

Cloudpath

Enrollment System

Configuring Ruckus Wireless LAN Controllers to Integrate With Cloudpath

Software Release 5.1

April 2017

Summary: This document describes the system requirements and configuration details for integrating Ruckus SmartZone and Zone Director controllers with Cloudpath.

Document Type: Configuration

Audience: Network Administrator



Configuring Ruckus Wireless LAN Controllers to Integrate With Cloudpath

Software Release 5.1

April 2017

Copyright © 2017 Ruckus Wireless, Inc. All Rights Reserved.

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

ZoneFlex™, BeamFlex™, MediaFlex™, ChannelFly™, and the Ruckus Wireless logo are trademarks of Ruckus Wireless, Inc. All other brands and product names are trademarks of their respective holders.

Copyright © 2017 Ruckus Wireless, Inc. All rights reserved.

Configuring Ruckus Wireless LAN Controllers to Integrate With Cloudpath

Configuring the Ruckus Wireless Controllers

This document describes how to configure the Ruckus Zone Director and SmartZone controllers to integrate with the Cloudpath system, and includes the following steps:

- Set up Cloudpath as an AAA Authentication Server
- Create AAA Accounting Server (Optional)
- Create Hotspot Services
- Set Up the Walled Garden
- Create the Onboarding SSID
- Create the Secure SSID

Set up Cloudpath as an AAA Authentication Server

Create AAA authentication and accounting servers for the Cloudpath onboard RADIUS server. The following images show this configuration on the Ruckus Zone Director and SmartZone controllers.

FIGURE 1. Create AAA Authentication Server on Zone Director

The screenshot shows the 'Editing (R-AOnboard)' configuration window. The fields are as follows:

Name	R-AOnboard
Type	<input type="radio"/> Active Directory <input type="radio"/> LDAP <input checked="" type="radio"/> RADIUS <input type="radio"/> RADIUS Accounting <input type="radio"/> TACACS+
Auth Method	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP
Backup RADIUS	<input type="checkbox"/> Enable Backup RADIUS support
IP Address*	192.168.5.73
Port*	1812
Shared Secret*
Confirm Secret*
Retry Policy	
Request Timeout*	3 seconds
Max Number of Retries*	2 times

Buttons: OK, Cancel

FIGURE 2. Create AAA Authentication Server SmartZone

Enter the following values for the **Authentication** Server:

1. Name
2. Type = RADIUS
3. Auth Method = PAP
4. IP address = The IP address of the Cloudpath ES.
5. Port = 1812
6. Shared Secret = This must match the shared secret for the Cloudpath ES onboard RADIUS server. (*Configuration > RADIUS Server*).
7. Leave the default values for the remaining fields.

Create AAA Accounting Server (Optional)

Use the same process to create the AAA Accounting Server.

Enter the following values for the **Accounting** Server:

1. Name
2. Type = RADIUS
3. Auth Method = PAP
4. IP address = The IP address of the Cloudpath ES.
5. Port = 1813

Note >>

The Authentication server uses port 1812. The Accounting server uses port 1813.

6. Shared Secret = This must match the shared secret for the Cloudpath ES onboard RADIUS server. (*Configuration > RADIUS Server*).
7. Leave the default values for the remaining fields.

Run Authentication Test

You can test the connection between the controller and the Cloudpath ES RADIUS server.

At the bottom of the AAA server page, there is a section called Test Authentication/Accounting Servers Settings.

FIGURE 3. Authentication Test Zone Director

Enter a test User Name and Password and click the Test button on the bottom right of the page.

If you run the authentication test on the controller, you can get one of these responses:

- a) Failed! Connection timed out
- b) Failed! Invalid username and password
- c) Authentication Failed

If you receive:

Failed! Invalid username or password

This means that connectivity was established.

On the SmartZone controller, you are prompted to Test Authentication when you save a configuration for an AAA Authentication server.

FIGURE 4. Authentication Test SmartZone

The screenshot shows a dialog box titled "Test AAA Servers". It has three input fields: "Name:" with a dropdown menu showing "Lab AAA Auth", "User Name:" with a text box containing "bob", and "Password:" with a text box containing masked characters "....". Below the password field is a checkbox labeled "Show password". At the bottom right, there are two buttons: "Test" and "Cancel".

Create Hotspot Services

Enter the following values for the **Hotspot Service**:

1. Navigate to Hotspot Services (Hotspot WISPr on SmartZone).
2. Name the Hotspot Service.

FIGURE 5. Create Hotspot Service on Zone Director

The screenshot shows the "Editing (Lab Hotspot Services)" configuration page. The "Name" field is set to "Lab Hotspot Services". Under "Redirection", "WISPr Smart Client Support" is set to "None". The "Login Page*" field contains "Redirect unauthenticated user to https://training.cloudpath.net/enroll/AnnaTest/Production/for authentication." The "Start Page" section has "After user is authenticated," with the radio button "redirect to the URL that the user intends to visit." selected. Under "User Session", "Session Timeout" is set to "1440" minutes and "Grace Period" is set to "30" minutes. In the "Authentication/Accounting Servers" section, "Authentication Server" is "Lab AAA Auth" with "Enable MAC authentication bypass(no redirection)." checked. The radio button "Use device MAC address as authentication password." is selected. The "Accounting Server" is "Lab AAA Acct" with "Send Interim-Update every 5" minutes. Under "Wireless Client Isolation", the checkbox "Isolate wireless client traffic from all hosts on the same VLAN/subnet." is selected, and the "WhiteList" is set to "No WhiteList". At the bottom right, there are "OK" and "Cancel" buttons.

FIGURE 6. Create Hotspot WISPr on SmartZone

3. Point the unauthenticated user to the Cloudpath *Enrollment Portal URL*, which can be found on the Cloudpath Admin UI *Configuration > Workflows* page, in the *Workflows* table.
4. Check *Redirect to the URL that the user intends to visit*.
5. Select the Cloudpath RADIUS Authentication Server (ZoneDirector only).
6. Enable MAC authentication bypass redirection (ZoneDirector only).
7. Select *Use device MAC address as authentication password*.
8. Select the Cloudpath RADIUS Accounting Server (ZoneDirector only).
9. Leave the defaults for the remaining settings. Click OK.

Set Up the Walled Garden

Enter the following values for the Walled Garden:

1. On the *Hotspot Service > Configure* page, scroll to the bottom to the **Walled Garden** section below the Hotspot Service configuration created in the previous section.

FIGURE 7. Walled Garden Configuration for Zone Director

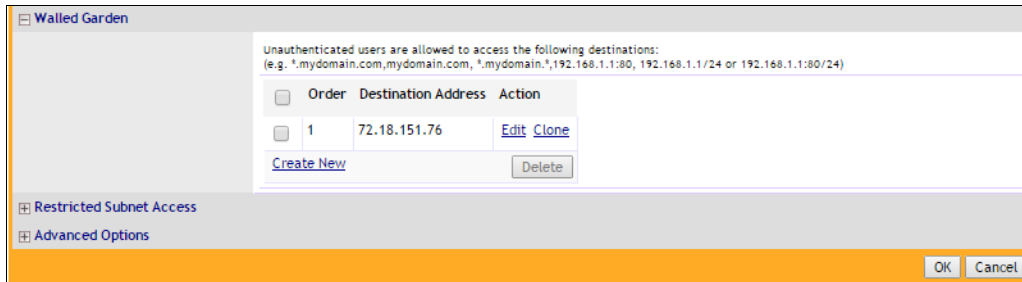
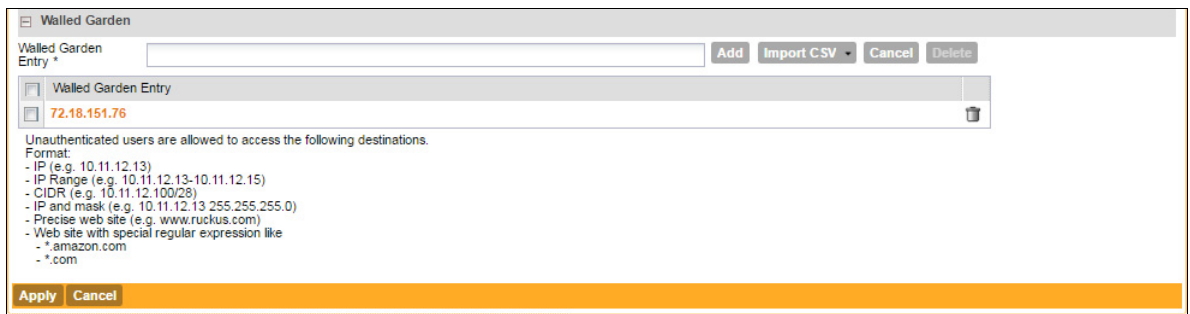


FIGURE 8. Walled Garden Configuration for SmartZone



2. Include the DNS or IP address of the Cloudpath system and **Save** (or **Apply**)

Create the Onboarding SSID

Enter the following values for the onboarding SSID:

1. Name the SSID.
2. Type=Hotspot Service (WISPr).

FIGURE 9. Onboarding SSID Configuration on Zone Director

Editing (Lab Onboard SSID)

General Options

Name/ESSID* ESSID

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

Options

Hotspot Services ▼

Priority High Low

[+ Advanced Options](#)

FIGURE 10. Onboarding SSID Configuration on SmartZone

Lab Onboard SSID

Web NONE Super

Edit WLAN Config: [Lab Onboard SSID] of zone [Cloudpath APs]

General Options

Name: * Lab Onboard SSID

SSID: * Lab Onboard SSID

HESSID:

Description:

WLAN Usage

Access Network: Tunnel WLAN traffic through Ruckus GRE

Authentication Type: * Standard usage (For most regular wireless networks)

Hotspot (WISPr)

Guest Access + Hotspot 2.0 Onboarding

Web Authentication

Hotspot 2.0 Access

Hotspot 2.0 Secure Onboarding (OSEN)

WeChat

Authentication Options

Method: * Open 802.1x EAP MAC Address

Encryption Options

Method: * WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None

Hotspot Portal

Hotspot (WISPr) Portal: * Lab Hotspot Services

Bypass CNA: Enable

Authentication Service: * Use the controller as proxy Lab AAA Auth

Accounting Service: Use the controller as proxy Lab AAA Acct Send interim update every 10 Minutes (0-1440)

Options

Acct Delay Time: Enable

Wireless Client Isolation: * Disable

Enable (Isolate wireless client traffic from all hosts on the same VLAN/subnet)

Priority: * High Low

RADIUS Options

Advanced Options

Apply Cancel

3. Authentication Option Method=Open.
4. Encryption Option Method=None.
5. Select the Hotspot Service created in Task 2.
6. Enable Bypass CNA.
 - For ZoneDirector, this setting is at the bottom of the screen in the Bypass Apple CNA Feature section. Check the Hotspot service box.
 - For SmartZone, this setting is in the Hotspot Portal Section.
7. Select the Cloudpath RADIUS Authentication Server (SmartZone only).
8. Select the Cloudpath RADIUS Accounting Server (SmartZone only).
9. Leave the defaults for the remaining settings and click OK (or Apply).

Create the Secure SSID

Enter the following values for the secure SSID:

1. Name the SSID.
2. Type=Standard Usage.
3. Authentication Option Method=802.1x EAP.
4. Encryption Option Method=WPA2
5. Encryption Option Algorithm=AES
6. Select the Cloudpath RADIUS Authentication Server.
7. Select the Cloudpath RADIUS Accounting Server (SmartZone only).
8. Leave the defaults for the remaining settings and click OK (or Apply).

FIGURE 11. Configure Secure SSID on the ZoneDirector controller.

Create New

General Options

Name/ESSID* ESSID

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

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

▼

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.

▼ (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

OK Cancel

FIGURE 12. Configure Secure SSID on the SmartZone controller.

Create New WLAN Configuration

General Options

Name: * Lab Secure SSID
 SSID: * Lab Secure SSID
 HESSID:
 Description:

WLAN Usage

Access Network: Tunnel WLAN traffic through Ruckus GRE
 Authentication Type: * Standard usage (For most regular wireless networks)
 Hotspot (WISPr)
 Guest Access + Hotspot 2.0 Onboarding
 Web Authentication
 Hotspot 2.0 Access
 Hotspot 2.0 Secure Onboarding (OSEN)
 WeChat

Authentication Options

Method: * Open 802.1x EAP MAC Address

Encryption Options

Method: * WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None
 Algorithm: * AES ALTO (TKIP+AES)
 802.11w MFP: * Disabled Capable Required

Authentication & Accounting Server

Authentication Server: * Use the Controller as Proxy Lab AAA Auth
 Accounting Server: Use the Controller as Proxy Lab AAA Acct. Send interim update every 5 Minutes (0-1440)

Options

Acct Delay Time: Enable
 Wireless Client Isolation: * Disable
 Enable (Isolate wireless client traffic from all hosts on the same VLAN/subnet)
 Priority: * High Low
 Zero-IT Activation: Enable Zero-IT Activation (WLAN users are provided with a wireless configuration installer after they log on)

RADIUS Options

Advanced Options

OK Cancel

The SSIDs are now configured on the wireless LAN controller. When the user connects to the onboarding (open) SSID they are redirected to the Cloudpath web page. When the user successfully completes the enrollment process, they are migrated to the secure SSID.

Select AAA Accounting Server for the WLAN on Zone Director Controller

To use Cloudpath onboard RADIUS Accounting and Connection Tracking, the AAA Accounting server must be selected for the WLAN.

Note >>

RADIUS Accounting and Connection tracking status can be viewed on the Cloudpath system, *Configuration > RADIUS Server*.

Select RADIUS Accounting server for the WLAN on Zone Director

Editing (eng-Anna40)

General Options

Name/ESSID* ESSID

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

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.

(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 Send Interim-Update every minutes

Accounting Server

-
-
-

1. Scroll down to the Advanced Options section for the Secure SSID configured for Cloudpath.
2. Expand Advanced Options.
3. Select the AAA accounting server previously configured for Cloudpath.
4. Leave the defaults for the remaining settings and click OK (or Apply).

Select AAA Accounting Server for the WLAN on SmartZone Controller

The AAA accounting server was selected during the Secure SSID configuration. No further action is required. See Figure 10 on page 8.