

Cloudpath Enrollment System Integration with Palo Alto Firewalls Configuration Guide, 5.4

Supporting Cloudpath Software Release 5.4

Copyright, Trademark and Proprietary Rights Information

© 2019 ARRIS Enterprises LLC. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from ARRIS International plc and/or its affiliates ("ARRIS"). ARRIS reserves the right to revise or change this content from time to time without obligation on the part of ARRIS to provide notification of such revision or change.

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

Contents

Integration with Palo Alto Firewalls.....	4
Palo Alto Firewall Prerequisites.....	4
Wireless Controller Configuration.....	4
Cloudpath Configuration.....	6
Palo Alto Output.....	7

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.

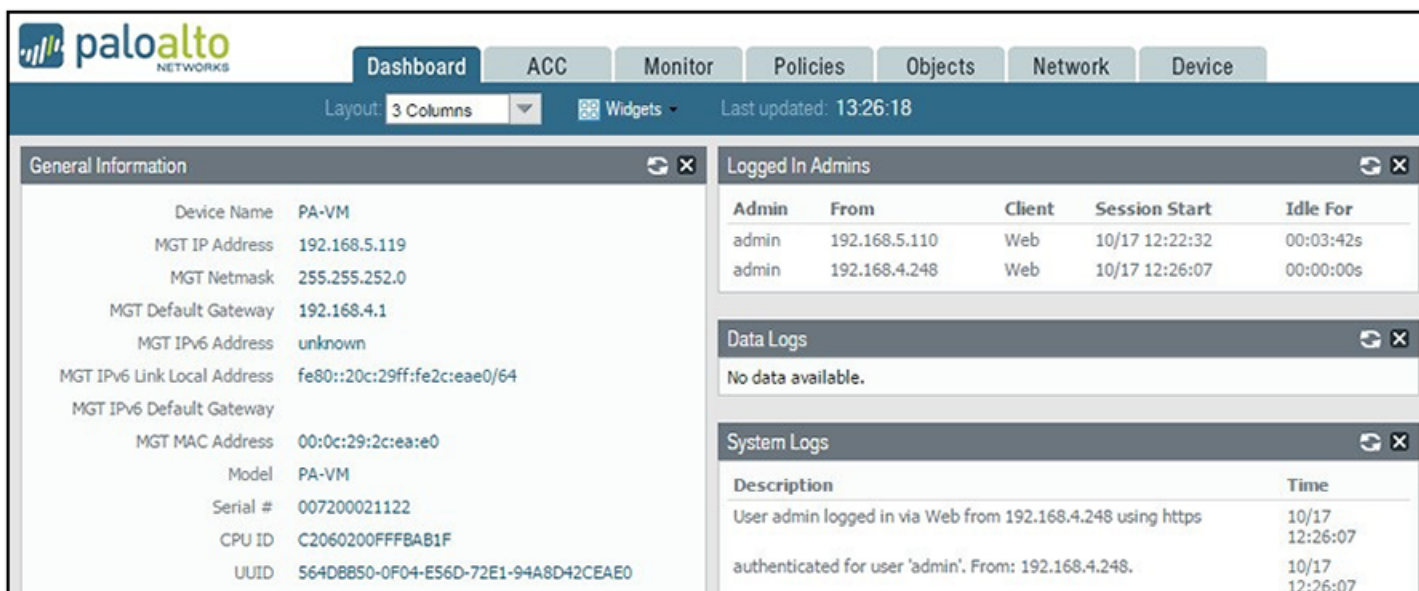
Palo Alto Firewall Prerequisites

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

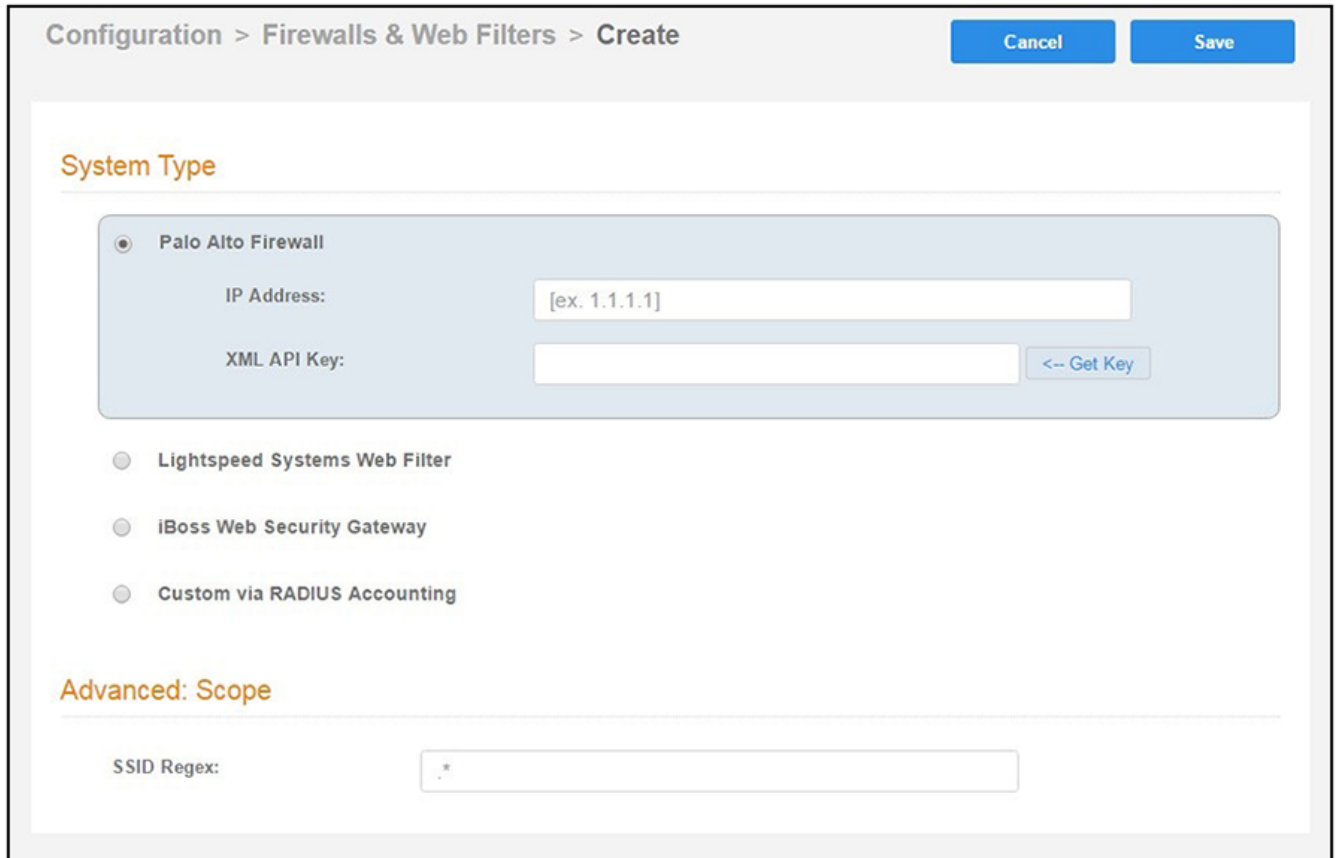
The screenshot shows the configuration page for a WLAN named 'eng-Anna40'. The interface is organized into several sections:

- General Options:** Name/ESSID is 'eng-Anna40', and the ESSID is also 'eng-Anna40'. The Description field is empty.
- WLAN Usages:** The Type is set to 'Standard Usage (For most regular wireless network usages.)'. Other options include Guest Access, Hotspot Service (WISPr), Hotspot 2.0, Autonomous, and Social Media.
- Authentication Options:** The Method is '802.1x EAP'. Other methods include Open, MAC Address, and 802.1x EAP + MAC Address. The 'Fast BSS Transition' checkbox for 'Enable 802.11r FT Roaming' is unchecked.
- Encryption Options:** The Method is 'WPA2' and the Algorithm is 'AES'. Other encryption methods include WPA-Mixed, WEP-64 (40 bit), WEP-128 (104 bit), and None.
- Options:** The Authentication Server is set to 'anna40'. Under 'Wireless Client Isolation', both checkboxes for isolating traffic are unchecked, and the 'No WhiteList' dropdown is selected. The 'Zero-IT Activation™' checkbox is also unchecked. The Priority is set to 'High'.
- Advanced Options:** The Accounting Server is 'anna40 acct' and the 'Send Interim-Update' interval is set to 10 minutes.

Cloudpath Configuration

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

FIGURE 3 Firewalls & Web Filters



The screenshot shows a web interface for configuring firewalls. The breadcrumb navigation at the top reads "Configuration > Firewalls & Web Filters > Create". There are "Cancel" and "Save" buttons in the top right corner. The main section is titled "System Type" and contains four radio button options: "Palo Alto Firewall" (which is selected), "Lightspeed Systems Web Filter", "iBoss Web Security Gateway", and "Custom via RADIUS Accounting". Under the "Palo Alto Firewall" option, there are two input fields: "IP Address:" with a placeholder "[ex. 1.1.1.1]" and "XML API Key:" with a "Get Key" button. Below this section is another section titled "Advanced: Scope" with an "SSID Regex:" input field containing the text ".*".

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

4. Click **Get Key**.

FIGURE 4 Palo Alto Credentials

Palo Alto Credentials [X]

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

Hostname:

Username:

Password:

Cancel Continue

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.



© 2019 ARRIS Enterprises LLC. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com