ADMINISTRATION GUIDE

Cloudpath ES for Hotspot 2.0 (Passpoint) Release 1 Configuration Guide

Supporting Cloudpath 5.2

Part Number: 800-72125-001 Rev A
Publication Date: 03 January 2019

Copyright, Trademark and Proprietary Rights Information

© 2019 ARRIS Enterprises LLC. All rights reserved.

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

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. ARRIS does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. ARRIS does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to ARRIS that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF ARRIS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, 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

Preface **5**
Document Conventions 5
Notes, Cautions, and Warnings 5
Command Syntax Conventions 6
Document Feedback 6
Ruckus Product Documentation Resources 6
Online Training Resources 7
Contacting Ruckus Customer Services and Support 7
What Support Do I Need? 7
Open a Case 7
Self-Service Resources 7

Hotspot 2.0 Release 1 Overview **9**

Hotspot 2.0 Release 1 Controller Configuration **11**
Controller Information 11
Configuring Hotspot 2.0 Release 1 Wi-Fi Operator Profile 11
Configuring Hotspot 2.0 Release 1 Identity Provider 12
Network Identifier Tab 13
Creating the Identity Provider - Authentication Tab 16
Creating the Identity Provider - Accounting Tab 19
Creating the Identity Provider - Review Tab 21
Creating a Hotspot Portal for Hotspot 2.0 Release 1 22
Configuring an Onboarding SSID for Hotspot 2.0 R1 24
Creating a Hotspot 2.0 WLAN Profile 26
Configuring a Secure SSID for Hotspot 2.0 R1 28

Configuring Hotspot 2.0 Release 1 on Cloudpath **31**
Creating a Hotspot 2.0 Release 1 Device Configuration 31
Adding a Hotspot 2.0 Release 1 branch to the Workflow 35
Adding a Device Configuration to the Workflow 37
Configuring the Certificate Template 38
Testing the Hotspot 2.0 Release 1 User Experience 39

Preface

- Document Conventions 5
- Command Syntax Conventions 6
- Document Feedback 6
- Ruckus Product Documentation Resources 6
- Online Training Resources 7
- Contacting Ruckus Customer Services and Support 7

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *Ruckus Small Cell Release Notes* for more information.

Notes, Cautions, and Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document Feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at ruckus-docs@arris.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- Ruckus SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

Ruckus Product Documentation Resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a Ruckus Support Portal user account. Other technical documentation content is available without logging in to the Ruckus Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

Online Training Resources

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at https://training.ruckuswireless.com.

Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Ruckus Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The Ruckus Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents

- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Hotspot 2.0 Release 1 Overview

Hotspot 2.0 (HS 2.0), often referred to as Wi-Fi Certified Passpoint, is the new standard for Wi-Fi public access that automates and secures the connection.

The focus of Release 1 is over-the-air security and network discovery and selection. The main enabling protocols are IEEE 802.11u, along with IEEE 802.1X, selected EAP methods, and IEEE 802.11i. Release 1 uses the WPA2-Enterprise certification program in the Wi-Fi Alliance.

The IEEE 802.11u protocol allows a mobile device to have a dialog with a Wi-Fi AP "pre-association" to determine the capabilities that the network can support. The two protocols that 802.11u uses to make this happen are the generic advertisement service (GAS) and the access network query protocol (ANQP). These protocols run on top of 802.11 and enable the Hotspot 2.0 experience.

Supported Devices:

Hotspot 2.0 Release 1 can be used with iOS devices running iOS 7 and later versions.

Main Steps:

The following is a list of the main steps you need to perform to configure Hotspot 2.0 Release 1 on your vSZ controller and your Cloudpath system:

1. Configuring Hotspot 2.0 Release 1 Wi-Fi Operator Profile on page 11: This profile defines all the properties pertaining to an operator. You configure the domain of your Cloudpath system here. This profile will later be linked to a WLAN profile.
2. Configuring Hotspot 2.0 Release 1 Identity Provider on page 12: This profile is where you enter network-identifying information such as Network Access Identifier (NAI) realms, and also where you can add authentication and accounting servers. This profile will also later be linked to a WLAN profile.
3. Creating a Hotspot Portal for Hotspot 2.0 Release 1 on page 22: This is where you create a captive hotspot portal to send unauthenticated users for Cloudpath enrollment.
4. Configuring an Onboarding SSID for Hotspot 2.0 R1 on page 24: This is the open, wireless LAN that you create for users to begin their onboarding process.
5. Creating a Hotspot 2.0 WLAN Profile on page 26: This profile is where you select the previously configured Wifi Operator and Identity Provider profiles.
6. Configuring a Secure SSID for Hotspot 2.0 R1 on page 28: This is the secure network you create to which Cloudpath users will be connected upon successful authentication and enrollment.
7. Configuring Hotspot 2.0 Release 1 on Cloudpath on page 31: This is the configuration you must perform on the Cloudpath UI to successfully link the Hotspot 2.0 Release 1 configuration you performed on the controller to a Hotspot 2.0 Release 1 Cloudpath workflow.

Hotspot 2.0 Release 1 Controller Configuration

- Controller Information....11
- Configuring Hotspot 2.0 Release 1 Wi-Fi Operator Profile....11
- Configuring Hotspot 2.0 Release 1 Identity Provider....12
- Creating a Hotspot Portal for Hotspot 2.0 Release 1....22
- Configuring an Onboarding SSID for Hotspot 2.0 R1....24
- Creating a Hotspot 2.0 WLAN Profile....26
- Configuring a Secure SSID for Hotspot 2.0 R1....28

Controller Information

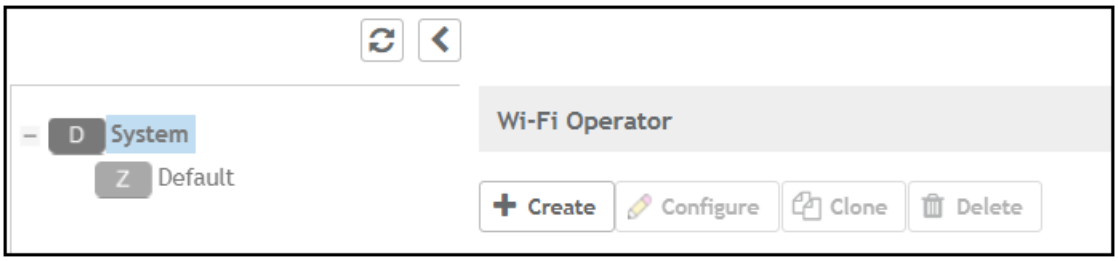
Hotspot 2.0 Release 1 is supported on the Ruckus Virtual SmartZone (vSZ) controller, version 3.2.1.0.245 and above. The configuration described here is for version 3.6.0. If you are running a different version of vSZ, refer to your controller documentation for differences.

Configuring Hotspot 2.0 Release 1 Wi-Fi Operator Profile

A Wi-Fi operator profile is required for Hotspot 2.0 Release 1.

1. Navigate to **Configuration > Services & Profiles > Hotspots & Portals**, then click the **Hotspot 2.0** tab.
2. Be sure that "System" is highlighted:

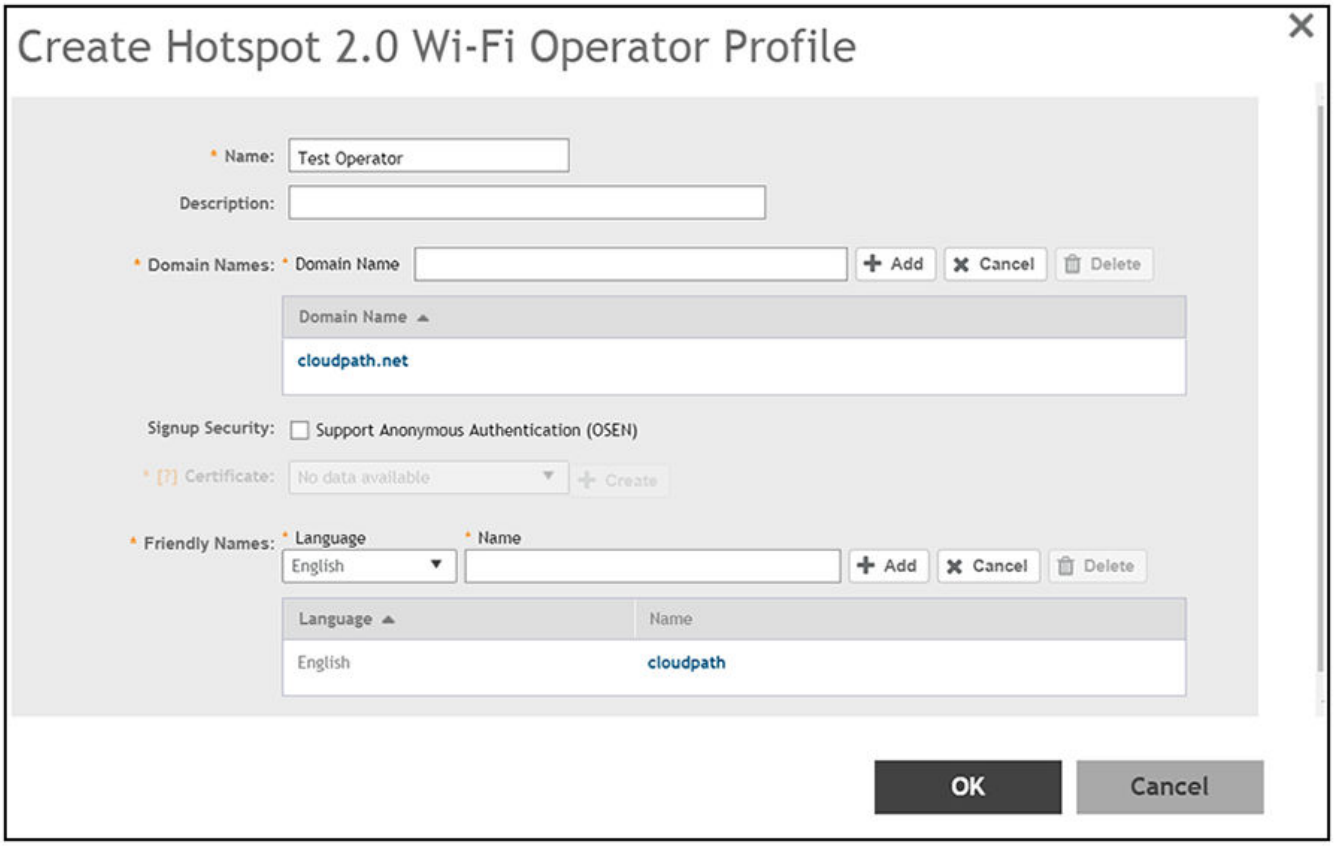
FIGURE 1 Highlighting the "System" Area Before Creating Wi-Fi Operator Profile



3. Under "WiFi Operator," click **Create**.

   The Create Hotspot 2.0 WiFi Operator Profile screen appears. An example of how you can configure this screen follows:

   FIGURE 2 Hotspot 2.0 Wi-Fi Operator Profile Screen



4. In the Name field, enter a descriptive name of your choice.
5. In the Domain Name field, enter the domain name of your Cloudpath system, then click **Add**. You can repeat this process to add multiple domain names.
6. For Friendly Names, select a Language, then enter the Friendly Name for the Cloudpath system and click **Add**. You can enter multiple languages for the same Friendly Name.
7. Click **OK**.

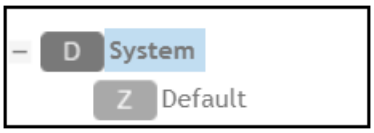
Configuring Hotspot 2.0 Release 1 Identity Provider

An identity provider is required for Hotspot 2.0 Release 1.

1. Navigate to **Configuration > Services & Profiles > Hotspots & Portals** , then click the **Hotspot 2.0** tab.

2. Be sure that "System" is highlighted:

   FIGURE 3 Highlighting "System" Before Creating Identity Provider Profile



3. Under the "Identity Provider" section of the screen, click **Create**.

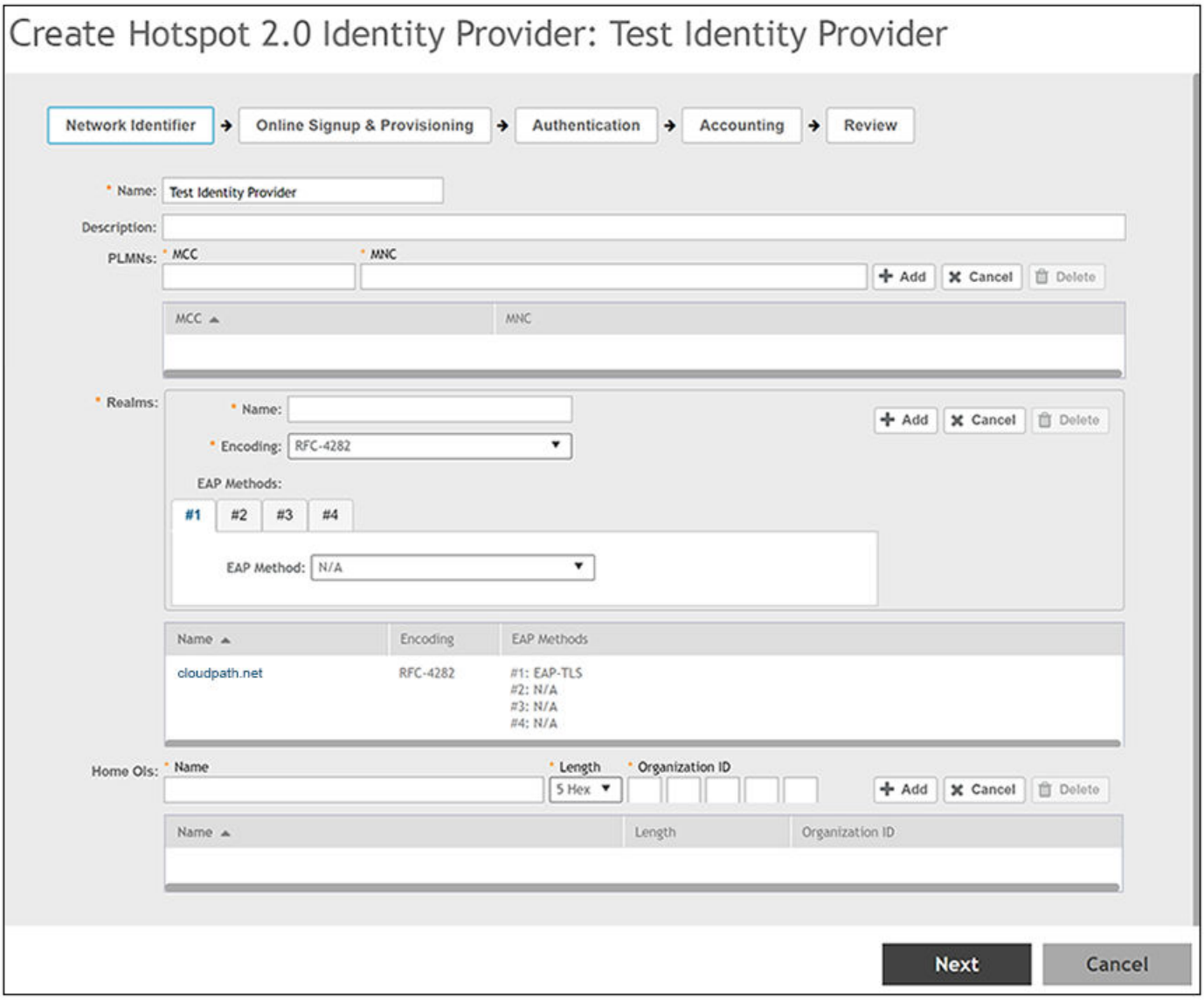
   The Create Hotspot 2.0 Identity Provider screen appears. The Hotspot Identity Provider screen consists of the following tabs, as shown in Figure 4 on page 14:

   - Network Identifier
   - Online Signup & Provisioning
   - AAA Authentication
   - AAA Accounting
   - Review

Network Identifier Tab

The Network Identifier tab of the Identity Provider screen is shown below, with an example configuration.

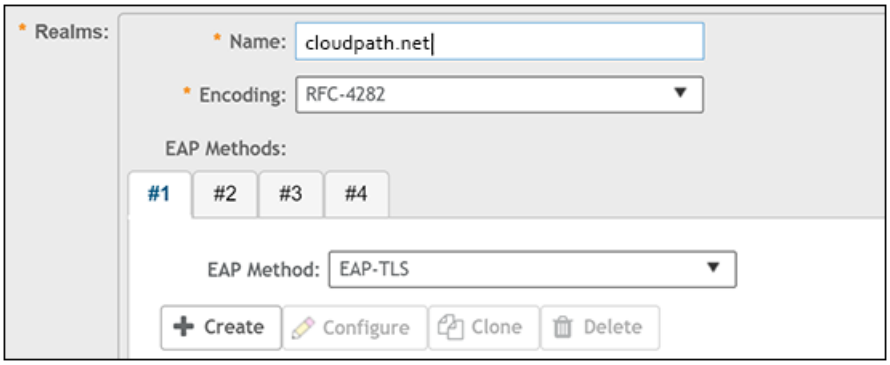
FIGURE 4 Creating the Identity Provider - Network Identifier Tab



1. In the Name field, enter a descriptive name for the identity provider.
2. The MCC and MNC fields can be left blank.

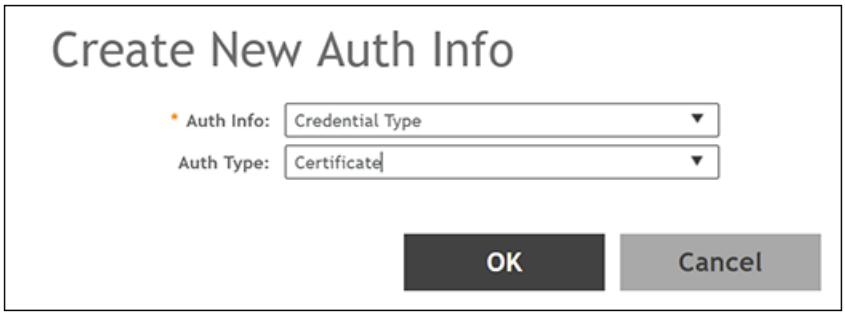
3. In the Realms section, do the following to create a Network Access Identifier (NAI) realm :
   a) Enter the name of the realm for the Cloudpath system.
   b) From the Encoding drop-down list, select RFC-4282.
   c) From the EAP Method drop-down list, select EAP-TLS for the identity provider. You can enter multiple EAP methods for the same realm.
   d) Click **Create** (see the following figure):

   FIGURE 5 Configuring a Realm



   e) In the ensuing Create New Auth Info screen, select "Credential Type" from the Auth Info drop-down list, and select "Certificate" from the Auth Type drop-down list:

   FIGURE 6 Selecting Auth Info and Auth Type for Realm



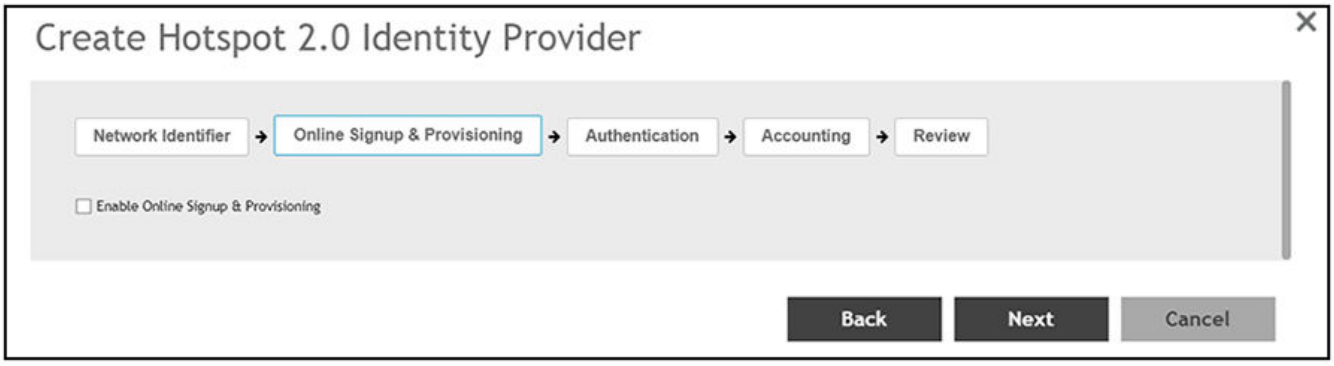
   f) Click **OK**.
   g) Click **Add** to add the realm to the list of configured realms.

   You can repeat this step to add additional realms. As many as 16 NAI realm entries can be created. Each NAI realm entry can contain up to four EAP methods.
4. Home OIs can be left blank.

5. Click **Next** to apply the configuration and continue to Online Signup & Provisioning.

   The following screen appears:

FIGURE 7 Do Not Enable Checkbox for Online Signup & Provisioning



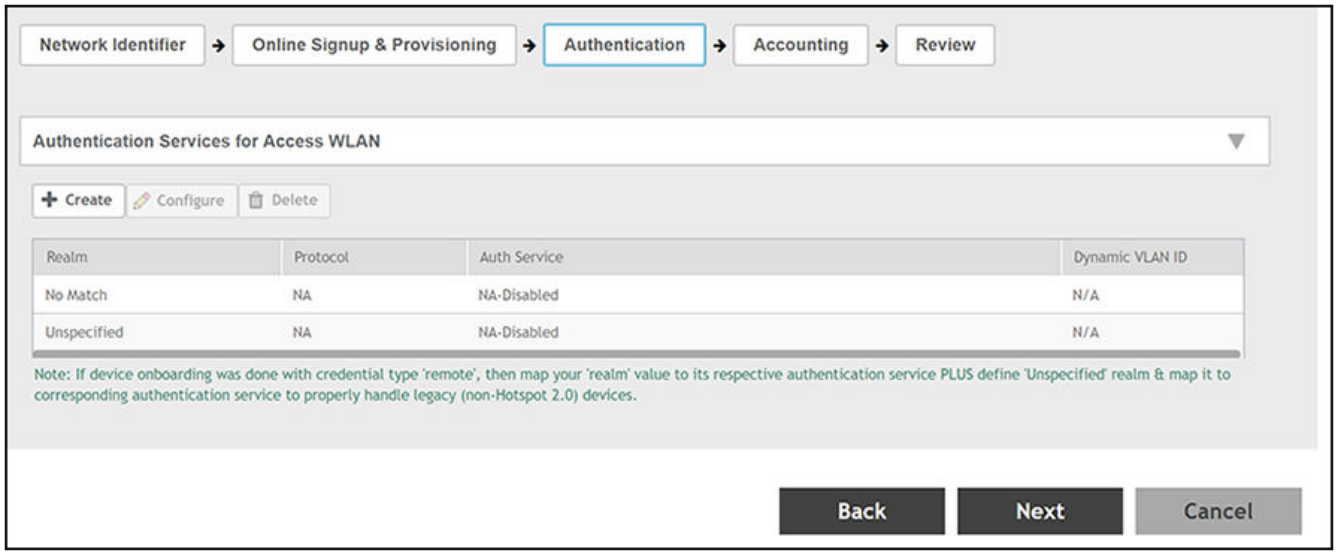
6. *Do not* check the Enable Online Signup & Provisioning box; click **Next** and continue to the **Authentication** tab.

Creating the Identity Provider - Authentication Tab

Add an authentication server during the Identity Provider configuration process by following these steps:

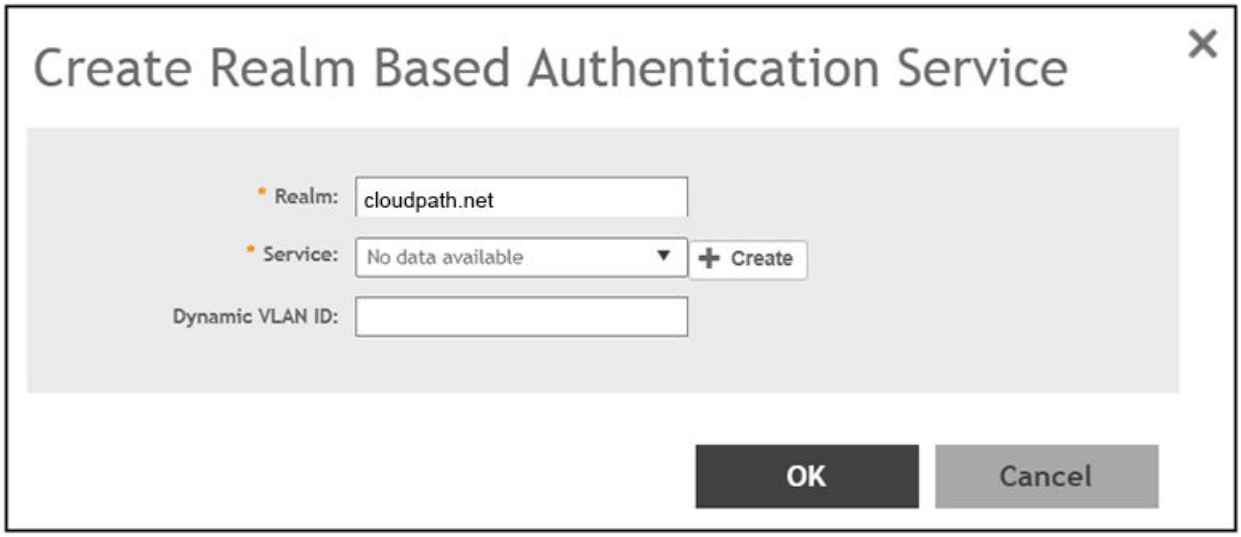
1. From the Authentication tab (see screen below), click **Create**.

FIGURE 8 Authentication Tab



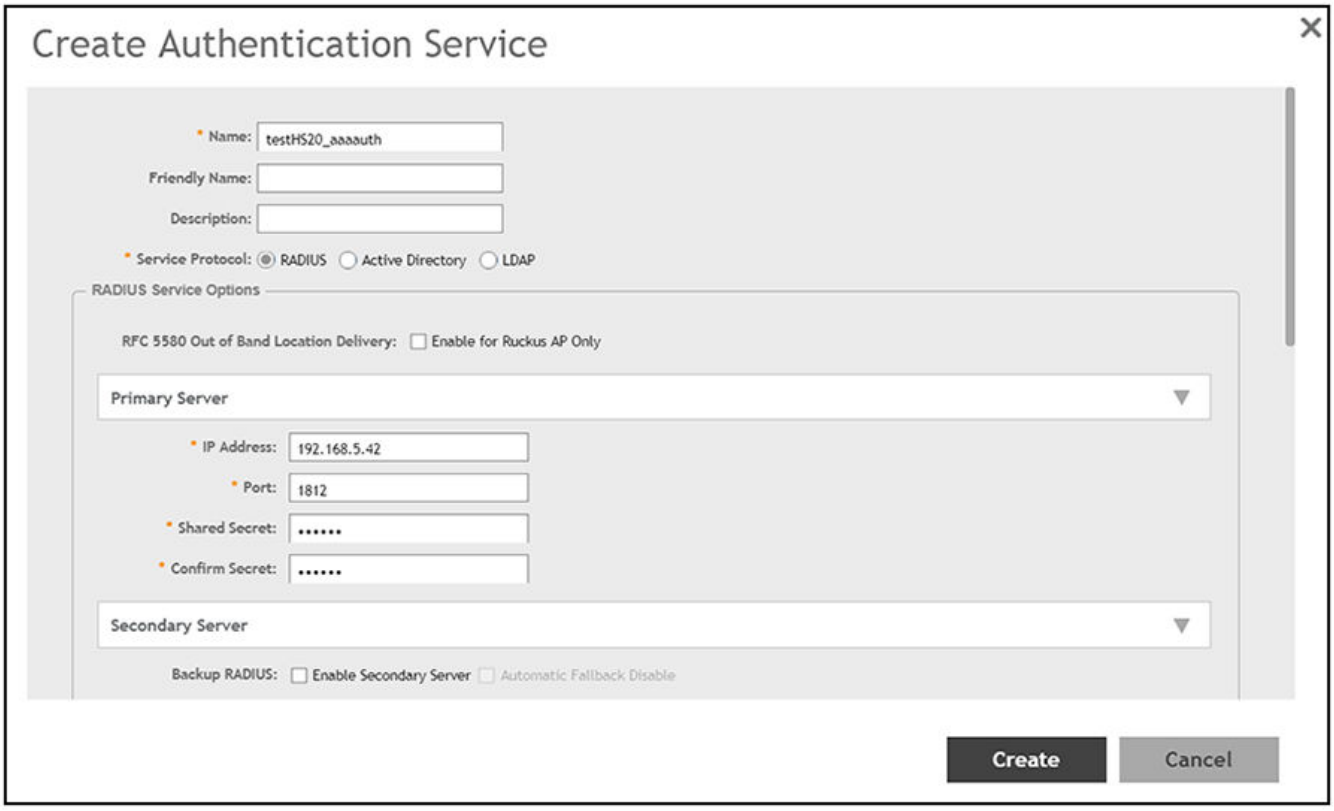
2. In the Create Realm Based Authentication Service screen, enter the name of the Realm, then click **Create**.

FIGURE 9 Creating Authentication Service for Realm



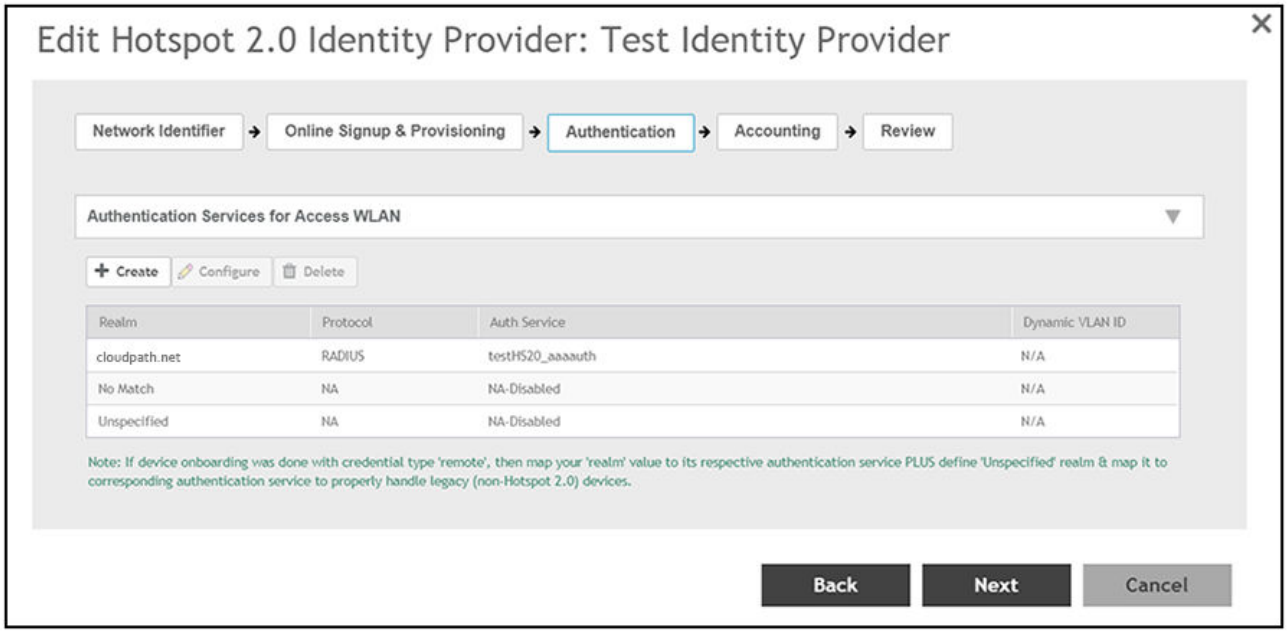
3. Configure the Create Authentication Service screen, as shown in the following example:

FIGURE 10 Configuring the Authentication Service



a) In the Name field, enter a descriptive name of your choice.
b) For Service Protocol, the radio button selected must be RADIUS.
c) In the IP Address field, enter the IP address of the Cloudpath system.
d) In the Port field, enter 1812.
e) The Shared Secret and Confirm Secret fields must match the shared secret for the Cloudpath onboard RADIUS server (the navigation path on your Cloudpath system is **Configuration > RADIUS Server**).
f) You can use the default values for remaining fields, then click **Create**.
g) When you are returned to the Create Realm Based Authentication Service screen, click **OK**.
h) The new authentication server should now appear in the "Authentication Services for Access WLAN" list.

FIGURE 11 Authentication Services List Displaying Newly Created Service



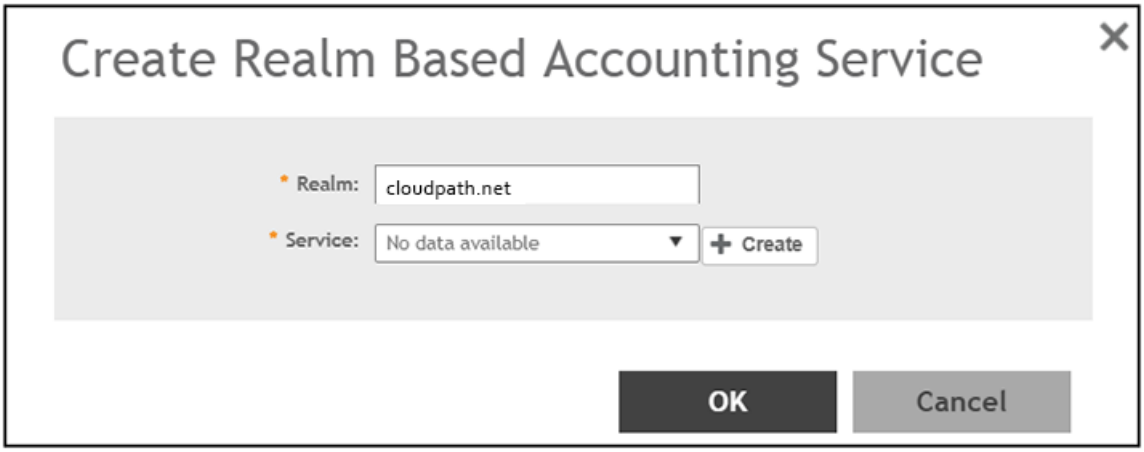
4. Click **Next** to proceed to the Accounting tab.

Creating the Identity Provider - Accounting Tab

Optionally, you can add an Accounting server during the Identity Provider configuration process by following these steps:

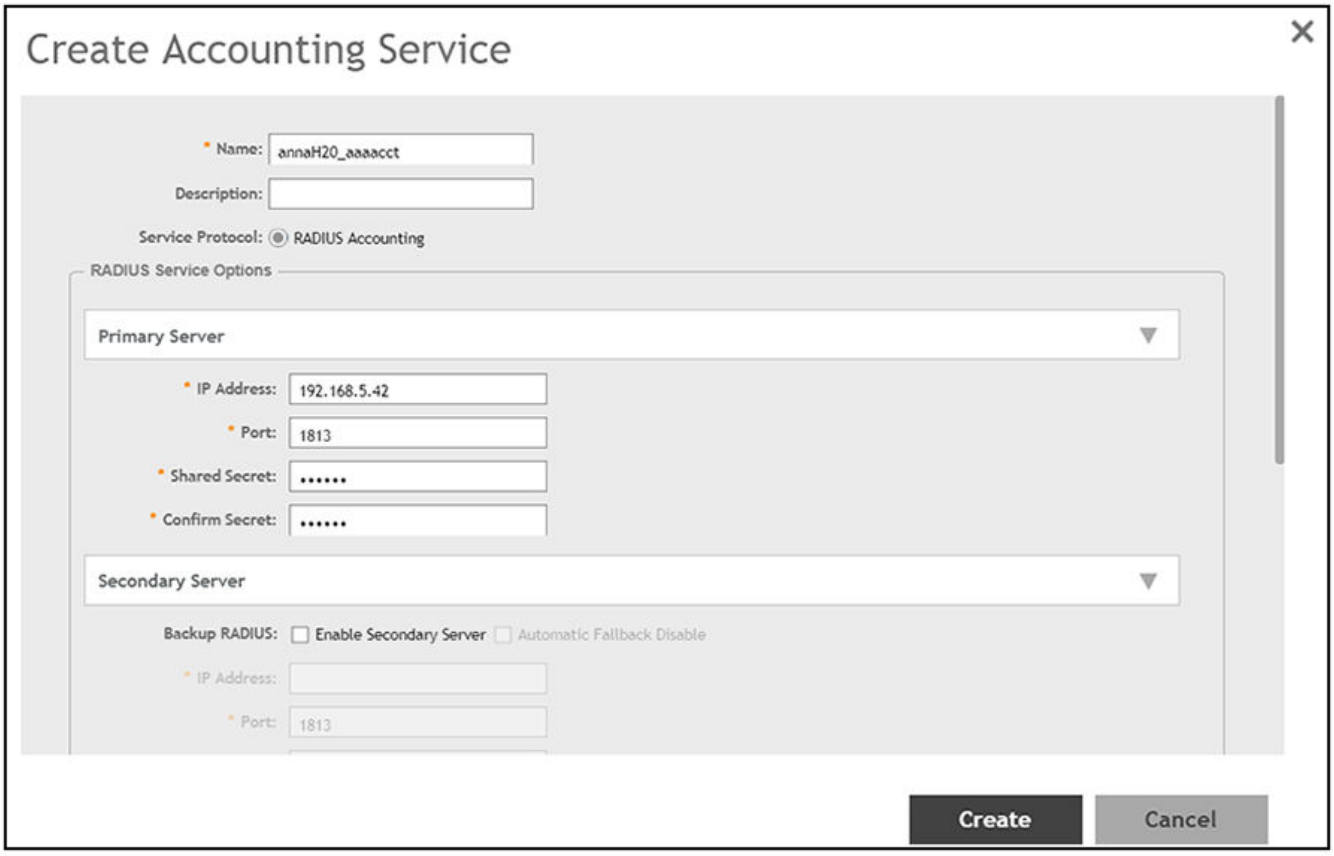
1. From the Accounting tab, check the **Enable Accounting** box.
2. Click **Create**.
3. In the Create Realm Based Accounting Service screen, enter the name of the Realm, then click **Create**.

FIGURE 12 Creating Accounting Service for Realm



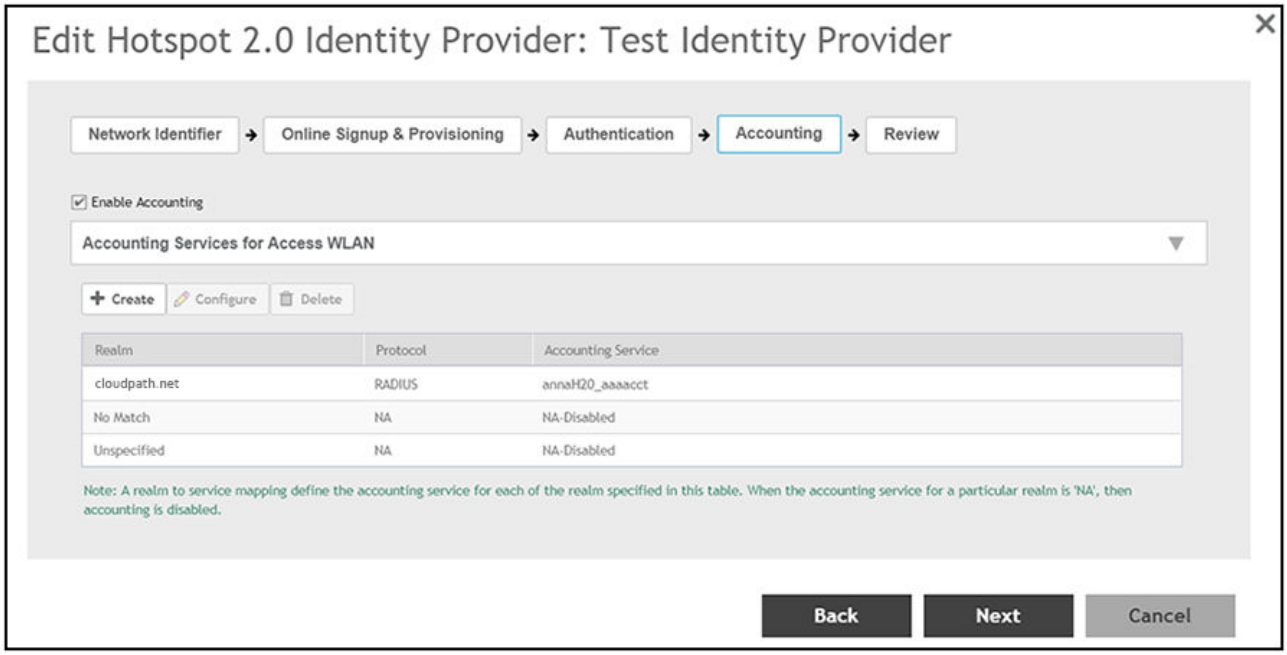
4. Configure the Create Accounting Service screen, as shown in the following example:

FIGURE 13 Configuring the Accounting Service



a) In the Name field, enter a descriptive name of your choice.
b) For Service Protocol, the radio button selected must be RADIUS Accounting.
c) In the IP Address field, enter the IP address of the Cloudpath system.
d) In the Port field, enter 1813.
e) The Shared Secret and Confirm Secret fields must match the shared secret for the Cloudpath onboard RADIUS server (the navigation path on your Cloudpath system is **Configuration > RADIUS Server**).
f) You can use the default values for remaining fields, then click **Create**.
g) When you are returned to the Create Realm Based Authentication Service screen, click **OK**.
h) The new Accounting server should now appear in the "Accounting Services for Access WLAN" list:

FIGURE 14 Accounting Services List Displaying Newly Created Service



5. Click **Next** to proceed to the Review tab.

Creating the Identity Provider - Review Tab

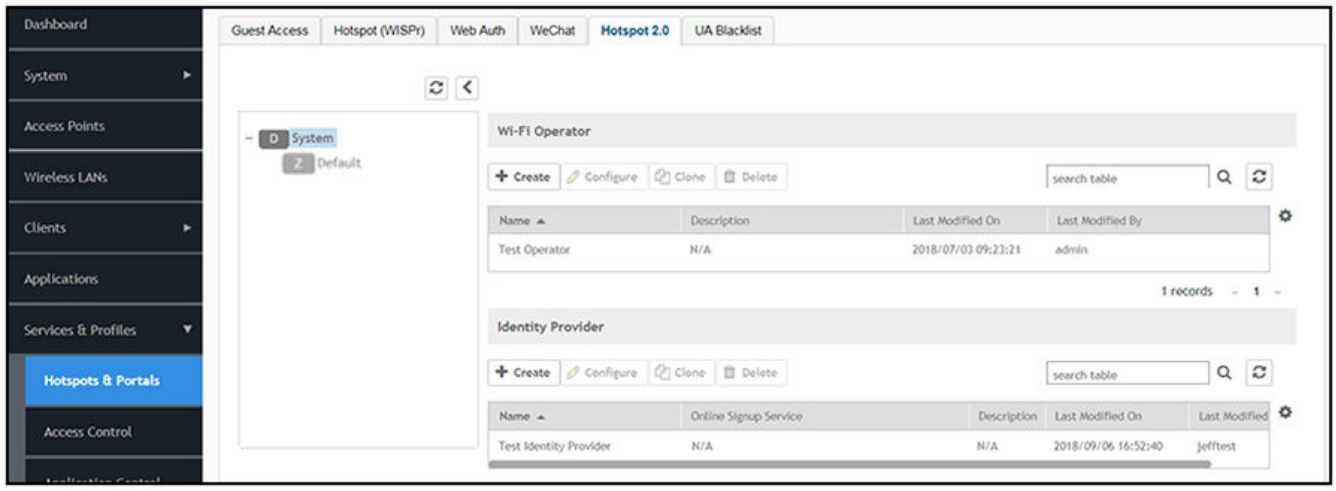
Use the Review tab to check all your previous steps.

1. If any of the information shown when you click on the Review tab needs to be changed, click the applicable tab to reconfigure any information, then return to the Review tab.

2. After you have checked all configuration information displayed in the Review tab, click **OK**.

   If you receive no error messages, the configuration of the Identity Provider is submitted to the controller, and you are returned to the main Hotspot 2.0 screen, as shown in the following example screen:

FIGURE 15 Main Hotspot 2.0 Screen After WiFi Operator and Identity Provider are Configured

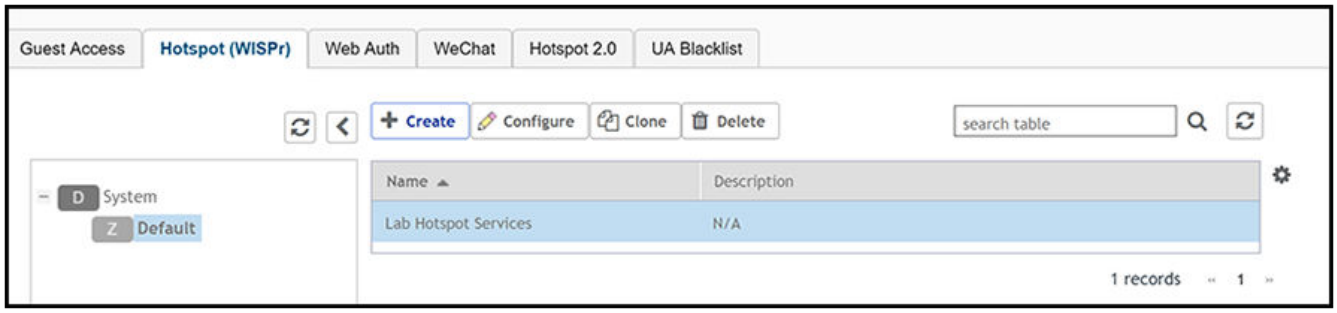


Creating a Hotspot Portal for Hotspot 2.0 Release 1

A hotspot portal is required for Hotspot 2.0 Release 1.

1. In the Controller UI, be sure to navigate to **Configuration > Services & Profiles > Hotspots & Portals**, then click the **Hotspot (WISPr)** tab.
2. Be sure to highlight the zone in which you wish to create the hotspot portal. (You cannot highlight "System" to create the hotspot portal.) In the example below, the Default zone is used.

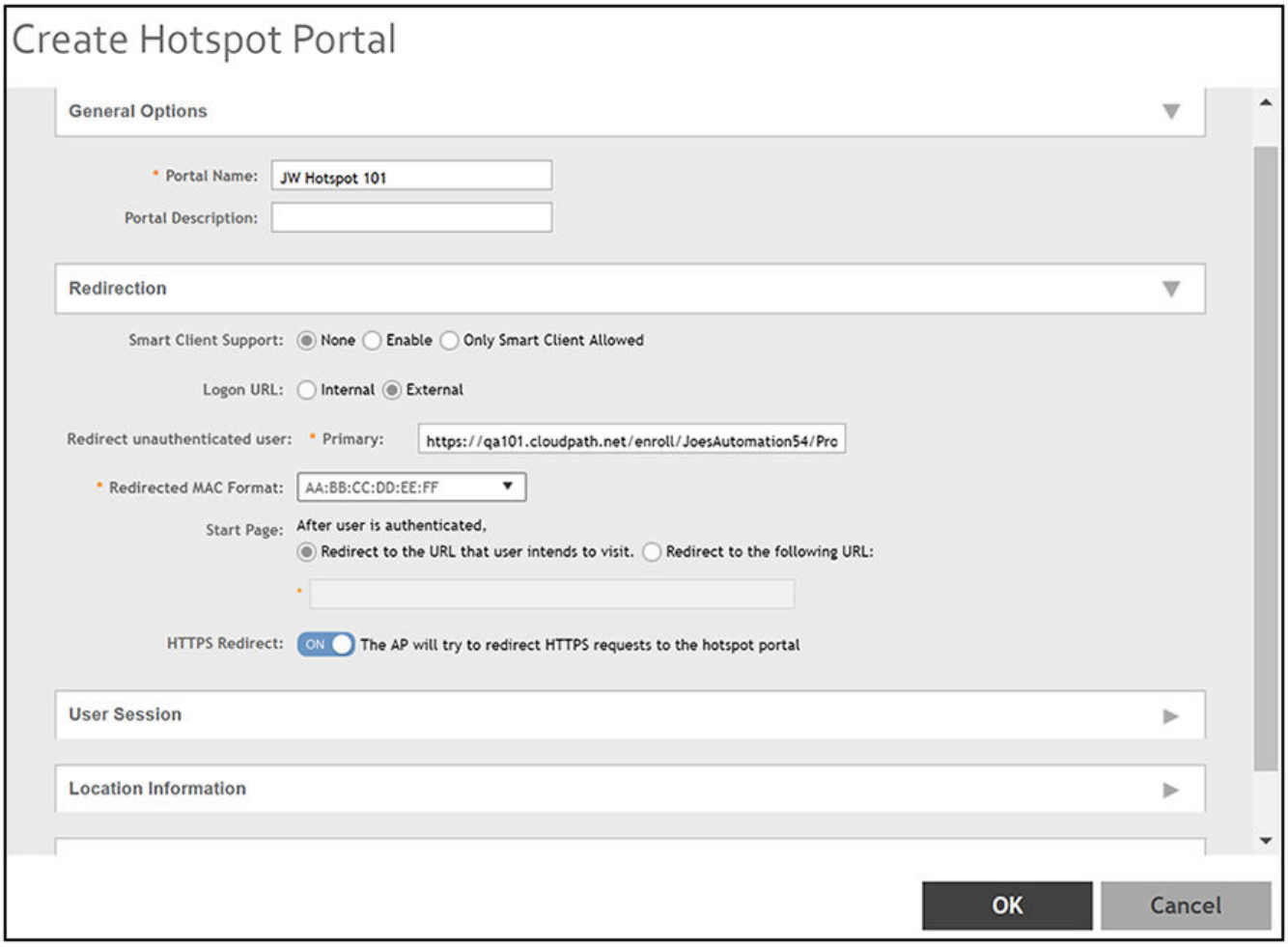
FIGURE 16 Highlighting the Zone Before Creating the Hotspot Portal



3. Click **Create**.

   The Create Hotspot Portal screen appears. An example of how you configure this screen follows:

   FIGURE 17 Creating a Hotspot Portal



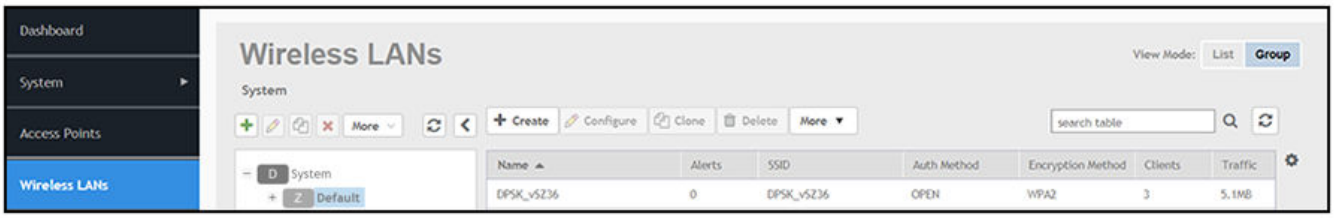
4. In the Name field, enter a descriptive name for the hotspot portal.
5. For the Smart Client Support field, select None.
6. For the Login URL field, select External.
7. In the Redirect unauthenticated user field, enter the URL to which you want to send an unauthenticated user. This is the URL that the user will be taken to begin the Cloudpath enrollment process. To find this URL, on your Cloudpath system go to **Configuration > Workflows**, then click the **Advanced** tab. Copy the Enrollment Portal URL from there and paste it into the **Redirect unauthenticated user** field in the screen shown above on your vSZ controller.
8. For the Start Page field, be sure that the radio button called "Redirect to the URL that user intends to visit." is selected.
9. Use the default values for the remaining fields, then click **OK**.

Configuring an Onboarding SSID for Hotspot 2.0 R1

An onboarding SSID is required for Hotspot 2.0 Release 1.

1. In the Controller UI, go to Wireless LANs.
2. Be sure to highlight the zone where you want to add the onboarding SSID. This example uses the Default zone.

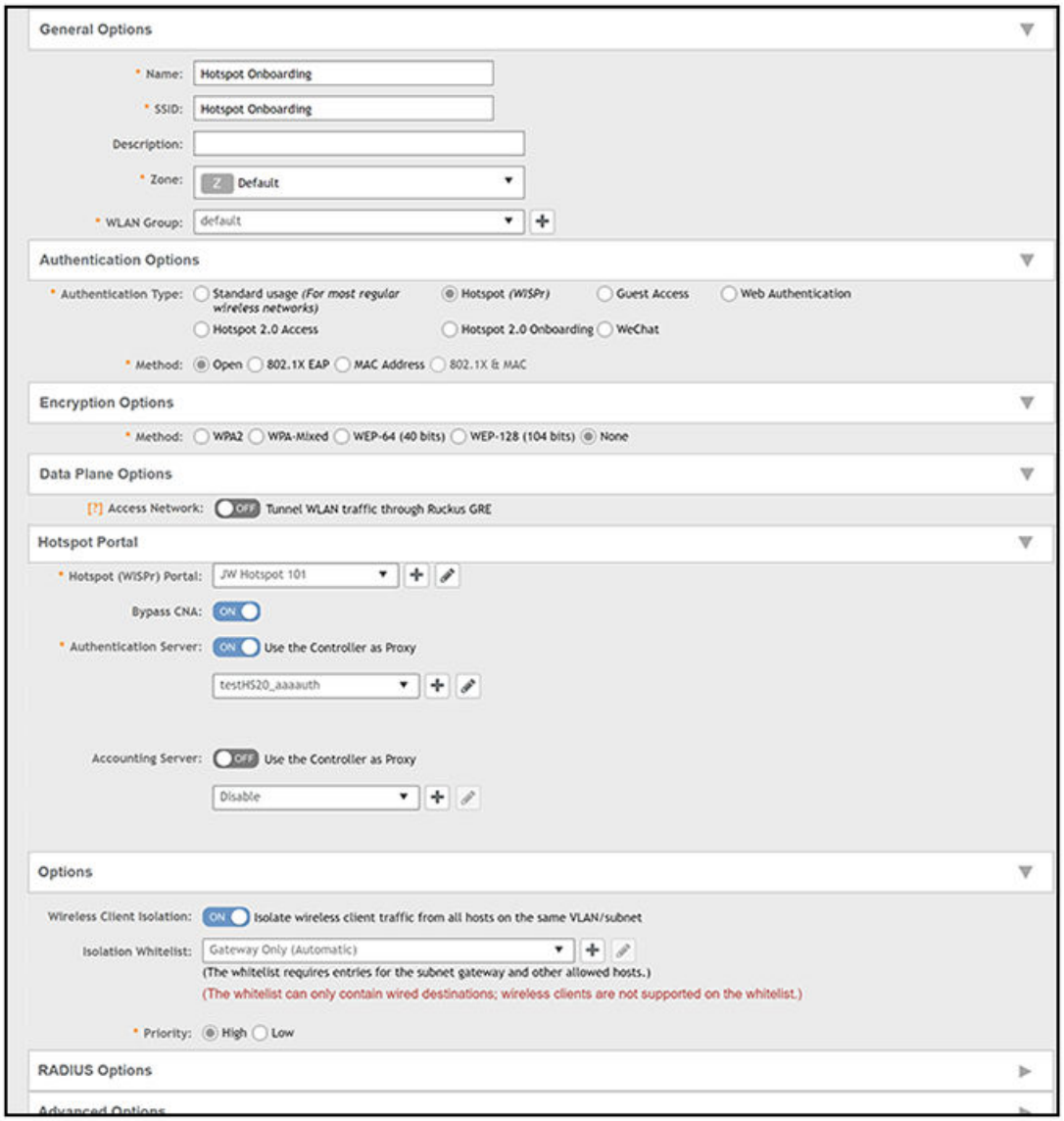
FIGURE 18 Highlighting the Zone in Which to Create the Onboarding SSID



3. Click **Create**.

   The Create WLAN Configuration screen appears. An example of how you configure this screen follows:

FIGURE 19 Creating a Hotspot 2.0 Onboarding SSID



4. In the Name field, enter a descriptive name for the onboarding SSID.
5. From the Zone drop-down list, make sure the correct zone for your onboarding SSID is selected.
6. From the WLAN Group drop-down list, make sure that you select the WLAN group where the onboarding SSID resides.
7. For Authentication Type, select Hotspot (WISPr).
8. For Authentication Method, select Open.
9. For Encryption Method, select None.
10. From the Hotspot (WISPr) Portal drop-down list, select the hotspot portal you previously configured.

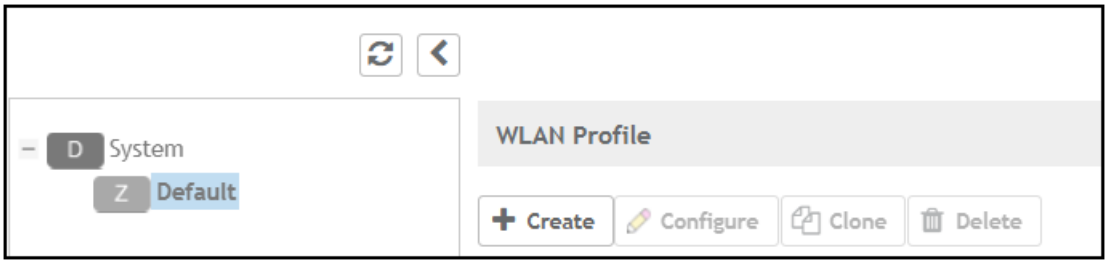
11. For the Authentication Server, be sure the corresponding button is ON, then select the authentication server from the drop-down list that you configured while you were setting up the Identity Provider.
12. For the Accounting Server, you can optionally set the corresponding button is ON, then select the accounting server from the drop-down list if you configured one while you were setting up the Identity Provider.
13. Use the default values for the remaining fields, and click **OK**.

Creating a Hotspot 2.0 WLAN Profile

A WLAN Profile is required for Hotspot 2.0 Release 1.

1. In the Controller UI, be sure to navigate to **Configuration > Services & Profiles > Hotspots & Portals**, then click the **Hotspot 2.0** tab.
2. Be sure to highlight the zone where you want this profile to reside. (You cannot create the WLAN profile with "System" highlighted.) The example below uses the Default zone.

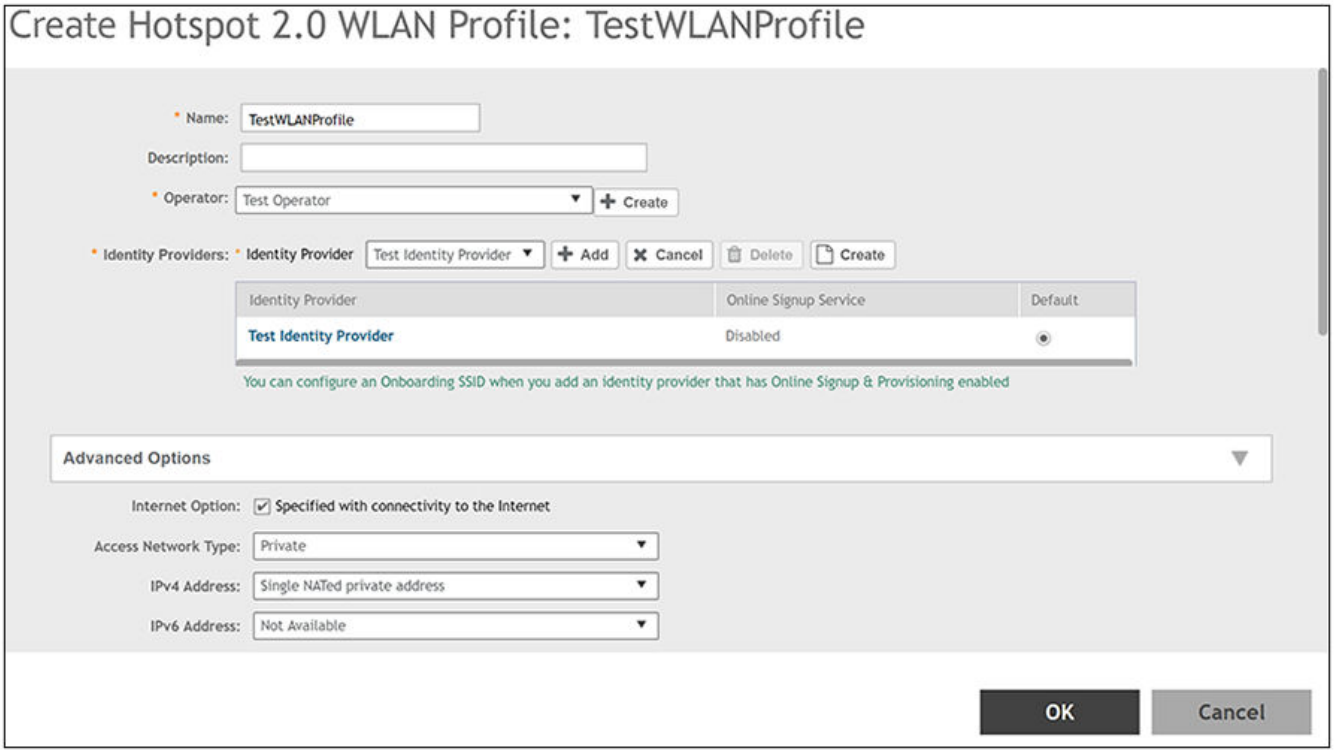
FIGURE 20 Highlighting the Zone Before Creating the Hotspot 2.0 WLAN Profile



3. In the WLAN Profile section of the screen (shown above), click **Create**.

   The Create Hotspot 2.0 WLAN Profile screen appears. An example of how you configure this screen follows:

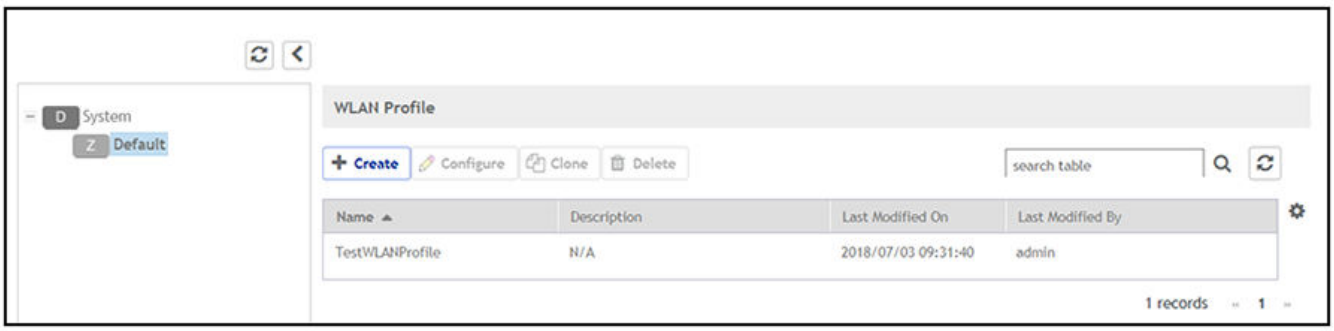
FIGURE 21 Creating a Hotspot 2.0 WLAN Profile



4. In the Name field, enter a descriptive name for the profile.
5. In the Operator field, use the drop-down list to select the previously configured Wi-Fi Operator.
6. In the Identity Providers field, use the drop-down list to select the previously configured Identity Provider, then click **Add**.
7. Use the default values for the remaining fields, then click **OK**.

   The WLAN profile should now appear in the list of configured WLAN profiles:

FIGURE 22 WLAN Profiles List



Configuring a Secure SSID for Hotspot 2.0 R1

A secure SSID is required for Hotspot 2.0 Release 1.

1. In the Controller UI, go to Wireless LANs.
2. Be sure to highlight the Zone in which you want to the Secure SSID to reside. This example uses the Default zone.

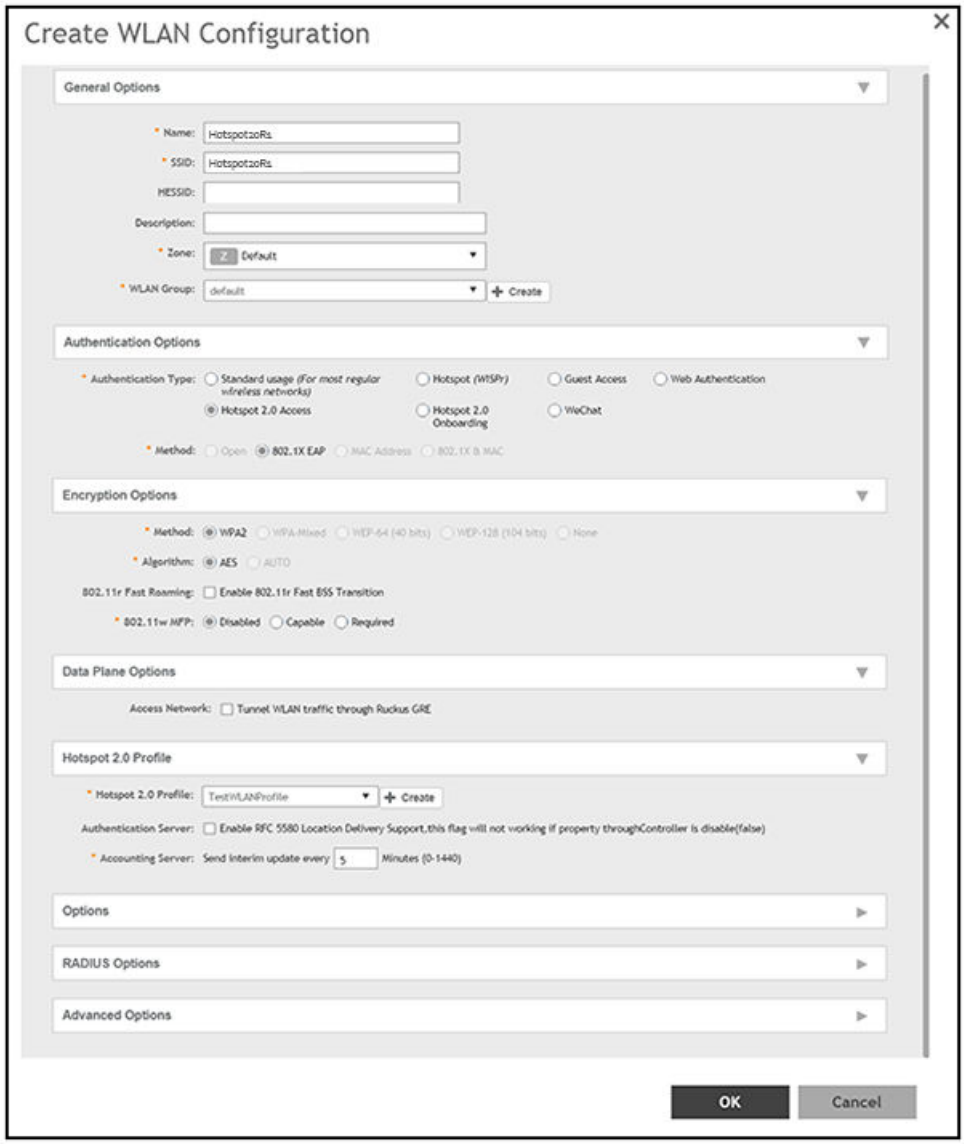
FIGURE 23 Highlighting the Zone in Which to Create the Secure SSID



3. Click **Create**.

   The Create WLAN Configuration screen appears. An example of how you configure this screen follows:

FIGURE 24 Creating a Hotspot 2.0 Secure SSID



4. In the Name field, enter a descriptive name for the secure SSID.
5. From the Zone drop-down list, be sure that the zone where the Secure SSID resides is selected.
6. From the WLAN Group drop-down list, select the WLAN group where the Secure SSID resides.
7. For Authentication Type, select Hotspot 2.0 Access.
8. For Authentication Method, select 802.1x EAP.
9. For Encryption Method, select WPA2.
10. For Encryption Algorithm, select AES.

11. For the Hotspot 2.0 profile, use the drop-down list to select the previously configured Hotspot 2.0 profile.
12. Use the default values for the remaining fields, and click **OK**.

    The secure SSID should now appear in the list of configured wireless LANs.

Configuring Hotspot 2.0 Release 1 on Cloudpath

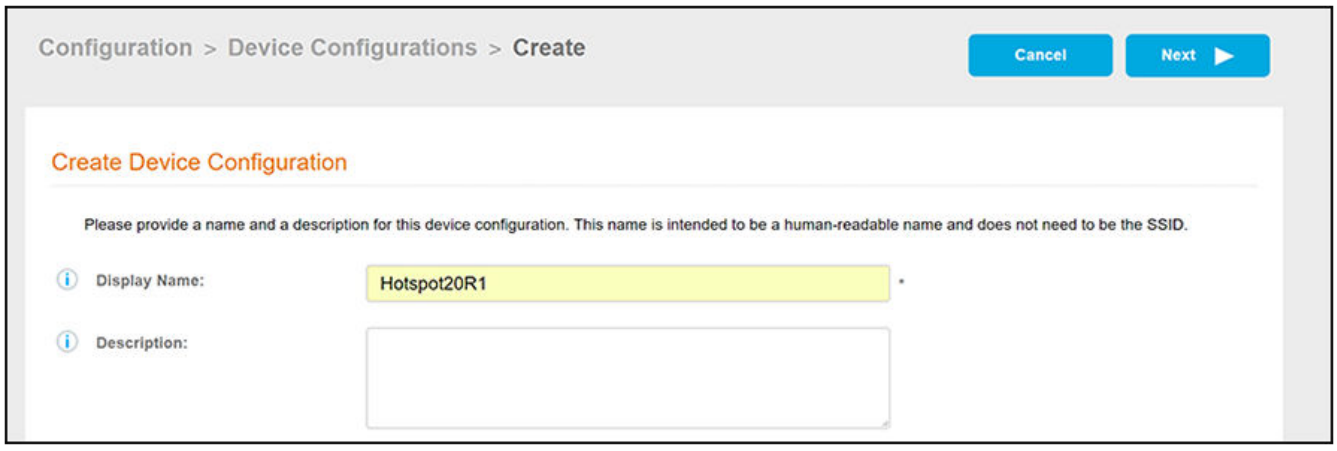
- Creating a Hotspot 2.0 Release 1 Device Configuration....31
- Adding a Hotspot 2.0 Release 1 branch to the Workflow....35
- Adding a Device Configuration to the Workflow....37
- Configuring the Certificate Template....38
- Testing the Hotspot 2.0 Release 1 User Experience....39

Once you configure a Hotspot 2.0 Release 1 on your SmartZone controller, you need to add a corresponding Hotspot 2.0 Release 1 configuration to a workflow on your Cloudpath system.

Creating a Hotspot 2.0 Release 1 Device Configuration

You can first create your device configuration, and then add it to your workflow for Hotspot 2 Release 1.

1. In the Cloudpath UI, navigate to **Configuration > Device Configurations**.
2. Click **Add Device Configuration**.
3. In the ensuing Create Device Configuration screen, give a meaningful name to the device configuration (as shown below), then click **Next**.



4. Configure the Connection Type information of the Create Device Configuration screen as shown and described below:

FIGURE 25 Connection Type Information



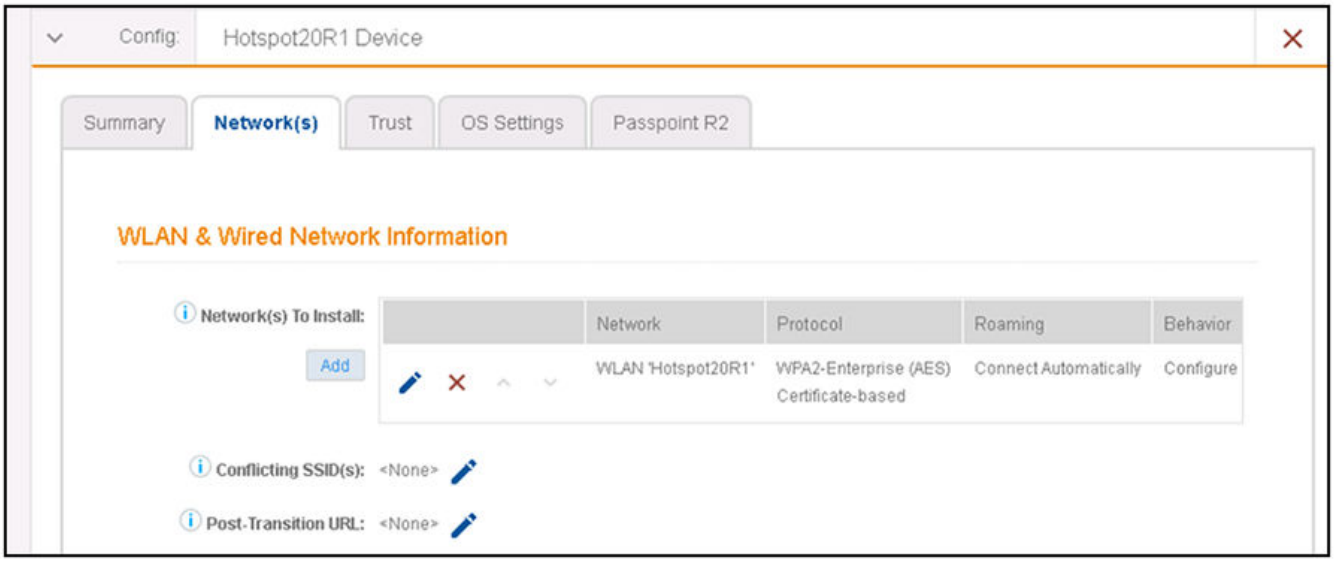
- The Wireless Connections button must be selected.
- SSID: This name must *exactly* match the SSID name you assigned during the Secure SSID configuration on your vSZ controller. Therefore, edit the name shown above accordingly.
- Authentication Style: Leave the default value of **Client Certificate [Recommended]**.
- Is this SSID Broadcast?: Leave the default value of **Yes, the SSID is broadcast**.

Click **Next**.

5. For the screens you are presented with next, you can keep all the default values and continue to click **Next** to progress through the screens, until you get to the Summary screen for the device configuration.

6. Click the **Network(s)** tab:

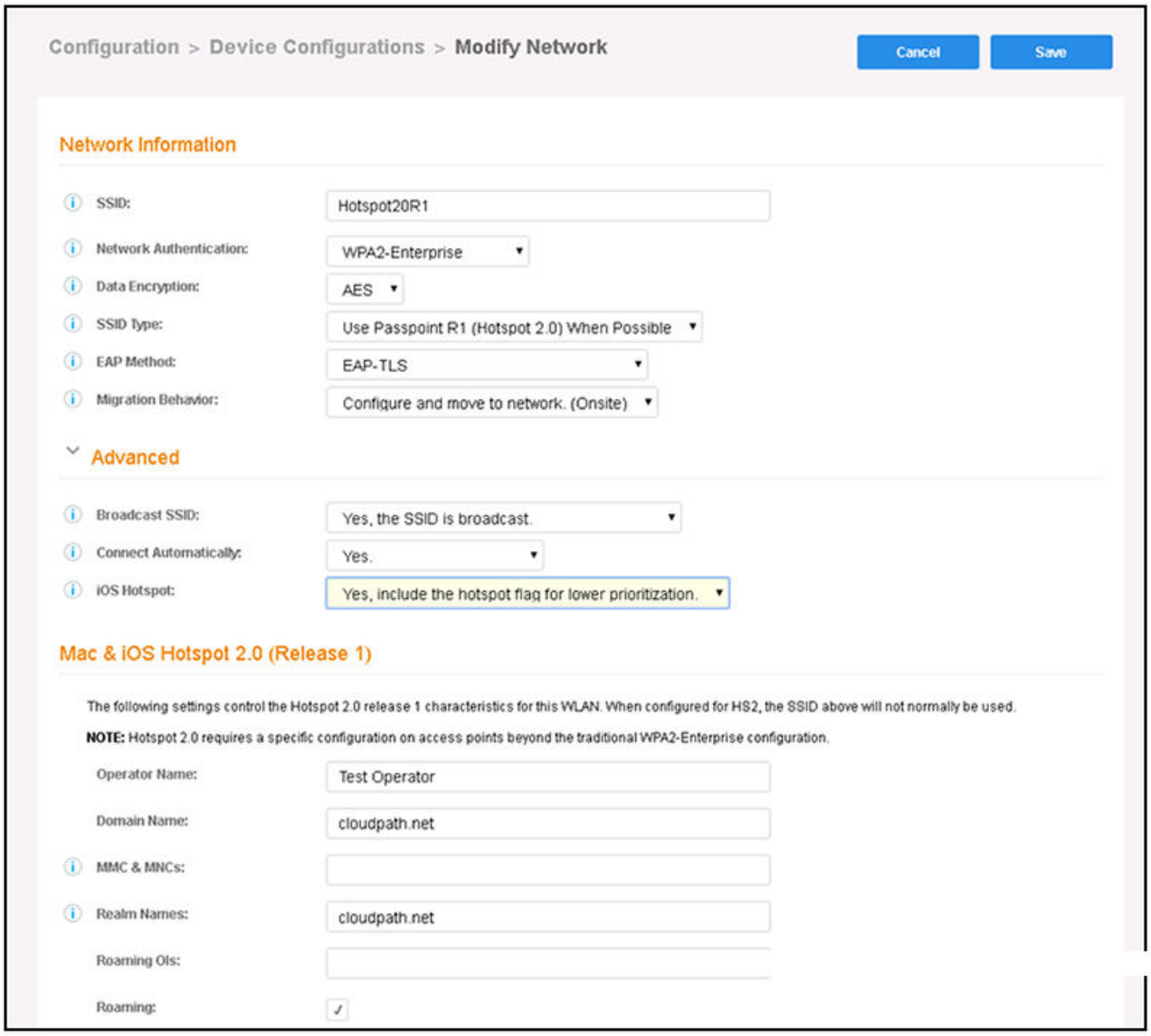
FIGURE 26 Device Configuration Network(s) Tab



7. Click the pencil icon below and slightly to the right of the "Network(s) to Install" label to go to the Modify Network configuration screen.

8. Configure the Modify Network screen, an example of which is shown and described below:

FIGURE 27 Modify Network Configuration Screen



a) In the SSID field, enter a descriptive name. (The SSID name can be any name you want because Hotspot 2.0 uses the Wifi operator and identity provider settings to identify the WLAN.)

b) For Network Authentication, select WPA2-Enterprise.

c) For Data Encryption, select AES.

d) For SSID Type, select "Use Passpoint R1 (Hotspot 2.0) When Possible."

e) For EAP Method, select EAP-TLS.

f) For Migration Behavior, select "Configure and move to network. (Onsite)"

g) For Broadcast SSID, select "Yes, the SSID is broadcast."

h) For Connect Automatically, select Yes.

i) For iOS Hotspot, "select Yes, include the Hotspot flag for lower priortization."

j) For Operator Name, enter the same name that you configured in the Wifi Operator screen. Refer to the Figure 2 on page 12.

k) For Domain Name, enter the same domain name that you configured in the Wifi Operator screen. Refer to the Figure 2 on page 12.

l) For MMC & MNCs (only needed if you configured these on the controller), enter the same two codes, separated by semicolons, that you configured in the Network Identifier tab of the Identity Provider configuration screen. Refer to the Figure 4 on page 14 screen.

m) For Realm Names, enter the name of the desired realm that you configured in the Network Identifier tab of the Identity Provider configuration screen. Refer to the Figure 4 on page 14 screen.

n) For Roaming OIs (only needed if you configured these on the controller), enter the hexadecimal Organizational ID address of the Home OI that you configured in the Network Identifier tab of the Identity Provider configuration screen. Refer to the Figure 4 on page 14 screen.

o) Enable Roaming.

p) When you complete the configuration, click **Save**.

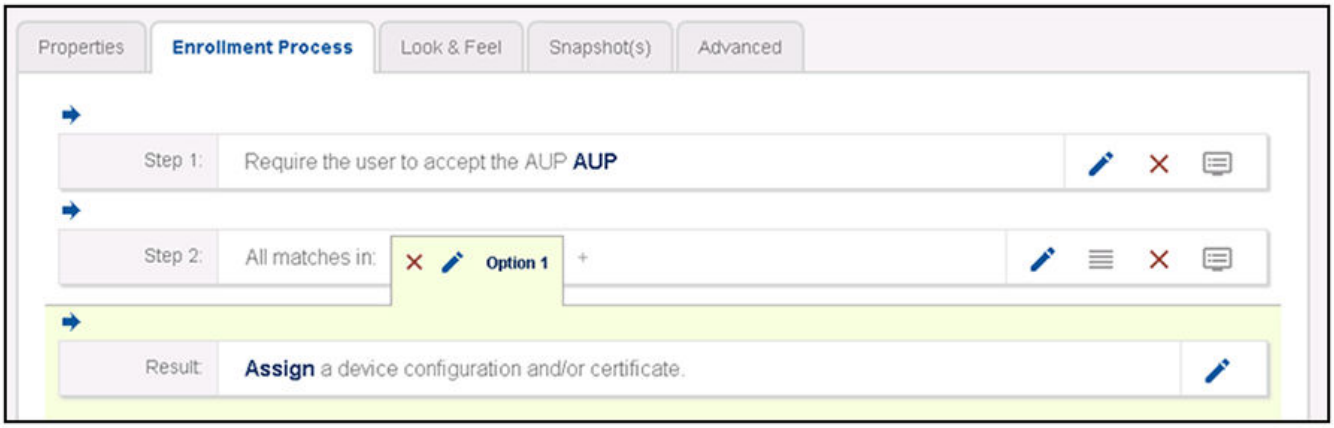
Adding a Hotspot 2.0 Release 1 branch to the Workflow

The concept of workflows and how to create one is described in detail in the *Cloudpath Deployment Guide* and the *Cloudpath Quick Start Guide*. Therefore, the purpose of the procedure in this section is to demonstrate how to add a Hotspot 2.0 Release 1 branch to an existing workflow. The same steps included below could also be used to create a new workflow with a Hotspot 2.0 Release 1 branch.

1. Log in to the Cloudpath user interface.
2. Go to **Configuration > Workflows**.

3. Click on a workflow to which you want to add a Hotspot 2.0 Release 1 branch. An example of a very simple workflow before adding a Hotspot 2.0 Release 1 branch is shown below:

FIGURE 28 Workflow Before Adding Hotspot 2.0 Release 1 Branch



4. Click the **+** button located to the right of the "Option 1" tab shown above to create a new branch in your workflow.

The Webpage Display Information screen is displayed, as shown below, and you add the necessary information.

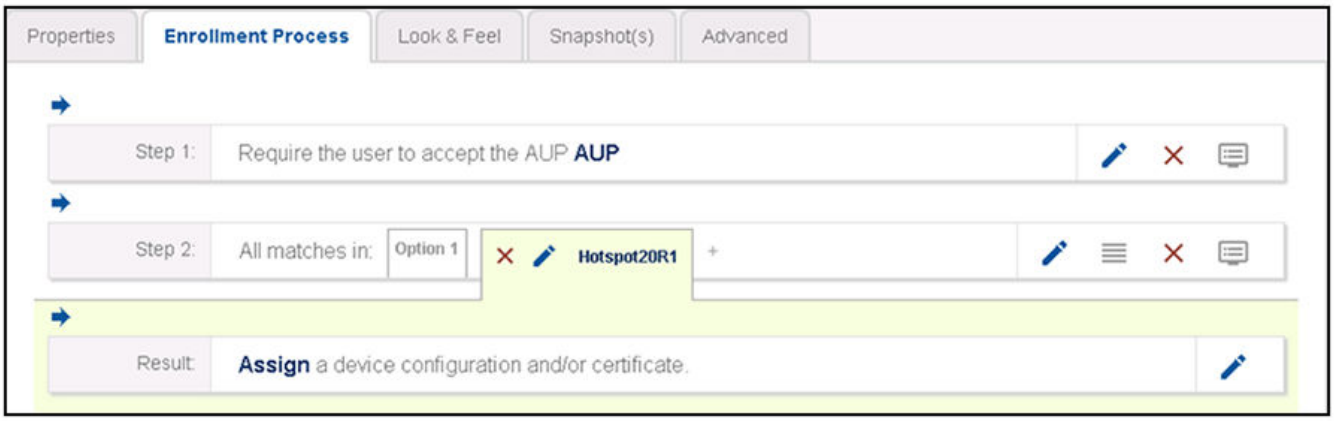
FIGURE 29 Webpage Display Information Screen is Displayed When You Add a Branch to a Workflow



Enter a Short Name and Display Title, and, optionally, Display Text, then click **Save**.

5. You are presented with a screen called **Configuration > Workflows > Modify Step** that shows the branch options. Click **Done** if the display is correct.
6. Check that your newly named branch ("Hotspot 20R1" in this example) now appears in your workflow, as shown below:

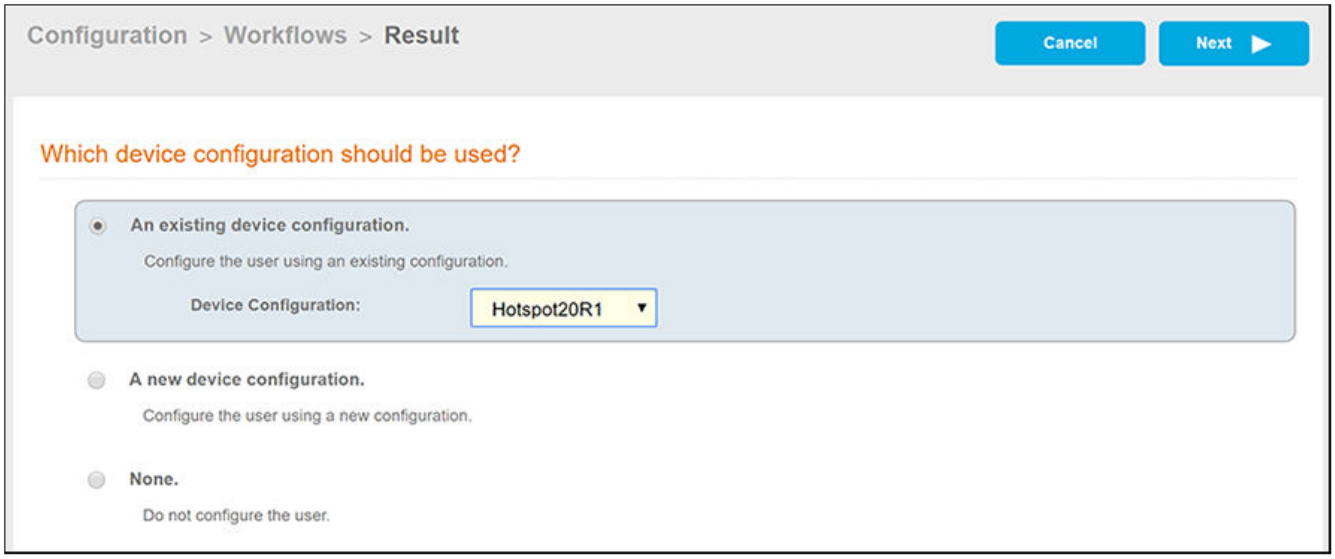
FIGURE 30 New Branch Name ("Hotspot 20R1") Appears in Workflow



Adding a Device Configuration to the Workflow

1. In the workflow, click the pencil icon to the right of the Result called "Assign a device configuration and/or certificate."

   You are presented with a screen that displays the question: **"Which device configuration should be used?"**
2. From the drop-down list of existing device configurations, select the device configuration you previously performed for Hotspot 2.0 Release 1, then click **Next**.



3. Proceed to Configuring the Certificate Template on page 38.

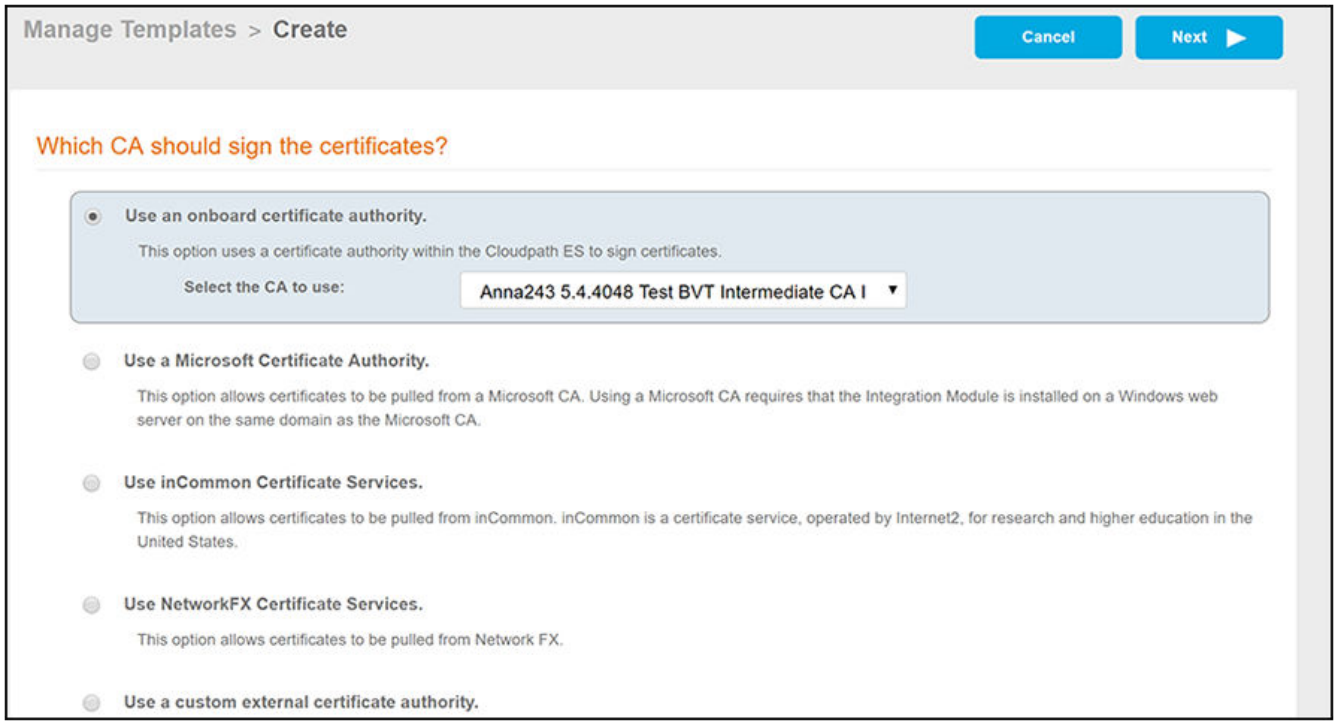
Configuring the Certificate Template

1. On the screen shown below, select the "A new certificate template" option, then click **Next**.

FIGURE 31 Certificate Template Screen



2. On the **Manage Templates > Create** screen, which has the question, "Which CA should sign the certificates?," select the "Use an onboard certificate authority" radio button and select the certificate from the drop-down list (shown below) , then click **Next**.



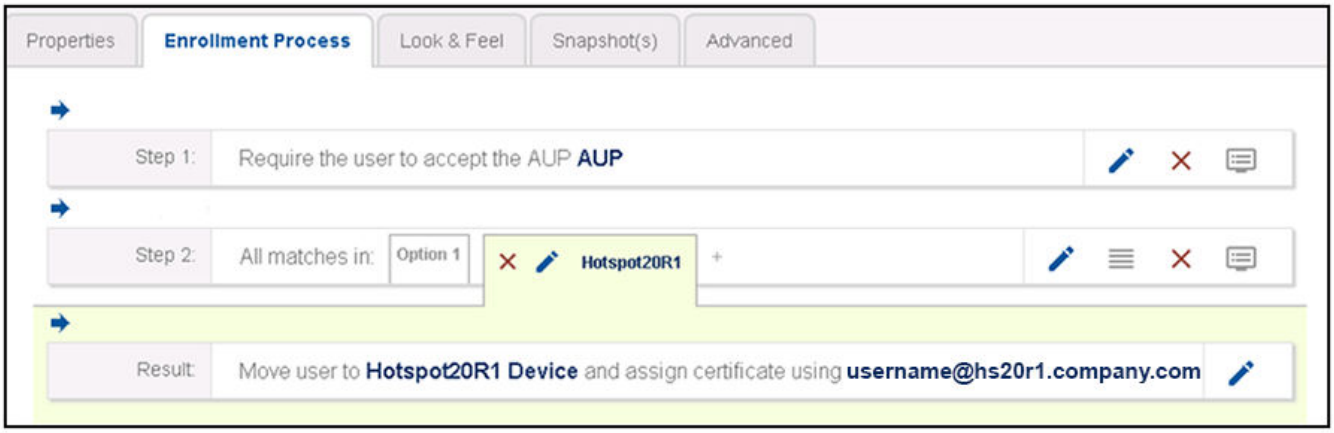
3. On the ensuing **Manage Templates > Create** screen, you can change username decorations as desired, shown in the example below, then click **Next**:

FIGURE 32 Username Decorations Screen



4. You are returned to the workflow. Make sure the Result step has been added successfully, as shown below:

FIGURE 33 Workflow After Completing the Device Configuration "Result"



Publish the workflow by clicking the **Publish** icon to the left of the workflow name at the top of the **Configuration > Workflows** screen.

Testing the Hotspot 2.0 Release 1 User Experience

Test the Enrollment process by performing the following steps:

1. On your iOS device, connect to the onboarding SSID.
2. When you presented with the with the Welcome screen, click **Start**.

3. When you are presented with various branches of your workflow, click the branch of the workflow that you created for Hotspot 2.0 Release 1.
4. Follow any prompts to continue. You are directed to download the configuration and install the wi-fi credentials to connect to the secure SSID.

NOTE
The user must set the iOS device to manually *forget* the onboarding SSID, then turn wi-fi off and on, and the device discovers the Hotspot 2.0 Release 1 secure SSID.



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