Ruckus Wireless™ SmartCell Gateway™ 200 and Virtual SmartZone High-Scale

Hotspot 2.0 Reference Guide for SmartZone 3.5.1

Part Number: 800-71526-001 Rev A
Published: 14 June 2017

Contents

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

About this Guide

This SmartCell Gateway™ (SCG) 200 and Virtual SmartZone High-Scale (vSZ-H) Hotspot 2.0 Reference Guide describes the Hotspot 2.0 technology and provides configuration guidelines that the SCG-200/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.

NOTE: Refer to the release notes shipped with your product to be aware of certain challenges when upgrading to the latest version of SmartZone.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support Web site at https://support.ruckuswireless.com/contact-us.

Document Conventions

Table 1: Text conventions on page 6 and Table 2: Notice conventions on page 6 list the text and notice conventions that are used throughout this guide.

Table 1: Text conventions

Convention	Description	Example
`message phrase`	Represents information as it appears on screen	`[Device Name] >`
`user input`	Represents information that you enter	`[Device Name] > set ipaddr 10.0.0.12`
user interface controls	Keyboard keys, software buttons, and field names	Click **Start** > **All Programs**
screen or page names		Click **Advanced Settings**. The **Advanced Settings** page appears.

Table 2: Notice conventions

Notice type	Description
NOTE:	Information that describes important features or instructions

Notice type	Description
CAUTION:	Information that alerts you to potential loss of data or potential damage to an application, system, or device
WARNING:	Information that alerts you to potential personal injury

Terminology

The table lists the terms used in this guide.

Table 3: 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

Terminology	Description
OSU	Online Sign-Up
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
SCG	Smart Cell Gateway
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

Related Documentation

For a complete list of documents that accompany this release, refer to the Release Notes.

Online Training Resources

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

https://training.ruckuswireless.com.

Documentation Feedback

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

You can email your comments to Ruckus Wireless at: docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title
- Document part number (on the cover page)
- Page number (if appropriate)
- For example:
  - Administrator Guide for SmartZone 3.5.1
  - Part number: 800-71526-001
  - Page 88

Hotspot 2.0 Brief Overview 1

In this chapter:

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

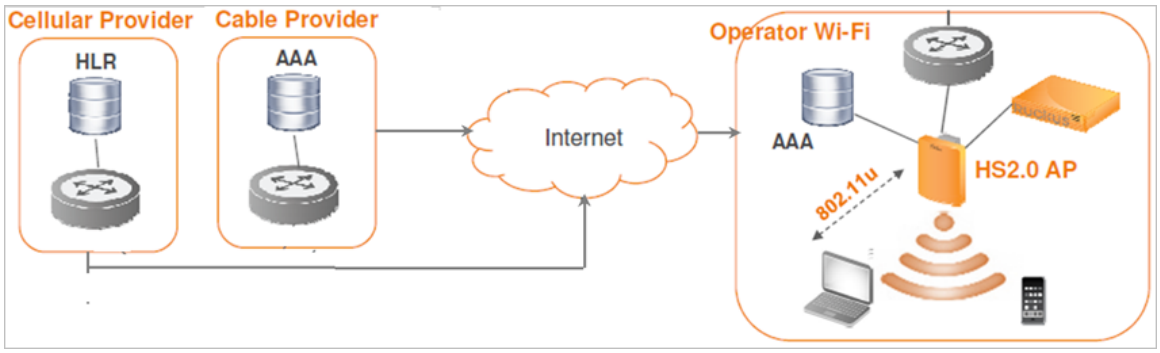
The Hotspot 2.0 Release 1 focuses on the Automated network discovery and selection and Secure authentication components, whereas release 2 goes into specification of Online sign-up and Policy management components.

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 figure below.

Figure 1: Working of Hotspot 2.0



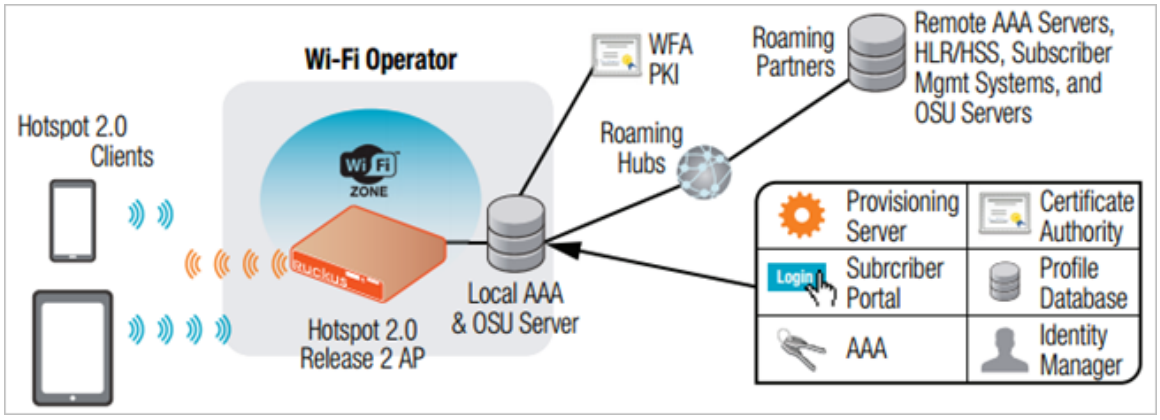
The onboarding WLAN for Hotspot 2.0 may be open WLAN or secure WLAN. The secure onboarding WLAN (OSEN) utilizes server-side only authentication, while the client side remains anonymous. The OSU service provider utilizes PPS-MO to provision necessary policy parameters such as expiration time, update interval, 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



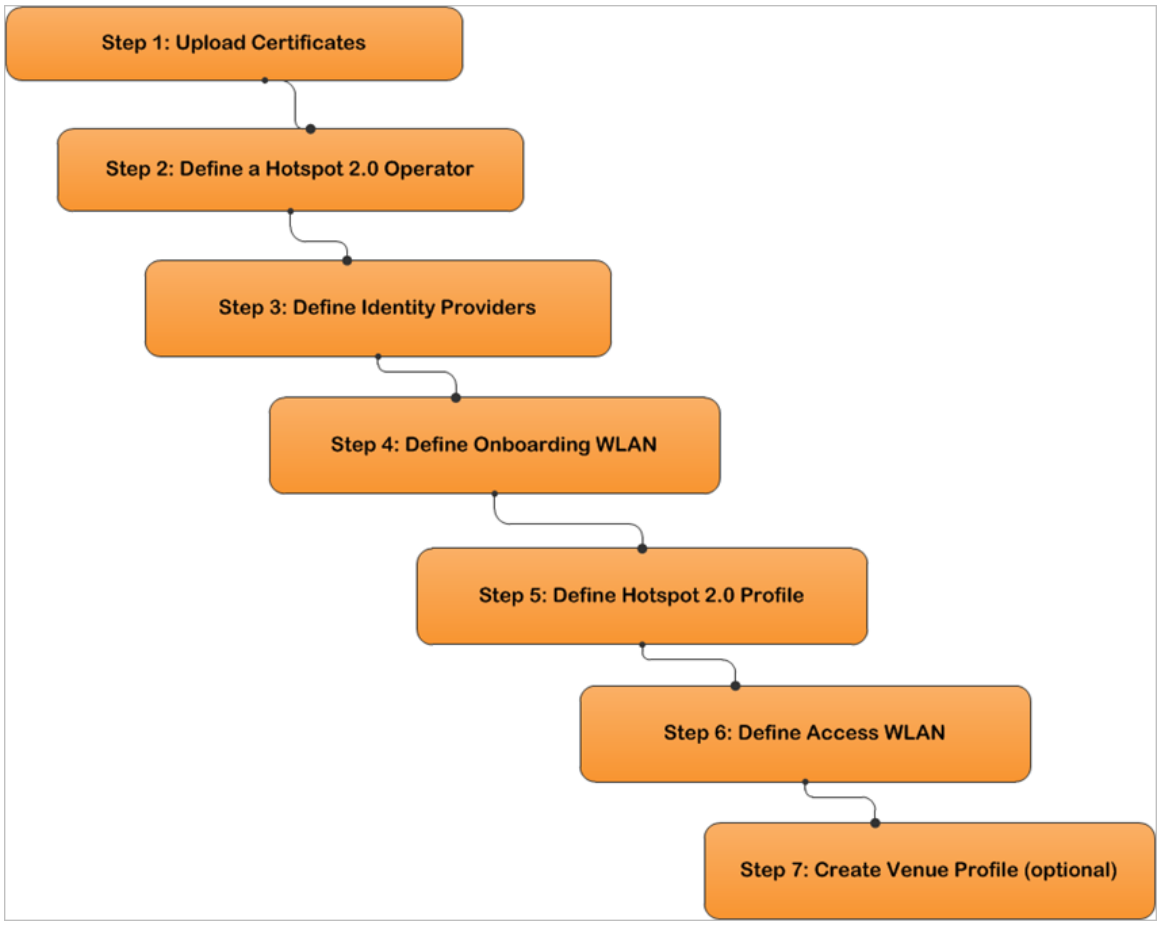
Configuring Hotspot 2.0

2

In this chapter:

The figure shows the entities that need to be configured to enable the Hotspot 2.0 R2 devices configuration flow.

Figure 3: Hotspot 2.0 Configuration Flow



NOTE: Hotspot 2.0 WLANs do not support IPv6.

Step 1: Uploading Certificates

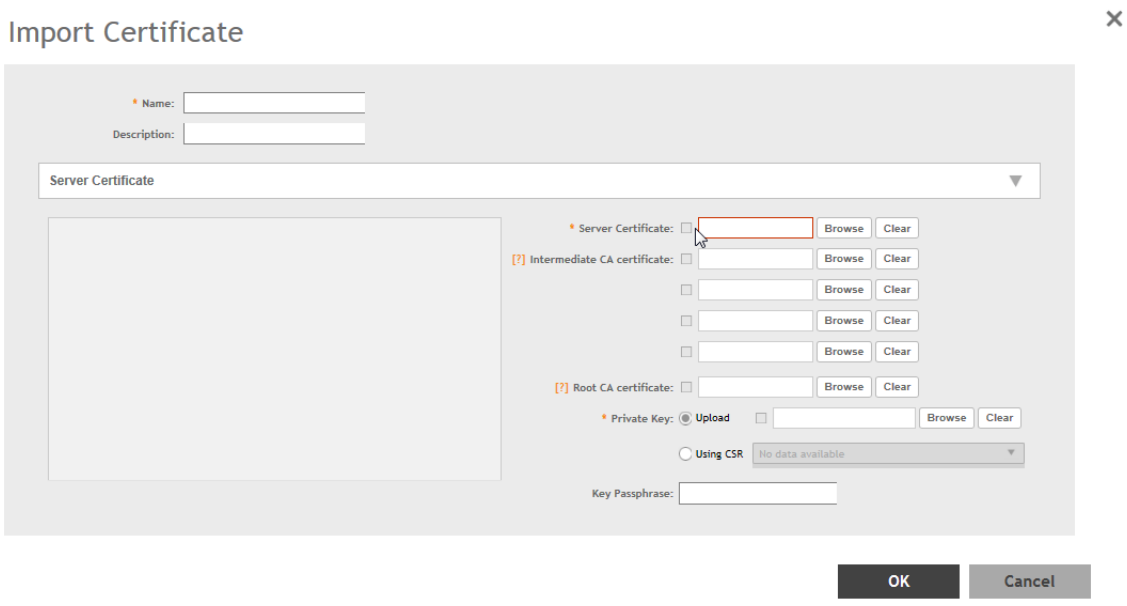
Uploading certificates is the first step in configuring Hotspot 2.0.

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

   For details on Certificate Store refer to the SmartCell Gateway 200 Administrator Guide (PDF) or the SmartCell Gateway 200 Online Help, which is accessible from the SCG Web interface.

Figure 4: Importing a Certificate



Step 2: Define Wi-Fi Operator Profile

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

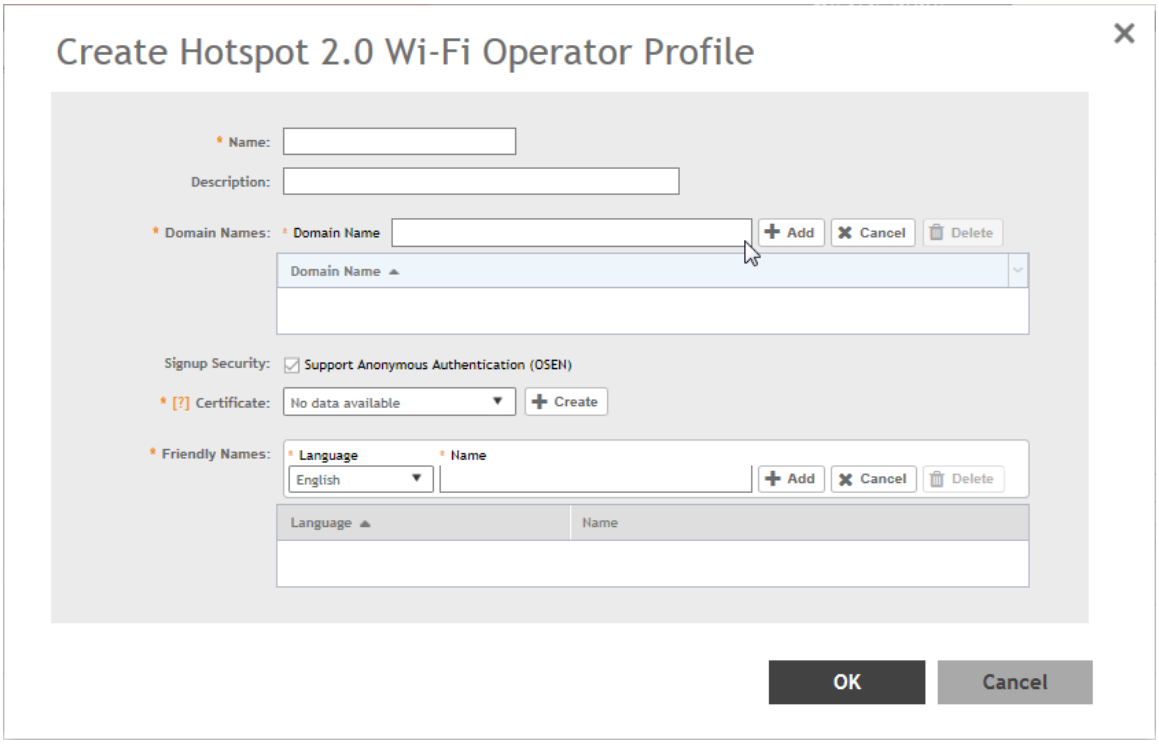
1. Click **Services & Profiles > Hotspots & Portals > Hotspot 2.0 > Wi-Fi Operator > Create** .
2. The **Create Hotspot 2.0 Wi-Fi Operator Profile**page appears.
3. Configure the settings in the table to create a Hotspot 2.0 Wi-Fi operator and set configuration options.

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.
Signup Security	This is an optional field and is disabled by default. Enabling would mean that operator supports secure onboarding (OSEN).
Certificate	Select the certificate for the operator - AAA. This can be the same certificate as the one used with OSU service.
Friendly Names	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 (OSEN).

NOTE: In case of Signup Security - Onboarding WLAN OSEN 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). OSEN 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**
5. Continue to Step 3: Define Identity Provider.

Figure 5: Hotspot Wi-Fi Operator Profile



6. You have completed defining the WiFi Operator Profile.

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 15
- Online SignUp and Provisioning on page 17
- Authentication on page 19
- Accounting on page 20
- Review on page 21

Network Identifier

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

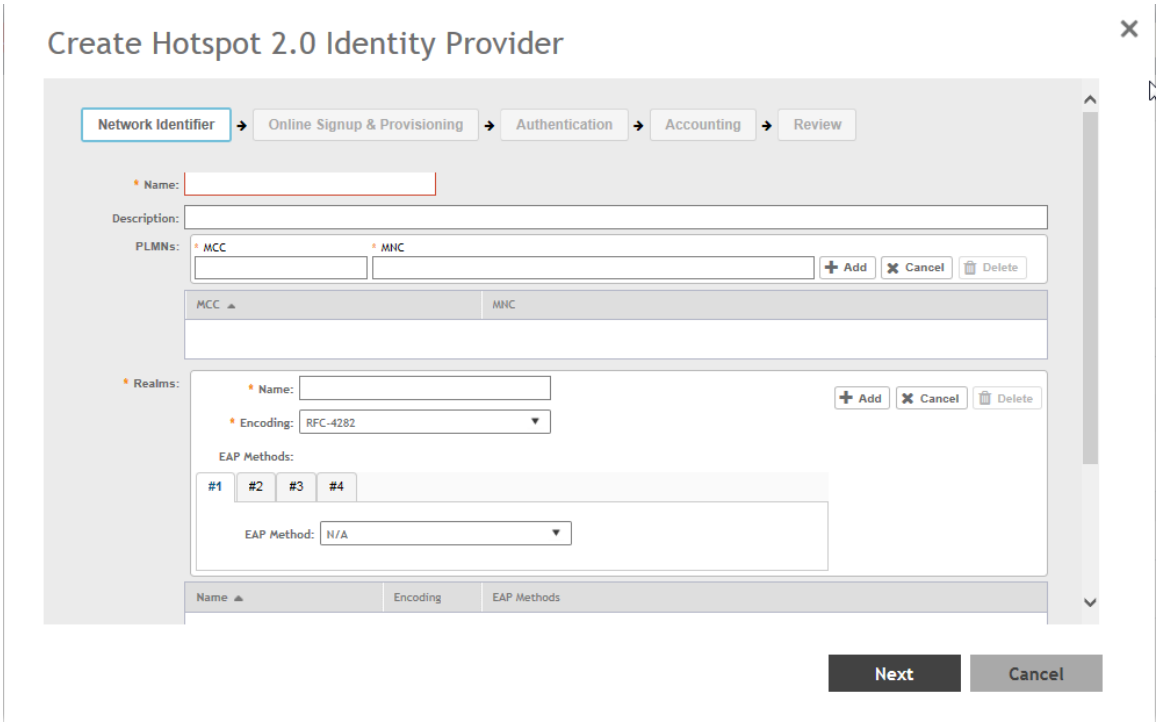
1. Click **Services & Profiles > Hotspots & Portals > Hotspot 2.0 > Identity Provider > Create**.
2. Configure the settings in the table to create a Hotspot 2.0 Network Identifier. Alternatively, the network identifier can be imported from an existing Hotspot 2.0 Wi-Fi operator.

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.

Figure 6: Hotspot Identity Provider - Network Identifier



Online SignUp and Provisioning

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

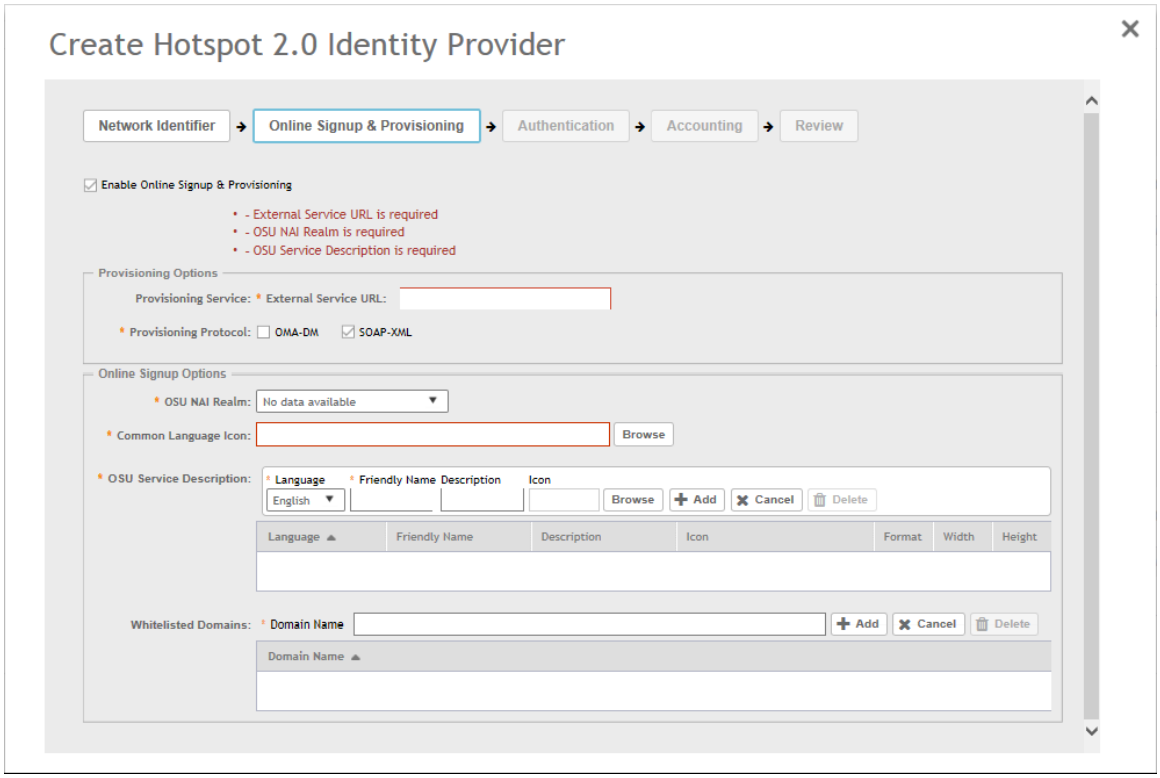
1. Click to enable **Online SignUp and Provisioning** to configure the service for the identity provider.
2. Alternatively you can skip this step to move to Authentication.
3. Configure the settings in the table below to create a Hotspot 2.0 SignUp and Provisioning.

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 or only with internal node/s of the PPS-MO. Administrator can select Internal Provisioning Service or External. By default it is internal, meaning the controller's online signup service provides this capability. In case external is selected, the administrator is required to fill the external OSU server URL. In this release only username/password credential are supported to be provisioned using the controller's Internal OSU. Policy and subscription parameters in the PPS-MO are not supported using the controller's internal OSU. Note:

Option	Description
	There can be only one identity provider configured for internal provisioning service.
Provisioning Protocol	If the provisioning service is internal, the protocol displayed is SOAP-XML. For external provisioning services, the communication protocols are OMA-DM and SOAP-XML by default.
OSU NAI Realm	This configuration is only for *External Provision Service*. In case of *Internal Provisioning Service*, the NAI realm should be configured per the authentication service, which is available during onboarding
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 Both External Provisioning URL and External Portal URL (in case it is internal provisioning server) will automatically be pushed to AP as whitelisted domains.

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

Figure 7: Hotspot Identity Provider - Online SignUp and Provisioning



Authentication

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

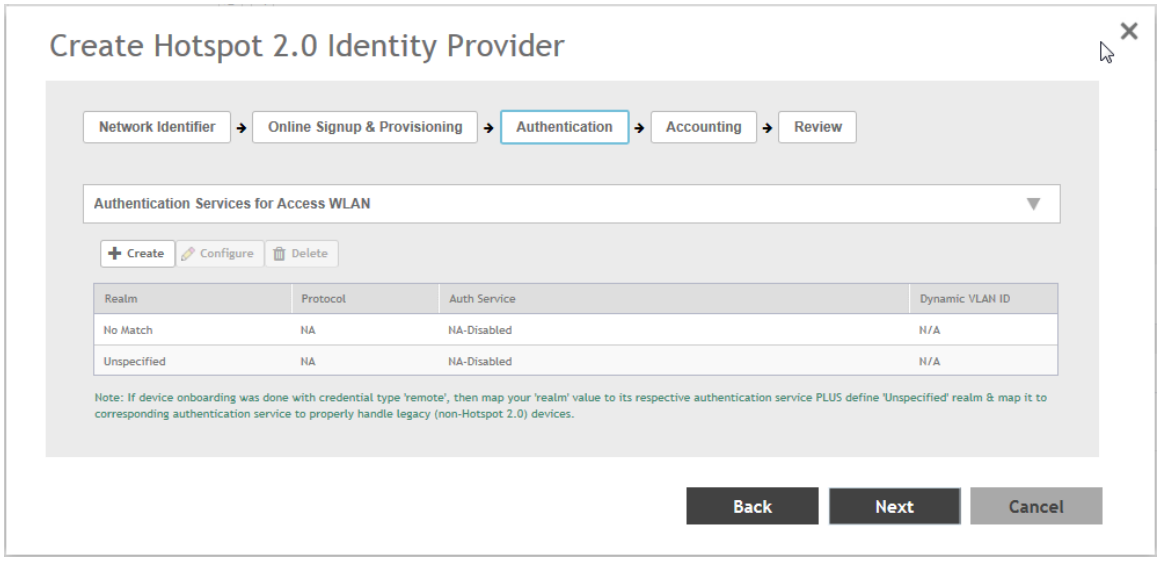
1. Click on Authentication to configure the service for the identity provider.
2. Configure the authentication option settings in the table to create a Hotspot 2.0 SignUp and Provisioning.

Option	Description
Option	**Description**
Realm	The administrator should configure the realm mapping to the authentication service. If the provisioned service is internal, meaning *Credential Type* is set to *Local* then the provisioning realm is bound to the Local database. For external provisioned service, meaning *Credential Type* is set to *Remote*, 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.

Figure 8: Hotspot Identity Provider - Authentication



Accounting

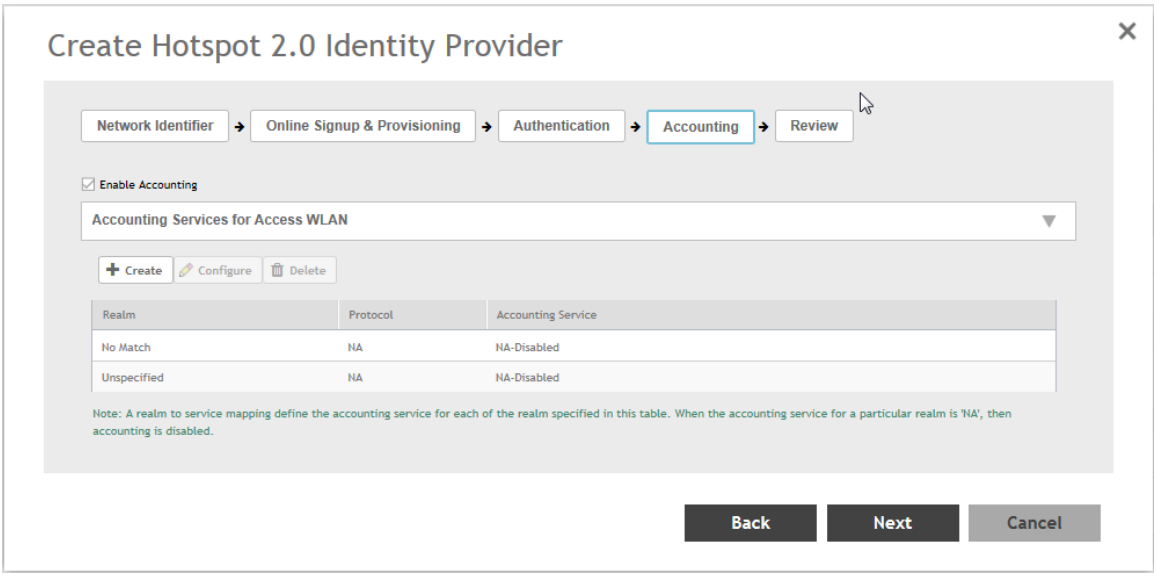
Follow these steps to create a Hotspot 2.0 Identity Provider - Accounting.

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	Description
Option	Description
Realm	If the authentication's realm is set as remote credential type, administrator should set this realm here to the customer's external accounting server. In case the authentication's realm is set as local credential type, the access accept will include the CUI attribute and its value will be the username which the user used for onboarding. This way, even if the access authentication is done with the controller's local database, accounting can still be proxy to the external accounting server based on CUI value. The controller's local database does not support accounting. The actual external accounting server should be preconfigured in **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.

Figure 9: 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 one Onboarding WLAN, which can be secure onboarding by selecting the Hotspot 2.0 secure signup (OSEN) or open onboarding by selecting guest onboarding, and access WLAN which is the Hotspot 2.0 WLAN.

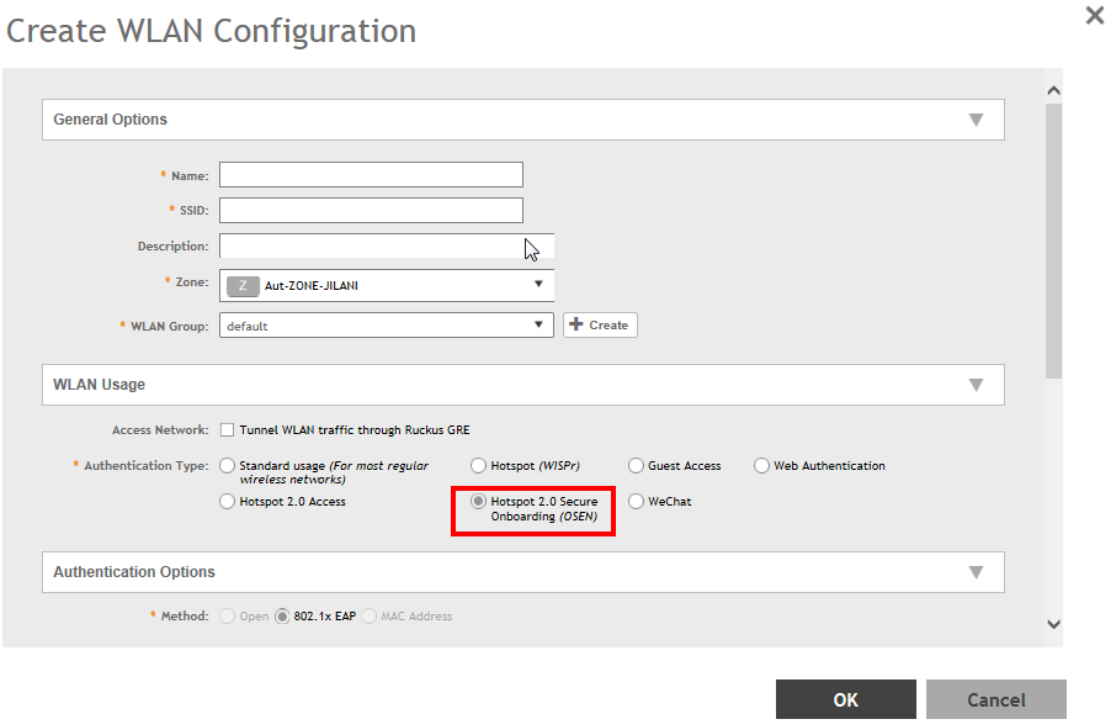
1. Define Secure Onboarding - Hotspot 2.0 OSEN
2. Define Open Onboarding - Guess Access
3. AP Zone - Guest Access

Define Secure Onboarding - Hotspot 2.0 OSEN

Follow these steps to configure Hotspot 2.0 OSEN authentication.

1. Click **Access Points > Access Points > AP Zones > WLANs > Create**.
2. On the *Create WLAN Configuration* page, navigate to **WLAN Usage> Authentication Type**
3. Enable **Hotspot 2.0 Secure Onboarding OSEN** profile.
4. Click **OK**. You have completed creating the Hotspot 2.0 OSEN authentication type.

Figure 10: Hotspot 2.0 Authentication Type

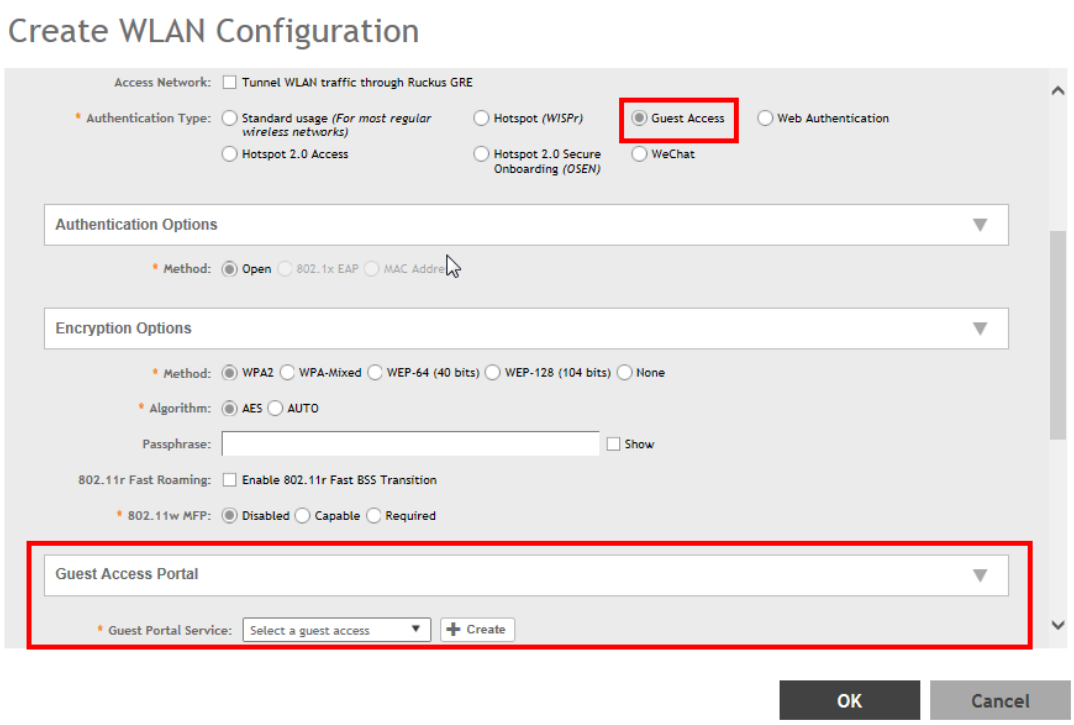


Define Open Onboarding - Guest Access

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

1. Click **Access Points > Access Points > AP Zones > WLAN > Create**.
2. On the Create WLAN Configuration page, select **WLAN Usage > Authentication Type > Guest Access** to enable Guest Access + Hotspot 2.0 Online Signup.
3. Click **OK**. You have completed enabling guest access for Hotspot 2.0 OSU.
4. Refer to Step 6: Define Access WLAN for defining Hotspot 2.0 WLAN.

Figure 11: Guest Access for Hotspot 2.0 OSU



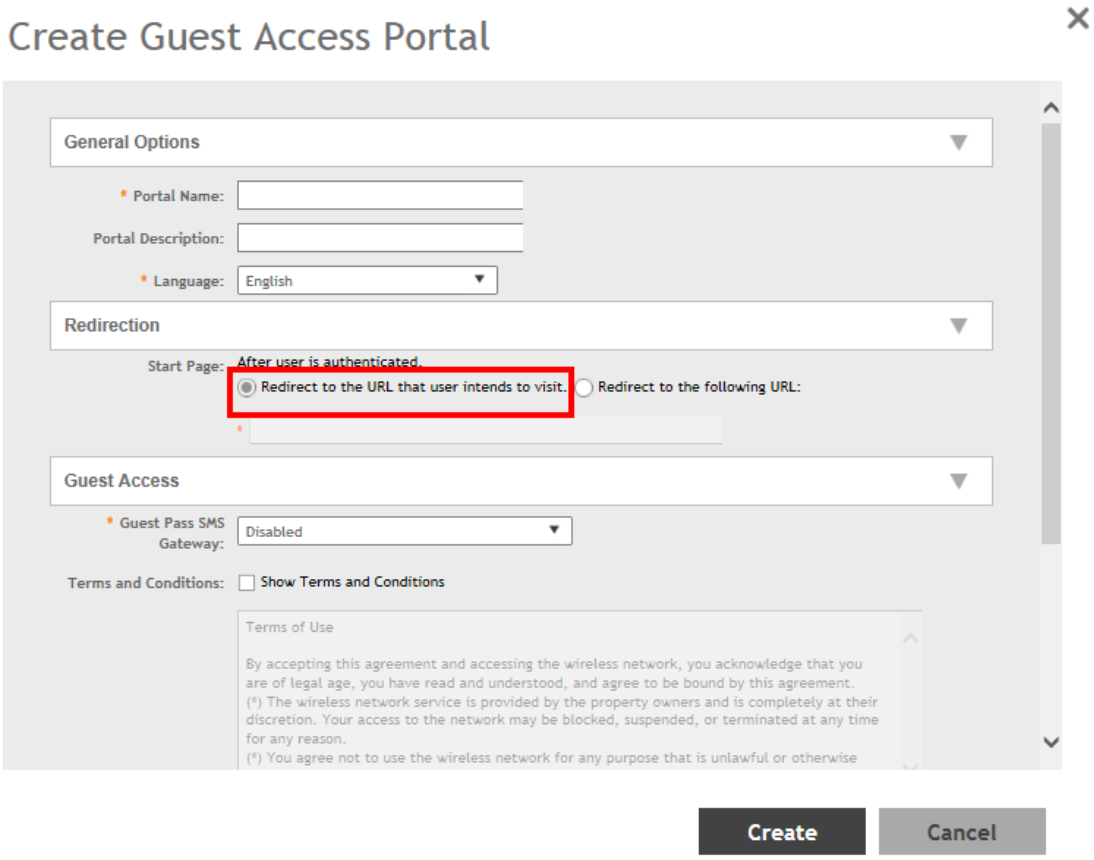
AP Zone - Guest Access

In addition to setting the guest access for Hotspot 2.0 OSU, the administrator needs to enable the Hotspot 2.0 device registration from this guest portal.

Follow these steps to enable Hotspot 2.0 device registration.

1. Click **Access Points > Access Points > AP Zones > WLAN > Create**.
2. On the Create WLAN Configuration page, select **WLAN Usage > Authentication Type > Guest Access** to enable Guest Access + Hotspot 2.0 Online Signup.
3. In the **Guest Access Portal** section, for **Guest Portal Service**, click **Create**.
4. On the *Guest Access Portal* page, for **Redirection > Start Page**, enable **Redirection to the URL that User intends to visit**.
5. In **Redirection > Start Page** enable *Redirect to the URL that the user intends to visit*.
6. Click **OK**. You have completed enabling Hotspot 2.0 device registration.

Figure 12: Guest Access



Step 5: Define Hotspot 2.0 Profile

Follow these steps to create a Hotspot 2.0 services profile.

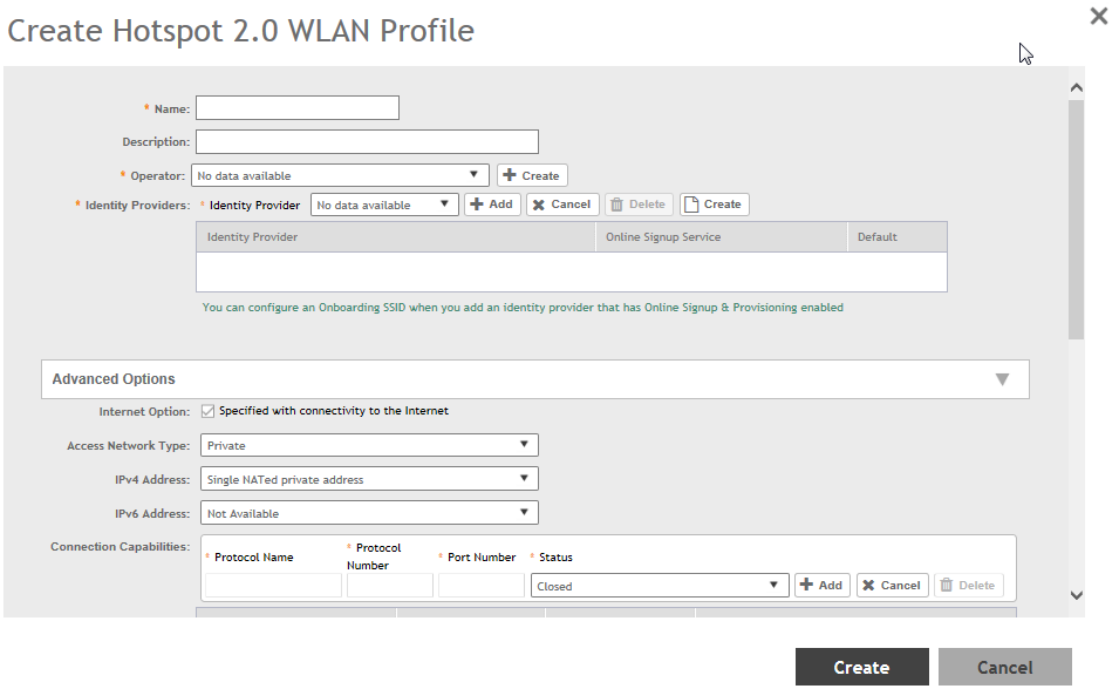
1. Click **Access Points > Access Points > AP Zones > WLAN > Create**.
2. On the Create WLAN Configuration page, select **WLAN Usage > Authentication Type > Hotspot 2.0 Access**.
3. In the **Hotspot 2.0 Profile** section, for **Hotspot 2.0 Profile**, click **Create**. The *Create Hotspot 2.0 WLAN Profile* page appears.
4. Configure the WLAN Profile Configuration Options in the table to create a Hotspot 2.0 WLAN profile.

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.

Option	Description
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. OSUSSID can be OSEN or OPEN [Guest]. **NOTE:** To create a new identity provider refer to Step 3: Define 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.
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.

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

Figure 13: Hotspot 2.0 Services Profile



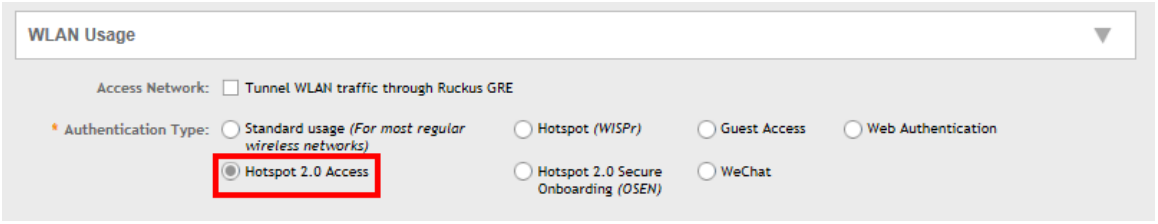
NOTE: Only provisioned devices with local database credentials can pass 802.1x Proxy and Hotspot 2.0 authentication.

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 **Access Points > Access Points > AP Zones > WLAN > Create**.
2. On the Create WLAN Configuration page, select **WLAN Usage > Authentication Type**
3. Enable **Hotspot 2.0 Access**.
4. Click **OK**. You have completed creating the Hotspot 2.0 authentication type.

Figure 14: Hotspot 2.0 Authentication Type



Step 7: Create Venue Profile

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

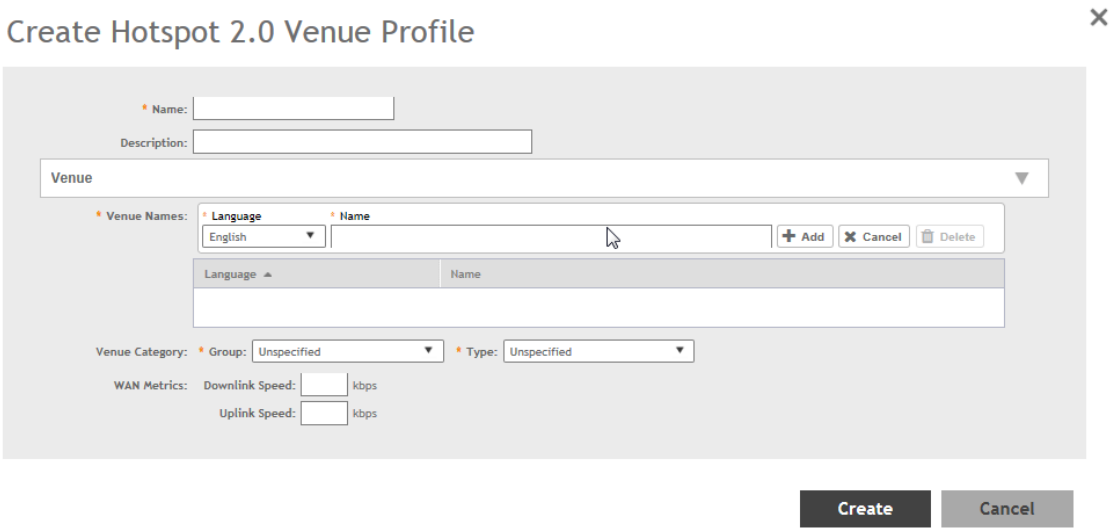
1. Click **Access Points** > **Access Points** > **AP Zones** > **Configuration** > **Configure**.
2. On the *Configure Group* page, go to Advanced Options section.
3. For **Hotspot 2.0 Venue Profile** click **Create**. The *Create Hotspot 2.0 Venue Profile* page appears.
4. Configure the Venue profile configuration options in the table below to create a Hotspot 2.0 WLAN profile.

Option	Description
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 Options	
Venue Names	Create a new venue name. Select the language and enter the venue name in that language.
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/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.

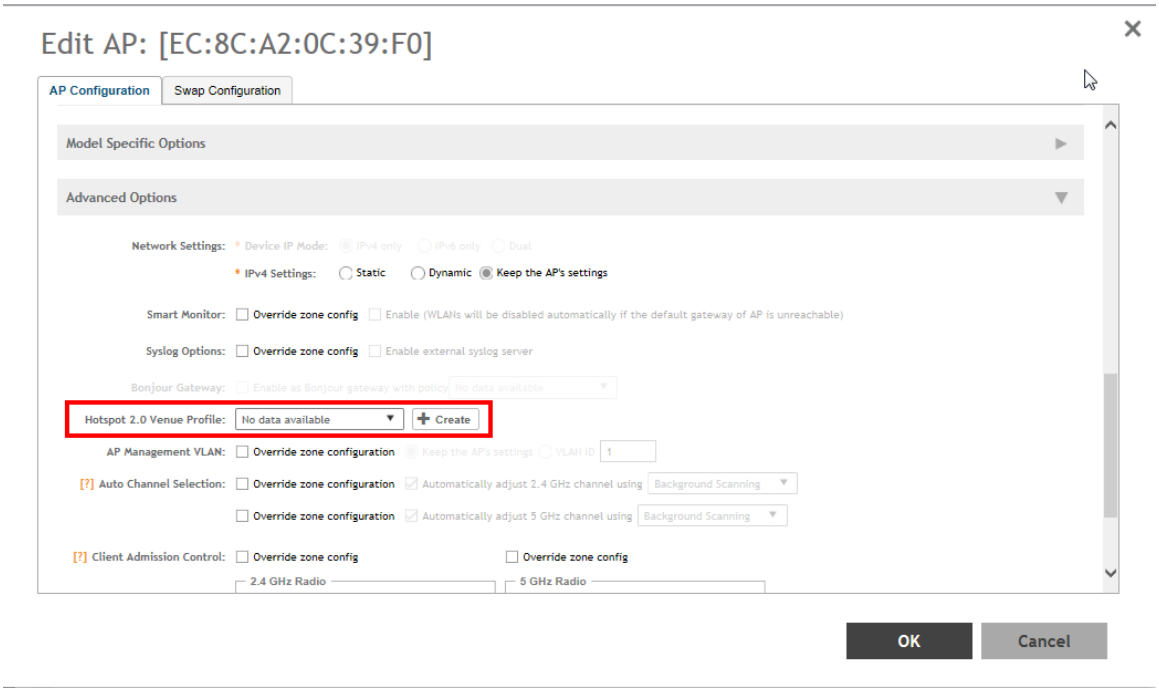
Figure 15: Hotspot 2.0 Venue Profile in AP Zone



Adding Venue Profile in AP

1. Click **Access Points** > **Access Points** > **AP** > **Configuration** > **Configure**.
2. On the *Configure Group* page, go to **Advanced Options** section.
3. For **Hotspot 2.0 Venue Profile** click **Create**. The *Create Hotspot 2.0 Venue Profile* page appears.
4. Configure the settings as explained in the above table.
5. Click **OK**.

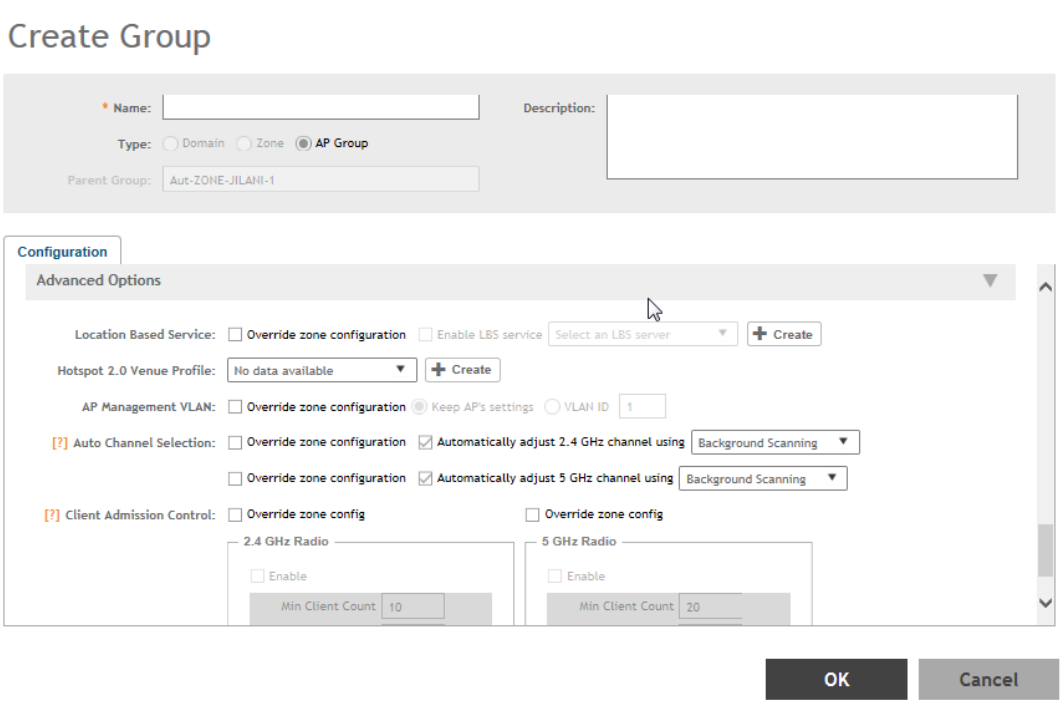
Figure 16: Hotspot 2.0 Venue Profile in AP



Adding Venue Profile in AP Group

1. Click **Access Points** > **Access Points** > **AP Groups** > **Configuration** > **Configure**.
2. On the *Configure Group* page, go to **Advanced Options** section.
3. For **Hotspot 2.0 Venue Profile** click **Create**. The *Create Hotspot 2.0 Venue Profile* page appears.
4. Configure the settings as explained in the above table.
5. Click **OK**.

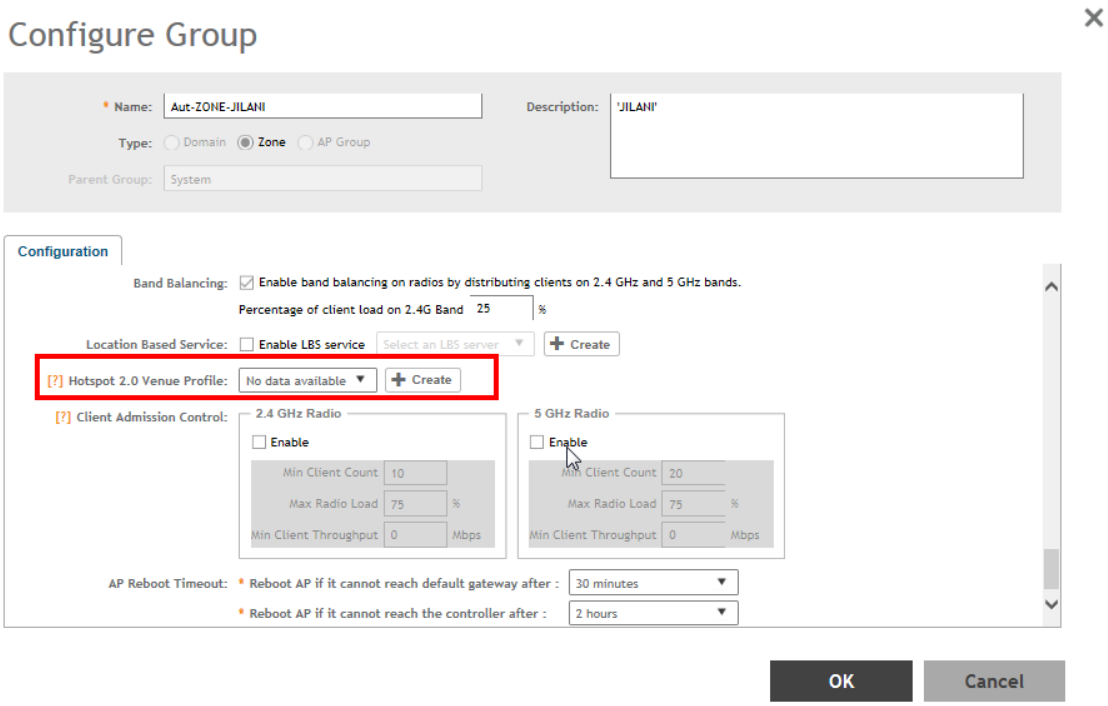
Figure 17: Hotspot 2.0 Venue Profile in AP Group



Adding Venue Profile in AP Zone

1. Click **Access Points** > **Access Points** > **Zone** > **Configuration** > **Configure**.
2. On the *Configure Group* page, go to **Advanced Options** section.
3. For **Hotspot 2.0 Venue Profile** click **Create**. The *Create Hotspot 2.0 Venue Profile* page appears.
4. Configure the settings as explained in the above table.
5. Click **OK**.

Figure 18: Hotspot 2.0 Venue Profile in AP Zone


Configure Group
* Name: Aut-ZONE-JILANI
Description: 'JILANI'
Type: Domain Zone AP Group
Parent Group: System
Configuration
Band Balancing: Enable band balancing on radios by distributing clients on 2.4 GHz and 5 GHz bands.
Percentage of client load on 2.4G Band 25 %
Location Based Service: Enable LBS service Select an LBS server Create
[?] Hotspot 2.0 Venue Profile: No data available Create
[?] Client Admission Control:
2.4 GHz Radio
Enable
Min Client Count 10
Max Radio Load 75 %
Min Client Throughput 0 Mbps
5 GHz Radio
Enable
Min Client Count 20
Max Radio Load 75 %
Min Client Throughput 0 Mbps
AP Reboot Timeout: * Reboot AP if it cannot reach default gateway after : 30 minutes
* Reboot AP if it cannot reach the controller after : 2 hours
OK
Cancel

Hotspot 2.0 R2 Device Workflow 3

In this chapter:

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 OSEN onboarding or OPEN onboarding.

- In case the OSU SSID is OSEN, 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 OSEN 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.

RAC uses the authentication's profile's realm mapping configuration (composed list of all authentication profiles related to all identity providers selected in the HS2.0 profile) to locate the authentication service for authenticating this device. The options are Local database or external RADIUS server. The Local database should be selected for realm, which is configured in the Online Signup & Provisioning as local credential type selected in the identity provider provides the internal provisioning service. In case of external RADIUS mapping, RAC only proxies the request, but in Local database case, RAC terminates the request using the OSU Server certificate. After terminating the request (for Local database mapping) RAC sends two JSON requests to IDM in sequence.

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 IBM'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

Short reference description.In SmartZone 3.1.1 authentication server includes RADIUS, AD, LDAP, Local database, OAuth. The table lists the available servers in each WLAN type.

Table 4: AAA Combinations

WLAN Type	Enable Proxy to the controller	RADIUS	AD	LDAP	Local Database	Always Accept	OAuth
802.1X	No				when proxy to the controller is enabled		
	Yes						
MAC Auth	No						
	Yes						
Hotspot (WISPr)	Yes						
Guest Access	Yes						
Onboarding	Yes						
Web Auth	No						
	Yes						

WLAN Type	Enable Proxy to the controller	RADIUS	AD	LDAP	Local Database	Always Accept	OAuth
Hotspot 2.0	Yes						

NOTE: Only provisioned devices with local database credentials can pass 802.1x Proxy and Hotspot 2.0 authentication.

Configuring Legacy Devices 4

In this chapter:

Legacy devices onboarding is an existing feature introduced in SmartZone 3.0 version. This release has the following enhancements:

- Onboarding portal is hosted at the controller instead at AP.
- New authentication service configuration. In addition to RADIUS, AD, and LDAP users can onboard using local database credential and their personal Facebook or Google+ or LinkedIn account.
- Group attribute mapping to user role is altered.

Online SignUp Portal Profile

Follow these steps to define the look and feel of the Online Signup Portal.

Context for the current task

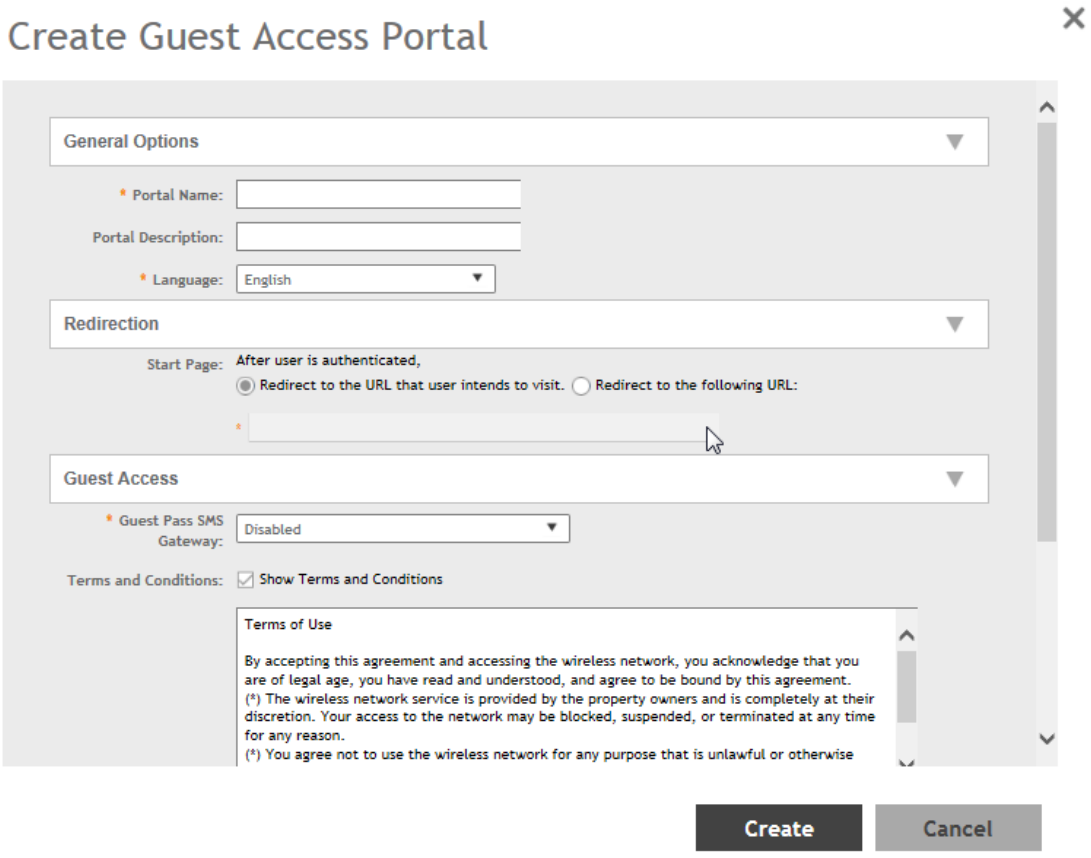
1. Click **Services & Profiles > Hotspots and Portals > Guest Access**.
2. Select the Zone and click **Create**. The Create Guest Access Portal page appears.
3. Configure the settings in the Table to create a Hotspot 2.0 OSU portal profile and set the Online SignUp Portal configuration options.

Option	Description
Portal Name	Enter the portal name.
Portal Description	Enter a description for the portal profile.
Language	This option allows the administrator to choose the language that the portal will be displayed to the user.
Start Page	Choose the URL redirection option once the user is authenticated.
Guest Pass SMS Gateway	Enter the gateway address through which the sms must be sent.
Terms and Conditions	Enter the terms and conditions that a user will accept on OSU. **NOTE:** Note: Portal title and T&C will NOT be presented in the selected language but in the same language as written in the Title and T&C text boxes.

Option	Description
Portal Logo	Choose the logo as seen by the user.
Portal Title	Enter the portal title as seen by the user.
Session Timeout	Enter the session timeout duration.
Grace Period	Enter the grace period duration.

4. Click **OK**. You have completed creating a Hotspot 2.0 online signup portal.

Figure 19: Online SignUp Portal form



Authentication Services

The administrator needs to configure the authentication services, which a user will be able to choose on onboarding. Follow these steps to define the authentication services.

1. Click **Services & Profiles > Hotspots & Portals > Identity Provideer > Authentication**.
2. The *Authentication Service for Access WLAN* page appears. Click **Create**.

3. The *Create Realm Based Authentication Service* page appears. Locate Service and click **Create**.
4. The *Create Authentication Service* page appears. Configure the Online SignUp Portal configuration options in the table to create an authentication service.

Option	Description
Option	**Description**
Name	Type a descriptive name for this authentication server (for example, “Active Directory”).
Friendly Name	The friendly name, which will be presented in the portal page.
Description (Optional)	Type a brief description of the profile.
Service Protocol	Choose the authentication services which the user will be able to choose on onboarding. (RADIUS, AD, LDAP, Local database, OAuth provider).
Group Attribute Value	Group attribute will potentially return from external authentication server after successful authentication. The controller uses it map the User Role (with all its attributes) to the user entity.

5. Click **Create** and click **OK**.

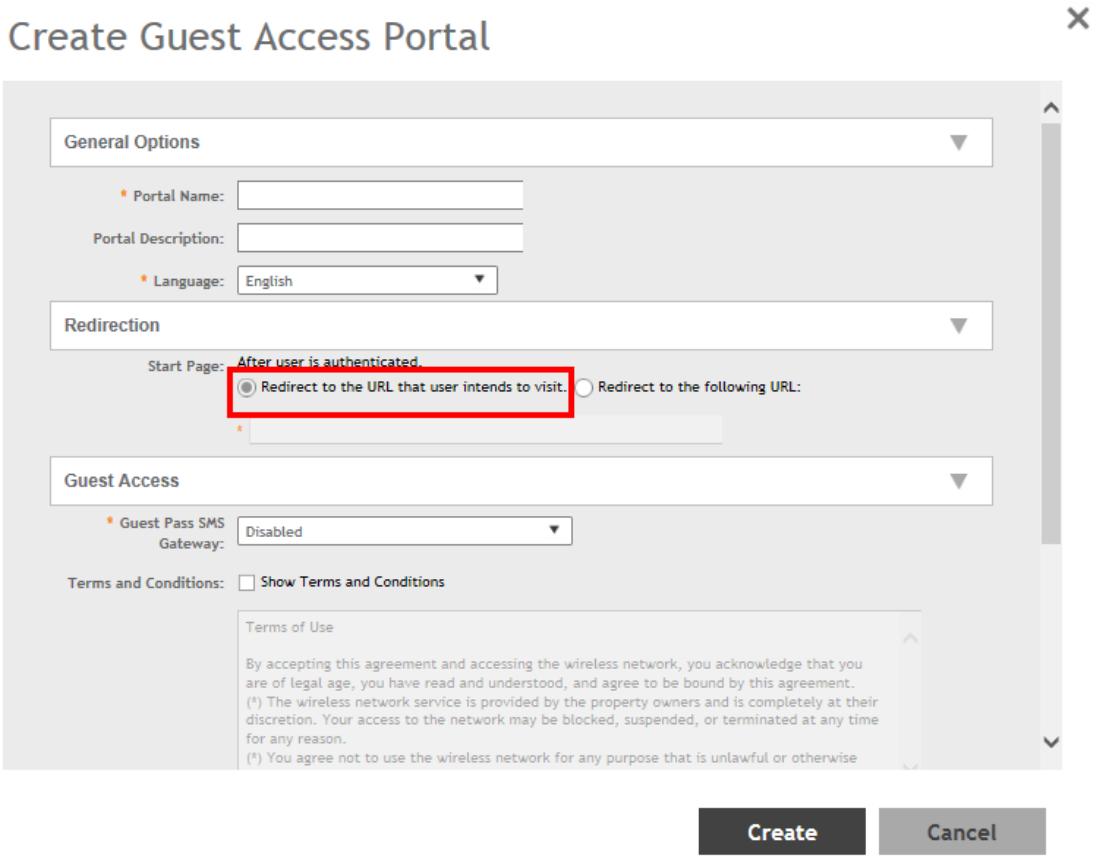
AP Zone - Guest Access

Users with legacy devices will have to manually select the onboard WLAN, the administrator will need to configure the guest access profile on the controller to facilitate the controller onboard in **WLAN > Guest WLAN**. This configuration sets the look and feel of the first page, which the user sees. This is run on the AP side.

Follow these steps to define the guest access configuration option.

1. Click **Access Points > Access Points > AP Zones > WLAN > Create**.
2. On the Create WLAN Configuration page, select **WLAN Usage > Authentication Type > Guest Access**.
3. In the **Guest Access Portal** section, for **Guest Portal Service**, click **Create**.
4. The related configuration options are language (labels on the URL page), title, logo and terms and conditions.
5. Click **OK**. You have completed creating / enabling guest access portal window.

Figure 20: Guest Access Redirection

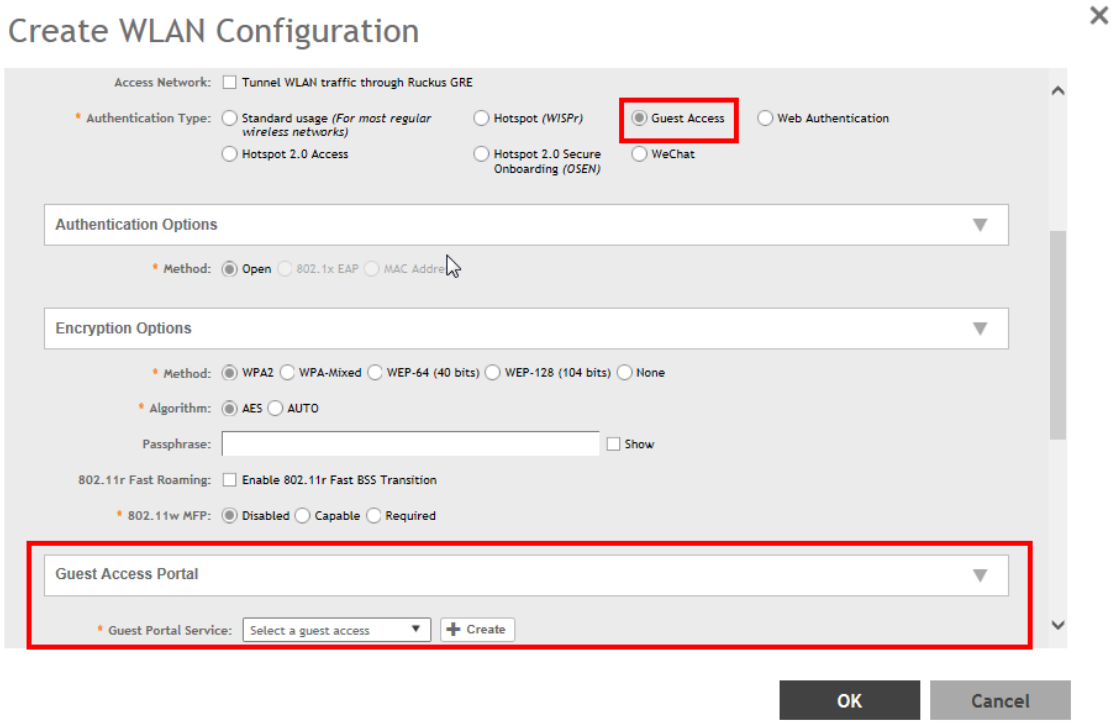


WLAN Guest Access

For legacy onboarding the user will have to manually select the open WLAN for onboarding. Follow these steps to configure the following settings.

1. Click **Access Points > Access Points > AP Zones > WLAN > Create**.
2. On the Create WLAN Configuration page, select **WLAN Usage > Authentication Type > Guest Access** enable Guest Access + Hotspot 2.0 Online Signup..
3. Click **OK**. You have completed enabling guest access for legacy devices.

Figure 21: Configuring Guest Access for Legacy Devices


Create WLAN Configuration
Access Network: Tunnel WLAN traffic through Ruckus GRE
* Authentication Type: Standard usage (For most regular wireless networks)
Hotspot (WISPr)
Guest Access
Web Authentication
Hotspot 2.0 Access
Hotspot 2.0 Secure Onboarding (OSEN)
WeChat
Authentication Options
* Method: Open 802.1x EAP MAC Addre
Encryption Options
* Method: WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None
* Algorithm: AES AUTO
Passphrase: Show
802.11r Fast Roaming: Enable 802.11r Fast BSS Transition
* 802.11w MFP: Disabled Capable Required
Guest Access Portal
* Guest Portal Service: Select a guest access Create
OK
Cancel

Appendix

A

External Onboarding and Remediation Portal Integration

In this chapter:

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 chapter.

Authentication in Onboarding Flow

Authentication against a remote database or against the local 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 as either LDAP/AD/ RADIUS/Local Database.

Request Content

```
{
"MSG-ID":< Unique ID for the message>,
"APIVersion":"3.1.0",
"Vendor" : "Ruckus",
"RequestPassword" : "<NBI password as set in SCG>,
"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 22: Authentication Configuration

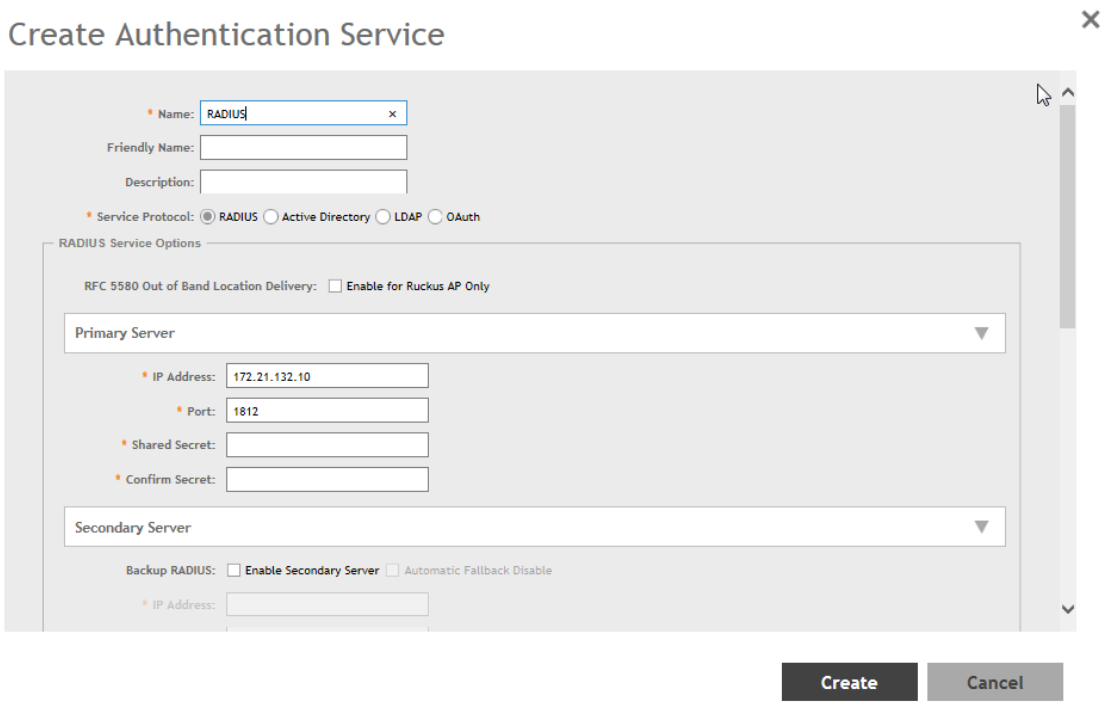
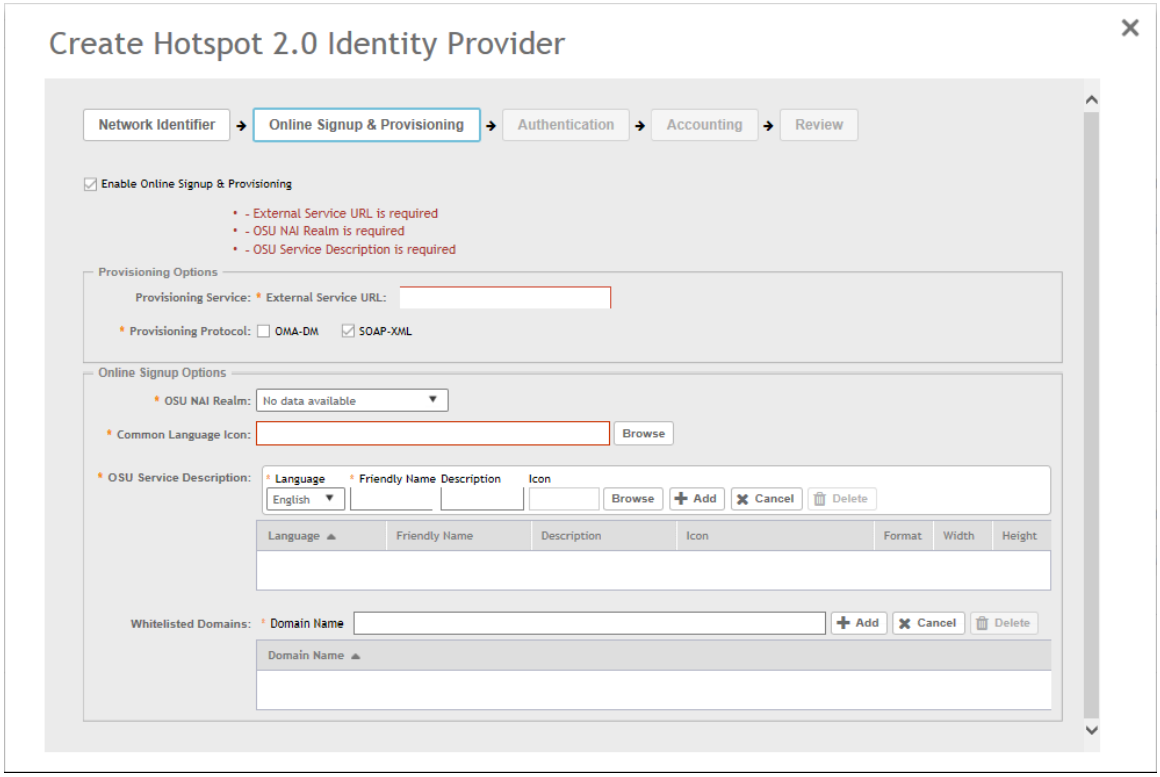


Figure 23: Identity Provider Configuration



Authentication in Remediation Flow

Short reference description.

In remediation, OSU module in 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**.

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 SCG>,
"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

Appendix

B

OCSP Stapling Support in SCG

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.

SmartZone 3.2 has 2 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 24: Interaction with OCSP server during Anonymous TLS

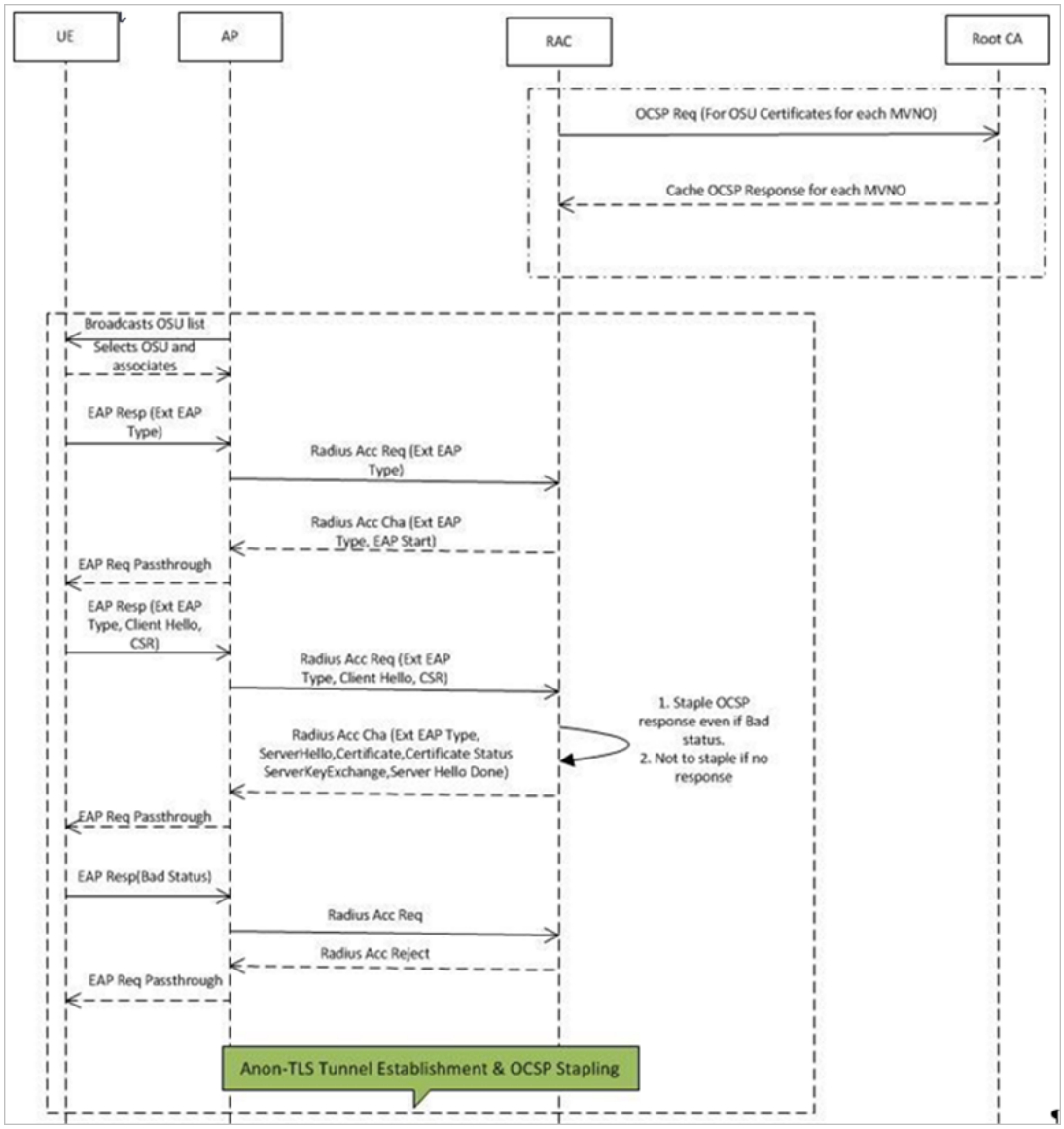
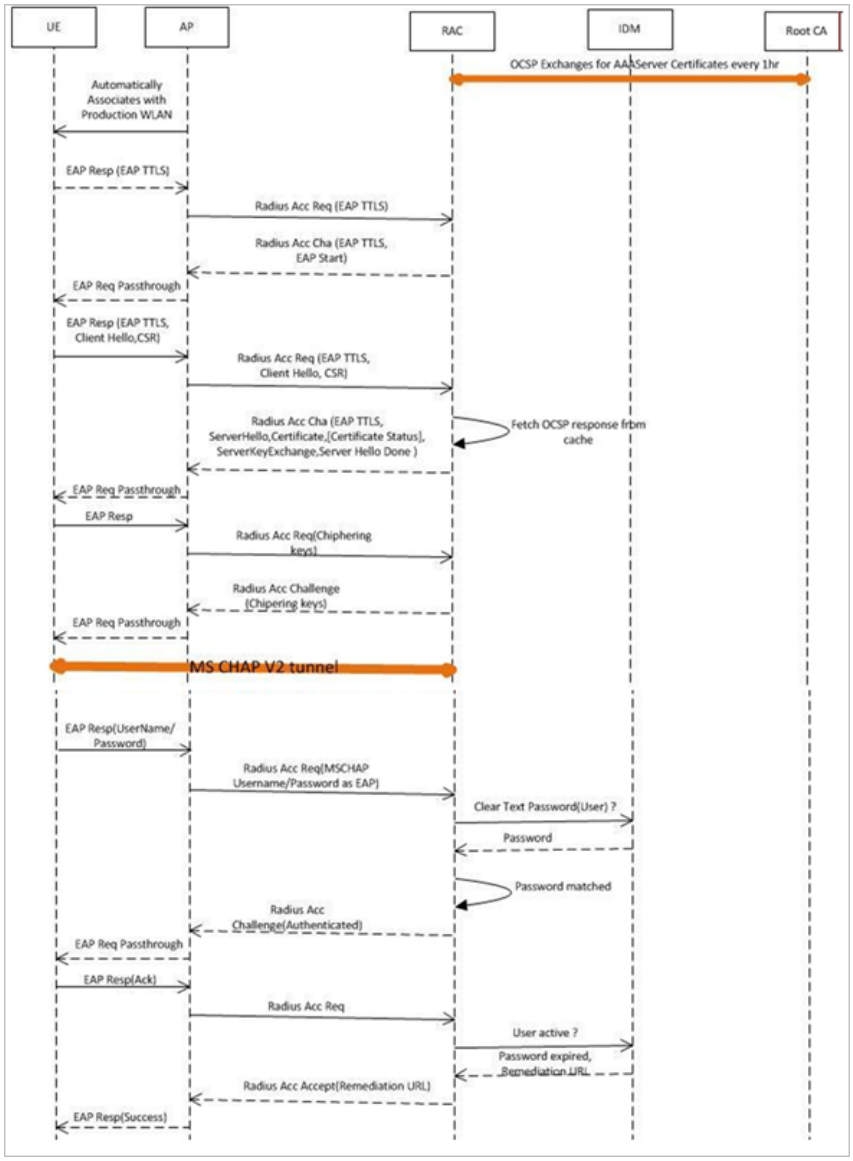


Figure 25: Interaction with OCSP server during EAP-TLS



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 26: Important OCSP Message

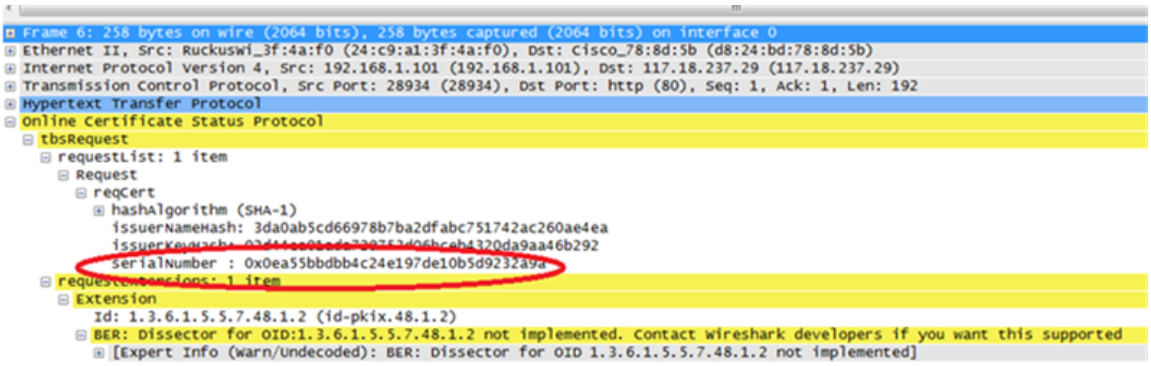
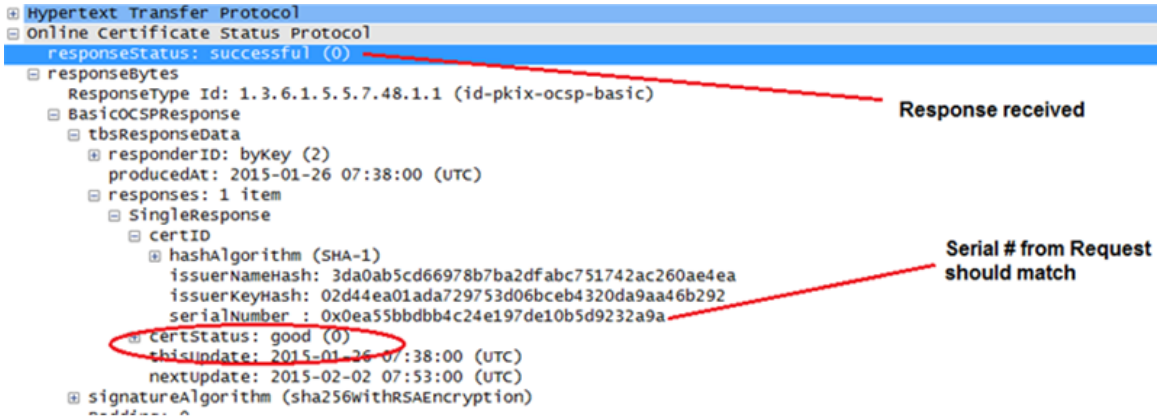


Figure 27: OCSP Response Message



Appendix

C

Apple and Samsung Hotspot 2.0 Release 1 (Passpoint) Devices

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 Wireless 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`