RSA NetWitness Logs

Event Source Log Configuration Guide

Cylance Protect

Last Modified: Friday, October 13, 2017

Event Source Product Information:

Vendor: Cylance

Event Source: Cylance Protect

Version: 1.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 Suite 10.0 and later
Event Source Log Parser: cylance
Collection Method: Syslog
Event Source Class.Subclass: Security.Antivirus

To configure the Cylance Protect event source, you must:

I. Configure Syslog Output on Cylance Protect

II. Configure RSA NetWitness Suite for Syslog Collection

Configure Syslog Output on Cylance Protect

The following details are reproduced from the *CylancePROTECT Syslog Guide*:

- Overview
- Regional IP Addresses
- CylancePROTECT Syslog Settings

Overview

CylancePROTECT can be configured to forward events to a Syslog server. The content of each event is Unicode plain text consisting of key-value pairs, separated by commas. Due to the size limitations of most Syslog servers, the details of each message (Cylance specific payload) is limited to 2048 characters.

Regional IP Addresses

Syslog messages are sent from the following CylancePROTECT IP addresses, based on the region from where you log on:

Asia-Pacific Northeast (protect-apne1.cylance.com):

- 13.113.53.36
- 13.113.60.117

Asia-Pacific Southeast (including Australia; protect-au.cylance.com):

- 52.63.15.218
- 52.65.4.232

North America (protect.cylance.com):

- 52.2.154.63
- 52.20.244.157
- 52.71.59.248

- 52.72.144.44
- 54.88.241.49

Europe - Central (protect-euc1.cylance.com):

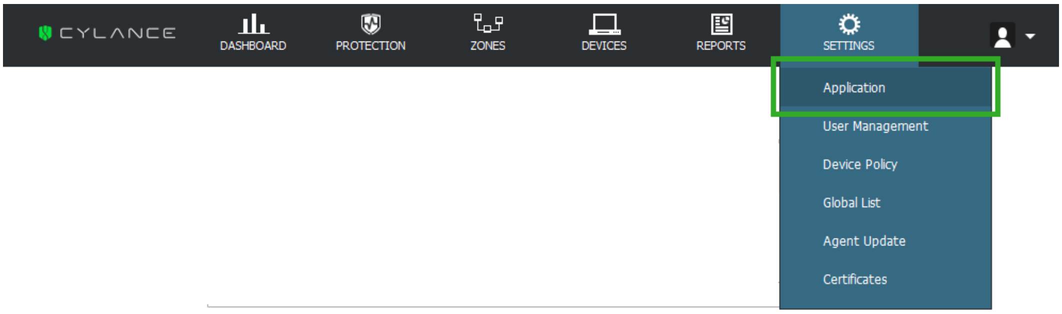
- 52.28.219.170
- 52.29.102.181
- 52.29.213.11

CylancePROTECT Syslog Settings

The following procedure describes how to configure Syslog output on CylancePROTECT.

To configure CylancePROTECT:

1. Log in to the CylancePROTECT Console.
2. Select **Settings** > **Application**.



3. Choose options as follows:
   - Under Integrations, click **Syslog/SIEM**.
   - **Event Type**: There are 7 different event types that Cylance supports . Choose whichever event types you need, based on the requirements for your organization. RSA supports all of the available options.
   - **SIEM**: this field can have any value.
   - **Protocol**: select **UDP**.
   - **IP/Domain**: enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector .

- **Port**: enter **514**.
- **Custom Token**: leave this field empty.

4. (Optional) Click **Test Connection** to test the IP/Domain, Port and Protocol settings. If you entered valid values, after a couple of moments, you should see a success confirmation pop-up:

Connection was successful.

5. Click **Save**.

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 **cylance**.

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.

Trademarks