CONFIGURATION GUIDE

# Cloudpath Integration with Palo Alto Firewalls

## Supporting Software Release 5.2

*Part Number: 800-71664-001*
*Publication Date: September 2017*

# Copyright Notice and Proprietary Information



# Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

# Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. BROCADE and RUCKUS WIRELESS, INC. AND THEIR LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. BROCADE and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

# Limitation of Liability

IN NO EVENT SHALL BROCADE or RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

# Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Brocade, the B-wing symbol, MyBrocade, and ICX are trademarks of Brocade Communications Systems, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

# 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.

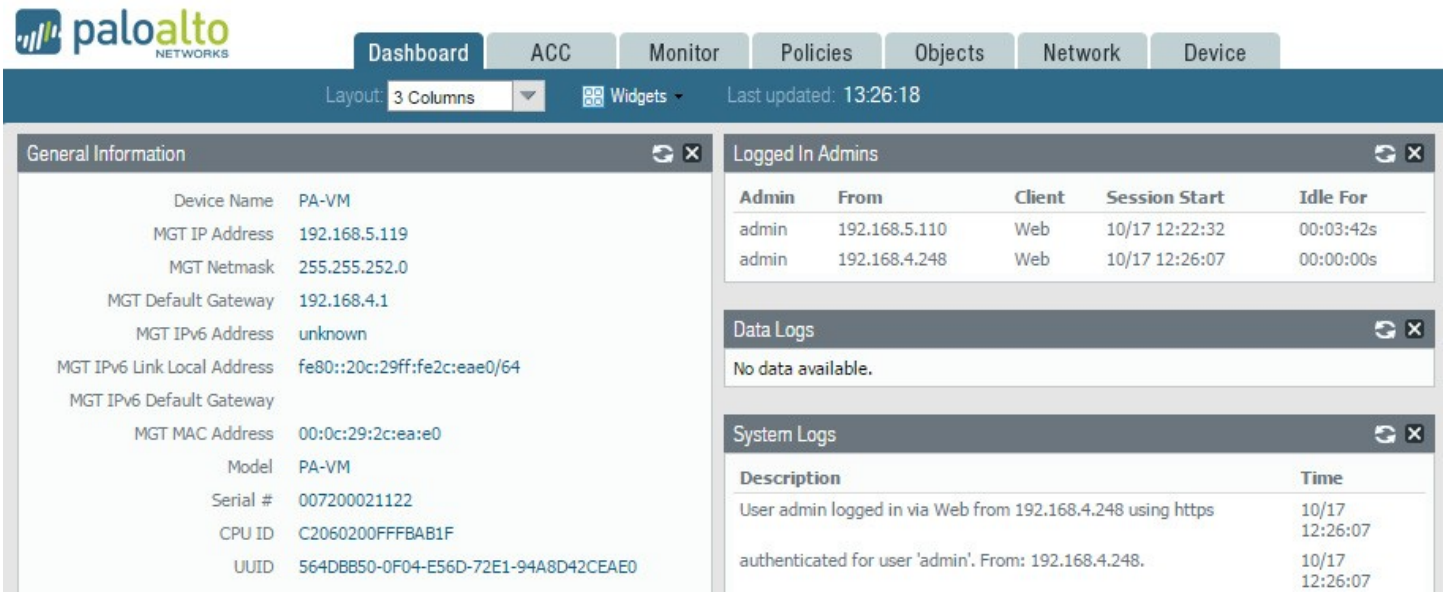
## Palo Alto Firewall Prerequisites

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




## Wireless Controller Configuration

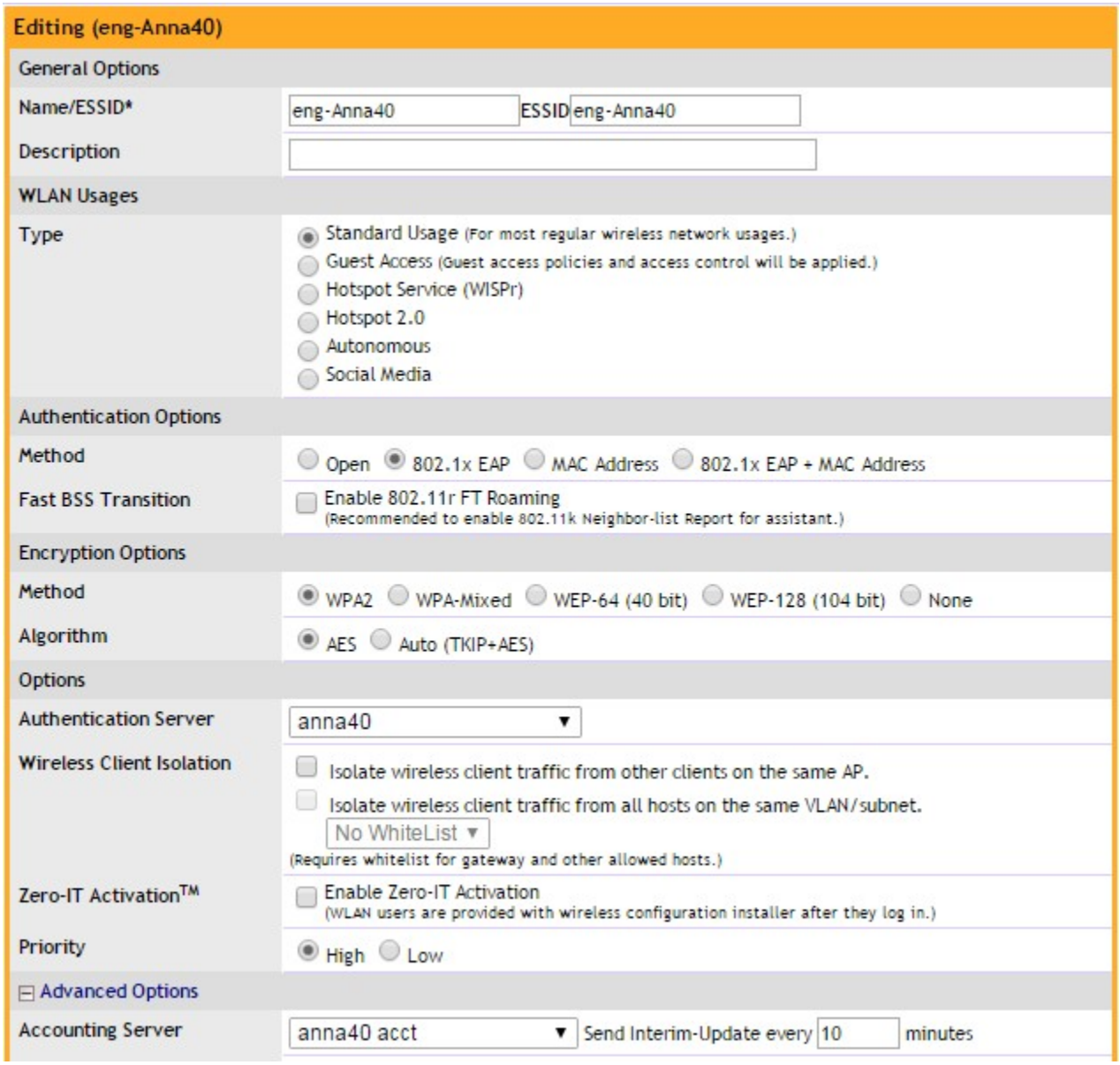
The examples in this section show Ruckus Wireless controllers. However, Cloudpath supports integration with Palo Alto firewalls using wireless controllers from most vendors.

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

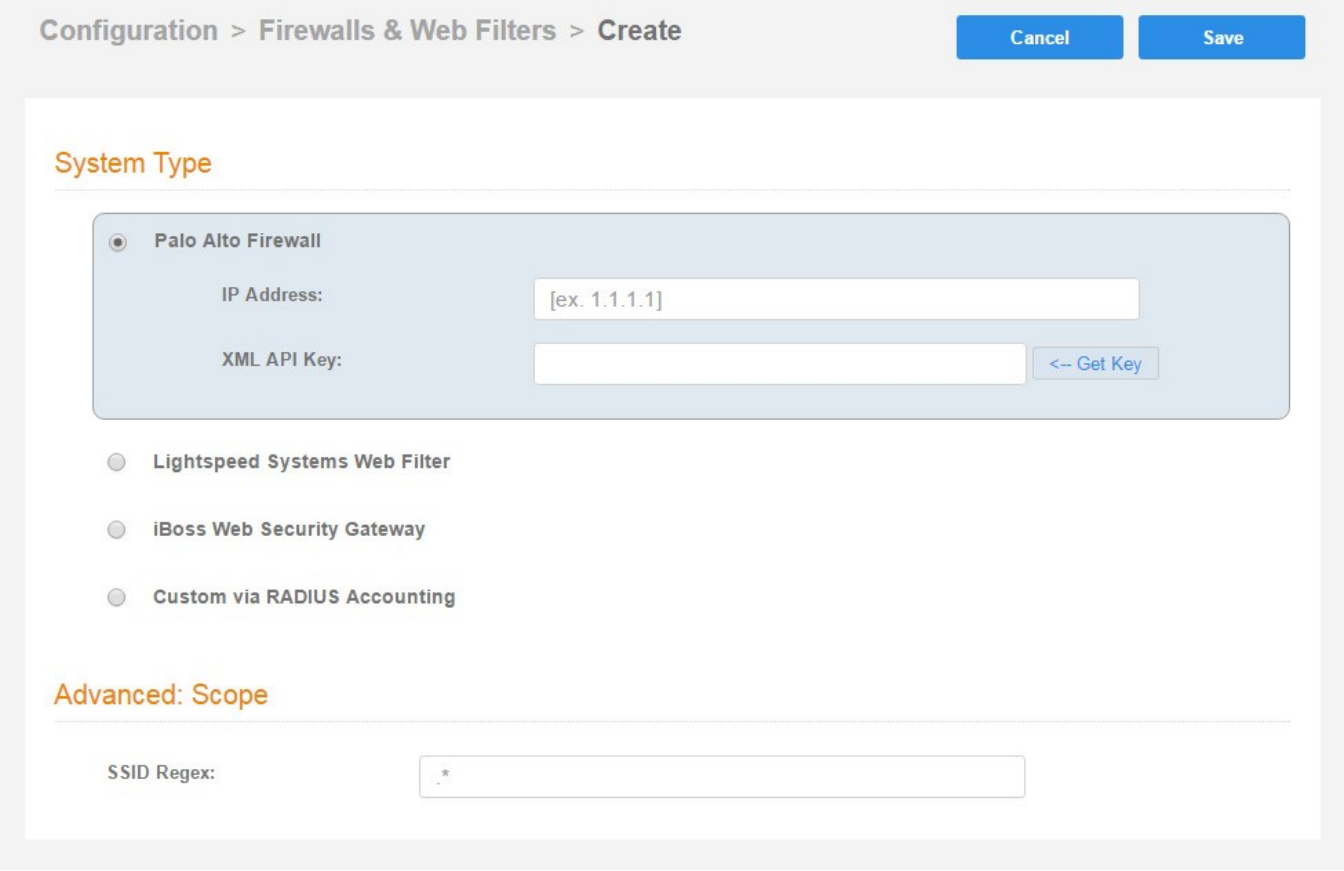
**FIGURE 2** WLAN Configuration with AAA Accounting Server



# Cloudpath Configuration

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

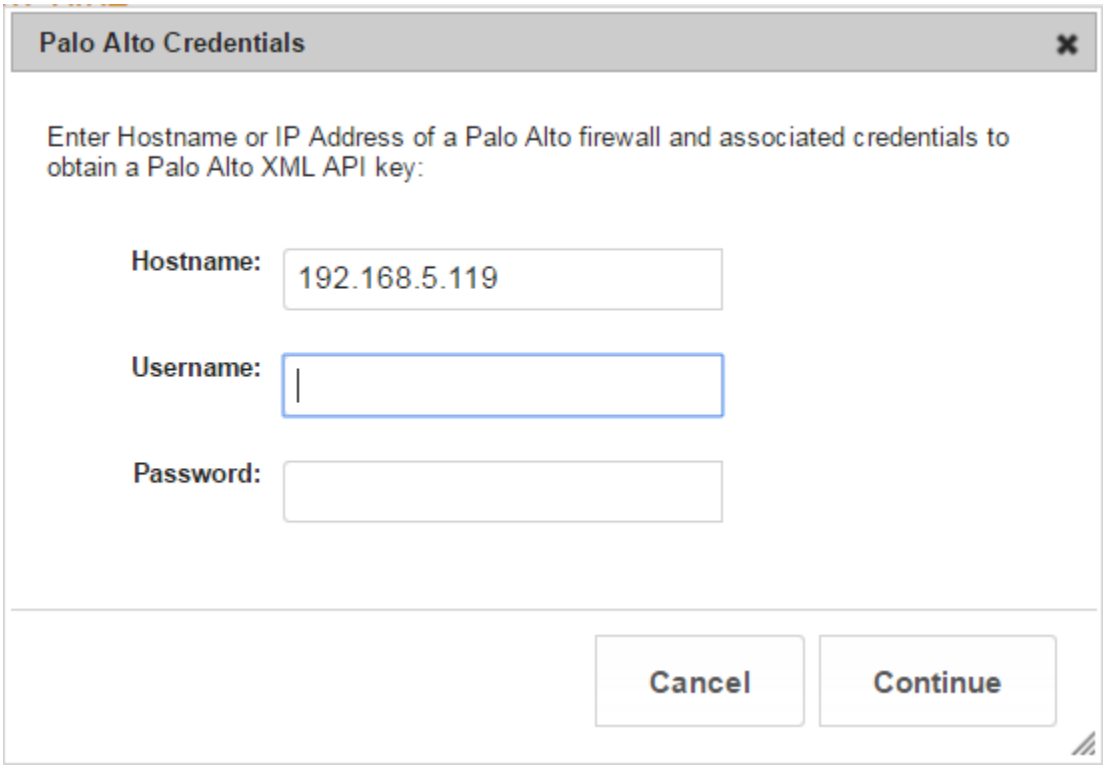
**FIGURE 3** Firewalls & Web Filters




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

4. Click **Get Key**.

**FIGURE 4** Palo Alto Credentials



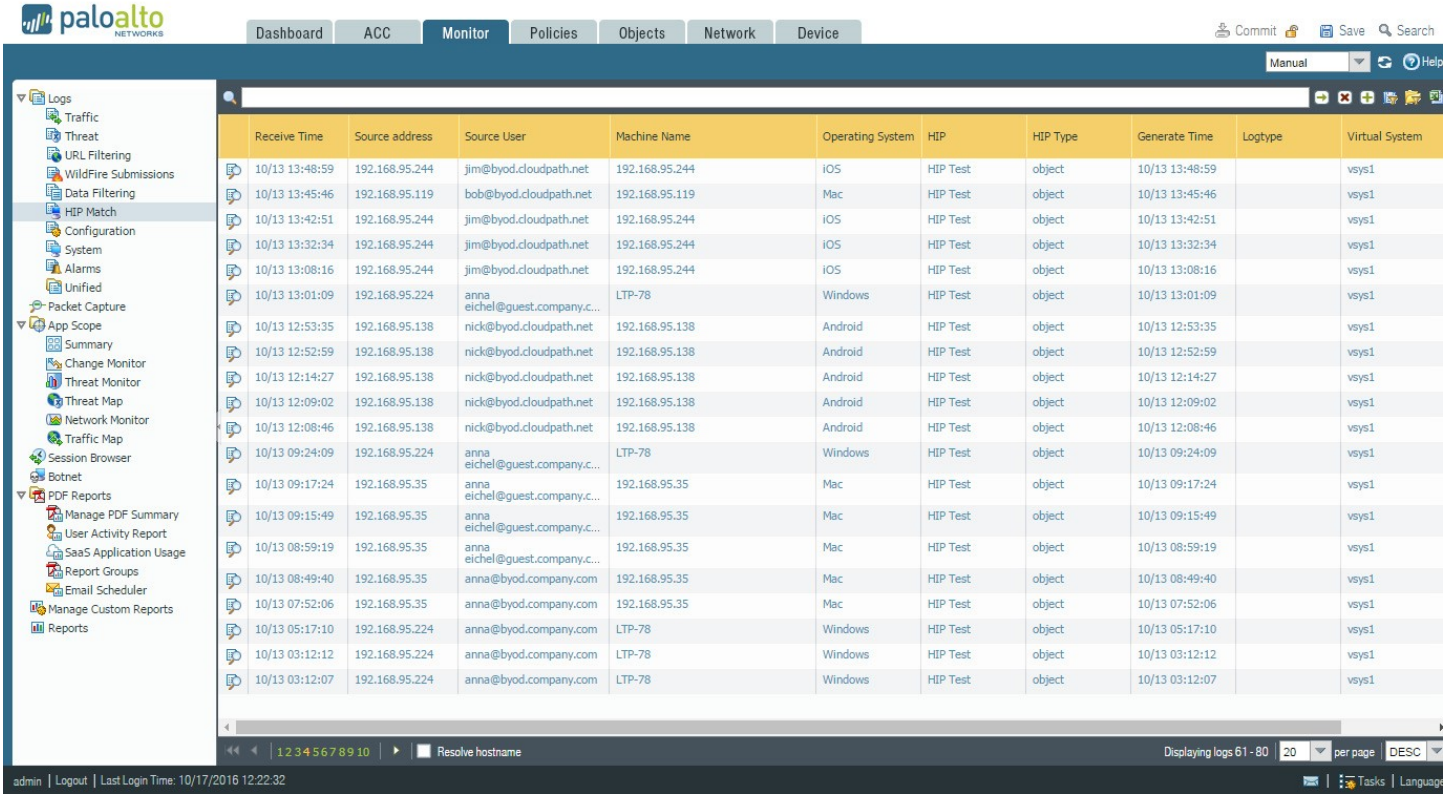

5. In the Palo Alto Credentials popup, enter:
   - Hostname or IP address of the Palo Alto firewall.
   - Palo Alto administrator username.
   - Palo Alto administrator password.

   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




The information displayed is obtained from the Cloudpath Enrollment Record.