**Overview**

Splunk for Palo Alto Networks is a security reporting and analysis tool, and is the result of a collaboration between Palo Alto Networks and Splunk. This document describes how to configure Splunk for Palo Alto Networks, and covers most problems in configuring Splunk for the first time.

**Note:** Download Splunk for Palo Alto Networks directly from the Splunk site at: <http://apps.splunk.com/app/491/>. Depending on the OS of the server that's running Splunk, follow the installation recommendations from the Splunk website.

If there are separate indexers and search head, install the application on all of them.

**Steps**

**On the Splunk Server:**

The Palo Alto Networks Next-generation Firewall uses udp/514 for syslog by default, but since this port is often used by other syslogs, we'll use udp/5514 in our examples. Choose any desired port. TCP and SSL syslogs are available in PAN-OS 6.0 and later.

1. Check the settings in the Splunk inputs.conf file and verify that no other configuration is using the UDP or TCP port you chose for syslogs from the firewall. Check the inputs.conf in the following directories:

**Note:** See the "Configuration file precedence" section in the Splunk Enterprise Admin Manual for more on the way precedences are checked on Splunk.

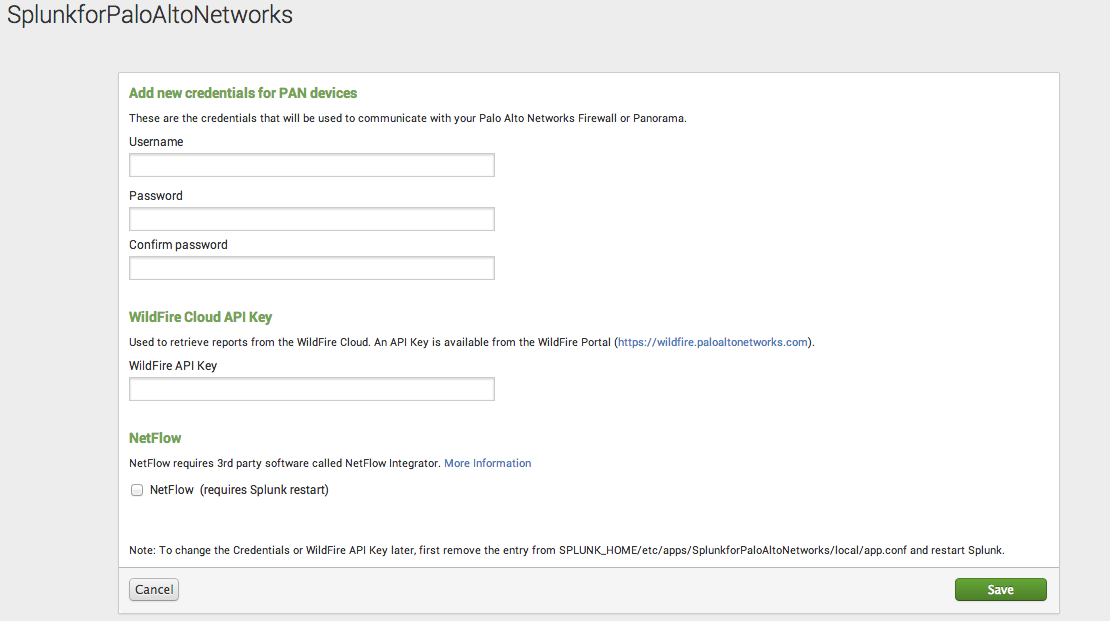
* + $SPLUNK\_HOME/etc/apps/SplunkforPaloAltoNetworks/local/
  + $SPLUNK\_HOME/etc/system/local/

1. In the inputs.conf file, add the following configuration. For UDP syslogs, make sure to include the line **no\_appending\_timestamp = true**.  
   [udp://5514]  
   index = pan\_logs  
   sourcetype = pan\_log  
   connection\_host = ip  
   **no\_appending\_timestamp = true**
2. Reset the Splunk service on the server running the Splunk for Palo Alto Networks app.

After configuring the data input, access and configure the app.

The first time running the app from the WebUI, a setup screen displays. You need the credentials only if you want to use the custom commands pantag, panblock, and panupdate. The WildFire API is required only for WildFire subscribers who want Splunk to index WildFire analysis reports from the cloud when a malware sample is analyzed. These credentials are stored in Splunk using encryption the same way other Splunk credentials are stored.

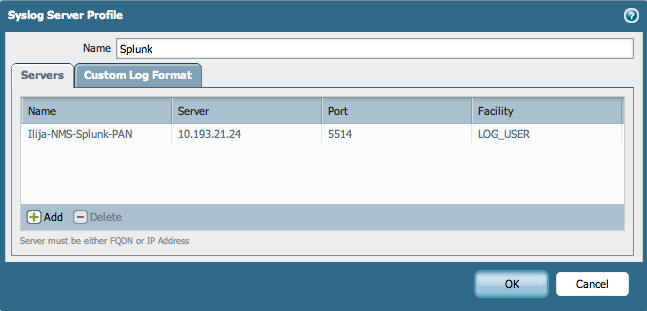
If you don't want to use these extra features, skip the setup screen by clicking Save.

* Go to Apps > Splunk for Palo Alto Networks. Add the appropriate username/password credentials for the Palo Alto Networks firewall and the WildFire API key.  
  

**Note:** After logging into the [WildFire Portal](https://wildfire.paloaltonetworks.com/) for WildFire subscribers, access the WildFire API key under the account. Copy and paste the key into the WildFire API Key (see example).

**On the Palo Alto Networks device:**

After completing setup on the Splunk site, set up the Palo Alto Networks device to send syslogs to Splunk.

1. Go to Device > Server Profiles > Syslog.
2. Configure the details for the Splunk server, including the UDP port (5514, for this example).  
     
   **Note:** Do not set a Custom Log Format. The logs must be in the default format or Splunk won't parse them.
3. Configure a logging mechanism on the firewall to use the syslog server. For example, configure a security policy rule with a Log Forwarding Profile that uses the Splunk syslog server. Or configure the firewall to log config or system events to the Splunk syslog server. Security policy rules are under Policies > Security. Other configurable syslog events are under Device > Log Settings.

**Test the configuration**

The easiest way to test that everything is working is to configure the firewall to syslog all config events. Go to Device > Log Settings > Config and commit. Make any configuration change and the firewall produces a config event syslog. You don't have to commit the change for the syslog to be produced--any uncommitted change to the configuration produces a log. You can verify the log reached Splunk by going to the Splunk for Palo Alto Networks app, click Search in the navigation bar, and enter:

    index=pan\_logs sourcetype=pan\_config

If Splunk is getting the syslogs from the firewall and parsing them correctly, then you'll see the config event syslogs show up here from the changes you made on the firewall configuration.

**Troubleshooting Steps**

**1.  Check that all initial configuration is complete**

* Verify inputs.conf is set up per the instructions above
* inputs.conf must have the line "no\_appending\_timestamp = true"
* Check the other inputs.conf configurations for other inputs using the same port
* Check that the firewall is not using a Custom Log Format (must use default)
* Check that the firewall is set to log something like system events, config events, traffic events, and so on.
* Check that the clocks on the firewall and Splunk server are the same.  If they are different, logs will not show up correctly.
* If using a TCP or SSL port for syslogs, try UDP instead first, then switch to TCP or SSL once UDP is working

**2.  Verify logs are indexed**

Use the method described in **Test the configuration** to produce some syslogs. Verify the logs are reaching the Splunk server by navigating to the Splunk for Palo Alto Networks app, click Search in the navigation bar, then enter:

    index=pan\_logs

If no logs show up, then the logs are not getting indexed correctly. Use these steps to find the problem:

* Verify the configuration from the **Troubleshooting** section above.
* Switch the search timeframe to All Time. If logs show up, verify the timestamp is correct on the logs. If time is wrong, check that the clocks on the Splunk server and firewall are the same.
* Use tcpdump or Wireshark on the Splunk server to verify the logs are actually reaching it. Also, verify that the pan\_logs index exists.

**3. Verify logs are parsed correctly**

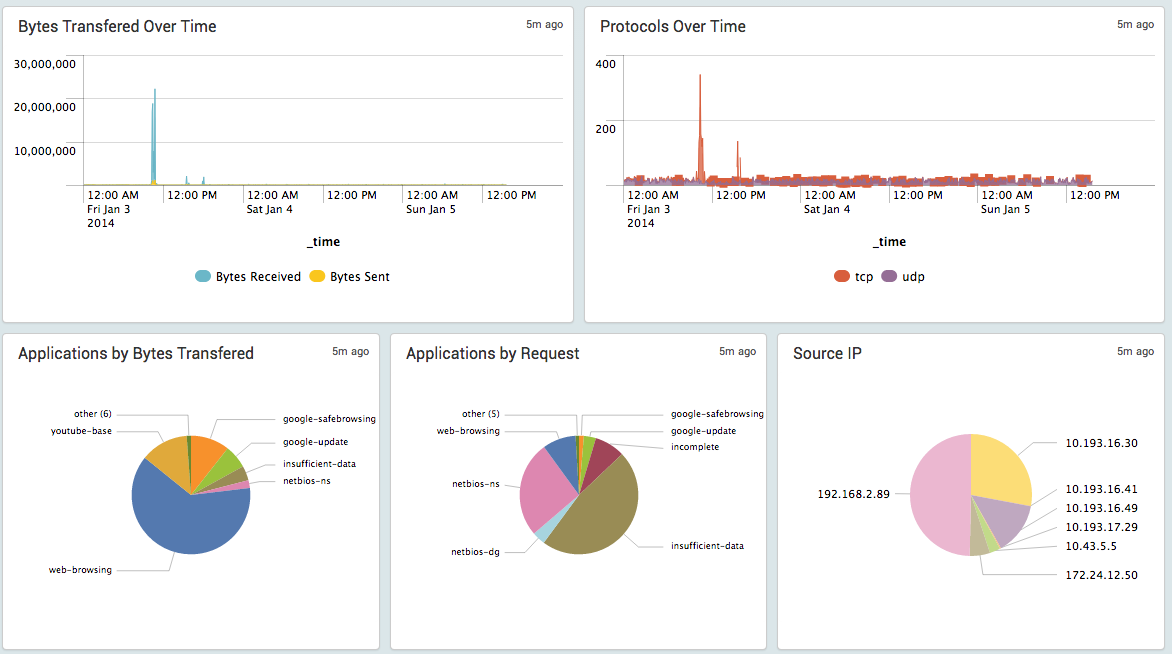
Use the method described above in the section **Test the configuration** to produce some syslogs. Verify the logs are reaching the Splunk server by navigating to the Splunk for Palo Alto Networks app, click 'Search' in the navigation bar, and enter the following search:

    index=pan\_logs sourcetype=pan\_config

If logs showed in step 2, but no logs show up now, then try sourcetype=pan\_logs instead of sourcetype=pan\_config.  If the logs start showing up after that change, then the logs are not getting parsed correctly:

* Check that you are not using a Custom Log Format in the syslog server setting on the firewall.
* Check that the inputs.conf file is configured with the line "no\_appending\_timestamp = true"
* If you're using a third-party syslog forwarder between the Palo Alto Networks device and Splunk, verify the forwarder isn't modifying the logs.

**4.  Check acceleration and summary indexing**



Check that the dashboards are populating with data. The Overview dashboard doesn't use acceleration, so it should work at this point. If it doesn't show data, then go back to troubleshooting. For all the other dashboards, after 5-8 minutes of syslogging to the Splunk server, the dashboards should populate with data. If the dashboards are populating, then acceleration and summary indexing are working. If not, check the following:

App Version 4.0 and earlier:

  Uses TSIDX for acceleration.

* Verify that saved searches for log collection are in the savedsearches.conf file. Check that they haven't been changed or overwritten.

App Version 4.1 and later:

  Uses Data Model for acceleration.

* Check acceleration settings in the data model under Settings > Data Model > Palo Alto Networks Logs, then edit the Acceleration settings and verify they are enabled for a reasonably large timeframe.
* Click the arrow next to the Palo Alto Networks logs data model and check data model build percentage. It should be 100% or very close to it.
* If the build percentage is stuck at less than 90%, the cause might be limited resources on the Splunk server being consumed by other apps. Check if Splunk CIM or Splunk ES apps are running on the Splunk server. If they are, try disabling both apps, and see if the build percentage increases over 90%. If it does, open a case with Splunk support to report the resource contention issue between the apps and get advice on how to proceed.