CONFIGURATION GUIDE

Cloudpath Enrollment System Integration with Palo Alto Firewalls Configuration Guide, 5.5

Supporting Cloudpath Software Release 5.5

Part Number: 800-72408-001 Rev A
Publication Date: 28 August 2019

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Integration with Palo Alto Firewalls

Cloudpath supplements data already captured by Palo Alto firewalls by adding mappings of the IP address to a User Id, allowing the captured traffic to be more identifiable. When a user joins the network via Cloudpath, the Palo Alto firewall is notified of the user's login. Similarly, when a user is known to have left the network, the firewall is notified of the logout.

Cloudpath also sends Host Information Profile (HIP) data to the firewall, which increases visibility on connections and allows filtering on the type of client (by operating system, etc).

This section describes how to integrate Cloudpath with a Palo Alto firewall.

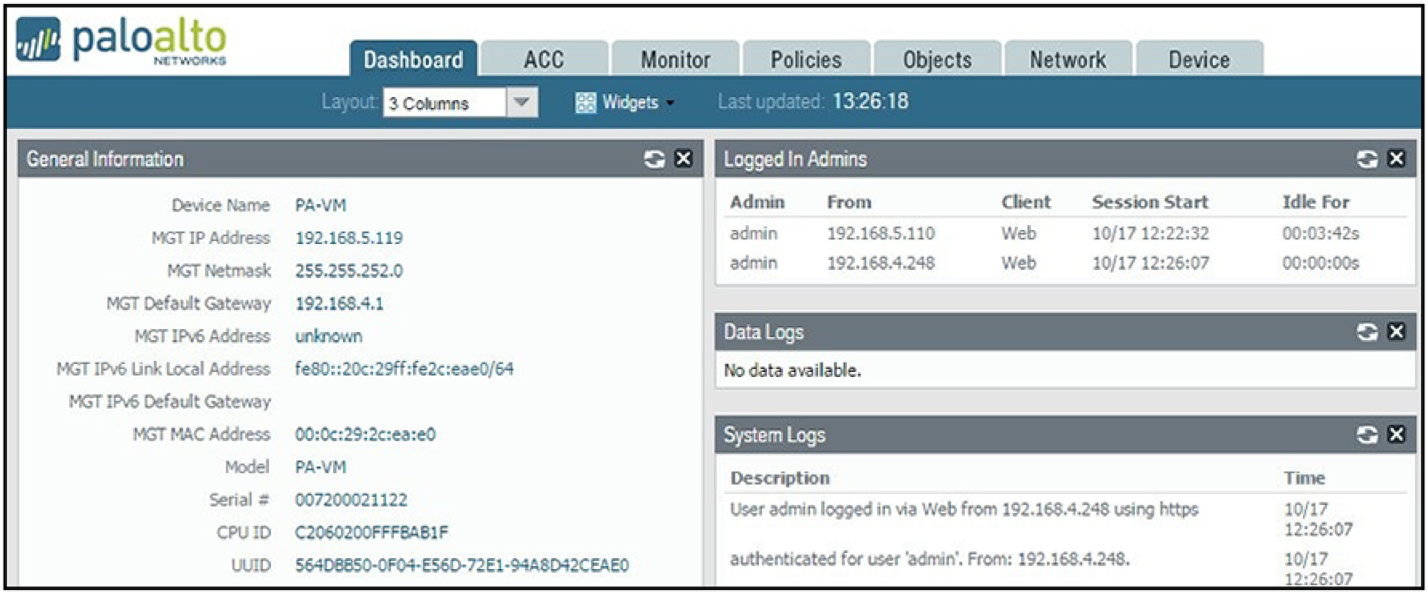
Palo Alto Firewall Prerequisites

Configuring Cloudpath to integrate with a Palo Alto firewall requires:

- Administrator credentials for the Palo Alto system

IP address or hostname of the Palo Alto system

FIGURE 1 Palo Alto Firewall System Information



Layout: 3 Columns

Last updated: 13:26:18

General Information

Device Name	PA-VM
MGT IP Address	192.168.5.119
MGT Netmask	255.255.252.0
MGT Default Gateway	192.168.4.1
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::20c:29ff:fe2c:eae0/64
MGT IPv6 Default Gateway	
MGT MAC Address	00:0c:29:2c:ea:e0
Model	PA-VM
Serial #	007200021122
CPU ID	C2060200FFFBAB1F
UUID	564DBB50-0F04-E56D-72E1-94A8D42CEAE0

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	192.168.5.110	Web	10/17 12:22:32	00:03:42s
admin	192.168.4.248	Web	10/17 12:26:07	00:00:00s

Data Logs

No data available.

System Logs

Description	Time
User admin logged in via Web from 192.168.4.248 using https	10/17 12:26:07
authenticated for user 'admin'. From: 192.168.4.248.	10/17 12:26:07

Wireless Controller Configuration

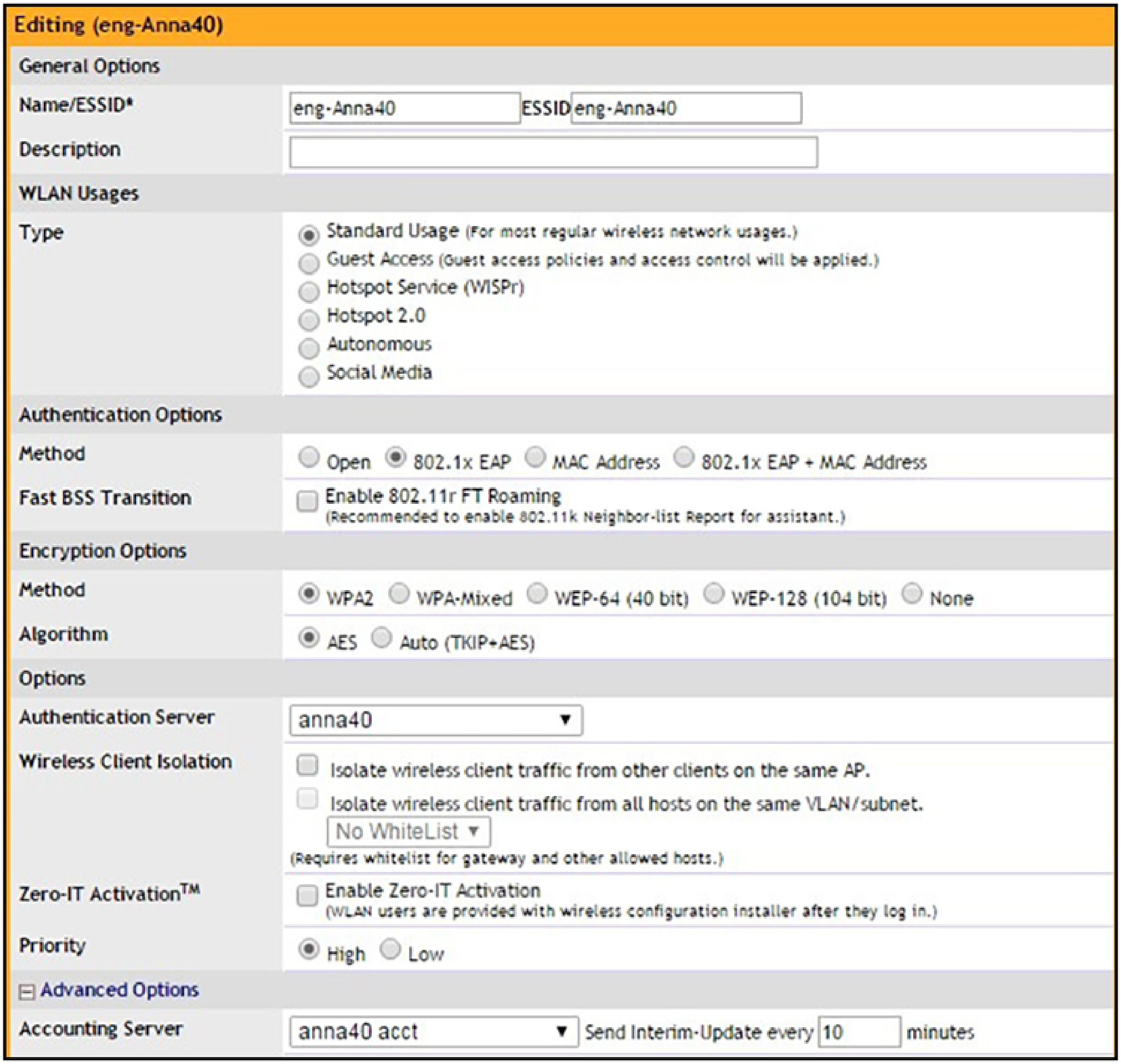
The examples in this section show Ruckus Wireless controllers. However, Cloudpath supports integration with Palo Alto firewalls using wireless controllers from most vendors.

The wireless controller configuration requirements:

- AAA authentication server and AAA accounting server.
  - RADIUS enabled (RADIUS Accounting for AAA Accounting server)
  - IP address of Cloudpath system
  - Authentication port =1812 (Accounting port=1813)

  - Shared must match the shared secret for the Cloudpath onboard RADIUS server (or shared secret for the external RADIUS server).
- WLAN configuration
  - Standard Usage
  - 802.1x EAP Method
  - WPA2 Encryption
  - AES Algorithm
  - Select AAA authentication server previously configured
  - In Advanced Options section, select AAA accounting server previously configured

FIGURE 2 WLAN Configuration with AAA Accounting Server



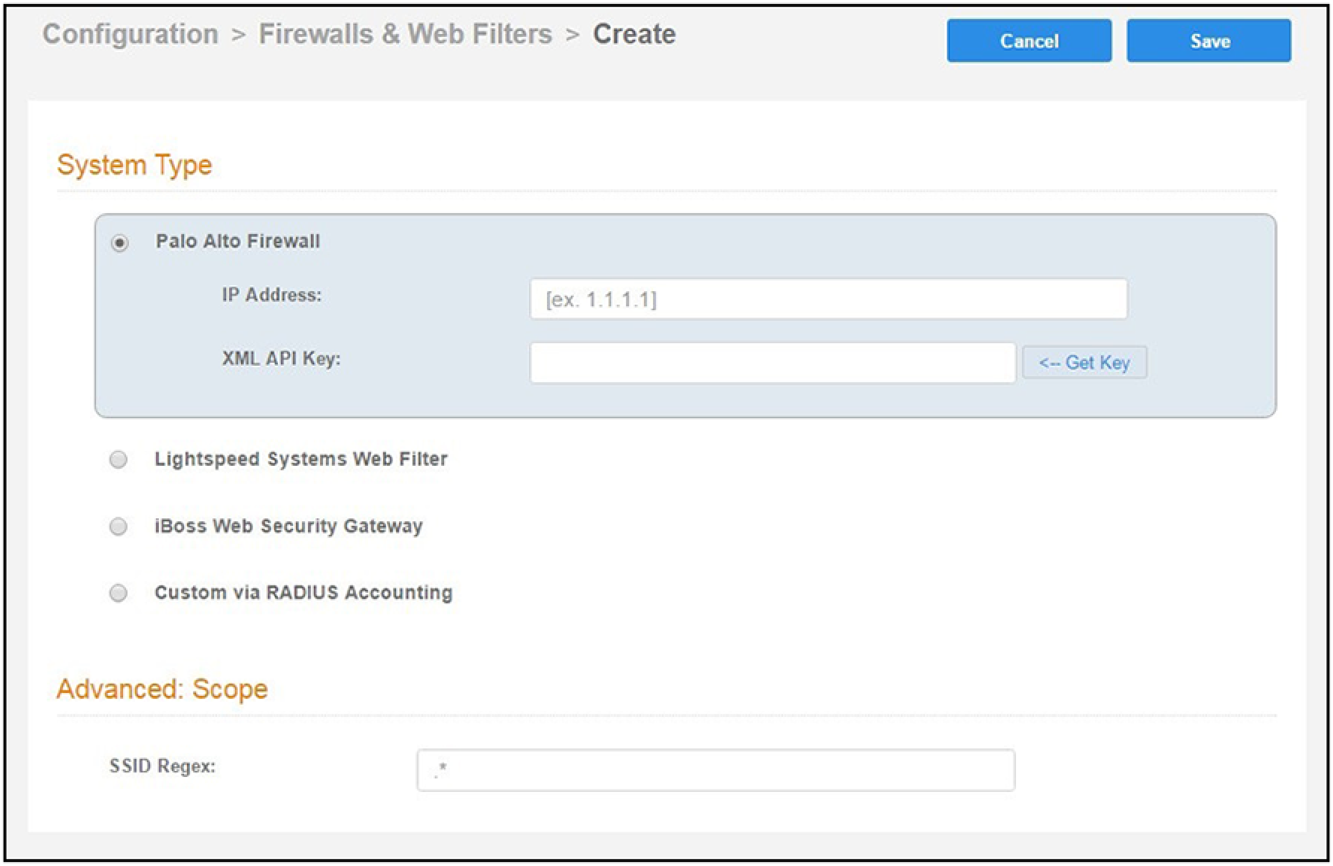
Editing (eng-Anna40)

General Options	
Name/ESSID*	eng-Anna40 ESSID eng-Anna40
Description	
WLAN Usages	
Type	● Standard Usage (For most regular wireless network usages.) ○ Guest Access (Guest access policies and access control will be applied.) ○ Hotspot Service (WISPr) ○ Hotspot 2.0 ○ Autonomous ○ Social Media
Authentication Options	
Method	○ Open ● 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address
Fast BSS Transition	□ Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)
Encryption Options	
Method	● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ○ None
Algorithm	● AES ○ Auto (TKIP+AES)
Options	
Authentication Server	anna40 ▼
Wireless Client Isolation	□ Isolate wireless client traffic from other clients on the same AP. □ Isolate wireless client traffic from all hosts on the same VLAN/subnet. No WhiteList ▼ (Requires whitelist for gateway and other allowed hosts.)
Zero-IT Activation™	□ Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
Priority	● High ○ Low
⊟ **Advanced Options**	
Accounting Server	anna40 acct ▼ Send Interim-Update every 10 minutes

Cloudpath Configuration

1. Navigate to **Configuration** > **Firewalls & Web Filters**.
2. Select **Palo Alto Firewall**.

FIGURE 3 Firewalls & Web Filters



System Type

● Palo Alto Firewall

IP Address: [ex. 1.1.1.1]

XML API Key:

○ Lightspeed Systems Web Filter

○ iBoss Web Security Gateway

○ Custom via RADIUS Accounting

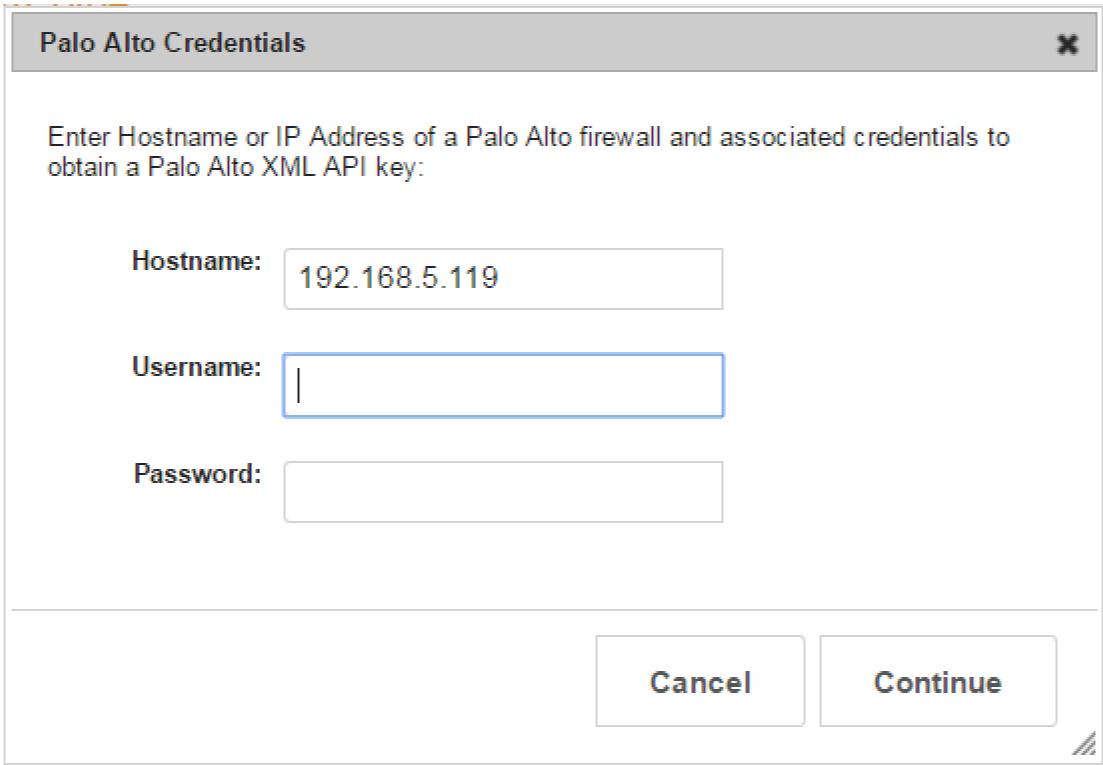
Advanced: Scope

SSID Regex: .*

3. Enter the management IP address of the Palo Alto system.

4. Click **Get Key**.

FIGURE 4 Palo Alto Credentials



Palo Alto Credentials

Enter Hostname or IP Address of a Palo Alto firewall and associated credentials to obtain a Palo Alto XML API key:

Hostname: 192.168.5.119

Username:

Password:

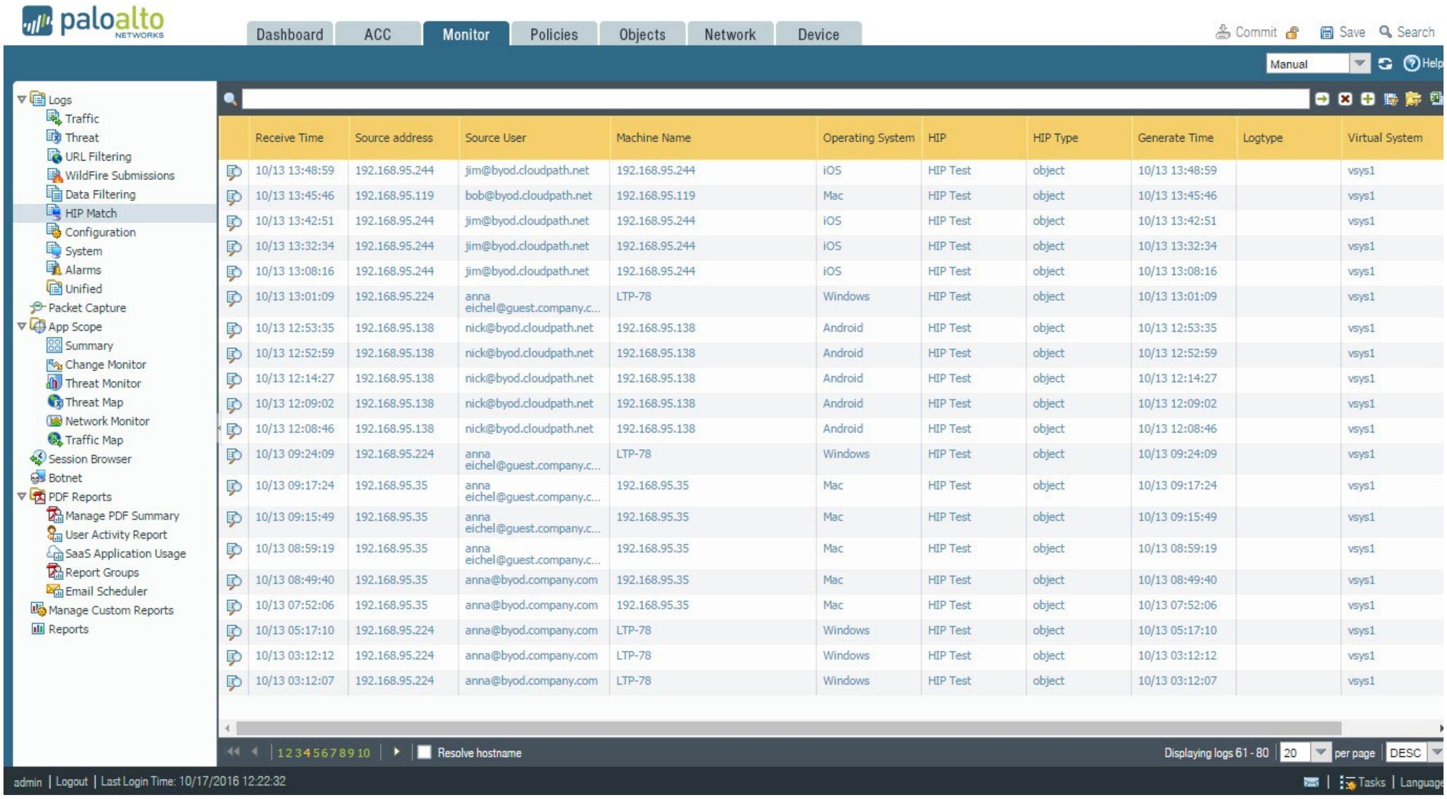
5. In the Palo Alto Credentials popup, enter:
   - Hostname or IP address of the Palo Alto firewall.
   - Palo Alto administrator username.
   - Palo Alto administrator password.

   The API key is generated by the system and displayed. This is the API key the Cloudpath system will use to communicate with the firewall.
6. **Scope** is optional. If you want only information from a specific SSID to be forwarded to the Palo Alto firewall (or other specified web filters), enter it in the **SSID Regex** field.

Palo Alto Output

The example output below displays the type of information displayed from the Palo Alto firewall **Monitor** tab, and **Host Information Profile (HIP) Match** logs. The **Source address** and **Source User** display the user data from the Cloudpath enrollment record. The **Machine Name** and **Operating System** fields, if known by Cloudpath, display the machine information.

FIGURE 5 Palo Alto Firewall Displaying Cloudpath Traffic



Receive Time	Source address	Source User	Machine Name	Operating System	HIP	HIP Type	Generate Time	Logtype	Virtual System
10/13 13:48:59	192.168.95.244	jim@byod.cloudpath.net	192.168.95.244	iOS	HIP Test	object	10/13 13:48:59		vsys1
10/13 13:45:46	192.168.95.119	bob@byod.cloudpath.net	192.168.95.119	Mac	HIP Test	object	10/13 13:45:46		vsys1
10/13 13:42:51	192.168.95.244	jim@byod.cloudpath.net	192.168.95.244	iOS	HIP Test	object	10/13 13:42:51		vsys1
10/13 13:32:34	192.168.95.244	jim@byod.cloudpath.net	192.168.95.244	iOS	HIP Test	object	10/13 13:32:34		vsys1
10/13 13:08:16	192.168.95.244	jim@byod.cloudpath.net	192.168.95.244	iOS	HIP Test	object	10/13 13:08:16		vsys1
10/13 13:01:09	192.168.95.224	anna eichel@guest.company.c...	LTP-78	Windows	HIP Test	object	10/13 13:01:09		vsys1
10/13 12:53:35	192.168.95.138	nick@byod.cloudpath.net	192.168.95.138	Android	HIP Test	object	10/13 12:53:35		vsys1
10/13 12:52:59	192.168.95.138	nick@byod.cloudpath.net	192.168.95.138	Android	HIP Test	object	10/13 12:52:59		vsys1
10/13 12:14:27	192.168.95.138	nick@byod.cloudpath.net	192.168.95.138	Android	HIP Test	object	10/13 12:14:27		vsys1
10/13 12:09:02	192.168.95.138	nick@byod.cloudpath.net	192.168.95.138	Android	HIP Test	object	10/13 12:09:02		vsys1
10/13 12:08:46	192.168.95.138	nick@byod.cloudpath.net	192.168.95.138	Android	HIP Test	object	10/13 12:08:46		vsys1
10/13 09:24:09	192.168.95.224	anna eichel@guest.company.c...	LTP-78	Windows	HIP Test	object	10/13 09:24:09		vsys1
10/13 09:17:24	192.168.95.35	anna eichel@guest.company.c...	192.168.95.35	Mac	HIP Test	object	10/13 09:17:24		vsys1
10/13 09:15:49	192.168.95.35	anna eichel@guest.company.c...	192.168.95.35	Mac	HIP Test	object	10/13 09:15:49		vsys1
10/13 08:59:19	192.168.95.35	anna eichel@guest.company.c...	192.168.95.35	Mac	HIP Test	object	10/13 08:59:19		vsys1
10/13 08:49:40	192.168.95.35	anna@byod.company.com	192.168.95.35	Mac	HIP Test	object	10/13 08:49:40		vsys1
10/13 07:52:06	192.168.95.35	anna@byod.company.com	192.168.95.35	Mac	HIP Test	object	10/13 07:52:06		vsys1
10/13 05:17:10	192.168.95.224	anna@byod.company.com	LTP-78	Windows	HIP Test	object	10/13 05:17:10		vsys1
10/13 03:12:12	192.168.95.224	anna@byod.company.com	LTP-78	Windows	HIP Test	object	10/13 03:12:12		vsys1
10/13 03:12:07	192.168.95.224	anna@byod.company.com	LTP-78	Windows	HIP Test	object	10/13 03:12:07		vsys1

The information displayed is obtained from the Cloudpath Enrollment Record.

Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com