CONFIGURATION GUIDE

Cloudpath Enrollment System Integration with Palo Alto Networks® Firewalls Configuration Guide, 6.0

Supporting all Cloudpath Software Releases 6.0

Part Number: 800-73685-001 Rev A
Publication Date: 26 August 2024

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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

New in This Document

TABLE 1 Key Features and Enhancements in this Release of the Product

Feature	Description	Reference
NAS-ID RADIUS attribute	Integrated systems such as Palo Alto Firewalls now support filtering RADIUS Accounting traffic forwarded by the NAS-ID RADIUS attribute.	Configuring Palo Alto Firewall and Web Filters on page 9

Integration with Palo Alto Networks® Firewalls

Cloudpath supplements data already captured by Palo Alto Networks® 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 Networks® 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.

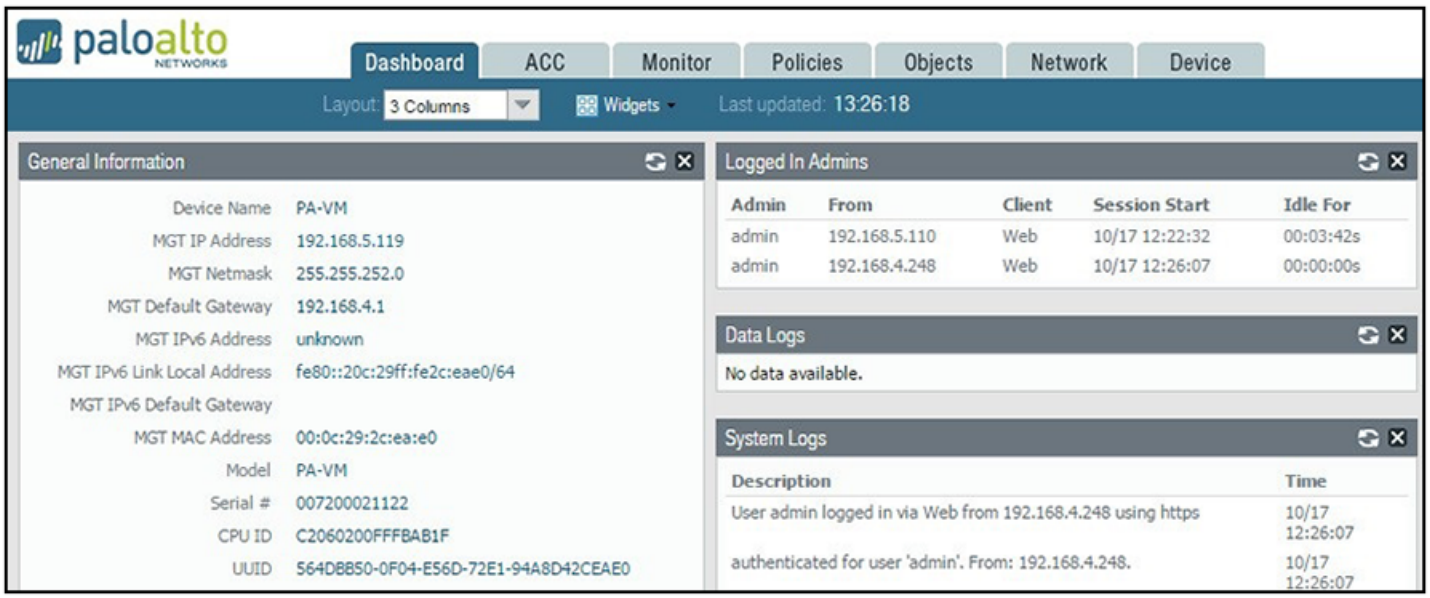
Palo Alto Networks® Firewall Prerequisites

Configuring Cloudpath to integrate with a Palo Alto Networks® firewall requires:

- Administrator credentials for the Palo Alto Networks® system

IP address or hostname of the Palo Alto Networks® system

FIGURE 1 Palo Alto Networks® Firewall System Information



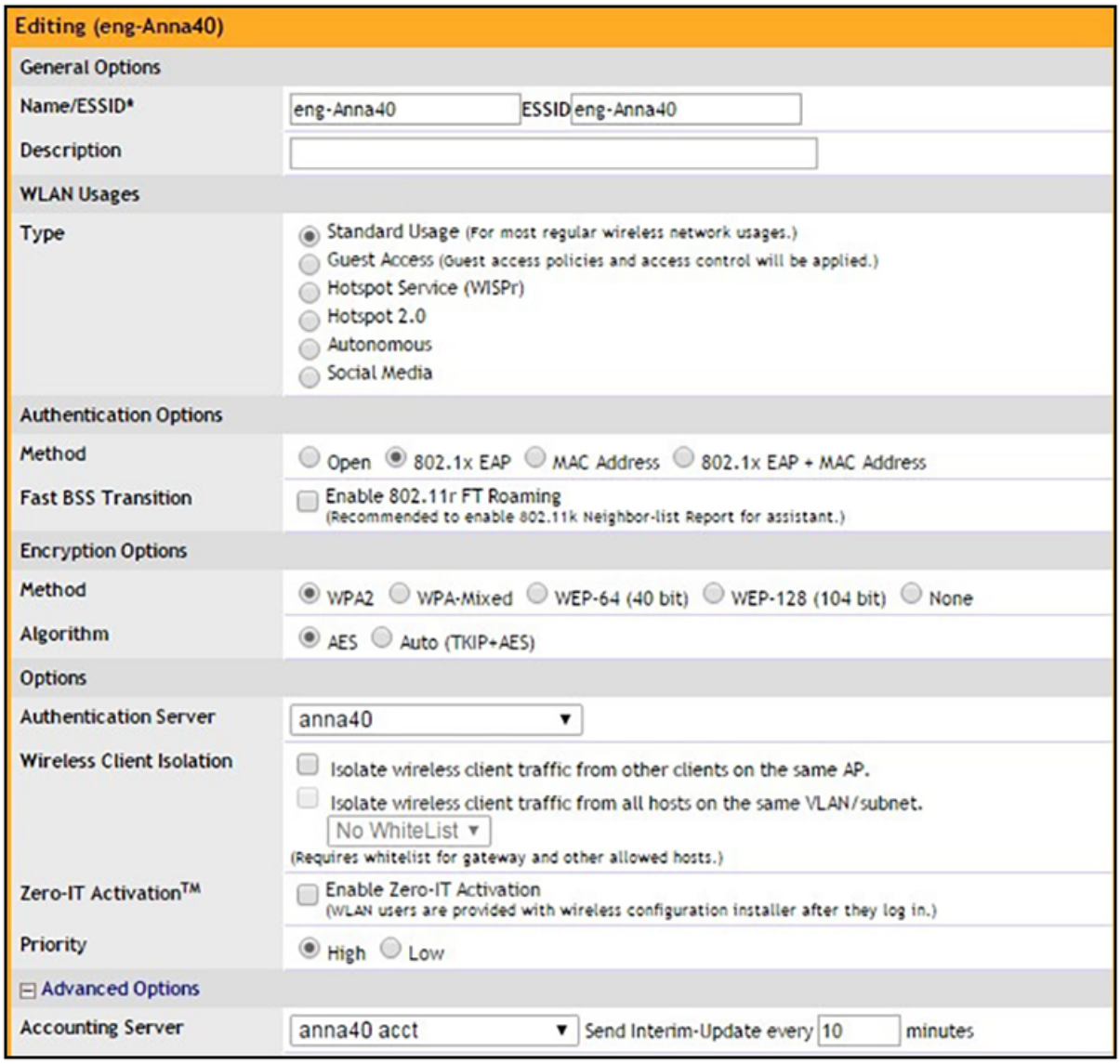
Wireless Controller Configuration

The examples in this section show RUCKUS Wireless controllers. However, Cloudpath supports integration with Palo Alto Networks® 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

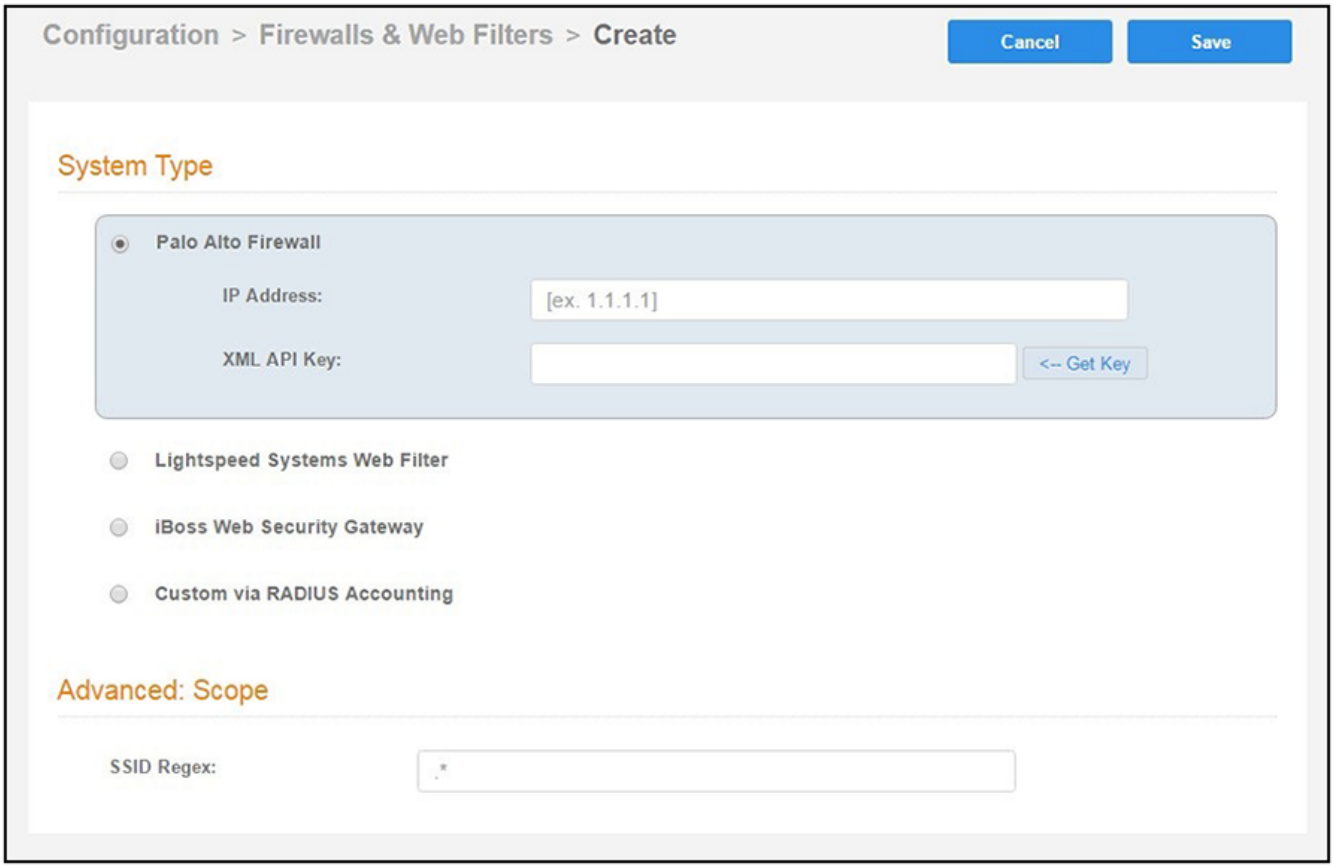


Configuring Palo Alto Firewall and Web Filters

1. Navigate to **Configuration** > **Firewalls & Web Filters**.

2. Select **Palo Alto Firewall**.

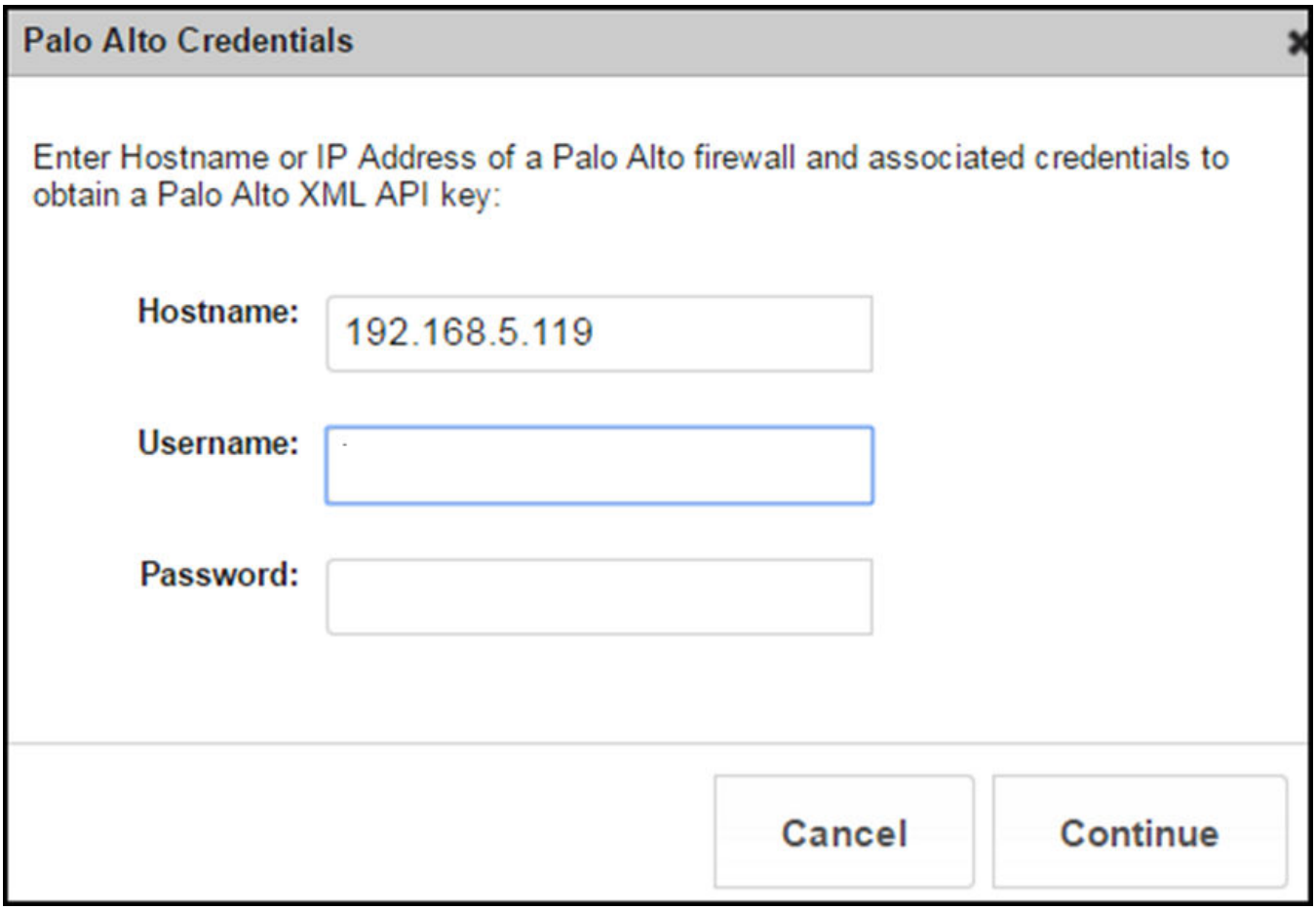
FIGURE 3 Firewalls & Web Filters



3. Enter the management IP address of the Palo Alto Networks® 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 Networks® firewall.
   - Palo Alto Networks® administrator username.
   - Palo Alto Networks® 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. **User ID Mapping Timeout (Minutes)** is optional. You can customize this value to set the maximum time period. The Palo Alto Networks® firewall is requested to consider User ID mapping values sent by Cloudpath for that duration as valid inputs, without additional updates. The default timeout value is 6 hours.
7. **Scope** is optional. If you want only information from a specific SSID to be forwarded to the Palo Alto Networks® firewall (or other specified web filters), enter it in the **SSID Regex** field. In the **NAS-ID Regex** field, enter a regular expression to specify the NAS Identifier(s) that will trigger RADIUS Accounting data forwarding to this external system. Data will only be forwarded if all specified NAS Identifiers match the connected network.

Support for NAS-ID in Palo Alto Firewall Configuration

Network Access Server Identifier (NAS-ID) is a unique identifier for a network access server (an AP or controller). For Palo Alto Network (PAN), NAS-ID is configured in the advanced scope that allows for granular control over policy application.

Feature Overview

Cloudpath 6.0 introduces NAS-ID filtering for RADIUS accounting integrations, for Palo Alto Firewalls. This feature allows you to precisely control which RADIUS accounting data is forwarded to a specific Palo Alto by defining the NAS-ID criteria. Use the new **NAS-ID Regex** option to specify a regular expression that matches the NAS-ID attribute in the incoming RADIUS accounting requests. For data forwarding to occur, both the SSID and NAS-ID scopes must be met. Only a single host information profile (HIP) match update is sent to Palo Alto upon device connection when both filters are satisfied. No intermediate or stop accounting updates are transmitted. If either or both filters fail to match, no update is sent to Palo Alto, and corresponding log messages are generated in Cloudpath.

Requirements

This feature has no special hardware or software requirements for feature enablement or usage.

Considerations

This feature has no special considerations or limitations pertaining to feature enablement or usage.

Best Practices

This feature has no special recommendations for feature enablement or usage.

Prerequisites

This feature has no prerequisites to feature enablement or usage.

Configuring Advanced Scope for Firewall for Palo Alto

For the Firewall for Palo Alto, you can configure advanced scope matching based on service set identifier (SSID) and network access server identifier (NAS-ID) filters.

Complete the following steps to configure the service set identifier (SSID) and network access server identifier (NAS-ID) filter for the Palo Alto Firewall configuration.

1. From the Cloudpath Enrollment System navigation bar, navigate to **Configuration** > **Integrated Systems**.

   By default, the **Ruckus Systems** tab is selected.
2. Select the **Firewalls & Web Filters** tab.

   The **Firewalls & Web Filters** page is displayed.
3. Click **Add Firewalls & Web Filters**.
4. Enter the management IP address of the Palo Alto Networks® system.

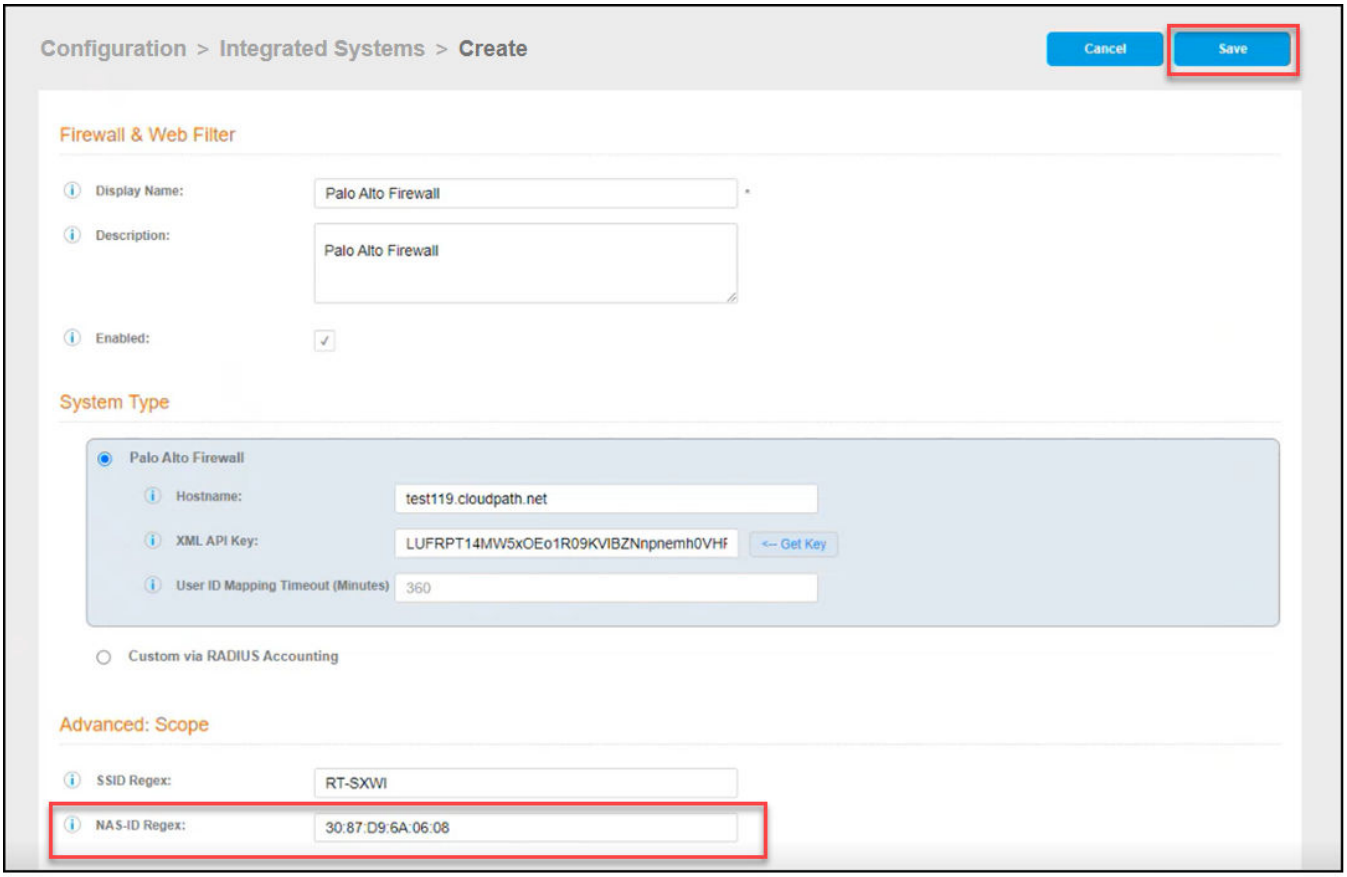
   Hostname or IP Address of Palo Alto Firewall. Port is specified by delimiting with colon, <hostname>:<port>

5. Click **Get Key** to get the key to get the XML key.

   The API Key obtained from Palo Alto Firewall for API-based integration. When you enter your Palo Alto username and password credentials to obtain an API key from a specific Palo Alto, your username and password are not stored.

6. In the **Advanced: Scope** section, add the following filters

FIGURE 5 Adding Advanced Scope: SSID and NAS-ID



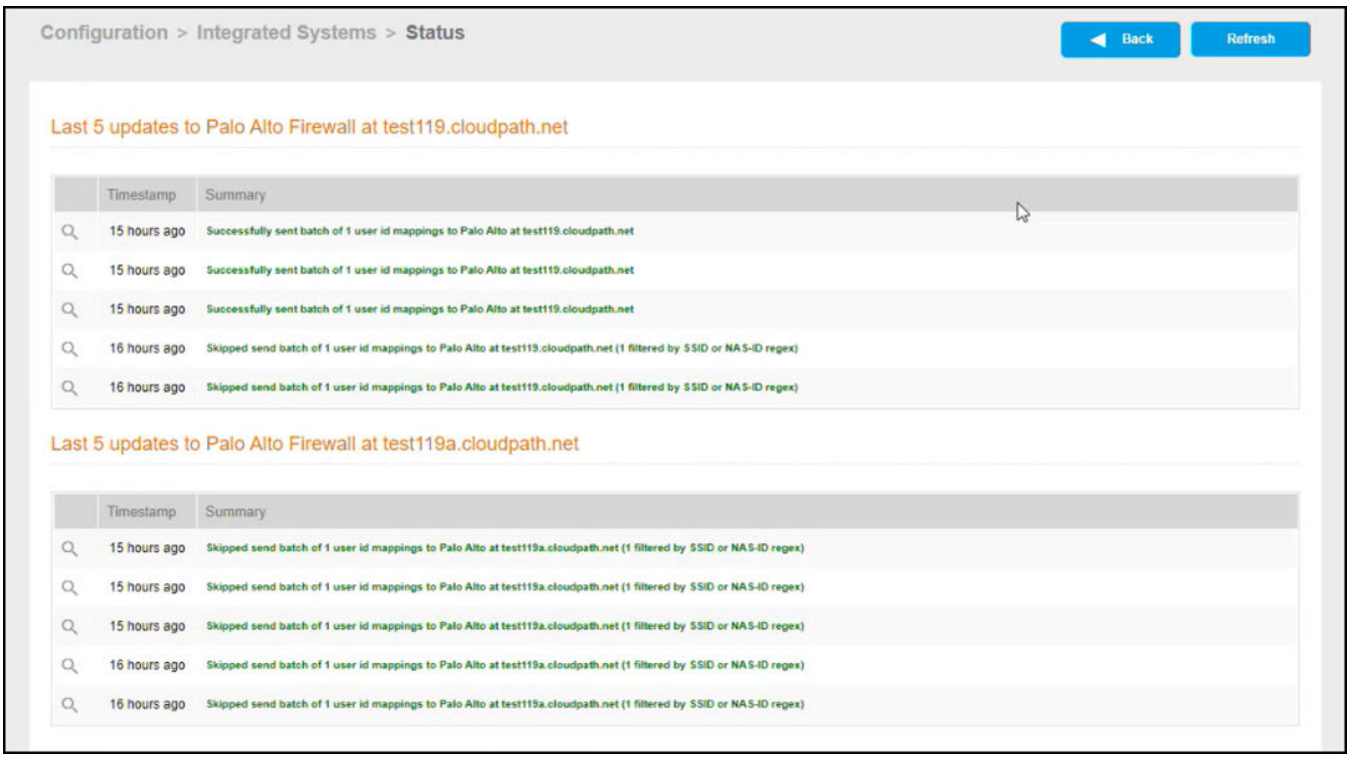
- **SSID Regex**: Enter a regular expression to specify the SSID(s) that will trigger RADIUS accounting data forwarding to this external system. Data will only be forwarded if all specified SSIDs match the connected network.
- **NAS-ID Regex**: Enter a regular expression to specify the NAS Identifier(s) that will trigger RADIUS Accounting data forwarding to this external system. Data will only be forwarded if all specified NAS Identifiers match the connected network..

7. Click **Save**.

8. (Optional) In the **Firewalls & Web Filters** page, click **Status** to view the status of Firewall and web filters.

   The Firewall and web filters status is displayed.

   FIGURE 6 Firewalls & Web Filters Status

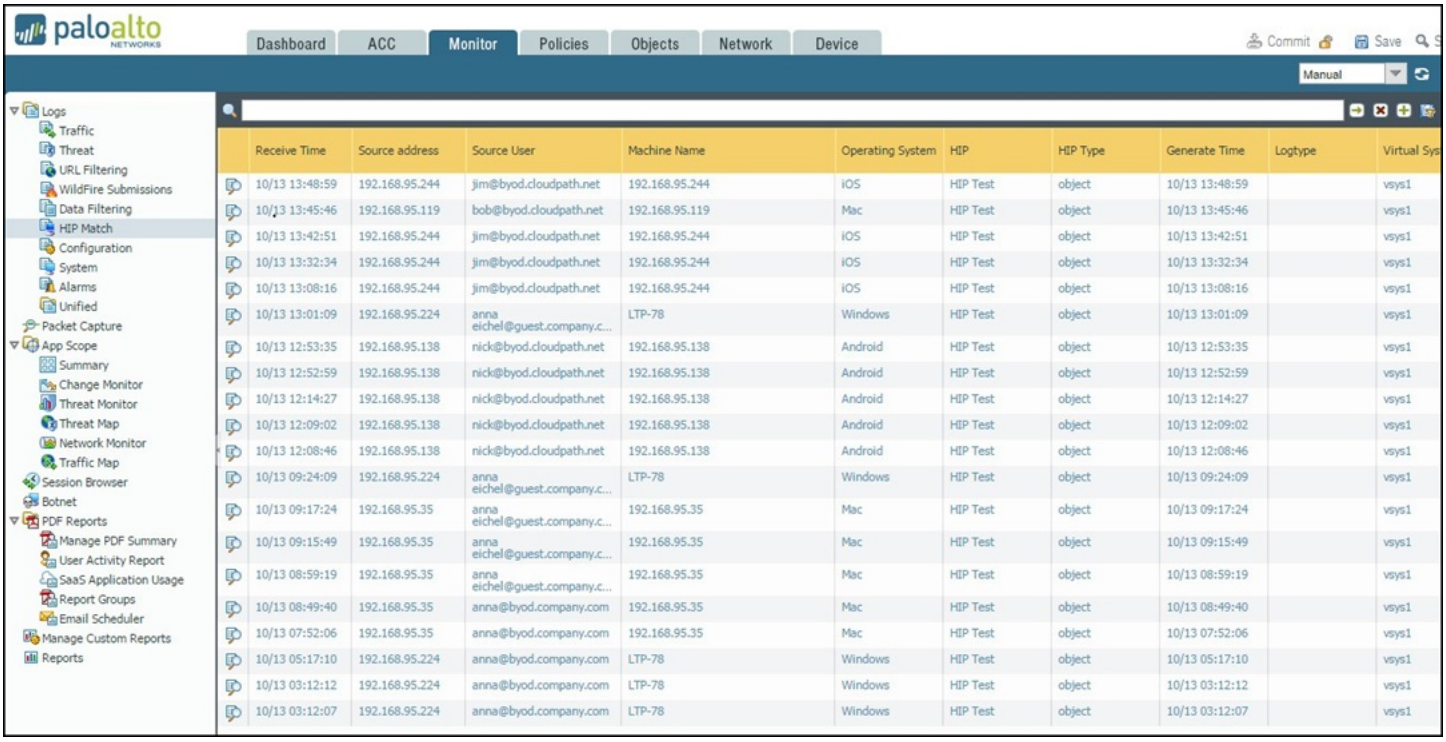


9. (Optional) To review the incoming NAS-ID for RADIUS accounting, go to **Dashboards** > **Connections** .

Palo Alto Networks® Output

The example output below illustrates the data displayed in the Palo Alto Networks® 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 and the **Machine Name** and **Operating System** fields, if known by Cloudpath, display the machine information.

FIGURE 7 Palo Alto Firewall Displaying Cloudpath Traffic



Note that the information displayed is obtained from the Cloudpath Enrollment Record.

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com