Pulse Secure®
Acquired by Ivanti

Pulse Policy Secure: Splunk Enterprise

Integration Guide

Product Release	9.1R5
Published	March 2021
Document Version	1.4

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

© 2021 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse Policy Secure: Splunk Enterprise

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Purpose of this Guide

This guide describes how to integrate Pulse Policy Secure (PPS) with Splunk Enterprise for Alert-based admission control. It also describes how to install Pulse Policy Secure Syslog Add-on on Splunk for receiving syslog data from one or more PPS servers. After the PPS syslog Add-On is installed, the Splunk Dashboard displays charts displaying the events captured from PPS syslog messages.

Prerequisites

This guide assumes you are familiar with the use of the following products and their related terminology.

- Pulse Policy Secure at version 9.1R5.
- Splunk Enterprise at version 7.3.1.1

© 2019 Pulse Secure, LLC.

PPS Integration with Splunk Enterprise

This section describes Splunk Enterprise SIEM device integration with PPS. It covers the following chapters:

© 2020 Pulse Secure, LLC.

Alert-Based Admission Control with Splunk Enterprise

Overview

Pulse Policy Secure (PPS) integration with the *Splunk Enterprise* provides complete visibility of network endpoints, including unmanaged endpoints and provide end to end network security. The PPS integration with Splunk integration allows Admin to perform user access control based on alerts received from the Splunk.

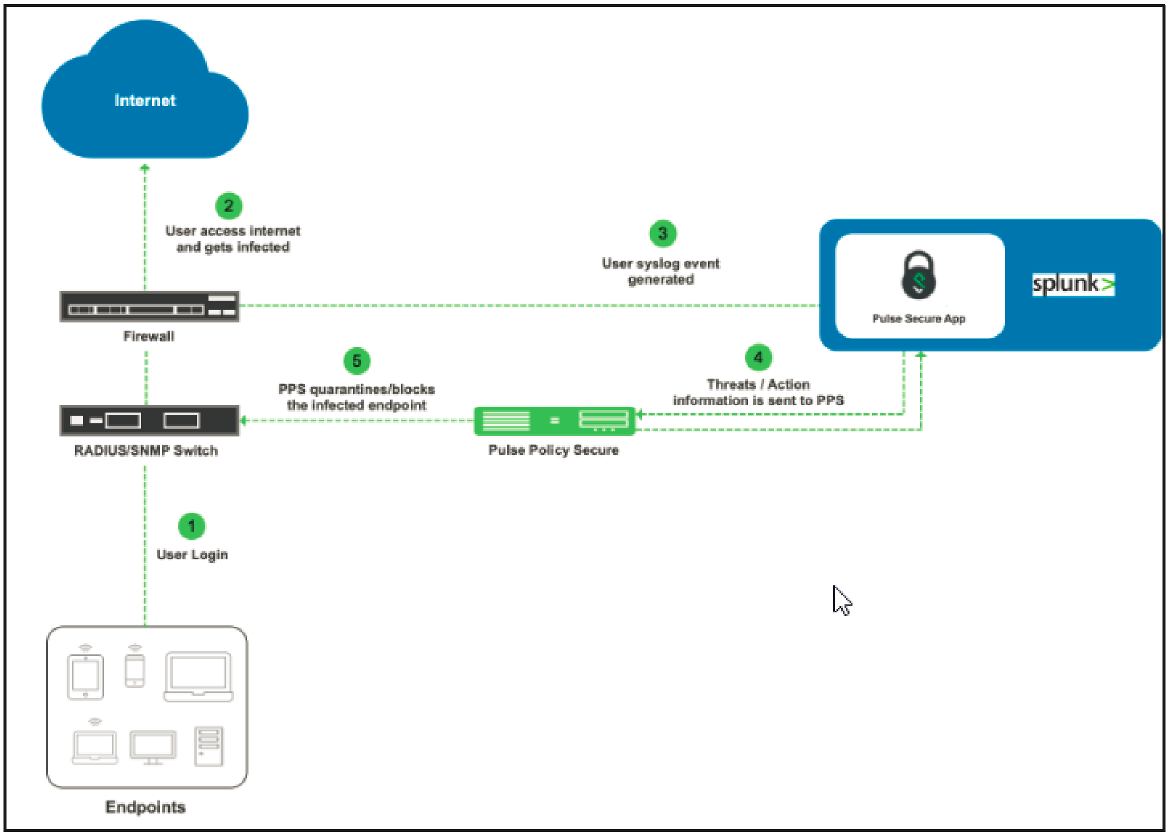
Splunk Enterprise receives log or threat information from various log sources such as Palo Alto Network firewall. Based on these logs/alerts a search query is created on Splunk to trigger alerts to PPS. PPS takes action on user session by blocking or quarantining the user.

The authentication process is described below:

1. User downloads a file from the Internet. The perimeter firewall scans the file and, based on user-defined policies, sends the file for analysis.
2. Firewall detects that the file contains malware and a threat alert sylog gets generated and sent to Splunk Enterprise.
3. Based on the alert rules configured on Splunk. It generates alerts and this has to be manually sent to PPS with the help of Pulse Policy Secure App.
4. The Alert includes severity for the affected endpoint to PPS.
5. The PPS server quarantines/blocks the endpoint based on the configured Admission control policies.

© 2020 Pulse Secure, LLC.

Figure 1 Deployment using PPS, Splunk Enterprise and Palo Alto Networks Firewall


Internet
2
User access internet and gets infected
3
User syslog event generated
Pulse Secure App
splunk>
Firewall
5
PPS quarantines/blocks the infected endpoint
4
Threats / Action information is sent to PPS
RADIUS/SNMP Switch
Pulse Policy Secure
1
User Login
Endpoints

In this example, the endpoint is connected to a third-party switch. The switch has 802.1X/MAB authentication enabled. As an alternate, SNMP enforcement mechanism can also be used.

Summary of Configuration

To prepare your network to perform alert-based admission control using Pulse Policy Secure, Splunk Enterprise and Firewall, perform the following tasks:

- "Configuring PPS with Splunk Enterprise" on page 5
- "Configuring Splunk Enterprise" on page 10

The following sections describe each of these steps in detail.

Configuring PPS with Splunk Enterprise

The PPS configuration requires defining the Splunk Enterprise as a client in PPS. PPS acts as a REST API server for Splunk Enterprise.

A high-level overview of the configuration steps needed to set up and run the integration is described below:

- The Administrator configures the basic PPS configurations such as creating an authentication server, authentication realm, user roles, and role mapping rules.

- Configure Splunk as a client in PPS. PPS acts as a REST API Server for Splunk. The REST API access for the admin user needs to be enabled by accessing the serial console or alternatively from the PPS admin UI (Authentication > Auth Server > Administrators > Users > click “admin”, enable Allow access to REST APIs).
- Configure PPS to block/quarantine the endpoint based on the threat prevention policy.
- Configure the Switches/WLC as RADIUS Client in PPS (Endpoint Policy > Network Access > Radius Clients > New Radius Client). Switch should be configured with PPS as a RADIUS server.
- Configure RADIUS return attribute policies to define the action upon receiving the event.

Note: Ensure that PPS has the endpoint IP Address for the enforcement to work correctly.

This section covers the following topics:

- “Admission Control Template” on page 6
- “Admission Control Client” on page 6
- “Admission Control Policies” on page 7

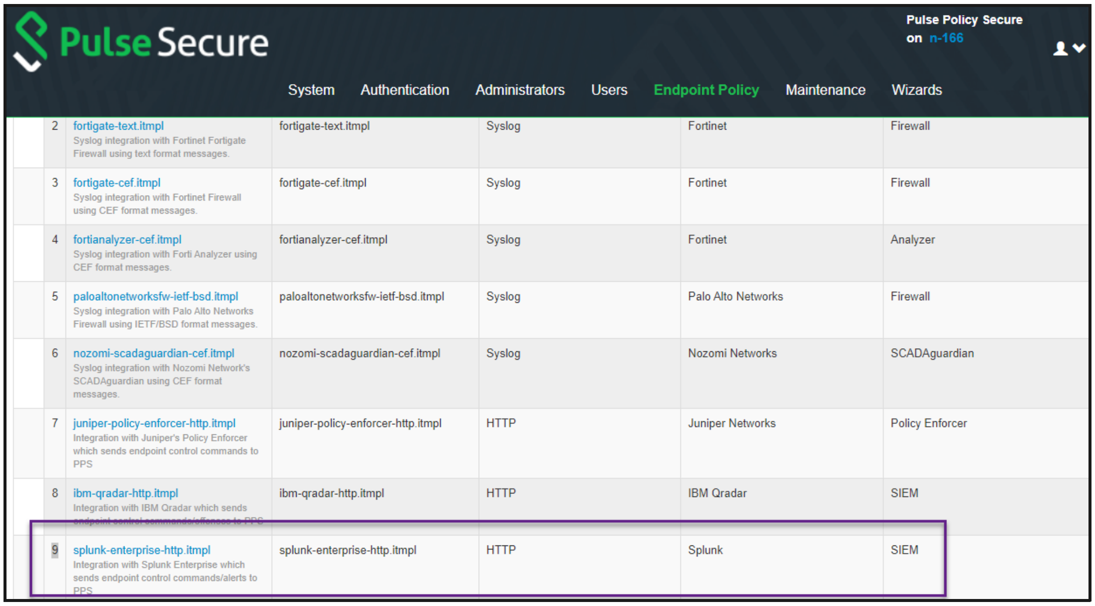
Admission Control Template

The admission control template provides the list of possible events that can be received from the network security device along with regular expression to parse the message. The template also provides possible actions that can be taken for an event. PPS is loaded with default templates for Splunk enterprise.

To view the admission control template in PPS:

1. Select **Endpoint Policy > Admission Control > Templates**.

Figure 2 Splunk Enterprise Template



2	fortigate-text.itmpl Syslog integration with Fortinet Fortigate Firewall using text format messages.	fortigate-text.itmpl	Syslog	Fortinet	Firewall
3	fortigate-cef.itmpl Syslog integration with Fortinet Firewall using CEF format messages.	fortigate-cef.itmpl	Syslog	Fortinet	Firewall
4	fortianalyzer-cef.itmpl Syslog integration with Forti Analyzer using CEF format messages.	fortianalyzer-cef.itmpl	Syslog	Fortinet	Analyzer
5	paloaltonetworksfw-ietf-bsd.itmpl Syslog integration with Palo Alto Networks Firewall using IETF/BSD format messages.	paloaltonetworksfw-ietf-bsd.itmpl	Syslog	Palo Alto Networks	Firewall
6	nozomi-scadaguardian-cef.itmpl Syslog integration with Nozomi Network's SCADAguardian using CEF format messages.	nozomi-scadaguardian-cef.itmpl	Syslog	Nozomi Networks	SCADAguardian
7	juniper-policy-enforcer-http.itmpl Integration with Juniper's Policy Enforcer which sends endpoint control commands to PPS	juniper-policy-enforcer-http.itmpl	HTTP	Juniper Networks	Policy Enforcer
8	ibm-qradar-http.itmpl Integration with IBM Qradar which sends endpoint control commands/offenses to PPS	ibm-qradar-http.itmpl	HTTP	IBM Qradar	SIEM
9	splunk-enterprise-http.itmpl Integration with Splunk Enterprise which sends endpoint control commands/alerts to PPS	splunk-enterprise-http.itmpl	HTTP	Splunk	SIEM

© 2020 Pulse Secure, LLC.

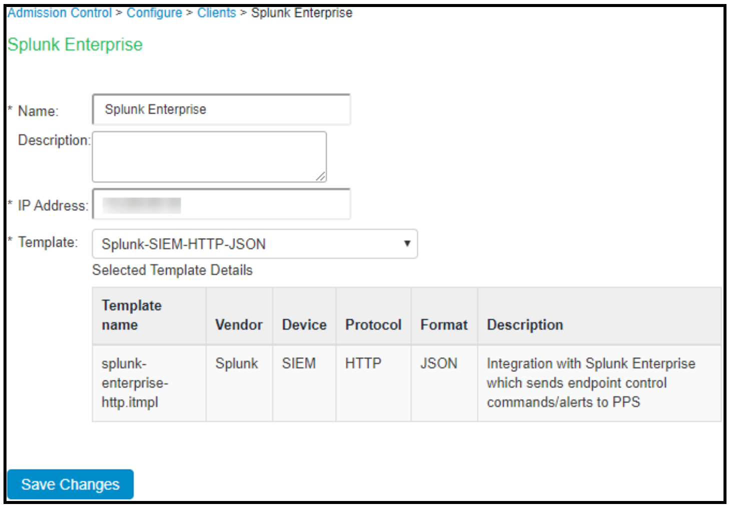
Admission Control Client

The admission control clients are the network security devices on which the syslog forwarding is enabled. The messages are received by the syslog server module running on PPS.

To add Splunk Enterprise as a client:

1. Select **Endpoint Policy > Admission Control > Clients**.
2. Click **New Client**.
3. Enter the name.
4. Enter the description.
5. Enter the IP address of the client.
6. Under Template, select Splunk-SIEM-HTTP-JSON.
7. Click **Save Changes**.

Figure 3 Template



Splunk Enterprise

* Name: Splunk Enterprise

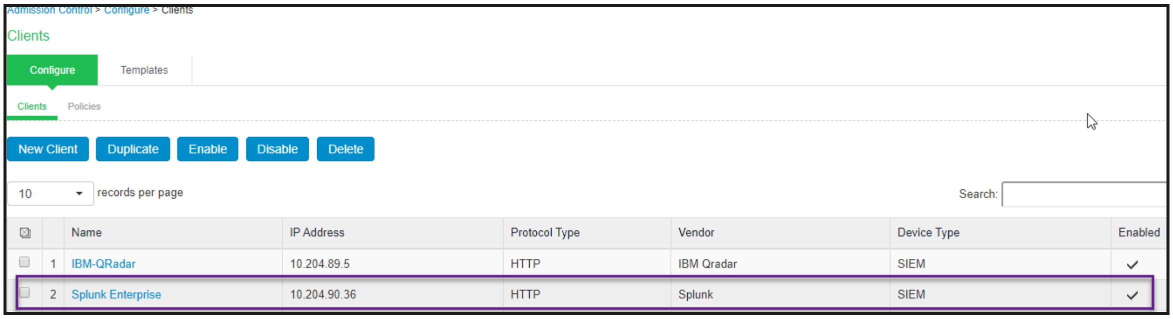
Description:

* IP Address: [redacted]

* Template: Splunk-SIEM-HTTP-JSON

Selected Template Details

Template name	Vendor	Device	Protocol	Format	Description
splunk-enterprise-http.itmpl	Splunk	SIEM	HTTP	JSON	Integration with Splunk Enterprise which sends endpoint control commands/alerts to PPS



10 records per page

Search:

☐		Name	IP Address	Protocol Type	Vendor	Device Type	Enabled
☐	1	IBM-QRadar	10.204.89.5	HTTP	IBM Qradar	SIEM	✓
☐	2	Splunk Enterprise	10.204.90.36	HTTP	Splunk	SIEM	✓

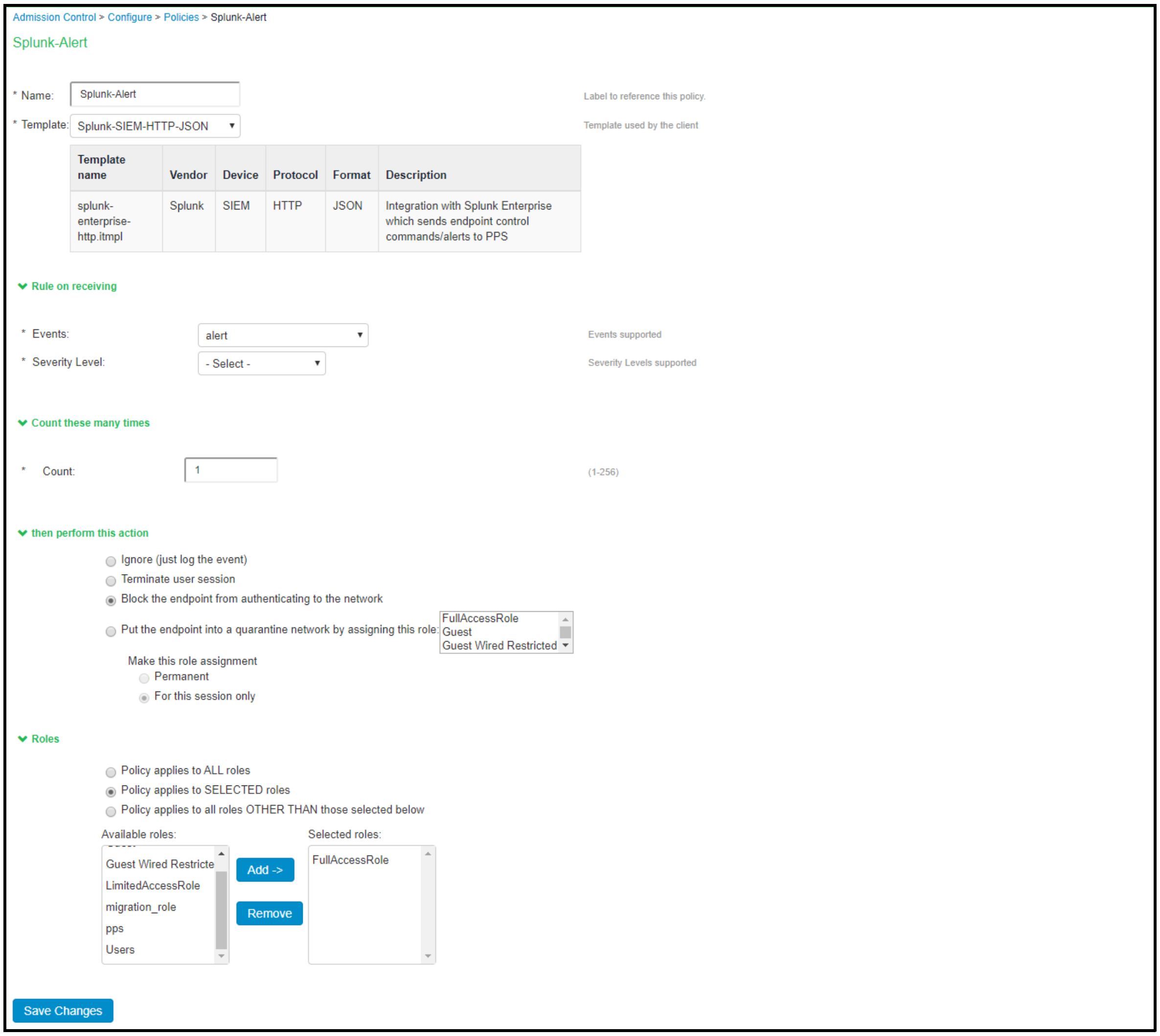
Admission Control Policies

The admission control policies define the list of actions to be performed on PPS for the user sessions. The actions are based on the event and the severity information received from the network security device.

1. To view and add the new integration policy:
2. Select **Endpoint Policy > Admission Control > Policies**.
3. Click **New Policy**.
4. Enter the policy name.
5. Select **Splunk-SIEM-HTTP-JSON** as a template.
6. Under Rule on Receiving, select the event type (block-endpoint, quarantine-endpoint, alert, any) and the severity level. The event types and the severity level are based on the selected template.
7. The actions on sessions supported are:
    - Block Endpoint: Blocks the host MAC Address on the PPS permanently. If admin choose to clear this, it can be cleared either by using Splunk application or by using the PPS Admin UI.
    - Quarantine Endpoint (Change user roles): Changes the roles assigned to the user on PPS so that restriction/privileges for the user can be changed.
    - Alert – Generated based on the Severity level of the alert. Specify the severity of the alert (High, Information, Low, Medium, Any)
8. Under then perform this action, select the desired action.
    - Block the endpoint from authenticating the network.
    - Put the endpoint into a quarantine network by assigning this role — choose the role to put endpoint in quarantine role. Specify whether to apply the role assignment permanently or only for the session.
    - Terminate user session—Terminates the user session on the PPS.
    - Ignore (log the event) —Received syslog event details are logged on the PPS and no specific action is taken.
9. Under Roles, specify:
    - Policy applies to ALL roles—To apply the policy to all users.
    - Policy applies to SELECTED roles—To apply this policy only to users who are mapped to roles in the Selected roles list. You must add roles to this list from the Available roles list.
    - Policy applies to all roles OTHER THAN those selected below—To apply this policy to all users except for those who map to the roles in the Selected roles list. You must add roles to this list from the Available roles list.

© 2020 Pulse Secure, LLC.

Figure 4 Configuration Policies



Admission Control > Configure > Policies > Splunk-Alert

Splunk-Alert

* Name: Splunk-Alert — Label to reference this policy.

* Template: Splunk-SIEM-HTTP-JSON — Template used by the client

Template name	Vendor	Device	Protocol	Format	Description
splunk-enterprise-http.itmpl	Splunk	SIEM	HTTP	JSON	Integration with Splunk Enterprise which sends endpoint control commands/alerts to PPS

Rule on receiving

* Events: alert — Events supported

* Severity Level: - Select - — Severity Levels supported

Count these many times

* Count: 1 — (1-256)

then perform this action

○ Ignore (just log the event)
○ Terminate user session
● Block the endpoint from authenticating to the network
○ Put the endpoint into a quarantine network by assigning this role: FullAccessRole / Guest / Guest Wired Restricted

Make this role assignment
○ Permanent
● For this session only

Roles

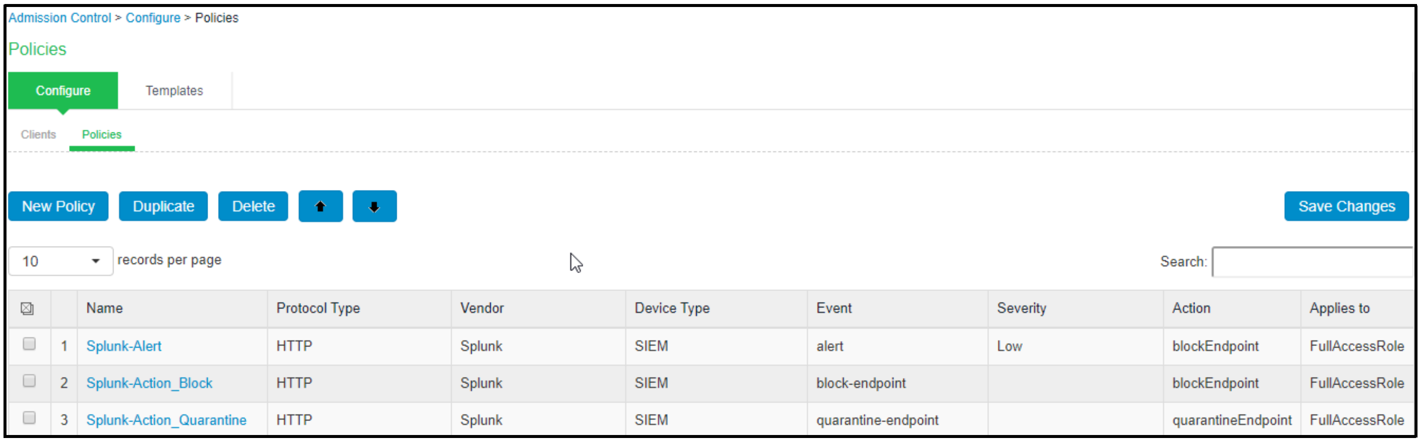
○ Policy applies to ALL roles
● Policy applies to SELECTED roles
○ Policy applies to all roles OTHER THAN those selected below

Available roles: Guest Wired Restricte, LimitedAccessRole, migration_role, pps, Users

Selected roles: FullAccessRole

10. Click **Save Changes**.

Once the policy is created. You can see the summary page as shown below. The following page shows the different policies created for different events with different user roles.



Admission Control > Configure > Policies

Policies

10 records per page   Search:

☒		Name	Protocol Type	Vendor	Device Type	Event	Severity	Action	Applies to
□	1	Splunk-Alert	HTTP	Splunk	SIEM	alert	Low	blockEndpoint	FullAccessRole
□	2	Splunk-Action_Block	HTTP	Splunk	SIEM	block-endpoint		blockEndpoint	FullAccessRole
□	3	Splunk-Action_Quarantine	HTTP	Splunk	SIEM	quarantine-endpoint		quarantineEndpoint	FullAccessRole

© 2020 Pulse Secure, LLC.

Configuring Splunk Enterprise

This section covers the following topics:

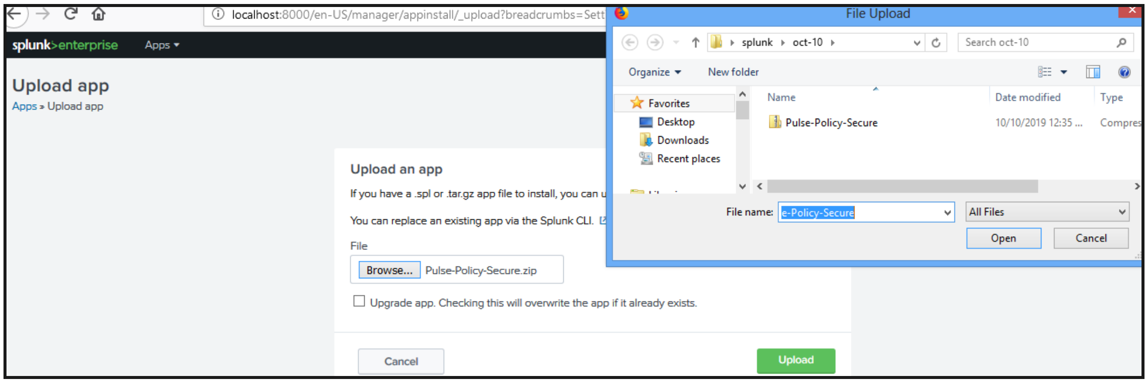
- “Install Pulse Policy Secure Alert Add-On for Splunk” on page 10
- “Alert Action Based on Source IP/MAC Address” on page 11

Install Pulse Policy Secure Alert Add-On for Splunk

Download the *ps-pps-9.1R3-splunk-alertaddon.tar.gz* file from Pulse Secure software downloads location and install them onto your Splunk server.

To configure the Pulse Policy Secure App:

1. Log into Splunk as an Admin user.
2. In the Splunk Enterprise Dashboard, select the **Admin tab > Manage Apps**.
3. Select **Apps > Upload App**
4. Click Browse and upload the Pulse-Policy-Secure.zip file to install the Pulse Secure App for Splunk.



Upload app

Apps » Upload app

Upload an app

If you have a .spl or .tar.gz app file to install, you can u

You can replace an existing app via the Splunk CLI.

File: Browse... Pulse-Policy-Secure.zip

☐ Upgrade app. Checking this will overwrite the app if it already exists.

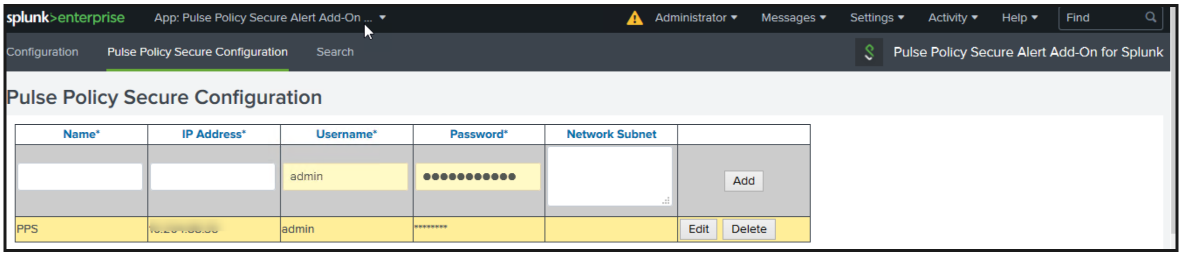
File Upload

File name: e-Policy-Secure

All Files

Note: For upgrading the existing Pulse Policy Secure app, select the upgrade app. Checking this will overwrite the app if already exists option.

5. After installation, Pulse Policy Secure Alert Add-On for Splunk appears in the App section
6. Select the Pulse Policy Secure Alert Add-On for Splunk Icon.
7. Enter the name, PPS IP address, user name, network subnet to send alerts/action. Click Add.
8. Click **Save**.



Pulse Policy Secure Configuration

Name*	IP Address*	Username*	Password*	Network Subnet	
		admin	●●●●●●●●●●●		Add
PPS	[redacted]	admin	********		Edit Delete

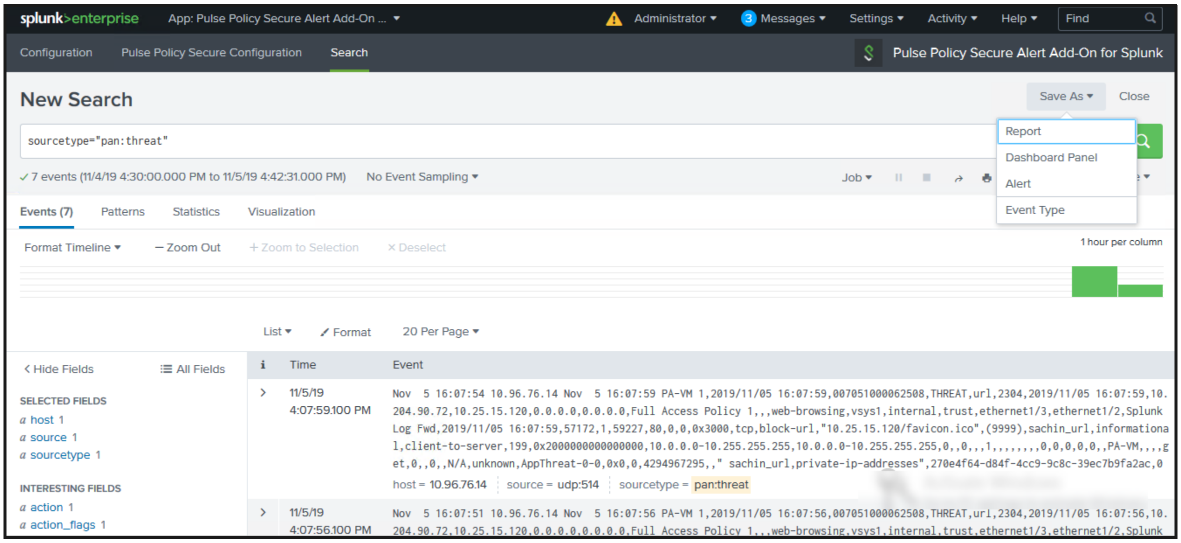
splunk>enterprise
App: Pulse Policy Secure Alert Add-On ... ▾
Administrator ▾
Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
Configuration
Pulse Policy Secure Configuration
Search
Pulse Policy Secure Alert Add-On for Splunk

© 2020 Pulse Secure, LLC.

Alert Action Based on Source IP/MAC Address

SIEM provides live streaming of the processed events and flows. SIEM admin live monitors these log and network activity. Expert SIEM admin can identify the malicious host by monitoring these data. Pulse Secure application provides an option for the SIEM admin to take action for such host based on IP Address even if these are not listed under alerts.

1. In the Pulse Secure Alert Add-on App for Splunk, run a search.
2. Under the Pulse Policy Secure Alert Add-On for Splunk logo select Save As and then Alert.
3. The Save As alert dialog opens.



New Search

```
sourcetype="pan:threat"
```

✓ 7 events (11/4/19 4:30:00.000 PM to 11/5/19 4:42:31.000 PM) No Event Sampling

SELECTED FIELDS
- host 1
- source 1
- sourcetype 1

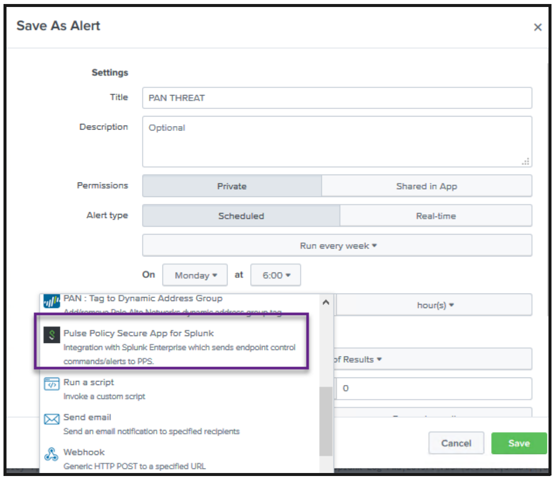
INTERESTING FIELDS
- action 1
- action_flags 1

Time	Event

11/5/19 4:07:59.100 PM	`Nov 5 16:07:54 10.96.76.14 Nov 5 16:07:59 PA-VM 1,2019/11/05 16:07:59,007051000062508,THREAT,url,2304,2019/11/05 16:07:59,10.204.90.72,10.25.15.120,0.0.0.0,0.0.0.0,Full Access Policy 1,,,web-browsing,vsys1,internal,trust,ethernet1/3,ethernet1/2,Splunk Log Fwd,2019/11/05 16:07:59,57172,1,59227,80,0,0,0x3000,tcp,block-url,"10.25.15.120/favicon.ico",(9999),sachin_url,informational,client-to-server,199,0x2000000000000000,10.0.0.0-10.255.255.255,10.0.0.0-10.255.255.255,0,,0,,,1,,,,,,,,0,0,0,0,,PA-VM,,,,get,0,,0,,N/A,unknown,AppThreat-0-0,0x0,0,4294967295,," sachin_url,private-ip-addresses",270e4f64-d84f-4cc9-9c8c-39ec7b9fa2ac,0`
	host = 10.96.76.14 source = udp:514 sourcetype = pan:threat

11/5/19 4:07:56.100 PM	`Nov  5 16:07:51 10.96.76.14 Nov  5 16:07:56 PA-VM 1,2019/11/05 16:07:56,007051000062508,THREAT,url,2304,2019/11/05 16:07:56,10.204.90.72,10.25.15.120,0.0.0.0,0.0.0.0,Full Access Policy 1,,,web-browsing,vsys1,internal,trust,ethernet1/3,ethernet1/2,Splunk`

4. Define the schedule and trigger conditions.
5. In the Trigger Actions section, select Add Actions and then select Pulse Policy Secure App for Splunk.



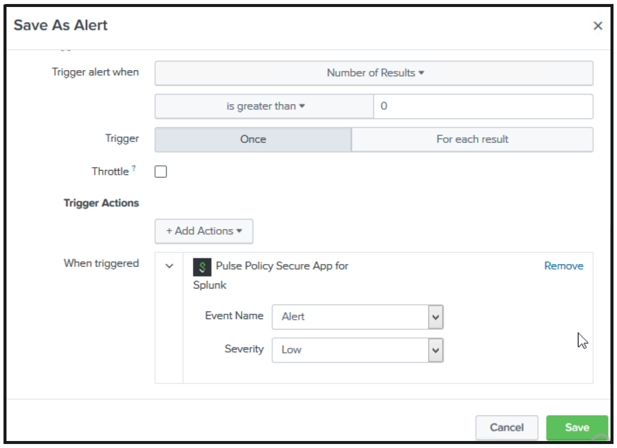
Save As Alert

Settings

Title	PAN THREAT
Description	Optional
Permissions	Private / Shared in App
Alert type	Scheduled / Real-time
	Run every week
	On Monday at 6:00

- PAN : Tag to Dynamic Address Group
  Add/remove Palo Alto Networks dynamic address group tag
- Pulse Policy Secure App for Splunk
  Integration with Splunk Enterprise which sends endpoint control commands/alerts to PPS.
- Run a script
  Invoke a custom script
- Send email
  Send an email notification to specified recipients
- Webhook
  Generic HTTP POST to a specified URL

6. Specify the Event Type and the severity and click Save.



Save As Alert

Trigger alert when: Number of Results

is greater than: 0

Trigger: Once | For each result

Throttle: □

Trigger Actions

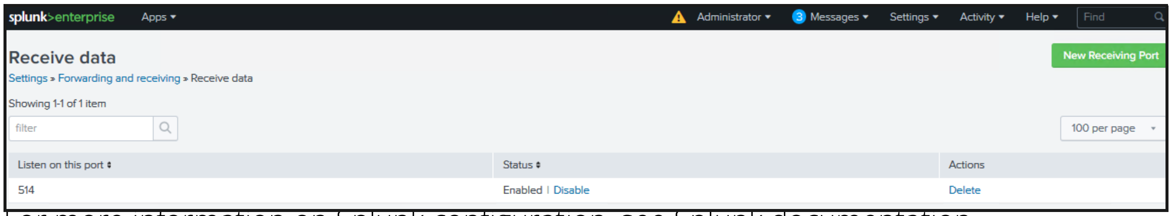
+ Add Actions

When triggered: Pulse Policy Secure App for Splunk — Remove

Event Name: Alert

Severity: Low

Note: Enable port 514 from Settings > Forward and receiving> Receive Data.



Receive data

Settings » Forwarding and receiving » Receive data

Showing 1-1 of 1 item

filter — 100 per page

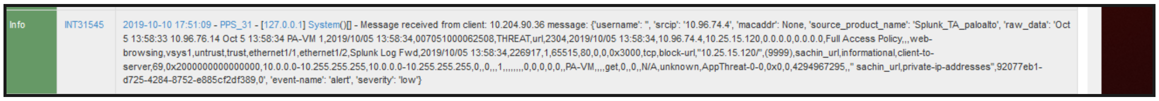
Listen on this port	Status	Actions
514	Enabled | Disable	Delete

For more information on Splunk configuration, see Splunk documentation.

Troubleshooting

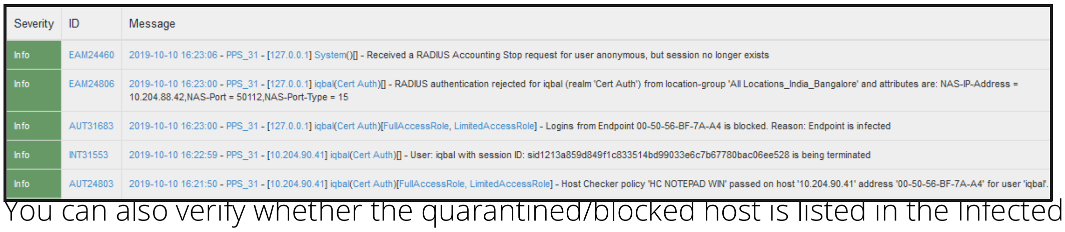
To verify the event logs on PPS, select System > Log/Monitoring > Events. Ensure Admission control events option is enabled in Event logs settings.

You can verify that the event logs are generated every time when an event is received from Splunk.



```
Info  INT31545  2019-10-10 17:51:09 - PPS_31 - [127.0.0.1] System()[] - Message received from client: 10.204.90.36 message: {'username': '', 'srcip': '10.96.74.4', 'macaddr': None, 'source_product_name': 'Splunk_TA_paloalto', 'raw_data': 'Oct
5 13:58:33 10.96.76.14 Oct 5 13:58:34 PA-VM 1,2019/10/05 13:58:34,007051000062508,THREAT,url,2304,2019/10/05 13:58:34,10.96.74.4,10.25.15.120,0.0.0.0,0.0.0.0,Full Access Policy,,,web-
browsing,vsys1,untrust,trust,ethernet1/1,ethernet1/2,Splunk Log Fwd,2019/10/05 13:58:34,226917,1,65515,80,0,0,0x3000,tcp,block-url,"10.25.15.120/",(9999),sachin_url,informational,client-to-
server,69,0x2000000000000000,10.0.0.0-10.255.255.255,10.0.0.0-10.255.255.255,0,,0,,,1,,,,,,,,0,0,0,0,0,,PA-VM,,,,get,0,,0,,N/A,unknown,AppThreat-0-0,0x0,0,4294967295,," sachin_url,private-ip-addresses",92077eb1-
d725-4284-8752-e885cf2df389,0', 'event-name': 'alert', 'severity': 'low'}
```

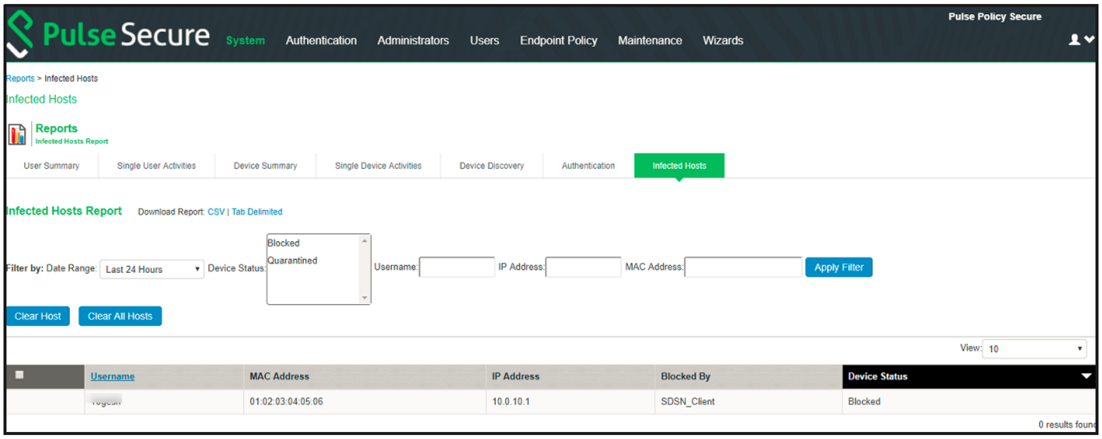
To verify the user access logs, select System >Logs & Monitoring > User Access to verify the user login related logs like realm, roles, username and IP address.



Severity	ID	Message
Info	EAM24460	2019-10-10 16:23:06 - PPS_31 - [127.0.0.1] System()[] - Received a RADIUS Accounting Stop request for user anonymous, but session no longer exists
Info	EAM24806	2019-10-10 16:23:00 - PPS_31 - [127.0.0.1] iqbal(Cert Auth)[] - RADIUS authentication rejected for iqbal (realm 'Cert Auth') from location-group 'All Locations_India_Bangalore' and attributes are: NAS-IP-Address = 10.204.88.42,NAS-Port = 50112,NAS-Port-Type = 15
Info	AUT31683	2019-10-10 16:23:00 - PPS_31 - [127.0.0.1] iqbal(Cert Auth)[FullAccessRole, LimitedAccessRole] - Logins from Endpoint 00-50-56-BF-7A-A4 is blocked. Reason: Endpoint is infected
Info	INT31553	2019-10-10 16:22:59 - PPS_31 - [10.204.90.41] iqbal(Cert Auth)[] - User: iqbal with session ID: sid1213a859d849f1c833514bd99033e6c7b67780bac06ee528 is being terminated
Info	AUT24803	2019-10-10 16:21:50 - PPS_31 - [10.204.90.41] iqbal(Cert Auth)[FullAccessRole, LimitedAccessRole] - Host Checker policy 'HC NOTEPAD WIN' passed on host '10.204.90.41' address '00-50-56-BF-7A-A4' for user 'iqbal'.

You can also verify whether the quarantined/blocked host is listed in the Infected Devices report, which lists the mac address, IP address, and the device status. To verify the reports, select System > Reports > Infected Devices.

© 2020 Pulse Secure, LLC.



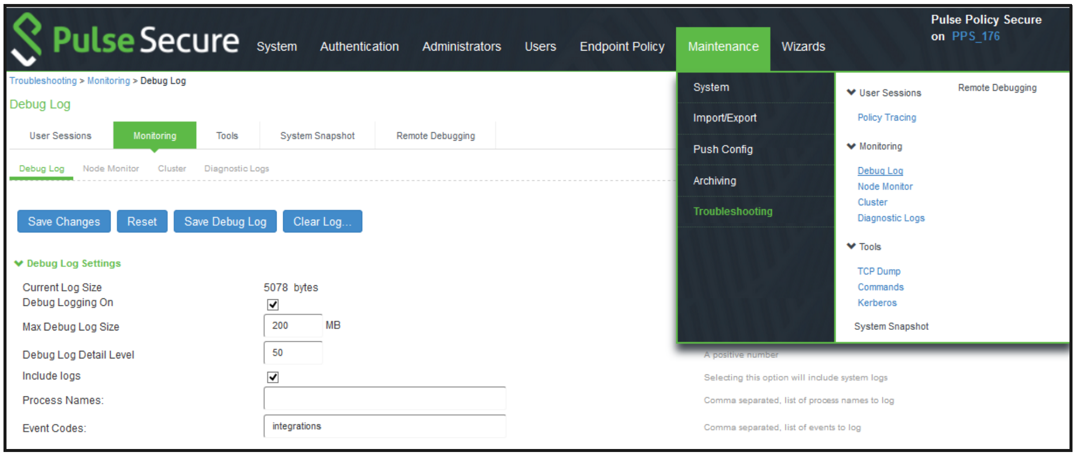
Filter by: Date Range: Last 24 Hours Device Status: Blocked Quarantined Username: IP Address: MAC Address:

View: 10

■	Username	MAC Address	IP Address	Blocked By	Device Status
	[redacted]	01:02:03:04:05:06	10.0.10.1	SDSN_Client	Blocked

0 results found

You can also enable debug logs to troubleshoot any issues. Select Maintenance > Troubleshooting > Monitoring > Debug Log to enable debug logs.



Debug Log Settings

Current Log Size	5078 bytes	
Debug Logging On	☑	
Max Debug Log Size	200 MB	
Debug Log Detail Level	50	A positive number
Include logs	☑	Selecting this option will include system logs
Process Names:		Comma separated, list of process names to log
Event Codes:	integrations	Comma separated, list of events to log

Pulse Policy Secure Syslog Add-On for Splunk

Pulse Policy Secure is a network and application access control (NAC) solution used extensively in small, midrange and large enterprises. PPS provides the capability to send various kinds of user access, device/user authentication, Host Checker compliance events, admission control events, profiler discovery, device profile, attribute update and device contextual information as Syslog messages to any Syslog receiver.

Splunk is a log management/SIEM solution that can receive Syslog messages from multiple sources. These messages are stored within Splunk and then can be correlated, searched, analyzed and displayed using its graphical user interface.

Splunk is also a platform that runs applications (Apps) as add-ons to Splunk, which are customized for specific external applications or products which send Syslogs. The App provides visualization of the received data without requiring the user to run complex searches within Splunk.

These apps typically consist of a number of dashboard elements like charts, tables and graphs that are accessible via a menu structure contained within the app, which are based on pre-defined searches. The PPS Splunk App is such an App developed by Pulse Secure for visualizing a Syslog feed from Pulse Policy Secure.

To integrate PPS with Splunk, perform the following:

Configuring PPS to send syslogs to Splunk

Add an instance of Splunk to PPS as syslog server. Add the Splunk IP address or hostname and port number at the appropriate place in the PPS administrative interface.

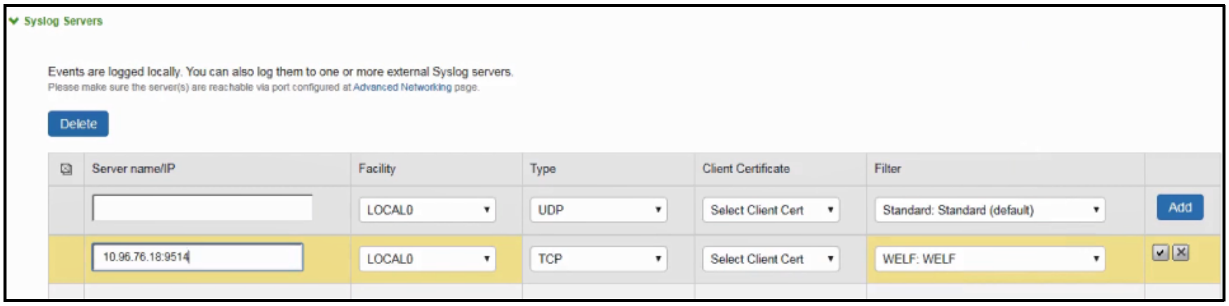
T o configure Splunk as a Syslog server:

1. Under **Log/Monitoring > <User Access/Events/Admin Access**>.
2. Click **Log Settings**.
3. Under **Syslog Servers**, Enter the Splunk Server name/IP and add port value as **9514**.

   Note: The port number can be customized from the inputs.conf file if desired.
4. Select the type as **TCP**.
5. Select the file format as **WELF**. Only WELF is supported.
6. Click **Add**.

© 2020 Pulse Secure, LLC.

Figure 5 Splunk Syslog server



Events are logged locally. You can also log them to one or more external Syslog servers.
Please make sure the server(s) are reachable via port configured at Advanced Networking page.

Server name/IP	Facility	Type	Client Certificate	Filter
	LOCAL0	UDP	Select Client Cert	Standard: Standard (default)
10.96.76.18:9514	LOCAL0	TCP	Select Client Cert	WELF: WELF

Configuring Splunk

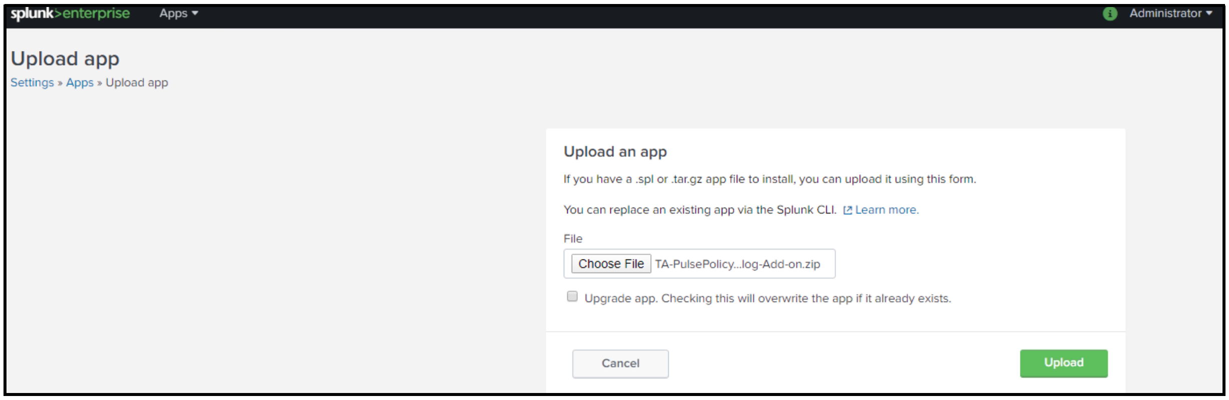
Install Pulse Policy Secure Syslog Add-On for Splunk

Download the TA_pulse_policy_secure_syslog_addon_1.0.0.tar.gz file from Pulse Secure software downloads location and install them onto your Splunk server.

To configure the Pulse Policy Secure syslog Add-On:

1. Log into Splunk as an Admin user.
2. In the Splunk Enterprise Dashboard, select the **Admin tab > Manage Apps**.
3. Select **Apps > Upload App**.
4. Click Browse and upload the TA_pulse_policy_secure_syslog_addon_1.0.0.tar.gz file to install the Pulse Secure Syslog Add-On for Splunk.

Figure 6 Syslog Add-On



Upload app

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. Learn more.

File: TA-PulsePolicy...log-Add-on.zip

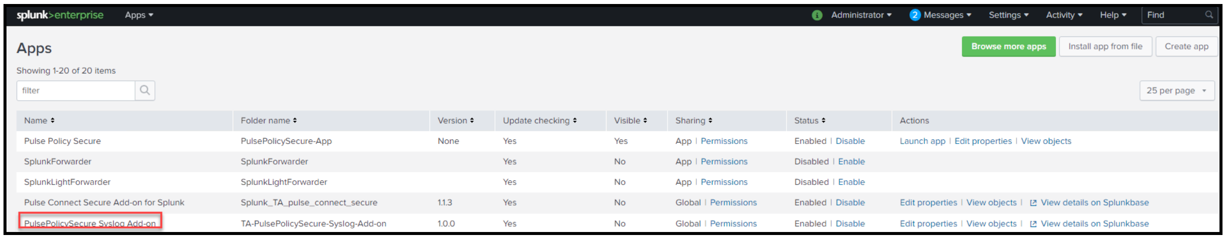
□ Upgrade app. Checking this will overwrite the app if it already exists.

Note: For upgrading the existing Pulse Policy Secure app, select the upgrade app. Checking this will overwrite the app if already exists option.

© 2020 Pulse Secure, LLC.

5. After installation, PulsePolicySecure Syslog-Add-On for Splunk appears in the App section with Splunk App version 1.0.0.

Figure 7 Install



Apps

Showing 1-20 of 20 items

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Pulse Policy Secure	PulsePolicySecure-App	None	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
Pulse Connect Secure Add-on for Splunk	Splunk_TA_pulse_connect_secure	1.1.3	Yes	No	Global | Permissions	Enabled | Disable	Edit properties | View objects | View details on Splunkbase
PulsePolicySecure Syslog Add-on	TA-PulsePolicySecure-Syslog-Add-on	1.0.0	Yes	No	Global | Permissions	Enabled | Disable	Edit properties | View objects | View details on Splunkbase

Create an index

Indexing is a mechanism to speed up the search process by giving numeric addresses to the piece of data being searched. We can create a new index with desired size by the data that is stored in Splunk. The additional data that comes in can use this newly created index with better search functionality.

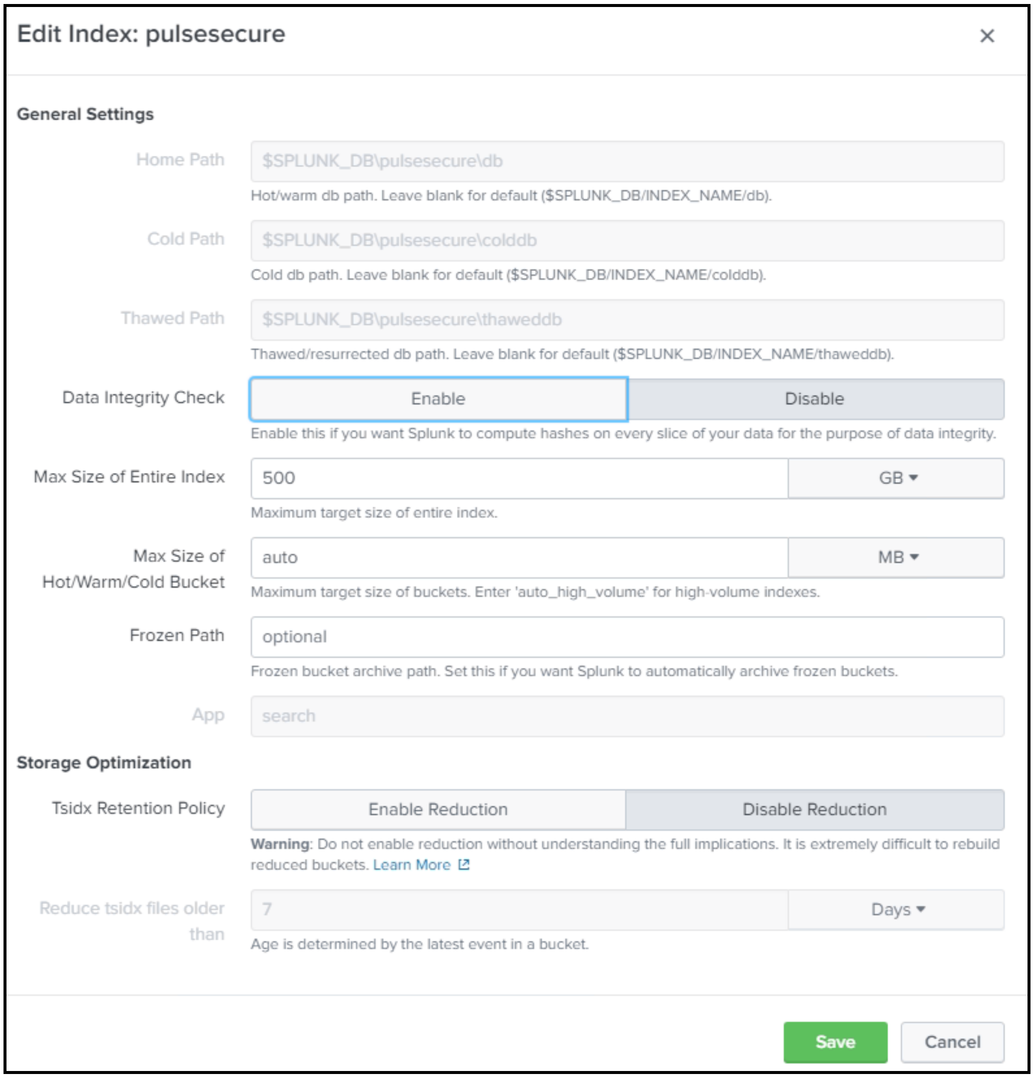
To create an index:

1. Select **Settings > Indexes > New Index.**

2. Create a new Index. For example, pulsesecure.

© 2020 Pulse Secure, LLC.

Figure 8 Index



Edit Index: pulsesecure ×

General Settings

Home Path: $SPLUNK_DB\pulsesecure\db
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: $SPLUNK_DB\pulsesecure\colddb
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: $SPLUNK_DB\pulsesecure\thaweddb
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable | Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB ▾
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto MB ▾
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path: optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App: search

Storage Optimization

Tsidx Retention Policy: Enable Reduction | Disable Reduction
Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild reduced buckets. Learn More

Reduce tsidx files older than: 7 Days ▾
Age is determined by the latest event in a bucket.

Save Cancel

Search Index

To see the data logged by Pulse Policy Secure:

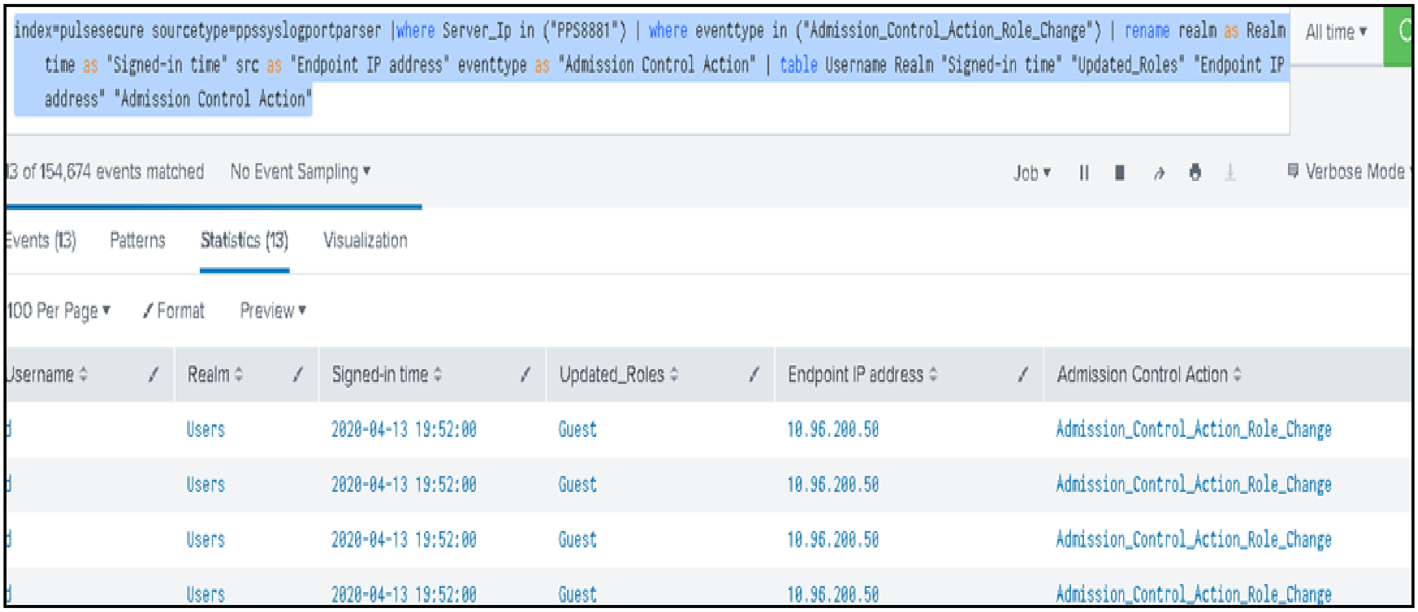
1. Under **App: Search & Reporting,** select the **Search** tab.
2. Select the Time from the drop down.
3. Enter the index query. For example, index=pulsesecure sourcetype=ppssyslogportparser. You can select multiple PPS IP address/host name for querying from multiple PPS servers.
4. Press **Enter**.

Example 1: Sample Query for Admission Control

This sample query displays all the events from Pulse Policy Secure for Admission Control role change based on the selected time frame. You can customize the Splunk search query as per your requirement. For example, src field from the sylog can be changed to Endpoint IP address.

```
index=pulsesecure sourcetype=ppssyslogportparser |where Server_Ip in ("PPS8881") | where
eventtype in ("Admission_Control_Action_Role_Change") | rename realm as Realm time as
"Signed-in time" src as "Endpoint IP address" eventtype as "Admission Control Action" |
table Username Realm "Signed-in time" "Updated_Roles" "Endpoint IP address" "Admission
Control Action"
```

Figure 9 Search

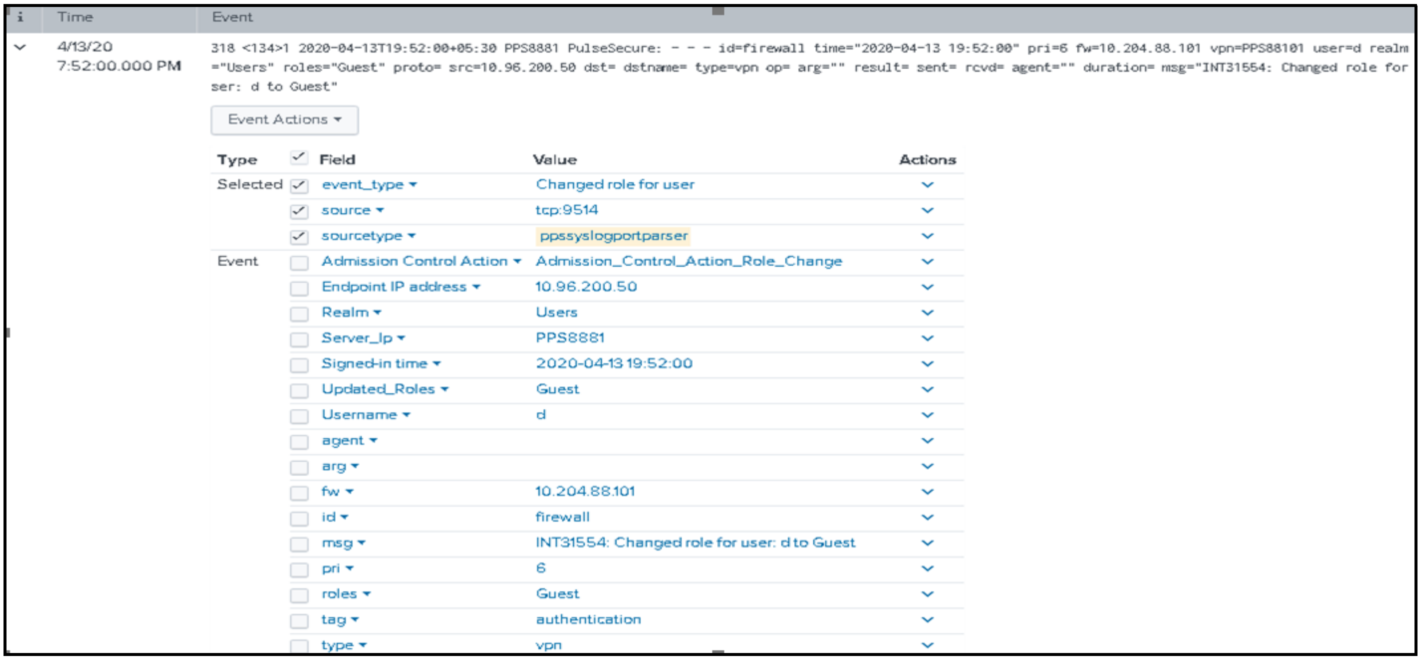


```
index=pulsesecure sourcetype=ppssyslogportparser |where Server_Ip in ("PPS8881") | where eventtype in ("Admission_Control_Action_Role_Change") | rename realm as Realm
   time as "Signed-in time" src as "Endpoint IP address" eventtype as "Admission Control Action" | table Username Realm "Signed-in time" "Updated_Roles" "Endpoint IP
   address" "Admission Control Action"
```

Username	Realm	Signed-in time	Updated_Roles	Endpoint IP address	Admission Control Action
d	Users	2020-04-13 19:52:00	Guest	10.96.200.50	Admission_Control_Action_Role_Change
d	Users	2020-04-13 19:52:00	Guest	10.96.200.50	Admission_Control_Action_Role_Change
d	Users	2020-04-13 19:52:00	Guest	10.96.200.50	Admission_Control_Action_Role_Change
d	Users	2020-04-13 19:52:00	Guest	10.96.200.50	Admission_Control_Action_Role_Change

You can click the down arrow to view the role change events and additional fields from syslog data.

Figure 10 Extracted Events



i	Time	Event
⌄	4/13/20 7:52:00.000 PM	318 <134>1 2020-04-13T19:52:00+05:30 PPS8881 PulseSecure: - - - id=firewall time="2020-04-13 19:52:00" pri=6 fw=10.204.88.101 vpn=PPS88101 user=d realm ="Users" roles="Guest" proto= src=10.96.200.50 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="INT31554: Changed role for ser: d to Guest"

Type	✓	Field	Value	Actions
Selected	☑	event_type ▾	Changed role for user	⌄
	☑	source ▾	tcp:9514	⌄
	☑	sourcetype ▾	ppssyslogportparser	⌄
Event	□	Admission Control Action ▾	Admission_Control_Action_Role_Change	⌄
	□	Endpoint IP address ▾	10.96.200.50	⌄
	□	Realm ▾	Users	⌄
	□	Server_Ip ▾	PPS8881	⌄
	□	Signed-in time ▾	2020-04-13 19:52:00	⌄
	□	Updated_Roles ▾	Guest	⌄
	□	Username ▾	d	⌄
	□	agent ▾		⌄
	□	arg ▾		⌄
	□	fw ▾	10.204.88.101	⌄
	□	id ▾	firewall	⌄
	□	msg ▾	INT31554: Changed role for user: d to Guest	⌄
	□	pri ▾	6	⌄
	□	roles ▾	Guest	⌄
	□	tag ▾	authentication	⌄
	□	type ▾	vpn	⌄

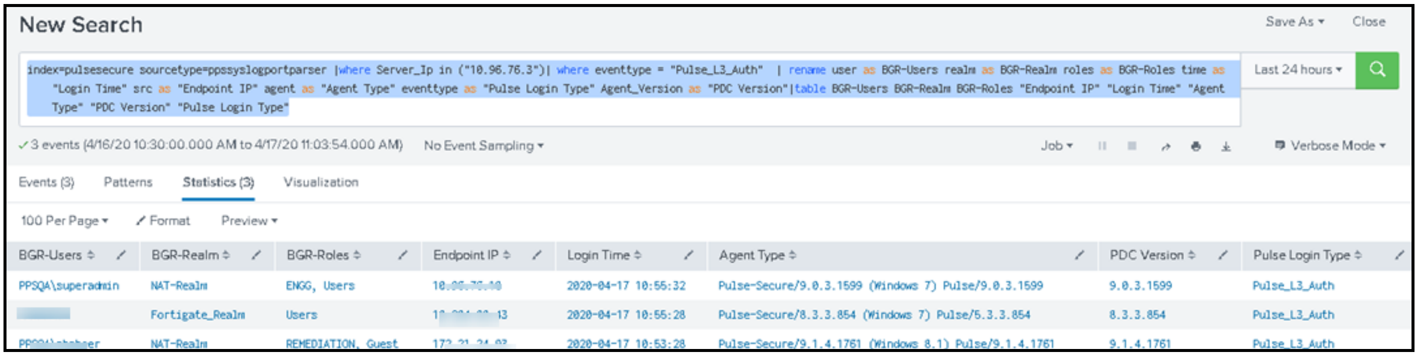
© 2020 Pulse Secure, LLC.

Example 2: Pulse Login Query for L3 agent login

```
This sample query displays all the events from Pulse Policy Secure for user login using
Pulse Client.
```

```
index=pulsesecure sourcetype=ppssyslogportparser |where Server_Ip in ("10.xx.xx.xx")|
where eventtype = "Pulse_L3_Auth"  | rename user as BGR-Users realm as BGR-Realm roles as
BGR-Roles time as "Login Time" src as "Endpoint IP" agent as "Agent Type" eventtype as
"Pulse Login Type" Agent_Version as "PDC Version"|table BGR-Users BGR-Realm BGR-Roles
"Endpoint IP" "Login Time" "Agent Type" "PDC Version" "Pulse Login Type"
```

Figure 11 Pulse Client Login



New Search

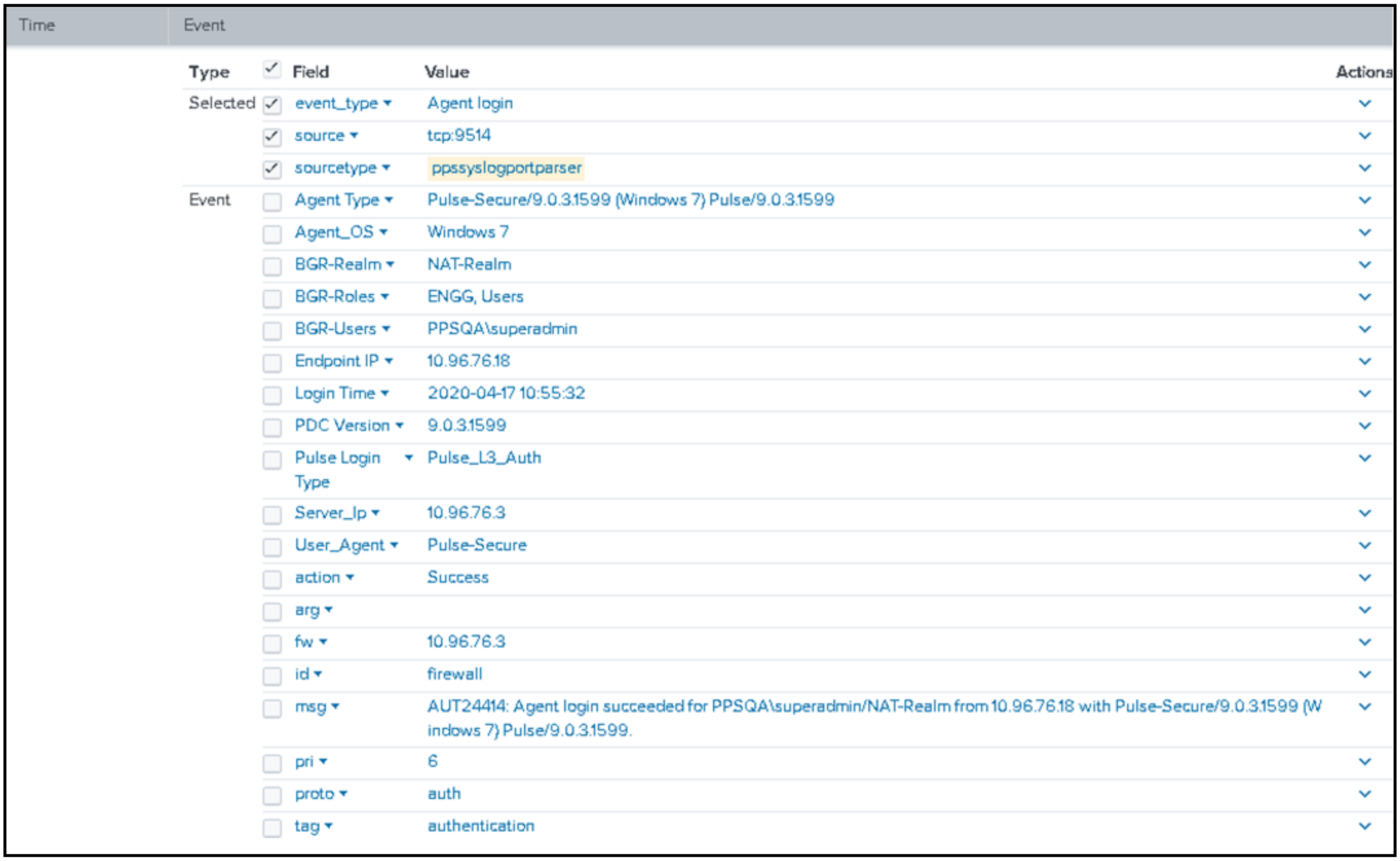
```
index=pulsesecure sourcetype=ppssyslogportparser |where Server_Ip in ("10.96.76.3")| where eventtype = "Pulse_L3_Auth"  | rename user as BGR-Users realm as BGR-Realm roles as BGR-Roles time as
    "Login Time" src as "Endpoint IP" agent as "Agent Type" eventtype as "Pulse Login Type" Agent_Version as "PDC Version"|table BGR-Users BGR-Realm BGR-Roles "Endpoint IP" "Login Time" "Agent
    Type" "PDC Version" "Pulse Login Type"
```

✓3 events (4/16/20 10:30:00.000 AM to 4/17/20 11:03:54.000 AM)

BGR-Users	BGR-Realm	BGR-Roles	Endpoint IP	Login Time	Agent Type	PDC Version	Pulse Login Type
PPSQA\superadmin	NAT-Realm	ENGG, Users	10.[redacted]	2020-04-17 10:55:32	Pulse-Secure/9.0.3.1599 (Windows 7) Pulse/9.0.3.1599	9.0.3.1599	Pulse_L3_Auth
[redacted]	Fortigate_Realm	Users	1[redacted]13	2020-04-17 10:55:28	Pulse-Secure/8.3.3.854 (Windows 7) Pulse/5.3.3.854	8.3.3.854	Pulse_L3_Auth
PPSQA\shabeer	NAT-Realm	REMEDIATION, Guest	172.21.24.93	2020-04-17 10:53:28	Pulse-Secure/9.1.4.1761 (Windows 8.1) Pulse/9.1.4.1761	9.1.4.1761	Pulse_L3_Auth

You can click the down arrow to view the event extract details.

Figure 12 Extracted fields from Pulse L3 events.



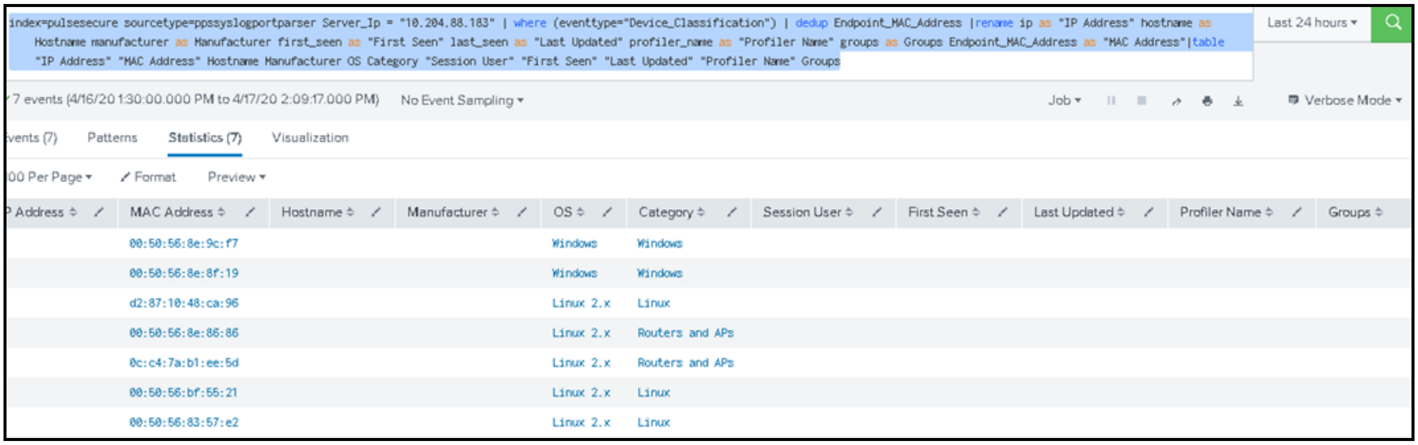
Type	✓	Field	Value
Selected	☑	event_type ▾	Agent login
	☑	source ▾	tcp:9514
	☑	sourcetype ▾	ppssyslogportparser
Event	☐	Agent Type ▾	Pulse-Secure/9.0.3.1599 (Windows 7) Pulse/9.0.3.1599
	☐	Agent_OS ▾	Windows 7
	☐	BGR-Realm ▾	NAT-Realm
	☐	BGR-Roles ▾	ENGG, Users
	☐	BGR-Users ▾	PPSQA\superadmin
	☐	Endpoint IP ▾	10.96.76.18
	☐	Login Time ▾	2020-04-17 10:55:32
	☐	PDC Version ▾	9.0.3.1599
	☐	Pulse Login Type ▾	Pulse_L3_Auth
	☐	Server_Ip ▾	10.96.76.3
	☐	User_Agent ▾	Pulse-Secure
	☐	action ▾	Success
	☐	arg ▾	
	☐	fw ▾	10.96.76.3
	☐	id ▾	firewall
	☐	msg ▾	AUT24414: Agent login succeeded for PPSQA\superadmin/NAT-Realm from 10.96.76.18 with Pulse-Secure/9.0.3.1599 (Windows 7) Pulse/9.0.3.1599.
	☐	pri ▾	6
	☐	proto ▾	auth
	☐	tag ▾	authentication

Example 3: Profiler Classification

This sample query displays all the events from Pulse Policy Secure based on Pulse Profiler classification of endpoints.

```
index=pulsesecure sourcetype=ppssyslogportparser Server_Ip = "10.204.xx.xxx" | where
(eventtype="Device_Classification") | dedup Endpoint_MAC_Address |rename ip as "IP
Address" hostname as Hostname manufacturer as Manufacturer first_seen as "First Seen"
last_seen as "Last Updated" profiler_name as "Profiler Name" groups as Groups
Endpoint_MAC_Address as "MAC Address"|table "IP Address" "MAC Address" Hostname
Manufacturer OS Category "Session User" "First Seen" "Last Updated" "Profiler Name" Groups
```

Figure 13 Profiler Classification



```
index=pulsesecure sourcetype=ppssyslogportparser Server_Ip = "10.204.88.183" | where (eventtype="Device_Classification") | dedup Endpoint_MAC_Address |rename ip as "IP Address" hostname as
    Hostname manufacturer as Manufacturer first_seen as "First Seen" last_seen as "Last Updated" profiler_name as "Profiler Name" groups as Groups Endpoint_MAC_Address as "MAC Address"|table
    "IP Address" "MAC Address" Hostname Manufacturer OS Category "Session User" "First Seen" "Last Updated" "Profiler Name" Groups
```

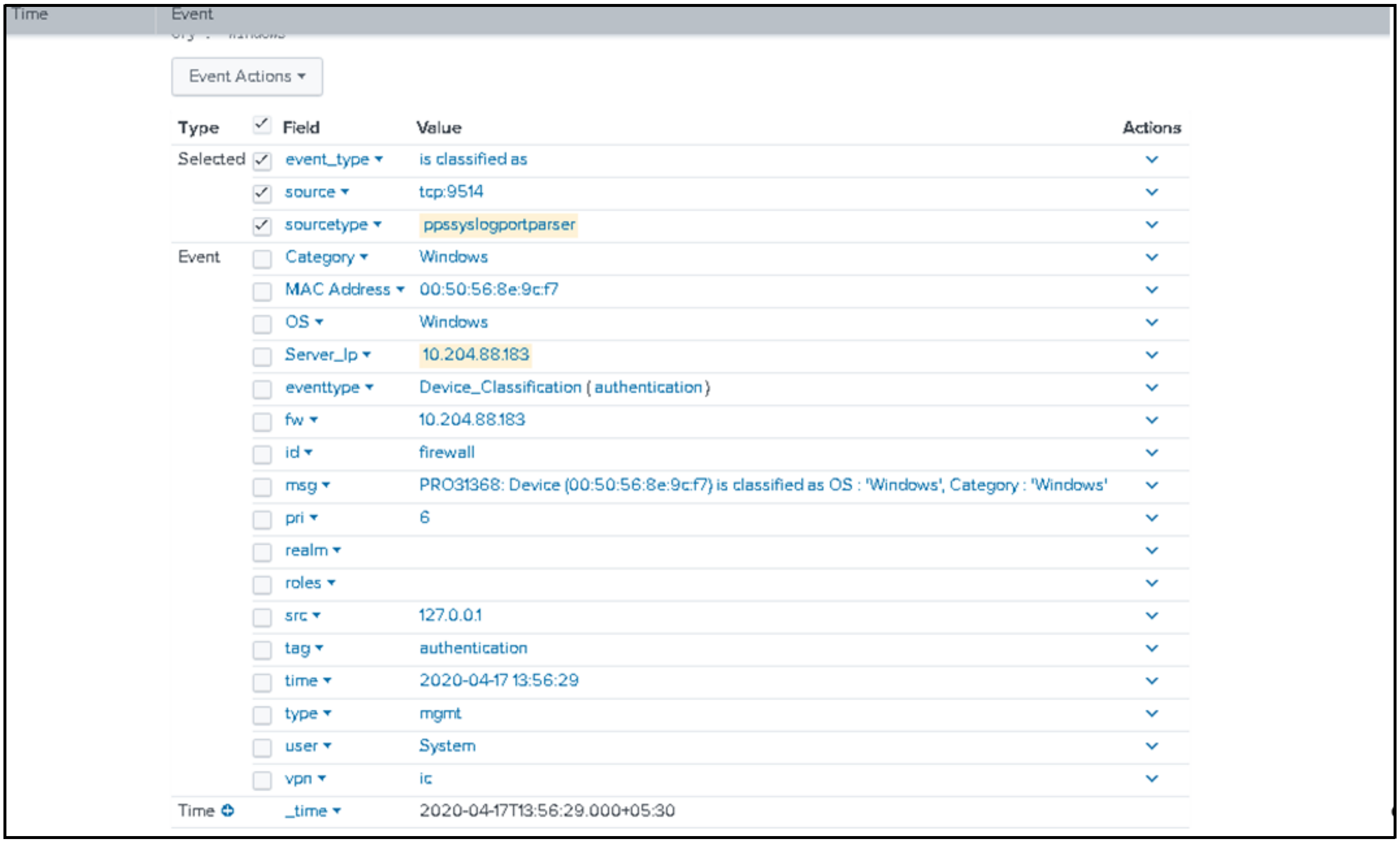
7 events (4/16/20 1:30:00.000 PM to 4/17/20 2:09:17.000 PM)

P Address	MAC Address	Hostname	Manufacturer	OS	Category	Session User	First Seen	Last Updated	Profiler Name	Groups
	00:50:56:8e:9c:f7			Windows	Windows					
	00:50:56:8e:8f:19			Windows	Windows					
	d2:87:10:48:ca:96			Linux 2.x	Linux					
	00:50:56:8e:86:86			Linux 2.x	Routers and APs					
	0c:c4:7a:b1:ee:5d			Linux 2.x	Routers and APs					
	00:50:56:bf:55:21			Linux 2.x	Linux					
	00:50:56:83:57:e2			Linux 2.x	Linux					

You can click the down arrow to view the event extract details.

© 2020 Pulse Secure, LLC.

Figure 14 Extracted Events



Type	✓ Field	Value	Actions
Selected	☑ event_type ▾	is classified as	⌄
	☑ source ▾	tcp:9514	⌄
	☑ sourcetype ▾	ppssyslogportparser	⌄
Event	□ Category ▾	Windows	⌄
	□ MAC Address ▾	00:50:56:8e:9c:f7	⌄
	□ OS ▾	Windows	⌄
	□ Server_Ip ▾	10.204.88.183	⌄
	□ eventtype ▾	Device_Classification (authentication)	⌄
	□ fw ▾	10.204.88.183	⌄
	□ id ▾	firewall	⌄
	□ msg ▾	PRO31368: Device (00:50:56:8e:9c:f7) is classified as OS : 'Windows', Category : 'Windows'	⌄
	□ pri ▾	6	⌄
	□ realm ▾		⌄
	□ roles ▾		⌄
	□ src ▾	127.0.0.1	⌄
	□ tag ▾	authentication	⌄
	□ time ▾	2020-04-17 13:56:29	⌄
	□ type ▾	mgmt	⌄
	□ user ▾	System	⌄
	□ vpn ▾	ic	⌄
Time ⊕	_time ▾	2020-04-17T13:56:29.000+05:30	

Splunk Dashboard

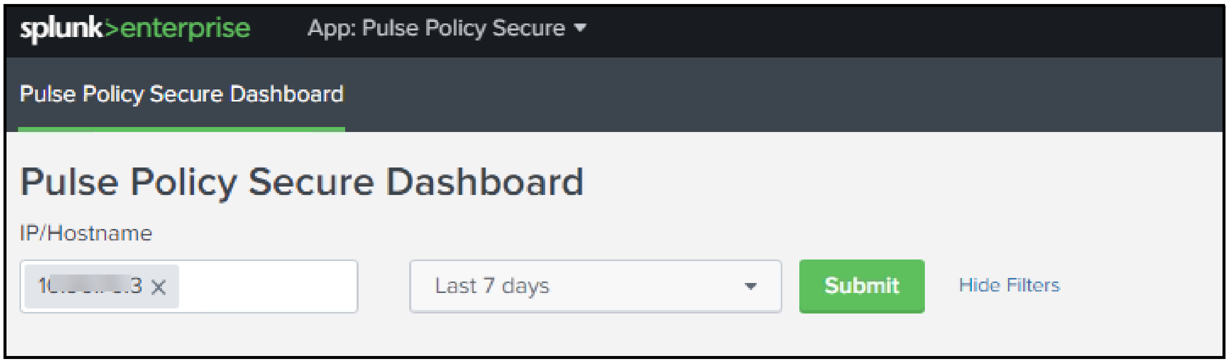
Splunk dashboard application for PPS uses the indexed data to render various charts and to show useful information on dashboard. The Pulse Policy Secure app for Splunk allows you to view PPS data in a dedicated, customizable Splunk dashboard. The PPS integration with Splunk allows security managers to quickly monitor the current operational/security posture.

The Pulse Policy Secure syslog add on for Splunk provides value to the PPS syslog data, it extracts various event types and additional fields from syslog data. The Pulse Policy Secure dashboard app for Splunk uses this data to provide various charts for compliance, login type, endpoint by categories, endpoint by OS and so on. The It analyzes the contextual data from Pulse Policy Secure to help administrators analyze and cross-correlate events on endpoints.

For multiple PPS sending data to Splunk at a time, Splunk app provides dashboard for multiple PPS servers. The user must select the IP/Hostname of multiple PPS server from the IP/Hostname field to view the dashboard.

Note: For clustering, all the IP/Hostnames must be selected in the IP/Hostname field for viewing the dashboard.

Figure 15 Splunk Dashboard



Pulse Policy Secure Dashboard

IP/Hostname: 1[redacted]3 ×

Last 7 days ▾

The Splunk application for PPS provides a dashboard with various types of authentication, Host Checker compliance, endpoint classification details. The dashboard presents 12 charts based on the endpoint properties reported by PPS by default.

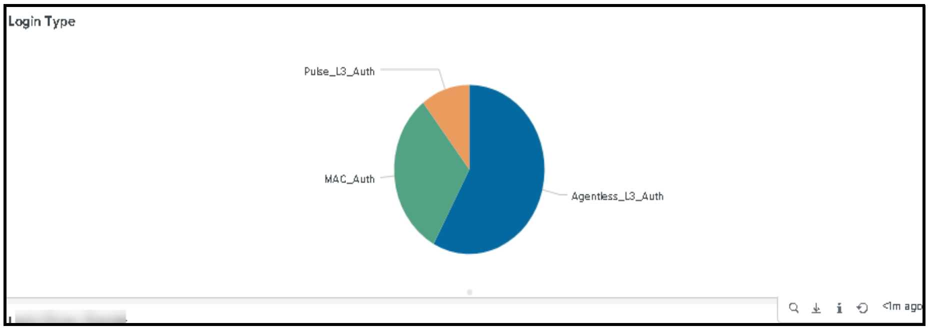
© 2020 Pulse Secure, LLC.

Table 1 Lists the Dashboard elements and their descriptions.

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Login Type</td><td>

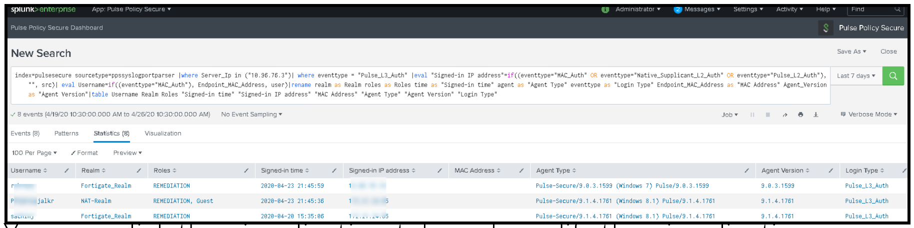
This panel shows the results of endpoint based on the login. The graph shows the number of endpoints connected using Pulse Client or through Web browser (Agentless). For example, Agentless L3 Auth, Pulse L3 Auth, Pulse L2 Auth, Mac Auth, Native Supplicant L2 Auth.

Figure 16 Login



Admin can also drill down to view the login details such as Username, IP address, MAC address, realm, roles, sign-in time, agent type, agent version, login type in a tabular format.

Figure 17 Drill Down



New Search

```
index=pulsesecure sourcetype=ppssyslogportparser |where Server_Ip in ("10.96.76.3")| where eventtype = "Pulse_L3_Auth" |eval "Signed-in IP address"=if((eventtype="MAC_Auth" OR eventtype="Native_Supplicant_L2_Auth" OR eventtype="Pulse_L2_Auth"),
    "", src)| eval Username=if((eventtype="MAC_Auth"), Endpoint_MAC_Address, user)|rename realm as Realm roles as Roles time as "Signed-in time" agent as "Agent Type" eventtype as "Login Type" Endpoint_MAC_Address as "MAC Address" Agent_Version
    as "Agent Version"|table Username Realm Roles "Signed-in time" "Signed-in IP address" "MAC Address" "Agent Type" "Agent Version" "Login Type"
```

✓ 8 events (4/19/20 10:30:00.000 AM to 4/26/20 10:30:00.000 AM) No Event Sampling ▾

<table>
<tr><th>Username</th><th>Realm</th><th>Roles</th><th>Signed-in time</th><th>Signed-in IP address</th><th>MAC Address</th><th>Agent Type</th><th>Agent Version</th><th>Login Type</th></tr>
<tr><td>r[redacted]</td><td>Fortigate_Realm</td><td>REMEDIATION</td><td>2020-04-23 21:45:59</td><td>1[redacted]</td><td></td><td>Pulse-Secure/9.0.3.1599 (Windows 7) Pulse/9.0.3.1599</td><td>9.0.3.1599</td><td>Pulse_L3_Auth</td></tr>
<tr><td>P[redacted]jalkr</td><td>NAT-Realm</td><td>REMEDIATION, Guest</td><td>2020-04-23 21:45:36</td><td>1[redacted]5</td><td></td><td>Pulse-Secure/9.1.4.1761 (Windows 8.1) Pulse/9.1.4.1761</td><td>9.1.4.1761</td><td>Pulse_L3_Auth</td></tr>
<tr><td>[redacted]</td><td>Fortigate_Realm</td><td>REMEDIATION</td><td>2020-04-20 15:35:06</td><td>1[redacted]</td><td></td><td>Pulse-Secure/9.1.4.1761 (Windows 8.1) Pulse/9.1.4.1761</td><td>9.1.4.1761</td><td>Pulse_L3_Auth</td></tr>
</table>

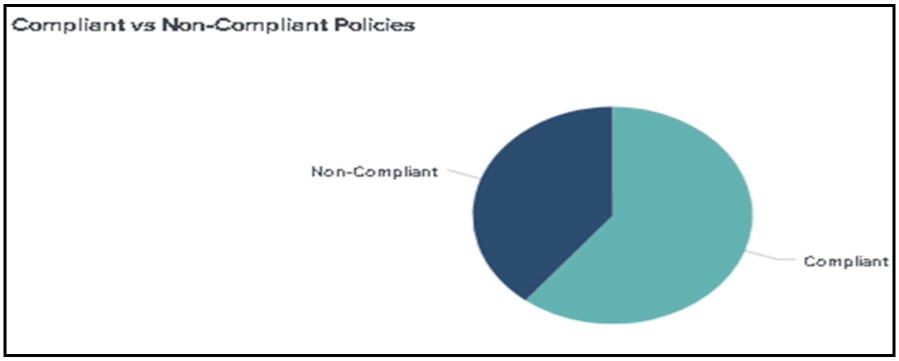
You can click the visualization tab and modify the visualization.

</td></tr>
</table>

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Compliant vs Non-Compliant Policies</td><td>

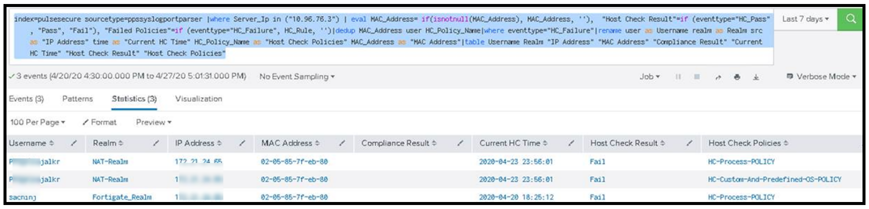
This panel displays the results of compliance and non-compliant policies. The graph shows the relative prevalence of compliant/non-compliant policies during the charted period, as a percentage of all endpoints within the reporting scope.

Figure 18   Compliance



The Admin can also drill-down to view the details of compliant and non-compliant policies/users (IP address, MAC address, Username, realm, HC Policy, HC result, compliance result, current HC time, etc.) in a tabular format.

Figure 19   Compliant vs Non Compliant



```
index=pulsesecure sourcetype=ppssyslogportparser |where Server_Ip in ("10.96.76.3") | eval MAC_Address= if(isnotnull(MAC_Address), MAC_Address, ''),  "Host Check Result"=if (eventtype="HC_Pass"
    , "Pass", "Fail"), "Failed Policies"=if (eventtype="HC_Failure", HC_Rule, '')|dedup MAC_Address user HC_Policy_Name|where eventtype="HC_Failure"|rename user as Username realm as Realm src
    as "IP Address" time as "Current HC Time" HC_Policy_Name as "Host Check Policies" MAC_Address as "MAC Address"|table Username Realm "IP Address" "MAC Address" "Compliance Result" "Current
    HC Time" "Host Check Result" "Host Check Policies"
```

✓3 events (4/20/20 4:30:00.000 PM to 4/27/20 5:01:31.000 PM)   No Event Sampling ▾

<table>
<tr><th>Username</th><th>Realm</th><th>IP Address</th><th>MAC Address</th><th>Compliance Result</th><th>Current HC Time</th><th>Host Check Result</th><th>Host Check Policies</th></tr>
<tr><td>P[redacted]jalkr</td><td>NAT-Realm</td><td>[redacted]</td><td>02-05-85-7f-eb-80</td><td></td><td>2020-04-23 23:56:01</td><td>Fail</td><td>HC-Process-POLICY</td></tr>
<tr><td>P[redacted]jalkr</td><td>NAT-Realm</td><td>1[redacted]</td><td>02-05-85-7f-eb-80</td><td></td><td>2020-04-23 23:56:01</td><td>Fail</td><td>HC-Custom-And-Predefined-OS-POLICY</td></tr>
<tr><td>sachinj</td><td>Fortigate_Realm</td><td>1[redacted]</td><td>02-05-85-7f-eb-80</td><td></td><td>2020-04-20 18:25:12</td><td>Fail</td><td>HC-Process-POLICY</td></tr>
</table>

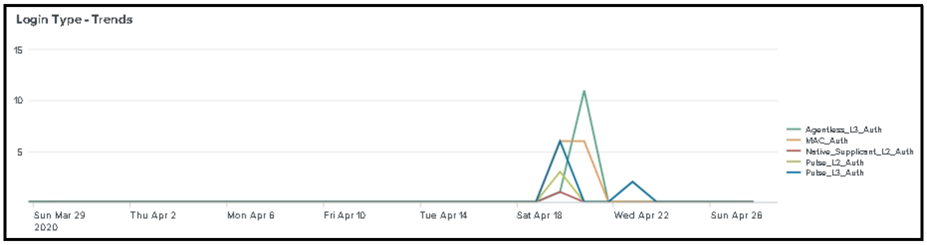
</td></tr>
<tr><td>LoginType -Trends</td><td>

This panel tracks the results of login type over time. The graph shows the number of endpoints connected using Pulse Client or through Web Browser (Agentless) over the specified period.

Trending analysis can be useful for multiple reasons.

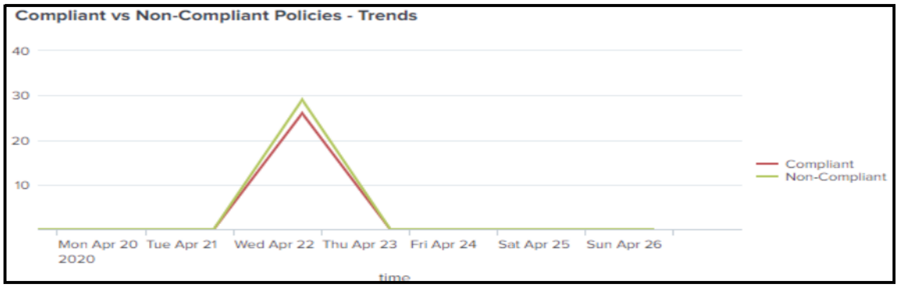
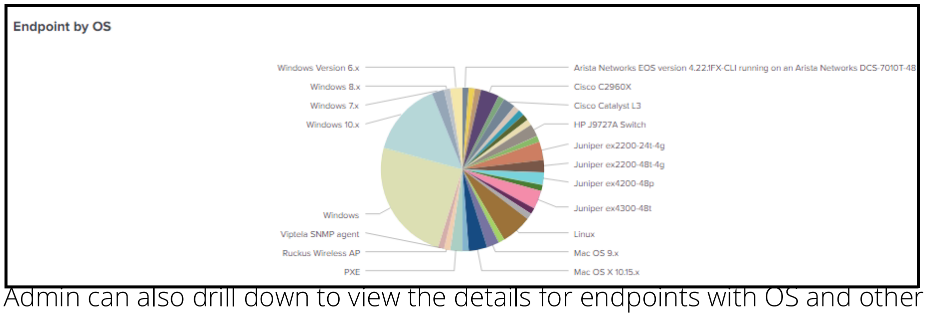
For example, for active users, it could be useful to know the workload at different time of the day and different day of the week. Then this information can be used for capacity planning and troubleshooting purpose.

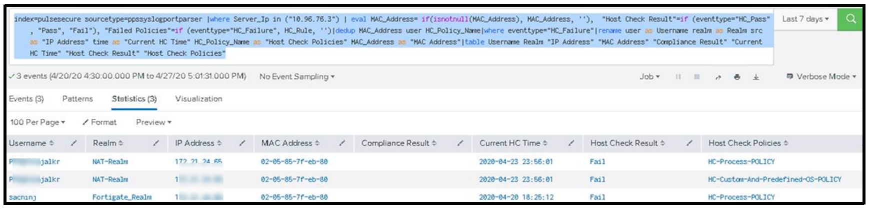
Figure 20   Login Trends



</td></tr>
</table>

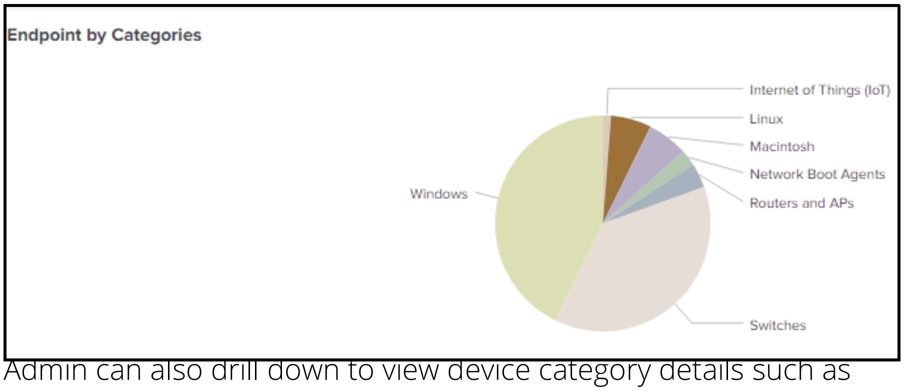
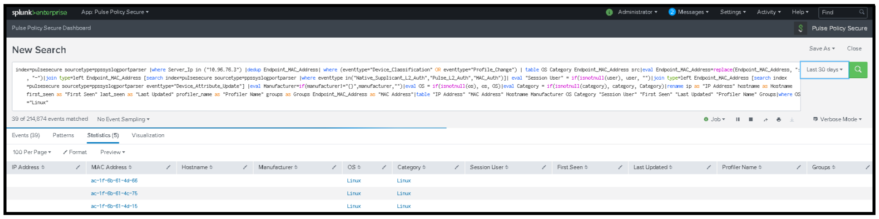
© 2020 Pulse Secure, LLC.

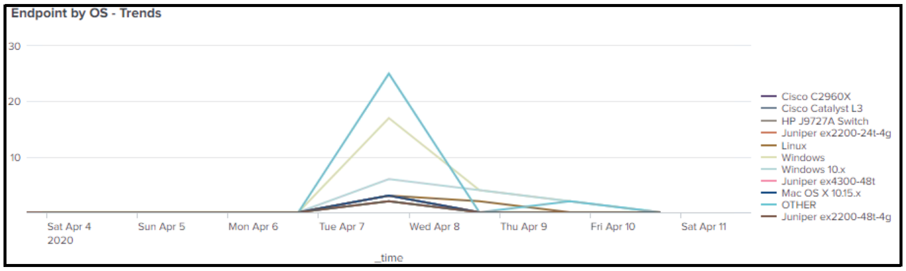
<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Compliance vs Non-Compliance Policies- Trends</td><td>This panel tracks the results of compliance policies over time. The graph shows the number of endpoints that were compliant or non-compliant over the specified period.
The trending analysis for compliance can be used to know the compliance of devices over the period of time for regulatory purpose.
Figure 21 Compliance Policies

</td></tr>
<tr><td>Endpoint by OS</td><td>This panel tracks the results of endpoint information based on Operating System (OS).
Figure 22 Endpoint by OS


Admin can also drill down to view the details for endpoints with OS and other contextual information (device ID i.e. MAC address, IP address, host name, OS, Category and other attributes) if available to Splunk via PPS/Profiler.
Figure 23 Endpoint by OS

index=pulsesecure sourcetype=ppssyslogportparser |where Server_Ip in ("10.96.76.3") | eval MAC_Address= if(isnotnull(MAC_Address), MAC_Address, ''), "Host Check Result"=if (eventtype="HC_Pass" , "Pass", "Fail"), "Failed Policies"=if (eventtype="HC_Failure", HC_Rule, '')|dedup MAC_Address user HC_Policy_Name|where eventtype="HC_Failure"|rename user as Username realm as Realm src as "IP Address" time as "Current HC Time" HC_Policy_Name as "Host Check Policies" MAC_Address as "MAC Address"|table Username Realm "IP Address" "MAC Address" "Compliance Result" "Current HC Time" "Host Check Result" "Host Check Policies"

✓3 events (4/20/20 4:30:00.000 PM to 4/27/20 5:01:31.000 PM)
<table>
<tr><th>Username</th><th>Realm</th><th>IP Address</th><th>MAC Address</th><th>Compliance Result</th><th>Current HC Time</th><th>Host Check Result</th><th>Host Check Policies</th></tr>
<tr><td>P[redacted]jalkr</td><td>NAT-Realm</td><td>172.21.24.65</td><td>02-05-85-7f-eb-80</td><td></td><td>2020-04-23 23:56:01</td><td>Fail</td><td>HC-Process-POLICY</td></tr>
<tr><td>P[redacted]jalkr</td><td>NAT-Realm</td><td>1[redacted]</td><td>02-05-85-7f-eb-80</td><td></td><td>2020-04-23 23:56:01</td><td>Fail</td><td>HC-Custom-And-Predefined-OS-POLICY</td></tr>
<tr><td>sacnnj</td><td>Fortigate_Realm</td><td>1[redacted]</td><td>02-05-85-7f-eb-80</td><td></td><td>2020-04-20 18:25:12</td><td>Fail</td><td>HC-Process-POLICY</td></tr>
</table></td></tr>
</table>

Label	Description

Endpoint by Categories	This panel shows the endpoint by category or device manufacturer.
	Figure 24 Endpoint Categories
	
	
	Admin can also drill down to view device category details such as Windows, Linux, Mac, Routers, Network Boot Agents and so on.
	Figure 25 Endpoint by Categories
	
	 splunk>enterprise
	App: Pulse Policy Secure
	Administrator
	2 Messages
	Settings
	Activity
	Help
	Find
	Pulse Policy Secure Dashboard
	Pulse Policy Secure
	New Search
	Save As
	Close
	Last 30 days
	Job
	Verbose Mode
	Events (39)
	Patterns
	Statistics (5)
	Visualization
	100 Per Page
	Format
	Preview
	`index=pulsesecure sourcetype=ppsyslogportparser |where Server_Ip in ("10.96.76.3") |dedup Endpoint_MAC_Address| where (eventtype="Device_Classification" OR eventtype="Profile_Change") | table OS Category Endpoint_MAC_Address src|eval Endpoint_MAC_Address=replace(Endpoint_MAC_Address, ":`
	`, "-")|join type=left Endpoint_MAC_Address [search index=pulsesecure sourcetype=ppsyslogportparser |where eventtype in("Native_Supplicant_L2_Auth","Pulse_L2_Auth","MAC_Auth")]| eval "Session User" = if(isnotnull(user), user, "")|join type=left Endpoint_MAC_Address [search index`
	`=pulsesecure sourcetype=ppsyslogportparser eventtype="Device_Attribute_Update"] |eval Manufacturer=if(manufacturer!="{}",manufacturer,"")|eval OS = if(isnotnull(os), os, OS)|eval Category = if(isnotnull(category), category, Category)|rename ip as "IP Address" hostname as Hostname`
	`first_seen as "First Seen" last_seen as "Last Updated" profiler_name as "Profiler Name" groups as Groups Endpoint_MAC_Address as "MAC Address"|table "IP Address" "MAC Address" Hostname Manufacturer OS Category "Session User" "First Seen" "Last Updated" "Profiler Name" Groups|where OS`
	`="Linux"`
	39 of 214,874 events matched No Event Sampling
	IP Address · MAC Address · Hostname · Manufacturer · OS · Category · Session User · First Seen · Last Updated · Profiler Name · Groups
	ac-1f-6b-61-4d-66 · Linux · Linux
	ac-1f-6b-61-4c-75 · Linux · Linux
	ac-1f-6b-61-4d-15 · Linux · Linux

Endpoint by OS- Trends	This panel tracks the results of endpoint information based on Operating System (OS) over the specific period. Figure 26 OS Trends 

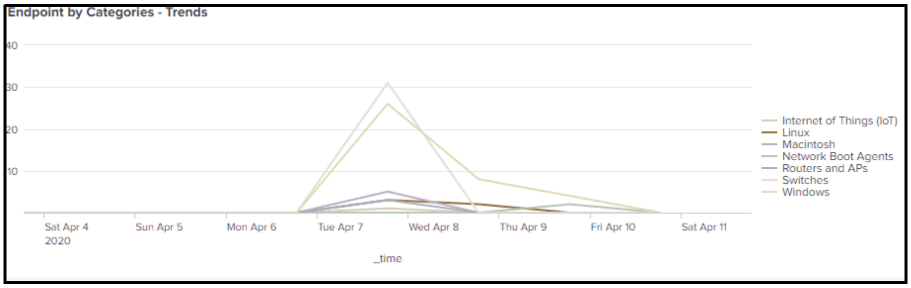
© 2020 Pulse Secure, LLC.

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Endpoint by Categories - Trends</td><td>

This panel shows the endpoint by category or device manufacturer over the specific period.

Trending analysis for endpoint by OS/Category could be useful to know the devices with various category and OS getting connected to network over the period of time. It could also be useful to know how frequently particular category (for example, IoT devices) of devices are getting connected to corporate network.

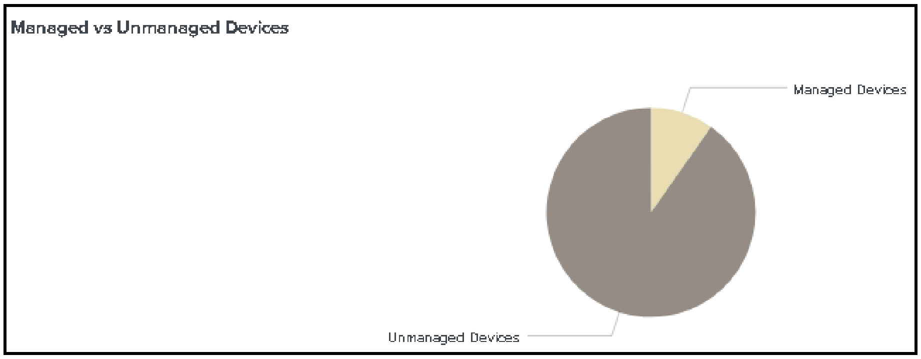
Figure 27 Categories Trends



</td></tr>
<tr><td>Managed vs Unmanaged Devices</td><td>

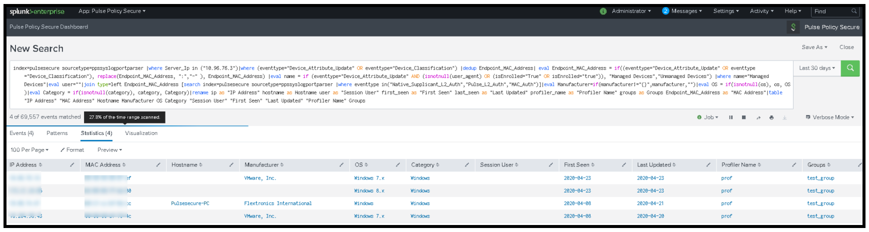
This panel shows the managed and unmanaged devices.

Figure 28 Managed vs Unmanaged



The Admin can drill-down to view the details (various available device attributes known to Splunk. For example, device MAC address, IP address, host name, OS, Category, Manufacturer etc.) of managed and unmanaged devices.

Figure 29 Managed Devices



New Search

```
index=pulsesecure sourcetype=ppssyslogportparser |where Server_Ip in ("10.96.76.3")|where (eventtype="Device_Attribute_Update" OR eventtype="Device_Classification") |dedup Endpoint_MAC_Address| eval Endpoint_MAC_Address = if((eventtype="Device_Attribute_Update" OR eventtype
    ="Device_Classification"), replace(Endpoint_MAC_Address, ":","-" ), Endpoint_MAC_Address) |eval name = if (eventtype="Device_Attribute_Update" AND (isnotnull(user_agent) OR (isEnrolled="True" OR isEnrolled="true")), "Managed Devices","Unmanaged Devices") |where name="Managed
    Devices"|eval user=""|join type=left Endpoint_MAC_Address [search index=pulsesecure sourcetype=ppssyslogportparser |where eventtype in("Native_Supplicant_L2_Auth","Pulse_L2_Auth","MAC_Auth")]|eval Manufacturer=if(manufacturer!="()",manufacturer,"")|eval OS = if(isnotnull(os), os, OS
    )|eval Category = if(isnotnull(category), category, Category)|rename ip as "IP Address" hostname as Hostname user as "Session User" first_seen as "First Seen" last_seen as "Last Updated" profiler_name as "Profiler Name" groups as Groups Endpoint_MAC_Address as "MAC Address"|table
    "IP Address" "MAC Address" Hostname Manufacturer OS Category "Session User" "First Seen" "Last Updated" "Profiler Name" Groups
```

4 of 69,557 events matched 27.8% of the time range scanned.

<table>
<tr><th>IP Address</th><th>MAC Address</th><th>Hostname</th><th>Manufacturer</th><th>OS</th><th>Category</th><th>Session User</th><th>First Seen</th><th>Last Updated</th><th>Profiler Name</th><th>Groups</th></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td></td><td>VMware, Inc.</td><td>Windows 7.x</td><td>Windows</td><td></td><td>2020-04-23</td><td>2020-04-23</td><td>prof</td><td>test_group</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td></td><td></td><td>Windows 8.x</td><td>Windows</td><td></td><td>2020-04-23</td><td>2020-04-23</td><td>prof</td><td>test_group</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>Pulsesecure-PC</td><td>Flextronics International</td><td>Windows</td><td>Windows</td><td></td><td>2020-04-08</td><td>2020-04-21</td><td>prof</td><td>test_group</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td></td><td>VMware, Inc.</td><td>Windows 7.x</td><td>Windows</td><td></td><td>2020-04-08</td><td>2020-04-20</td><td>prof</td><td>test_group</td></tr>
</table>

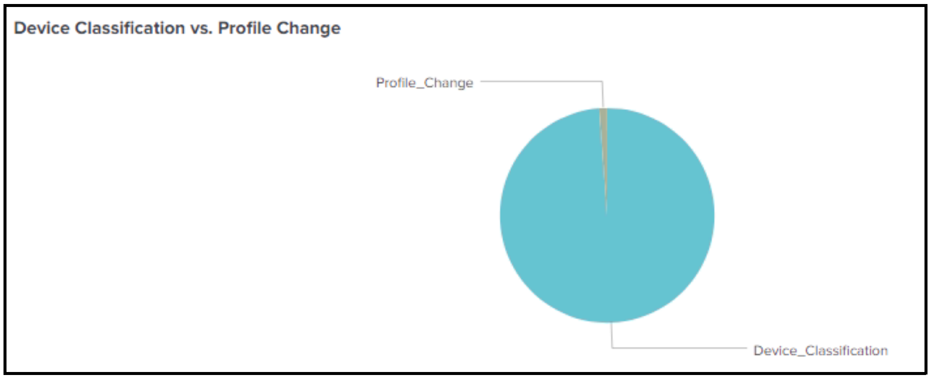
</td></tr>
</table>

© 2020 Pulse Secure, LLC.

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Device Classification vs Profile Change</td><td>

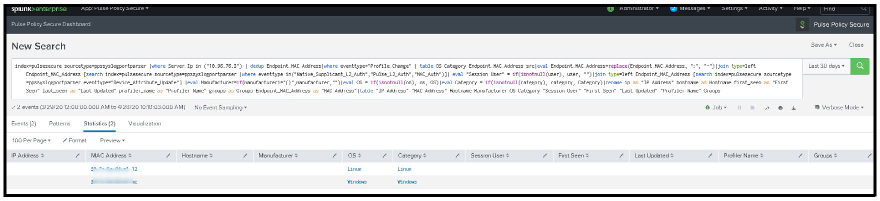
This panel shows the comparison between the number of devices classified and the number of devices with profile changed.

Figure 30 Device Classification vs Profile change



The Admin can also view the details (various available device attributes known to Splunk e.g. device MAC address, IP address, host name, OS, Category, Manufacturer etc.) of classified and profile change devices.

Figure 31 Device classification



New Search

```
index=pulsesecure sourcetype=ppssyslogportparser |where Server_Ip in ("10.96.76.3") | dedup Endpoint_MAC_Address|where eventtype="Profile_Change" | table OS Category Endpoint_MAC_Address src|eval Endpoint_MAC_Address=replace(Endpoint_MAC_Address, ":", "-")|join type=left
    Endpoint_MAC_Address [search index=pulsesecure sourcetype=ppssyslogportparser |where eventtype in("Native_Supplicant_L2_Auth","Pulse_L2_Auth","MAC_Auth")]| eval "Session User" = if(isnotnull(user), user, "")|join type=left Endpoint_MAC_Address [search index=pulsesecure sourcetype
    =ppssyslogportparser eventtype="Device_Attribute_Update"] |eval Manufacturer=if(manufacturer!="()",manufacturer,"")|eval OS = if(isnotnull(os), os, OS)|eval Category = if(isnotnull(category), category, Category)|rename ip as "IP Address" hostname as Hostname first_seen as "First
    Seen" last_seen as "Last Updated" profiler_name as "Profiler Name" groups as Groups Endpoint_MAC_Address as "MAC Address"|table "IP Address" "MAC Address" Hostname Manufacturer OS Category "Session User" "First Seen" "Last Updated" "Profiler Name" Groups
```

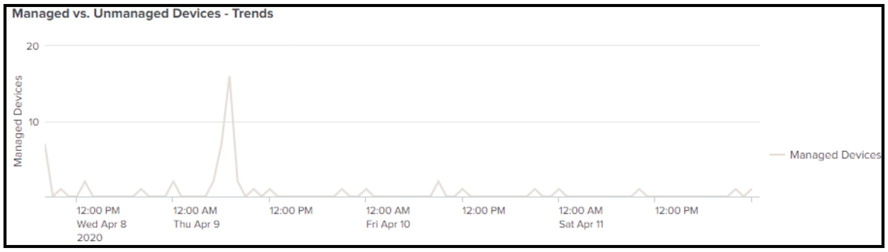
✓ 2 events (3/29/20 12:00:00.000 AM to 4/28/20 10:18:03.000 AM) No Event Sampling ▾

IP Address	MAC Address	Hostname	Manufacturer	OS	Category	Session User	First Seen	Last Updated	Profiler Name	Groups
	[redacted]			Linux	Linux					
	[redacted]			Windows	Windows					

</td></tr>
<tr><td>Managed vs Unmanaged Devices - Trends</td><td>

This panel shows the managed and unmanaged devices over the specific period.

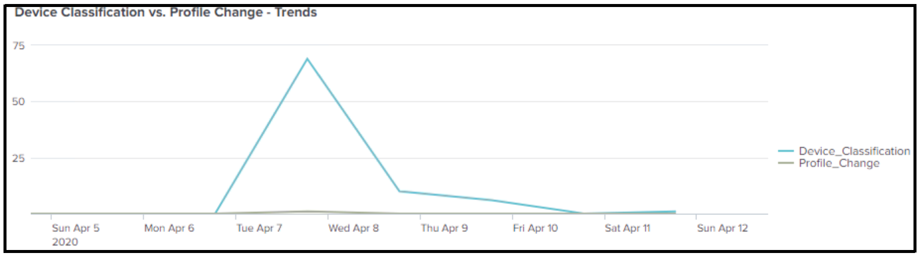
Figure 32 Managed vs Unmanaged Trends



</td></tr>
<tr><td>Device Classification vs Profile Change - Trends</td><td>

This panel shows the comparison between the number of devices classified and the number of devices with profile changed over the specific period.

Figure 33 Device Classification Profile Change Trends



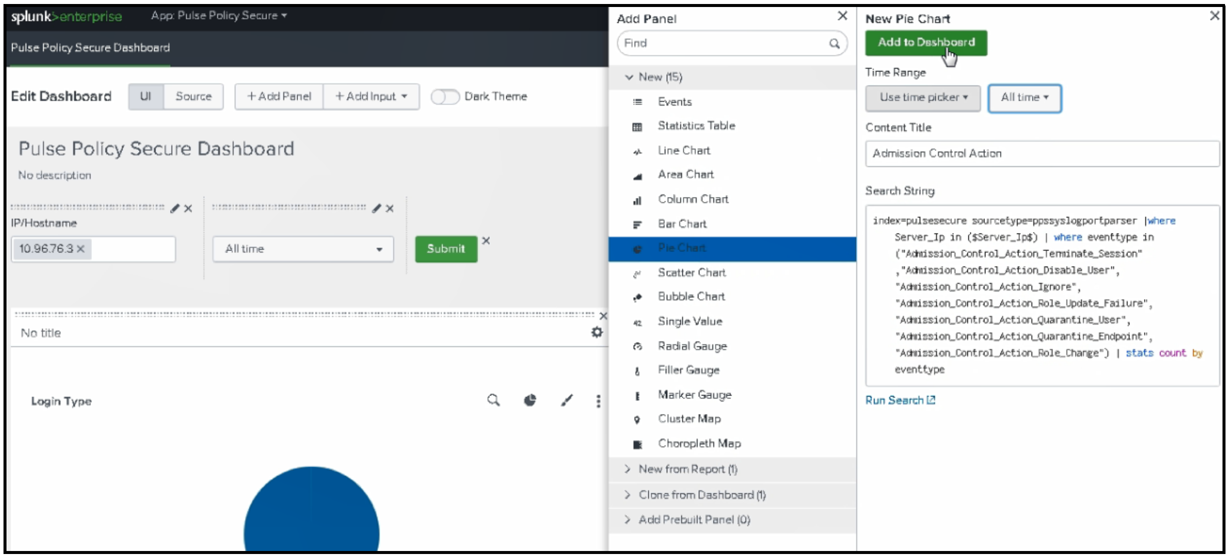
</td></tr>
</table>

Experienced Splunk users can customize the searches and dashboards provided with the PPS Syslog Add-On. The Admin must click the Edit option from the dashboard and then choose either to edit directly from the source, or from UI using Add Panel, Add Input.

To customize the dashboard:

1. Open the Dashboard editor and from the Dashboards listing page.
2. Click **Edit** to open the dashboard editor.
3. Select UI or Source to change the editing mode.
4. (Optional) Preview dashboard edits as you make them and click Save to save changes. Click Cancel at any point to discard changes.
5. At the top right of each panel, editing icons appear. The first editing icon represents the search for the panel. The search icon varies to represent the type of search being used.
6. Click **Add Panel,** select the type of chart.
7. Enter the Content Title, Enter the required index query in the Search String.
8. Click **Add to Dashboard**.

Figure 34 Edit Dashboard



Content Title

Admission Control Action

Search String

```
index=pulsesecure sourcetype=ppssyslogportparser |where
    Server_Ip in ($Server_Ip$) | where eventtype in
    ("Admission_Control_Action_Terminate_Session"
    ,"Admission_Control_Action_Disable_User",
    "Admission_Control_Action_Ignore",
    "Admission_Control_Action_Role_Update_Failure",
    "Admission_Control_Action_Quarantine_User",
    "Admission_Control_Action_Quarantine_Endpoint",
    "Admission_Control_Action_Role_Change") | stats count by
    eventtype
```

Figure 35 Customized Dashboard for Admission Control Action

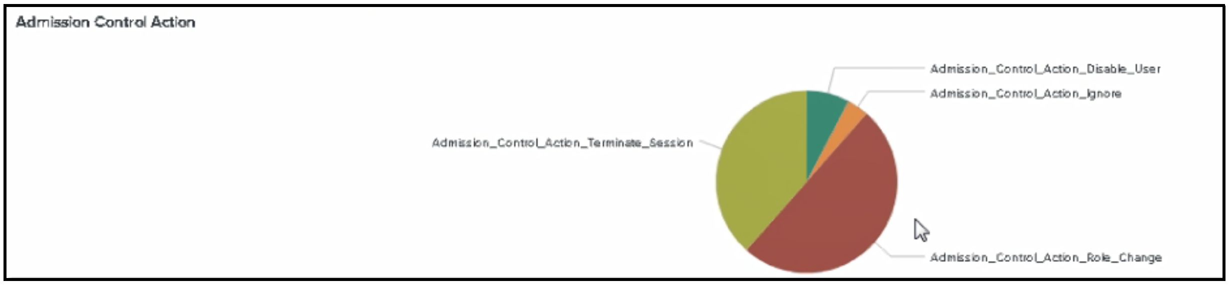
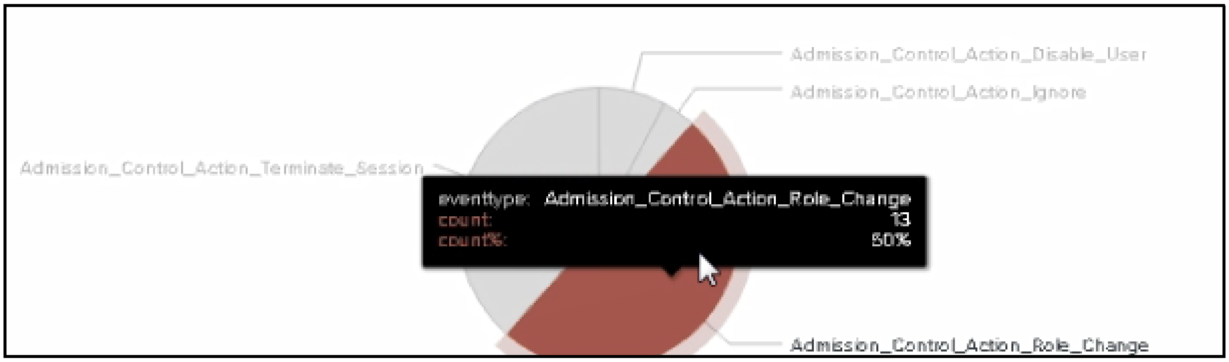


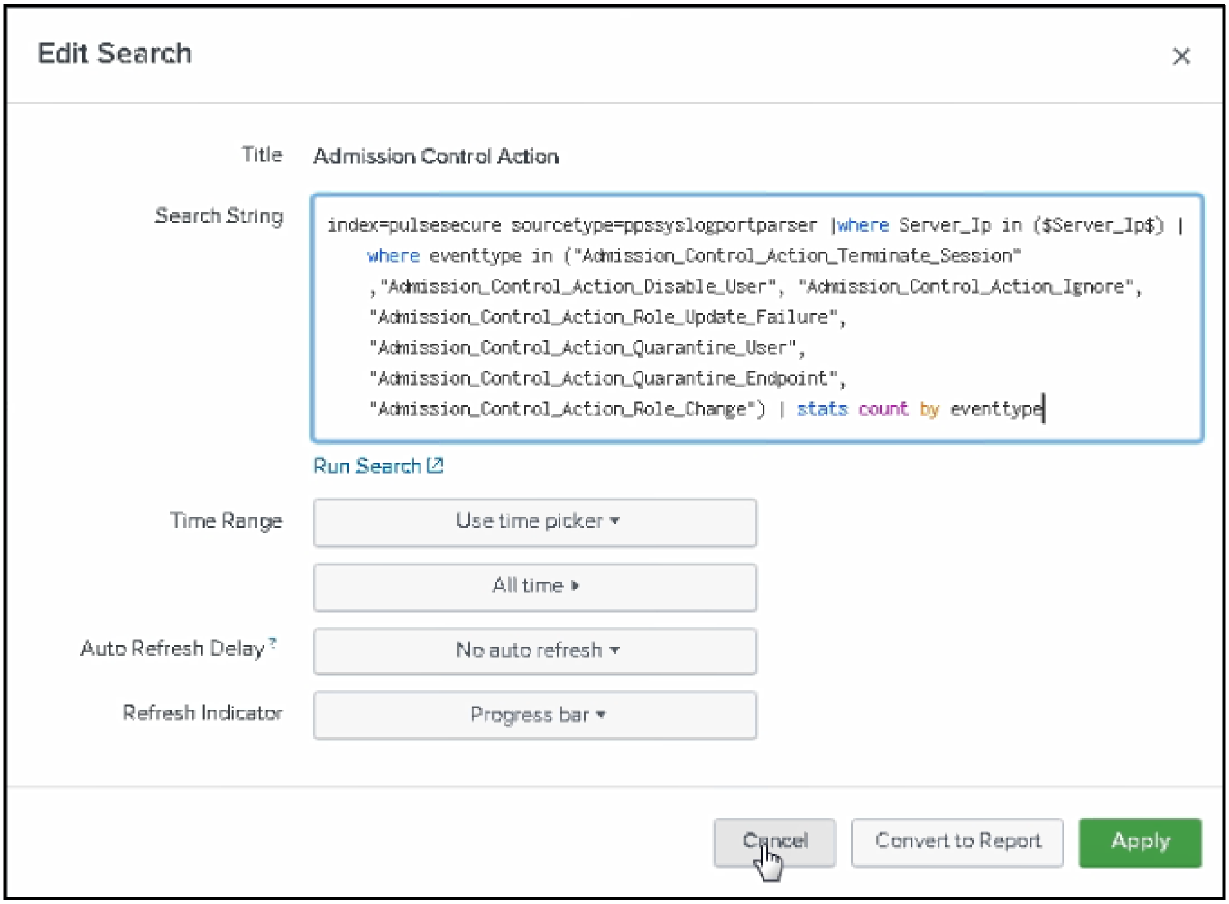
Figure 36 Drill Down


Admission_Control_Action_Disable_User
Admission_Control_Action_Ignore
Admission_Control_Action_Terminate_Session
Admission_Control_Action_Role_Change

eventtype: Admission_Control_Action_Role_Change
count: 13
count%: 50%

You can also choose to edit the search string, time range (i.e last 24 hours, 7 days, 30 days or All), refresh interval (i.e. 5 minutes, 10 minutes, 30 minutes, 60 minutes, No auto refresh to disable auto refresh of chart data is also provided), refresh indicator.

Figure 37 Editing Search



Title: Admission Control Action

Search String:

```
index=pulsesecure sourcetype=ppssyslogportparser |where Server_Ip in ($Server_Ip$) |
    where eventtype in ("Admission_Control_Action_Terminate_Session"
    ,"Admission_Control_Action_Disable_User", "Admission_Control_Action_Ignore",
    "Admission_Control_Action_Role_Update_Failure",
    "Admission_Control_Action_Quarantine_User",
    "Admission_Control_Action_Quarantine_Endpoint",
    "Admission_Control_Action_Role_Change") | stats count by eventtype
```

Time Range: Use time picker ▾

All time ▸

Auto Refresh Delay ?: No auto refresh ▾

Refresh Indicator: Progress bar ▾

Appendix

Below tables list different PPS messages which can be sent to SIEM systems for correlation, creating dashboards, reports and generating alerts.

© 2020 Pulse Secure, LLC.

Feature	Category	Sample Syslog	Event Type
Authentication	Primary authentication Success	`'<134>1 2019-07-01T00:47:59-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-01 00:47:59" pri=6 fw=10.204.57.142 vpn=ic user=demouser realm="Users" roles="" proto=auth src=172.21.8.199 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT24326: Primary authentication successful for demouser/System Local from 172.21.8.199"'`	Primary_Auth_Success
Authentication	Primary authentication failed	`<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-01 02:34:01" pri=6 fw=10.204.57.142 vpn=ic user=demouser realm="Users" roles="" proto=auth src=172.21.8.199 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT24327: Primary authentication failed for demouser/System Local from 172.21.8.199"'`	Primary_Auth_Failure

Authentication	Secondary authentication success	`<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-18 02:48:51" pri=6 fw=10.204.57.142 vpn=ic user=demouser realm="Users" roles="" proto=auth src=172.21.24.57 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT24326: Secondary authentication successful for demouser/System Local from 172.21.24.57"`	Secondary_Auth_Success
Authentication	Secondary authentication failed	`<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-18 02:53:14" pri=6 fw=10.204.57.142 vpn=ic user=demouser realm="Users" roles="" proto=auth src=172.21.24.57 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT24327: Secondary authentication failed for demouser/System Local from 172.21.24.57"`	Secondary_Auth_Failure

© 2020 Pulse Secure, LLC.

User login	Pulse L3 login success	'<134>1 2019-07-01T00:38:27-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-01 00:38:27" pri=6 fw=10.204.57.142 vpn=ic user=demouser realm="Users" roles="Users, Guest" proto=auth src=172.21.8.199 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="Pulse-Secure/9.0.3.1071 (Macintosh 10_14) Pulse/9.0.3.1071" duration= msg="AUT24414: Agent login succeeded for demouser/Users from 172.21.8.199 with Pulse-Secure/9.0.3.1071 (Macintosh 10_14) Pulse/9.0.3.1071."'	Pulse_L3_Auth
User login	Pulse 802.1x login success	'<134>1 2019-07-01T02:34:01-04:00 10.204.xx.xxx PulseSecure: - - - id=firewall time="2019-12-12 12:39:38" pri=6 fw=10.96.xx.xx vpn=ic user=demo_user realm="Users" roles="Users" proto=auth src=127.0.0.1 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="Pulse-Secure/9.1.4.1655 (Windows 7) Pulse/9.1.4.1655" duration= msg="AUT24414: Agent login succeeded for demo_user/Users from 8c-70-5a-98-62-08 with Pulse-Secure/9.1.4.1655 (Windows 7) Pulse/9.1.4.1655."	Pulse_L2_Auth

User login	Agent-less login success	'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-19 09:32:10" pri=6 fw=10.204.57.142 vpn=ic user=demouser realm="Users" roles="Users" proto=auth src=172.21.24.88 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:70.0) Gecko/20100101 Firefox/70.0" duration= msg="AUT31504: Login succeeded for demouser/Users (session:1c4e764b) from 172.21.24.88 with Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:70.0) Gecko/20100101 Firefox/70.0."	Agentless_L3_Auth
User login	native supplicant login	'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-17 12:22:04" pri=6 fw=10.96.78.19 vpn=ic user=test1 realm="Users" roles="Remediation" proto=auth src=127.0.0.1 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT24414: Agent login succeeded for test1/Users from 00-21-cc-c5-c7-69 ."	Native_Supplicant_L2_Auth

© 2020 Pulse Secure, LLC.

User login	Login failure	'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-01 02:34:01" pri=6 fw=10.204.57.142 vpn=ic user=demouser realm="Users" roles="" proto=auth src=172.21.8.199 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT23457: Login failed. Reason: No Roles"'	Login_Failure_no_roles
User login	Login failure	'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-01 02:34:01" pri=6 fw=10.204.57.142 vpn=ic user=demouser realm="Users" roles="" proto=auth src=172.21.8.199 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT23457: Login failed using auth server System Local (Local Authentication). Reason: Failed"'	Login_Auth_Failure
L2 Auth	MAC Auth	'<134>1 2019-07-01T02:10:58-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-01 02:10:58" pri=6 fw=10.204.57.142 vpn=ic user=System realm="" roles="" proto=auth src=127.0.0.1 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT24562: MAC address login succeeded for 00:21:86:f5:d6:ae /Guest Wired from 00-21-86-f5-d6-ae."'	MAC_Auth

L2 Auth	Radius Auth	'<134>1 2019-07-01T02:10:58-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-01 02:10:58" pri=6 fw=10.204.57.142 vpn=ic user=00:21:86:f5:d6:ae realm="Guest Wired" roles="Guest Wired Restricted" proto= src=127.0.0.1 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="EAM24805: RADIUS authentication accepted for 00:21:86:f5:d6:ae (realm \'Guest Wired\') from location-group \'Default\' and attributes are: NAS-IP-Address = 10.204.88.50,NAS-Port = 103,NAS-Port-Type = 15 "'	Radius_Auth_Success
Logout	User Logout	'<134>1 2019-07-30T01:45:43-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-30 01:45:43" pri=6 fw=10.204.57.142 vpn=ic user=demouser realm="Users" roles="Users, Guest" proto=auth src=172.21.8.199 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT22673: Logout from 172.21.8.199 (session:fd4a5bc4)"'	User_Logout

© 2020 Pulse Secure, LLC.

Logout	User Logout on receiving Radius Accounting STOP	'<134>1 2019-07-30T01:45:43-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-11 11:36:03" pri=6 fw=10.96.78.19 vpn=ic user=demo_user realm="Users" roles="Users" proto= src=10.96.74.62 dst= dstname= type=vpn op= arg="" result= sent =rcvd= agent="" duration= msg="EAM24460: Received a RADIUS Accounting Stop request. Terminated session"	User_Logout_on_Radius_Accounting_STOP
Logout	User logout because of max session time out	'<134>1 2019-07-30T01:45:43-04:00 10.204.57.142 PulseSecure: - - -id=firewall time="2019-12-12 06:45:35" pri=6 fw=10.204.57.142 vpn=ic user=demouser realm="Users" roles="Users" proto=auth src=172.21.24.61 dst= dstname= type=vpn op= arg="" result= sent = rcvd= agent="" duration= msg="AUT20914: Max session timeout for demouser/Users (session:6016f3a1)."	User_Logout_Max_Session_Timeout

Logout	User idle timeout for routine system scan	<134> 1 2019-06-12T17:07:19+05:30 10.204.58.32 PulseSecure: - - - id=firewall time="2019-06-12 17:07:19" pri=6 fw=10.204.58.32 vpn=ic user=demouser realm="Users" roles="remediate" proto=auth src=127.0.0.1 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT20915: Session timed out for demouser/Users (session:f5dd3a33) due to inactivity (last access at 16:35:39 2019/06/12).Idle session identified during routine system scan."	User_Logout_Session_Timeout_routine_scan
Logout	User Idle Timeout after user request	<134> 1 2019-06-12T17:07:19+05:30 10.204.58.32 PulseSecure: - - - id=firewall time="2019-06-12 17:07:19" pri=6 fw=10.204.58.32 vpn=ic user=demouser realm="Users" roles="remediate" proto=auth src=127.0.0.1 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT20915: Session timed out for demouser/Users (session:f5dd3a33) due to inactivity (last access at 16:35:39 2019/06/12). Idle session identified after user request."	User_Session_Timeout_user_request

L2 Access Control	Radius Disconnect	<134> 1 2019-06-12T17:07:19+05:30 10.204.58.32 PulseSecure: - - - id=firewall time="2019-12-17 12:22:29" pri=6 fw=10.96.78.19 vpn=ic user=test1 realm="Users" roles="Users, Remediation" proto= src=0.0.0.0 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="COA24753: Session Deletion Disconnect Message sent to RADIUS Client Cisco 3850 for agent at 00-21-cc-c5-c7-69 has succeeded."	Radius_COA_Success
L2 Access Control	Radius COA	<134> 1 2019-06-12T17:07:19+05:30 10.204.58.32 PulseSecure: - - - id=firewall time="2019-12-17 12:22:29" pri=6 fw=10.96.78.19 vpn=ic user=test1 realm="Users" roles="Users, Remediation" proto= src=0.0.0.0 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="COA31277: VLAN/RADIUS Attribute Change of Authorization Message sent to RADIUS Client C2960X-VLAN60 for agent at 00-21-cc-5d-d9-0f has succeeded."'	Radius_COA_Success

© 2020 Pulse Secure, LLC.

Host Checker	Host Checker policy success	''<134>1 2019-07-01T00:58:00-04:00 10.204.xx.xxx PulseSecure: - - - id=firewall time="2019-07-01 00:58:00" pri=6 fw=10.204.xx.xxx vpn=ic user=demouser realm="Users" roles="Guest" proto=auth src=172.21.x.xxx dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT24803: Host Checker policy \'firewall policy\' passed on host \'172.xx.x.xxx\' address \'ac-bc-32-77-44-27\' for user \'demouser\' <134>1 2019-07-01T00:48:00-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-01 00:48:00" pri=6 fw=10.204.xx.xxx vpn=ic user=demouser realm="Users" roles="" proto=auth src=172.21.x.xxx dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT24804: Host Checker policy \'firewall policy\' failed on host \'172.xx.xx.xx\' address \'ac-bc-32-77-44-27\' for user \'demouser\' reason \'Rule-firewall:Mac OS X Builtin Firewall 10.14.5 does not comply with policy. Compliance requires firewall to be turned on.\'.	HC_Pass

© 2020 Pulse Secure, LLC.

Host Checker	Host Checker policy failure	'<134>1 2019-07-01T00:48:00-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-01 00:48:00" pri=6 fw=10.204.57.142 vpn=ic user=demouser realm="Users" roles="" proto=auth src=172.21.8.199 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT24804: Host Checker policy \'firewall policy\' failed on host \'172.21.8.199\' address \'ac-bc-32-77-44-27\' for user \'demouser\' reason \'Rule-firewall:Mac OS X Builtin Firewall 10.14.5 does not comply with policy. Compliance requires firewall to be turned on.\'."'	HC_Failure
Role Change	Role Change	'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-17 12:31:25" pri=6 fw=10.96.78.19 vpn=ic user=test1 realm="Users" roles="Users, Remediation" proto=auth src=10.204.90.68 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT23077: Roles for user test1 on host 10.204.90.68 changed from <Users,Remediation> to <Remediation>."	role_change

Session Bridging	Browser session bridge	'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-17 12:22:27" pri=6 fw=10.96.78.19 vpn=ic user=test1 realm="Users" roles="Remediation" proto=auth src=127.0.0.1 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT31498: Browser connection bridged for test1/Users (session:06dc44e3) from 10.204.90.68."	agentless_session_bridge
IP Assignment	IP assignment because of Radius Accounting START	'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-11 11:34:11" pri=6 fw=10.96.78.19 vpn=ic user=demo_user realm="Users" roles="Users" proto= src=10.96.74.62 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="SBR31642: User demo_user has been assigned IP address 10.96.74.62"	Accounting_START_IP_Address_Assignment

© 2020 Pulse Secure, LLC.

IP Release	IP release because of Radius Accounting STOP	`'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-11 11:36:03" pri=6 fw=10.96.78.19 vpn=ic user=demo_user realm="Users" roles="Users" proto=auth src=10.96.74.62 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT31643: IP Address 10.96.74.62 has been released for the user demo_user"`	Accounting_STOP_IP_Address_Release
SSH Enforcement	SSH ACL Enforcement	`'<134>1 2019-07-29T15:42:59+05:30 ppsqa1 PulseSecure: - - - id=firewall time="2019-07-29 15:42:59" pri=6 fw=10.96.76.4 vpn=ic user=System realm="" roles="" proto= src=127.0.0.1 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="EAM24460: Successfully created configuration for applying ACL \'PPS-3COM-Default-ACL\' on interface Ethernet1/0/9 of Switch 10.204.88.17"'`	SSH_ACL_Enforcement

SSH Enforcement	SSH VLAN Enforcement	'<134>1 2019-07-30T12:36:41+05:30 ppsqa1 PulseSecure: - - - id=firewall time="2019-07-30 12:36:41" pri=6 fw=10.96.76.4 vpn=ic user=System realm="" roles="" proto= src=127.0.0.1 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="EAM24460: Successfully created configuration for applying vlanId = \'65\' on interface Ethernet1/0/9 of Switch 10.204.88.17"'	SSH_VLAN_Enforcement
SSH Enforcement	SNMP MAC Auth session end	'<134>1 2019-07-29T15:42:56+05:30 ppsqa1 PulseSecure: - - - id=firewall time="2019-07-29 15:42:56" pri=6 fw=10.96.76.4 vpn=ic user=00:21:cc:da:a8:d3 realm="Guest Wired" roles="" proto= src=127.0.0.1 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="EAM24460: Terminated SNMP based MAC Auth Session"'	SNMP_MAC_Auth_Session_End

© 2020 Pulse Secure, LLC.

Admission Control Action	Change of role	`'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-11 11:36:03" pri=6 fw=10.96.78.19 vpn=ic user=demo_user realm="Users" roles="Guest" proto= src=10.204.90.72 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="INT31554: Changed role for endpoint: 10.204.90.72(00-21-CC-5D-D9-0F) to Guest"'`	Admission_Control_Action_Role_Change
Admission Control Action	Quarantine Endpoint	`'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-11 11:36:03" pri=6 fw=10.96.78.19 vpn=ic user=00-21-CC-5D-D9-0F realm="Users" roles="Guest" proto= src=10.204.90.72 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="INT31555: Endpoint with MAC address: 00-21-CC-5D-D9-0F has been quarantined"'`	Admission_Control_Action_Quarantine_Endpoint
Admission Control Action	Quarantine User	`'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-11 11:36:03" pri=6 fw=10.96.78.19 vpn=ic user=00-21-CC-5D-D9-0F realm="Users" roles="Guest" proto= src=10.204.90.72 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="INT31555: User: demouser has been quarantined"'`	Admission_Control_Action_Quarantine_User

Admission Control Action	Terminate User Session	`'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-11 11:36:03" pri=6 fw=10.96.78.19 vpn=ic user=00-21-CC-5D-D9-0F realm="Users" roles="Guest" proto= src=10.204.90.72 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="INT31553: User: demouser with session ID: sid123456 is being terminated"'`	Admission_Control_Action_Terminate_Session
Admission Control Action	Disable User	`'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-11 11:36:03" pri=6 fw=10.96.78.19 vpn=ic user=00-21-CC-5D-D9-0F realm="Users" roles="Guest" proto= src=10.204.90.72 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="INT31552: User: demouser with session ID: sid123456 has been disabled"'`	Admission_Control_Action_Disable_User
Admission Control Action		`'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-11 11:36:03" pri=6 fw=10.96.78.19 vpn=ic user=00-21-CC-5D-D9-0F realm="Users" roles="Guest" proto= src=10.204.90.72 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="INT31547: Policy: policy1 Action: Ignore for sid: sid1234567890`	Admission_Control_Action_Ignore

© 2020 Pulse Secure, LLC.

Admission Control Action	Update role failure	'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-11 11:36:03" pri=6 fw=10.96.78.19 vpn=ic user=00-21-CC-5D-D9-0F realm="Users" roles="Guest" proto= src=10.204.90.72 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="INT31546: Failed to update role for sid: sid1234567890"'	Admission_Control_Action_Role_Update_Failure

Below Profiler logs are captured in PPS Events logs and same can be used to show the number of discovered devices.

Feature	Sub-Feature	Sample Syslog	Event Type
Profiler	Device OS Classification	<134>1 2019-07-23T04:52:10-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-23 04:52:10" pri=6 fw=10.204.57.142 vpn=ic user=System realm="" roles="" type=mgmt proto= src=127.0.0.1 dst= dstname= sent= rcvd= msg="PRO31368: Device (ac:1f:6b:62:28:bb) is classified as Linux."	Device_Classification
Profiler	Device profile Change	<134>1 2019-07-23T04:53:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-23 04:53:01" pri=6 fw=10.204.57.142 vpn=ic user=System realm="" roles="" type=mgmt proto= src=127.0.0.1 dst= dstname= sent= rcvd= msg="PRO31369: Device (00:50:56:8e:dc:16) has changed profile from category Linux to Routers and APs."	Profile_Change

Profiler	Device attribute update (from PPS session)	<134>1 2019-07-23T03:35:52-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-07-23 03:35:52" pri=6 fw=10.204.57.142 vpn=ic user=System realm="" roles="" type=mgmt proto= src=127.0.0.1 dst= dstname= sent= rcvd= msg="PRO31459: Device(ac-bc-32-77-44-27)\'s attributes got updated from (first_seen = {2019-07-23 07:12:20.531374+00:00} previous_category = {} os = {Macintosh 10_14} category = {Macintosh} ip = {172.21.8.199} previous_os = {} last_seen = {2019-07-23 07:35:44.369781+00:00} macaddr = {ac:bc:32:77:44:27} manufacturer = {Apple, Inc.} profiler_name = {profiler} status = {approved}) to (first_seen = {2019-07-23} previous_category = {} os = {Macintosh 10_14} category = {Macintosh} ip = {172.21.8.199} previous_os = {} last_seen = {2019-07-23} macaddr = {ac:bc:32:77:44:27} manufacturer = {Apple, Inc.} profiler_name = {profiler} status = {approved})."	Device_Attribute_Update
Concurrent Users	Number of concurrent users	<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-19 16:00:44" pri=6 fw=10.96.7.66 vpn=n-166 user=System realm="" roles="" type=mgmt proto= src=127.0.0.1 dst= dstname= sent= rcvd= msg="STS20641: Number of concurrent users logged in to the device: 3"	Number_Of_CC_Users

Below Profiler logs are captured in PPS Events logs and same can be used to show the number of discovered devices, device information by OS/Category, the number devices with profile change etc

© 2020 Pulse Secure, LLC.

Table 2 Profiler Logs

Feature	Category	Sample Syslog	Event Type
Third Party Device management	Enforcer addition	<134>1 2019-08-08T02:01:21-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-08-08 02:01:21" pri=6 fw=10.204.57.142 vpn=ic user=admin realm="Admin Users" roles=".Administrators" type=mgmt msg="ADM23472: Added Enforcer \'PAN firewall\'"	New_Enforcer
	Enforcer removal	<134>1 2019-08-08T02:09:28-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-08-08 02:09:28" pri=6 fw=10.204.57.142 vpn=ic user=admin realm="Admin Users" roles=".Administrators" type=mgmt msg="ADM23473: Deleted Enforcer \'PAN firewall\'"'	Enforcer_Deleted
	Radius Client addition	<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-19 03:43:28" pri=6 fw=10.204.57.142 vpn=ic user=admin realm="Admin Users" roles=".Administrators" type=mgmt msg="ADM24357: Added RADIUS Client 'cisco'"	New_Radius_Client
	Radius Client Removal	<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-19 03:51:46" pri=6 fw=10.204.57.142 vpn=ic user=admin realm="Admin Users" roles=".Administrators" type=mgmt msg="ADM24358: Deleted RADIUS Client 'cisco'"	Radius_Client_Delete

	Admission Control Client addition	`<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-19 04:04:05" pri=6 fw=10.204.57.142 vpn=ic user=admin realm="Admin Users" roles=".Administrators" type=mgmt msg="ADM31536: Admission Control Client added: 'Juniper_SDSN'"`	New_Admission_Control_Client
	Admission Control Client removal	`<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-19 04:06:34" pri=6 fw=10.204.57.142 vpn=ic user=admin realm="Admin Users" roles=".Administrators" type=mgmt msg="ADM31538: Admission Control Client deleted: 'Juniper_SDSN'"`	Admission_Control_Client_Delete
	SNMP Switch addition	`<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-19 06:08:34" pri=6 fw=10.204.57.142 vpn=ic user=admin realm="Admin Users" roles=".Administrators" type=mgmt msg="ADM31358: Added SNMP switch 'Cisco'"`	New_SNMP_Switch
	SNMP Switch removal	`'<134>1 2019-07-01T02:34:01-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-12-19 09:04:03" pri=6 fw=10.204.57.142 vpn=ic user=admin realm="Admin Users" roles=".Administrators" type=mgmt msg="ADM31359: Deleted SNMP Switch 'Cisco'"`	SNMP_Switch_Delete

© 2020 Pulse Secure, LLC.

License	License Added	<134>1 2019-08-08T02:18:42-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-08-08 02:18:42" pri=6 fw=10.204.57.142 vpn=ic user=admin realm="Admin Users" roles=".Administrators" type=mgmt msg="LIC10201: License for \'Pulse Policy Secure License 100 Concurrent Sessions - Subscription 1 Year\' - \'kernel ice soccer holiday camel integrity equator square bracelet world falcon\' installed"	License_Added
License	License Removed	<134>1 2019-08-08T02:18:33-04:00 10.204.57.142 PulseSecure: - - - id=firewall time="2019-08-08 02:18:33" pri=6 fw=10.204.57.142 vpn=ic user=admin realm="Admin Users" roles=".Administrators" type=mgmt msg="LIC10202: License for \'Pulse Policy Secure License 100 Concurrent Sessions - Subscription 1 Year\' - \'kernel ice soccer holiday camel integrity equator square bracelet world falcon\' removed"	License_Removed

© 2020 Pulse Secure, LLC.

© 2020 Pulse Secure, LLC.