Table of Contents

1 Overview
   1.1 About the App .............................................. 3
   1.2 Splunk Version Compatibility .............................. 4
   1.3 Features .................................................. 4
   1.4 Requirements ............................................ 4
   1.5 Install from Github .................................... 5

2 Getting Started
   2.1 Step 1: Install the App and Add-on .................... 7
   2.2 Step 2: Initial Setup .................................. 9
   2.3 Step 3: Create the Splunk data input .................. 12
   2.4 Step 4: Configure the Firewall or Endpoint Security Manager .............. 13
   2.5 Step 5: Test the configuration ........................ 13

3 Upgrade
   3.1 Upgrade to App Version 5.0 .............................. 15
   3.2 Upgrade to App Version 4.1 .............................. 17

4 Advanced Features
   4.1 WildFire ................................................ 19
   4.2 Sync user login events with User-ID .................. 20
   4.3 Share context with Dynamic Address Groups .......... 22
   4.4 IP Classification ...................................... 22
   4.5 Un/Sanctioned SaaS Detection .......................... 23
   4.6 Automated Remediation ................................ 23
   4.7 Update metadata from content packs .................. 23
   4.8 External Search for AutoFocus ......................... 24
   4.9 External Search for Log Link ......................... 25
   4.10 AutoFocus Export List ................................ 25

5 User-ID with Splunk
   5.1 Method 1: Splunk Forwarding ........................... 29
   5.2 Method 2: Searchbar Command ......................... 29
   5.3 Distribute User-ID .................................... 30

6 Searchbar Commands
   6.1 panuserupdate ........................................ 31
Warning:

This documentation is deprecated in Splunk App and Add-on version 6.0. The latest documentation is now available here: http://splunk.paloaltonetworks.com
1.1 About the App

Palo Alto Networks and Splunk have partnered to deliver an advanced security reporting and analysis tool. The collaboration delivers operational reporting as well as simplified and configurable dashboard views across Palo Alto Networks family of next-generation firewalls.

Splunk for Palo Alto Networks leverages the data visibility provided by Palo Alto Networks’s firewalls and endpoint protection with Splunk’s extensive investigation and visualization capabilities to deliver an advanced security reporting and analysis tool. This app enables security analysts, administrators, and architects to correlate application and user activities across all network and security infrastructures from a real-time and historical perspective.
Complicated incident analysis that previously consumed days of manual and error-prone data mining can now be completed in a fraction of the time, saving not only manpower but also enabling key enterprise security resources to focus on critical, time-sensitive investigations.

**App Author:** Brian Torres-Gil – email - splunkbase - github
Paul Nguyen – email - splunkbase - github

### 1.2 Splunk Version Compatibility

<table>
<thead>
<tr>
<th>Splunk Version</th>
<th>App Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk 6</td>
<td>Palo Alto Networks App 4.x or 5.x</td>
</tr>
<tr>
<td>Splunk 5</td>
<td>Palo Alto Networks App 3.x</td>
</tr>
</tbody>
</table>

### 1.3 Features

The **Palo Alto Networks App** and **Add-on** have different features that are designed to work together, and with Splunk Enterprise Security when available.

**Palo Alto Networks App**

- Dashboards to track SaaS application usage, user activity, system health, configuration changes for audits, Wildfire malware, GlobalProtect and other Palo Alto Networks specific features.
- Advanced correlations in each dashboard
- Datamolds with pivots for easy access to data and visualizations
- Index the *behavioral footprint* of malware seen by Wildfire
- *Sync user login events with User-ID*
- *Share context with Dynamic Address Groups*
- *Update metadata from content packs*
- *Special searchbar commands*
- Macros for easy access to logs

**Palo Alto Networks Add-on**

- Fully CIM compliant and designed for use with Splunk Enterprise Security
- Field extraction for Palo Alto Networks logs from Firewalls, Panorama, and Traps Endpoint Security
- *IP Classification* tailored to your network environment
- *Designate SaaS applications* as sanctioned or unsanctioned for your organization
- App and Threat metadata from the Palo Alto Networks content and signature packs

### 1.4 Requirements

The Palo Alto Networks App and Add-on for Splunk has varying system requirements depending on the number of logs sent to Splunk. The firewall administrator has granular control over the quantity of logs sent. The more logs sent to Splunk, the more visibility is available into the traffic on the network.
If the compute resources of the servers are oversubscribed, the firewall administrator can reduce the volume of logs sent from the firewall by turning off unnecessary logs. Common high-volume low-value candidates are traffic start logs, non-container URL logs, benign WildFire logs, and logs from policy rules that pass a lot of traffic that is not highly relevant (e.g. local SAN traffic).

**App:** The Palo Alto Networks App for Splunk contains a datamodel and dashboards. The dashboards use the datamodel to pull logs quickly for visualization. The dashboards don’t require a lot of compute resources or memory, and neither does the datamodel once it is built. However, the process of building the datamodel is very CPU intensive, and is an ongoing process as new logs are indexed and need to be added to the datamodel summary index. By building the datamodel and spending the compute resources to summarize the data when logs are indexed, it allows the dashboards and visualizations to pull the data quickly without intensive compute.

Care should be taken to ensure the datamodel summary indexing has enough compute resources available to keep up with the flow of logs to the index. If there aren’t enough compute resources available, the dashboards may lag behind the data in the index.

**Add-on:** The Palo Alto Networks Add-on for Splunk handles the parsing of the logs into the index. It is highly optimized, but can require significant compute resources for high volumes of logs.

### 1.5 Install from Github

This App is available on SplunkBase and Github. Optionally, you can clone the github repository to install the App. Please feel free to submit contributions to the App using pull requests on github.

**App:** From the directory `$SPLUNK_HOME/etc/apps/`, type the following command:

```bash
git clone https://github.com/PaloAltoNetworks-BD/SplunkforPaloAltoNetworks.git SplunkforPaloAltoNetworks
```

**Add-on:** From the directory `$SPLUNK_HOME/etc/apps/`, type the following command:

```bash
git clone https://github.com/PaloAltoNetworks-BD/Splunk_TA_paloalto.git Splunk_TA_paloalto
```

**Warning:**

This documentation is deprecated in Splunk App and Add-on version 6.0. The latest documentation is now available here: [http://splunk.paloaltonetworks.com/installation.html](http://splunk.paloaltonetworks.com/installation.html)
2.1 Step 1: Install the App and Add-on

- Palo Alto Networks App
- Palo Alto Networks Add-on

If upgrading to App 4.1 or 5.0, read the Upgrade Guide.

The Palo Alto Networks Splunk App and Add-on are designed to work together, and with Splunk Enterprise Security if available. The Add-on can be used with or without the App.

Note: The Palo Alto Networks App and Add-on must be installed on all Searchheads, Indexers, and Heavy Forwarders. Do not install on Universal Forwarders.

Compatibility between App and Add-on (TA):

<table>
<thead>
<tr>
<th>App</th>
<th>Add-on (TA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 5.4</td>
<td>Splunk_TA_paloalto 3.8.0 or higher</td>
</tr>
<tr>
<td>Version 5.3</td>
<td>Splunk_TA_paloalto 3.7.x</td>
</tr>
<tr>
<td>Version 5.2</td>
<td>Splunk_TA_paloalto 3.6.x</td>
</tr>
<tr>
<td>Version 5.1</td>
<td>Splunk_TA_paloalto 3.6.x</td>
</tr>
<tr>
<td>Version 5.0</td>
<td>Splunk_TA_paloalto 3.5.x or 3.6.x</td>
</tr>
<tr>
<td>Version 4.x</td>
<td>No Add-on required</td>
</tr>
<tr>
<td>Version 3.x</td>
<td>No Add-on required</td>
</tr>
</tbody>
</table>

Note: The Add-on (TA) called TA_paloalto is deprecated and should be replaced with Splunk_TA_paloalto.

Advanced Endpoint Security (Traps) support:
Install the Palo Alto Networks App by downloading it from the App homepage, or by installing it from within Splunk.

<table>
<thead>
<tr>
<th>Traps</th>
<th>App / Add-on</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traps 4.0.0 and higher</td>
<td>Add-on 3.8.0 and higher</td>
</tr>
<tr>
<td>Traps 3.3.2 and higher</td>
<td>Add-on 3.6.0 and higher</td>
</tr>
<tr>
<td>Traps 3.3.0 and 3.3.1</td>
<td>Not supported</td>
</tr>
<tr>
<td>Traps 3.2.x</td>
<td>App 4.2 or Add-on 3.5.x with App 5.0</td>
</tr>
</tbody>
</table>

Fig. 2.1: Downloading the App and Add-on from within Splunk Enterprise.

**Note:** In a **single node** environment, the latest Add-on (TA) is installed automatically by the App, and does not need to be installed separately. In **clustered** environments, the App and Add-on should be installed separately. Both can be installed by a deployment server.
2.2 Step 2: Initial Setup

To use Adaptive Response, modular alerts/actions, or the custom searchbar commands, please configure the Add-on using the set up screen.

To configure when the App is installed, navigate to the App, click the Palo Alto Networks menu in the top left of the App, and click Configuration.

To configure when the App is not installed, navigate to the Splunk App Manager. Find the Add-on (Palo Alto Networks Add-on for Splunk) in the list and on the right side click Set up.
Firewall Credentials

Note: Only a single Firewall credential can be added.

Enter the credentials for your Firewall or Panorama. The credentials are encrypted by Splunk and used for the following features:

- Sync user login events with User-ID
- Share context with Dynamic Address Groups
- Update metadata from content packs

Optionally, you can create a user for Splunk on the firewall or Panorama, and reduce the user’s role to just what is required. To use pantag, panuserupdate, or any the Dynamic Address Group Adaptive Response action, the firewall admin must have User-ID Agent permissions in the XML API tab. To use pancontentpack, the firewall admin must have Configuration permissions in the XML API tab.

Wildfire API Key

Enter a WildFire API key. Splunk can index malware behavioral fingerprints by downloading malware reports from the WildFire cloud. Get your WildFire API key from the WildFire portal in the Accounts tab: https://wildfire.paloaltonetworks.com

See also:
- WildFire

Note: The WildFire indexing feature is only available for WildFire subscribers

AutoFocus API Key
Fig. 2.2: Firewall permissions required for App special features
Enter an AutoFocus API key. Splunk can retrieve export lists created in AutoFocus. Get your AutoFocus API key from the Settings tab: https://autofocus.paloaltonetworks.com

See also:

Note: If none of these features are desired, leave the fields blank and click Save to continue.

2.3 Step 3: Create the Splunk data input

Syslogs are sent to Splunk using the following protocols:

<table>
<thead>
<tr>
<th>Product</th>
<th>Syslog Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next generation Firewall</td>
<td>UDP, TCP, or SSL</td>
</tr>
<tr>
<td>Panorama</td>
<td>UDP, TCP, or SSL</td>
</tr>
<tr>
<td>Traps Endpoint Security &gt;= 3.3</td>
<td>UDP, TCP, or SSL</td>
</tr>
<tr>
<td>Traps Endpoint Security 3.2</td>
<td>UDP</td>
</tr>
</tbody>
</table>

Use the GUI to create a Data Input, or create it in inputs.conf. This document will explain how to create the Data Input using inputs.conf.

First, create the inputs.conf in the correct directory for your version:

<table>
<thead>
<tr>
<th>App version</th>
<th>inputs.conf location</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.x w/ Add-on</td>
<td>$SPLUNK_HOME/etc/apps/Splunk_TA_paloalto/local/inputs.conf</td>
</tr>
<tr>
<td>3.x or 4.x</td>
<td>$SPLUNK_HOME/etc/apps/SplunkforPaloAltoNetworks/local/inputs.conf</td>
</tr>
</tbody>
</table>

Note: The local directory is not created during installation, so you may need to create it.

Add the following lines to the inputs.conf file. This examples uses the default syslog port UDP 514. Change the port as needed.

```plaintext
## App version 5.x or Add-on
[udp://514]
sourcetype = pan:log
no_appending_timestamp = true

## App version 4.x and 3.x
[udp://514]
index = pan_logs
sourcetype = pan_log
no_appending_timestamp = true
```

The index, sourcetype, and no_appending_timestamp setting must be set exactly as in the example. For TCP or SSL syslogs, remove the no_appending_timestamp setting.

Note: Firewalls, Panorama, and Traps ESM can all send logs to the same data input port.
2.4 Step 4: Configure the Firewall or Endpoint Security Manager

There are two ways to send logs from a Next generation Firewall to Splunk:

1. All firewalls syslog directly to Splunk
2. All firewalls log to Panorama, then Panorama syslogs to Splunk

The Palo Alto Networks syslog documentation describes each option in detail:

**Firewall and Panorama syslog to Splunk:** [https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/monitoring/use-external-services-for-monitoring.html](https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/monitoring/use-external-services-for-monitoring.html)


**Note:** Traps logs must be in CEF format (CEF is the default on ESM)

2.5 Step 5: Test the configuration

The easiest way to test that everything is working is to configure the firewall to syslog all config events. On the firewall or Panorama, navigate to the **Device** tab, then **Log Settings**. Enable config logs and commit the configuration.

Now, make any configuration change and the firewall to produce 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.

Verify the log reached Splunk by going to the Palo Alto Networks App click Search in the navigation bar, and enter:

```
eventtype=pan_config
```

**Note:** Use the default Search app if using just the Palo Alto Networks Add-on.

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.

If you don’t see the syslog, verify the steps above or try the **Troubleshooting Guide**.
CHAPTER 3

Upgrade

This documentation is deprecated in Splunk App and Add-on version 6.0. The latest documentation is now available here: http://splunk.paloaltonetworks.com/upgrade.html

Most upgrades don’t require any special action. Just upgrade like any other Splunk app. For the versions below, there are some considerations or actions needed to migrate to the new version.

3.1 Upgrade to App Version 5.0

This applies if upgrading from a pre-5.0 version of this app to 5.0.0 or higher.

3.1.1 Add-on (TA)

Starting with App v5.0.0, the App now requires the Palo Alto Networks Add-on for Splunk. The required version of the TA is always listed in the README.md file in the Palo Alto Networks App, and in the Release Notes, and this Add-on is always included in the App.

You do not need to install the Add-on (TA) separately. It is installed or upgraded automatically when the Palo Alto Networks App v5.0.0 or higher is installed.

**ACTION REQUIRED:** You must remove the deprecated TA, called TA_paloalto. This usually applies if you use Splunk Enterprise Security version 3.x because it comes with TA_paloalto. Recreate any inputs from the old TA in the new TA using the instructions in the Getting Started guide. Check the apps directory in Splunk and take the necessary action according to the table:

<table>
<thead>
<tr>
<th>Existing TA</th>
<th>Action Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_paloalto</td>
<td>Delete this TA directory, recreate data inputs in new TA</td>
</tr>
<tr>
<td>Splunk_TA_paloalto</td>
<td>No action required, TA is upgraded automatically by App</td>
</tr>
<tr>
<td>No TA installed</td>
<td>No action required, TA is installed automatically by App</td>
</tr>
</tbody>
</table>
3.1.2 Index

The new App 5.0 and Add-on 3.5 do not use the `pan_logs` index that previous versions used. Now, logs can be stored in any index. Since the App no longer specifies the `pan_logs` index, if you are upgrading, you will need to specify the index yourself.

**ACTION REQUIRED**: Create a new index called `pan_logs` using the Splunk GUI or on the command line. Also, in your Splunk role settings, add the `pan_logs` index to the list of *Indexes searched by default*.

Splunk will not overwrite the data previously indexed, and you will have access to all the data indexed before the upgrade. Logs will continue to be stored in the `pan_logs` index according to the data inputs from the previous App version, unless otherwise specified. The data input can optionally be changed to store logs in a different index.

Results still might not show up during a search. This is because the `pan_logs` index is not searched by default. To add the `pan_logs` index to the list of indexes searched by default, in your Splunk settings, navigate to *Access controls* -> *Roles* -> `<your role>`. Scroll down to the section *Indexes searched by default*. Move `pan_logs` (or *All non-internal indexes*) to the right column.

3.1.3 Lookups

The lookups have been moved to the Add-on (TA). However, Splunk Enterprise does not remove lookup tables during the upgrade process. So you must remove the lookup tables from the App after the upgrade, or you will see errors while searching within the App.

**ACTION REQUIRED**: Delete any lookups in the App that you did not create. If you did not create any lookups in the App directory, then you can safely delete the entire lookup directory from the App. The path to the lookup directory is `$SPLUNK_HOME/etc/apps/SplunkforPaloAltoNetworks/lookups`

For example:

```
rm -rf $SPLUNK_HOME/etc/apps/SplunkforPaloAltoNetworks/lookups
```

3.1.4 Sourcetype

The sourcetype format has changed:

<table>
<thead>
<tr>
<th>Old sourcetype</th>
<th>New sourcetype</th>
</tr>
</thead>
<tbody>
<tr>
<td>pan_log</td>
<td>pan:log</td>
</tr>
<tr>
<td>pan_traffic</td>
<td>pan:traffic</td>
</tr>
<tr>
<td>pan_threat</td>
<td>pan:threat</td>
</tr>
<tr>
<td>pan_config</td>
<td>pan:config</td>
</tr>
<tr>
<td>pan_system</td>
<td>pan:system</td>
</tr>
</tbody>
</table>

No action is required. The old sourcetypes will be interpreted as the new sourcetype automatically. Optionally the data input can be changed to store logs with the sourcetype `pan:log` instead of `pan_log`. This is more correct, but will not change the way logs are retrieved from the index.

**Note**: The data input should only specify `pan:log` or `pan_log` for the sourcetype. The logs are automatically parsed into the other sourcetypes (pan_traffic, pan_threat, etc) by the Add-on, so they should not be referenced in the data input.
3.2 Upgrade to App Version 4.1

This applies if upgrading from a pre-4.1 version of this app to 4.1.0 or higher.

Starting in version 4.1 of this app, all of the dashboards use the Splunk 6 Datamodel feature, which allows for pivot of Palo Alto Networks data and better control and acceleration of summary indexes used by the dashboards. This replaces the TSIDX feature from Splunk 5.

After upgrade to 4.1 or higher, you may delete the TSIDX files that were generated by the previous version of the app. To delete the TSIDX files, look under $SPLUNK_HOME$/var/lib/splunk/tsidxstats/ and remove any directories that start with pan_. There could be up to 10 directories.

Splunk will backfill the datamodel with historic data up to 1 year old. It may take some time for historic data to show up in the dashboards, but it will be available in the pivot interface and search immediately. The time range for historic data to be available in the dashboards can be adjusted in the datamodel accelerations settings.

If you have customized the built-in dashboards of a previous app version, then they will no longer work because the customized dashboards will still use TSIDX. Remove your custom dashboards from the local directory of the app to use the new datamodel-based dashboards. You can add your customizations to the new dashboards.

Warning:

This documentation is deprecated in Splunk App and Add-on version 6.0. The latest documentation is now available here: http://splunk.paloaltonetworks.com
4.1 WildFire

The Palo Alto Networks App can download a behavioral fingerprint of any malware seen by WildFire on your network in the form of a WildFire report. This report is indexed by Splunk and can be used for advanced correlations to detect malicious behavior and indicators of compromise.

Two steps are needed to enable WildFire report indexing:

**Step 1: Add the Wildfire API key to the Palo Alto Networks App configuration**

During the *initial setup*, provide the WildFire API key. The WildFire API key is found in the WildFire portal on the **Account** tab: [https://wildfire.paloaltonetworks.com](https://wildfire.paloaltonetworks.com)

To access the configuration screen after initial setup, navigate to the **Palo Alto Networks** menu and click **Configuration**.
Step 2: Send WildFire logs to Splunk from a Firewall or Panorama

To send WildFire logs to Splunk, you must configure the firewall (or Panorama) with a syslog server, a log forwarding profile that includes WildFire logs, and a security rule with the log forwarding profile and a WildFire profile attached. Use the following links to configure WildFire logging:

- Configure syslog and log forwarding profiles
- Configure WildFire (PAN-OS 7.0)
- Configure WildFire (PAN-OS 6.1 and earlier)

**Note:** The WildFire API key won’t be used unless there are WildFire logs coming from the Firewall or Panorama. The WildFire API key is leveraged to get more context around the syslogs from the firewall.

After you’ve completed both steps, you should see the WildFire dashboard start to populate with data. If not, verify the WildFire and logging configuration on the firewall.

### 4.2 Sync user login events with User-ID

The Palo Alto Networks firewall will inform Splunk of the user generating each connection or event via the syslogs it sends to Splunk. This assumes that the firewall is getting the login information from AD or some other authentication system, to know what user is logged into the device generating the traffic.

If authentication logs are being indexed by Splunk, then Splunk can synchronize knowledge of where users are logged in with the firewall. For example, if Splunk is receiving a radius authentication log where ‘user’ is the field containing the user who authenticated, and ‘ip’ is the field containing the IP address where the user logged in, then you can map the user to the ip on the firewall.

In this situation, it is often preferred to use Splunk syslog forwarding to a User-ID agent or firewall because it is more efficient. But there are some cases where the user and IP are not in the same log. For example, if an authentication log
Fig. 4.1: WildFire dashboard with data
contains the user and MAC address, and the DHCP log contains the MAC address and IP. A correlation must be done on the MAC address to know which IP the user logged in from. In this situation, the panuserupdate command is the preferred solution.

See also:

- User-ID with Splunk
- Searchbar Command: panuserupdate

### 4.3 Share context with Dynamic Address Groups

Tagging an IP address means setting metadata or context on the firewall for that IP, which causes it to be added to corresponding Dynamic Address Groups in the firewall security policy. For example, you could create a rule in the security policy that blocks any IP address with the tag ‘bad-actor’. Initially, no IP addresses would be blocked, but you can create a search in Splunk for criteria that represents a problem device, and trigger a tagging of that IP address with the ‘bad-actor’ tag. The firewall would add the IP address to the Dynamic Address Group in the policy automatically and begin blocking the IP.

Blocking a bad actor is just the beginning, and you aren’t limited to allow or deny as your options. You could tag an IP address for additional scrutiny by the Threat Prevention engine, or as a known trusted server to be given additional permissions. The behaviors are defined by your security policy, and how you treat IP addresses with specific tags.

See also:

- Command reference: pantag

Webinar that explains the concept of automated remediation and demonstrates a case study of a real customer using this technique with Splunk and Palo Alto Networks today:

**Webinar: Defeat APT with Automated Remediation in Splunk**

Video from a session at Ignite 2015 explains Dynamic Address Groups in more detail with several use cases including asset management:

**Video: Applying Order to Computing Chaos**

### 4.4 IP Classification

Classify IP addresses in Splunk by any criteria relevant to your environment. IP ranges can be designated as DMZ, datacenter, VMware, serverfarm, webtier, or any other relevant keyword to help distinguish and classify a group of IP addresses during a search.

Classifications will show up in the src_class and dest_class fields.

Classifications are set in the lookup file `ip_classifications.csv`. Add subnets and their classification to the `ip_classifications.csv` file, one per line.

For example:

<table>
<thead>
<tr>
<th>cidr</th>
<th>classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>private</td>
</tr>
<tr>
<td>172.16.0.0/12</td>
<td>private</td>
</tr>
<tr>
<td>192.168.0.0/16</td>
<td>private</td>
</tr>
</tbody>
</table>

1 The field is called `dst_class` in App versions before 5.0

2 Starting in App version 5.0, the `ip_classifications.csv` file is located in the Splunk_TA_paloalto Add-on. Before 5.0, it is in the SplunkforPaloAltoNetworks App.
**4.5 Un/Sanctioned SaaS Detection**

*Added in App version 5.0*

Classify SaaS applications as sanctioned or unsanctioned for your organization. This designation is used in searches using the Splunk searchbar and to separate information in the App’s SaaS Dashboard.

SaaS applications are designated as sanctioned in the lookup file `sanctioned_saas.csv` in the Splunk_TA_paloalto Add-on.

Add each sanctioned SaaS app in the lookup file, one per line. For example:

```plaintext
app,sanctioned_saas
paloalto-wildfire-cloud,yes
boxnet,yes
dropbox,yes
gmail-enterprise,yes
skype,yes
facebook-base,yes
gmail-chat,yes
```

Sanctioned designation is found in the field `app:is_sanctioned_saas`.

For a list of all SaaS applications, visit Applipedia and under the Characteristics header, click SaaS.

**4.6 Automated Remediation**

Use the `pantag` command to share context from Splunk to the firewall for automated remediation.

This webinar explains the concept of automated remediation and demonstrates a case study of a real customer using this technique with Splunk and Palo Alto Networks today:

Webinar: Defeat APT with Automated Remediation in Splunk

**4.7 Update metadata from content packs**

*Added in App version 5.0*

The Palo Alto Networks Add-on (TA) comes with two lookup files with metadata about applications and threat signatures called `app_list.csv` and `threat_list.csv`, respectively. These lookup tables are responsible for populating the `app:xyz` and `threat:xyz` fields used in the dashboards and displayed during a search.

The lookup table files are updated with each TA release, but can get out of date between releases. To keep the files up to date, they can be updated dynamically from the content pack metadata in your firewall or Panorama. This is done...
by creating a saved search inside the TA to periodically pull the metadata from the firewall or Panorama and update the lookup tables.

Create the following saved searches in the TA, by creating the file: `$SPLUNK_HOME/etc/apps/Splunk_TA_paloalto/local/savedsearches.conf`

```plaintext
[Palo Alto Networks - Retrieve ContentPack Apps]
cron_schedule = 5 0 * * 6
dispatch.earliest_time = -1m
displayview = flashtimeline
enableSched = 1
realtime_schedule = 0
request.ui_dispatch_view = flashtimeline
search = | pancontentpack <IP-or-hostname> apps | outputlookup createinapp=true app_lookup
disabled = 0

[Palo Alto Networks - Retrieve ContentPack Threats]
cron_schedule = 10 0 * * 6
dispatch.earliest_time = -1m
displayview = flashtimeline
enableSched = 1
realtime_schedule = 0
request.ui_dispatch_view = flashtimeline
search = | pancontentpack <IP-or-hostname> threats | outputlookup createinapp=true threat_lookup
disabled = 0
```

Set `<IP-or-hostname>` to the IP or hostname of your Firewall or Panorama. Ensure you set the credentials for this device in the App configuration. This example updates the lookup tables every Saturday at 12:05 AM for apps and 12:10 AM for threats. Change the cron_schedule to your desired update schedule.

**Note:** The Palo Alto Networks App version 5.0 or higher must be installed for the lookup table update to work. But the saved searches must be created in the TA, not the App.

If using a custom admin role on the firewall, it must have Configuration permissions for the XML API. See Step 2: Initial Setup in the Getting Started Guide.

### 4.8 External Search for AutoFocus

External Search can be used with AutoFocus Remote Search feature. Remote search is a feature in AutoFocus providing a way to search for IOC’s in an external system. The Palo Alto Networks Splunk App can receive a search request from AutoFocus and provide log events that match the search criteria.

**Note:** This feature is only available on Palo Alto Networks App and requires access to AutoFocus.

Setting up remote search and how to use it in AutoFocus is documented on the Palo Alto Networks Website and will not be covered here. The values needed in Step 3 of the documentation are provided here along with the link to the documentation.

- Setup AutoFocus remote search
- **Values to be used in Step 3 of the doc** System Type: Custom
4.9 External Search for Log Link

Palo Alto Networks Firewall has a feature called Log Link, which allows you to cross launch into an external search from the Firewall UI. This feature can be used with the Palo Alto Networks Splunk App External Search page.

**Note:** This feature is only available on Palo Alto Networks App and requires access to PAN-OS CLI.

Example CLI command

```
```

Other possible fields to search

```
(dest_ip%20eq%20'{dst}')
(src_ip%20eq%20'{src}')
(dest_port%20eq%20'{dport}')
(src_port%20eq%20'{sport}')
(protocol%20eq%20'{proto}')
```

4.10 AutoFocus Export List

With the Palo Alto Networks Splunk Add-on an AutoFocus export list can be added as a modular input in Splunk. The modular input utilizes AutoFocus's REST API to periodically sync an Export List from AutoFocus. The list of artifacts are stored in the KVStore and can be accessed via `inputlookup` macros. This data can then be used to correlate against other logs.

Two steps are needed to enable AutoFocus export list syncing:

**Step 1: Add the AutoFocus API key to the Add-on configuration**

During the *initial setup*, provide the AutoFocus API key. The AutoFocus API key is found in the AutoFocus portal on the **Settings** tab: https://autofocus.paloaltonetworks.com

To access the configuration screen after initial setup, navigate to the **Palo Alto Networks** menu and click **Configuration**.
Step 2: Add AutoFocus Export List to Splunk from a Data Input

- Learn more about creating an Export List

To retrieve the export list from AutoFocus, you must configure a data input. From the Settings menu click on Data Inputs. Under Local inputs types select AutoFocus Export List and add a new list.

Give your new data input a name by entering it in the Name field.

Set the name of your export list in the label field. This field must match the export list name from AutoFocus.

Verify the data is being synced by running a search `| `pan_autofocus_export`
Macros

There are several new macros that can be used to correlate a search with the artifacts imported from the AutoFocus Export List.

`| pan_autofocus_export` - A macro to search on all export lists. This will return all entries from all AutoFocus inputs.

The remaining macros require one argument. Set the `label` of the export list you want to search against. Each macro is separated by the artifact types.

`| pan_autofocus_export_dns(label)`
`| pan_autofocus_export_connection(label)`
`| pan_autofocus_export_registry(label)`
`| pan_autofocus_export_file(label)`
`| pan_autofocus_export_process(label)`

Warning:

This documentation is deprecated in Splunk App and Add-on version 6.0. The latest documentation is now available here: http://splunk.paloaltonetworks.com/userid.html
The Palo Alto Networks firewall will inform Splunk of the user generating each connection or event via the syslogs it sends to Splunk. This assumes that the firewall is getting the login information from AD or some other authentication system, to know what user is logged into the device generating the traffic.

Often a system like a RADIUS server sends authentication logs to Splunk to be indexed. When these logs arrive at Splunk, Splunk can synchronize with the firewall the knowledge of where users logged in. This keeps the firewall’s User-ID up to date for policy enforcement and monitoring. There are two ways to synchronize user-id information to the firewall, depending on how your authentication logs are formatted in Splunk.

5.1 Method 1: Splunk Forwarding

This is the recommended method.

When Splunk receives authentication logs from an external system (like a RADIUS server), forward the authentication logs from Splunk to a User-ID Agent or User-ID Firewall. The logs must contain both the user and the IP address where they logged in/out.

This method is recommended because it is more efficient.

**Step 1:** Configure log forwarding on Splunk [http://docs.splunk.com/Documentation/Splunk/6.3.0/Forwarding/Forwarddatatothird-partysystems](http://docs.splunk.com/Documentation/Splunk/6.3.0/Forwarding/Forwarddatatothird-partysystems)

**Step 2:** Configure syslog receiving on User-ID firewall/agent [https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/user-id/configure-user-id-to-receive-user-mappings-from-a-syslog-sender.html](https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/user-id/configure-user-id-to-receive-user-mappings-from-a-syslog-sender.html)

5.2 Method 2: Searchbar Command

Use the `panuserupdate` command that is included with the app.

For this method, the logs are not required to contain both the user and ip in the same log. For example, where there is an authentication log with user and MAC address, and a DHCP log with MAC address and IP address. Splunk can
do a search correlating the user to the IP using the MAC as the common value, then pass the search results to the `panuserupdate` command which will update the mapping on the firewall.

See `panuserupdate` in the Searchbar Command documentation.

**5.3 Distribute User-ID**

To simplify administration, you can configure one firewall to be the redistribution firewall that collects all the mapping information and shares it with other firewalls. You configure the receiving firewalls to retrieve the mapping information from the redistribution firewall.


**Warning:**

This documentation is deprecated in Splunk App and Add-on version 6.0. The latest documentation is now available here: [http://splunk.paloaltonetworks.com/commands.html](http://splunk.paloaltonetworks.com/commands.html)
There are several custom commands in the app that can communicate to the Palo Alto Networks next-generation firewall to make changes. These commands take the events from the search as input, and add context the firewall so it can better enforce its security policy.

### 6.1 panuserupdate

The `panuserupdate` command synchronizes user login events with Palo Alto Networks User-ID. More information: *User-ID with Splunk*

Added in App version 5.0. For previous versions, refer to the `panupdate` command.

**Syntax:**

```bash
panuserupdate device=<hostname>|panorama=<hostname>
[serial=<serial-of-device-in-panorama>] [vsys=<vsys#>]
[action=<login|logout>] [ip_field=<field-containing-IPs>]
user_field=<field-containing-usernames>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>device</td>
<td></td>
<td>IP or hostname of firewall</td>
</tr>
<tr>
<td>panorama</td>
<td></td>
<td>IP or hostname of Panorama</td>
</tr>
<tr>
<td>serial</td>
<td>vsys1</td>
<td>Serial of firewall (required if using panorama parameter)</td>
</tr>
<tr>
<td>vsys</td>
<td></td>
<td>VSYS ID (e.g. vsys2)</td>
</tr>
<tr>
<td>action</td>
<td>login</td>
<td>Tell the firewall user logged in or logged out</td>
</tr>
<tr>
<td>ip_field</td>
<td>src_ip</td>
<td>Log field containing IP address</td>
</tr>
<tr>
<td>user_field</td>
<td>user</td>
<td>Log field containing the username</td>
</tr>
</tbody>
</table>

**Example 1:** When a radius authentication log is received by Splunk, tell the firewall that the user logged. This command would cause the firewall with management IP 192.168.4.211 to receive the user-to-IP mapping:

```bash
index=main sourcetype=radius | panuserupdate device="192.168.4.211"
```
Example 2: The previous example assumes the user and ip are in fields named user and src_ip. If this is not the case, rename the fields or tell the command what fields to use.

Rename the fields:

```splunk
index=main sourcetype=radius | rename addr AS ip | rename authuser AS user | → panuserupdate panorama="10.5.5.8" serial="0001A13800105"
```

Call out the fields:

```splunk
index=main sourcetype=radius | panuserupdate panorama="10.5.5.8" serial= → "0001A13800105" vsys="vsys4" ip_field="addr" user_field="authuser"
```

The first search renames the fields before passing them to the panuserupdate command. It also uses Panorama to connect to a firewall with the serial number 0001A13800105. This is the User-ID firewall connected to Panorama.

The second search tells the panuserupdate command which fields contain the ip and user. It also passes this information via Panorama to a firewall, but this example specifies the update is for vsys4 on the firewall.

Example 3: Notifies the firewall of a radius user logout via Panorama. The default fields src_ip and user are used to gather the IP and Username:

```splunk
sourcetype=radius logout | panuserupdate panorama="10.4.4.4" serial="004001028200 →" action="logout"
```

See also:

- User-ID with Splunk
- Sync user login events with User-ID

6.2 pantag

The pantag command shares context with the firewall by tagging IP addresses found in Splunk into Dynamic Address Groups.

Command added in App version 4.1. New parameters added in App version 5.0.

Syntax:

```splunk
pantag device=<hostname>|panorama=<hostname> [serial=<serial-of-device-in-panorama>] [vsys=<vsys#>] [action=<add|remove>] [ip_field=<field-containing-IPs>][tag=<tag>|tag_field=<field-containing-tags>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Added in</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>device</td>
<td>4.1</td>
<td></td>
<td>IP or hostname of firewall</td>
</tr>
<tr>
<td>panorama</td>
<td>5.0</td>
<td></td>
<td>IP or hostname of Panorama</td>
</tr>
<tr>
<td>serial</td>
<td>5.0</td>
<td></td>
<td>Serial of firewall (required if using panorama parameter</td>
</tr>
<tr>
<td>vsys</td>
<td>vsys1</td>
<td>5.0</td>
<td>VSYS ID (eg. vsys2)</td>
</tr>
<tr>
<td>action</td>
<td>add</td>
<td>4.1</td>
<td>Add or remove the tag</td>
</tr>
<tr>
<td>ip_field</td>
<td>src_ip</td>
<td>4.1</td>
<td>Same as ip_field parameter (deprecated in 5.0, use ip_field)</td>
</tr>
<tr>
<td>tag</td>
<td>src_ip</td>
<td>5.0</td>
<td>Log field containing IP address to tag</td>
</tr>
<tr>
<td>tag_field</td>
<td></td>
<td>4.1</td>
<td>Tag for the IP, referenced in the Dynamic Address Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.0</td>
<td>Log field containing the tag for IP address in the same log</td>
</tr>
</tbody>
</table>
Note: Prior to App version 5.0, the `ip_field` parameter is just `field`.

**Example 1:** Any IP on the network that generated a spyware (command-and-control traffic) alert is tagged as an infected host on the firewall at 10.1.1.1:

```
|pan_threat| log_subtype="spyware" | stats dc(src_ip) by src_ip | pantag device="10.1.1.1" action="add" tag="infected-host"
```

In this example, any device that is sending command and control traffic will be tagged with `infected-host`. Your security policy could limit the reach of IP addresses with this tag until the incident is remediated. Or it could present a captive portal to the user indicating the problem and steps to contact IT.

**Example 2:** Tag any IP that is generating linux syslogs as a linux host on the firewall. Tag is applied to the firewall with serial 0005001028200 via the Panorama at 10.4.4.4:

```
sourcetype="linux_messages_syslog" | pantag panorama="10.4.4.4" serial="0005001028200" ip_field="host" tag="linux-host"
```

**Example 3:** Tag every IP address on the firewall with their Splunk classification (from the IP classification lookup table):

```
|pan_traffic| pantag device="10.1.1.1" ip_field="src_ip" tag_field="src_class"
```

**Example 4:** If anyone tries to connect to www.splunk.com, remove the tag 'suspicious-ip-address' from the IP of the website. Tag is removed on vsys3 of firewall with hostname main-fw.company.com:

```
|pan_url| dest_hostname="www.splunk.com" | pantag device="main-fw.company.com" vsys="vsys3" action="remove" ip_field="dest_ip" tag="suspicious-ip-addresses"
```

Note: The IP is tagged on the firewall immediately, however, it can take up to 60 seconds for the tagged IP addresses to show up in the corresponding Dynamic Address Group in the security policy. This delay is intentional to prevent accidental DoS scenarios.

### 6.3 pancontentpack

Update the app and threat lookup tables from the latest firewall content pack.

Added in App version 5.0

For usage instructions, see *Update metadata from content packs*.

### 6.4 Legacy commands

#### 6.4.1 panblock

Deprecated in App version 4.1. Use `pantag` instead.

Removed in App version 5.2.
Modify the configuration of the firewall address groups to include IP addresses from events in Splunk. This is similar to tagging IP addresses and works the same way, but is much less dynamic than tagging because it is modifying the firewall configuration and requires a configuration commit.

```
index=pan_logs sourcetype=pan_threat log_subtype=vulnerability | stats dc (src_ip) → by (src_ip) | panblock device="1.0.0.1" action="add" group="attackers"
```

### 6.4.2 `panupdate`

Deprecated in App version 5.0. Use `panuserupdate` instead.

Removed in App version 5.2.

The Palo Alto Networks firewall will inform Splunk of the user generating each connection via the syslogs it sends to Splunk. This assumes that the firewall is getting the login information from AD or some other authentication system, to know what user is logged into the device generating the traffic.

If authentication logs are being indexed by Splunk, then Splunk can share knowledge of where users are logged in to the firewall. For example, if Splunk is receiving a radius authentication log where ‘user’ is the field containing the user who authenticated, and ‘ip’ is the field containing the IP address where the user logged in, then you can map the user to the ip on the firewall using the `panupdate` command like so:

```
index=main sourcetype=radius | rename user AS addruser | rename ip AS addrip | → panupdate device="192.168.4.211"
```

This would cause the firewall with management IP 192.168.4.211 to receive the user-to-IP mapping. The mapping times out after 30 minutes.

**Warning:**

This documentation is deprecated in Splunk App and Add-on version 6.0. The latest documentation is now available here: [http://splunk.paloaltonetworks.com/universal-forwarder.html](http://splunk.paloaltonetworks.com/universal-forwarder.html)
This document assumes you already have syslog-ng, Splunk Universal Forwarder and Splunk installed and will not cover installation.

You should also have the Palo Alto Networks for Splunk app and add-on installed as described in Getting Started

Note: The App and Add-on do not need to be installed on the Universal Forwarder.

### 7.1 Step 1: Setup Syslog-ng

Add the following lines to the `/etc/syslog-ng/syslog-ng.conf` file. This example uses the default install location of syslog-ng on an ubuntu server. Change the directory as need.

Under “Sources” add a source in syslog-ng to listen for logs on a port. This example uses port UDP 514:

```plaintext
source s_udp514 {
    network(
        transport("udp")
        port(514)
        flags(no-parse)
    );
};
```

Under “Destinations” specify a .log file destination:

```plaintext
destination d_udp514 { file("/YOURPATH/udp514.log" template("$MSG\n")); }
```

Under “Log paths” specify the path of the log:

```plaintext
log { source(s_udp514); destination(d_udp514); }
```

Save `syslog-ng.conf` and restart syslog-ng:
7.2 Step 2: Configure Splunk Universal Forwarder

Configure the Universal Forwarder to monitor the `/YOURPATH/udp514.log` file created in step 1.

Create or modify `/opt/splunkforwarder/etc/system/local/inputs.conf` and add a monitoring stanza:

```
[monitor:///YOURPATH/udp514.log]
sourcetype = pan:log
```

Create or modify `/opt/splunkforwarder/etc/system/local/outputs.conf` and add a tcpout stanza:

```
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 192.168.0.3:9997

[tcpout-server://192.168.0.3:9997]
```

**Note:** Replace the IP address 192.168.0.3 with the IP of Splunk indexer.

To forward to multiple Splunk servers use this tcpout stanza instead:

```
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 192.168.0.1:9997,192.168.0.2:9997,192.168.0.3:9997

[tcpout-server://192.168.0.1:9997]
[tcpout-server://192.168.0.2:9997]
[tcpout-server://192.168.0.3:9997]
```

Restart Splunk Universal Forwarder:

```
$ /opt/splunkforwarder/bin/splunk restart
```

7.3 Step 3: Configure Splunk Indexer

If it doesn’t exist, add a listening port on Splunk Indexer:

1. From the Web Interface navigate to Settings->Forwarding and receiving
2. Under Receive Data, click on Configure receiving
3. If port 9997 is already listed then you are done
4. Otherwise, click on New
5. Add port 9997 to Listen on this port
6. Click Save
7.4 Step 4: Verify

Verify logs are being forwarded correctly by searching for the following:

```
source="/YOURPATH/udp514.log"
```

Change the source to the directory and file you are monitoring.

Verify that `sourcetype` is being transformed. You should see `pan:traffic, pan:system, pan:threat, pan:config` as the sourcetype.

If `log sourcetype` is `pan:log` then syslog-ng is changing the logs and they are not being transformed. Go back to step 1 and verify you made the correct changes.

**Note:** If the Indexer has not been running and receiving for a lengthy period of time. It may take awhile for logs to show up.

**Warning:**

This documentation is deprecated in Splunk App and Add-on version 6.0. The latest documentation is now available here: [http://splunk.paloaltonetworks.com/faq.html](http://splunk.paloaltonetworks.com/faq.html)
8.1 Why use Splunk with my Palo Alto Networks products?

Palo Alto Networks products provide exceptional levels of visibility into network traffic and malicious activity, both in the network and on the endpoint. Combining this visibility with Splunk allows a customer to make correlations and perform analytics around different kinds of data. These correlations can be between different kinds of Palo Alto Networks data, for example, correlating WildFire reports against traffic logs to detect infected hosts, or correlating firewall logs with endpoint logs. But the real power of Splunk is correlations and analytics across multiple sources of data and multiple vendors, for example, correlating firewall logs with webserver logs, or advanced endpoint security logs with Windows event logs.

8.2 Why use Palo Alto Networks with my Splunk?

Splunk has unmatched ability to consume and analyze data, but for Splunk to present usable and actionable insights, it must have the highest level of visibility and knowledge possible. Palo Alto Networks provides that level of visibility into the network and the endpoint to detect and even predict malicious activity. When an indicator of compromise is detected, Palo Alto Networks and Splunk work together to take action and remediate problems automatically to keep the network secure.

8.3 What can the Palo Alto Networks Splunk App do?

The Splunk for Palo Alto Networks app is one of the most downloaded apps for Splunk and is completely free. Splunk apps tell Splunk how to handle data and come with dashboards that display visualizations and analysis of the data. The Splunk for Palo Alto Networks app brings in syslogs from firewalls, Panorama, and Traps Endpoint Security Manager and makes the data easily searchable, analyzes the data with correlations, and displays the data including any anomalies visually. When actionable alerts are produced, Splunk can take action by leveraging the firewall and Panorama APIs to add context that the firewall uses to prevent targeted threats.

Learn more:
8.4 What kinds of data does the app take in?

The Splunk for Palo Alto Networks app accepts syslogs from Firewalls, Panorama, and Endpoint Security Manager. Also, WildFire malware reports are pulled from the WildFire portal as XML. These reports represent a behavioral fingerprint of any malware detected by WildFire which you can correlate against other logs to detect indicators of compromise.

8.5 Does the app have a Data Model?

Yes! In Splunk 6.x, the data model feature allows Splunk users to quickly visualize and analyze data with a point-and-click interface (instead of the Splunk searchbar language). This capability requires that the data be modeled into a Splunk Data Model which is a highly accelerated summary index of the data. Not only is there a data model for all Palo Alto Networks logs, all the app’s dashboards are based on this accelerated data model for extremely fast data retrieval and visualization. So the app itself is using the same Data Model that Splunk administrators would use to generate visualizations.

8.6 Does the app conform to the Common Information Model?

Yes! The Common Information Model (CIM) is a set of standards and an app that help other apps conform to a common naming and tagging scheme. This allows Splunk users to search for data across multiple kinds of logs from multiple vendors using the same field names to access the data, which eases correlations across different kinds of data. For example, a Splunk user could correlate between firewall logs and webserver logs. The Splunk for Palo Alto Networks app conforms strictly to the Common Information Model.

8.7 Does the app work with the Splunk Enterprise Security app?

Yes! The Splunk Enterprise Security app (or “ES”), is a set of security log parsers and security related dashboards that conform to the Common Information Model. The Enterprise Security app contains a TA (parsers) for Palo Alto Networks firewall logs. The Splunk for Palo Alto Networks app and Enterprise Security app can be used individually, or together. The Palo Alto Networks Add-on 3.7 supports the new Adaptive Response capabilities of Splunk Enterprise Security.

8.8 I use Splunk ES with the Palo Alto Add-on (TA), why use the App?

The Palo Alto Networks App offers significant additional benefits including:

- Take immediate action to stop threats with automated remediation
- Index the behavioral footprint of malware seen by Wildfire
- Sync user logins from authentication logs to User-ID
- Update content pack metadata for apps and threats
- Datamodel with Pivots for easy access to data and visualizations
• Macros for easy access to logs
• Dashboards to track SaaS application usage, user activity, system health, configuration changes for audits, Wildfire malware, and other Palo Alto Networks specific features.

8.9 My question isn’t answered here, how do I get answers?

Here are a few ways to get your questions answered. Search for answers in this order:

• Check the App Documentation at http://pansplunk.readthedocs.io
• Search on Splunk Answers
• If you can’t find an answer or need support, ask a question using the instructions on the Get Support page.

Warning:
This documentation is deprecated in Splunk App and Add-on version 6.0. The latest documentation is now available here: http://splunk.paloaltonetworks.com/troubleshoot.html
CHAPTER 9

Troubleshooting

9.1 Common Problems and Solutions

9.1.1 Problem after upgrading the App/Add-on

Check the Release Notes for actions needed during App/Add-on upgrade and ensure you completed all required actions for upgrade.

When upgrading any app in Splunk, configuration created by the Splunk administrator is leftover in the app’s local directory. If the file in the local directory in the app is not compatible with the new version, then unexpected problems can happen. This is true for all apps in Splunk and a best practice is to backup and delete the local directory in the app after upgrading it if there are problems after the upgrade. Note that you might need to leave inputs.conf if that is how your logs are getting into Splunk.

9.1.2 Dashboards not working

All dashboards have no data

Perform a search for `eventtype=pan` with ‘All time’ as the timeframe. If logs show up, then verify the timestamp of the logs is correct. If it is wrong, check that the clock and timezone on the Firewall/Panorama matches the Splunk server, or use NTP on both. See Troubleshooting Step 2 below for more detail.

Only ‘Overview’ dashboard has data

The ‘Overview’ dashboard has data, but other dashboards do not, usually the datamodel is not fully built. This can happen on a Splunk server with not enough resources to summary index the data as it comes in. Increase the time range on the dashbaords with no data to ‘All Time’ to see if data shows up. Check the datamodel to see if it is 100% built. See Troubleshooting Step 4 below for more detail.

‘Overview’ dashboard has no data

The ‘Overview’ dashboards has no data, but other dashboards work correctly, the clock on your firewall is a few minutes off, or the timezone is set wrong. The ‘Overview’ dashboard is a real-time 5 minute search, while the other
dashboards pull a larger timeframe from the data model. So the ‘Overview’ is more susceptible to minor variations in system clock. Please verify the clock and timezone on Splunk and the Firewall/Panorama are set exactly the same.

9.1.3 No WildFire Data

The WildFire dashboard is empty or no WildFire data is appearing in the index. For Splunk to take advantage of WildFire, you log WildFire events from the Firewall/Panorama first. Splunk will leverage the WildFire cloud API to pull reports and IOC’s from the WildFire analysis only after it receives notification of the WildFire event from the Firewall/Panorama.

Some things to check to get WildFire data into Splunk:

- If upgrading to App 5.3 or higher from a version before 5.3, you must set the WildFire API key in the Add-on Setup Screen, even if you previously set it in the App. See the release notes for more information.
- Verify there are WildFire Submission logs in the Monitor tab on the Firewall/Panorama
- Verify WildFire logs are enabled in the Log Forwarding Profile on the Security policy rule which is generating WildFire events
- Verify WildFire events are received by Splunk with this search: `eventtype=pan_wildfire`
- If there are WildFire events (syslogs), verify there are also WildFire reports (XML) with this search: `eventtype=pan_wildfire_report`
- If there are WildFire events (syslogs) but not WildFire reports (XML), check the report gathering logs for errors in `$SPLUNK_HOME/var/log/splunk/python.log`.
- Check that you have configured the TA with the WildFire API Key, especially if upgrading from a pre-5.3 version of the App.

9.2 Troubleshooting Steps

Follow these troubleshooting steps if there are problems getting the dashboards to show data.

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

- Verify inputs.conf is set up per the instructions. inputs.conf must have the line `no_appending_timestamp = true` for UDP syslogs
- Check for other inputs.conf outside the App or Add-on that might be using the same port
- Check the firewall is not using a Custom Log Format (must use the default log format)
- Check the Endpoint Security Manager is using CEF format
- Check the firewall is set to log something like system events, config events, traffic events, and so on.
- Check that the clocks and timezones 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, then switch to TCP or SSL once UDP is working

**Step 2. Verify logs are indexed**

Use the method described in the Test the configuration section 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:

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

- Verify the configuration from Step 1 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 Splunk server and firewall have the same time and timezone set. Use NTP if possible.
- Use tcpdump or Wireshark on the Splunk server to verify the logs are actually reaching it.
- Verify the App (and Add-on when using App v5.0 and higher) is installed on all searchheads, indexers, and heavy forwarders.
- If using App v3.x or 4.x, verify the pan_logs index exists.

**Step 3. Verify logs are parsed correctly**

Use the method described above in the *Test the configuration* section to produce some syslogs. Verify the logs are reaching the Splunk server by navigating to the Palo Alto Networks App, click ‘Search’ in the navigation bar, and enter the following search:
If logs showed in step 2, but no logs show up now, 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 using UDP syslogs.
- 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.
- Verify the App (and Add-on when using App v5.0 and higher) is installed on all searchheads, indexers, and heavy forwarders.

Step 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, then go back to the previous troubleshooting steps. 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 > and find the Palo Alto Networks datamodels. (There may be 1 or 3 datamodels depending on the App version)
- Verify that acceleration is enabled for all Palo Alto Networks datamodels.
- Click the arrow next to the Palo Alto Networks data models and check the 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. Try disabling unused apps, removing acceleration from other datamodels, or adding hardware resources. If you need help troubleshooting performance problems with datamodels, you can open a case with Splunk Support. Note that Splunk Support will not troubleshoot the Palo Alto Networks App, but they can tell you what is causing any performance problems that prevent your datamodels from accelerating fast enough to keep up with new data.

**Step 5. Get support**

If you get to the end of these troubleshooting steps and you still can’t figure out what’s wrong, please search Splunk Answers or ask a question using the information on the Get Support page.
This documentation is deprecated in Splunk App and Add-on version 6.0. The latest documentation is now available here: http://splunk.paloaltonetworks.com
Information on how to sample the Palo Alto Networks Splunk App and Add-on.

10.1 Event Gen

Event Gen is an app provided by Splunk in order to feed sample data into Splunk. The Event Gen app and documentation is available on Splunk Base
With Event Gen App installed and enabled with Palo Alto Networks App and Add-on, demo data will appear in the app.

Warning:
This documentation is deprecated in Splunk App and Add-on version 6.0. The latest documentation is now available here: http://splunk.paloaltonetworks.com/support.html
Get Support

Setup and configuration: See Getting Started

Troubleshooting Guide: See Troubleshooting

Need more help? Click the Ask a Question button at: http://splunkbase.splunk.com/app/491

Found a bug or need a feature? Open an issue on github

Note: The Palo Alto Networks App and Add-on are supported via the Ask a Question button on the App homepage. A notification is sent to a team of technical representatives at Palo Alto Networks and Splunk, including the developers of the app, who will respond as soon as possible.

Warning:

This documentation is deprecated in Splunk App and Add-on version 6.0. The latest documentation is now available here: http://splunk.paloaltonetworks.com/release-notes.html
12.1 App

v5.4.1

• Endpoint Dashboard bug fix

12.2 Add-on

v3.8.1

• Configuration screen bug fix

12.3 Previous Versions

12.3.1 App v5.4.0

• Endpoint Operations Dashboard
• Endpoint Security Dashboard
• Endpoint Dashboard support new Traps 3.4 fields
• Support for AutoFocus Remote Search via External Search Handler
• Support for Firewall Log Link via External Search Handler
• Improved AutoFocus cross launch
12.3.2 Add-on v3.8.0

- AutoFocus Export List modular input
- Improved configuration screen allows credentials to be changed

12.3.3 App v5.3.1

- Changes made to meet new certification requirements

12.3.4 Add-on v3.7.1

- Changes made to meet new certification requirements

12.3.5 App v5.3.0

- GlobalProtect Dashboard
- Other updates are in the Add-on (see below)

Note:

- App 5.3.x requires Add-on 3.7.x
- REQUIRED ACTION: The App setup screen has moved to the Add-on. If you had previously set firewall credentials or a WildFire API key in the App setup screen, you’ll need to set them again in the Add-on setup screen. See Step 2: Initial Setup in the updated Getting Started Guide. You may delete the file $SPLUNK_HOME/etc/apps/SplunkforPaloAltoNetworks/local/passwords.conf to remove the credentials from the App, since they are no longer used.
- Datamodel acceleration might rebuild itself after installation due to updated constraints
- Eventtype pan_threat no longer includes these log_subtypes: url, data, file, and wildfire. You might need to update custom searches or panels you created that leverage the pan_threat eventtype. There are new eventtypes for each of the removed log_subtypes: pan_url, pan_data, pan_file, and pan_wildfire.

12.3.6 Add-on v3.7.0

- Integration with new Splunk Adaptive Response
- Tag to dynamic address group using modular actions and Adaptive Response
- Submit URL’s from any log in Splunk to WildFire
- Logs with malware hashes have a new event action that links directly to that hash in Autofocus
- Improved tagging for Splunk Enterprise Security, based on customer feedback
- New parser for GlobalProtect logs

Note: Eventtype pan_threat no longer includes these log_subtypes: url, data, file, and wildfire. You might need to update custom searches or panels you created that leverage the pan_threat eventtype. There are new eventtypes for each of the removed log_subtypes: pan_url, pan_data, pan_file, and pan_wildfire.
12.3.7 App v5.2

- Certified by Splunk
- Removed deprecated commands (panblock and panupdate) as a requirement for certification.
- Removes support for Splunk 6.1 and earlier as a requirement for certification.

**Note:** If you are using Splunk 6.1 or earlier, you must upgrade to Splunk 6.2 or later before upgrading to App v5.2.0. If you currently use panblock or panupdate commands, please update your usage of the App to leverage pantag and panuserupdate instead.

12.3.8 Add-on v3.6

v3.6.1
- Certified by Splunk
- Add logo files for Splunkbase

v3.6.0
- Support new Traps 3.3.2 log format

**Note:** Traps versions before 3.3.2 are no longer supported beginning with Add-on 3.6.0 and App 5.1.0.

12.3.9 App v5.1.0

- Datamodel updated to support new Traps 3.3.2 fields
- Endpoint Dashboard updated to support new Traps 3.3.2 fields

**WARNING:** Traps versions before 3.3.2 are no longer supported beginning with this App version

12.3.10 App v5.0.1

- Fix error when using pantag command with single firewall
- Fix error when using pancontentpack command
- Improved searchbar command logging

12.3.11 Add-on v3.5.3

- Fix issue where endpoint logs would show up in CIM apps, but not Palo Alto Networks app

12.3. Previous Versions
12.3.12 App v5.0.0

This major release re-architects the Palo Alto Networks App by splitting it into an App and an Add-on. The Palo Alto Networks Add-on is included in the Palo Alto Networks App and is installed or upgraded automatically with the App. Review the Upgrade Guide to upgrade to version 5.0.0.

In addition to the new Palo Alto Networks Add-on, this version also has the following new features:

- New SaaS dashboard with Un/Sanctioned SaaS Detection
- CIM 4.x compliance
- Optimized Datamodel for better performance and storage efficiency
- Logs are no longer required to be stored in the pan_logs index
- Auto update script for app and threat lookup tables
- New panuserupdate command for User-ID update
- Enhanced pantag command to leverage log data for tags
- Both commands now support Panorama and VSYS targets, and are more efficient and scalable
- Better command documentation
- Changed from CC license to ISC license
- All new documentation website at http://pansplunk.readthedocs.io

12.3.13 Add-on v3.5.1

- Add support for PAN-OS 7.0 new fields
- Add hip-match log type from Firewall and Panorama
- Add sourcetype category
- Add Sanctioned SaaS lookup table (see Un/Sanctioned SaaS Detection)
- Update app_list.csv and threat_list.csv lookup tables with new format and data
- Fix incorrect value in report_id field for Wildfire logs in PAN-OS 6.1 or higher
- Fix src_category field should be dest_category

12.3.14 Add-on v3.5.0

Included with Splunk Enterprise Security 4.

This new Add-on (TA) for Palo Alto Networks supports logs from Palo Alto Networks Next-generation Firewall, Panorama, and Traps Endpoint Security Manager. It is CIM 4.x compliant and designed to work with Splunk Enterprise Security 4 and the Palo Alto Networks App for Splunk v5.

12.3.15 v4.2.2

- Fix drilldowns in Wildfire and Content dashboards
- Fix panel in Content dashboard to display correct data
12.3.16 v4.2.1

- Fix Wildfire Report downloader and Applipedia New App check
- Fix Wildfire Dashboard Drilldowns
- Fix Threat Details Dashboard datamodel reference
- Fix Endpoint Dashboard would not work on Splunk 6.0.x
- Fix time range inconsistent on Overview Dashboard
- Fix issue where Endpoint Dashboard disappears if Netflow is enabled.

12.3.17 v4.2

- New Palo Alto Networks Advanced Endpoint Protection
- Support Palo Alto Networks PAN-OS 6.1

12.3.18 v4.1.3

- Special commands (panblock, panupdate, pantag) now available from other apps
- Fix issue with unknown lookup errors during search
- Fix issue with meta scope and global namespace

12.3.19 v4.1.2

- Fix some Threat dashboard drilldowns
- Fix scope of CIM fields to remove conflict with some apps
- Remove macros from datamodel that were causing slower acceleration

Note: changes to datamodel may require the acceleration to be rebuilt before data will show up in the dashboards

12.3.20 v4.1.1

- Handle new fields in latest PAN-OS syslogs and WildFire reports
- Significant improvements to indexing efficiency
- Improved handling of Dynamic Address Group tagging
- Improvements and minor updates for Splunk 6.1.x
- Fix minor dashboard issues
- Fix minor field parsing issue

12.3. Previous Versions
12.3.21 v4.1

This is a major update. If upgrading from a previous version, please read the Upgrade Notes in the documentation.

- PAN-OS Data model including acceleration
- Data model accelerated dashboards (replaces TSIDX-based dashboards)
- New command: pantag - tag IP addresses on the firewall into Dynamic Address Groups
- IP Classification - add metadata to your CIDR blocks, classifying them as internet/external/dmz/datacenter/etc.
- Applipedia change notifications and highlighting - know when Palo Alto Networks releases new application signatures and if those applications are on your network

12.3.22 v4.0.2

- Fix: Overview dashboard optimizations
- Fix: Top Applications panel would sometimes show error
- Fix: Traffic dashboard form filter works

12.3.23 v4.0.1

- Fix: Config dashboard shows all events
- Fix: Better handling of navbar changes

12.3.24 v4.0

- Splunk 6 support
- Dashboards converted to Splunk 6 SimpleXML, meaning dashboards can now:
  - Print
  - Export as pdf
  - Produce scheduled reports
  - Use pre-populated dropdowns in filters
  - Change using SplunkWeb by editing the panels
- Maps converted to Splunk 6 built-in maps (removes dependencies on other apps)
- Updated navbar including icons and colors

12.3.25 v3.4

- NetFlow support using NetFlow Integrator, a 3rd party program from NetFlow Logic
  - New set of dashboards, charts and graphs centered around NetFlow records from Palo Alto Networks devices
  - App-ID and User-ID information is available in NetFlow records

Download a 30-day free trial of NetFlow Integrator at https://www.netflowlogic.com/downloads
Steps to configure NetFlow are available in the NetFlow section of the app documentation and README.
12.3.26 v3.3.2

- Fix: URL in WildFire dashboard corrected
- Fix: Overview dashboard colors were gray on some servers, set back to white
- Fix: Corrected description fields in commands.conf that resulted in log errors
- Fix: Corrected sourcetype in inputs.conf.sample

12.3.27 v3.3.1

- Fix: App setup screen allows blank values
- Fix: Several GUI fixes and enhancements

12.3.28 v3.3

- Malware analysis reports from the WildFire Cloud are dynamically downloaded and indexed when a WildFire log is received from a firewall.
- WildFire dashboard
  - Recent WildFire events
  - Graphs of WildFire statistical data
  - Detect compromised hosts using malware behavior to traffic log correlation

Note: Malware analysis report retrieval requires a WildFire API Key from https://wildfire.paloaltonetworks.com

12.3.29 v3.2.1

Bug Fixes:

- savedsearches.conf: changed hard coded index=pan_logs to pan_index in scheduled searches. Thanks to Genti Zaimi for finding the issue and providing the fix
- pan_overview_switcher_maps.xml: modified geoip search to include localop to force the search to run on the searchhead. Thanks to Genti Zaimi for identifying the problem and providing the fix