

Cloudpath Enrollment System Integration with RUCKUS WLAN Controllers Configuration Guide, 5.9R4

Supporting Cloudpath Software Release 5.9R4

Copyright, Trademark and Proprietary Rights Information

© 2022 CommScope, Inc. 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 CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope 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, 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

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

| | |
|--|-----------|
| Configuring the Ruckus Wireless Controllers..... | 4 |
| Configuring Virtual SmartZone..... | 4 |
| Setting up Cloudpath as an AAA RADIUS Authentication Server..... | 4 |
| Creating AAA RADIUS Accounting Server (Optional)..... | 4 |
| Testing AAA Servers..... | 4 |
| Creating a Hotspot (WISPr) Portal..... | 5 |
| Setting Up the Walled Garden..... | 5 |
| Creating the Onboarding SSID..... | 6 |
| Configuring Unleashed..... | 6 |
| Setting up Cloudpath as an AAA RADIUS Authentication Server..... | 6 |
| Creating AAA Accounting Server (Optional)..... | 7 |
| Testing AAA Servers..... | 7 |
| Creating a Hotspot (WISPr) Portal..... | 7 |
| Setting Up the Walled Garden..... | 8 |
| Creating the Onboarding SSID..... | 8 |
| Configuring ZoneDirector..... | 9 |
| Setting up Cloudpath as an AAA RADIUS Authentication Server..... | 9 |
| Creating AAA RADIUS Accounting Server (Optional)..... | 9 |
| Testing AAA Servers..... | 9 |
| Creating a Hotspot (WISPr) Portal..... | 10 |
| Setting Up the Walled Garden..... | 10 |
| Creating the Onboarding SSID..... | 11 |
| Creating the Secure SSID..... | 11 |

Configuring the Ruckus Wireless Controllers

This section describes how to configure RUCKUS Virtual SmartZone, RUCKUS Unleashed, and RUCKUS ZoneDirector to integrate with the Cloudpath system. The information provided here is specific to integrating Cloudpath with one of these controllers. Consult your controller documentation for more information.

Configuring Virtual SmartZone

This section includes tables of configuration fields and values for setting up the Virtual SmartZone (vSmartZone) Controller. For more information, such as how to navigate the vSmartZone UI, how to find more information about configuration fields, and to view screen shots of the vSmartZone UI, refer to the *RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide*.

NOTE

For any configuration fields that are not described in the following sections, you can use their default values.

Setting up Cloudpath as an AAA RADIUS Authentication Server

TABLE 1 Fields/Values to Use for vSmartZone AAA Authentication Service

| AAA Authentication Service Section in vSmartZone UI | Configuration Field and Corresponding Value |
|---|--|
| General Options | Name: Any descriptive name for the AAA authentication service |
| | Type: RADIUS |
| Primary Server | IP Address: The IP address of the Cloudpath Enrollment System. |
| | Port: 1812 is typically used and is the default. |
| | Shared Secret: This must match the shared secret for the Cloudpath ES onboard RADIUS server (Configuration > RADIUS Server). |
| | Confirm Secret: The shared secret (entered again). |

Creating AAA RADIUS Accounting Server (Optional)

TABLE 2 Fields/Values to Use for SmartZone AAA Accounting Service

| AAA Accounting Service Section in vSmartZone UI | Configuration Field and Corresponding Value |
|---|--|
| General Options | Name: Any descriptive name for the AAA accounting service |
| | Type: RADIUS ACCOUNTING |
| Primary Server | IP Address: The IP address of the Cloudpath Enrollment System. |
| | Port: 1813 is typically used and is the default. |
| | Shared Secret: This must match the shared secret for the Cloudpath ES onboard RADIUS server (Configuration > RADIUS Server). |
| | Confirm Secret: The shared secret (entered again). |

Testing AAA Servers

To test the connection between the controller and the Cloudpath RADIUS server, RUCKUS strongly recommends testing the AAA server after you set it up. Refer to the instructions in the *RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide*.

Creating a Hotspot (WISPr) Portal

TABLE 3 Fields/Values to Use for Creating a Hotspot (WISPr) Portal

| Creating a Hotspot (WISPr) Portal section in vSmartZone UI | Configuration Field and Corresponding Value |
|--|---|
| General Options | Portal Name: Any descriptive name for the hotspot portal. |
| Redirection | Login URL: Select "External." |
| | Redirect unauthenticated user: The Cloudpath Enrollment Portal URL, which should be contained in the applicable workflow in the Cloudpath UI (Configuration > Workflows). |
| | Start Page: After user is authenticated,; Select "Redirect to the URL that the user intends to visit." This lets you set a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address for the redirection. |

Setting Up the Walled Garden

To add a walled garden configuration to your existing Hotspot Services, refer to the instructions in the *RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide*.

Also, when configuring the walled garden, include the following steps:

1. Include the DNS or IP address of the Cloudpath system, then click **OK**
2. 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.

NOTE

There will still be about a 15-to-20-second delay when the full application is 33 percent complete (about 40 MB) in its download.

The recommended destinations to add for the walled garden are:

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

NOTE

The **thawte.com* destination is the OSCP URL of the SSL certificate of the Cloudpath server. This URL can be found by clicking the *lock* icon in your web browser and viewing the details of your certificate.

3. If you are still experiencing issues, you can try adding the following destinations to the walled garden:

```
*.clients.google.com
*.l.google.com
*.googleusercontent.com
*.appengine.google.com
*.cloud.google.com
*.android.com
```

```
*.cloudfront.net
*.akamaihd.net
172.217.0.0/16
216.58.0.0/16
```

Creating the Onboarding SSID

TABLE 4 Fields/Values to Use for SmartZone Onboarding SSID

| Creating a WLAN Configuration (for Onboarding SSID) section in vSmartZone UI | Configuration Field and Corresponding Value |
|--|--|
| General Options | Name: Name of the SSID |
| | SSID: Name of the WLAN |
| | Zone: Zone in which the WLAN will reside |
| | WLAN Group: Group in which the WLAN will reside |
| Authentication Options | Authentication Type: Hotspot (WISPr) |
| | Method: MAC Address |
| | MAC Authentication: Unchecked |
| | MAC Address Format: Recommended format is AA:BB:CC:DD:EE:FF |
| Encryption options | Method: None |
| Hotspot Portal | Hotspot (WISPr) Portal: Drop-down list to select the already-created hotspot service. |
| | Bypass CNA: Enable |
| | Authentication Server: Drop-down list to select the Cloudpath RADIUS Authentication Server |
| | Accounting Server: Drop-down list to select the Cloudpath RADIUS Accounting Server |

Configuring Unleashed

This section includes tables of configuration fields and values for setting up the RUCKUS Unleashed platform. For more information, such as how to navigate the Unleashed UI, how to find more information about configuration fields, and to view screen shots of the Unleashed UI, refer to the *RUCKUS Unleashed User Guide*.

NOTE

For any configuration fields that are not described in the following sections, you can use their default values.

Setting up Cloudpath as an AAA RADIUS Authentication Server

TABLE 5 Fields/Values to Use for Unleashed AAA Authentication Service

| Configuration Field | Corresponding Value |
|---------------------|---|
| Name | Name: Any descriptive name for the AAA authentication service |
| Type | RADIUS |
| Auth Method | PAP |
| IP Address | The IP address of the Cloudpath Enrollment System. |
| Port | 1812 is typically used and is the default. |

TABLE 5 Fields/Values to Use for Unleashed AAA Authentication Service (continued)

| Configuration Field | Corresponding Value |
|---------------------|---|
| Shared Secret | This must match the shared secret for the Cloudpath ES onboard RADIUS server (Configuration > RADIUS Server). |
| Confirm Secret | Confirm Secret: The shared secret (entered again). |

Creating AAA Accounting Server (Optional)

TABLE 6 Fields/Values to Use for Unleashed AAA RADIUS Accounting Service

| Configuration Field | Corresponding Value |
|---------------------|---|
| Name | Name: Any descriptive name for the AAA accounting service |
| Type | RADIUS ACCOUNTING |
| IP Address | The IP address of the Cloudpath Enrollment System. |
| Port | 1813 is typically used and is the default. |
| Shared Secret | This must match the shared secret for the Cloudpath ES onboard RADIUS server (Configuration > RADIUS Server). |
| Confirm Secret | Confirm Secret: The shared secret (entered again). |

Testing AAA Servers

To test the connection between Unleashed and the Cloudpath RADIUS server, RUCKUS strongly recommends testing the AAA server after you set it up. Refer to the instructions in the *RUCKUS Unleashed User Guide*.

Creating a Hotspot (WISPr) Portal

TABLE 7 Fields/Values to Use for Creating a Hotspot (WISPr) Portal

| Creating a Hotspot (WISPr) Portal Section in Unleashed UI | Configuration Field and Corresponding Value |
|---|---|
| General tab | Name: Any descriptive name for the hotspot portal. |
| Redirection (General tab) | <p>Redirect unauthenticated user: The Cloudpath Enrollment Portal URL, which should be contained in the applicable workflow in the Cloudpath UI (Configuration > Workflows).</p> <p>Start Page: After user is authenticated,; Select "Redirect to the URL that the user intends to visit." This lets you set a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address for the redirection.</p> |
| Authentication/Accounting Servers (Authentication tab) | <p>Authentication Server: Drop-down list to select the Cloudpath RADIUS Authentication Server.</p> <p>NOTE Enabling this option allows users with registered MAC addresses to be transparently authorized without having to log in. A user entry on the RADIUS server needs to be created using the client MAC address as both the user name and password. For the MAC address format, RUCKUS recommends using AA:BB:CC:DD:EE:FF.</p> |
| Authentication/Accounting Servers (Authentication tab) | Accounting Server: Drop-down list to select the Cloudpath RADIUS Accounting Server (if applicable). |

Setting Up the Walled Garden

To add a walled garden configuration, refer to the instructions in the *RUCKUS Unleashed User Guide*.

Also, when configuring the walled garden, include the following steps:

1. Include the DNS or IP address of the Cloudpath system, then click **OK**
2. 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.

NOTE

There will still be about a 15-to-20-second delay when the full application is 33 percent complete (about 40 MB) in its download.

The recommended destinations to add for the walled garden are:

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

NOTE

The `*thawte.com` destination is the OCSP URL of the SSL certificate of the Cloudpath server. This URL can be found by clicking the *lock* icon in your web browser and viewing the details of your certificate.

3. If you are still experiencing issues, you can try adding the following destinations to the walled garden:

```
*.clients.google.com
*.l.google.com
*.googleusercontent.com
*.appengine.google.com
*.cloud.google.com
*.android.com
*.cloudfront.net
*.akamaihd.net
172.217.0.0/16
216.58.0.0/16
```

Creating the Onboarding SSID

TABLE 8 Fields/Values to Use for Unleashed Onboarding SSID

| Configuration Field | Corresponding Value |
|---------------------|--|
| Name | Name of the SSID |
| Usage Type | Hotspot Service known as WISPr |
| Hotspot Services | Drop-down list to select the already-created hotspot service |

NOTE

RUCKUS recommends enabling the "Bypass Apple CNA" feature. For instructions, refer to the *RUCKUS Unleashed User Guide*.

Configuring ZoneDirector

This section includes tables of configuration fields and values for setting up the ZoneDirector Controller. For more information, such as how to navigate the ZoneDirector UI, how to find more information about configuration fields, and to view screen shots of the vSmartZone UI, refer to the *RUCKUS ZoneDirector User Guide*.

NOTE

For any configuration fields that are not described in the following sections, you can use their default values.

Setting up Cloudpath as an AAA RADIUS Authentication Server

TABLE 9 Fields/Values to Use for ZoneDirector AAA Authentication Service

| Configuration Field | Corresponding Value |
|---------------------|---|
| Name | Name: Any descriptive name for the AAA authentication service |
| Type | RADIUS |
| Auth Method | PAP |
| IP Address | The IP address of the Cloudpath Enrollment System. |
| Port | 1812 is typically used and is the default. |
| Shared Secret | This must match the shared secret for the Cloudpath ES onboard RADIUS server (Configuration > RADIUS Server). |
| Confirm Secret | Confirm Secret: The shared secret (entered again). |

Creating AAA RADIUS Accounting Server (Optional)

TABLE 10 Fields/Values to Use for ZoneDirector AAA Accounting Service

| Configuration Field | Corresponding Value |
|---------------------|---|
| Name | Name: Any descriptive name for the AAA accounting service |
| Type | RADIUS ACCOUNTUING |
| Auth Method | PAP |
| IP Address | The IP address of the Cloudpath Enrollment System. |
| Port | 1813 is typically used and is the default. |
| Shared Secret | This must match the shared secret for the Cloudpath ES onboard RADIUS server (Configuration > RADIUS Server). |
| Confirm Secret | Confirm Secret: The shared secret (entered again). |

Testing AAA Servers

To test the connection between the controller and the Cloudpath RADIUS server, RUCKUS strongly recommends testing the AAA server after you set it up. Refer to the instructions in the *RUCKUS ZoneDirector User Guide*.

Creating a Hotspot (WISPr) Portal

TABLE 11 Fields/Values to Use for Creating a Hotspot (WISPr) Portal

| Creating a Hotspot (WISPr) Portal section in ZoneDirector UI | Configuration Field and Corresponding Value |
|--|--|
| Top portion of configuration fields area | Name: Any descriptive name for the hotspot portal. |
| Redirection | Login URL: Select "External." |
| | Login Page Redirect unauthenticated user: The Cloudpath Enrollment Portal URL, which should be contained in the applicable workflow in the Cloudpath UI (Configuration > Workflows). |
| | Start Page After user is authenticated,: Select "Redirect to the URL that the user intends to visit." This lets you set a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address for the redirection. |
| Authentication/Accounting Servers (Authentication tab) | Authentication Server: Drop-down list to select the Cloudpath RADIUS Authentication Server. NOTE Enabling this option allows users with registered MAC addresses to be transparently authorized without having to log in. A user entry on the RADIUS server needs to be created using the client MAC address as both the user name and password. For the MAC address format, RUCKUS recommends using AA:BB:CC:DD:EE:FF. |
| Authentication/Accounting Servers (Authentication tab) | Accounting Server: Drop-down list to select the Cloudpath RADIUS Accounting Server (if applicable). |

Setting Up the Walled Garden

To add a walled garden configuration to your existing Hotspot Services, refer to the instructions in the *RUCKUS ZoneDirector User Guide*.

Also, when configuring the walled garden, include the following steps:

1. Include the DNS or IP address of the Cloudpath system, then click **OK**
2. 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.

NOTE

There will still be about a 15-to-20-second delay when the full application is 33 percent complete (about 40 MB) in its download.

The recommended destinations to add for the walled garden are:

```
*.ggpht.com
*.play.googleapis.com
*.googleapis.com
*.play.google.com
android.clients.google.com
*.gvtl.com
connectivitycheck.android.com
connectivitycheck.google.com
*.gstatic.com
*.clients3.google.com
*.thawte.com
```

NOTE

The *thawte.com destination is the OSCP URL of the SSL certificate of the Cloudpath server. This URL can be found by clicking the *lock* icon in your web browser and viewing the details of your certificate.

- If you are still experiencing issues, you can try adding the following destinations to the walled garden:

```
*.clients.google.com
*.l.google.com
*.googleusercontent.com
*.appengine.google.com
*.cloud.google.com
*.android.com
*.cloudfront.net
*.akamaihd.net
172.217.0.0/16
216.58.0.0/16
```

Creating the Onboarding SSID

TABLE 12 Fields/Values to Use for ZoneDirector Onboarding SSID

| Creating a WLAN Configuration (for Onboarding SSID) section in ZoneDirector UI | Configuration Field and Corresponding Value |
|--|--|
| General Options | Name/ESSID: Name of the SSID |
| | Zone: Zone in which the WLAN will reside |
| WLAN Usages | Type: Hotspot (WISPr) |
| Authentication Options | Method: Open |
| Encryption Options | Method: None |
| Options | Hotspot Services Drop-down list to select the already-created hotspot service. |

NOTE

RUCKUS recommends enabling the "Bypass Apple CNA" feature. For instructions, refer to the *RUCKUS ZoneDirector User Guide*.

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.

- Name the SSID.
- Type=Standard Usage.
- Authentication Option Method=802.1x EAP.
- Encryption Option Method=WPA2 (not applicable for Unleashed once the 802.1x EAP authentication option method is selected).
- Encryption Option Algorithm=AES (not applicable for Unleashed once the 802.1x EAP authentication option method is selected).
- Select the Cloudpath RADIUS authentication server.
- 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 1 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 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)
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.

(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 2 Select RADIUS Accounting Server on ZoneDirector

The screenshot displays the 'Advanced Options' configuration window for a RADIUS Accounting Server. The settings are as follows:

- Accounting Server:** Jeff AAA acct (dropdown), Create New button, Send Interim-Update every 10 minutes.
- Access Control:** L2/MAC (dropdown), No ACLs (dropdown), Create New button.
- L3/4/IP address:** No ACLs (dropdown), Create New button.
- Device Policy:** None (dropdown), Create New button.
- Precedence Policy:** Default (dropdown), Create New button.
- 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 Disabled (dropdown), Per Station Downlink Disabled (dropdown).
- SSID Rate Limiting:** Uplink Enable 0 mbps (0.1~200), DownLink Enable 0 mbps (0.1~200).

A red warning message at the bottom states: "Per STA rate limiting will not work if SSID rate limiting is enabled." The window includes OK and Cancel buttons at the bottom right.

FIGURE 3 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 WFP: 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 v5Z [+ Create](#)
- Accounting Service: Use the controller as proxy
Jeff AAA Acct v5Z [+ 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 4 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.



© 2022 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>