API REFERENCE GUIDE

RUCKUS SmartZone Hotspot 2.0 Interface Reference Guide, 6.0.0

Supporting SmartZone 6.0.0

Part Number: 800-72595-001 Rev A
Publication Date: April 2021

Copyright, Trademark and Proprietary Rights Information

© 2021 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

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

About This Guide **9**
- Overview 9
- Terminology 9
- What's New in this Document 10

Hotspot 2.0 Brief Overview **13**
- Hotspot 2.0 Introduction 13
- Basic Operation of Hotspot 2.0 13
- Operators and Service Providers 14

Configuring Hotspot 2.0 ..... **15**
- Configuring Hotspot 2.0 Overview 15
- Configuring Wi-Fi Operators 16
- Defining the Hotspot 2.0 WLAN Profile 18
- Step 1: Uploading Certificates 19
- Step 2: Define Wi-Fi Operator Profile 20
- Step 3: Define Identity Provider 24
  - Network Identifier 24
  - Online SignUp and Provisioning 26
  - Authentication 28
  - Accounting 29
  - Review 30
- Step 4: Define Onboard WLAN 30
  - Define Onboarding - Hotspot 2.0 Onboarding 30
  - Define Onboarding - WISPr + Allow Hotspot 2.0 Onboarding 31
- Step 5: Define Hotspot 2.0 WLAN Profile 32
- Step 6: Define Access WLAN 35
- Step 7: Create Venue Profile 36
  - Adding Venue Profile in AP 39
  - Adding Venue Profile in AP Group 39
  - Adding Venue Profile in AP Zone 40
- Adding a Venue Profile in an AP 41

Hotspot 2.0 R2 Device Workflow **43**
- Hotspot 2.0 R2 Device Workflow Introduction 43
- Onboarding Flow 43

Access Hotspot 2.0 44
De-Auth 44
Remediation 45
Password Expired 45
Update Identifier 45
AAA Combinations 45

External Onboarding and Remediation Portal Integration 47
External Onboarding and Remediation Portal Integration Overview 47
Authentication in Onboarding Flow 47
Authentication in Remediation Flow 49
Request Content 50

OCSP Stapling Support 51
OCSP Stapling Support Overview 51

Apple and Samsung Hotspot 2.0 Release 1 (Passpoint) Devices 55
Apple and Samsung Hotspot 2.0 Release 1 (Passpoint) Devices Overview 55

Preface

- Document Conventions 5
- Command Syntax Conventions 5
- Document Feedback 6
- RUCKUS Product Documentation Resources 6
- Online Training Resources 6
- 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 Safety 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.

Convention	Description
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@commscope.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 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.

About This Guide

- Overview 9
- Terminology 9
- What's New in this Document 10

Overview

This SmartZone 300 (SZ300), SmartZone 100 (SZ100), Virtual SmartZone High-Scale (vSZ-H), and Virtual SmartZone-Essentials (vSZ-E) Hotspot 2.0 Reference Guide describes the Hotspot 2.0 technology and provides configuration guidelines that the SZ300/SZ100/vSZ-E/ vSZ-H (collectively referred to as “the controller” throughout this guide) uses to enable Hotspot 2.0 based features on the RUCKUS platform.

This guide is written for service operators and system administrators who are responsible for managing, configuring, and troubleshooting Wi-Fi networks. It assumes basic working knowledge of local area networks, wireless networking, and wireless devices.

Terminology

The table lists the terms used in this guide.

TABLE 2 Terms used in this guide

Terminology	Description
ANQP	Access Network Query Protocol
AP	Access Point
CN	Common Name
CP	Captive Portal
CUI	Chargeable User Identity
EAP	Extensible Authentication Protocol
FQDN	Fully Qualified Domain Name
GAS	Generic Advertisement Service
HS2.0	Hotspot 2.0
IDM	Identity Management
MCC	Mobile Country Code
MNC	Mobile Network Code
MNO	Mobile Network Operator
MO	Managed Object
MSO	Multiple System Operator
GTPv2-C	GPRS Tunnelling Protocol for Control plane
NBI	Northbound Interface
OCSP	Online Certificate Status Protocol
OI	Organization Identifier
OMA-DM	Open Mobile Alliance’s Device Management
OSEN	OSU Server-only authenticated layer 2 Encryption Network
OSU	Online Sign-Up

TABLE 2 Terms used in this guide (continued)

Terminology	Description
Passpoint	Hotspot 2.0 certification
PKI	Public Key Infrastructure
PPS-MO	Per Provider Subscription Management Object
RAC	Radio Access Controller
RADIUS	Remote Access Dial In User Service
Release1 Device	Hotspot 2.0 Release1 specification compliant device
Release 2 Device	Hotspot 2.0 Release 2 compliant device
RSN	Robust Security Network
SZ300/vSZ-H	Controller platforms
SSID	Service Set Identifier
SSL	Secure Socket Layer
T&C	Terms and Conditions
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTLS	Tunneled TLS
UDI	User Define Interface
UE	User Equipment
UE-IP	User Equipment - IP Address
UE-MAC	User Equipment - MAC Address
UI	User Interface
URI	Uniform Resource Identifier
USIM	Universal Subscriber Identity Module
UTP	User Traffic Profile
UUID	Universal Unique Identifier
VSA	Vendor Specific Attributes
WAN	Wide Area Network
WFA	Wi-Fi Alliance
WLAN	Wireless Local Area Network

What's New in this Document

TABLE 3 Summary of Enhancements in SmartZone Release 6.0.0

Revision Number	Description	Location	Publication Date
A	Addition of new field in Venue profile.	Step 7: Create Venue Profile on page 36	April 2021
	Addition of new fields Advice of Charge, Operator Icon, and Terms and conditions in the Wi-Fi operator profile.	Step 5: Define Hotspot 2.0 WLAN Profile on page 32	April 2021
	Addition of new fields Single SSID, and Onboarding SSID in WLAN Profile.	Step 5: Define Hotspot 2.0 WLAN Profile on page 32	April 2021

TABLE 3 Summary of Enhancements in SmartZone Release 6.0.0 (continued)

Revision Number	Description	Location	Publication Date
	Adding Fast Roaming Feature in "Define Access WLAN topic".	Step 6: Define Access WLAN on page 35	April 2021
	Addition of new field Single SSID NAI in the Indentity Provider Profile.	Online SignUp and Provisioning on page 26	April 2021

Hotspot 2.0 Brief Overview

- Hotspot 2.0 Introduction..... 13
- Basic Operation of Hotspot 2.0..... 13
- Operators and Service Providers..... 14

Hotspot 2.0 Introduction

The Wi-Fi Alliance (WFA) ratified 802.11u (a.k.a. Hotspot 2.0) specification in February 2011. One of the primary objectives of the Hotspot 2.0 technology is to simplify mobile device's access to Wi-Fi networks.

The main components of the technology are:

- Automated network discovery and selection
- Secure authentication
- Online sign-up
- Policy management

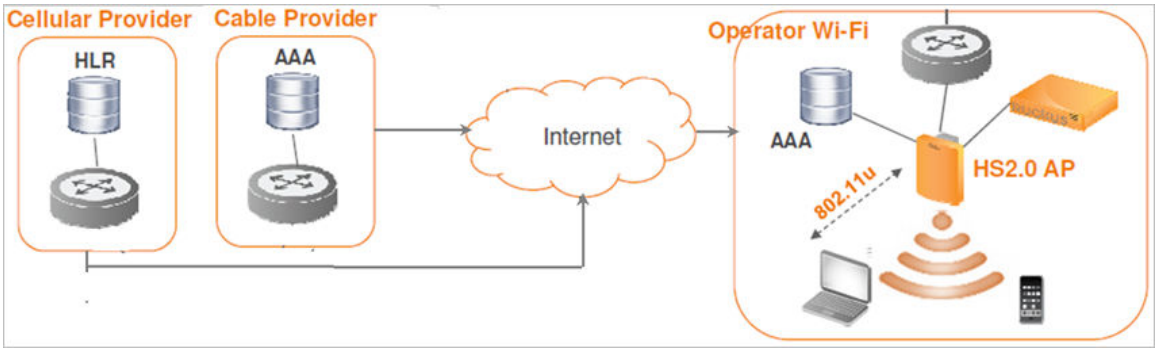
The Hotspot 2.0 Release 1 focuses on the Automated network discovery and selection and Secure authentication components, whereas release 2 goes into specification of Online sign-up and Policy management components.

Basic Operation of Hotspot 2.0

A Hotspot 2.0 compliant mobile device communicates with Hotspot 2.0 compliant Wi-Fi infrastructure (Access Points) to discover the network SSID (Service Set Identifier) to associate with it.

It then securely connects to that SSID by presenting its access credentials. Post successful authentication, the device gets securely connected to Hotspot 2.0 enabled Wi-Fi. If a mobile device does not have any pre-existing credentials, then it will not get automatically associated with Hotspot 2.0 WLAN. Instead, the user will be notified of the Online Signup (OSU) services if available. If the user elects to sign up with one of these OSU services, then he/she will be directed to a sign-up portal over Hotspot 2.0 onboarding WLAN. Upon successful authentication, user will be provisioned with Hotspot 2.0 standards-based management object, known as Per-Provider Subscription Management object (PPS-MO). User will then be disconnected from onboarding WLAN and reconnected on the secure Hotspot 2.0 access WLAN. The Hotspot 2.0 technology allows users to seamlessly roam between his/her provider's home Wi-Fi network and the visited Wi-Fi network in different location. A Wi-Fi provider can partner with several roaming partners to provide Wi-Fi access to partner's subscribers. The roaming partners can include MSOs, MNOs, wireline operators, public venues, enterprises, and basically any entity that has Wi-Fi assets as shown in the following figure.

FIGURE 1 Working of Hotspot 2.0



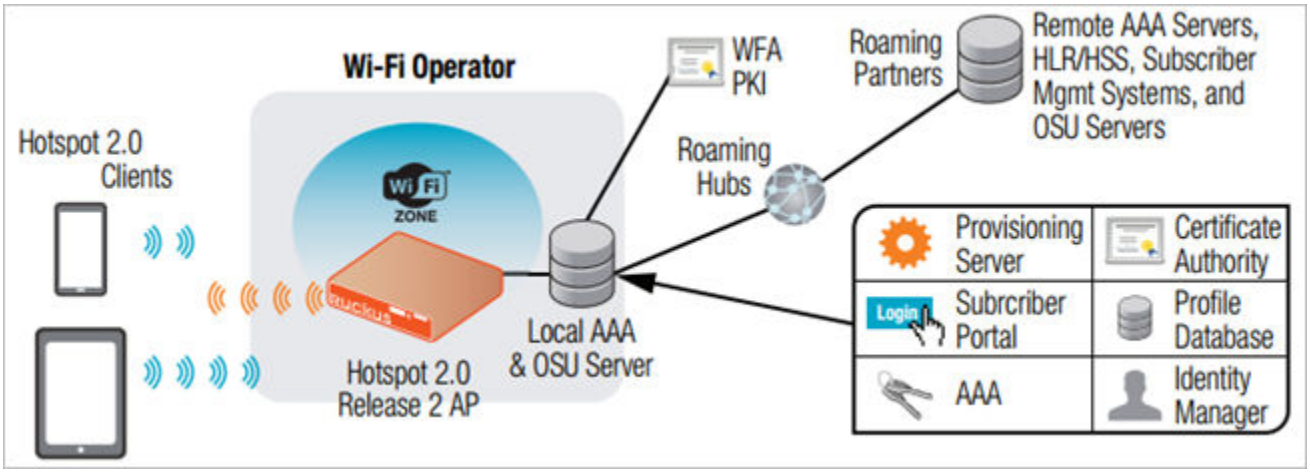
The onboarding WLAN for Hotspot 2.0 may be open WLAN or secure WLAN. The onboarding WLAN utilizes server-side only authentication, while the client side remains anonymous. The OSU service provider utilizes PPS-MO to provision necessary policy parameters such as expiration time, update interval, data usage limit etc. In a Hotspot 2.0 based network topology, entity offering Wi-Fi infrastructure may be termed as Wi-Fi operator, while the entity owning user database may be termed as Identity provider. A Wi-Fi operator may also act as an Identity provider and may partner with one or more external Identity providers.

Operators and Service Providers

Hotspot 2.0 has two entities – operators and service providers.

An operator is the owner of a set of Hotspot 2.0 enabled access points. Each operator can resell their Hotspot 2.0 service to a number of service providers. The operators deal mostly with physical network elements while the service providers keep track of user subscriptions and billing. An operator profile defines all the properties pertaining to an operator while a service profile defines the properties related to a service provider. If a WLAN is configured to provide Hotspot 2.0 service, it must be linked exactly as that of Hotspot 2.0 operator profile. However, each operator profile can simultaneously provide service to a number of service profiles.

FIGURE 2 Components of Hotspot 2.0



Configuring Hotspot 2.0

- Configuring Hotspot 2.0 Overview 15
- Configuring Wi-Fi Operators 16
- Defining the Hotspot 2.0 WLAN Profile 18
- Step 1: Uploading Certificates 19
- Step 2: Define Wi-Fi Operator Profile 20
- Step 3: Define Identity Provider 24
- Step 4: Define Onboard WLAN 30
- Step 5: Define Hotspot 2.0 WLAN Profile 32
- Step 6: Define Access WLAN 35
- Step 7: Create Venue Profile 36
- Adding a Venue Profile in an AP 41

Configuring Hotspot 2.0 Overview

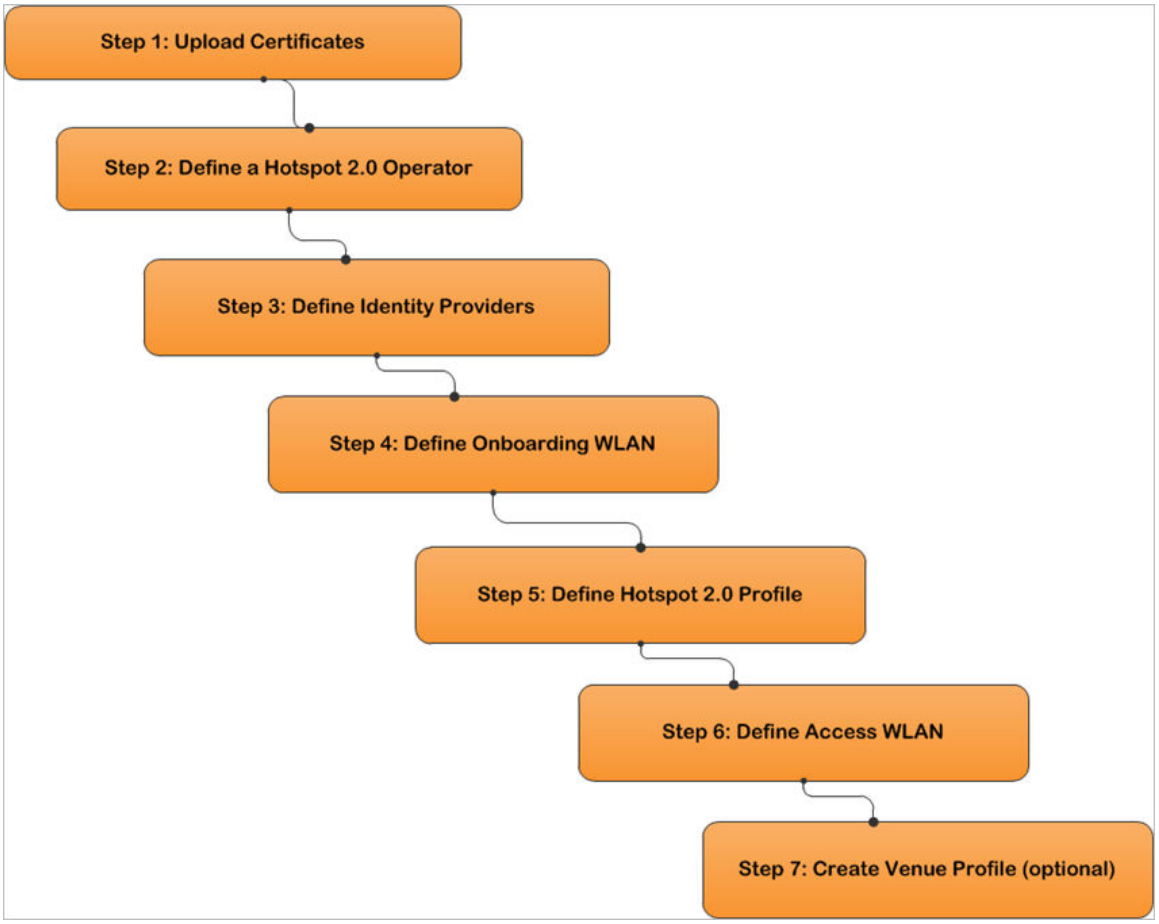
Various tasks need to be performed in a specific order to enable Hotspot 2.0 release 2 (R2) devices.

ATTENTION

This section is applicable for SmartZone 300 and SmartZone 100 controllers only. This is not applicable for vSZ-H or vSZ-E controllers.

The below figure shows the entities that need to be configured to enable the Hotspot 2.0 release 2 (R2) devices configuration flow.

FIGURE 3 Hotspot 2.0 Configuration Flow



NOTE
Hotspot 2.0 WLANs do not support IPv6.

Configuring Wi-Fi Operators

Follow these steps to define a Wi-Fi operator profile.

1. Click **Services&Profiles >Hotspot & Portals > Hotspot 2.0** to view the Hotspot 2.0 page.
2. In the Wi-Fi Operator section, click **Create**.
3. Configure the settings in the table to create a Hotspot 2.0 Wi-Fi operator and set configuration options.

TABLE 4 Wi-Fi operator configuration options

Option	Description
Name	Enter a name for this Wi-Fi operator profile.
Description (Optional)	Enter a description for the venue profile.
Domain Names	HS2.0 operator's domain name is a mandatory field, which specifies the operator's domain name. Hotspot 2.0 AP broadcasts the domain name to indicate the home Wi-Fi providers.

TABLE 4 Wi-Fi operator configuration options (continued)

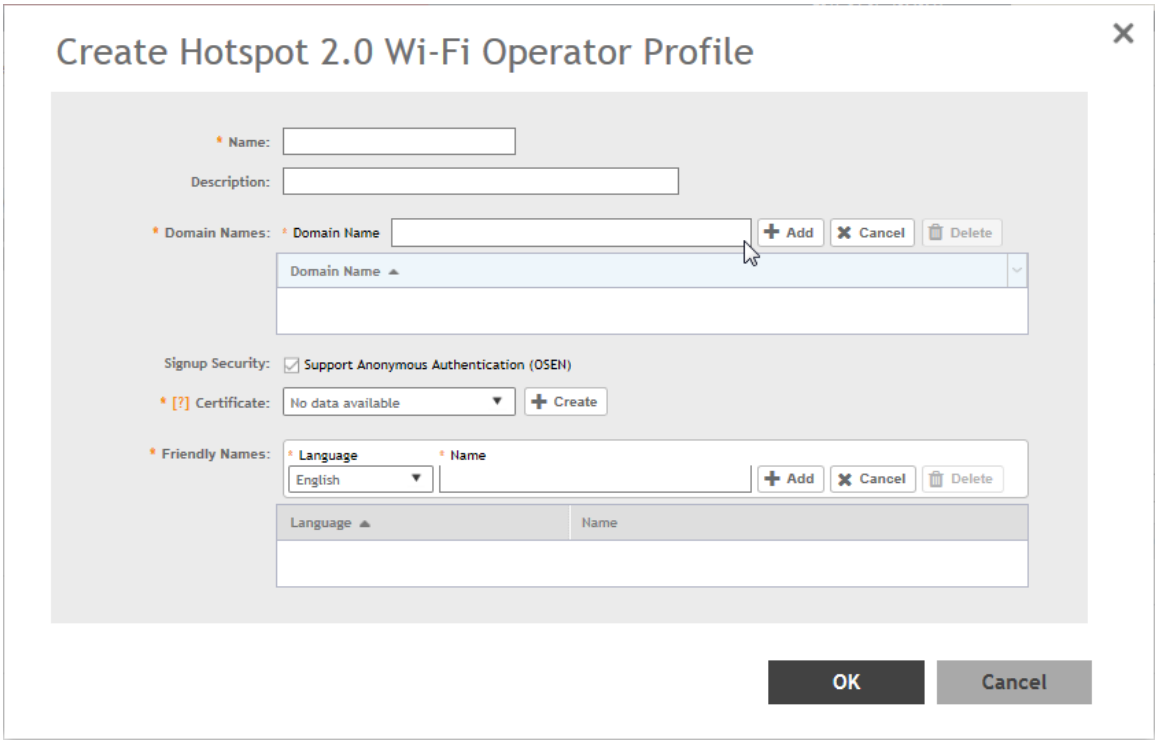
Option	Description
Signup Security	This is an optional field and is disabled by default. Enabling would mean that operator supports secure onboarding.
Certificate	Select the certificate for the operator - AAA. This can be the same certificate as the one used with OSU service.
Friendly Name	HS2.0 operator's friendly name is a mandatory field. Operator's friendly name is displayed on mobile client's screen. It is also used for operator verification during secure onboarding.

NOTE

In case of Signup Security - Onboarding WLAN assumes that the server possesses credentials that can be used to authenticate it to the client. In this case, the administrator should select the required AAA server certificate (which can be the certificate used for OSU). Onboarding WLAN facilitates network authentication before the actual onboarding. The server provides the certificate to the client and the later validates the server certificate before proceeding to online signup call flow. The certificate uploaded in the operator page can be same as the OSU certificate for the same operator.

4. Click **OK**

FIGURE 4 Hotspot Wi-Fi Operator Profile



5. Continue to Step 3: Define Identity Provider. You have completed defining the WiFi Operator Profile.

Defining the Hotspot 2.0 WLAN Profile

Follow these steps to create a Hotspot 2.0 WLAN profile.

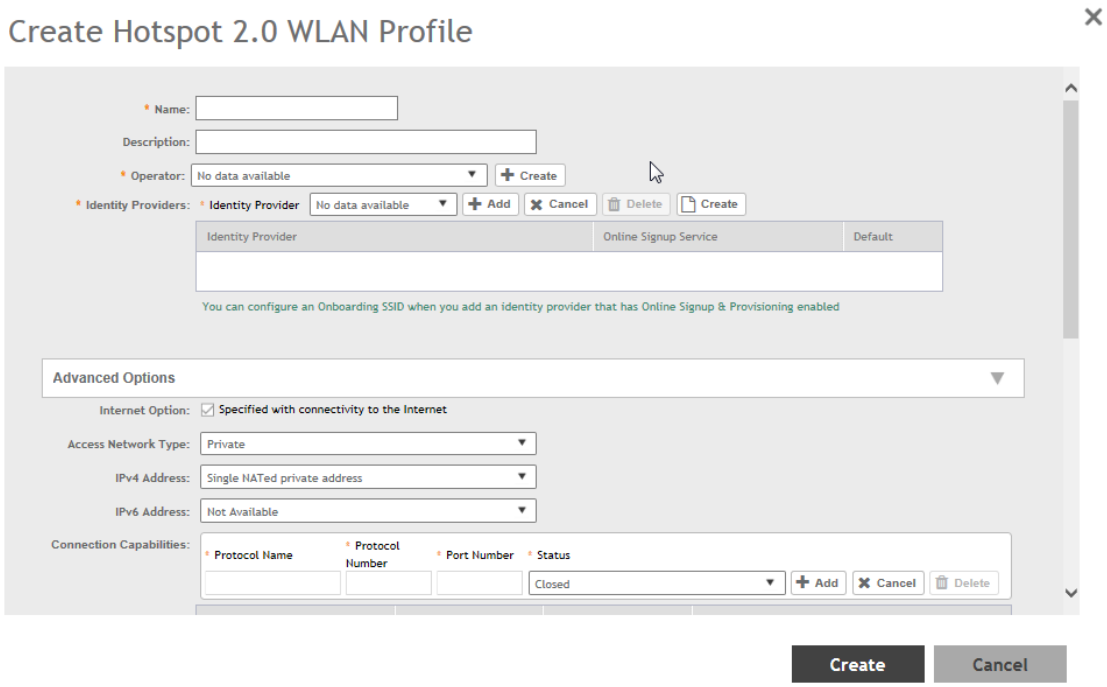
1. On the controller web interface, navigate to **Wireless LANs**.
2. Select **Zone**, and click **Create**.
3. On the **Create WLAN Configuration** page, in the section **Authentication Options**, go to the field **Authentication Type**, and select **Hotspot 2.0 Access**
4. In the Hotspot 2.0 Profile section, click **Create**.
5. Configure the settings in the table below to create a Hotspot 2.0 WLAN profile.

TABLE 5 WLAN profile configuration options

Option	Description
Name	Enter a name for this WLAN profile. This name identifies the WLAN profile when assigning an HS2.0 service to a HS2.0 WLAN.
Description (Optional)	Enter a description for the WLAN profile.
Operator	Select the operator profile. This name identifies the service operator when assigning an HS2.0 service to a HS2.0 WLAN.
Identify Providers	Choose one or more identity providers. Choose the identity provider. You can configure an OSU SSID when you add an Identity Provider which enables OSU and provisioning. Since there may be more than one identity provider per Hotspot 2.0 profiles having its own authentication profile, the No Match and Unspecified mapping could be duplicated. To avoid duplication, the default identity provider is taken as the correct configuration for No Match and Unspecified mapping. OSU SSID can be Hotspot 2.0 Onboarding; Open or 802.1X EAP. **NOTE** To create a new identity provider refer to Defining the Identity Provider.
Internet Option	Specify if this HS2.0 network provides connectivity to the Internet.
Access Network Type	Access network type (private, free public, chargeable public, etc.), as defined in IEEE802.11u, Table 7-43b.
IP Address Type	Select IP address type availability information, as defined in IEEE802.11u, 7.3.4.8.
Connection Capability	Provides information on the connection status within the hotspot of the most commonly used communications protocols and ports. 11 static rules are available, as defined in WFA Hotspot 2.0 Technical Specification, section 4.5.
Custom Connection Capability	Allows addition of custom connection capability rules. Up to 21 custom rules can be created.

6. Click **OK**. You have completed creating a Hotspot 2.0 services profile.

FIGURE 5 Hotspot 2.0 Services Profile



Step 1: Uploading Certificates

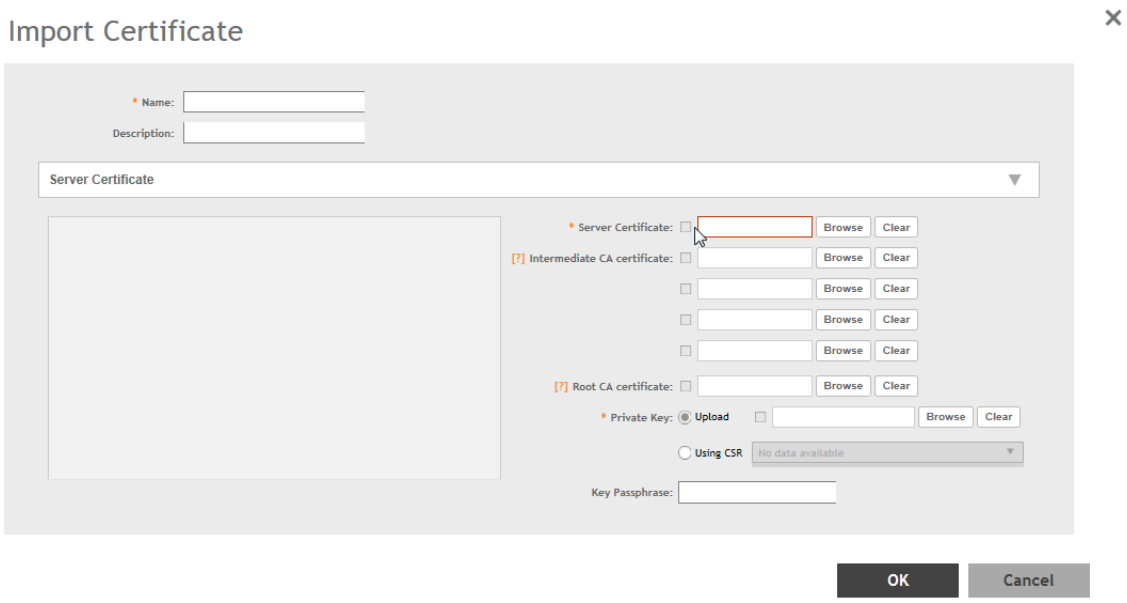
Uploading certificates is the first step in configuring Hotspot 2.0.

Follow these steps to create a trust root certificate, server or intermediate certificate and private key.

1. Click **System > Certificates > Installed Certs > Import**
2. The **Import Certificate** page appears. For **Server Certificate**, click **Browse** and select the file.
3. For **Intermediate CA certificate**, click **Browse** and select the file.
4. For **Root CA certificate**, click **Browse** and select the file.
5. For **Private Key**, select the **Upload** option and click **Browse** and select the file.
6. Enter the **KeyPassphrase**.
7. Continue to Step 2: Define Wi-Fi Operator Profile on page 20

   For details on Certificate Store refer to the Administrator Guide (PDF) or Online Help, which is accessible from the controller web interface.

FIGURE 6 Importing a Certificate



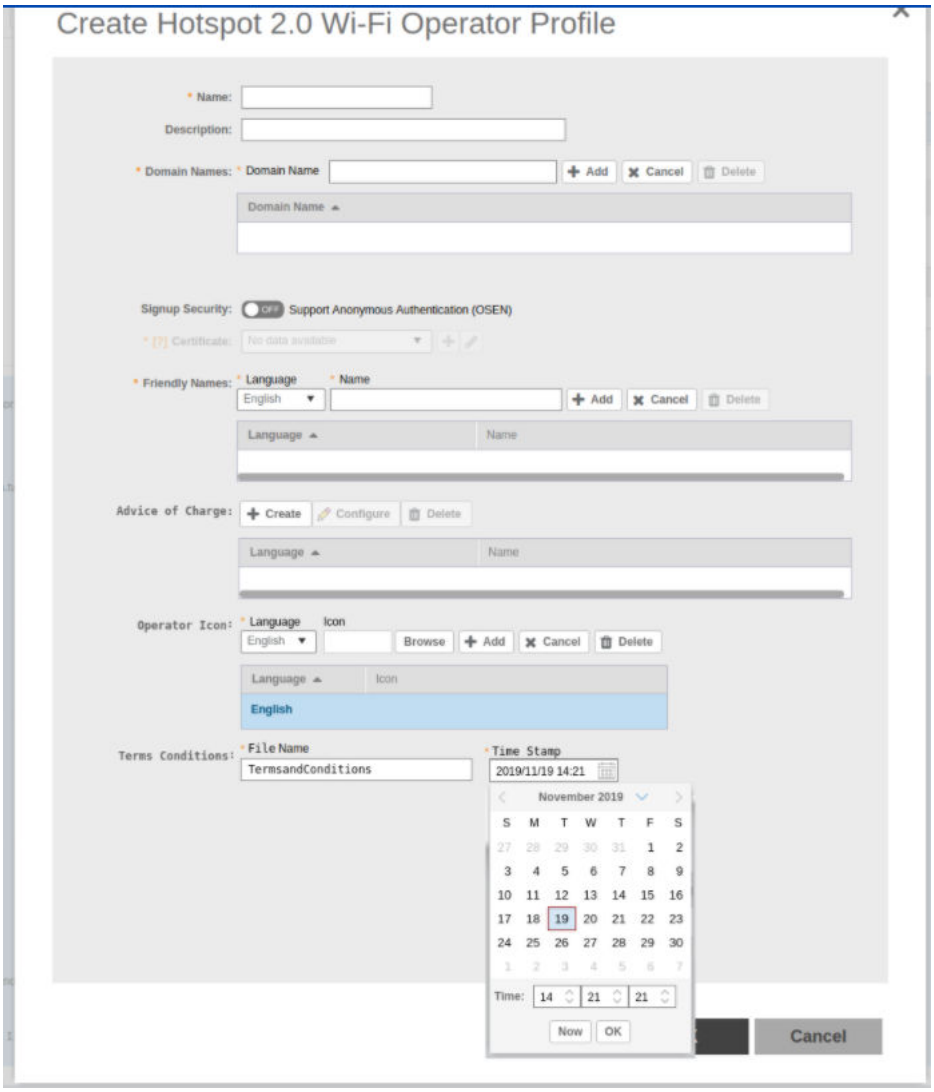
Step 2: Define Wi-Fi Operator Profile

Follow these steps to define a Wi-Fi operator profile.

1. Go to **Services** > **Hotspot 2.0**.
2. Click the **Hotspot 2.0** tab.
3. Click the **System**.
4. In the Wi-Fi Operator section, click **Create**.

5. The **Create Hotspot 2.0 Wi-Fi Operator Profile** page appears.

FIGURE 7 Hotspot Wi-Fi Operator Profile



Complete the following configuration.

6. **Name**: Enter the name for the Wi-Fi operator profile.
7. **Description (Optional)**: Enter description for the venue profile.
8. **Signup Security**: This is an optional field and is disabled by default. Enabling would mean that operator supports onboarding.

> **NOTE**
> Onboarding WLAN assumes that the server possesses credentials that can be used to authenticate it to the client. In this case, the administrator should select the required AAA server certificate (which can be the certificate used for OSU). Onboarding WLAN facilitates network authentication before the actual onboarding. The server provides the certificate to the client and the later validates the server certificate before proceeding to online signup call flow. The certificate uploaded in the operator page can be same as the OSU certificate for the same operator.

9. **Certificate**: Select the certificate for the operator - AAA. This can be the same certificate as the one used with OSU service.
10. **Friendly Names**: Enter the HS2.0 operator's friendly name.

    NOTE
    The operator's friendly name is displayed on mobile client's screen. It is also used for operator verification during onboarding.

11. **Advice of Charge**: Click **Create** to create Advice of Charge.

    The **Create Advice of Charge** page appears. Complete the following configuration.

    a) **Type**: Select any one from the following options: **Time-Based**, **Data-Volume-Based**, **Time-and-Data-Volume-Based**, and **Unlimited**.
    b) **Encoding**: Select the NAI Realm Information code from the drop-down.
    c) **Name**: Enter the name of the realm.

    NOTE
    You must acknowledge the **Advice of Charge** before being able to access services through this Wi-Fi network. This service is only used when the device automatically gets connected with the roaming Passpoint network.

12. In the **Plan Information** field, click **Create**.

    The **Create Plan Information** page appears. Complet the following information.

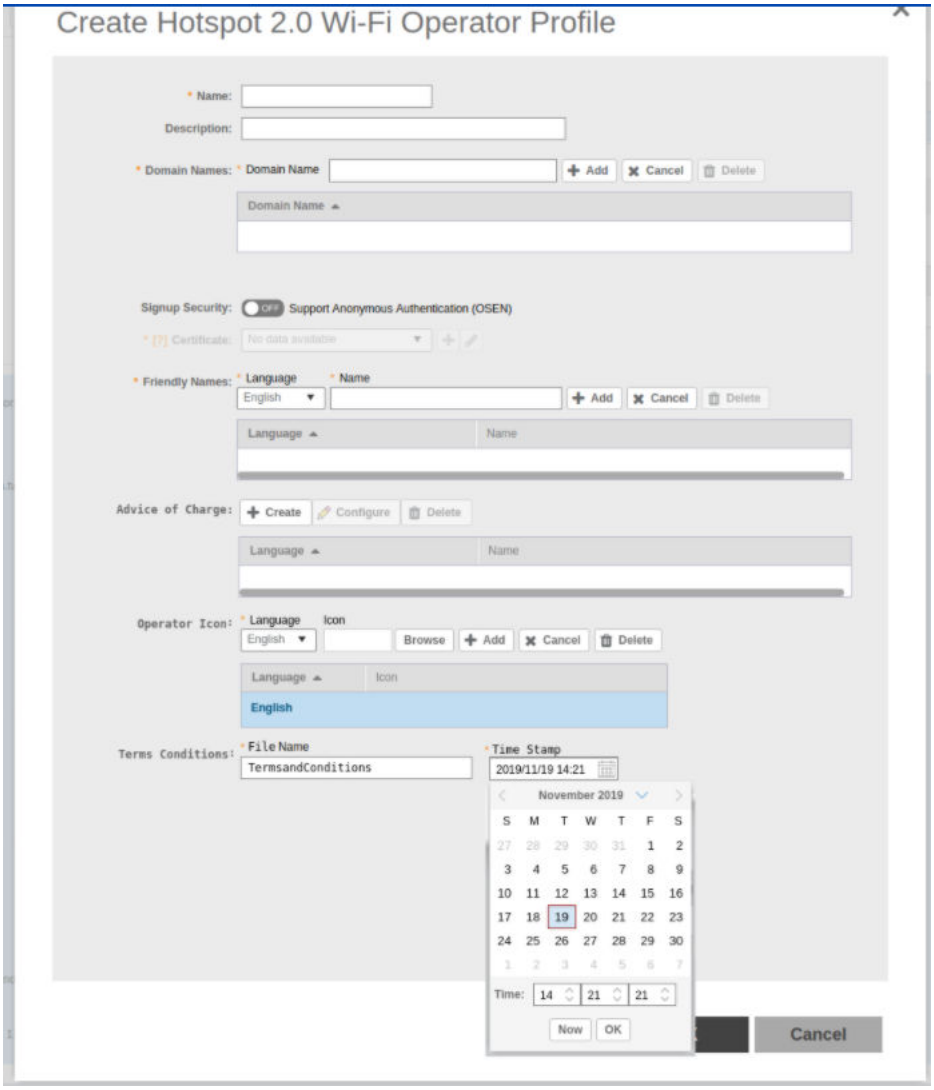
    a) **Language**: Select language code value from the drop-down. The Language Code value is a two or three character language code selected from ISO-639.
    b) **Currency Code**: Select the currency numeric code ISO 4217 from the drop-down.
    c) **XML Content**: Click **Browse** to select the UTF-8 formatted file that carries an XML description of an Advice of Charge plan.

    NOTE
    The maximum length of one plan information 300, and the maximum number of plan information is 5.

13. **Operator Icon**: Click **Browse** to import an icon in the operator profile.

    NOTE
    You can upload multiple icon for one operator. One language allows only one operator. The n maximum permitted size of icon is 65536 bytes or 64 KB.

FIGURE 8 Hotspot Wi-Fi Operator Profile



14. **Terms and Conditions**: Allows the operators to communicate to users of their Wi-Fi services, the terms and conditions (T&Cs) associated with that service. Complete the following information.

    a) **Filename**: Enter the filename listing the terms and conditions.

    NOTE
    The maximum length of the file is 247 characters.

    b) **Time Stamp** Timestamp is associated with the time of the T&C file. In seconds since January 1, 1900 00:00 UTC. Configure the timestamp, and click **OK**.

15. Click **OK**.
16. You have completed defining the Wi-Fi Operator Profile.
17. Continue to Step 3: Define Identity Provider on page 24.

Step 3: Define Identity Provider

Hotspot 2.0 Identity provider provides authentication, accounting and online signup service. There can be one or more identity providers per Hotspot 2.0 access WLAN.

Hotspot 2.0 identity provider contains multiple configurations and therefore it is split into different sub sections:

- Network Identifier on page 24
- Online SignUp and Provisioning on page 26
- Authentication on page 28
- Accounting on page 29
- Review on page 30

Network Identifier

Follow these steps to create a Hotspot 2.0 Identity Provider - Network Identifier.

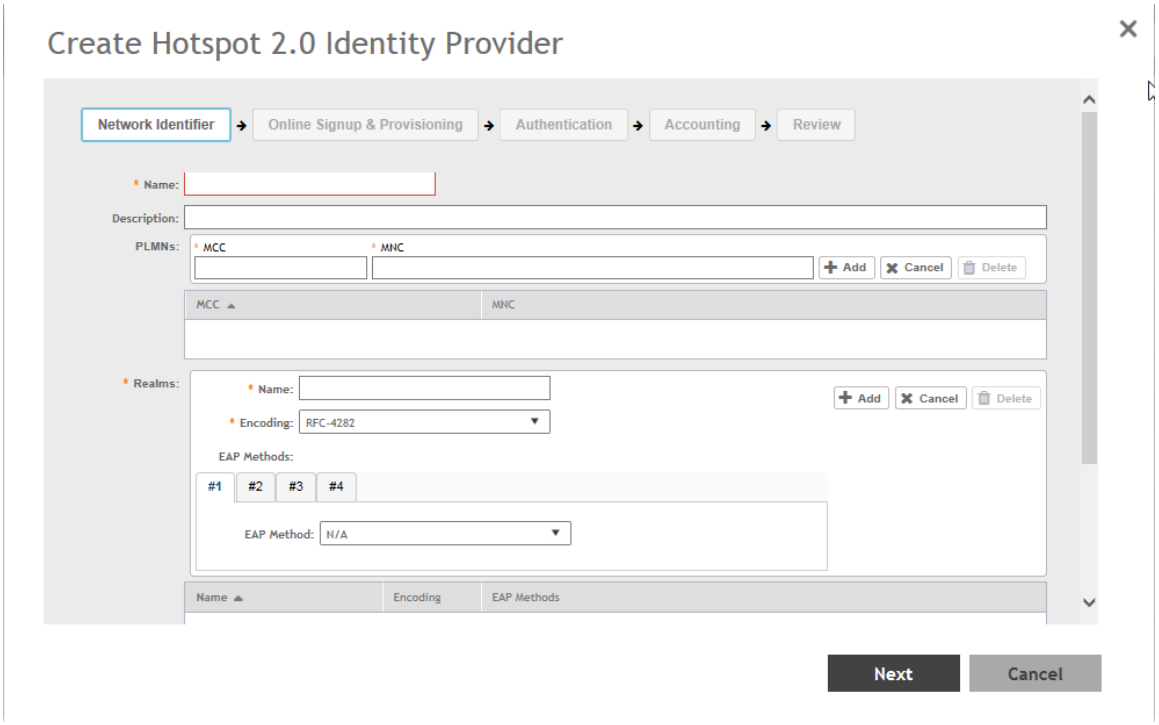
1. Click **Services & Profiles > Hotspots & Portals > Hotspot 2.0 > Identity Provider > Create**.

2. Configure the settings in the table to create a Hotspot 2.0 Network Identifier. Alternatively, the network identifier can be imported from an existing Hotspot 2.0 Wi-Fi operator.

Option	Description
Name	Enter a name or this network identifier profile.
Description (Optional)	Enter a description for the network identifier profile.
PLMNs	Each record contains MCC and MNC. • MCC: Set the correct country code for the geographical location. This is required when the controller sends MAP authentication information. Type the mobile country code digits. Decimal digit strings with maximum length of 3 and minimum length of 2. • MNC: Set the mobile network code based on the geographical location. This is required when controller sends MAP authentication information. Type the mobile network code digits. Decimal digit strings with maximum length of 3 and minimum length of 2.
Realms	List of NAI realms corresponding to service providers or other entities whose networks or services are accessible via this AP. Up to five NAI realm entries can be created. Each NAI realm entry can contain up to four EAP methods. Each EAP method can contain up to four authentication types. Realm entry is automatically generated according to PLMN grid and cannot be removed. The realm value cannot be changed.
Home OIs	Organization Identifier (OI) is a unique value assigned to the organization. The user can configure more than 3 OI values and can adjust the order since the AP takes only 3 OIs in the beacon.

3. Click **Next**. You have completed creating a Hotspot 2.0 Identity Provider - Network Identifier.
4. Continue to Online SignUp and Provisioning on page 26.

FIGURE 9 Hotspot Identity Provider - Network Identifier



Online SignUp and Provisioning

Follow these steps to create a Hotspot 2.0 Identity Provider- OSU and Provisioning.

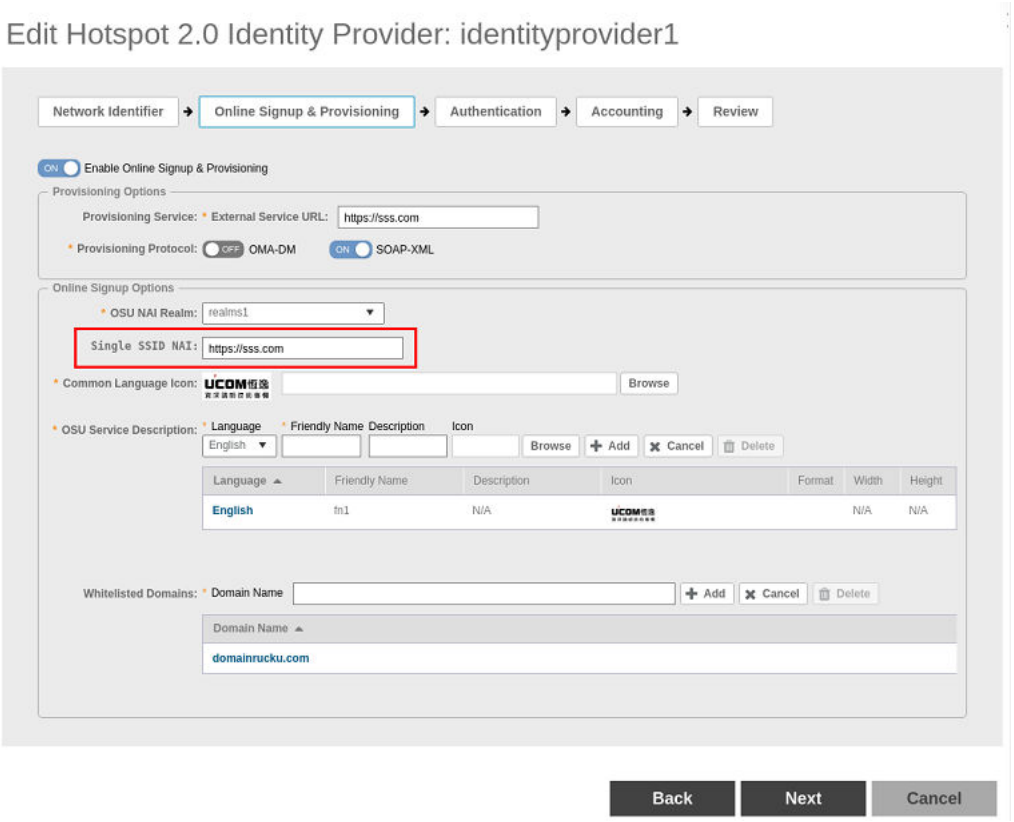
1. Click to enable **Online SignUp and Provisioning** to configure the service for the identity provider.
2. Alternatively you can skip this step to move to Authentication on page 28.

3. Configure the settings in the table below to create a Hotspot 2.0 SignUp and Provisioning.

Option	Description
Provisioning Service	The provisioning service is responsible for any subscription provisioning process in which messages are communicated between the UE and the controller resulting in a PPS-MO provisioned into the UE. The provisioning supports both SOAP-XML and OMA-DM as communication protocols for the process based on the initial request coming from the UE. The provisioning service supports signup, remediation and policy update flows where the UE is provisioned with a full PPS -MO.
Provisioning Protocol	For provisioning services, the communication protocols are OMA-DM and SOAP-XML by default.
OSU NAI Realm	Enter the OSU Network URL.
Single SSID NAI	The maximum length for Single SSID NAI is 255 characters. **NOTE** Single SSID is shown in WLAN configuration only when the Identity Providers has enabled Single SSID NAI in Online Signup & Provisioning.
Common Language Icon	This is the default icon presented in the Release 2 device for this identity provider in case the device does not find any match for other icons per language in the table.
OSU Service Description	This table configures the friendly name, description and icon per language. This information is presented on the device when it receives ANQP message which includes OSU providers. Friendly names, which are required to be part of the OSU certificate is automatically populated in this table. In case description is also included in the OSU certificate it is automatically populated into the table. Administrators are required to set the matched icon per language as included in the OSU certificate.
Whitelisted Domain	The Administrator needs to add the domains of: • Remediation URL in case it is different from the external provisioning server domain • External Portal domain in case the provisioning server is external

4. Click Next. You have completed creating a Hotspot 2.0 Identity Provider SignUp and Provisioning step.
5. Continue to Authentication on page 28.

FIGURE 10 Hotspot Identity Provider - Online SignUp and Provisioning



Authentication

Follow these steps to create a Hotspot 2.0 Identity Provider - Authentication.

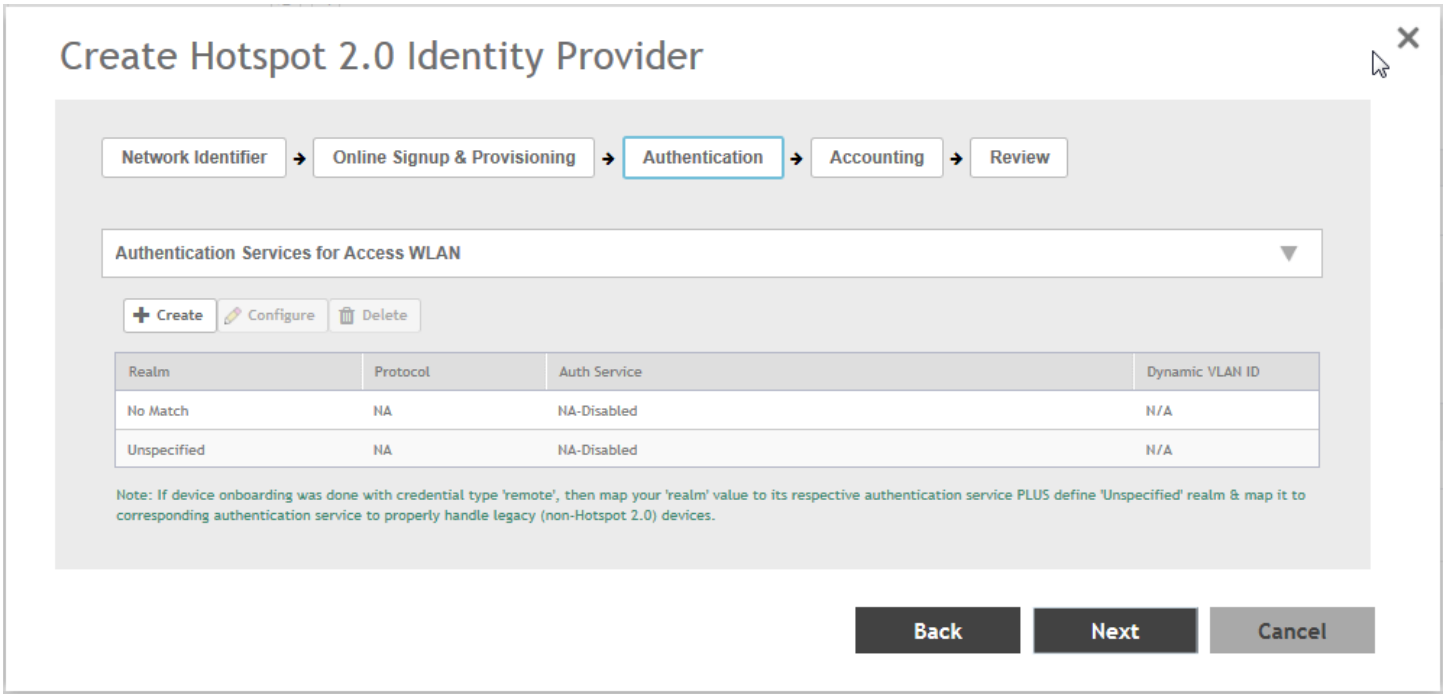
1. Click on **Authentication** to configure the service for the identity provider.
2. Configure the authentication option settings in the table to create a Hotspot 2.0 SignUp and Provisioning.

   Option

Option	Description
Realm	The administrator should map the realm to an external RADIUS server which should be preconfigured in **Services & Profiles > Hotspots & Portals > Hotspot 2.0 > Identity Provider > Authentication**. The default EAP method which the controller responds to is EAP-TTLS. In case the client is using other EAP methods (for example EAP-PEAP in legacy on-board devices) the controller falls back to the required EAP method.

3. Click **Next**. You have completed creating a Hotspot 2.0 Identity Provider - Authentication step.
4. Continue to Accounting on page 29.

FIGURE 11 Hotspot Identity Provider - Authentication



Accounting

Follow these steps to create a Hotspot 2.0 Identity Provider - Accounting.

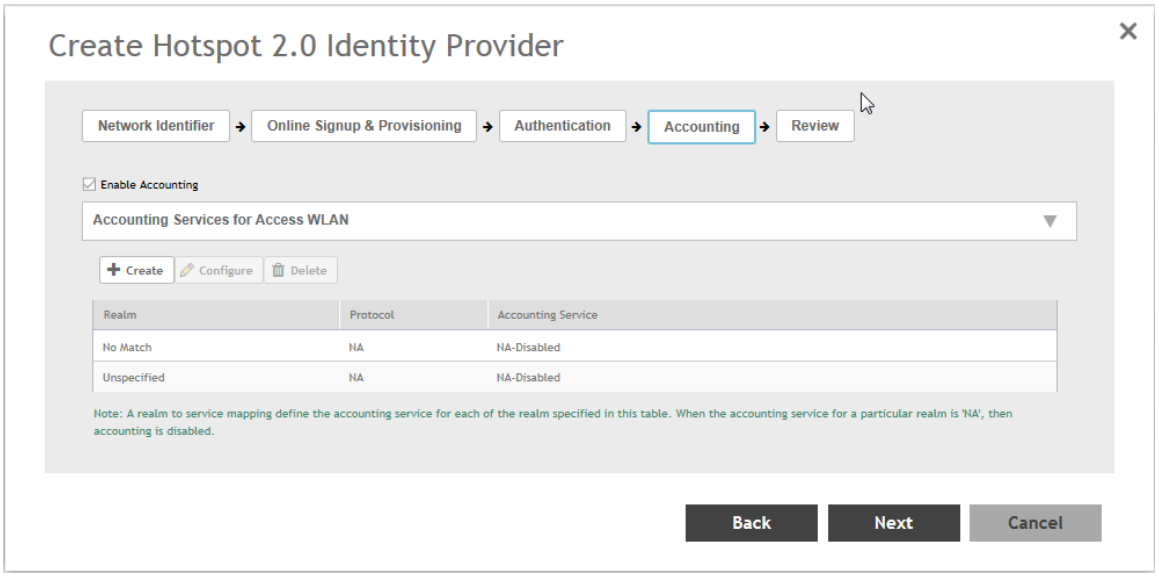
1. Click to enable Accounting for configuring the accounting service.
2. Configure the settings in the table below to create a Hotspot 2.0 Accounting.

   Option

Option	Description
Realm	If the authentication's realm is set as remote credential type, administrator should set this realm here to the **Services & Profiles > Hotspots & Portals > Hotspot 2.0 > Identity Provider > Accounting**.

3. Click **Next**. You have completed creating a Hotspot 2.0 Identity Provider - Accounting step.
4. Continue to Review on page 30.

FIGURE 12 Hotspot Identity Provider - Accounting



Review

Follow the step to review the created Hotspot 2.0 Identity Provider.

1. Click **Review** to review the configuration on one page before committing the changes to the server side. For each section is the review page, the administrator has the “Edit” button to bring the controller web interface back to the corresponding section.
2. Click **Submit** to create the Hotspot 2.0 Identity Provider.

Step 4: Define Onboard WLAN

The Administrator should configure Onboarding WLAN, by defining Hotspot 2.0 Onboarding and defining WISPr + Allow Hotspot 2.0 Onboarding.

1. Define Onboarding - Hotspot 2.0 Onboarding on page 30
2. Define Onboarding - WISPr + Allow Hotspot 2.0 Onboarding on page 31

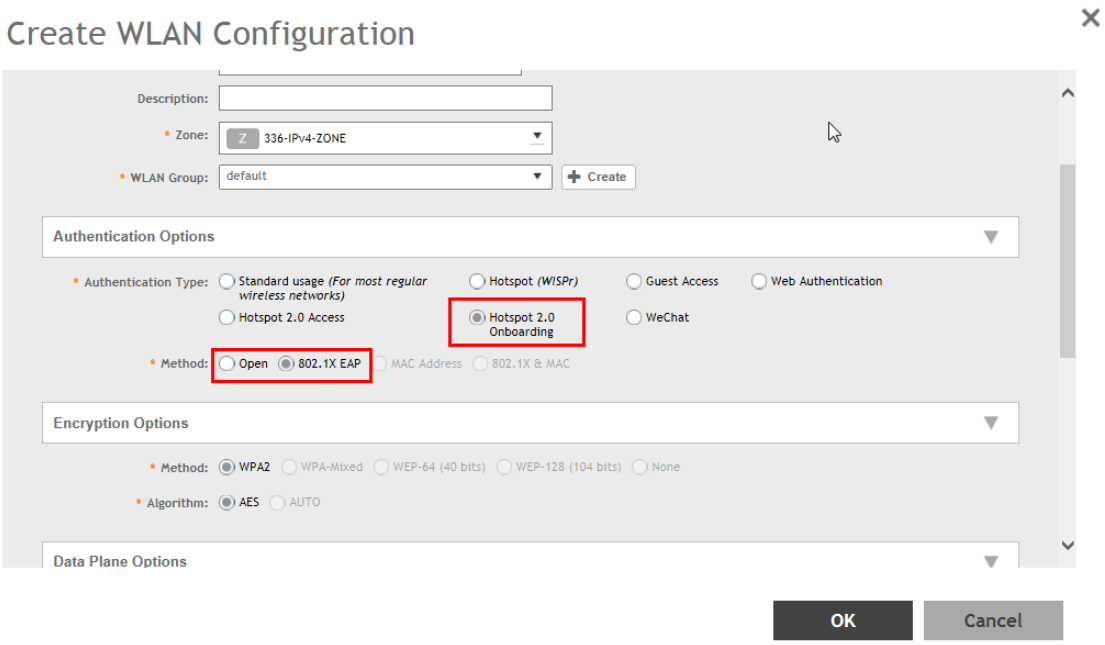
Define Onboarding - Hotspot 2.0 Onboarding

Follow these steps to configure Hotspot 2.0 Onboarding authentication.

1. Go to **Network** > **Wireless LANs**.
2. Select a Zone, and click **Create**.

   The **Create WLAN Configuration** page appears.
3. Go to **Authentication Options > Authentication Type** .
4. Select **Hotspot 2.0 Onboarding** option.
5. Choose one of the following Method:
   - **Open**
   - **802.1X EAP**
6. Click **OK**. You have completed creating the Hotspot 2.0 Onboarding authentication type.

FIGURE 13 Creating WLAN Configuration



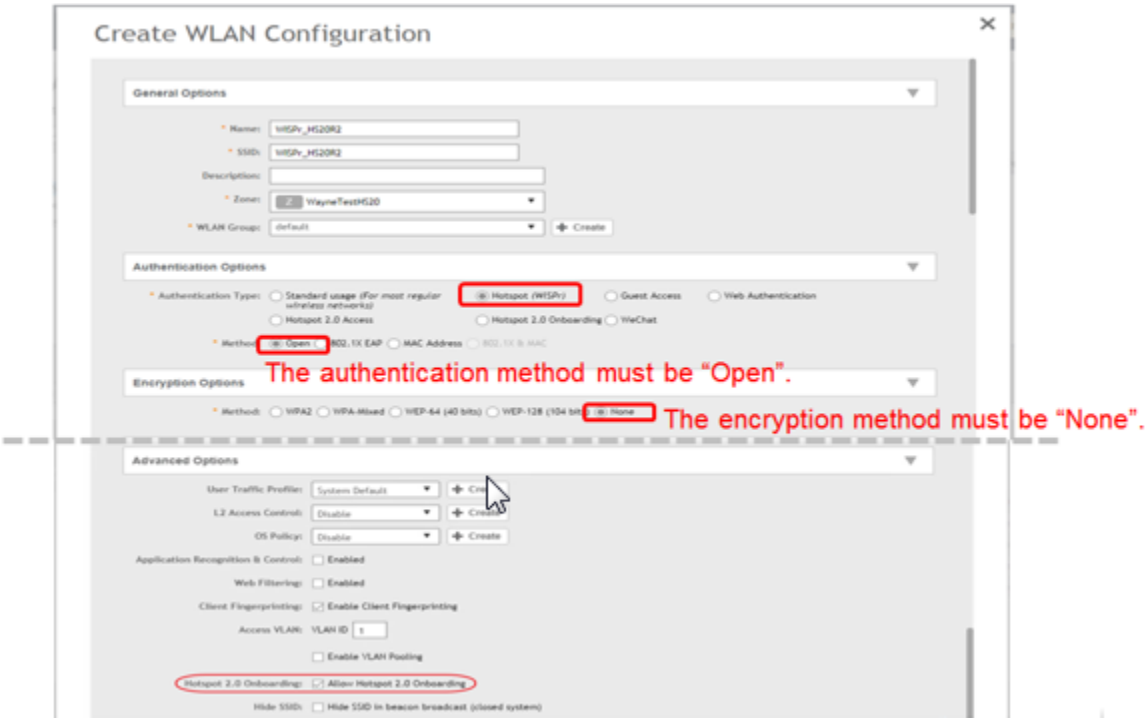
Define Onboarding - WISPr + Allow Hotspot 2.0 Onboarding

Follow these steps to configure WISPr onboarding WLAN for Hotspot 2.0 R2.

1. Click **Wireless LANs > Create**.
2. On the Create WLAN Configuration page, navigate to **Authentication Options** > **Authentication Type**.
3. Select the **Hotspot (WISPr)** option.
4. Navigate to **Authentication Options > Method** and ensure that the **Open** option is selected.
5. Navigate to **Encryption Options > Method** and ensure that **None** option is selected.

6. Navigate to **Advanced Options > Hotspot 2.0 Onboarding** and select the **Allow Hotspot 2.0 Onboarding** check box.

FIGURE 14 WISPr for Hotspot 2.0 Onboarding



Step 5: Define Hotspot 2.0 WLAN Profile

Follow these steps to create a Hotspot 2.0 services profile.

1. On the controller web interface, go to **Services** > **Hotspot 2.0**
2. Select a **Zone**, and click **Create** under the **WLAN Profile** section.

   The **Create Hotspot 2.0 WLAN Profile** page appears.

> **NOTE**
> You can also create Hotspot 2.0 WLAN Profile by clicking **Network** > **Wireless LANs** The **Wireless LANs** page appears. Click **Create**. Go to the section **Authentication Type** , select > **Hotspot 2.0 Access**, and navigate to the section Hotspot 2.0 Profile. In this section, visit the **Hotspot 2.0 Profile** field, and click **+** to create Hotspot 2.0 WLAN profile. The **Create Hotspot 2.0 WLAN Profile** page appears. Follow the steps 3 and 4 to configure the fields on the page.

3. Configure the following to create a Hotspot 2.0 WLAN profile.

Option	
Name	Enter a name for the WLAN profile. The name identifies the WLAN profile while assigning an HS2.0 service to a HS2.0 WLAN.
Description (Optional)	Enter the description for the WLAN profile.
Operator	Select the operator profile. The operator profile name identifies the service operator while assigning an HS2.0 service to a HS2.0 WLAN.
Identify Providers	Choose one or more identity providers. Choose the identity provider. You can configure OSU SSID when you add an Identity Provider which enables OSU and provisioning. Since there may be more than one identity provider per Hotspot 2.0 profiles having its own authentication profile, the No Match and Unspecified mapping could be duplicated. To avoid duplication, the default identity provider is taken as the correct configuration for No Match and Unspecified mapping. OSU SSID can be Onboarding or OPEN. **NOTE** To create a new identity provider refer to Step 3: Define Identity Provider on page 24
Single SSID	Single SSID provides the capability to support OSU network and production network on the same WLAN. Single SSID is only shown when the Identity Providers has enabled Online Signup & Provisioning
Onboarding SSID	When Single SSID is checked, Onboarding SSID is an optional field. When Single SSID is unchecked, Onboarding SSID will be a must field.
Internet Option	Specify if this HS2.0 network provides connectivity to the Internet.
Access Network Type	Access network type (private, free public, chargeable public, etc.), as defined in IEEE802.11u, Table 7-43b.
IPv4 Address	Select IP address type availability information, as defined in IEEE802.11u, 7.3.4.8
IPv6 Address	Select IP address type availability information, as defined in IEEE802.11u, 7.3.4.8
Connection Capability	Provides information on the connection status within the hotspot of the most commonly used communications protocols and ports. 11 static rules are available, as defined in WFA Hotspot 2.0 Technical Specification, section 4.5.
Custom Connection Capability	Allows addition of custom connection capability rules. Up to 21 custom rules can be created.
DGAF	When WLAN choose a HS2.0 WLAN Profile with Single SSID checked, the Downstream Group-Addresses Forwarding (DGAF) must be disabled.

4. Click **OK**.

FIGURE 15 Hotspot 2.0 Services Profile

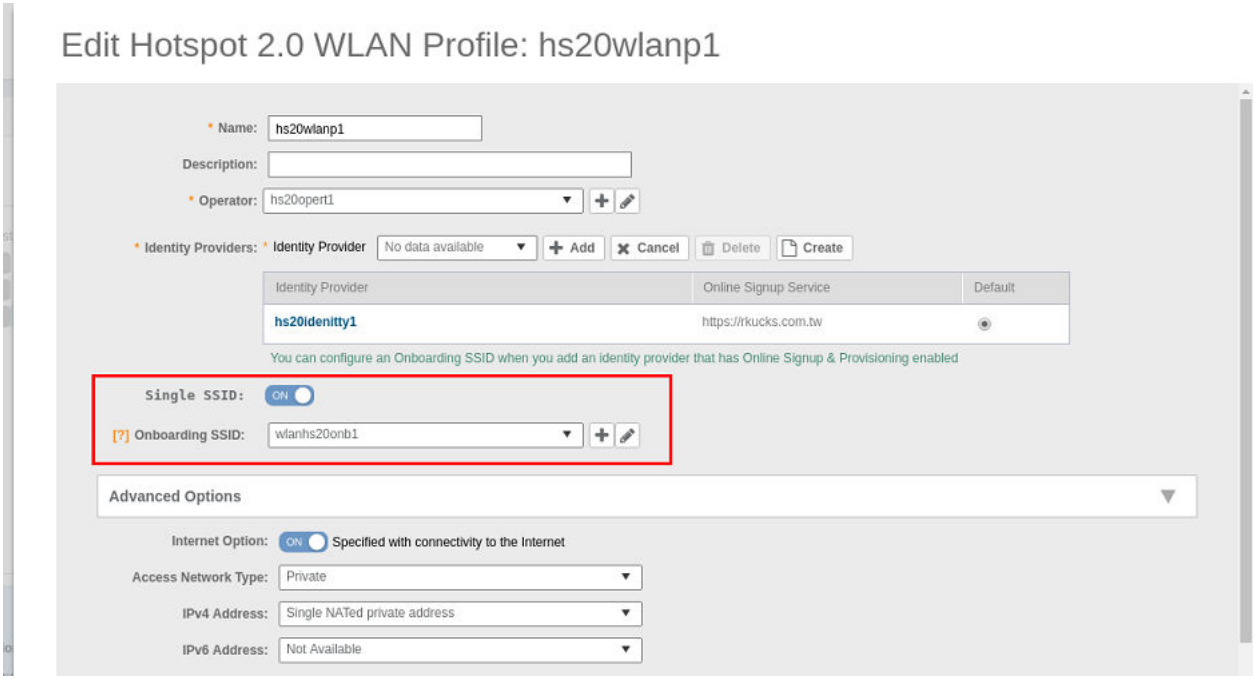
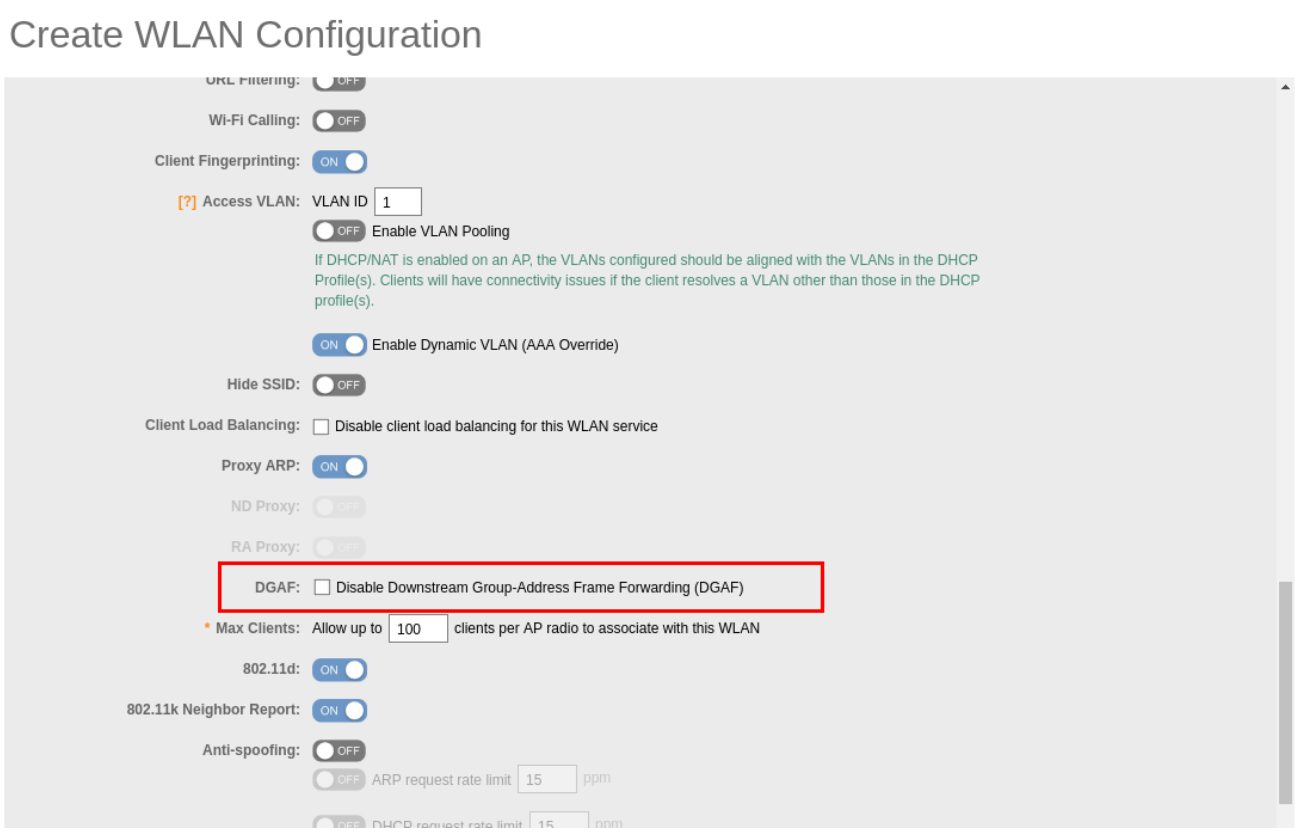


FIGURE 16 Enabling Downstream Group Addressed Forwarding



NOTE
The provisioned devices that have database credentials can execute the 802.1x Proxy and Hotspot 2.0 authentication.

Step 6: Define Access WLAN

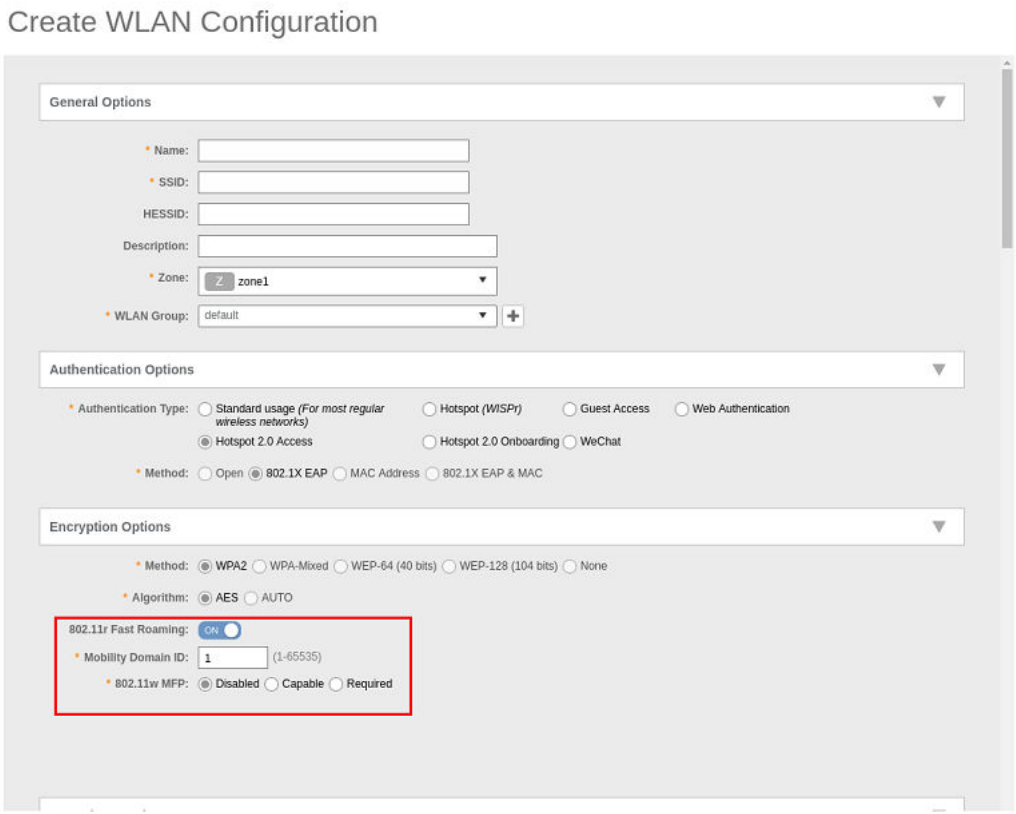
For open onboarding the administrator needs to configure guest onboarding and access WLAN which is the Hotspot 2.0 WLAN. Follow these steps to configure Hotspot 2.0 WLAN authentication.

1. Click **Network** > **Wireless LANs**.
2. Select a zone, and click **Create**.

   The **Create WLAN Configuration** page appears.
3. Go to **Authentication Options** > **Authentication Type**.
4. Select the **Hotspot 2.0 Access** option.

5. Choose **802.1X EAP** method.

FIGURE 17 Hotspot 2.0 Authentication Type



6. Go to **Encrytion** option.
7. Enable **802.11r Fast Roaming**.
8. Set the value of **Mobility Domain ID** as one. Its value ranges from 1 to 65535.
9. The 802.11w MFP field has three options: **Disabled**, **Capable** and **Required**. Select **Disabled** option when **802.11r Fast Roaming** is enabled.
10. Click **OK**.

Step 7: Create Venue Profile

Follow these steps to create a Hotspot 2.0 Venue profile, which is an optional step.

1. Go to **Services** > **Hotspot 2.0**.
2. Select **Zone**
3. In the **Venue Profile** section, click **Create**.

NOTE
You can **Configure**, **Delete** or **Clone** the Venue profile.

4. The **Create Hotspot 2.0 Venue Profile** page appears.Configure the Venue profile configuration options in the table below to create a Hotspot 2.0 WLAN profile.

   Option

Option	**Description**
Name	Enter a name for this venue profile. This name identifies the venue profile when assigning an HS2.0 service to a HS2.0 venue.
Description (Optional)	Enter a description for the venue profile.
Venue Names	Click **Create** to create a new venue name. Select the type of language from the **Venue Names** drop-down. Type the name of the venue in the **Names** field. Type the URL link in the **URL** field. **NOTE** The maximum URL length is 254. One venue name can map to up to four venue URLs.
Venue Category	Select venue category and venue type as defined in IEEE802.11u, Table 7.25m/n.
WAN Metrics	Provides information about the WAN link connecting an IEEE 802.11 access network and the Internet; includes link status and backhaul uplink/downlink speed estimates

5. Click **OK**. You have completed creating a Hotspot 2.0 venue profile in AP Zone.

NOTE
Venue configuration can be assigned to AP, AP Group or AP Zone and its priority is in the same order. This means that its first AP configuration followed by AP group and last AP zone configurations. Venue profile cannot be selected at WLAN level.

FIGURE 18 Hotspot 2.0 Venue Profile in AP Zone

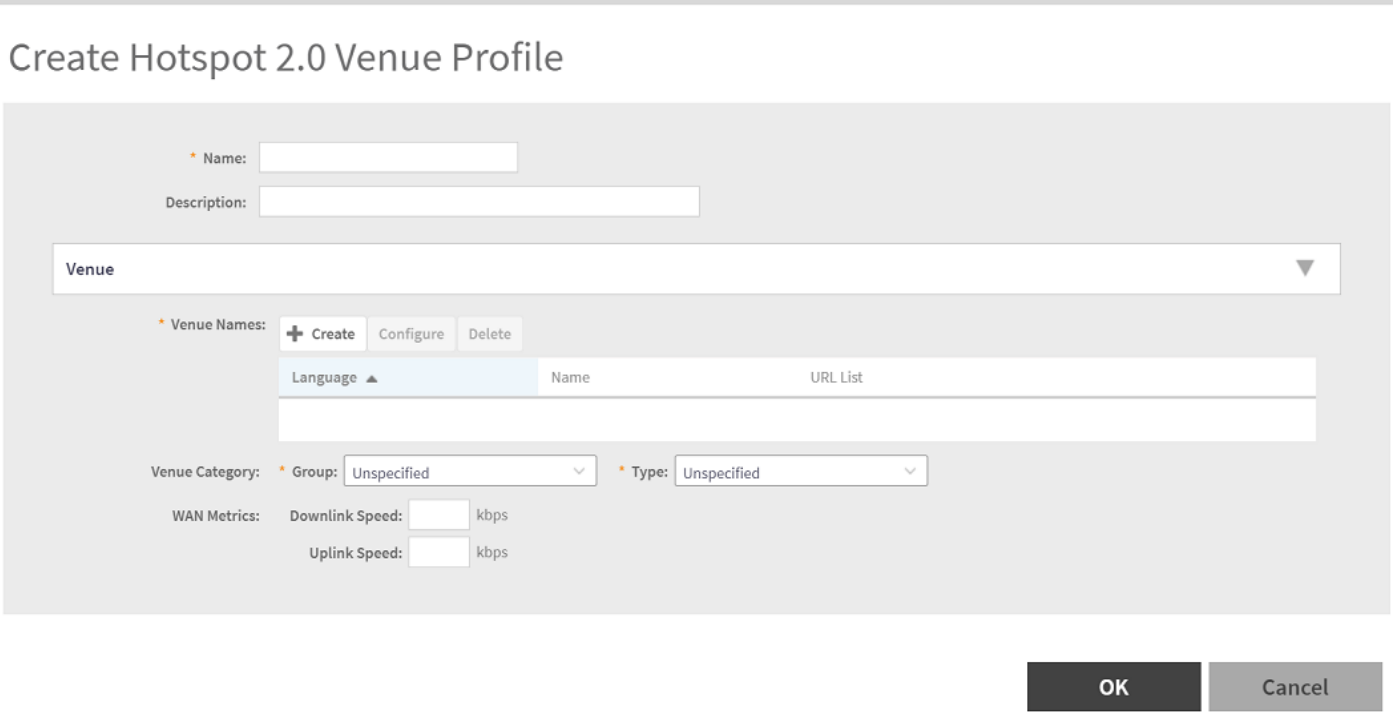
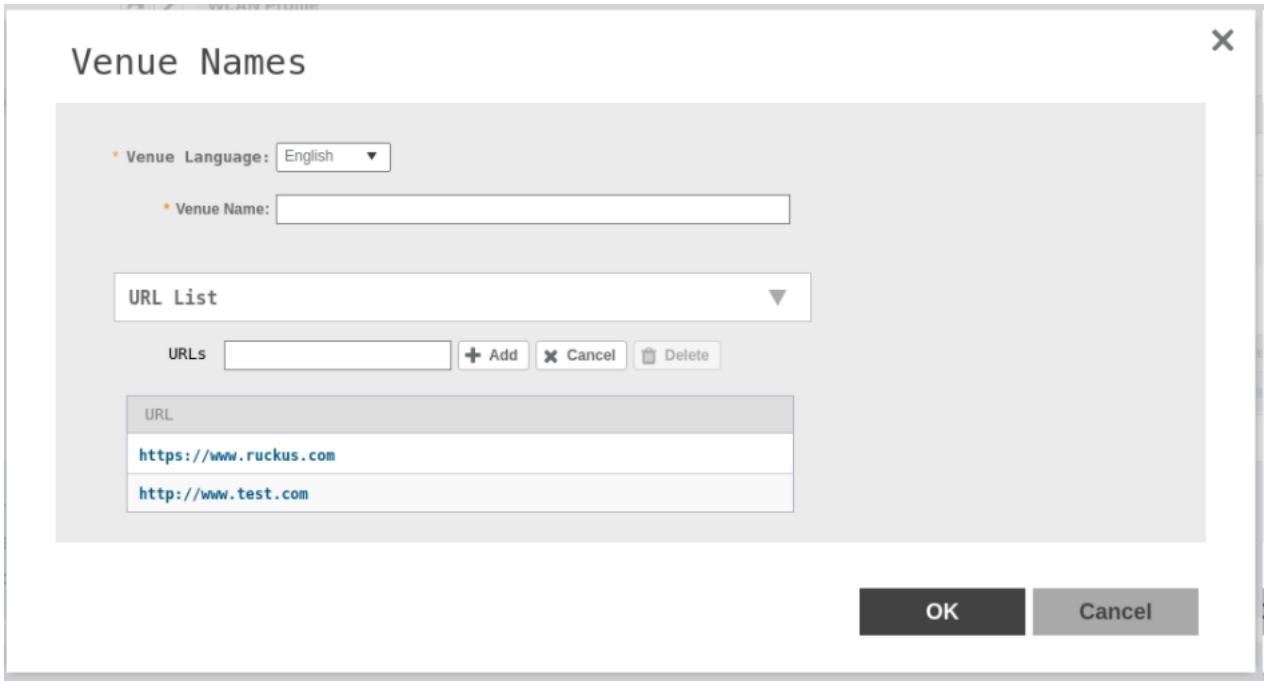


FIGURE 19 Entering Venue Name



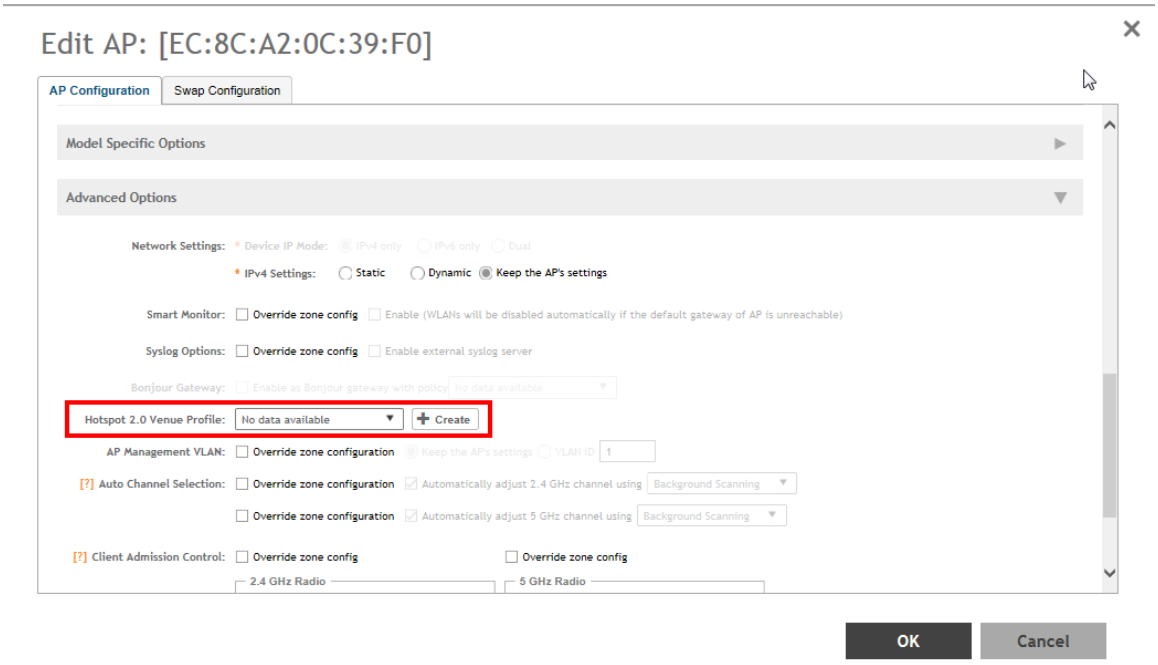
Adding Venue Profile in AP

1. Click **Network** > **Access Points**.
2. In the **Access Point** page, select zone and click **Configure**.

   NOTE
   You can **Configure**, **Delete** or **Clone** the Venue profile.

   The **Configure Zone** page appears.
3. In the **Advanced Options** section, select the field **Hotspot 2.0 Venue Profile**, and click **+** to create Hotspot 2.0 Venue Profile.
4. Configure the settings as explained in the above table.
5. Click **OK**.

FIGURE 20 Hotspot 2.0 Venue Profile in AP



Adding Venue Profile in AP Group

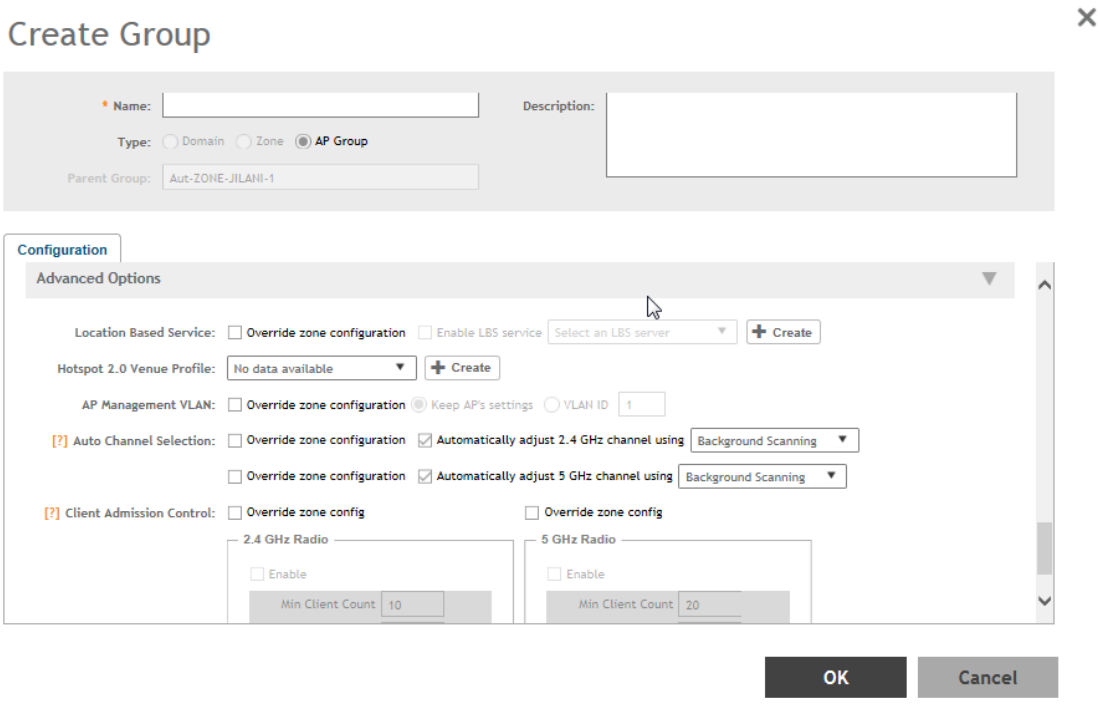
1. Click **Network** > **Access Points**.
2. In the **Access Point** page, select AP Group, and click **Configure**.

   NOTE
   You can **Configure**, **Delete** or **Clone** the Venue profile.

   The **Configure Zone** page appears.
3. In the **Advanced Options** section, select the field **Hotspot 2.0 Venue Profile**, and click **+** to create Hotspot 2.0 Venue Profile.
4. The **Create Hotspot 2.0 Venue Profile** page appears.
5. Configure the settings as explained in the above table.

6. Click **OK**.

FIGURE 21 Hotspot 2.0 Venue Profile in AP Group



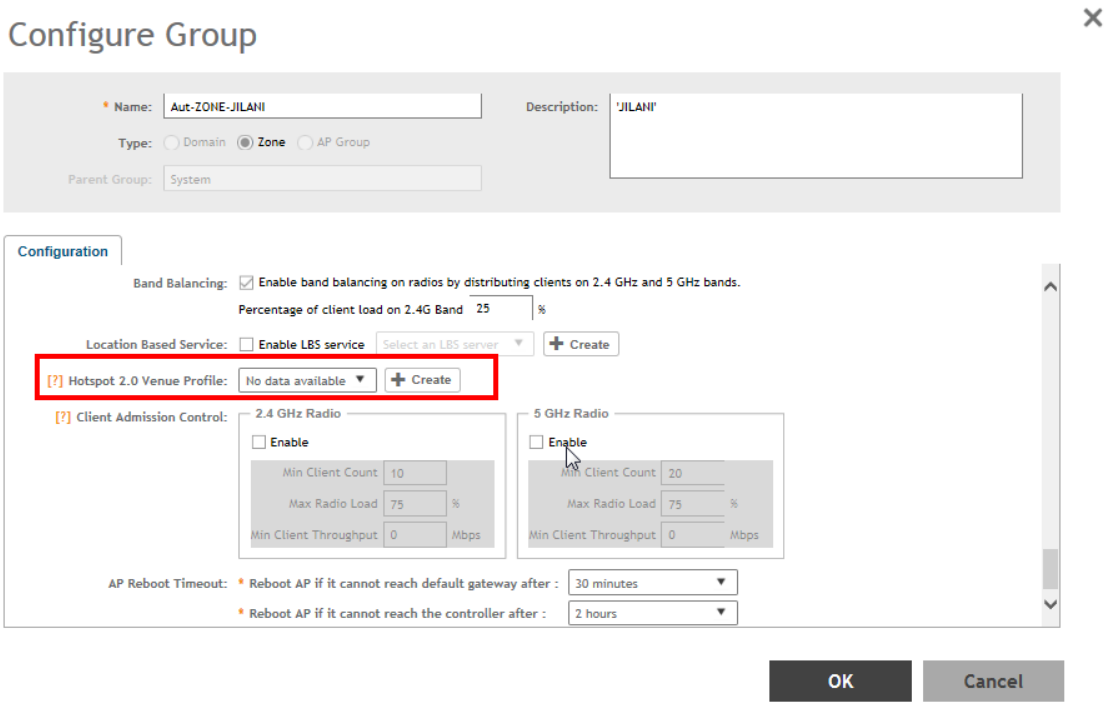
Adding Venue Profile in AP Zone

1. Click **Network** > **Access Points**
2. In the **Access Point** page, select Zone, and click **Configure**.

   NOTE
   You can **Configure**, **Delete** or **Clone** the Venue profile.

   The **Configure Zone** page appears.
3. In the **Advanced Options** section, select the field **Hotspot 2.0 Venue Profile**, and click **+** to create Hotspot 2.0 Venue Profile.
4. The **Create Hotspot 2.0 Venue Profile** page appears.
5. Configure the settings as explained in the above table.
6. Click **OK**.

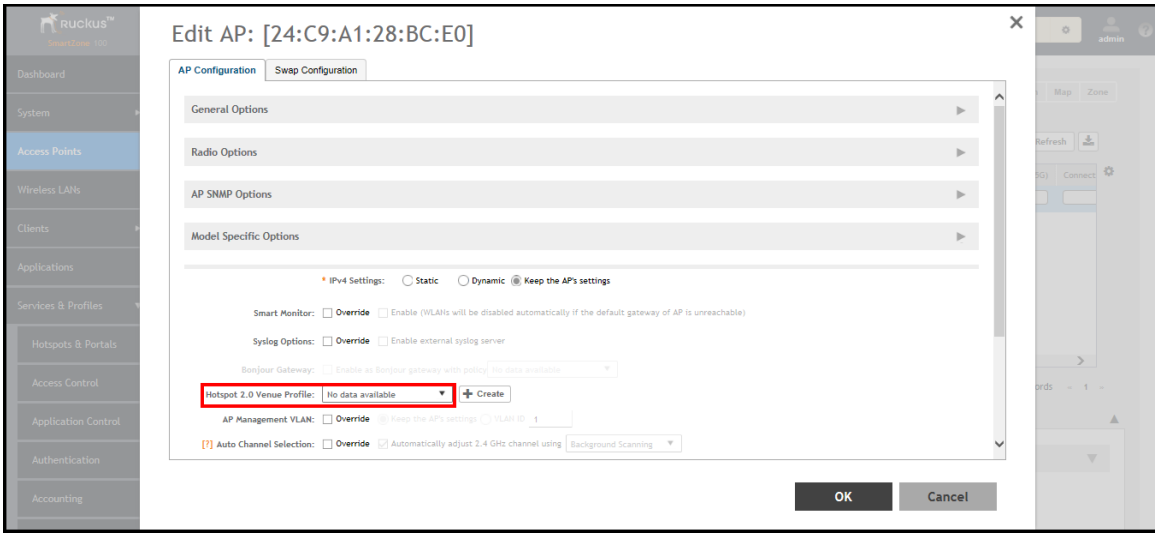
FIGURE 22 Hotspot 2.0 Venue Profile in AP Zone



Adding a Venue Profile in an AP

1. Click **Network** > **Access Points**.
2. In the **Access Point** page, select an **Access Point**, and click **Configure**.
3. Go to **AP Configuration > Advanced Options** to set the Hotspot 2.0 Venue profile from the drop down list as seen in the figure below.
4. Click **OK**.

FIGURE 23 Hotspot 2.0 Venue Profile in the AP



Hotspot 2.0 R2 Device Workflow

- Hotspot 2.0 R2 Device Workflow Introduction....43
- Onboarding Flow....43
- Access Hotspot 2.0....44
- De-Auth....44
- Remediation....45
- Password Expired....45
- Update Identifier....45
- AAA Combinations....45

Hotspot 2.0 R2 Device Workflow Introduction

ATTENTION
This section is applicable for SmartZone 300 and SmartZone 100 controllers only. This is not applicable for vSZ-H or vSZ-E controllers.

This section describes the Hotspot 2.0 R2 device workflow in detail.

Onboarding Flow

Based on the access WLAN configuration, the AP sends beacon frames with extra information suitable for interpretation by a Hotspot 2.0 R2 compliant device. This information includes the Realm, EAP method, the SSID for onboarding and a list of OS and their provisioning server URLs.

A list of OSU (pairs of icon and friendly name) is presented at the network selection and the user is required to click on one of the icons. This list will be displayed if there are no MO or matching realms to those configured on the UE.

The device is then associated to the OSU SSID, which is either onboarding or OPEN onboarding.

- In case the OSU SSID is Onboarding, an anonymous TLS handshake is executed between the UE and the controller, handled by the RAC module. Anonymous TLS is between UE and controller. The OCSP stapling is executed to validate the Onboarding certificate by the server.
- In case the OSU SSID is OPEN, the anonymous TLS will not be executed.

The UE sends a HTTPS SOAP-XML request to the OSU server (also called as provisioning server) including UE's MAC address, the URL of the portal, and redirect URI. The controller pushes the domains of the OSU and portal to AP who passes requests to them without DNAT or redirecting them.

The NGINX component acts as a proxy for all HTTPS requests to the OSU server and OSU portal. It handles certificates and OCSP stapling (server side certificate validation against the CA), which is a new requirement in Passpoint standard.

After sending a successful OCSP response to the UE, the OSU server generates a session ID for this UE. It responds to the UE with the URL of the portal as per the configuration.

Each authentication service in the controller has in its configuration group attribute mapping to the controller user role. Among other attributes, the user role defines (used more in legacy devices) the maximum number of devices a user can on board with. IDM validates the number of devices used does not exceed the maximum devices configured in the user role.

After successful authentication (regardless of the authentication service used), the IDM generates a user entry in Cassandra with all its related information. It also generates a MO credential composed of username and password. The username structure is UUID and is randomly generated during creation.

The portal redirects the UE to the URL stored in the **redirectUri parameter**, the value supplied by the UE upon initially contacting the portal. The UE initiate another HTTPS SOAP-XML request to the OSU server. The OSU server uses the session ID (generated at the beginning) to retrieve the user's

credentials to generate PPS-MO entity provided to the UE in an SOAP-XML format. Among its attributes, this PPS-MO is set for EAP-TTLS authentication.

This PPS-MO includes all required information for the UE to connect a Hotspot 2.0 SSID (the realm leaf node is defined by the realm value set in **Identity Provider** > **Online Signup& Provisioning** > **Authentication configuration**). At this point the UE disconnects from the onboarding WLAN and automatically connects to the Hotspot 2.0 SSID as per the information in PPS-MO.

Access Hotspot 2.0

Based on access WLAN configuration AP sends beacon transmitting which can be captured by R2 device. Among the information provided are: Realm, EAP method, List of OS's [provisioning server URLs], SSID of onboarding, etc.

Since UE already has PPS-MO, it finds a match between the configured realms in the PPS-MO to the realm transmitted by AP which is related to one of the identity providers configured in the Hotspot 2.0 profile. At this point, the UE initiates an EAP-TTLS request and the AP proxies it to the controller's RAC (Radio Access Controller) module.

Since UE already has PPS-MO, it finds a match between the configured realms in the PPS-MO to the realm transmitted by AP which is related to one of the identity providers configured in the Hotspot 2.0 profile. At this point, the UE initiates an EAP-TTLS request and the AP proxies it to the controller's RAC (Radio Access Controller) module.

NOTE
In this release AP's direct RADIUS authentication request to an external server for Hotspot 2.0 WLAN is not supported.

1. Read Password - RAC sends the username to IDM. IDM locates the user and replies with its password. RAC matches it to the password received from the UE in the EAP-TTLS request. In case the match is successful, RAC sends the second request otherwise the access reject is sent back to UE.
2. Authorization Status - RAC sends the username again and the IDM tries authorizing the user according to:
   a. Password expiration
   b. Update Identifier
   c. User's status

In case any one of the above three validations fail IDM responds back with an appropriate response to RAC which triggers the following use case described in De-Auth.

In case the validation is successful, IDM responds correspondingly to RAC, which returns the access accept to the UE and the UE is authenticated and authorized to browse the Internet.

RAC includes the outer identity of the EAP-TTLS in the username attribute of the access accept response. RAC includes the new *UE-Username* attribute from the IDM response for authorization status request in the CUI attribute of the access accept response. This *UE-Username* includes the username which the user used for onboarding.

De-Auth

De-Auth is available in case IDM finds user’s expiration has expired it sends a special response to RAC.

The RAC responds to the access accept with the new De-Auth attribute including the De-Auth URL. It means that the UE is not yet authorized. When the UE receives this kind of response (access accept with De-Auth attribute) it initiates the HTTPS request to the De-Auth URL provided in the RADIUS response. This URL is handled by the controller's portal, which displays the message that the user is disabled.

Remediation

In case IDM finds the user's expiration has expired or the update identifier attribute in the EAP-TTLS request does not match the value in IDM's record for the user, it sends a response to RAC, which includes the remediation URL.

RAC identifies this response and replies with the access accept including the new remediation URL attribute. It means that the UE is not yet authorized.

When the UE receives this kind of response (access accept with remediation URL) it initiates the HTTPS SOAP-XML request to the remediation URL (handled by OSU server) provided in the RADIUS response. This is followed by the digest request to the OSU server, which queries the IDM for the remediation reason.

In case the credential type is set to *Remote*, SmartZone OSU server does not support any remediation flows, as elaborated in this section.

Password Expired

In case IDM finds that the user's expiration has expired the OSU server redirects the UE to a specific path into the SGC portal.

In case the original onboarding authentication server is not an OAuth provider, the portal presents the regular username and password page with the username being filled. The user would need to provide the password used during onboarding. The portal sends the authentication request to the IDM similar to the onboarding process.

Update Identifier

In case the reason for remediation is that the update identifier does not match the OSU server generates an updated PPS-MO with the updated identifier. It responds back to the UE, which initiates the new access request along with the new updated PPS-MO information.

AAA Combinations

In SmartZone 5.0 authentication server is the RADIUS server. The table lists the available servers in each WLAN type.

TABLE 6 AAA Combinations

WLAN Type	Enable Proxy to the controller	RADIUS
Open	Yes	✓
802.1X	Yes	✓
Hotspot (WISPr)	Yes	✓
Onboarding	Yes	✓
Hotspot 2.0	Yes	✓

External Onboarding and Remediation Portal Integration

- External Onboarding and Remediation Portal Integration Overview 47
- Authentication in Onboarding Flow 47
- Authentication in Remediation Flow 49

External Onboarding and Remediation Portal Integration Overview

This document contains the integration requirements for configuring external portal for onboarding and remediation.

The external portal communicates through the controller's NBI. The NBI IP address (nbiIp) is the same as controller Management IP address and is included in the redirection URL from the OSU. One of the required parameters to NBI is the NBI password. NBI password is configured in the controller web interface. Navigate to **Systems > General Settings > Northbound Interface** to set or modify the password. HS2.0 R2 specification requires OCSP Stapling for HTTPS related requests. Since this external portal handles HTTPS requests, it also supports OCSP Stapling. A recommended approach is to use NGINX as a proxy for the external portal to handle OCSP Stapling. The Onboarding and Remediation flows, are related to the flows as described in Hotspot 2.0 R2 Device Workflow Introduction on page 43 chapter.

Authentication in Onboarding Flow

Authentication against a remote database is performed by the NBI in the onboarding flow. The portal collects the required information, such as user name, password, and sends a HTTP request (JSON) to the NBI. The URL path, which the external onboarding portal sends as HTTP request to NBI are one of the below:

```
http://nbiIP:9080/portalintf
```

```
https://nbiIP:9443/portalintf
```

NOTE
9080 is plain-text and 9443 is HTTPS (SSL).

The OSU redirects the UE to the portal path with the following parameters:

- WsgWlanId - WLAN ID
- ClientMac- UE MAC address
- RedirectURI - The URL, which the portal redirects the UE at the end of the flow.

For example:

```
https://EXTERNAL_PORTAL_FQDN:EXTERNAL_PORTAL_PORT/
EXTERNAL_PORTAL_PATH?WsgWlanId=1&ClientMac=98:0C:82:5E:34:10&
RedirectURI=http%3A%2F%2F127.0.0.1:12345
```

The following is the request content for onboarding authentication with authentication type with RADIUS server.

Request Content

```
{
"MSG-ID":< Unique ID for the message>,
```

```
"APIVersion":"3.1.0",
"Vendor" : "Ruckus",
"RequestPassword" : "<NBI password as set in controller>,
"UE-MAC":<Device MAC>
"RequestType":"RegistrationOnboarding",
"RequestCategory":"UserManagement",
"Input":{
"hsReleaseVersion":"2",
"credentials":{
"loginName":<user login name>,
"loginPassword":<user password>
"authenticationServerName":<authentication sever name>
},
"remediation":"false"
}
}
```

Parameters:

- MSG-ID identifies the related request and response
- UE-MAC value is taken from the request parameter -*ClientMac*
- Login name and password are user inputs
- Authentication server name is taken from the authentication service configuration specified in **Services & Profiles** > **Hotspots & Portals** > **Hotspot 2.0** > **Identity Provider** > **Authentication** > **Create** > **Service** > **Create** in the controller web interface as seen in the figure. This configuration is applied to the specific Online Signup & Provisioning in **Services & Profiles** > **Hotspots & Portals** > **Hotspot 2.0** > **Identity Provider**.

FIGURE 24 Authentication Configuration

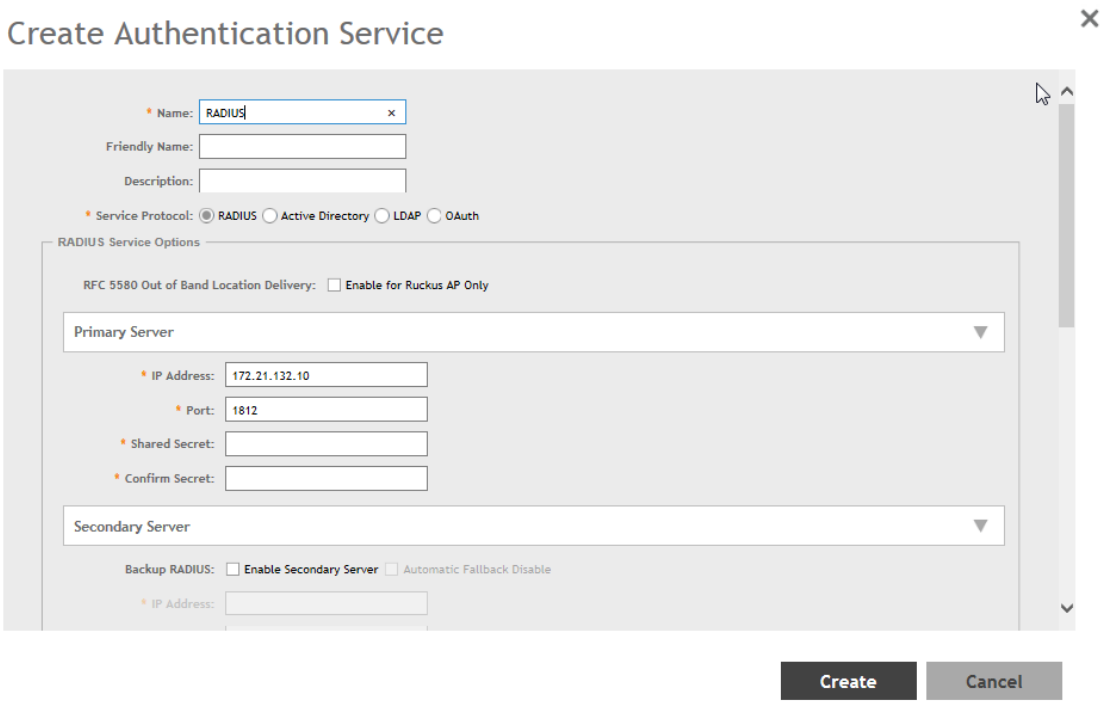
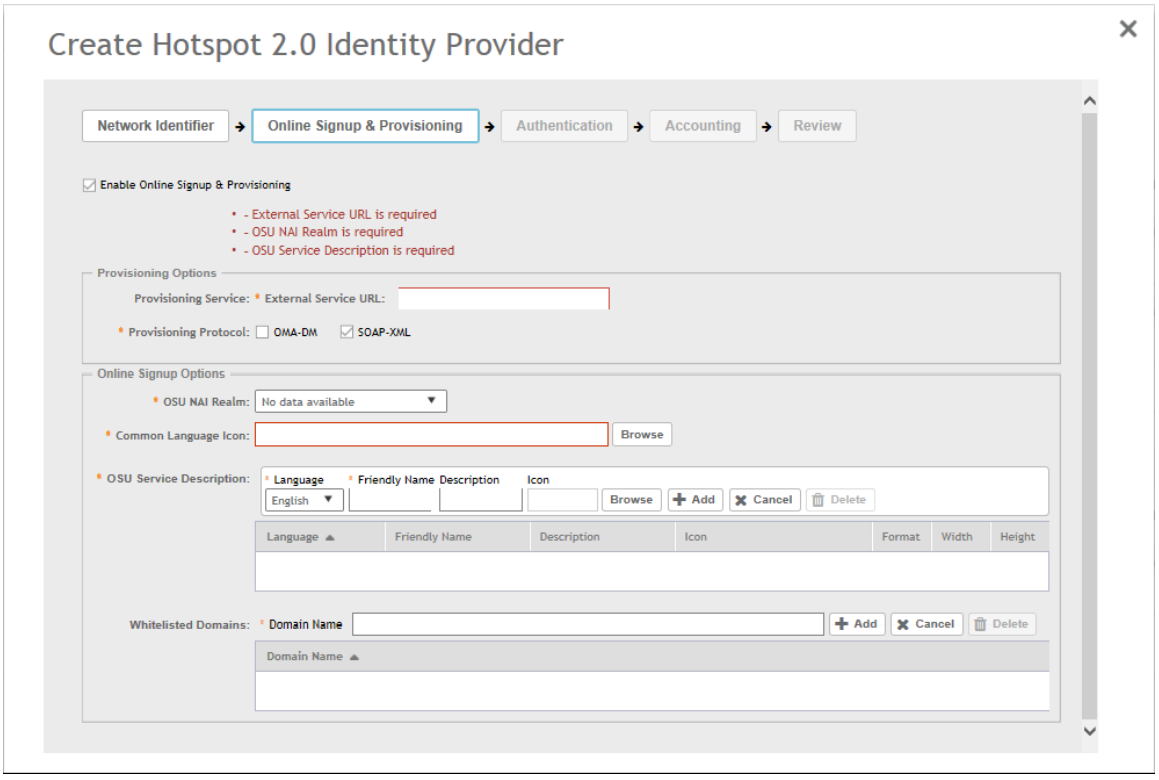


FIGURE 25 Identity Provider Configuration



Authentication in Remediation Flow

In remediation, the OSU module in the controller provides the URL to the device as the URL for the portal. This is for manual remediation flow. The OSU redirects the UE to the portal path with the following parameters:

- WsgWlanId—WLAN ID
- ClientMac—UE MAC address
- RedirectURI—URL, which the portal redirects to the UE at the end of the flow.
- ExternalUsername—Username used for remote authentication
- InternalUsername—Username sent for digest authentication
- AuthServerName—Authentication name as seen in the controller web interface - **Services & Profiles** > **Hotspots and Portals** > **Hotspot 2.0** > **Identity Provider > Authentication**.

For example:

```
https://EXTERNAL_PORTAL_FQDN:EXTERNAL_PORTAL_PORT/ EXTERNAL_PORTAL_PATH?WsgWlanId=1&ClientMac=98:0C:82:5E:
34:10&RedirectURI=http://127.0.0.1:1234 &ExternalUsername= testuser1-uid&InternalUsername=
e552a465-1873-4d44@osuserver.hs20.ruckus&AuthServerName=radius&RemediationReason=expired_password
```

The following is the request content for remediation authentication.

Request Content

```
{
"MSG-ID":< Unique ID for the message>,
"APIVersion":"3.1.0",
"Vendor" : "Ruckus",
"RequestPassword" : <NBI password as set in the controller>,
"UE-MAC":<Device MAC>
"RequestType":"RegistrationOnboarding",
"RequestCategory":"UserManagement",
"Input":{
"userLookupParameters":{
"loginName":<internal user name>,
"authenticationMethod":"MO"
},
"hsReleaseVersion":"2",
"credentials":{
"loginName":<external user name>,
"loginPassword":<user password>
"authenticationServerName":<authentication sever name>
},
"remediation":"true"
}
}
```

Parameters

- *MSG-ID* identifies the related request and response
- *UE-MAC* value is taken from the request parameter - *ClientMac*
- *loginName* (internal user name and external user name) and *UE-MAC* is retrieved from request parameters using the value names respectively - *InternalUsername*, *ExternalUsername* and *ClientMac*
- *loginPassword* is taken from user input

OCSP Stapling Support

- OCSP Stapling Support Overview..... 51

OCSP Stapling Support Overview

Hotspot 2.0 (R2) technical specification requires OCSP Stapling as specified in RFC 6066 section 8 (certificate status request) as part of the TLS extension. It requires the devices to get the certificate revocation status and check that AAA server (for Anon-TLS or EAP-TTLS) certificates or OSU server certificate have not been revoked using OCSP within the TLS connection.

Controller has two different modules which handles this requirement:

1. NGINX - Provisioning and remediation servers in the controller are running on the top of Tomcat, but Tomcat does not support OCSP Stapling. To support OCSP Stapling, NGINX, which is a 3rd party proxy server is used. NGINX is positioned ahead of the Tomcat web server, proxying the content of each request to the Tomcat server once the TLS has been established.
2. RAC - For Hotspot 2.0, there are two points in the call flow where the controller RAC module interacts with the OCSP server.
    a. During Anonymous TLS for onboarding call flow as seen in the figure.
    b. During EAP-TTLS access flow as seen in the figure.

Client (mobile device) includes the Certificate Status request in the TLS request message and RAC module includes the Certificate Status in the TLS response message.

The OCSP message is a standard message derived based on the certificate uploaded for the given service provider.

FIGURE 26 Interaction with OCSP server during Anonymous TLS

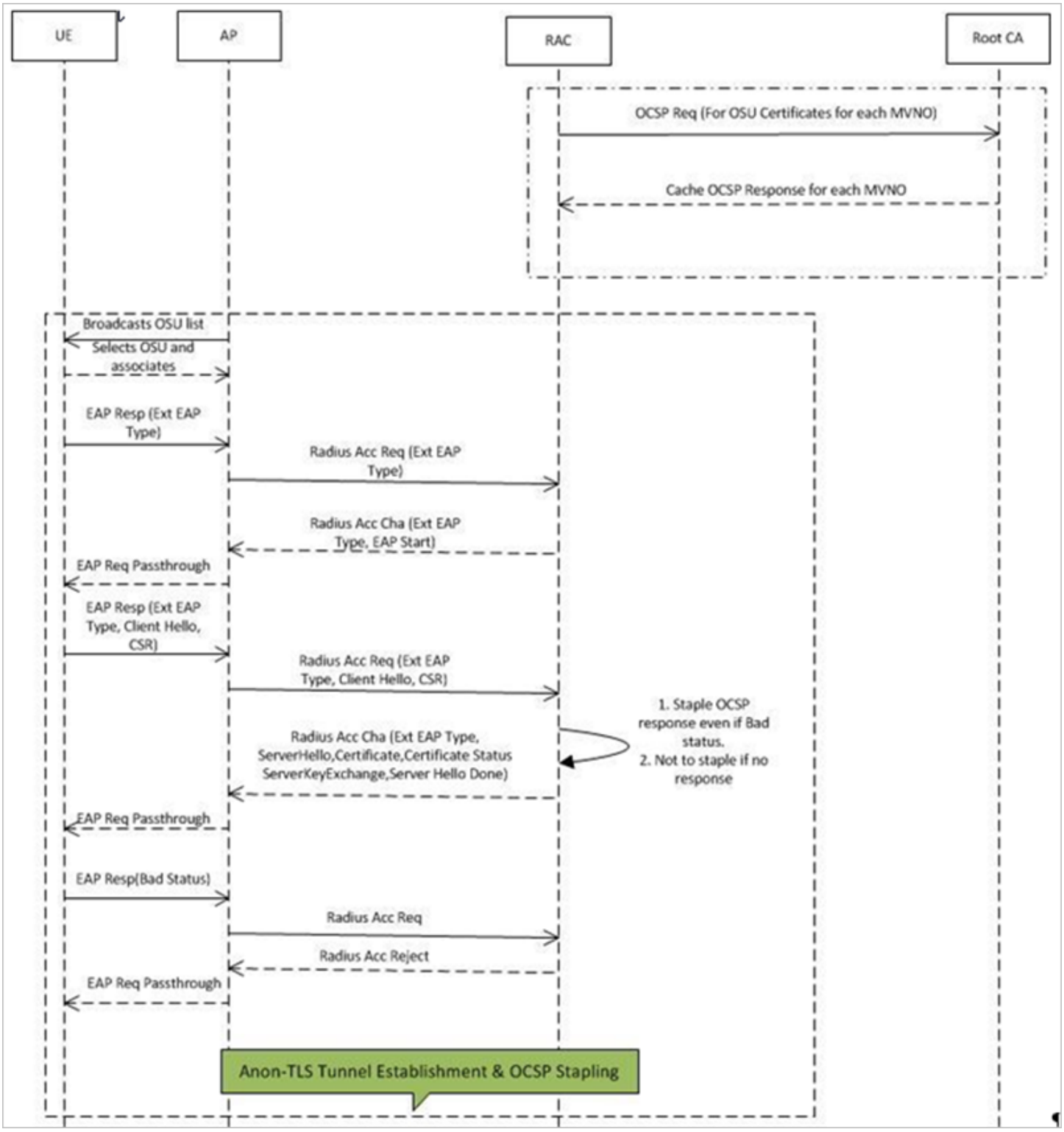
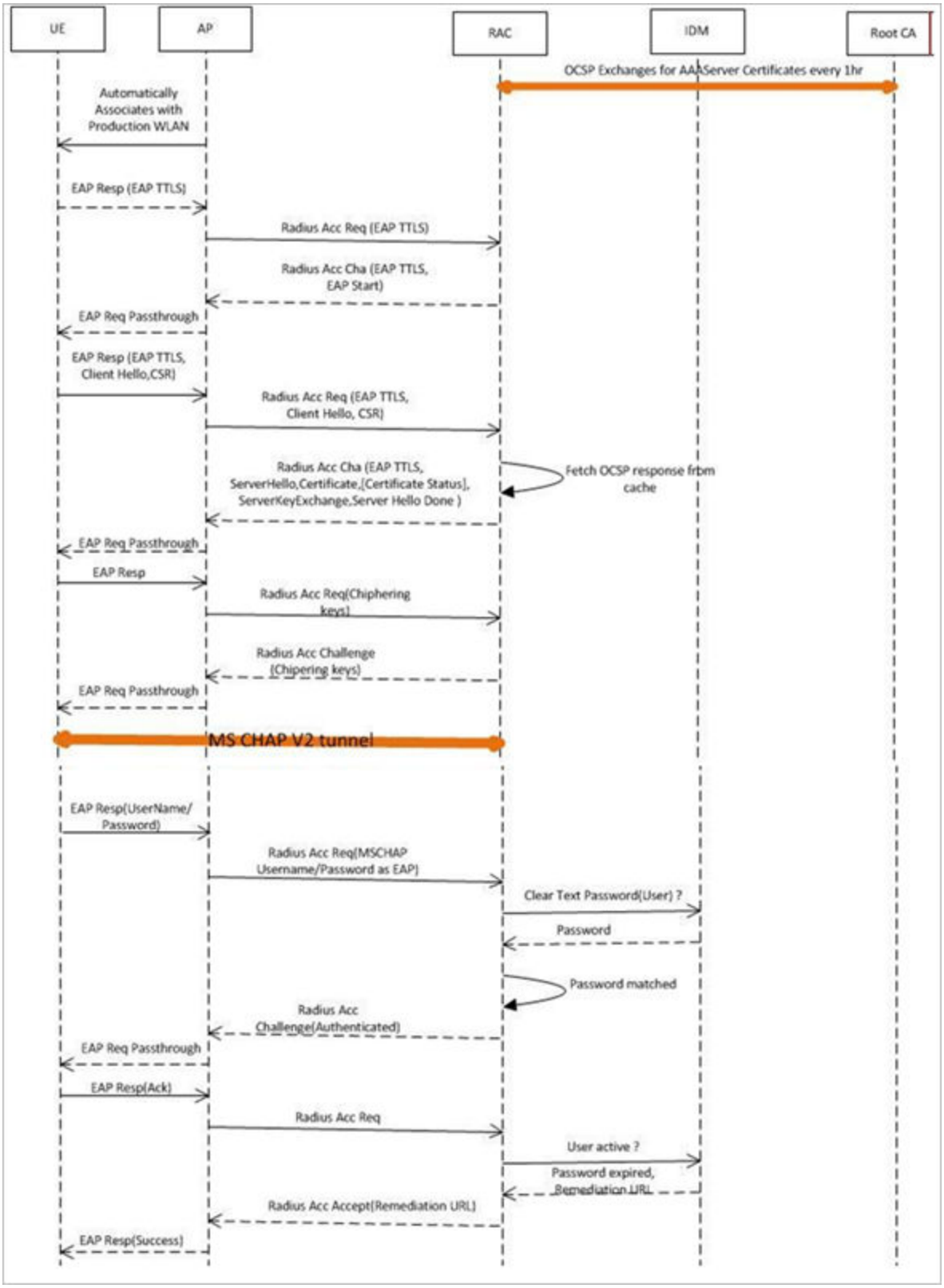


FIGURE 27 Interaction with OCSP server during EAP-TLS



The figures show the important fields in the OCSP messages. These are standard message, which operators and administrators should be aware of for successful call flows. Possible values of the certificate status field is good, bad or revoked.

> **NOTE**
> If the client (mobile device) requests for Certificate Status request, RAC provides the status if it is available. In case the certificate status is not provided it is up to the client if it wants to continue or abort the call.

FIGURE 28 Important OCSP Message

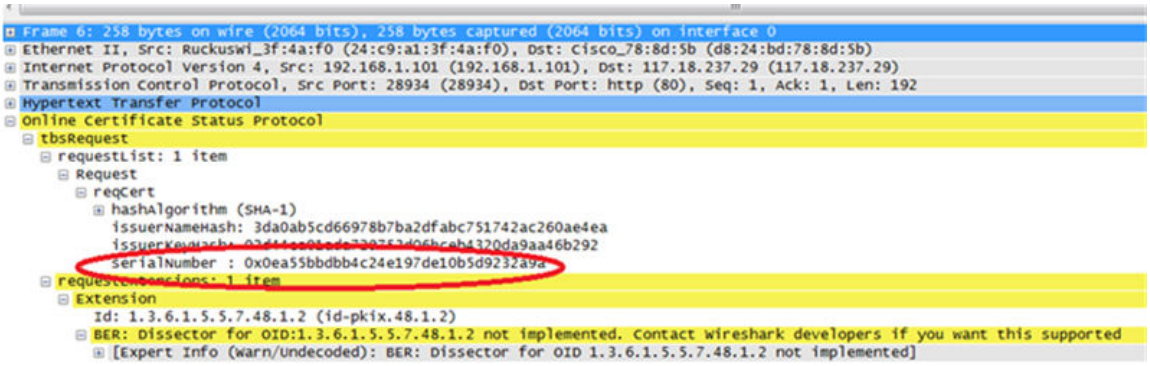
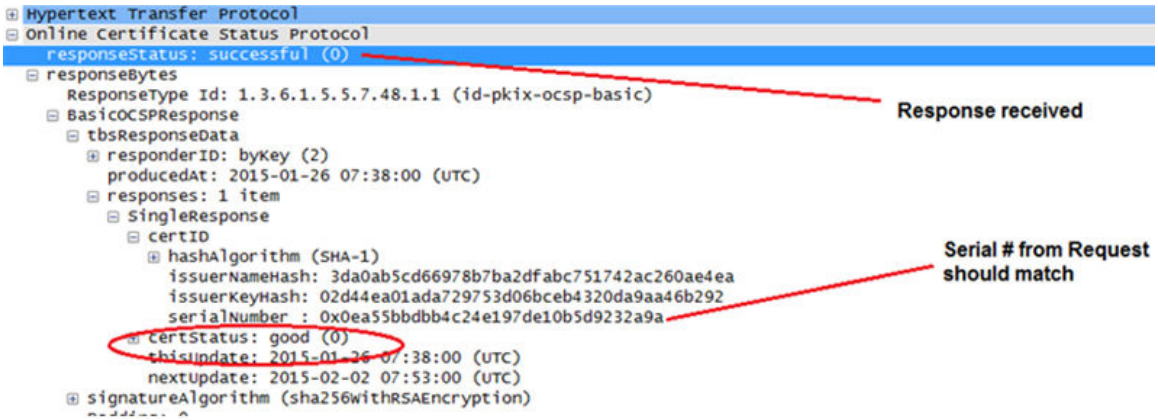


FIGURE 29 OCSP Response Message



Apple and Samsung Hotspot 2.0 Release 1 (Passpoint) Devices

- Apple and Samsung Hotspot 2.0 Release 1 (Passpoint) Devices Overview..... 55

Apple and Samsung Hotspot 2.0 Release 1 (Passpoint) Devices Overview

Apple and Samsung have a subset of new devices, which support new configuration file format (XML based) with credentials for accessing authentication of Hotspot 2.0 SSIDs.

The following are the Apple devices that support the R1 provisioning via a mobile configuration profile:

- iOS7 (5, 5C, 5S) and newer supports R1
- Mac OS X Mavericks and newer supports R1

NOTE
It was impossible to distinguish between the iPad 2 (which does not support HS2.0 R1) and the iPad Mini v1 (which does support HS2.0 R1). Due to that, Ruckus chose to exclude iPad 2 from the provisioning option so as not to offer provisioning to unsupported devices.

To view the Samsung devices that support the R1 provisioning via a mobile configuration profile, click on the following link. `http://www.wi-fi.org/product-finder-results?sort_by=default&sort_order=desc&categories=1,2,4,5,3&capabilities=1&companies=362`

COMMSCOPE®
RUCKUS®

© 2021 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com