TECHNICAL DOCUMENTATION

Cloudpath

Enrollment System

Configuring Cloudpath to Integrate With a Ruckus Wireless LAN Controller

Software Release 5.0

December 2016

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 Cloudpath ES to Redirect Through a Ruckus Wireless LAN Controller

Software Release 5.0

December 2016

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.

Configuring Cloudpath to Integrate With a Ruckus Wireless LAN Controller

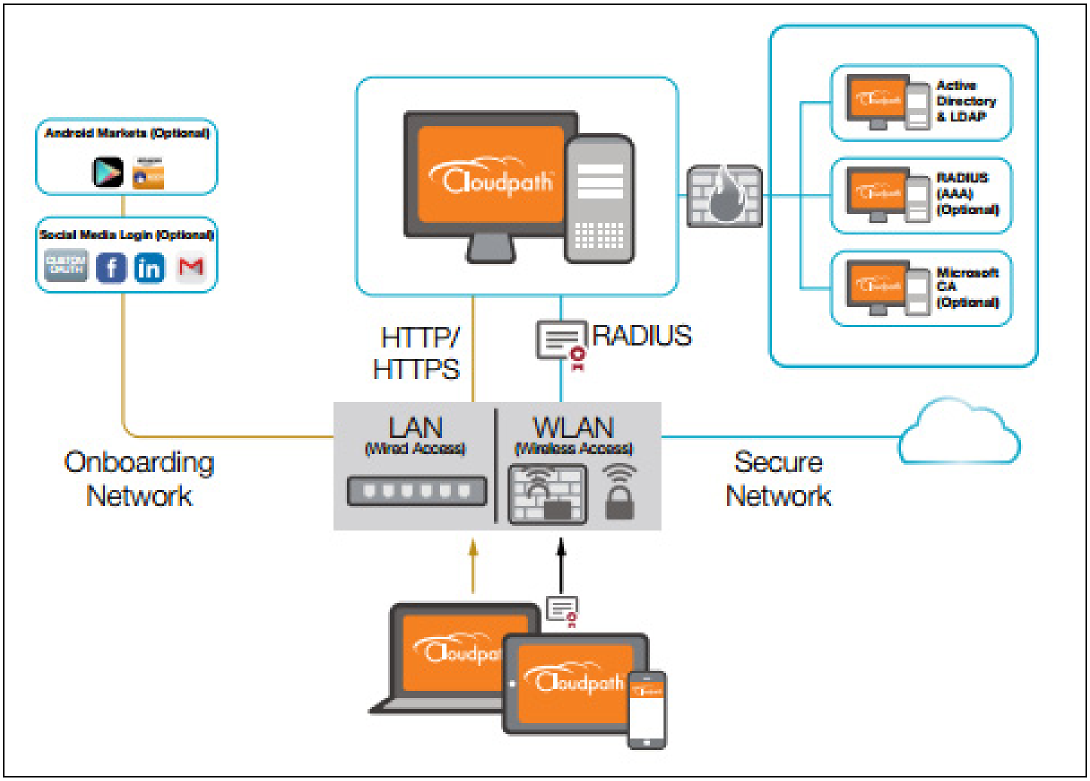
Cloudpath Security and Management Platform Overview

Cloudpath Enrollment System (ES) software is a security and policy management platform that enables any IT organization to protect the network by easily and definitively securing users and their wired and wireless devices—while freeing those users and IT itself from the tyranny of passwords.

Available cloud-managed or as a virtual instance and priced per user, Cloudpath software lets IT do with one system what usually requires many, while easily and automatically integrating with existing access and network security infrastructure.

Cloudpath software consolidates and simplifies the deployment of multiple services that are typically disparate and complex to manage: Certificate Management, Policy Management and Device Enablement.

FIGURE 1. Cloudpath Security and Policy Management Platform



Configuring the Ruckus Wireless Controllers

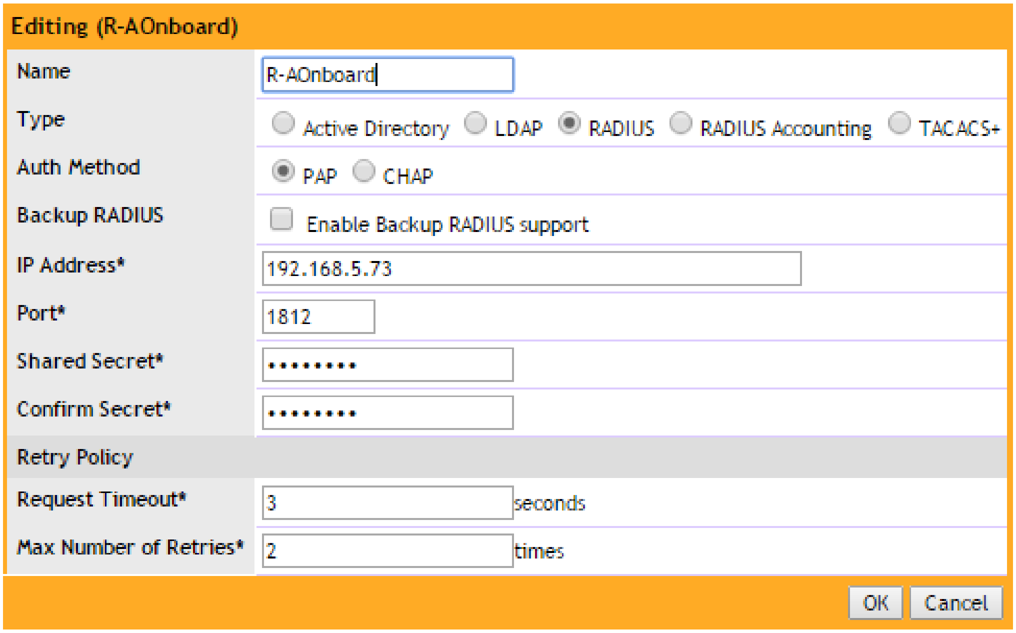
This document describes how to configure the Ruckus Zone Director and SmartZone controllers to integrate with the Cloudpath system, and includes the following steps:

- Set up the Cloudpath ES 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 the Cloudpath ES as an AAA Authentication Server

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

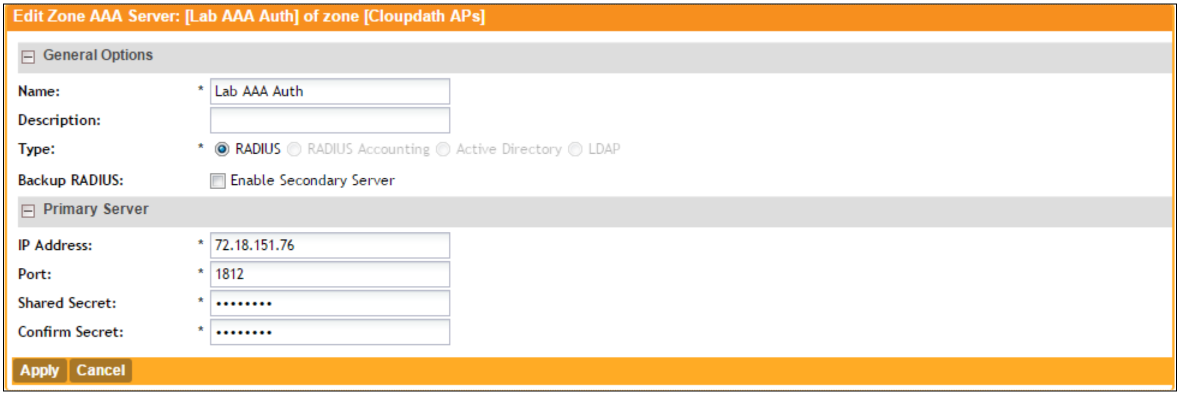
FIGURE 2. Create AAA Authentication Server on Zone Director



Editing (R-AOnboard)

Name	R-AOnboard
Type	○ Active Directory ○ LDAP ● RADIUS ○ RADIUS Accounting ○ TACACS+
Auth Method	● PAP ○ CHAP
Backup RADIUS	□ 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

FIGURE 3. Create AAA Authentication Server SmartZone



Edit Zone AAA Server: [Lab AAA Auth] of zone [Cloudpath APs]

⊟ General Options

Name: * Lab AAA Auth

Description:

Type: * ● RADIUS ○ RADIUS Accounting ○ Active Directory ○ LDAP

Backup RADIUS: □ Enable Secondary Server

⊟ Primary Server

IP Address: * 72.18.151.76

Port: * 1812

Shared Secret: * ••••••••

Confirm Secret: * ••••••••

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 > Advanced > 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.

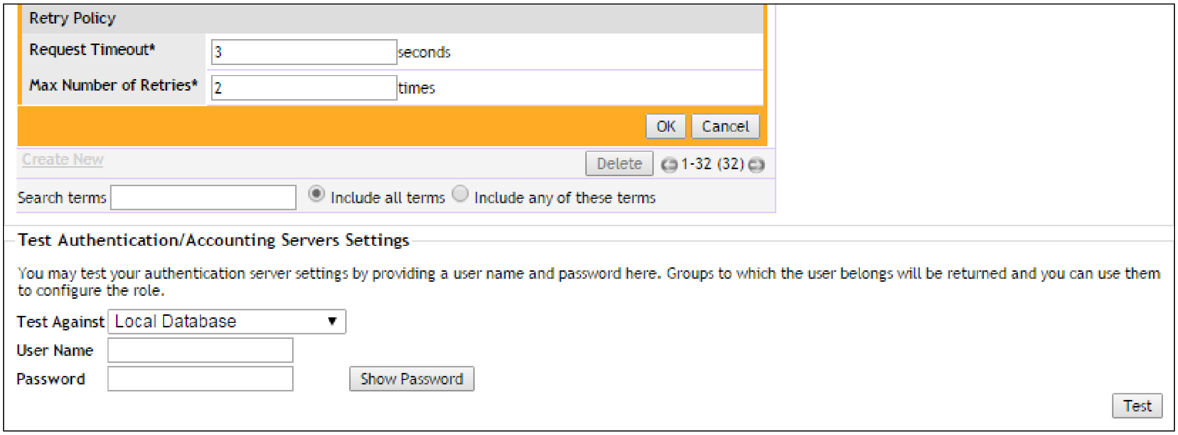
6. Shared Secret = This must match the shared secret for the Cloudpath ES onboard RADIUS server. (*Configuration > Advanced > RADIUS Server*).
7. Leave the default values for the remaining fields.

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 4. Authentication Test Zone Director



Retry Policy

Request Timeout* 3 seconds

Max Number of Retries* 2 times

Search terms ● Include all terms ○ Include any of these terms

Test Authentication/Accounting Servers Settings

You may test your authentication server settings by providing a user name and password here. Groups to which the user belongs will be returned and you can use them to configure the role.

Test Against: Local Database

User Name

Password

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

If you receive:

Failed! Invalid username or password

This means that connectivity was established.

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

a) Failed! Connection timed out

b) Failed! Invalid username and password

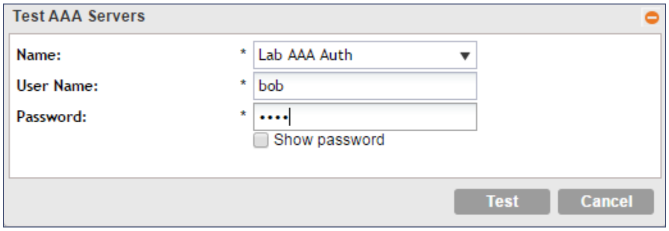
c) Authentication Failed

this one means that connectivity was established

Failed! Invalid username and password

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

FIGURE 5. Authentication Test SmartZone



Test AAA Servers

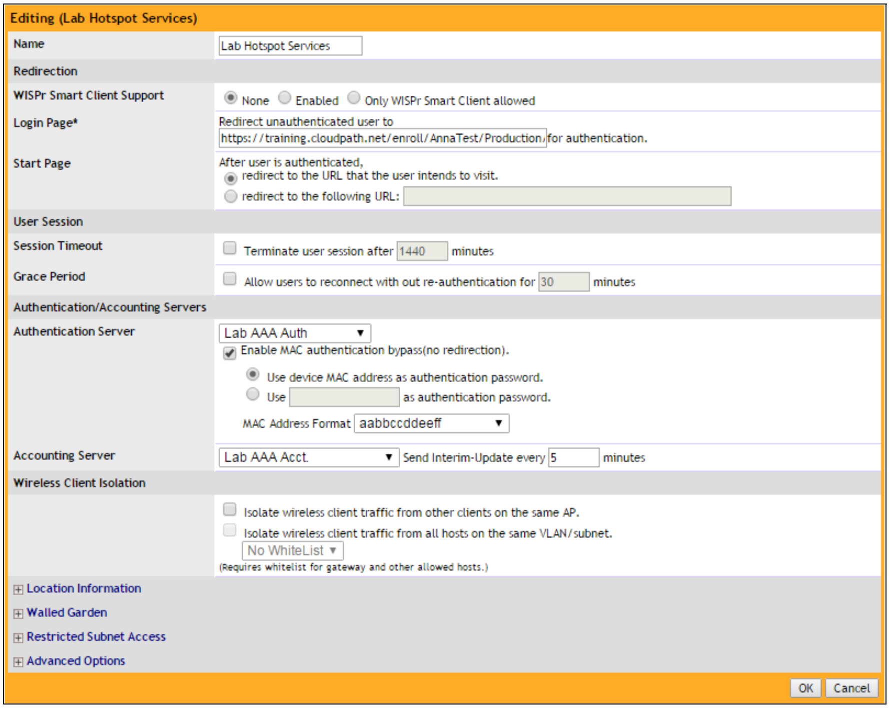
Name:	* Lab AAA Auth ▼
User Name:	* bob
Password:	* ••••
	□ Show password

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.

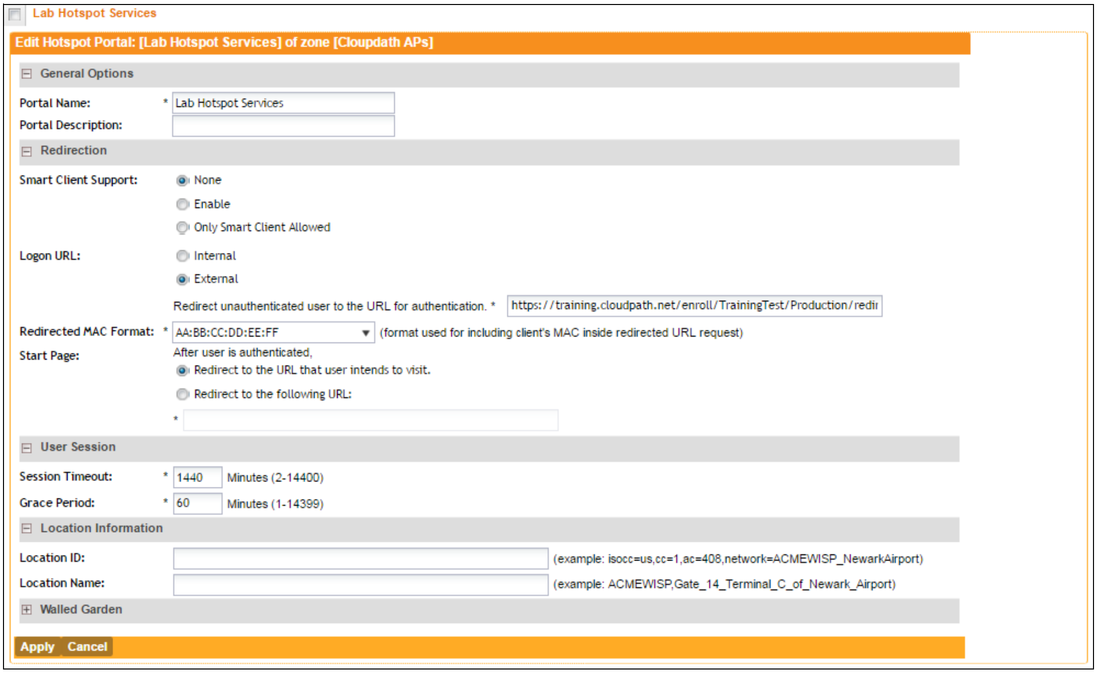
FIGURE 6. Create Hotspot Service on Zone Director



Editing (Lab Hotspot Services)

Name	Lab Hotspot Services
Redirection	
WISPr Smart Client Support	● None ○ Enabled ○ Only WISPr Smart Client allowed
Login Page*	Redirect unauthenticated user to https://training.cloudpath.net/enroll/AnnaTest/Production/ for authentication.
Start Page	After user is authenticated, ● redirect to the URL that the user intends to visit. ○ redirect to the following URL:
User Session	
Session Timeout	□ Terminate user session after 1440 minutes
Grace Period	□ Allow users to reconnect with out re-authentication for 30 minutes
Authentication/Accounting Servers	
Authentication Server	Lab AAA Auth ▼ ☑ Enable MAC authentication bypass(no redirection). ● Use device MAC address as authentication password. ○ Use as authentication password. MAC Address Format aabbccddeeff ▼
Accounting Server	Lab AAA Acct. ▼ Send Interim-Update every 5 minutes
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.)

FIGURE 7. Create Hotspot WISPr on SmartZone



□ Lab Hotspot Services

Edit Hotspot Portal: [Lab Hotspot Services] of zone [Cloupdath APs]

⊟ General Options

Portal Name: * Lab Hotspot Services

Portal Description:

⊟ Redirection

Smart Client Support: ● None ○ Enable ○ Only Smart Client Allowed

Logon URL: ○ Internal ● External

Redirect unauthenticated user to the URL for authentication. * https://training.cloudpath.net/enroll/TrainingTest/Production/redir

Redirected MAC Format: * AA:BB:CC:DD:EE:FF (format used for including client's MAC inside redirected URL request)

Start Page: After user is authenticated,
● Redirect to the URL that user intends to visit.
○ Redirect to the following URL:
*

⊟ User Session

Session Timeout: * 1440 Minutes (2-14400)

Grace Period: * 60 Minutes (1-14399)

⊟ Location Information

Location ID: (example: isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport)

Location Name: (example: ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport)

⊞ Walled Garden

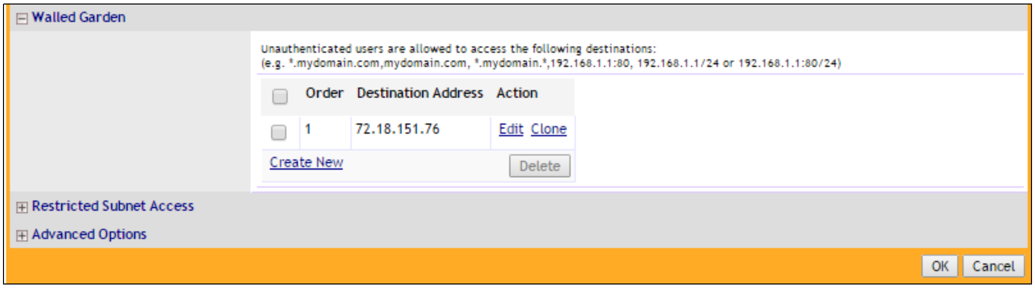
3. Point the unauthenticated user to the Cloudpath redirect URL. Enter the WLAN Redirect URL, which can be found on the Cloudpath Admin UI Configure > Deploy page.
4. Check Redirect to the URL that the user intends to visit.
5. Select the Cloudpath RADIUS Authentication Server (ZoneDirector only).
6. 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 8. Walled Garden Configuration for Zone Director

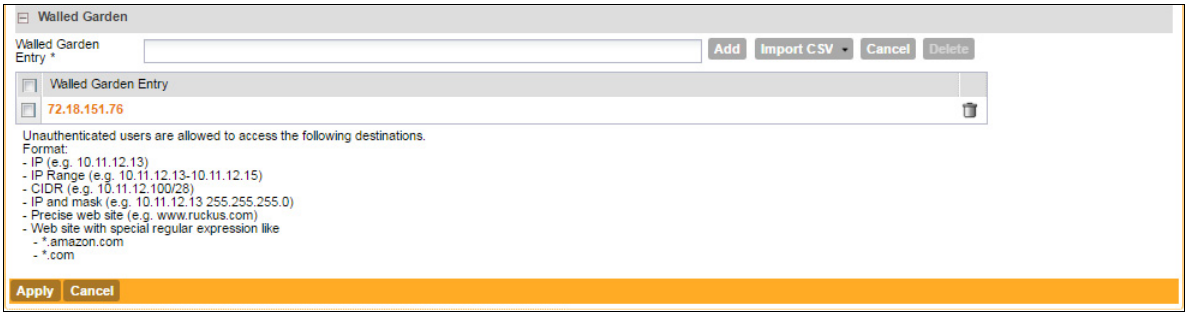


⊟ Walled Garden

Unauthenticated users are allowed to access the following destinations:
(e.g. *.mydomain.com,mydomain.com, *.mydomain.*,192.168.1.1:80, 192.168.1.1/24 or 192.168.1.1:80/24)

□	Order	Destination Address	Action
□	1	72.18.151.76	Edit Clone

FIGURE 9. Walled Garden Configuration for SmartZone



⊟ Walled Garden

□	Walled Garden Entry
□	72.18.151.76

Unauthenticated users are allowed to access the following destinations.
Format:
- IP (e.g. 10.11.12.13)
- IP Range (e.g. 10.11.12.13-10.11.12.15)
- CIDR (e.g. 10.11.12.100/28)
- IP and mask (e.g. 10.11.12.13 255.255.255.0)
- Precise web site (e.g. www.ruckus.com)
- Web site with special regular expression like
  - *.amazon.com
  - *.com

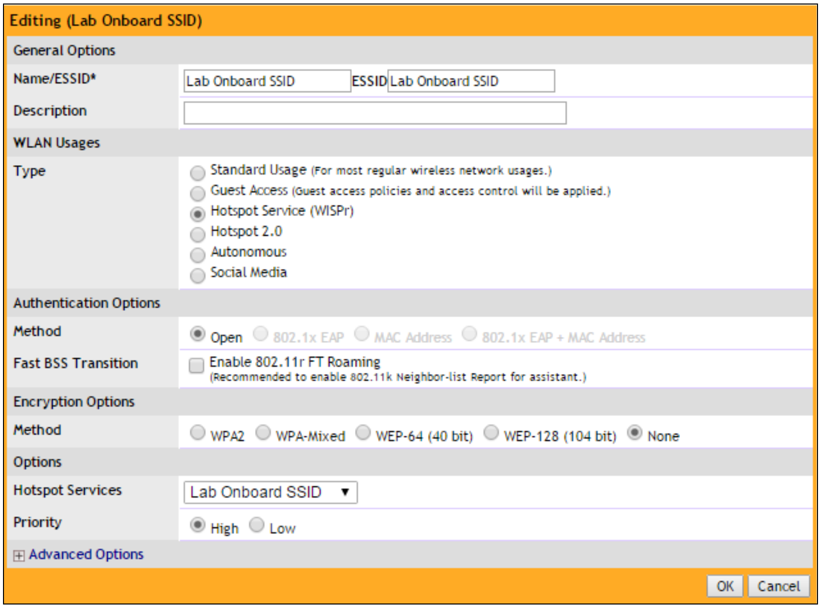
2. Include the DNS or IP address of the Cloudpath system and **Save** (or Apply)

Create the Onboarding SSID

Enter the following values for the onboarding SSID:

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

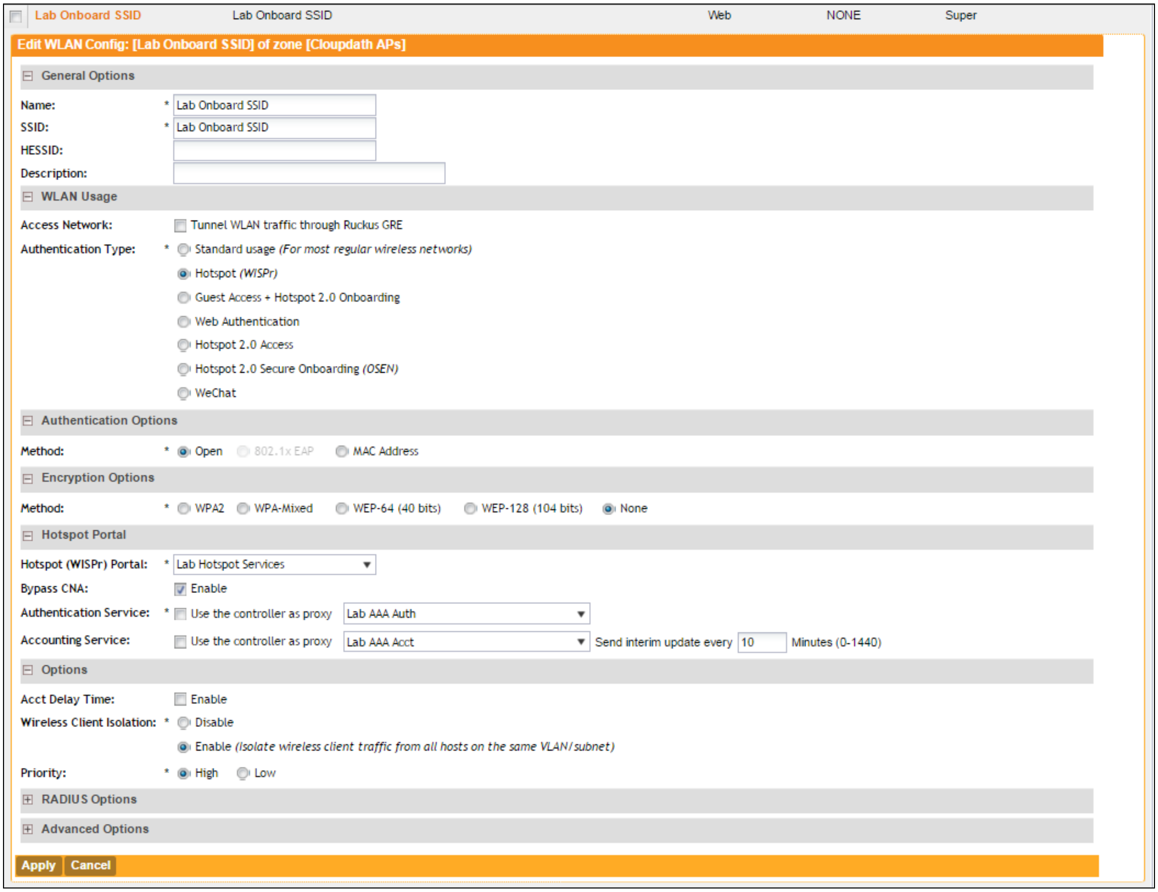
FIGURE 10. Onboarding SSID Configuration on Zone Director



Editing (Lab Onboard SSID)

General Options	
Name/ESSID*	Lab Onboard SSID ESSID Lab Onboard SSID
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	Lab Onboard SSID ▼
Priority	● High ○ Low
⊞ Advanced Options	

FIGURE 11. Onboarding SSID Configuration on SmartZone



□ Lab Onboard SSID | 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

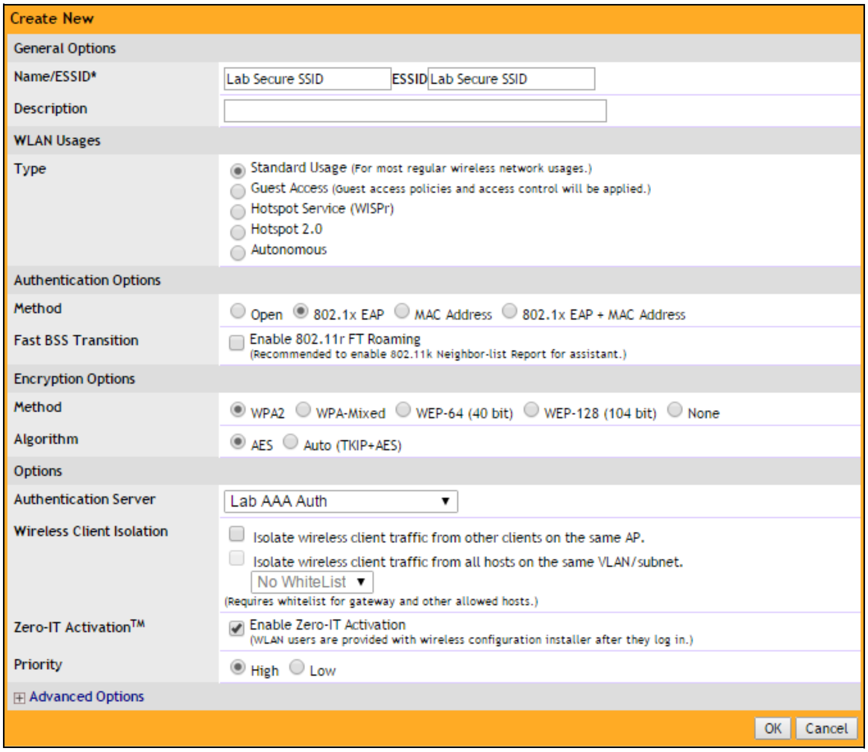
3. Authentication Option Method=Open.
4. Encryption Option Method=None.
5. Select the Hotspot Service created in Task 2.
6. Enable Bypass CNA.
   - For ZoneDirector, this setting is at the bottom of the screen in the Bypass Apple CNA Feature section. Check the Hotspot service box.
   - For SmartZone, 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:

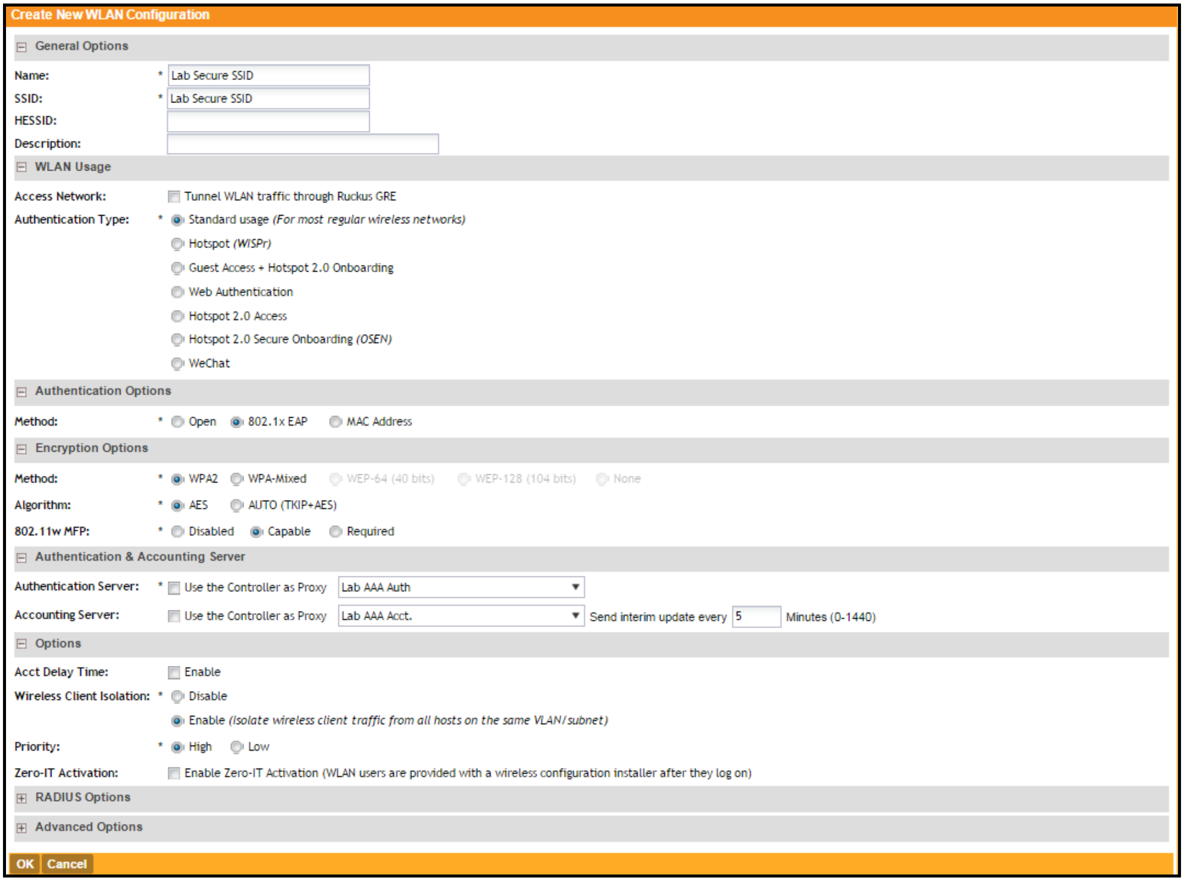
1. Name the SSID.
2. Type=Standard Usage.
3. Authentication Option Method=802.1x EAP.
4. Encryption Option Method=WPA2
5. Encryption Option Algorithm=AES
6. Select the Cloudpath RADIUS Authentication Server.
7. Select the Cloudpath RADIUS Accounting Server (SmartZone only).
8. Leave the defaults for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

FIGURE 12. Configure Secure SSID on the ZoneDirector controller.



Create New	
General Options	
Name/ESSID*	Lab Secure SSID ESSID Lab Secure SSID
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	Lab AAA Auth ▼
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^{TM}	☑ Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
Priority	● High ○ Low
⊞ Advanced Options	
	OK Cancel

FIGURE 13. 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 ○ AUTO (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

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.

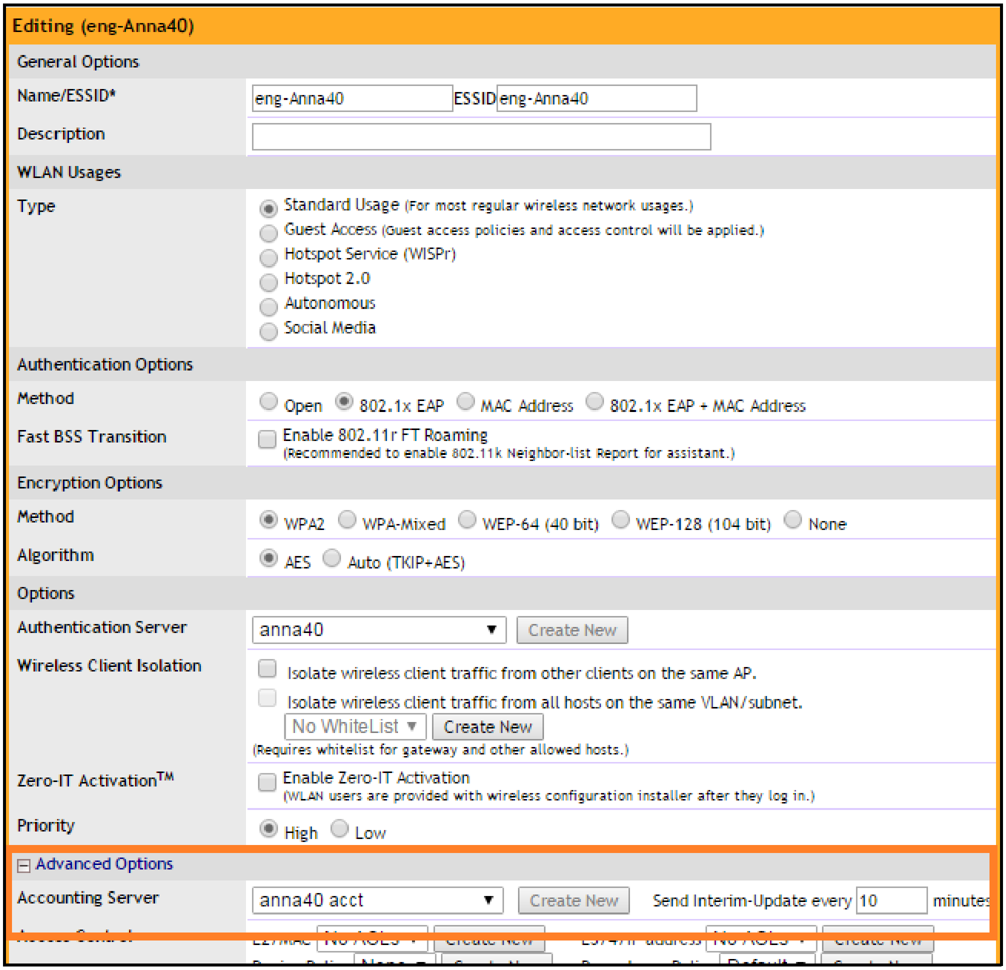
Select AAA Accounting Server for the WLAN on Zone Director Controller

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 > Advanced > RADIUS Server.*

Select RADIUS Accounting server for the WLAN on Zone Director



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 ▼ Create New

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 ▼ Create New
(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 ▼ Create New Send Interim-Update every 10 minutes

Access Control L2/MAC No ACLs ▼ Create New L3/4/IP address No ACLs ▼ Create New

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 11 on page 9.