



# Integration Guide

**Splunk**

# 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.

# Splunk Integration Overview

---

This document describes the steps to integrate Splunk with your WatchGuard Firebox so that the Splunk administrator can index syslog messages sent from the Firebox.

## Platform and Software

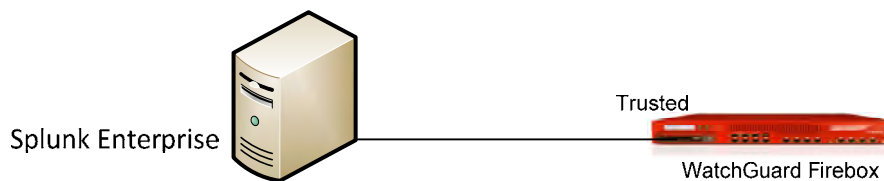
The hardware and software used to complete the steps outlined in this document include:

- Firebox or WatchGuard XTM device installed with Fireware v11.10.x
- Splunk Enterprise 6.3 installed on a Windows 2012r2 computer

## Configuration

---

To complete this integration, you must first deploy Splunk Enterprise software.



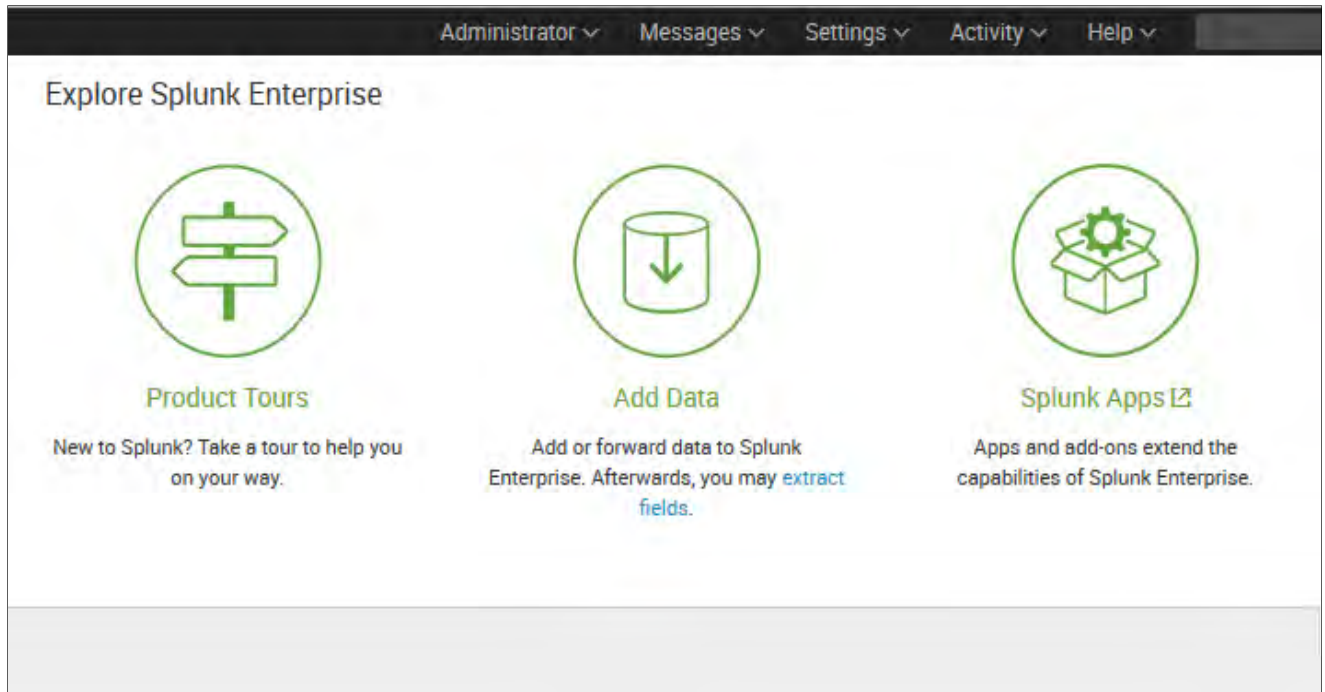
To set up the Splunk environment, please refer to the Splunk Installation Guide. In this document, we describe the procedure to listen, receive, and index syslog data from the Firebox on Splunk Enterprise.

## Set Up Splunk Enterprise

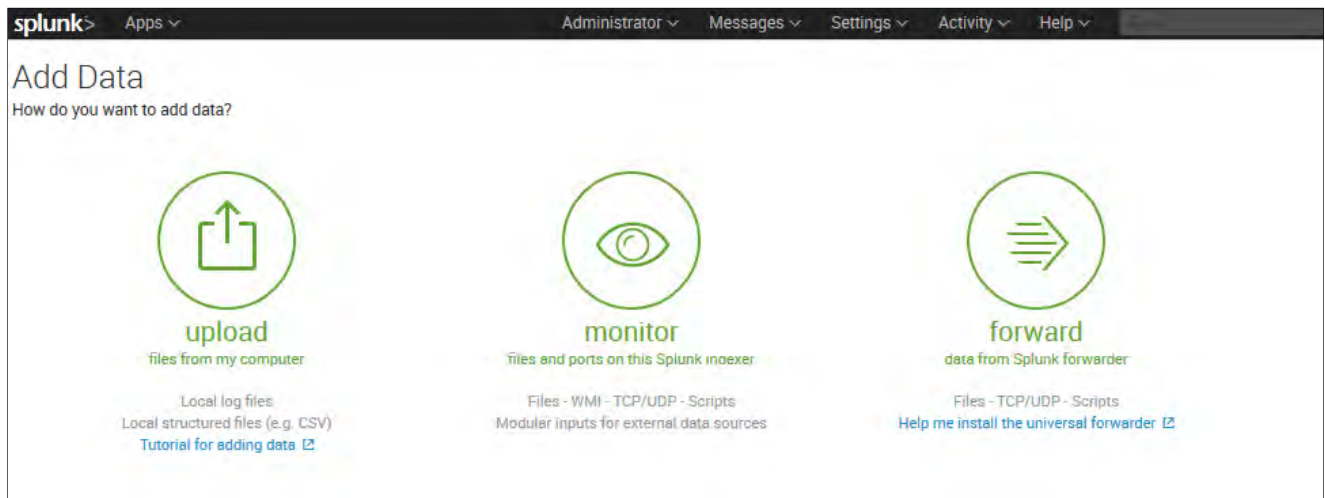
---

1. On the server where Splunk Enterprise is installed, connect to <http://localhost:8000/en-US/account/login>. The first time you log in, use the default user name **admin** and the default password **changeme**. You can then change the password to one you choose and log in again with your new password.

- From Splunk Home, select **Add Data**. The **Add Data** page launches.



- Select **monitor** to get data from TCP and UDP ports.



- Select the **TCP/UDP > UDP** tab. Note that Firebox syslog support is only available for UDP.
- In the **Port** text box, type 514. This port must match the port configured on the Firebox for the syslog server.

6. In the **Only accept connection from** text box, type the IP address of your Firebox. In our example, we used 10.0.1.1.

The screenshot shows the Splunk 'Add Data' configuration interface. The top navigation bar includes 'splunk>', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below the navigation bar, the 'Add Data' section has a progress indicator with steps: 'Select Source', 'Input Settings', 'Review', and 'Done'. The 'Next >' button is highlighted in green.

The left sidebar lists various data sources:

- Local Event Logs
- Remote Event Logs
- Files & Directories
- HTTP Event Collector
- TCP / UDP** (selected)
- Local Performance Monitoring
- Remote Performance Monitoring
- Registry monitoring

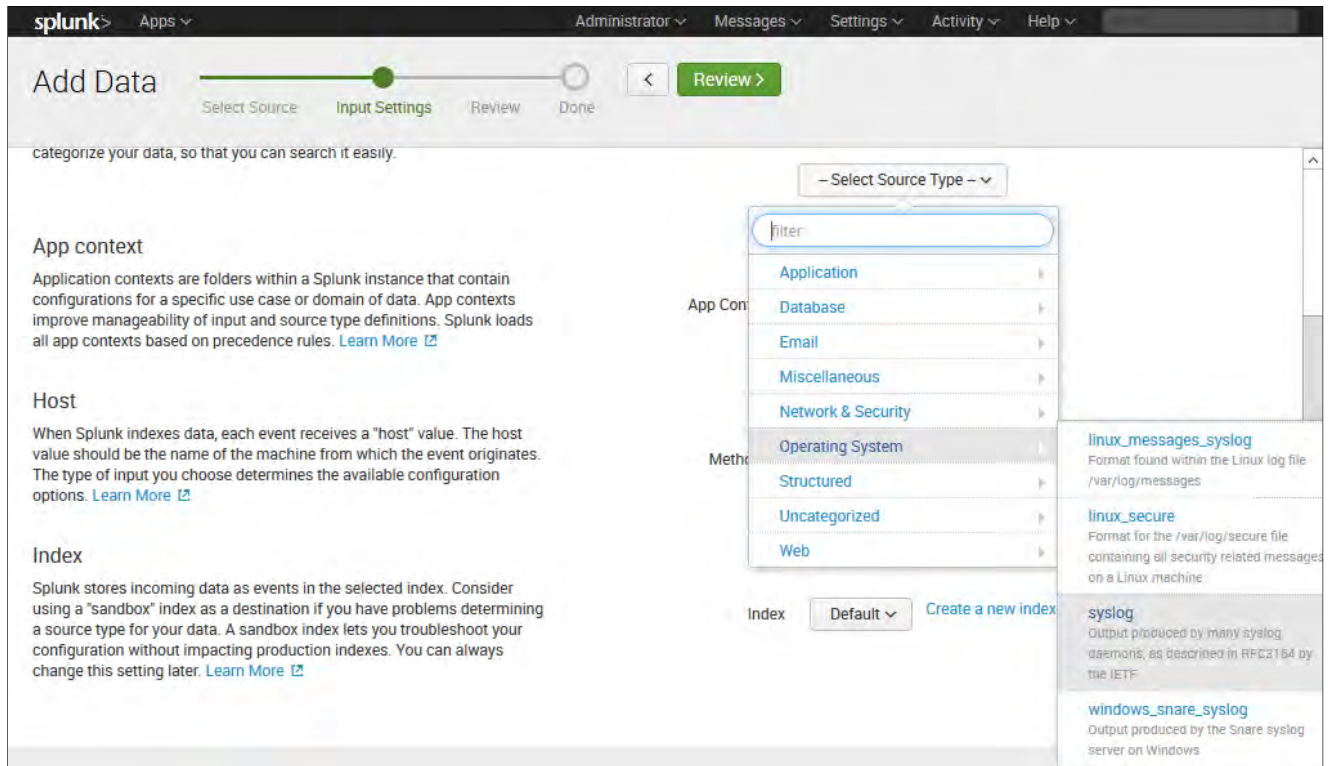
The main configuration area for 'TCP / UDP' includes:

- Radio buttons for 'TCP' and 'UDP'.
- 'Port?' field with value '514' and example '514'.
- 'Source name override?' field with value 'optional' and example 'host:port'.
- 'Only accept connection from?' field with value '10.0.1.1' and example '10.1.2.3, !badhost.splunk.com, \*.splunk.com'.

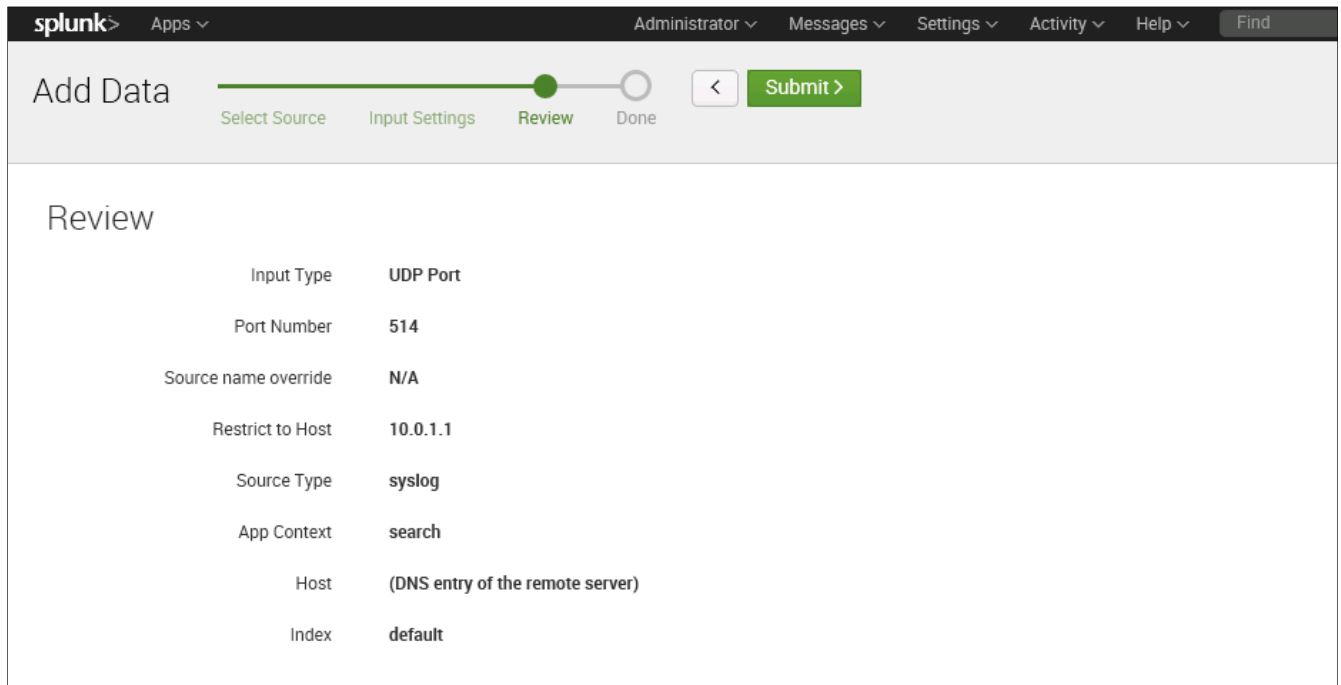
Below the configuration fields is an 'FAQ' section with the following questions:

- > How should I configure Splunk for syslog traffic?
- > What's the difference between receiving data over TCP versus UDP?
- > Can I collect syslog data from Windows systems?
- > What is a source type?

- From the **Select Source Type** drop-down list, select **Operating System > syslog**. Click **Review** to continue.



- Click **Submit**. Splunk will now automatically receive syslog messages from the Firebox IP address you specified.



# Set Up Your Firebox to Send Syslog Messages to Splunk

1. Connect to your Firebox with WatchGuard System Manager > Policy Manager or Fireware Web UI. In this example, we use Policy Manager.
2. Select **Setup > Logging**.

Use these settings to configure where the device sends log messages.

This device can send log messages to more than one destination at the same time. Select one or more check boxes to specify where log messages are sent: WatchGuard Log Server, syslog server, or Firebox internal storage.

**WatchGuard Log Server**

Send log messages to these WatchGuard Log Servers:

Log Servers 1 | Log Servers 2

The servers you specify on the **Log Servers 2** tab are only available for devices with Fireware XTM OS v11.10 and higher.

**Syslog Server**

Send log messages to this syslog server:

IP address: 10.0.1.2

Port: 514

Log format: Syslog

**Firebox Internal Storage**

Send log messages to Firebox internal storage

Send log messages when the configuration for this device is changed

OK Cancel Help

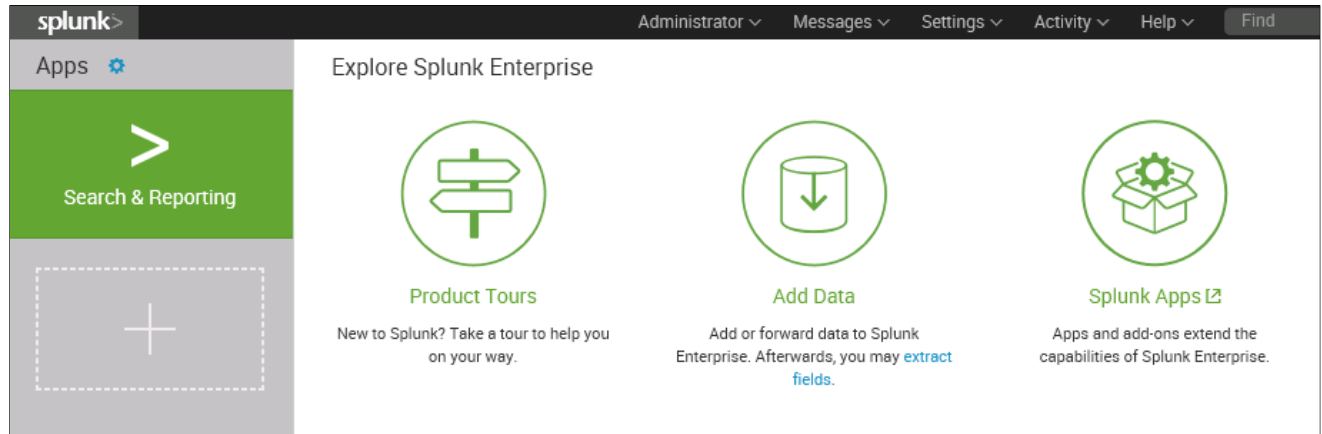
3. Select the **Send log messages to this syslog server** check box.
4. In the **IP address** text box, type the IP addresses of your server on which Splunk is installed. In this example, we use 10.0.1.2.
5. From the Port selector, select **514**.
6. From the **Log format** drop-down list, select **Syslog**.

7. Click **OK**. Save the configuration to your Firebox.

## Search and Report on syslog Data from Splunk

---

1. Sign in to the Splunk Home Page with the user **admin** and your administrative password.
2. Click **Search & Reporting**.





- In the **New Search** text box, type a search command to find a log message, using Splunk's supported search language commands. For example, this screenshot shows a search for log messages related to website browsing of an internal host through the Firebox.

The screenshot shows the Splunk Search & Reporting interface. The search bar contains the command `sourcetype="syslog" fqdn allow`. The results are displayed in a list view with columns for Time and Event. The event details show firewall logs for various domains like `www.yahoo.com` and `www.163.com`.

Time	Event
3/3/16 11:24:12.000 AM	Mar 3 11:24:12 172.16.1.134 Mar 3 03:20:31 WatchGuard-XTM firewall: msg_id="3000-0148" fqdn_dst_match="www.yahoo.com" Allow 3-Optional-2 1-External1 60 tcp 20 63 172.16.1.11 116.214.12.74 59470 443 offset 10 S 1038808966 win 2105 (HTTPS-00) fqdn_dst_match = www.yahoo.com host = 172.16.1.134 source = udp:514 sourcetype = syslog
3/3/16 11:24:12.000 AM	Mar 3 11:24:12 172.16.1.134 Mar 3 03:20:31 WatchGuard-XTM firewall: msg_id="3000-0148" fqdn_dst_match="www.yahoo.com" Allow 3-Optional-2 1-External1 60 tcp 20 63 172.16.1.11 116.214.12.74 60676 80 offset 10 S 1710584263 win 2105 (HTTP-00) fqdn_dst_match = www.yahoo.com host = 172.16.1.134 source = udp:514 sourcetype = syslog
3/3/16 11:24:06.000 AM	Mar 3 11:24:06 172.16.1.134 Mar 3 03:20:29 WatchGuard-XTM firewall: msg_id="3000-0148" fqdn_dst_match="www.163.com" Allow 3-Optional-2 1-External1 60 tcp 20 63 172.16.1.11 124.161.224.46 37734 80 offset 10 S 2720000502 win 2105 (HTTP-00) fqdn_dst_match = www.163.com host = 172.16.1.134 source = udp:514 sourcetype = syslog
3/3/16 11:23:59.000 AM	Mar 3 11:23:59 172.16.1.134 Mar 3 03:20:22 WatchGuard-XTM firewall: msg_id="3000-0148" fqdn_dst_match="www.yahoo.com" Allow 3-Optional-2 1-External1 60 tcp 20 63 172.16.1.11 116.214.12.74 59467 443 offset 10 S 3722847071 win 2105 (HTTPS-00) fqdn_dst_match = www.yahoo.com host = 172.16.1.134 source = udp:514 sourcetype = syslog

- With Splunk reporting, we can count the number of times an internal host visited any website.

The screenshot shows the Splunk Search & Reporting interface. The search bar contains the command `sourcetype="syslog" fqdn allow|top fqdn_dst_match`. The results are displayed in a table view showing the top domains visited, including `www.163.com`, `www.sina.com`, and `www.yahoo.com`.

fqdn_dst_match	count	percent
www.163.com	16	55.172414
www.sina.com	9	31.034483
www.yahoo.com	4	13.793103

5. Click the **Visualization** tab to visualize the report resulting from your search. In our example, we selected to view the data as a pie chart.

