

# RSA NetWitness Platform

## Event Source Log Configuration Guide



## F-Secure

Last Modified: Wednesday, August 7, 2019

### Event Source Product Information:

**Vendor:** [F-Secure](#)

**Event Source:** F-Secure Client Security, F-Secure Linux Security

**Versions:** 5.x, 14.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.

### RSA Product Information:

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

**Event Source Log Parser:** fsecureav and cef

**Collection Method:** Syslog, Windows Event Logs

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

F-Secure Policy Manager is a comprehensive security management tool. IT administrators can manage and add new workstations, servers or remote offices using one central console. Policy Manager can be used to deploy security applications, define and distribute security policies, and monitor security throughout the organization.

You must configure the F-Secure server as well as each of the Windows and Unix computers so that messages logged to those computers are collected by RSA enVision.

### **Perform the following procedures to configure F-Secure:**

- I. [Configure F-Secure Server](#)
- II. Configure all the event sources on the network:
  - [Configure Windows event sources](#)
  - [Configure Unix or Linux event sources](#)
- III. Configure RSA NetWitness Platform for Syslog

## **Configure F-Secure Server**

---

You must set parameters on the F-Secure server, and then configure each Windows and Unix computer on the network. Note that the instructions for Windows and Unix differ.

### **To configure the F-Secure server:**

1. Open the Policy Manager console.
2. Click **Root** to expand the root domain, then click **Settings > Alert Sending**.
3. Enable all settings in the **Event viewer** and **System logger, Syslog** columns.

**Note:** Configure all other columns as appropriate for your organization.

4. Click the **Summary** tab.
5. For **Policy Distribution Status**, change the setting to **undistributed**.
6. Click the **Distribute Policies** link and then click **OK**.

## Configure Windows Event Sources

---

This section describes how to set up the legacy Windows collector, which you must use for Microsoft Windows Server 2003 event sources. For Microsoft Windows Server 2008 event sources, there is no configuration necessary; RSA NetWitness Platform automatically collects the log messages.

### Set Up Your Windows Legacy Event Source Domain

**Important:** You only need to perform this task if this the first time you are configuring Windows Legacy event collection for RSA NetWitness Platform and have not set up your event source domain for NetWitness Windows Legacy collection.

To set up your event source domain for Windows Legacy event source collection:

1. Depending on your version, download one of the following guides from RSA Link:
  - For Security Analytics 10.6.x: **RSA Security Analytics Legacy Windows Collection Update and Installation** at <https://community.rsa.com/docs/DOC-41196>
  - For NetWitness Platform 11.x: **RSA NetWitness Platform Windows Legacy Collection Configuration** at <https://community.rsa.com/docs/DOC-75593>.
2. Follow the instructions in this document to set up your event source domain so that the RSA NetWitness Log Collector can collect events from Windows Legacy event sources.

### Configure the Windows Legacy Event Source in RSA NetWitness Platform:

To configure the Windows Legacy Event Source in RSA NetWitness Platform:

1. Visit RSA Link for NetWitness and search for the help topic **Configure Windows Legacy and NetApp Event Sources**.
2. Complete the steps in this topic using the following value for the **Event Log Name**:  
**Application**

## Configure Linux Event Sources

---

### To configure Linux to send Syslog to RSA NetWitness Platform:

1. On the Linux appliance, open the `/etc/syslog.conf` file in a text editor. If you are using Redhat Linux 6.0, open `/etc/rsyslog.conf`.
2. To configure the event source to log all messages of debug level and higher to the syslog server, add the following line:

```
*.debug @xxx.xxx.xxx.xxx
```

where `xxx.xxx.xxx.xxx` is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

3. Save the file, and close the text editor.
4. To restart the syslog service:
  - For Redhat Linux 6.0 and newer, run this command:

```
service rsyslog restart
```
  - For other versions of Linux, run this command:

```
service syslog restart
```

## 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 **fsecureav**. If logs are coming in CEF format, the required parser is **cef**.



### 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 **ADMIN > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > System**.

- 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:

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

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

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

The Add Source dialog is displayed.
- 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 RSA NetWitness Platform for WinRM

---

## To configure Windows Event Logs Collection:

1. To set up your event source domain for Windows event source collection, see the [Configure Windows Collection](#) topic on RSA Link. Follow the instructions in this document.

**Important:** You only need to perform this task if this the first time you are configuring Windows event collection for the RSA NetWitness Platform and have not configured your Windows systems for RSA NetWitness Platform.

2. Download the [Microsoft WinRM Configuration Guide](#) from RSA Link, and follow the directions in this 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](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).