

Configuring Ruckus Wireless LAN Controllers to Integrate With Cloudpath

Software Release 5.2

Copyright, Trademark and Proprietary Rights Information

© 2018 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

Configuring the Ruckus Wireless Controllers.....	4
Setting up Cloudpath as an AAA Authentication Server.....	4
Creating AAA Accounting Server (Optional).....	7
Running Authentication Test.....	8
ZoneDirector.....	8
SmartZone.....	8
Unleashed.....	9
Possible Results from Authentication Test.....	9
Creating Hotspot Services.....	10
Setting Up the Walled Garden.....	15
Creating the Onboarding SSID.....	17
Enabling Bypass CNA on ZoneDirector.....	21
Enabling Bypass CNA on Unleashed.....	22
Creating the Secure SSID.....	23

Configuring the Ruckus Wireless Controllers

This document describes how to configure the Ruckus ZoneDirector, SmartZone, and Unleashed 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

NOTE

The screen shots and corresponding instructions in this manual are based on the following Ruckus Controller versions:

- ZoneDirector 10.1.1
- Virtual SmartZone 3.6.0 (High Scale)
- Unleashed 200.6

If you are using different versions of any controller, please consult your controller documentation because you may encounter some differences in the user interface.

Setting up Cloudpath as an AAA Authentication Server

Create an AAA authentication server for the Cloudpath onboard RADIUS server. The following images show this configuration on the Ruckus ZoneDirector, SmartZone, and Unleashed controllers.

On ZoneDirector, go to **Services & Profiles > AAA Servers**. On SmartZone, go to **Services & Profiles > Authentication**. On Unleashed, go to **Admin & Services > Services > AAA Servers > Authentication Servers**.

FIGURE 1 Create AAA Authentication Server on ZoneDirector

Create New

Name	<input type="text" value="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+
Encryption	<input type="checkbox"/> TLS
Auth Method	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP
Backup RADIUS	<input type="checkbox"/> Enable Backup RADIUS support
IP Address*	<input type="text" value="192.168.5.73"/>
Port*	<input type="text" value="1812"/>
Shared Secret*	<input type="password" value="*****"/>
Confirm Secret*	<input type="password" value="*****"/>
Retry Policy	
Request Timeout*	<input type="text" value="3"/> seconds
Max Number of Retries*	<input type="text" value="2"/> times

FIGURE 2 Create AAA Authentication Server on SmartZone

Create AAA Server

General Options

Name: Lab AAA Auth

Description:

Type: RADIUS Active Directory LDAP

Backup RADIUS: Enable Secondary Server

Primary Server

IP Address: 72.18.151.56

Port: 1812

Shared Secret:

Confirm Secret:

User Role Mapping

OK Cancel

FIGURE 3 Create AAA Authentication Server on Unleashed

Create New

Name

Type Active Directory RADIUS RADIUS Accounting

Encryption TLS

Auth Method PAP CHAP

Backup RADIUS Enable Backup RADIUS support

IP Address*

Port*

Shared Secret*

Confirm Secret*

Retry Policy

Request Timeout* seconds

Max Number of Retries* times

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

1. Name
2. Type = RADIUS
3. Auth Method (not applicable for SmartZone) = 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.

Creating AAA Accounting Server (Optional)

Use the same process to create the AAA Accounting Server.

NOTE

To navigate to the correct screen on Ruckus SmartZone, go to **Services & Profiles > Accounting**.

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

1. Name
2. Type = RADIUS ACCOUNTING.
3. IP address = The IP address of the Cloudpath ES.

4. Port = 1813

NOTE

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

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

Running Authentication Test

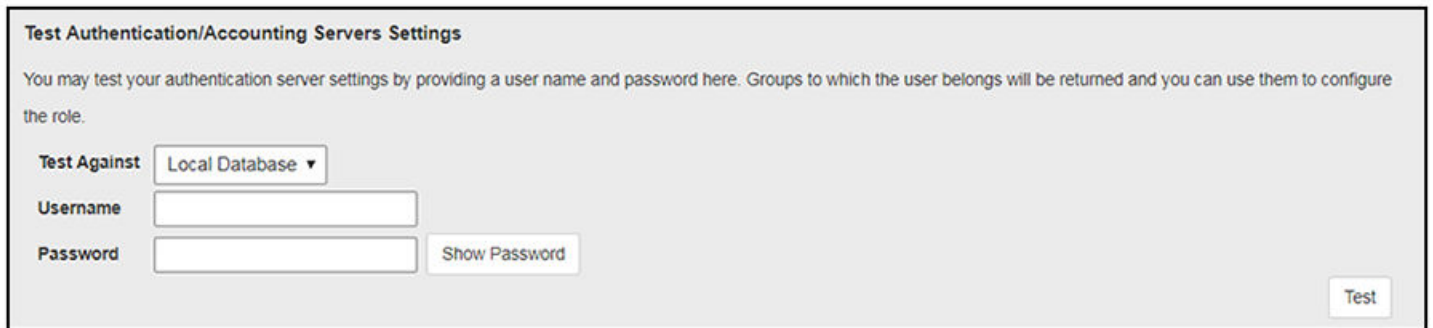
You can test the connection between the controller and the Cloudpath ES RADIUS server.

Follow the instructions for the applicable controller. For the possible results, see [Possible Results from Authentication Test](#).

ZoneDirector

At the bottom of the AAA server page, there is a section called "Test Authentication/Accounting Servers Settings." The Test Against field should be Local Database, as shown below. Enter a test User Name and Password, then click the **Test** button.

FIGURE 4 Authentication Test on ZoneDirector



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 ▾

Username

Password Show Password

Test

SmartZone

When you save a configuration for an AAA Authentication server in SmartZone, you can click the **Test AAA** tab at the top of the screen, select the server from the drop-down list, enter your credentials, then click the **Test** button.

FIGURE 5 Authentication Test on SmartZone

Test AAA Servers

* Name: Jeff AAA Auth vSZ

* Protocol: PAP CHAP

* User Name: bob

* Password: ****
 Show password

Test Cancel

Unleashed

Enter the test credentials on the Test Authentication Servers Settings tab, then click the **Test** button.

FIGURE 6 Authentication Test on Unleashed

Authentication Servers Test Authentication 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 Anna43Unleashed

User Name

Password Show Password

Test

Possible Results from Authentication Test

If you run the authentication test, you receive one of these responses:

- Failed! Connection timed out
- Failed! Invalid username and password

Creating Hotspot Services

- Authentication Failed

The only one of these responses that means that connectivity was established is:

Failed! Invalid username or password

Creating Hotspot Services

You can configure the Hotspot Service on the ZoneDirector, SmartZone, or Unleashed controllers.

1. Navigate to: For ZoneDirector, go to **Services & Profiles > Hotspot Services**. For SmartZone, go to **Services & Profiles > Hotspots & Portals > Hotspot WISPr**. For Unleashed, go to **Admin & Services > Services > Hotspot Services**, then use both the **General** tab and the **Authentication** tab, as instructed later in this section.

2. Name the Hotspot Service.

FIGURE 7 Create Hotspot Service on ZoneDirector

Create New

Name	Lab Hotspot Services
Redirection	
WISPr Smart Client Support	<input checked="" type="radio"/> None <input type="radio"/> Enabled <input type="radio"/> Only WISPr Smart Client allowed
Login Page*	Redirect unauthenticated user to <input type="text" value="https://training.cloudpath.net/e"/> for authentication.
Start Page	After user is authenticated, <input checked="" type="radio"/> redirect to the URL that the user intends to visit. <input type="radio"/> redirect to the following URL: <input type="text"/>
User Session	
Session Timeout	<input type="checkbox"/> Terminate user session after <input type="text" value="1440"/> minutes
Grace Period	<input type="checkbox"/> Allow users to reconnect without re-authentication for <input type="text" value="30"/> minutes
Authentication/Accounting Servers	
Authentication Server	Jeff AAA Auth <input checked="" type="checkbox"/> Enable MAC authentication bypass(no redirection). <input checked="" type="radio"/> Use device MAC address as authentication password. <input type="radio"/> Use <input type="text"/> as authentication password. MAC Address Format <input type="text" value="AA:BB:CC:DD:EE:FF"/>
Accounting Server	Jeff AAA acct Send Interim-Update every <input type="text" value="5"/> minutes
Wireless Client Isolation	
<input type="checkbox"/> Isolate wireless client traffic from other clients on the same AP. <input type="checkbox"/> Isolate wireless client traffic from all hosts on the same VLAN/subnet. <input type="text" value="No WhiteList"/> <small>(Requires whitelist for gateway and other allowed hosts.)</small>	
<input type="checkbox"/> Location Information <input type="checkbox"/> Walled Garden <input type="checkbox"/> Restricted Subnet Access <input type="checkbox"/> Advanced Options	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

FIGURE 8 Create Hotspot WISPr on SmartZone

Create Hotspot Portal

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/Produc

Redirected MAC Format: AA:BB:CC:DD:EE:FF

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

HTTPS Redirect: If enabled, the AP will try to redirect HTTPS requests to the hotspot portal

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

OK Cancel

FIGURE 9 Create Hotspot Service on Unleashed - General Tab

Create New ✕

General

Authentication

WalledGarden

Policy

Name

Redirection

WISPr Smart Client Support None Enabled Only WISPr Smart Client allowed

Login Page Redirect unauthenticated user to 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 (Requires whitelist for gateway and other allowed hosts.)

Terminate user session after minutes

Grace Period Allow users to reconnect without re-authentication for minutes

Intrusion Prevention Temporarily block Hotspot clients with repeated authentication attempts.

FIGURE 10 Create Hotspot Service on Unleashed - Authentication Tab

The screenshot shows the 'Authentication' tab of a configuration window. At the top, there are four tabs: 'General', 'Authentication', 'WalledGarden', and 'Policy'. The 'Authentication' tab is active. Below the tabs, there are three main sections:

- Authentication/Accounting Servers:**
 - Authentication Server:** A dropdown menu is set to 'Anna43Unleashed' with a 'Create New' button next to it.
 - Three radio buttons are present:
 - Enable MAC authentication bypass(no redirection).
 - Use device MAC address as authentication password.
 - Use [MAC Address] as authentication password.
 - MAC Address Format:** A dropdown menu is set to 'AA:BB:CC:DD:EE:FF'.
 - Accounting Server:** A dropdown menu is set to 'Anna43UnleashedACCT' with a 'Create New' button next to it.
 - Send Interim-Update every:** A text input field contains '10' followed by the word 'minutes'.
- Wireless Client Isolation:**
 - Two checkboxes:
 - Isolate wireless client traffic from other clients on the same AP.
 - Isolate wireless client traffic from all hosts on the same VLAN/subnet.
 - A dropdown menu is set to 'No WhiteList' with a 'Create New' button next to it.
 - Text below: '(Requires whitelist for gateway and other allowed hosts.)'
- Location Information:**
 - Location ID:** An empty text input field with a hint '(e.g. isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport)'. The hint text is in a smaller font.
 - Location Name:** An empty text input field with a hint '(e.g. ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport)'. The hint text is in a smaller font.

At the bottom right of the window, there are two buttons: 'OK' and 'Cancel'.

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**. Applicable only for ZoneDirector and Unleashed (**Authentication** tab) in this screen.
6. Select **Enable MAC authentication bypass (no redirection)**. Applicable only for ZoneDirector and Unleashed (**Authentication** tab) in this screen. Selecting this field allows users with registered MAC addresses to be transparently authorized without having to log in.
7. For MAC Address Format (which appears when you select **Enable MAC authentication bypass (no redirection)** in the preceding step, it is recommended that you select the following option from the drop-down list: AA:BB:CC:DD:EE:FF
8. Select the **Cloudpath RADIUS Accounting Server**. Applicable only for ZoneDirector and Unleashed (**Authentication** tab).
9. Leave the defaults for the remaining settings. Click **OK**.

Setting Up the Walled Garden

Perform the following steps to add a walled garden configuration to your existing Hotspot Services configuration:

1. Navigate to: For ZoneDirector, go to **Services & Profiles > Hotspot Services**. For SmartZone, go to **Services & Profiles > Hotspots & Portals > Hotspot WISPr**. For Unleashed, go to **Admin & Services > Services > Hotspot Services**.

- For ZoneDirector and SmartZone, use the **edit** function on the existing Hotspot Services configuration, then scroll to the **Walled Garden** section and expand this section. For Unleashed, click the **WalledGarden** on the existing Hotspot Services configuration.

FIGURE 11 Walled Garden Configuration for ZoneDirector

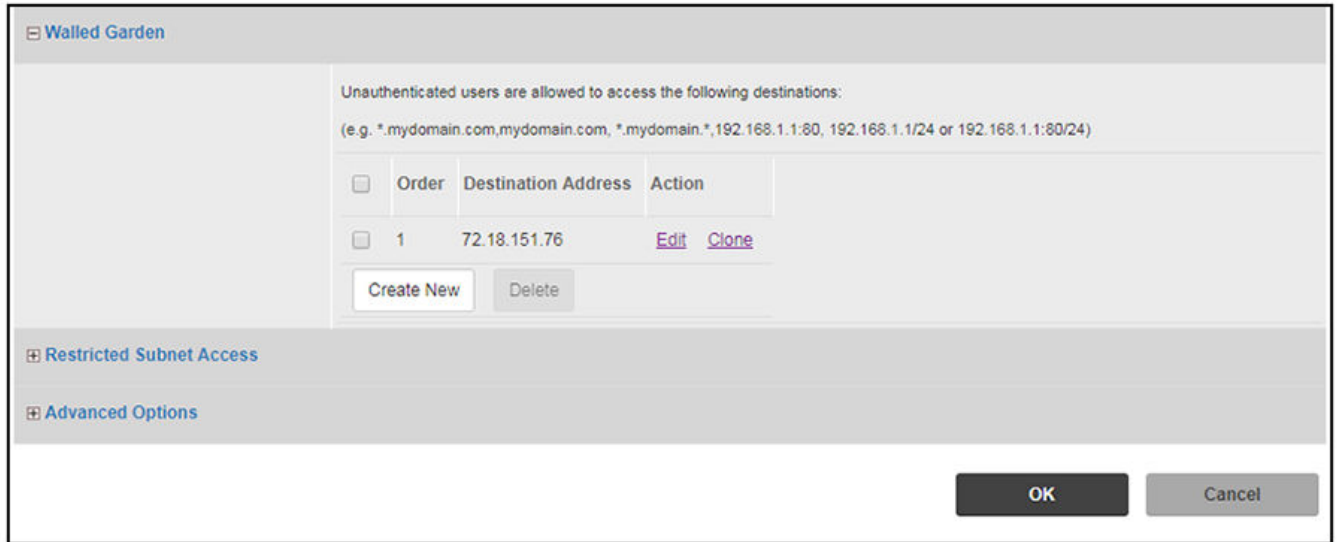


FIGURE 12 Walled Garden Configuration for SmartZone

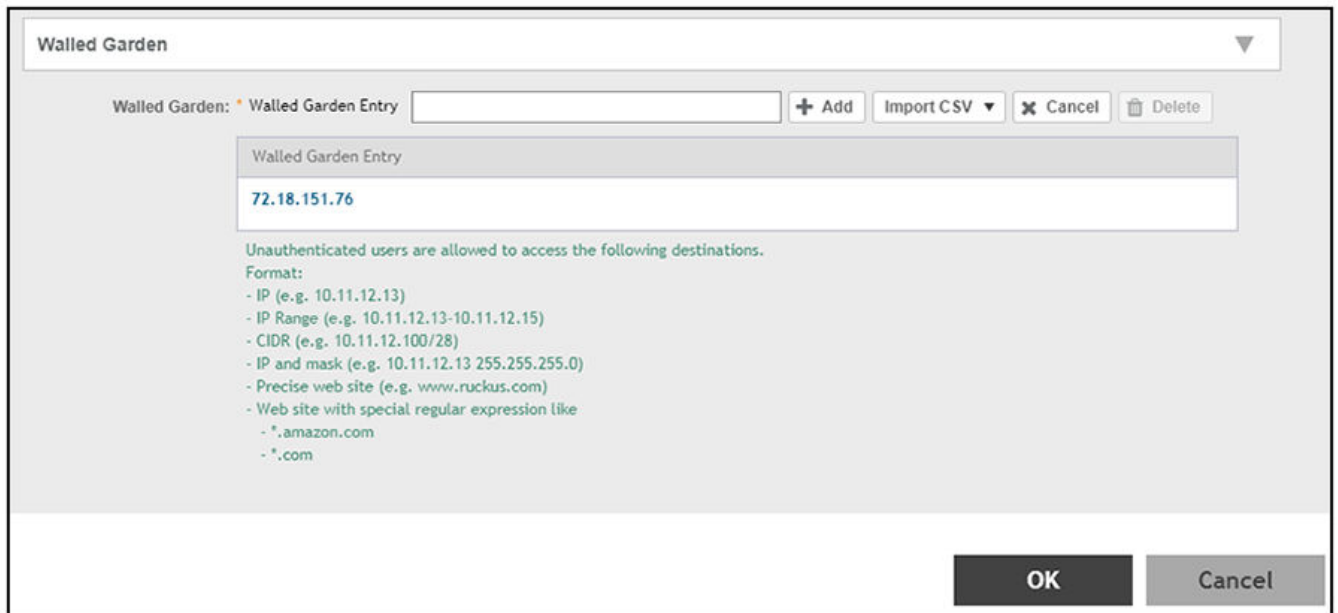


FIGURE 13 Walled Garden Configuration for Unleashed

Edit ✕

General Authentication **WalledGarden** Policy

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)

<input type="checkbox"/>	Order	Destination Address	Action
<input type="checkbox"/>	1	192.168.5.42	Save Cancel

[Create New](#) Advanced Options Delete

OK Cancel

3. Include the DNS or IP address of the Cloudpath system, then click **OK**.
4. Optionally, there are some domains that you can add to the walled garden on all controllers to:
 - Prevent the Apple CNA mini-browser from appearing on Apple devices.
 - Avoid being blocked or slowed when attempting to download the Cloudpath wizard.

These recommended destinations for the walled garden are:

```
*.ggpht.com
*.play.googleapis.com
*.play.google.com
*.android.clients.google.com
*.www.googleapis.com
*.gvt1.com
*.connectivitycheck.android.com
*.gstatic.com
*.clients3.google.com
```

Creating the Onboarding SSID

To configure the onboarding SSID, navigate to: For ZoneDirector and SmartZone, go to the Wireless LANS section of the controller UI; for Unleashed, go to **Wifi Networks** to create the WLAN.

1. Name the SSID.

Creating the Onboarding SSID

2. Type=Hotspot Service (WISPr).

FIGURE 14 Onboarding SSID Configuration on ZoneDirector

The screenshot displays the 'Create WLAN' configuration window in ZoneDirector. The window is titled 'Create WLAN' and has a close button (X) in the top right corner. It is divided into several sections:

- General Options:** Contains fields for 'Name' (Lab Onboard SSID), 'ESSID' (Lab Onboard SSID), and 'Description'.
- WLAN Usages:** Contains a 'Type' section with radio buttons for: Standard Usage (For most regular wireless network usages), Guest Access (Guest access policies and access control will be applied), Hotspot Service (WISPr) (selected), Hotspot 2.0, Autonomous, Social Media, and WeChat.
- Authentication Options:** Contains a 'Method' section with radio buttons for: Open (selected), 802.1x EAP, MAC Address, and 802.1x EAP + MAC Address. It also has a 'Fast BSS Transition' section with a checkbox for 'Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)'.
- Encryption Options:** Contains a 'Method' section with radio buttons for: WPA2, WPA-Mixed, WEP-64 (40 bit), WEP-128 (104 bit), and None (selected).
- Options:** Contains a 'Hotspot Services' dropdown menu (set to 'Lab Hotspot Services') and a 'Create New' button. It also has a 'Priority' section with radio buttons for: High (selected) and Low.
- Advanced Options:** A section with a right-pointing arrow.

At the bottom right of the window, there are 'OK' and 'Cancel' buttons.

FIGURE 15 Onboarding SSID Configuration on SmartZone

Create WLAN Configuration

General Options

- Name: Lab Onboard SSID
- SSID: Lab Onboard SSID
- Description:
- Zone: Default
- WLAN Group: default + Create

Authentication Options

- Authentication Type: Standard usage (for most regular wireless networks) Hotspot (HSP) Guest Access Web Authentication
- Hotspot 2.0 Access Hotspot 2.0 Onboarding WPA-Chat
- Method: Open 802.1X EAP MAC Address 802.1X B MAC
- MAC Authentication: Use user-defined text as authentication password (default is device MAC address):
- MAC Address Format: AA:BB:CC:DD:EE:FF

Encryption Options

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

Data Plane Options

- Access Network: Tunnel WLAN traffic through Ruckus GRE

Hotspot Portal

- Hotspot (HSP) Portal: Lab Hotspot Services + Create
- Bypass OMA: Enable
- Authentication Service: Use the controller as proxy Use RADIUS-based profile
- Auth Service: Jiff AAA Auth v52 + Create
- Accounting Service: Use the controller as proxy
- Acc Service: Jiff AAA Acc v52 + Create
- Send interim update every: 10 Minutes (0-1440)

Options

- Asst Delay Time: Enable
- Wireless Client Isolation: Disable Enable (isolate wireless client traffic from all hosts on the same VLAN/subnet)
- Isolation Whitelist: Gateway Only (Automatic) + Create
- Priority: High Low

RADIUS Options

Advanced Options

OK **Cancel**

FIGURE 16 Onboarding SSID Configuration for Unleashed

Create WLAN [X]

* **Name:**

Usage Type:

- Standard for most regular wireless network usage
- Guest Access guest access policies and access control will be applied
- Hotspot Service known as WISPr
- Social Media authenticate through social media network
- WeChat

Hotspot Services:

Show Advanced Options ▶

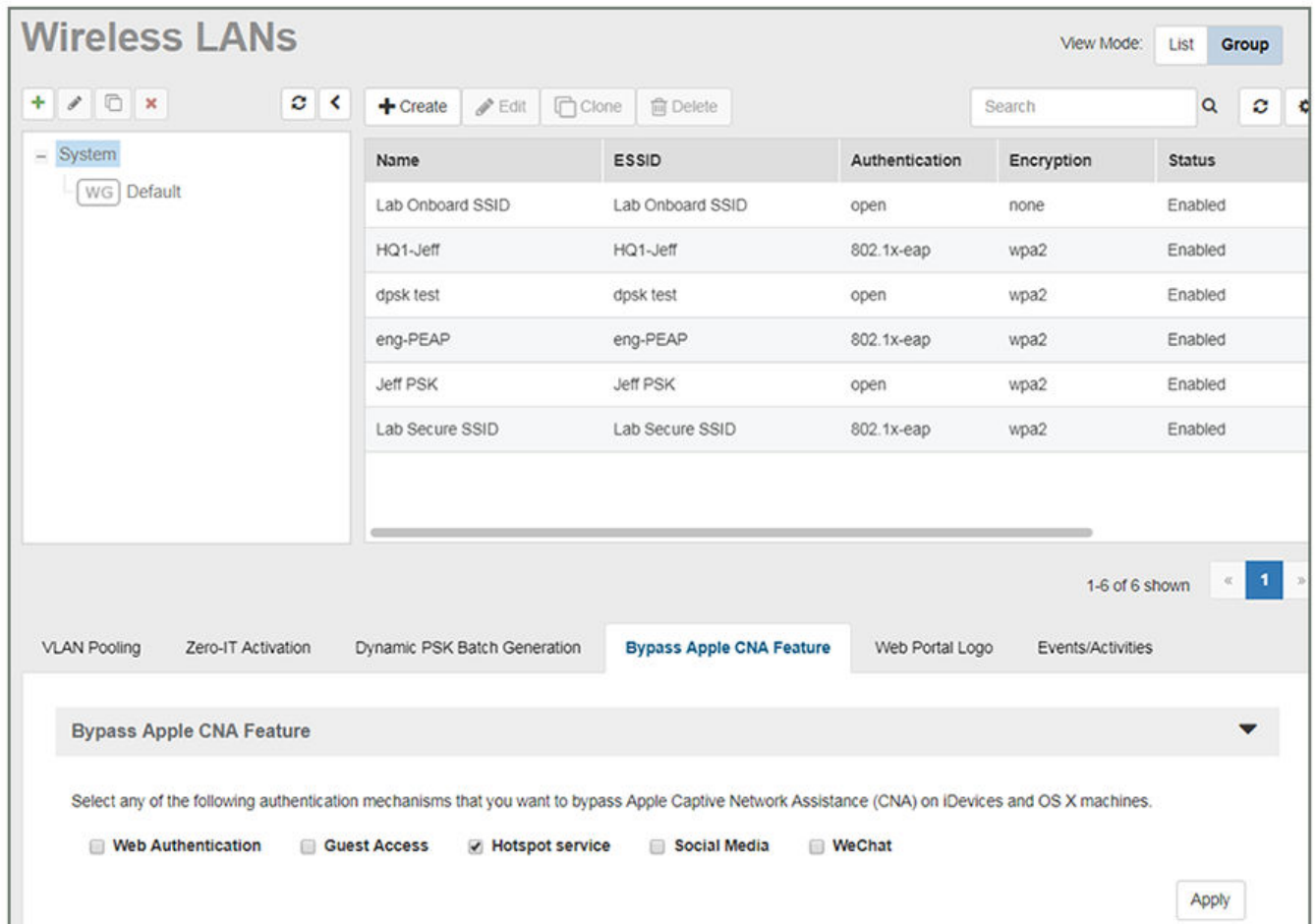
3. Authentication Options Method=Open for ZoneDirector, MAC Address for SmartZone. (Not applicable for Unleashed.)
4. The checkbox next to MAC Authentication (SmartZone only) called "Use user defined text as authentication password (default is device MAC address):" can be left unchecked.
5. The MAC Address Format (SmartZone only) recommended selection is: AA:BB:CC:DD:EE:FF. This is the default for most RADIUS servers.
6. Encryption Options Method=None (ZoneDirector and SmartZone).
7. Select the Hotspot Service from the drop-down list that you should already have created in a previous step procedure.
8. Enable the **Bypass CNA** feature as follows, depending on the controller:
 - For SmartZone: Check the box to enable "Bypass CNA," as shown in [Figure 15](#).
 - For ZoneDirector, after you finish configuring the onboarding SSID, refer to [Figure 17](#) on page 21.
 - For Unleashed, after you finish configuring the onboarding SSID, refer to [Figure 19](#) on page 22.
9. Select the Cloudpath RADIUS Authentication Server (SmartZone only).
10. Select the Cloudpath RADIUS Accounting Server (SmartZone only).
11. Leave the defaults for the remaining settings and click **OK** (or **Apply**).

Enabling Bypass CNA on ZoneDirector

It is recommended to enable the "Bypass Apple CNA Feature," which you can do globally for wireless LANs in ZoneDirector.

1. In the Wireless LANs main screen, click on **Bypass Apple CNA Feature**, as shown in the following figure:

FIGURE 17 Enabling the Bypass Apple CNA Feature Globally on ZoneDirector



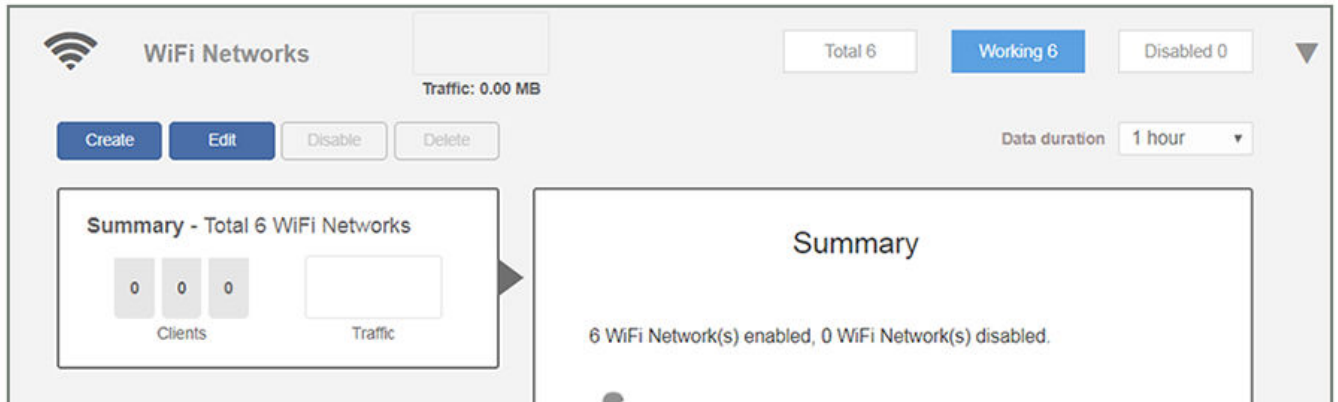
2. In the "Bypass Apple CNA Feature" area of the screen, check the "Hotspot service" box.
3. Click **Apply** to enable the "Bypass Apple CNA Feature" globally on all Wireless LANs that are configured as type "Hotspot Service (WISPr)."

Enabling Bypass CNA on Unleashed

It is recommended to enable the "Bypass Apple CNA Feature," which you can do globally for wireless LANs in Unleashed.

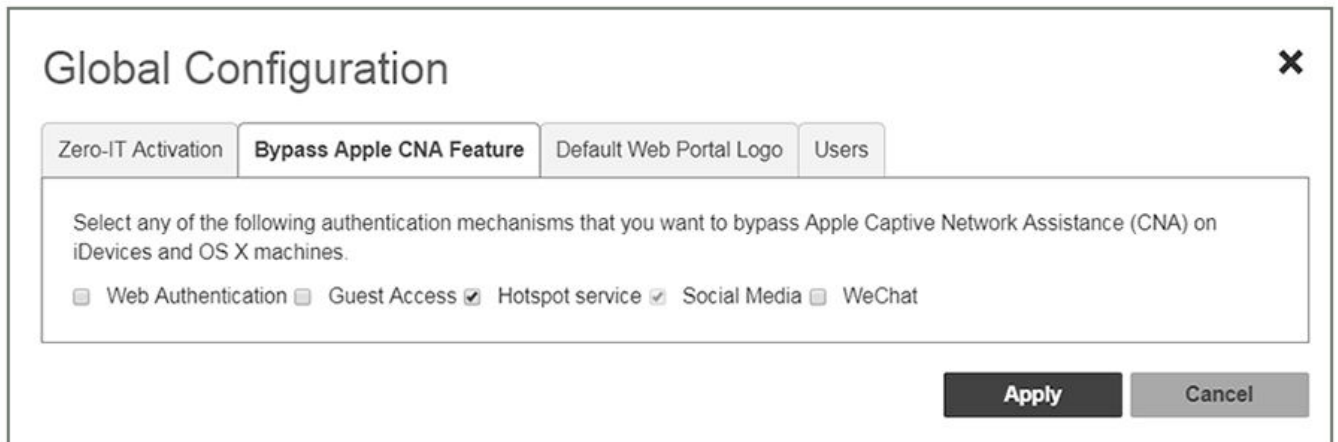
1. In the WiFi Networks main screen (see figure below), click **Edit**.

FIGURE 18 Clicking the Edit Button Brings you to Global Configuration



2. In the Global Configuration screen that pops up, click **Bypass Apple CNA Feature**.

FIGURE 19 Enabling the Bypass Apple CNA Feature Globally on Unleashed



3. In the "Bypass Apple CNA Feature" area of the screen, check the "Hotspot service" box.
4. Click **Apply** to enable the "Bypass Apple CNA Feature" globally on all Wireless LANs that are configured as type "Hotspot Service (WISPr)."

Creating the Secure SSID

To configure the onboarding SSID, navigate to: For ZoneDirector and SmartZone, go to the Wireless LANS section of the controller UI; for Unleashed, go to **Wifi Networks** to create the WLAN.

1. Name the SSID.
2. Type=Standard Usage.
3. Authentication Option Method=802.1x EAP.
4. Encryption Option Method=WPA2 (not applicable for Unleashed once the 802.1x EAP authentication option method is selected).
5. Encryption Option Algorithm=AES (not applicable for Unleashed once the 802.1x EAP authentication option method is selected).
6. Select the Cloudpath RADIUS authentication server.
7. Select the Cloudpath RADIUS accounting server (required only if you are using Cloudpath onboard RADIUS Accounting and Connection Tracking). **Note:** For ZoneDirector, you need to expand the Advanced Options section of the screen to locate the drop-down selection for the accounting server.

Creating the Secure SSID

8. Leave the defaults for the remaining settings and click **OK**.

FIGURE 20 Configure Secure SSID on the ZoneDirector controller

Create WLAN

General Options

Name: 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
 Social Media
 WeChat

Authentication Options

Method: Open 802.1x EAP MAC Address 802.1x EAP + MAC Address
Fast BSS Transition: Disable 802.11r FT Roaming (Recommended to enable 802.11r Neighbour-List Report for assistant.)

Encryption Options

Method: WPA2 WPA-Mixed WEP-64 (40 bit) WEP-128 (104 bit) None
Algorithm: AES Auto (TKIP+AES)
802.11w MFP: Disabled Optional Required

Options

Authentication Server: Jeff 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™: Enable Zero-IT Activation
(WLAN users are provided with wireless configuration installer after they log in.)
Priority: High Low

Advanced Options

FIGURE 21 Select RADIUS Accounting Server on ZoneDirector

Advanced Options

Accounting Server: Jeff AAA acct Send Interim-Update every 10 minutes

Access Control: L2/MAC

L3/4/IP address

Device Policy Precedence Policy

Enable Role based Access Control Policy

Application Recognition & Control: Enable

Call Admission Control: Enforce CAC on this WLAN when CAC is enabled on the radio

Rate Limiting: Per Station Uplink Per Station Downlink

SSID Rate Limiting: UpLink Enable 0 mbps (0.1~200)

DownLink Enable 0 mbps (0.1~200)

Per STA rate limiting will not work if SSID rate limiting is enabled.

FIGURE 22 Configure Secure SSID on the SmartZone controller

Create WLAN Configuration

General Options

- Name: Lab Secure SSID
- SSID: Lab Secure SSID
- Description:
- Zone: Default
- WLAN Group: Default + Create

Authentication Options

- Authentication Type: Standard usage (for most regular wireless networks) Hotspot (WISPr) Guest Access Web Authentication
- Hotspot 2.0 Access Hotspot 2.0 Onboarding YipeChat
- Method: Open 802.1X EAP MAC Address 802.1X & MAC

Encryption Options

- Method: WPA2 WPA.Mixed WEP-44 (40 bits) WEP-128 (104 bits) None
- Algorithm: AES AUTO
- 802.11r Fast Roaming: Enable 802.11r Fast BSS Transition
- 802.11w WPA: Disabled Capable Required

Data Plane Options

- Access Network: Tunnel WLAN traffic through Ruckus GRE

Authentication & Accounting Service

- Authentication Service: Use the controller as proxy
Jeff AAA Auth v52 + Create
- Accounting Service: Use the controller as proxy
Jeff AAA Acct v52 + Create Send Interim update every 5 Minutes (0-1440)

Options

- Asst Delay Time: Enable
- Wireless Client Isolation: Disable Enable (isolate wireless client traffic from all hosts on the same VLAN/subnet)
- Isolation Whitelist: Gateway Only (Automatic) + Create
(The whitelist requires entries for the subnet gateway and other allowed hosts.)
(The whitelist can only contain wired destinations, wireless clients are not supported on the whitelist.)
- Priority: High Low

RADIUS Options

Advanced Options

OK Cancel

FIGURE 23 Configure Secure SSID on the Unleashed controller

Create WLAN ✕

Name:

Usage Type: **Standard** for most regular wireless network usage
 Guest Access guest access policies and access control will be applied
 Hotspot Service known as WISPr
 Social Media authenticate through social media network
 WeChat

Authentication Method: Open **802.1X EAP** MAC Address

Authentication Server:

Accounting Server:

Send Interim-Update every minutes

Show 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.



© 2018 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