Field	Value
IP Address	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
UDP Port	514

4. Click **Save**.

Configure RSA NetWitness Platform for Syslog

Perform the following steps in RSA NetWitness Platform:

- 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 Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN > 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 **trendmicroiwws**.

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 , 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 InterScan Web Security File collection

To configure File collection for Trend Micro InterScan Web Security 5.6 or 3.1, complete the following tasks:

1. Set up the SFTP Agent
2. 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 SFTP Shell Script File Transfer](#)

The following steps provide additional details for the previous PDF guides:

1. Download the sample files, **nicsftpagent.conf.trendmicroiwss1** and **nicsftpagent.conf.trendmicroiwss2** from the RSA NetWitness Event Source Additional Downloads space on RSA Link: [Trend Micro InterScan Web Security Additional Downloads](#).
2. Change the name of the **nicsftpagent.conf.trendmicroiwss1** file to **nicsftpagent.conf**, and save it to the **/usr/local/nic1/** directory.
3. Change the name of the **nicsftpagent.conf.trendmicroiwss2** file to **nicsftpagent.conf**, and save it to the **/usr/local/nic2/** directory.
4. Update the parameters in these files as follows:
 - a. For the sample file located in the **/usr/local/nic1/** directory, make the following changes:

Setting	Description
ENVISION	Set this value to the IP address of the RSA Log Collector.

Setting	Description
ENVISION_DIRECTORY	<p>TMIWSS_IP_address</p> <p>Where <i>IP_address</i> is the IP address for the event source.</p> <p>For example, if the Trend Micro InterScan Web Security server IP address is 172.16.0.51, set the parameter as follows:</p> <pre>ENVISION_DIRECTORY=TMIWSS_172.16.0.51</pre>

- b. For the sample file located in the `/usr/local/nic2/` directory, make the following changes:

Setting	Description
ENVISION	Set this value to the IP address of the RSA Log Collector.
ENVISION_DIRECTORY	<p>TMIWSS.AUDIT_IP_address</p> <p>Where <i>IP_address</i> is the IP address for the event source.</p> <p>For example, if the Trend Micro InterScan Web Security server IP address is 172.16.0.51, set the parameter as follows:</p> <pre>ENVISION_DIRECTORY=TMIWSS.AUDIT_172.16.0.51</pre>

Configure the Log Collector for File Collection

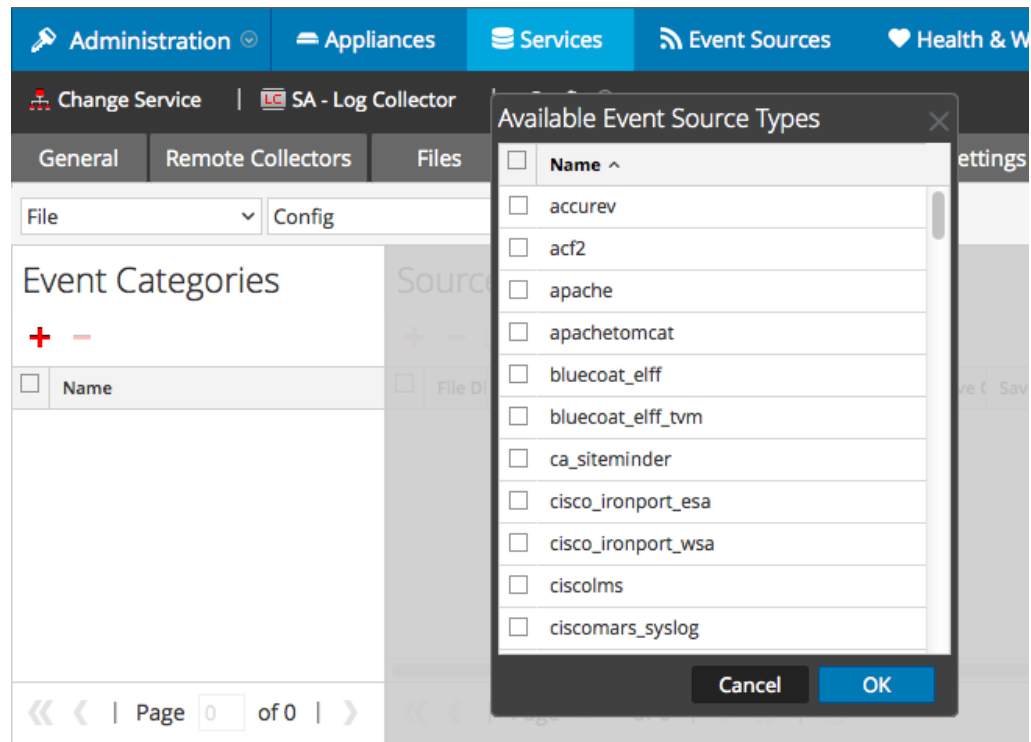
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

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

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

The Available Event Source Types dialog is displayed.



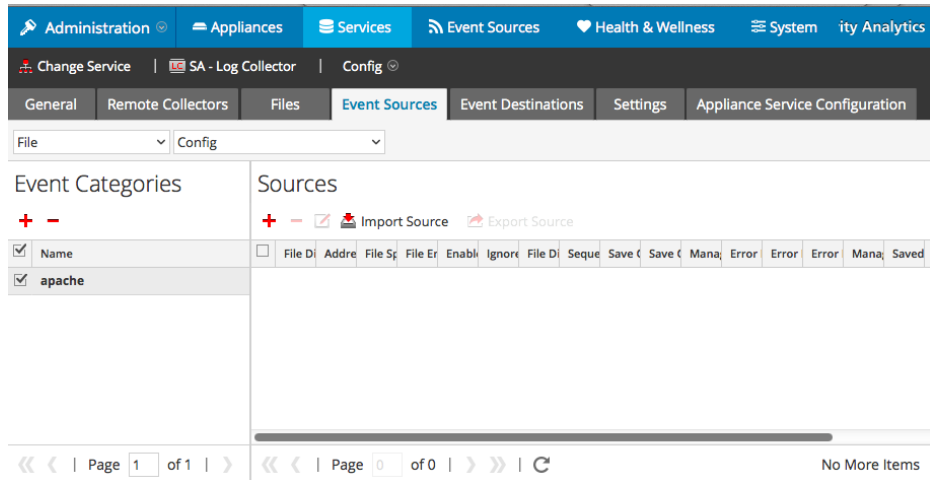
5. Select the correct type from the list, and click **OK**.

Perform this entire procedure twice, so that you can select both of the following from the **Available Event Source Types** dialog:

- Select **tmiwss**, then the next time,
- Select **tmiwss_audit** to collect the audit logs.

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

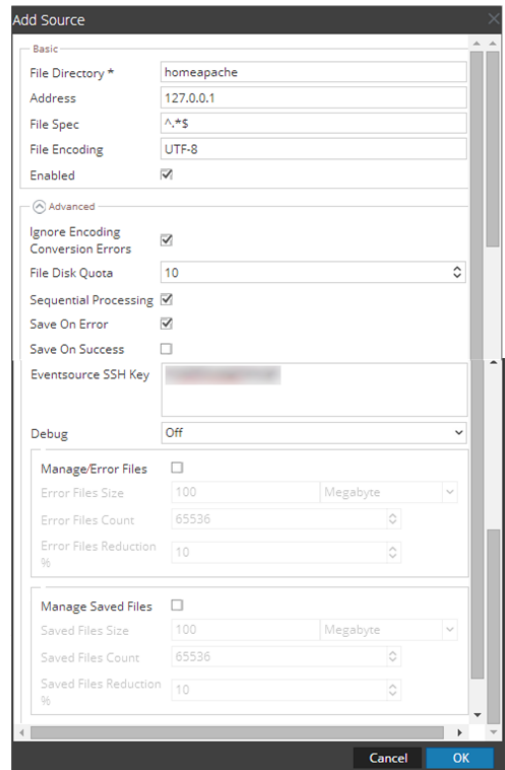
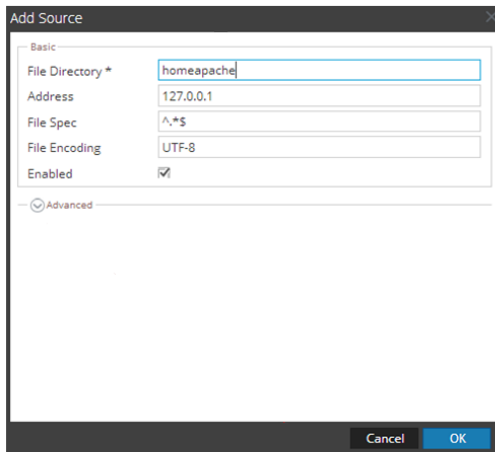
Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



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

The Add Source dialog is displayed.

Note: Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



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.

Configure Trend Micro InterScan Web Security ODBC collection for version 3.1

To configure ODBC collection in RSA NetWitness Platform, perform the following procedures:

- I. Ensure the required parser is enabled
- II. Configure a DSN
- III. Add the Event Source Type

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 from RSA NetWitness Platform Live.


Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN > 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 **trendmicroiws**.

Configure a DSN

Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select **ADMIN > 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 **ODBC/DSNs** from the drop-down menu.
5. The DSNs panel is displayed with the existing DSNs, if any.
6. Click **+** to open the **Add DSN** dialog.


Note: If you need to add a DSN template, see the "Configure DSNs" topic in the *Log Collection Configuration Guide*, available in [RSA Link](#).

7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
Parameters section	
Database	Specify the database used by Trend Micro InterScan Web Security
PortNumber	Specify the Port Number. The default port number is 1433
HostName	Specify the hostname or IP Address of Trend Micro InterScan Web Security
Driver	Depending on your NetWitness Log Collector version: <ul style="list-style-type: none"> • For 10.6.2 and newer, use <code>/opt/netwitness/odbc/lib/R3sqls27.so</code> • For 10.6.1 and older, use <code>/opt/netwitness/odbc/lib/R3sqls26.so</code>

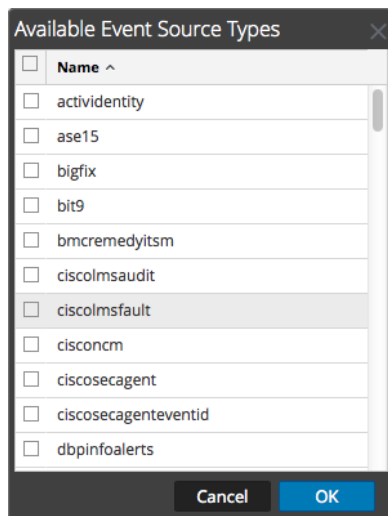
Add the Event Source Type

Add the ODBC Event Source Type:

1. In the **NetWitness** menu, select **ADMIN > 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 **ODBC/Config** from the drop-down menu.

The Event Categories panel is displayed with the existing sources, if any.

5. Click **+** to open the **Available Event Source Types** dialog.



6. Choose the log collector configuration type for your event source type and click **OK**.

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

7. In the **Event Categories** panel, select the event source type that you just added.
8. In the **Sources** panel, click **+** to open the **Add Source** dialog.

The screenshot shows a dialog box titled "Add Source" with a close button (X) in the top right corner. It is divided into two sections: "Basic" and "Advanced".

Basic Section:

- DSN * (text input field)
- Username * (text input field)
- Password (text input field with asterisks)
- Enabled (checkbox, checked)
- Address * (text input field)

Advanced Section:

- Max Cell Size (text input field with value 2048)
- Nil Value (text input field with value (null))
- Polling Interval (text input field with value 180)
- Max Events Poll (text input field with value 5000)
- Debug (text input field with value Off)
- Initial Tracking Id (text input field)
- Filename (text input field)

At the bottom of the dialog are two buttons: "Cancel" and "OK".

9. Enter the DSN you configured during the **Configure a DSN** procedure.
10. For the other parameters, see the "ODBC Event Source Configuration Parameters" topic in the *RSA NetWitness Platform Log Collection Guide*.

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

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