Integration Guide

HP ArcSight Data Platform

Revised: 12 April 2016

About This Guide

Guide Type

Documented Integration — WatchGuard or a Technology Partner has provided documentation demonstrating integration.

Guide Details

WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

HP ArcSight Data Platform Integration Overview

ArcSight Data Platform (formerly called ArcSight Logger) is a universal log management software to unify log messages across the enterprise for compliance, regulation, security, IT operations, and log analytics. This document describes the steps to integrate ArcSight Logger with your WatchGuard Firebox so the ArcSight Logger administrator can index Firebox syslog messages.

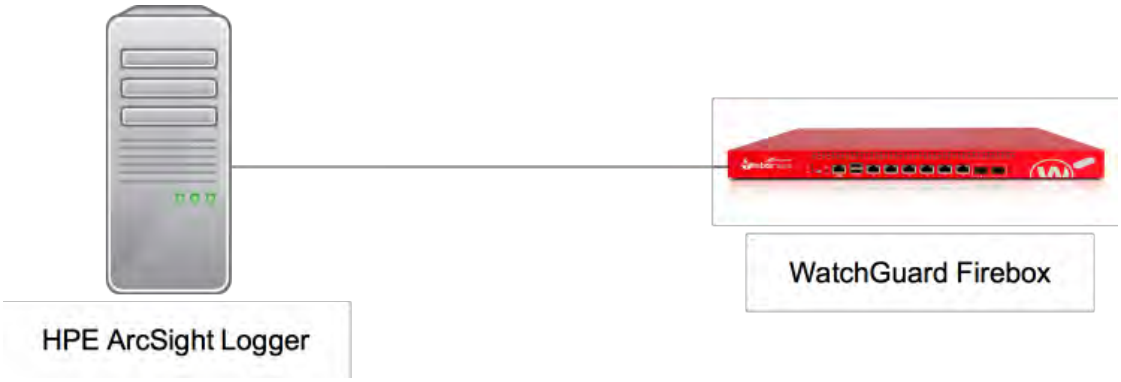
Platform and Software

The hardware and software used to complete the steps outlined in this document include:

- Firebox or WatchGuard XTM device installed with Fireware v11.10.x.
- HP ArcSight Logger 6.1.0.7504.1 for VMware VM (deployed in VMware ESXi server with an OVA template file provided by HP).

Configuration

To complete this integration, you must first deploy HP ArcSight Logger software.



To set up ArcSight Logger, please refer to the *ArcSight Logger Installation Guide*. This document describes how to listen, receive, and index syslog data from the Firebox on ArcSight Logger.

Set Up Firebox to Send Syslog Messages to ArcSight Logger

You can configure the Firebox to send syslog messages to ArcSight Logger with Fireware Web UI or Policy Manager. In this document, we use Fireware Web UI.

1. Select **SYSTEM > Logging**.

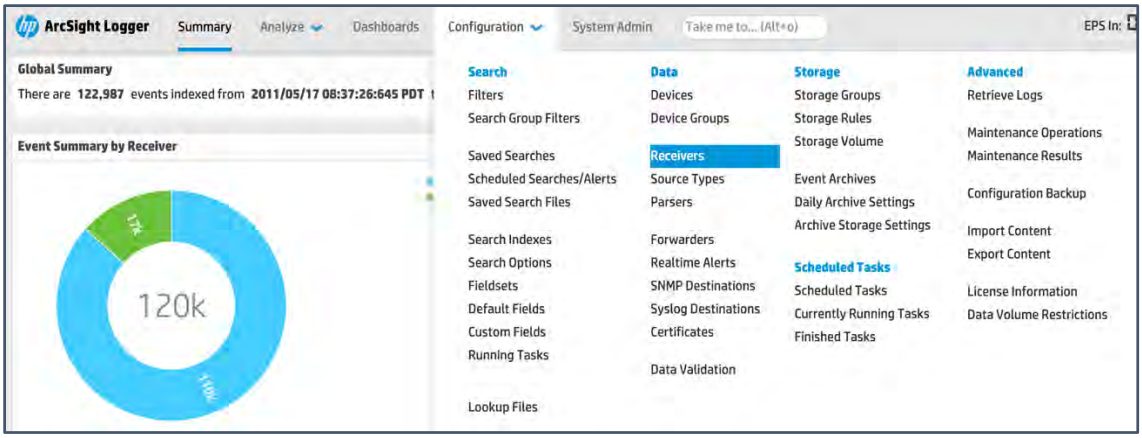
2. Select the **Send log messages to the syslog server at this IP address** check box.
3. In the **IP Address** text box, type the IP address of the ArcSight Logger.
4. In the **Port** text box, type the port configured on ArcSight to receive syslog sourced messages. By default, if ArcSight Logger is installed by a root user, the ArcSight listens on UDP port 514 and TCP port 515. If ArcSight Logger is installed by a non-root user, the UDP port is 8514 and the TCP port is 8515. In this example, syslog messages are sent with UDP in a topology where ArcSight Logger is installed by a non-root user.
5. From the **Log Format** drop-down list, select **Syslog**.

Set Up HP ArcSight Logger

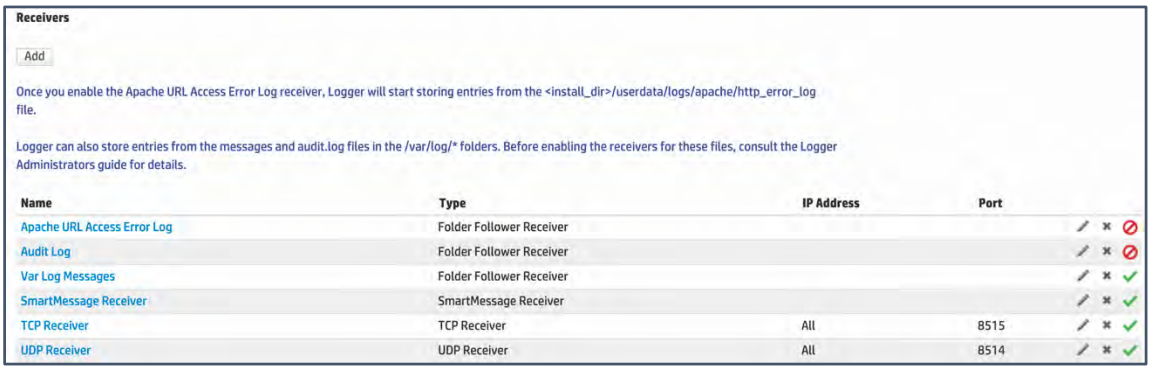
To configure ArcSight Logger, log in to the Logger UI.

Configure the Receiver

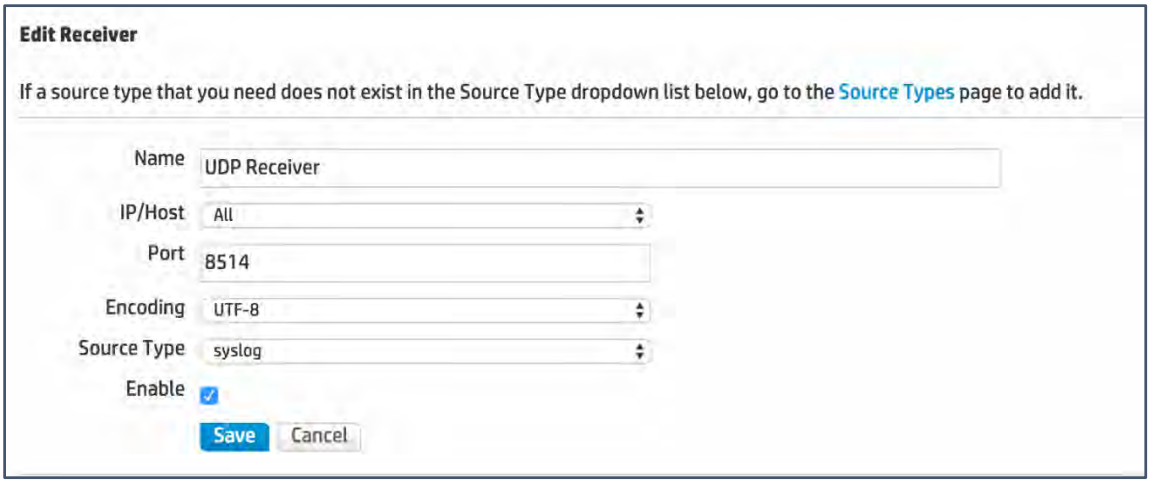
1. Select **Configuration > Data > Receivers**.



A list of predefined receivers is displayed.



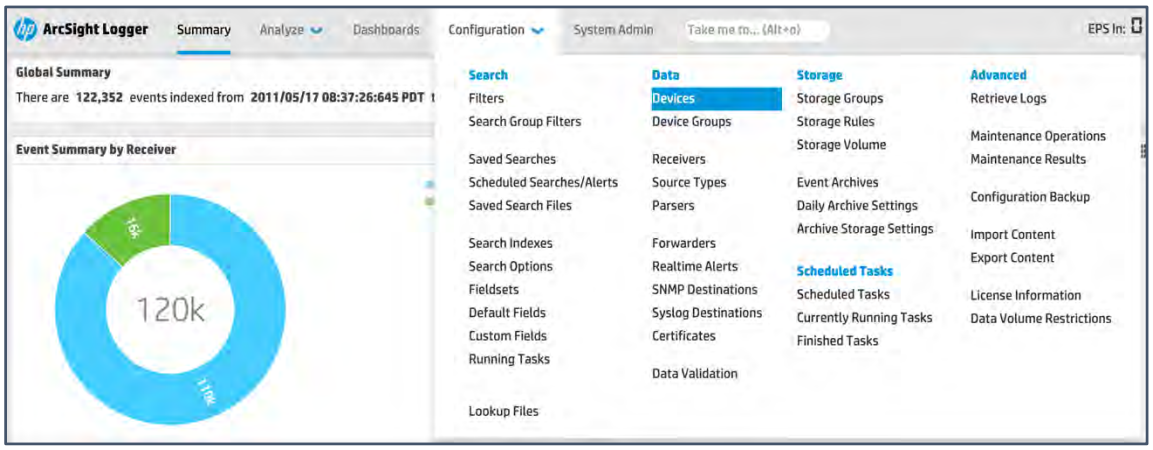
2. In the name column, click **UDP Receiver** or the pen icon to the left of the **UDP Receiver** name to edit this receiver. Or, click **Add** at the top to add a new receiver. By default, port 8514 is used for the UDP receiver.



3. From the **Source Type** drop-down list, select **syslog**.
4. Click **Save** to save the configuration.

Add Device

1. Select **Configuration > Data > Devices**.



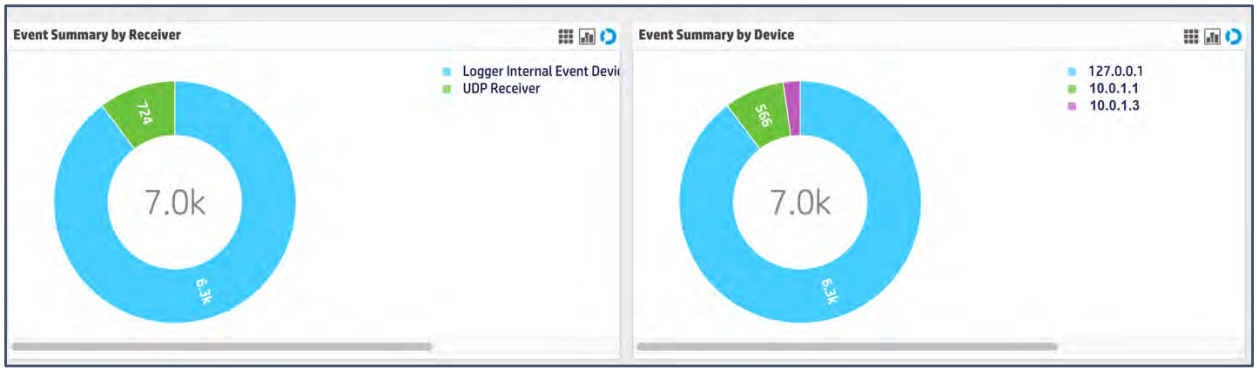
2. If you have not previously added a device, the **Add Device** page appears automatically. If not, click **Add** to add a new device.

3. In the **Name** text box, type a meaningful name for the Firebox you want to monitor.
4. In the **IP Address,** text box type the IP address of the Firebox.
5. From the **Receiver** drop-down list, select **UDP Receiver**.
6. Click **Save**.

Test the Integration

Summary View

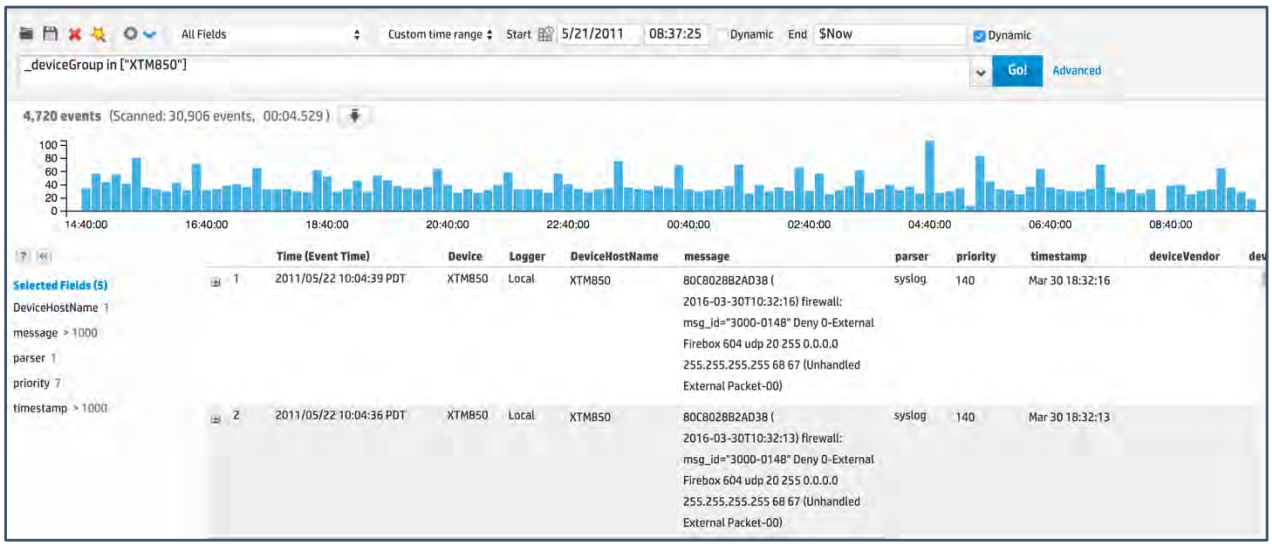
After you add the device, select **Summary** in the menu bar at the top of the page to see a summary of log messages.



In Receiver view, the pie chart is separated by receivers (the way the log messages were received). In this figure, for example, some log messages are received by a UDP Receiver while others are received by a TCP Receiver. In Device view, each pie slice represents a device monitored by ArcSight.

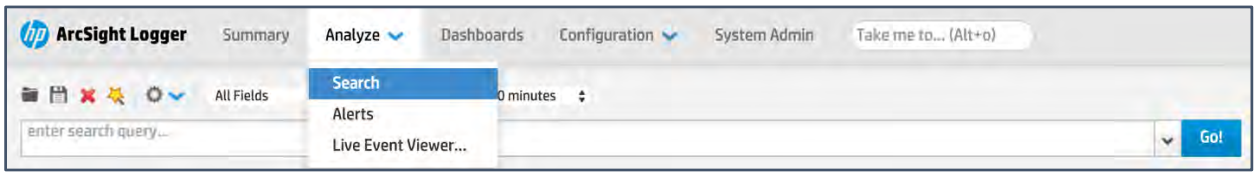
In the figure above, two devices (10.0.1.1 and 10.0.1.3) were added, both with a UDP Receiver. In Receiver view, the slice for UDP Receiver represents the total amount of log messages from both 10.0.1.1 and 10.0.1.3. The number of log messages from the device at 10.0.1.3 is 724-566=158.

To change the view from pie chart to column chart or grid view, select the corresponding icon in the top-right of each section. Here we take the pie chart as an example. In Device view, click the slice in the pie chart that represents the Firebox or the name of the item. The details page will look something like this:



Searching View

You can also use **Analyze > Search** to see detailed log messages.

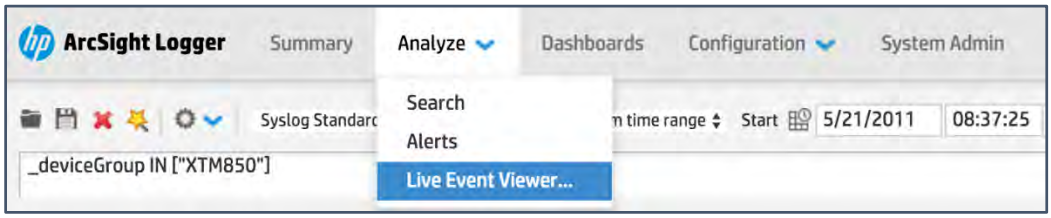


Type the filter you want to use for the log message list. For example, to search for all log messages for the Firebox we added in this example, type “_deviceGroup in [“XTM850”]”, then click **Go!** All log messages for the Firebox appear as shown in the previous image.

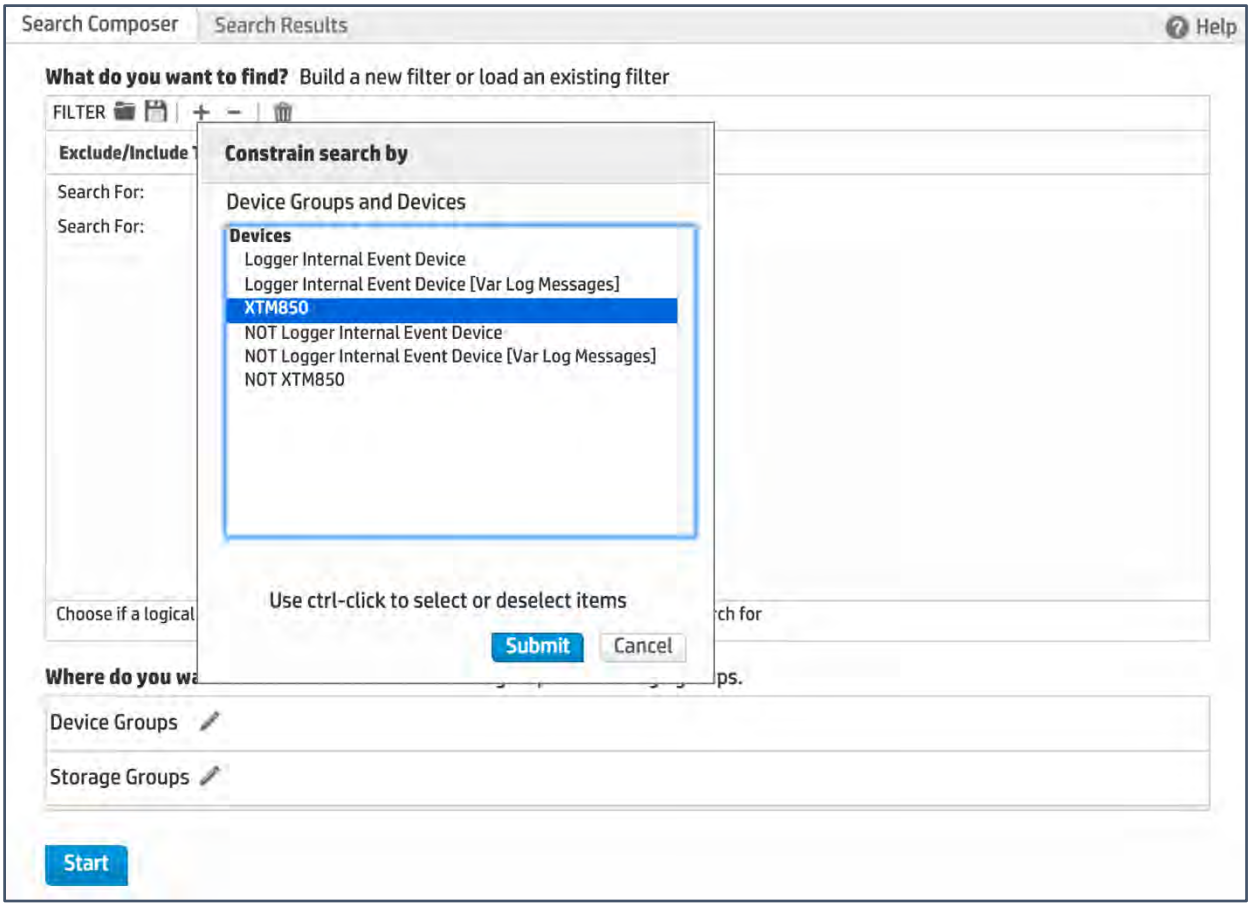
Live Event Viewer

The **Live Event Viewer** provides a real-time view of incoming events that match the criteria you specify. This functionality is useful in environments where the need to view an event quickly is important.

Select **Analyze > Live Event Viewer**.



A search dialog appears with two tabs—**Search Composer** and **Search Results**. The **Search Composer** tab is where you define the search criteria. The **Search Results** tab displays the matching events in real time.



For example, to monitor all live events from a Firebox, click the pen icon next to **Device Groups** and select the Firebox name. Click **Submit** and then click **Start**. The live events collected from the Firebox appear in the **Search Results** tab.