Simply Better Wireless.

Ruckus Wireless™ SmartCell Gateway™ 200 and Virtual SmartZone High-Scale Hotspot 2.0

Reference Guide for SmartZone 3.5

Part Number: 800-71301-001 Rev A
Published: 20 February 2017

www.ruckuswireless.com

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

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 v and Table 2: Notice conventions on page v 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	Network Access Identifier
NBI	Northbound Interface
OCSP	Online Certificate Status Protocol
OI	Organization Identifier
OMA-DM	Open Mobile Alliance’s Device Management

Terminology	Description
OSEN	OSU Server-only authenticated layer 2 Encryption Network
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

Terminology	Description
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
  - Part number: 800-70917-001
  - Page 88

Hotspot 2.0 Brief Overview 1

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 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.

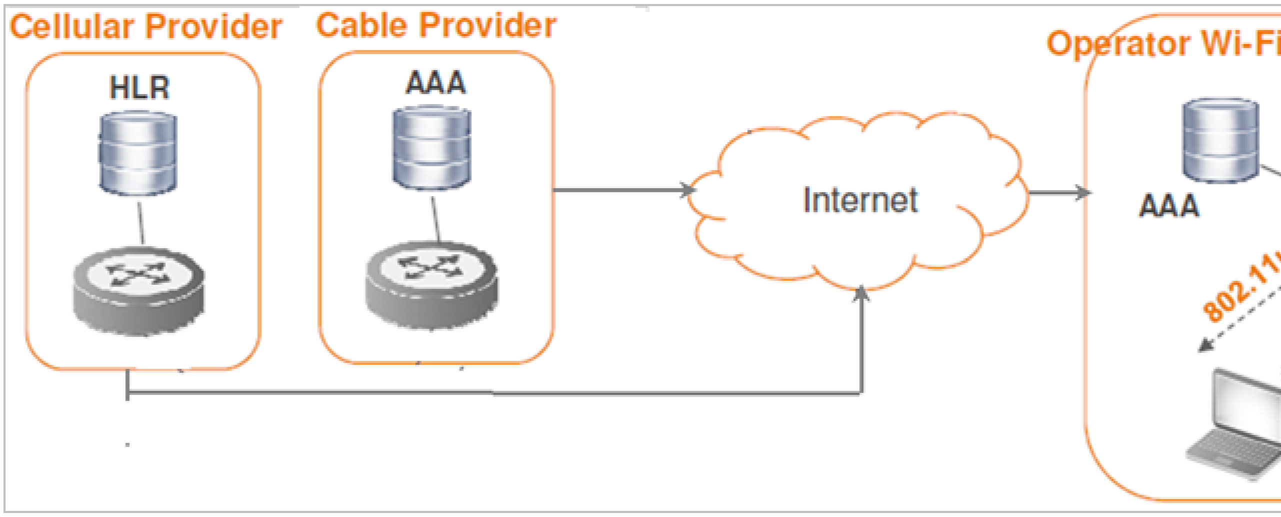


Figure 1: Working of Hotspot 2.0

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. Refer to the figure below.

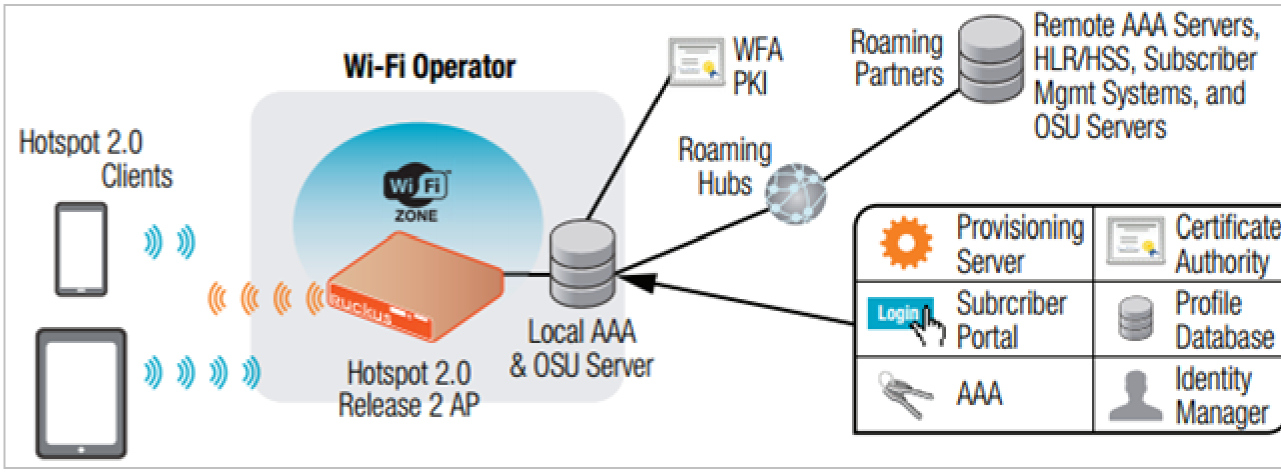


Figure 2: Components of Hotspot 2.0

Operators and Service Providers

Hotspot 2.0 has two entities – operators and service providers.

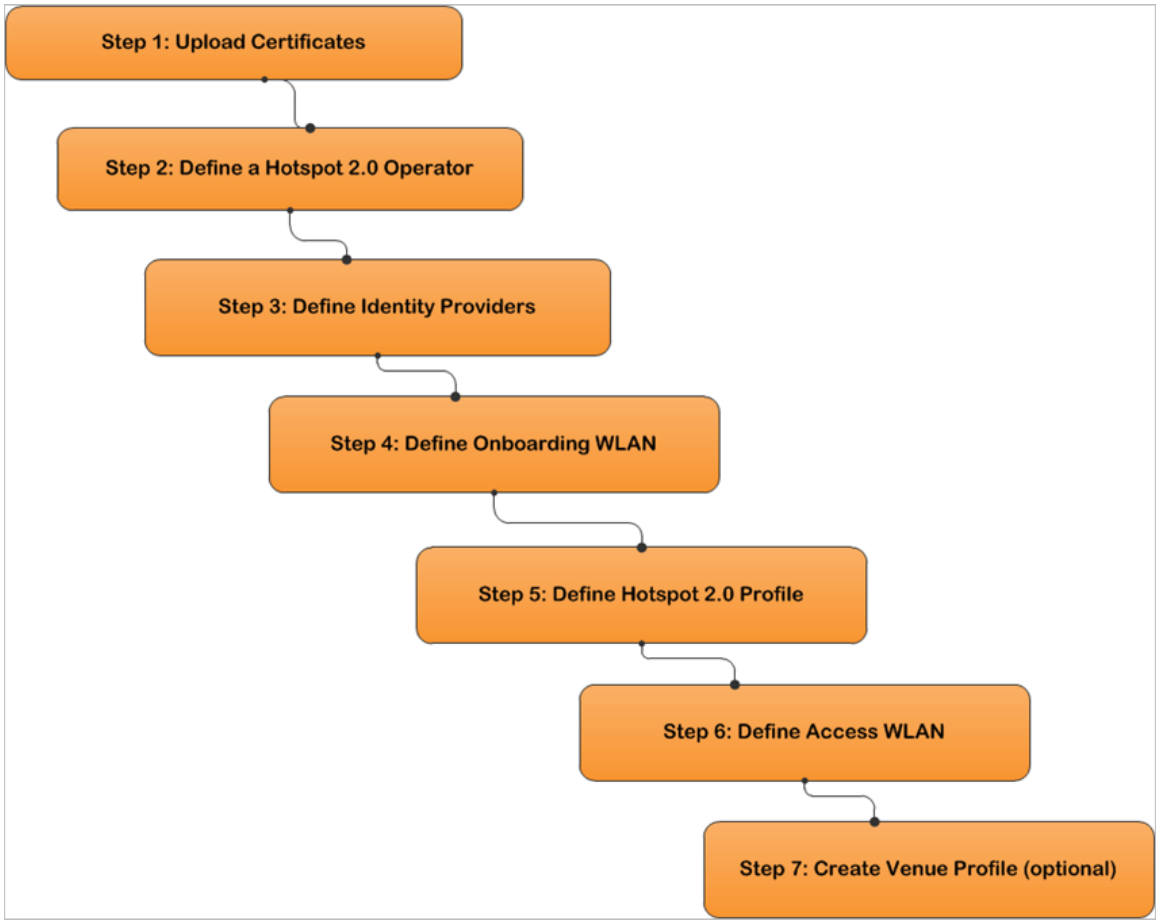
An operator is the owner of a set of Hotspot 2.0 enabled access points. Each operator can resell their Hotspot 2.0 service to a number of service providers. The operators deal mostly with physical network elements while the service providers keep track of user subscriptions and billing. An operator profile 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.

Configuring Hotspot 2.0

2

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


Step 1: Upload Certificates
Step 2: Define a Hotspot 2.0 Operator
Step 3: Define Identity Providers
Step 4: Define Onboarding WLAN
Step 5: Define Hotspot 2.0 Profile
Step 6: Define Access WLAN
Step 7: Create Venue Profile (optional)

NOTE Hotspot 2.0 WLANs do not support IPv6.

Step 1: Uploading Certificates

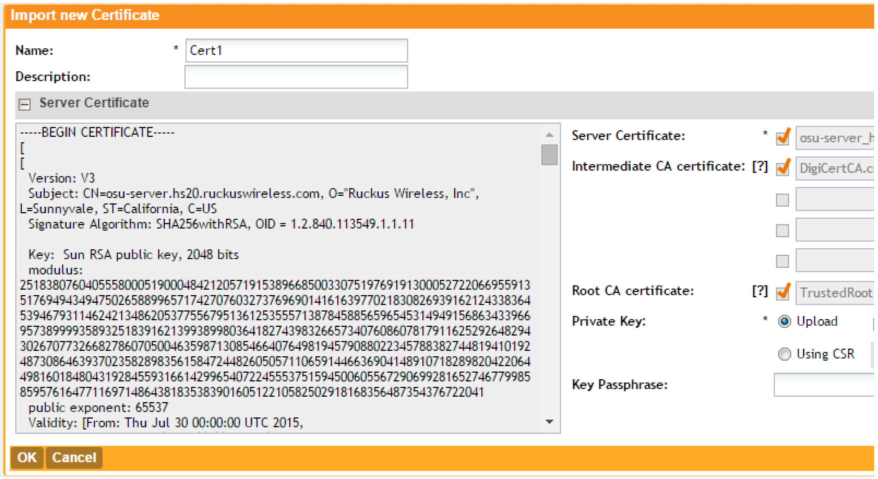
Uploading certificates is the first step in configuring Hotspot 2.0.

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

1. Click **Configuration > SCG Systems > Certificates > Certificate Store**
2. The **Certificate Store** page appears. Click **Import New**.
3. Use the **Browse** option to choose the root certificate file.
4. Click **Upload** to upload the root certificate.
5. Click **Apply** and review the certificate in the left pane text area.
6. Click **OK** to complete uploading the root certificate.
7. Use the **Browse** option to choose the server certificate file. Use the **Browse** and **More Upload** option to upload intermediate certificates.
8. Click **Upload** to upload the server certificate.
9. Click **Apply** and review the certificate in the left pane text area.
10. Click **OK** to complete uploading the server certificate.
11. Use the **Browse** option to select the private key file.
12. Click **Upload** to upload the private key file.
13. Click **Apply** and review the certificate in the left pane text area.
14. Click **OK** to completing uploading the private key file. You have completed adding a root and server certificates. You also have completed adding the private key file. To view the certificate click on the certificate name listed on the landing page.
15. 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



Name: * Cert1

Description:

```
-----BEGIN CERTIFICATE-----
[
[
  Version: V3
  Subject: CN=osu-server.hs20.ruckuswireless.com, O="Ruckus Wireless, Inc",
L=Sunnyvale, ST=California, C=US
  Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

  Key:  Sun RSA public key, 2048 bits
  modulus:
251838076040555800051900048421205719153896685003307519769191300052722066955913
517694943494750265889965717427076032737696901416163977021830826939162124338364
539467931146242134862053775567951361253555713878458856596545314949156863433966
957389999358932518391621399389980364182743983266573407608607817911625292648294
302670773266827860705004635987130854664076498194579088022345788382744819410192
487308646393702358289835615847244826050571106591446636904148910718289820422064
498160184804319284559316614299654072245553751594500605567290699281652746779985
859576164771169714864381835383901605122105825029181683564873543767722041
  public exponent: 65537
  Validity: [From: Thu Jul 30 00:00:00 UTC 2015,
```

Server Certificate: * ☑ osu-server_h

Intermediate CA certificate: [?] ☑ DigiCertCA.c

☐

☐

☐

Root CA certificate: [?] ☑ TrustedRoot

Private Key: * ● Upload ○ Using CSR

Key Passphrase:

Step 2: Define Wi-Fi Operator Profile

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

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

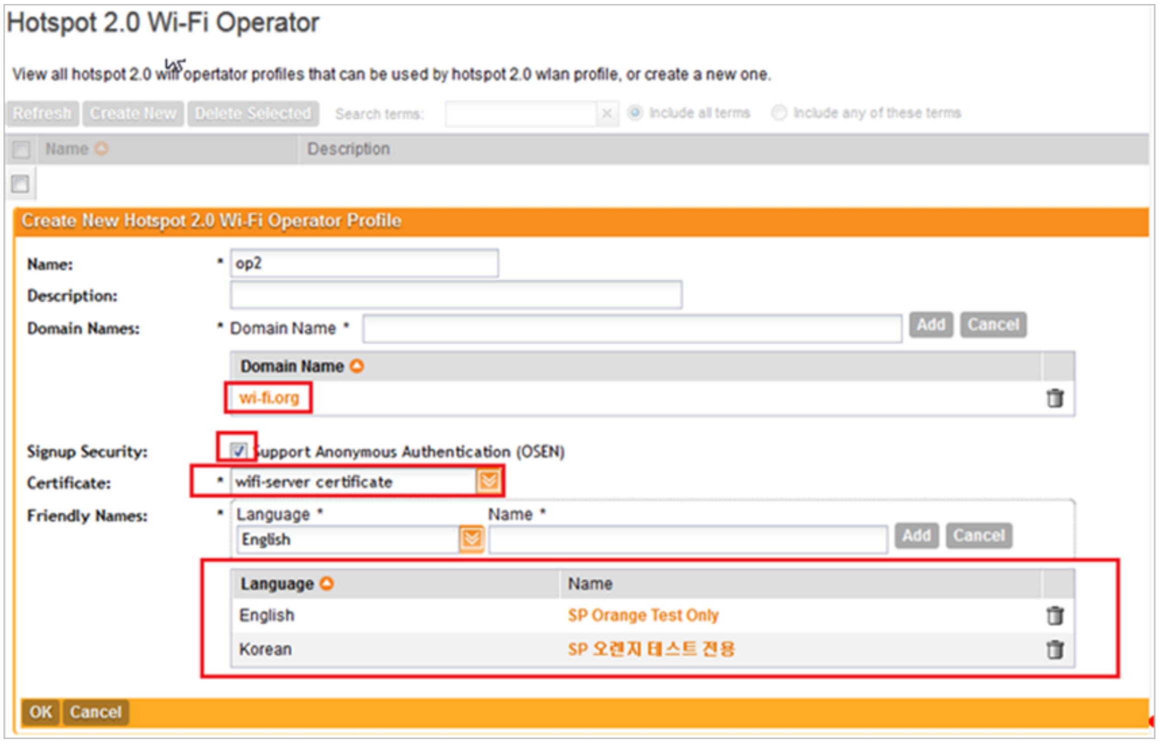
Option	Description
Name	Enter a name for this Wi-Fi operator profile.
Description (Optional)	Enter a description for the venue profile.
Domain Names	HS2.0 operator's domain name is a mandatory field, which specifies the operator’s domain name. Hotspot 2.0 AP broadcasts the domain name to indicate the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

Option	Description
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 (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



Hotspot 2.0 Wi-Fi Operator

View all hotspot 2.0 wifi opertator profiles that can be used by hotspot 2.0 wlan profile, or create a new one.

□	Name	Description
□		

Create New Hotspot 2.0 Wi-Fi Operator Profile

Name: * op2

Description:

Domain Names: * Domain Name *

Domain Name
wi-fi.org

Signup Security: ☑ Support Anonymous Authentication (OSEN)

Certificate: * wifi-server certificate

Friendly Names: * Language * English Name *

Language	Name
English	SP Orange Test Only
Korean	SP 오렌지 테스트 전용

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
- Online SignUp and Provisioning
- Online Signup Portal Profile
- Authentication
- Accounting
- Review

Network Identifier

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

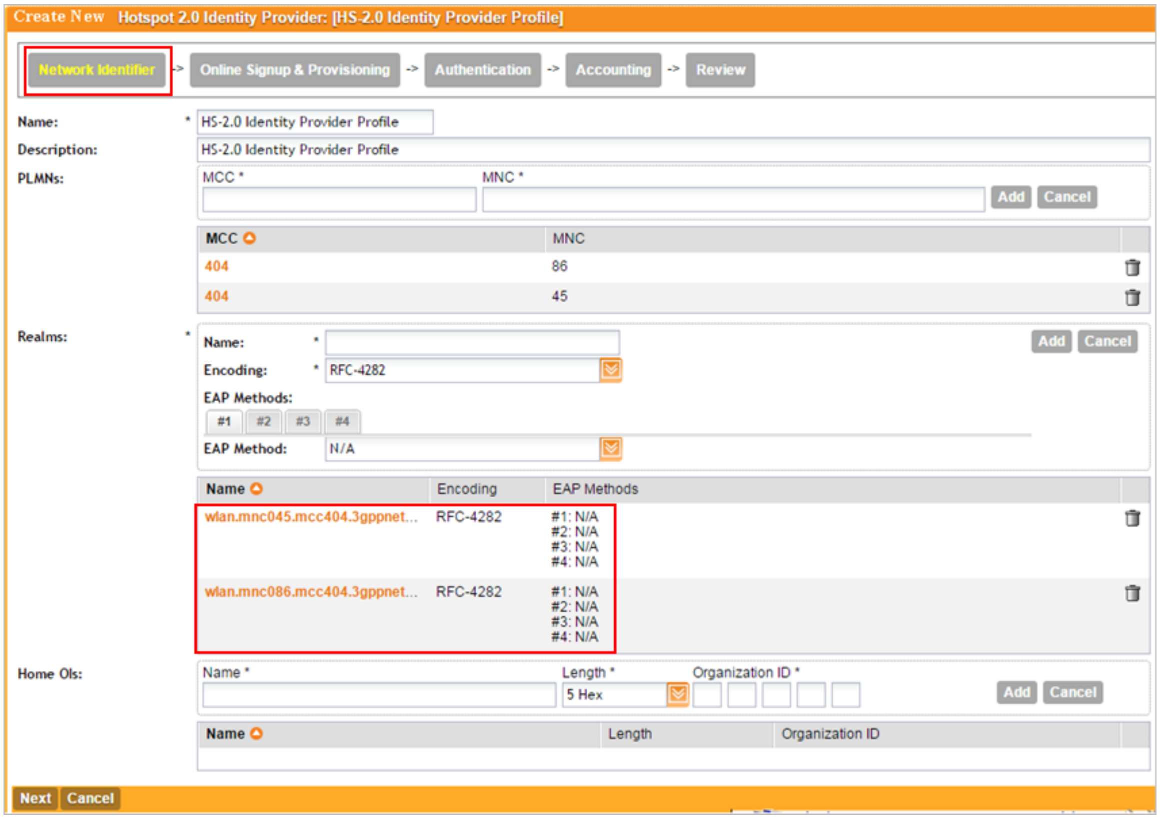
1. Click **Configuration > Services&Profiles > Hotspot 2.0 Identity**. The `Hotspot 2.0 Identity` page appears.
2. Click **Create New**
3. Configure the settings in the table to create a Hotspot 2.0 Network Identifier. Alternatively, the network identifier can be imported from an existing Hotspot 2.0 Wi-Fi operator.

Option	Description
Name	Enter a name or this network identifier profile.
Description (Optional)	Enter a description for the network identifier profile.

Option	Description
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.

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

Figure 6: Hotspot Identity Provider - Network Identifier



Hotspot 2.0 Identity Provider: [HS-2.0 Identity Provider Profile]

Name: * HS-2.0 Identity Provider Profile

Description: HS-2.0 Identity Provider Profile

PLMNs: MCC * MNC *

MCC	MNC
404	86
404	45

Realms: *

Name: *

Encoding: * RFC-4282

EAP Methods:

EAP Method: N/A

Name	Encoding	EAP Methods
wlan.mnc045.mcc404.3gppnet...	RFC-4282	#1: N/A #2: N/A #3: N/A #4: N/A
wlan.mnc086.mcc404.3gppnet...	RFC-4282	#1: N/A #2: N/A #3: N/A #4: N/A

Home OIs: Name * Length * 5 Hex Organization ID *

Name	Length	Organization ID

Online SignUp and Provisioning

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

1. Click to enable **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: 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.

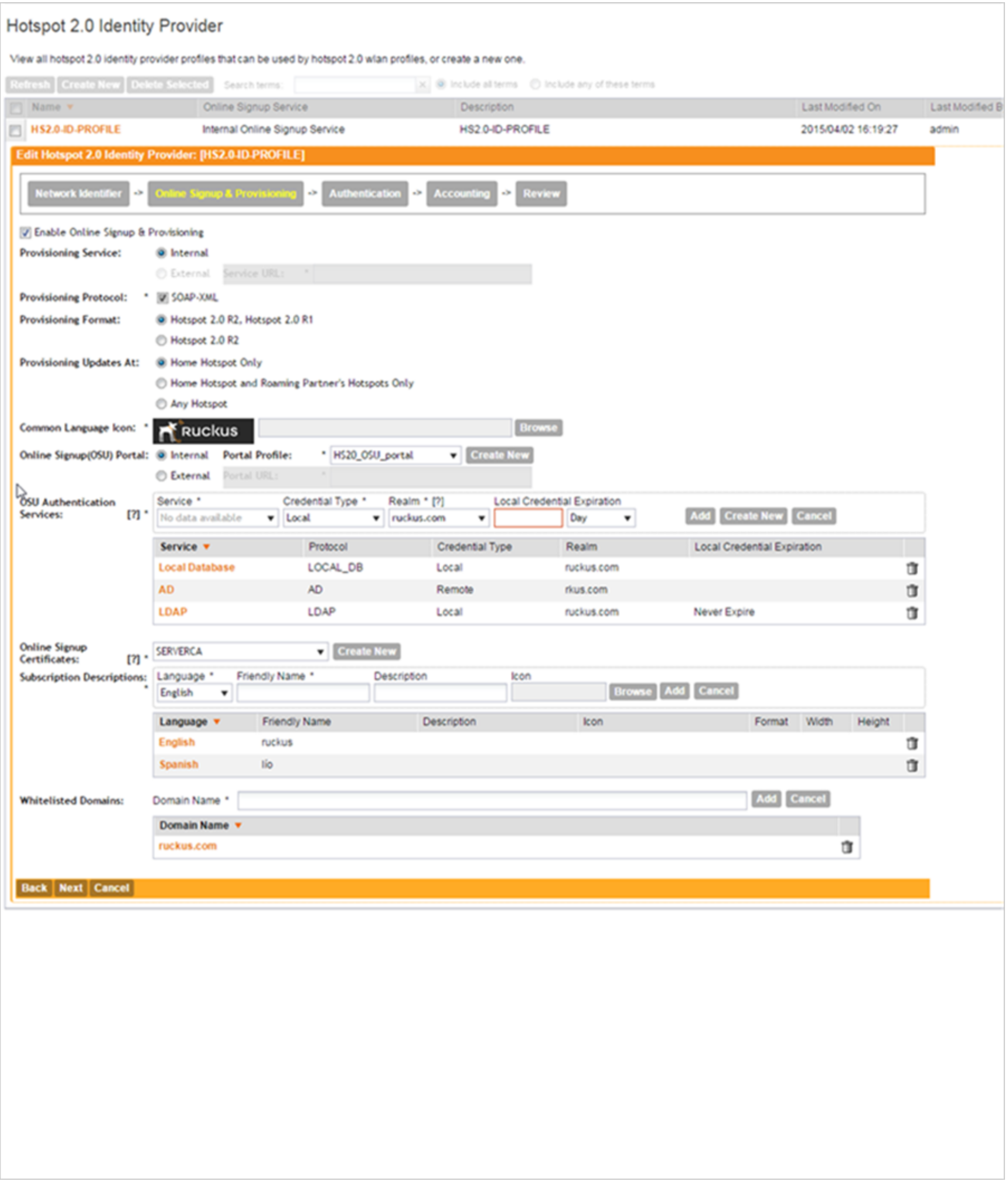
Option	Description
Provisioning Format	This options allows the administrator to choose: • Hotspot 2.0 R2, Hotspot 2.0 R1 - in case the Release 1 device is doing the onboarding the configuration file downloaded should be Release 1configuration file. • Hotspot 2.0 Release2. Note: This option is available when the provisioning service is internal.
Provisioning Updates At	This option is available when the provisioning service is internal. Select the provisioning updates to be sent to the user: If the value is set to: • Home hotspot - the mobile device updates its policy only when it is connected to a hotspot operated by its Home SP. • Home hotspot and roaming partner's hotspot - the mobile device may update its PPS - MO when it is associated to a roaming partner's HS2.0 compliant hotspot or its home SP's HS2.0 compliant hotspot. • Any hotspot - the mobile device may update its PPS -MO when connected to any WLAN, which is connected to the public Internet.
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 Portal	OSU portal is the portal configuration for onboarding. In case it is set to external, the administrator needs to configure the URL. If it is set to Internal, the administrator needs to choose the OSU portal profile from the list.

Option	Description
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
OSU Authentication Services	The administrator can select the authentication services the user is able to choose for onboarding. Local means that the controller's identity management generates local random credentials and the OSU provisions it to the device. Remote means that same credentials used for onboarding with external RADIUS is provisioned to the device. Realm is another attribute required per authentication service and defines what will be the value in the realm leaf node in the PPS-MO. The available realm list is retrieved from the realms configured in the Network Identifier tab. Additional attribute per selected authentication service is *Local Credential Expiration* available (only if the *Local Credential* is selected) and impacts the expiration of the credentials in the PPS-MO. This realm is used when the device tries finding the realm match based on ANQP response from AP. This configuration is available in **Configuration>Services&Profiles>Services>Authentication.** **NOTE** For further details see: OSU Authentication Services
Online SignUp Certificates	This option should be selected based on the certificate uploaded in the Certificate Store.

Option	Description
Subscription 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



Hotspot 2.0 Identity Provider

View all hotspot 2.0 identity provider profiles that can be used by hotspot 2.0 wlan profiles, or create a new one.

Refresh
Create New
Delete Selected
Search terms:
● Include all terms
○ Include any of these terms

□	Name	Online Signup Service	Description	Last Modified On	Last Modified B
□	HS2.0-ID-PROFILE	Internal Online Signup Service	HS2.0-ID-PROFILE	2015/04/02 16:19:27	admin

Edit Hotspot 2.0 Identity Provider: [HS2.0-ID-PROFILE]

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

☑ Enable Online Signup & Provisioning

Provisioning Service: ● Internal ○ External Service URL: *

Provisioning Protocol: * ☑ SOAP-XML

Provisioning Format: ● Hotspot 2.0 R2, Hotspot 2.0 R1 ○ Hotspot 2.0 R2

Provisioning Updates At: ● Home Hotspot Only ○ Home Hotspot and Roaming Partner's Hotspots Only ○ Any Hotspot

Common Language Icon: * RUCKUS

Online Signup(OSU) Portal: ● Internal Portal Profile: * HS20_OSU_portal ○ External Portal URL: *

OSU Authentication Services: [?] *

Service * No data available; Credential Type * Local; Realm * [?] ruckus.com; Local Credential Expiration Day

Service	Protocol	Credential Type	Realm	Local Credential Expiration
Local Database	LOCAL_DB	Local	ruckus.com	
AD	AD	Remote	rkus.com	
LDAP	LDAP	Local	ruckus.com	Never Expire

Online Signup Certificates: [?] * SERVERCA

Subscription Descriptions: *

Language * English; Friendly Name *; Description; Icon

Language	Friendly Name	Description	Icon	Format	Width	Height
English	ruckus					
Spanish	lio					

Whitelisted Domains: Domain Name *

Domain Name
ruckus.com

Authentication

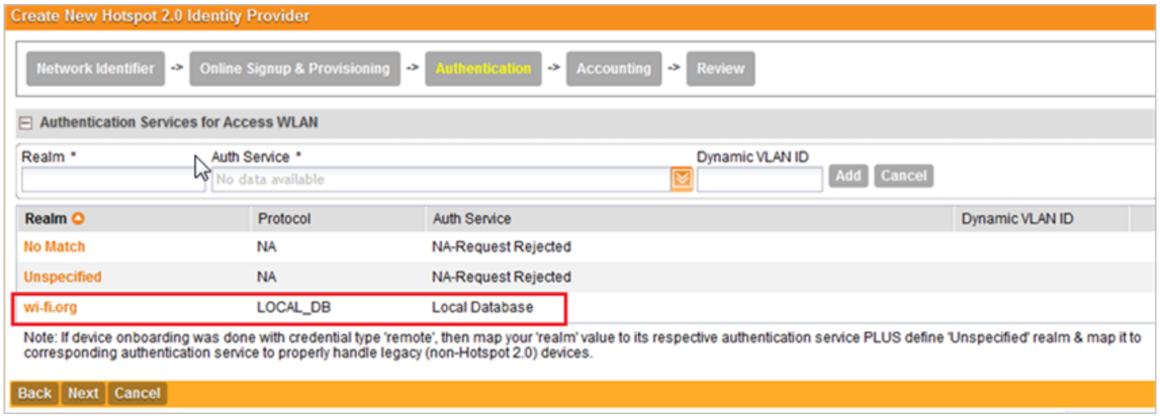
Follow these steps to create a Hotspot 2.0 Identity Provider - Authentication.

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 **Configuration>Services&Profiles>Services>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


Create New Hotspot 2.0 Identity Provider
Network Identifier -> Online Signup & Provisioning -> Authentication -> Accounting -> Review
Add
Cancel
Back
Next
Cancel

Authentication Services for Access WLAN

Realm * | Auth Service * No data available | Dynamic VLAN ID

Realm	Protocol	Auth Service	Dynamic VLAN ID
No Match	NA	NA-Request Rejected	
Unspecified	NA	NA-Request Rejected	
wi-fi.org	LOCAL_DB	Local Database	

Note: If device onboarding was done with credential type 'remote', then map your 'realm' value to its respective authentication service PLUS define 'Unspecified' realm & map it to corresponding authentication service to properly handle legacy (non-Hotspot 2.0) devices.

Accounting

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

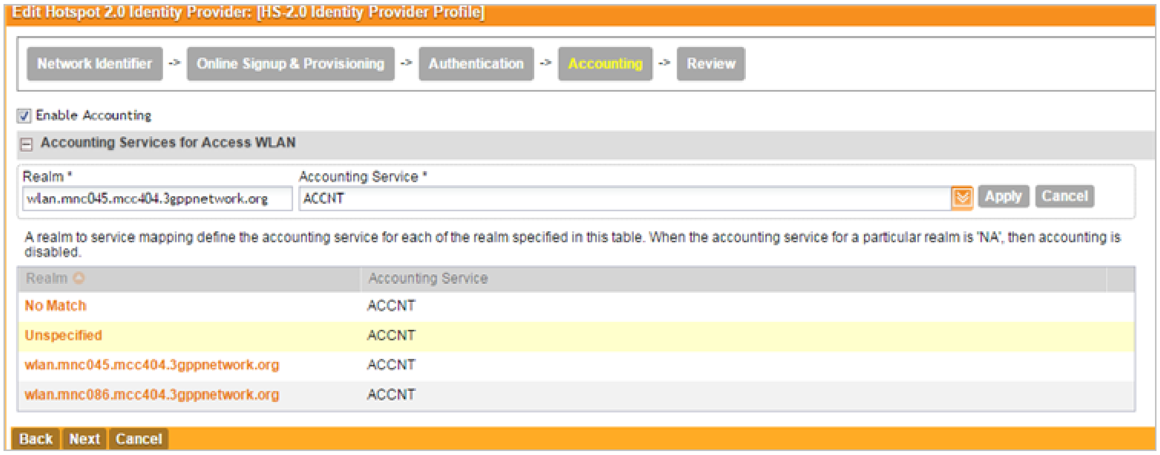
1. Click to enable Accounting for configuring the accounting service.
2. Configure the settings in the table below to create a Hotspot 2.0 Accounting.

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 **Configuration>Services&Profiles>Services>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



Edit Hotspot 2.0 Identity Provider: [HS-2.0 Identity Provider Profile]

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

☑ Enable Accounting

Accounting Services for Access WLAN

Realm * wlan.mnc045.mcc404.3gppnetwork.org

Accounting Service * ACCNT

A realm to service mapping define the accounting service for each of the realm specified in this table. When the accounting service for a particular realm is 'NA', then accounting is disabled.

Realm	Accounting Service
No Match	ACCNT
Unspecified	ACCNT
wlan.mnc045.mcc404.3gppnetwork.org	ACCNT
wlan.mnc086.mcc404.3gppnetwork.org	ACCNT

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

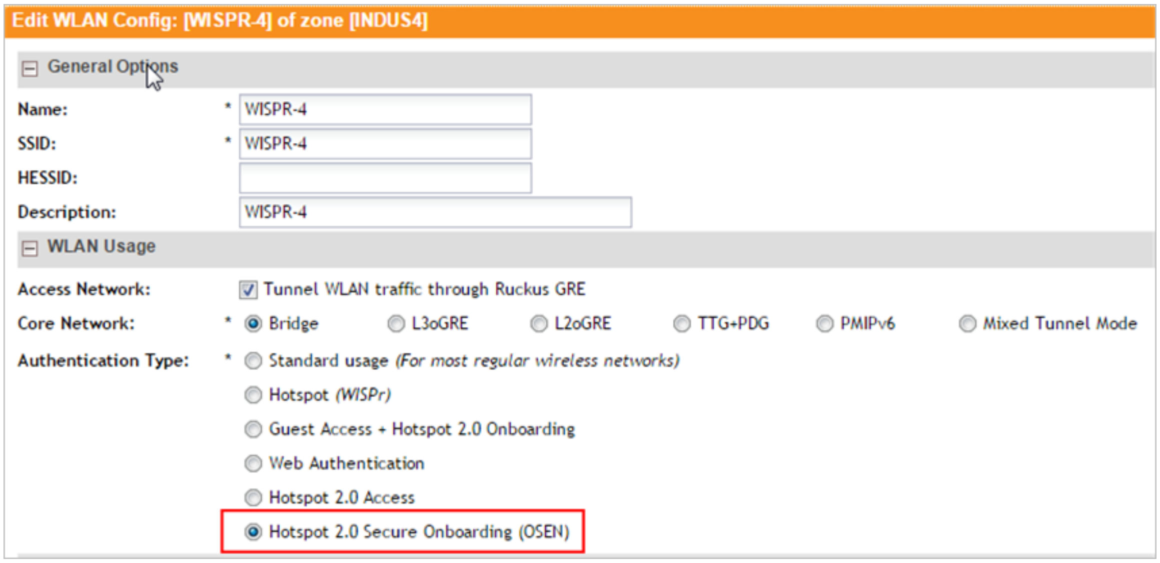
Define Secure Onboarding - Hotspot 2.0 OSEN

Follow these steps to configure Hotspot 2.0 OSEN authentication.

1. Click **Configuration > AP Zones > WLAN**.
2. On the *AP Zone List* page, select the AP zone in the WLAN Services & Group page.

3. Navigate to **WLAN Usage> Authentication Type**
4. Enable Hotspot 2.0 OSEN profile.
5. Click **Apply**. You have completed creating the Hotspot 2.0 OSEN authentication type.

Figure 10: Hotspot 2.0 Authentication Type



Edit WLAN Config: [WISPR-4] of zone [INDUS4]

⊟ General Options

Name: * WISPR-4
SSID: * WISPR-4
HESSID:
Description: WISPR-4

⊟ WLAN Usage

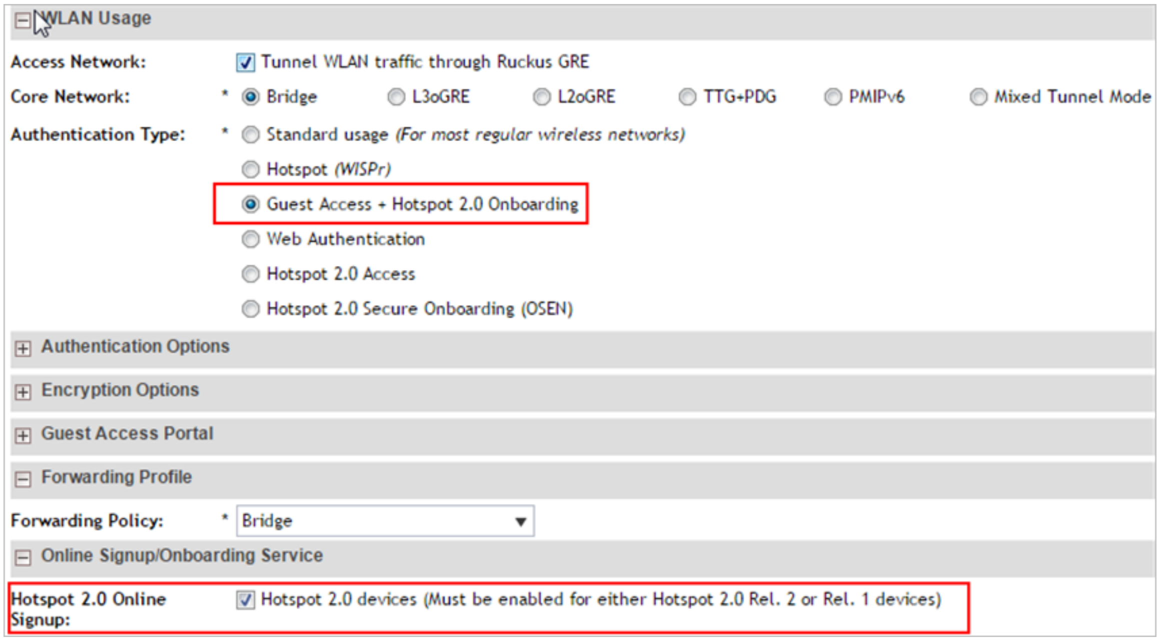
Access Network: ☑ Tunnel WLAN traffic through Ruckus GRE
Core Network: * ● Bridge ○ L3oGRE ○ L2oGRE ○ TTG+PDG ○ PMIPv6 ○ Mixed Tunnel Mode
Authentication Type: * ○ Standard usage *(For most regular wireless networks)*
○ Hotspot *(WISPr)*
○ Guest Access + Hotspot 2.0 Onboarding
○ Web Authentication
○ Hotspot 2.0 Access
● Hotspot 2.0 Secure Onboarding (OSEN)

Define Open Onboarding - Guest Access

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

1. Click **Configuration** > **AP Zones** > **WLAN**.
2. On the AP Zone List page, select the AP zone in the WLAN Services & Group page in **WLAN Usage> Authentication Type** to enable Guest Access + Hotspot 2.0 Online Signup.
3. In Online SignUp / Onboarding Service enable the option of Hotspot 2.0 onboarding.
4. Click **Apply**. You have completed enabling guest access for Hotspot 2.0 OSU.
5. Refer to Step 6: Define Access WLAN for defining Hotspot 2.0 WLAN.

Figure 11: Guest Access for Hotspot 2.0 OSU



⊟ WLAN Usage

Access Network: ☑ Tunnel WLAN traffic through Ruckus GRE

Core Network: * ● Bridge ○ L3oGRE ○ L2oGRE ○ TTG+PDG ○ PMIPv6 ○ Mixed Tunnel Mode

Authentication Type: * ○ Standard usage *(For most regular wireless networks)*
○ Hotspot *(WISPr)*
● Guest Access + Hotspot 2.0 Onboarding
○ Web Authentication
○ Hotspot 2.0 Access
○ Hotspot 2.0 Secure Onboarding (OSEN)

⊞ Authentication Options

⊞ Encryption Options

⊞ Guest Access Portal

⊟ Forwarding Profile

Forwarding Policy: * Bridge ▼

⊟ Online Signup/Onboarding Service

Hotspot 2.0 Online Signup: ☑ Hotspot 2.0 devices (Must be enabled for either Hotspot 2.0 Rel. 2 or Rel. 1 devices)

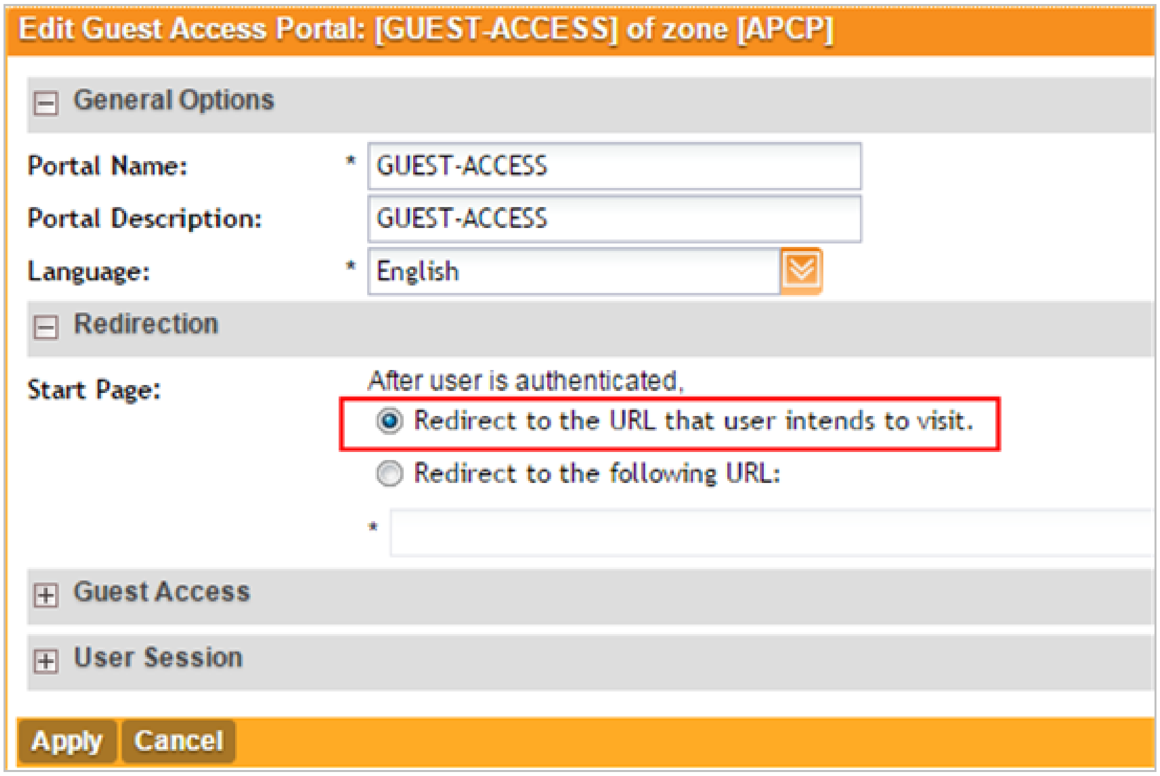
AP Zone - Guest Access

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 **Configuration** > **AP Zones** > **Guest Access**.
2. On the *Guest Access Portal* page, select the guest access.
3. In **Redirection > Start Page** enable *Redirect to the URL that the user intends to visit*.
4. Click **Apply**. You have completed enabling Hotspot 2.0 device registration.

Figure 12: Guest Access



Edit Guest Access Portal: [GUEST-ACCESS] of zone [APCP]

⊟ General Options

Portal Name:	*	GUEST-ACCESS
Portal Description:		GUEST-ACCESS
Language:	*	English

⊟ Redirection

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

Step 5: Define Hotspot 2.0 Profile

Follow these steps to create a Hotspot 2.0 services profile.

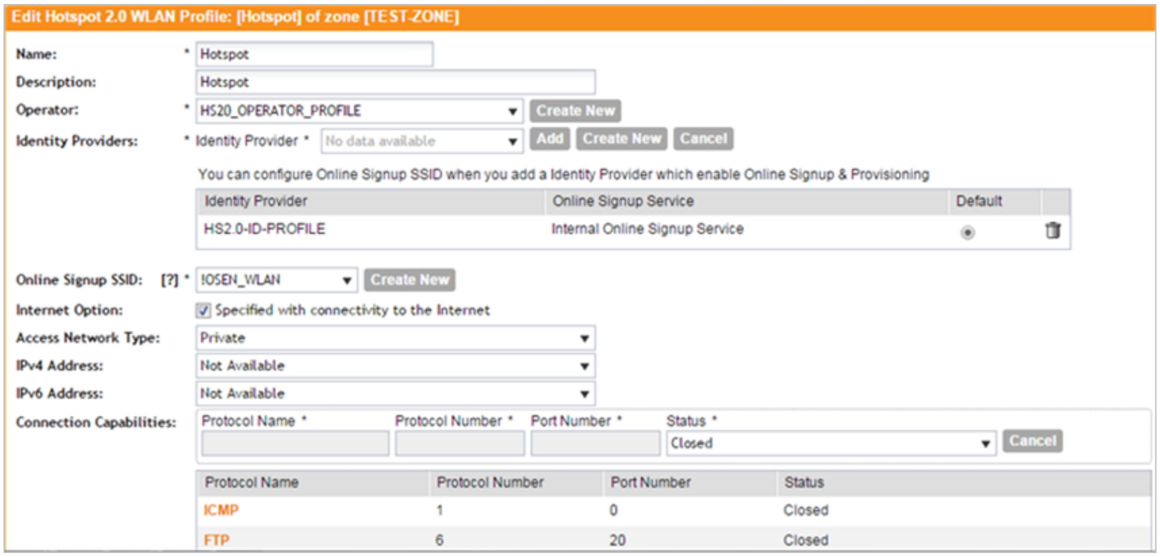
1. Click **Configuration** > **AP Zones**.
2. On the *AP Zone List* page, click the AP zone for which you want to create a Hotspot 2.0 service.
3. On the sidebar, click **Hotspot 2.0**. The *Hotspot 2.0 Services* page appears.
4. In the *Hotspot 2.0 WLAN Profiles* section, click **Create New**.
5. Configure 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.

Option	Description
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 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.
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 13: Hotspot 2.0 Services Profile



Edit Hotspot 2.0 WLAN Profile: [Hotspot] of zone [TEST-ZONE]

Name:	* Hotspot
Description:	Hotspot
Operator:	* HS20_OPERATOR_PROFILE ▾ Create New
Identity Providers:	* Identity Provider * No data available ▾ Add Create New Cancel

You can configure Online Signup SSID when you add a Identity Provider which enable Online Signup & Provisioning

Identity Provider	Online Signup Service	Default	
HS2.0-ID-PROFILE	Internal Online Signup Service	●	🗑

Online Signup SSID: [?]	* !OSEN_WLAN ▾ Create New
Internet Option:	☑ Specified with connectivity to the Internet
Access Network Type:	Private ▾
IPv4 Address:	Not Available ▾
IPv6 Address:	Not Available ▾
Connection Capabilities:	Protocol Name * Protocol Number * Port Number * Status * Closed ▾ Cancel

Protocol Name	Protocol Number	Port Number	Status
ICMP	1	0	Closed
FTP	6	20	Closed

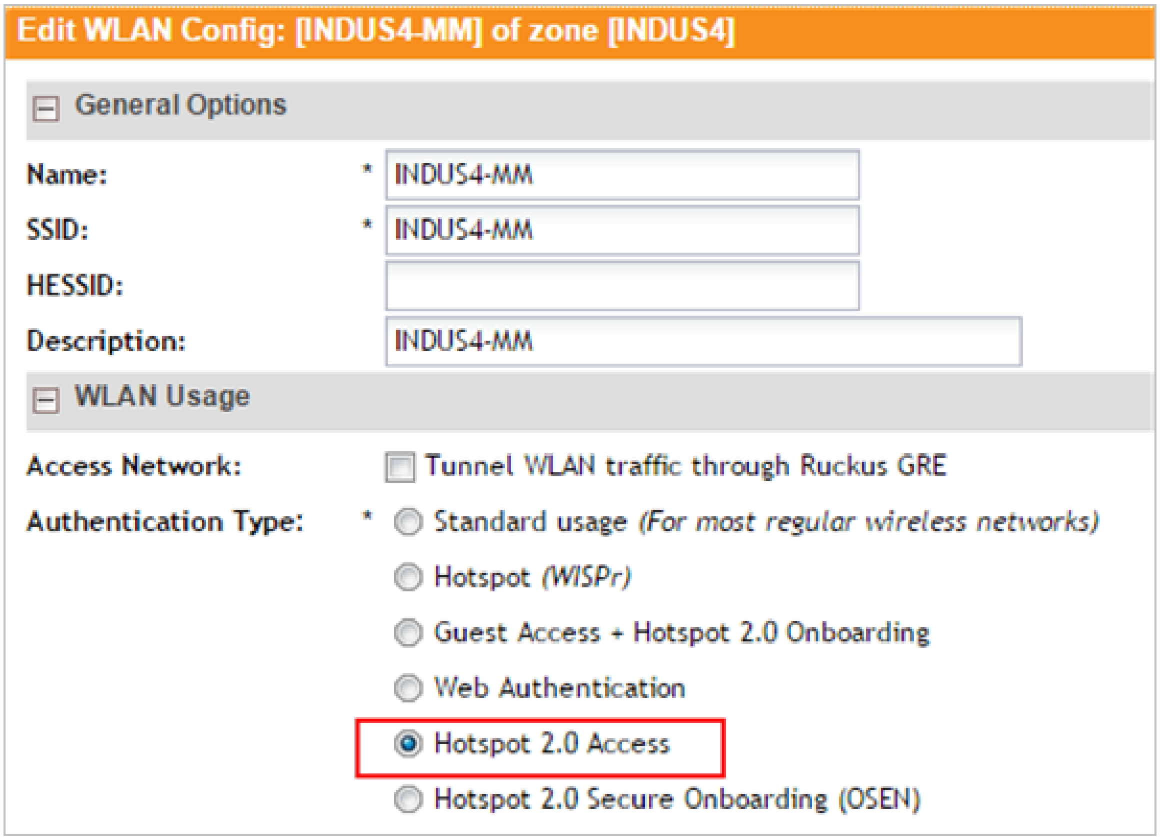
NOTE Only provisioned devices with local database credentials can pass 802.1x Proxy and Hotspot 2.0 authentication.

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 **Configuration** > **AP Zones** > **WLAN**.
2. On the *AP Zone List* page, select the AP zone in the WLAN Services & Group page.
3. Navigate to **WLAN Usage> Authentication Type**.
4. Enable Hotspot 2.0.
5. Click **Apply**. You have completed creating the Hotspot 2.0 authentication type.

Figure 14: Hotspot 2.0 Authentication Type



Edit WLAN Config: [INDUS4-MM] of zone [INDUS4]

General Options

Name:	*	INDUS4-MM
SSID:	*	INDUS4-MM
HESSID:		
Description:		INDUS4-MM

WLAN Usage

Access Network: □ Tunnel WLAN traffic through Ruckus GRE

Authentication Type: *
○ Standard usage *(For most regular wireless networks)*
○ Hotspot *(WISPr)*
○ Guest Access + Hotspot 2.0 Onboarding
○ Web Authentication
● Hotspot 2.0 Access
○ Hotspot 2.0 Secure Onboarding (OSEN)

Step 7: Create Venue Profile

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

1. Click **Configuration > AP Zones**.
2. On the *AP Zone List* page, click the AP zone for which you want to create a Hotspot 2.0 venue profile.
3. On the sidebar, click **Hotspot 2.0**. The *Hotspot 2.0 Services* page appears.
4. In the *Hotspot 2.0 Venue Profiles* section, click **Create New**.
5. Configure the Venue profile configuration options in the table below to create a Hotspot 2.0 WLAN profile.

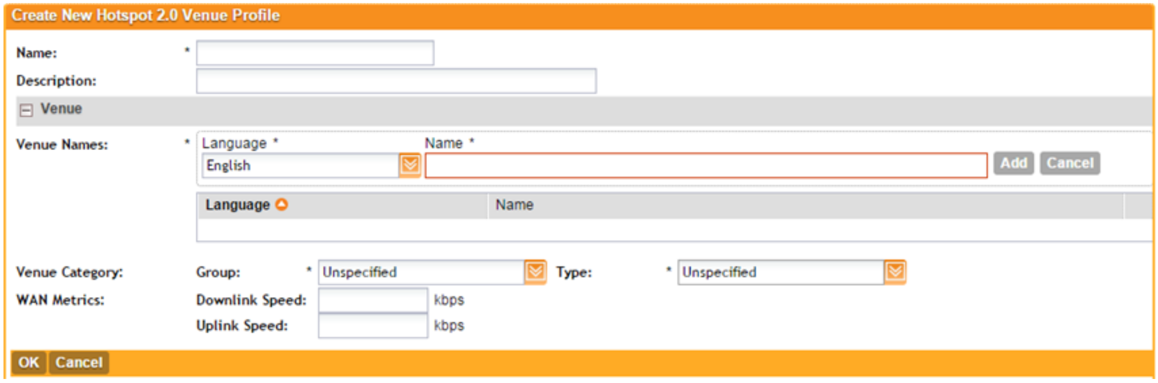
Option	Description
Option	**Description**

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

6. 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



Create New Hotspot 2.0 Venue Profile

Name: *

Description:

⊟ Venue

Venue Names: * Language * English Name * Add Cancel

Language	Name

Venue Category: Group: * Unspecified Type: * Unspecified

WAN Metrics: Downlink Speed: kbps

Uplink Speed: kbps

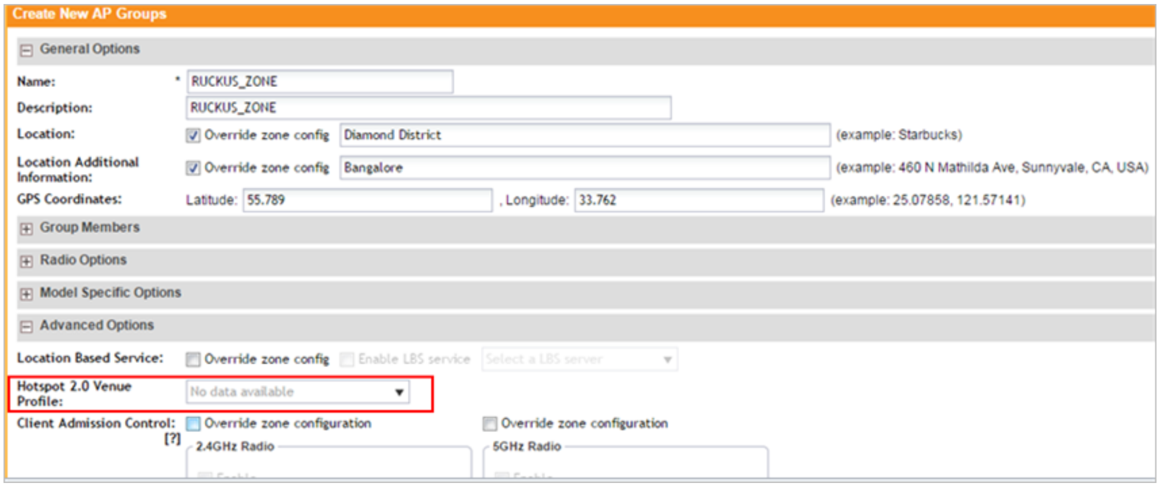
OK Cancel

Adding Venue Profile in AP

1. Click **Configuration > Access Points**.
2. Click **Create New** to create a new AP. Refer to the Administration Guide for details.

3. Click **Advanced Options** to set the Hotspot 2.0 Venue profile from the drop down list as seen in the figure.
4. Click OK.

Figure 16: Hotspot 2.0 Venue Profile in AP



Create New AP Groups

⊟ General Options

Name: * RUCKUS_ZONE
Description: RUCKUS_ZONE
Location: ☑ Override zone config Diamond District (example: Starbucks)
Location Additional Information: ☑ Override zone config Bangalore (example: 460 N Mathilda Ave, Sunnyvale, CA, USA)
GPS Coordinates: Latitude: 55.789 , Longitude: 33.762 (example: 25.07858, 121.57141)

⊞ Group Members

⊞ Radio Options

⊞ Model Specific Options

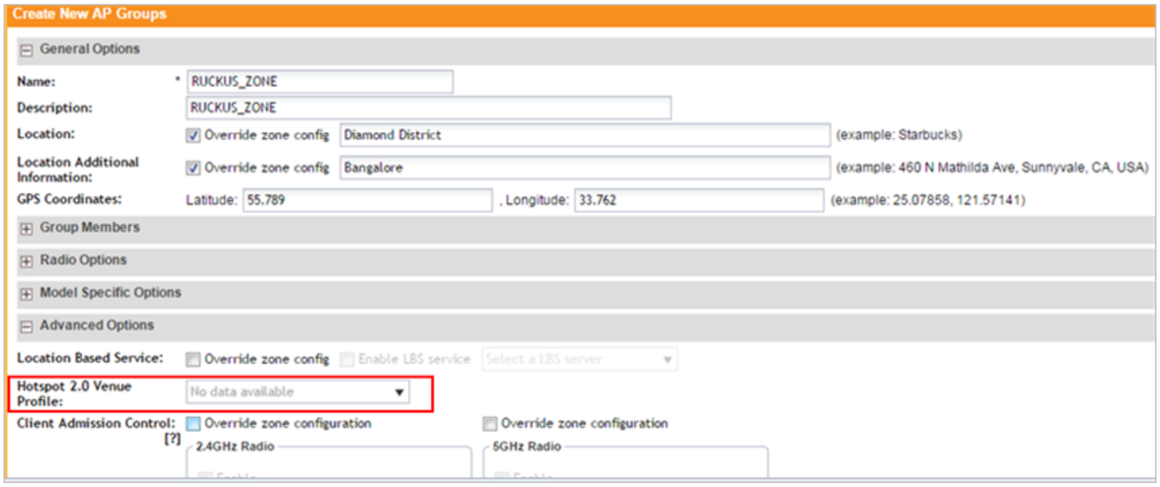
⊟ Advanced Options

Location Based Service: □ Override zone config □ Enable LBS service Select a LBS server ▾
Hotspot 2.0 Venue Profile: No data available ▾
Client Admission Control: [?] □ Override zone configuration □ Override zone configuration

Adding Venue Profile in AP Group

1. Click **Configuration** > **AP Zones** > **AP Group**.
2. Click **Create New** to create a new AP Group. Refer to the Administration Guide for details.
3. Click **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 17: Hotspot 2.0 Venue Profile in AP Group



Create New AP Groups

⊟ General Options

Name: * RUCKUS_ZONE

Description: RUCKUS_ZONE

Location: ☑ Override zone config Diamond District (example: Starbucks)

Location Additional Information: ☑ Override zone config Bangalore (example: 460 N Mathilda Ave, Sunnyvale, CA, USA)

GPS Coordinates: Latitude: 55.789 , Longitude: 33.762 (example: 25.07858, 121.57141)

⊞ Group Members

⊞ Radio Options

⊞ Model Specific Options

⊟ Advanced Options

Location Based Service: □ Override zone config □ Enable LBS service Select a LBS server ▾

Hotspot 2.0 Venue Profile: No data available ▾

Client Admission Control: [?] □ Override zone configuration □ Override zone configuration

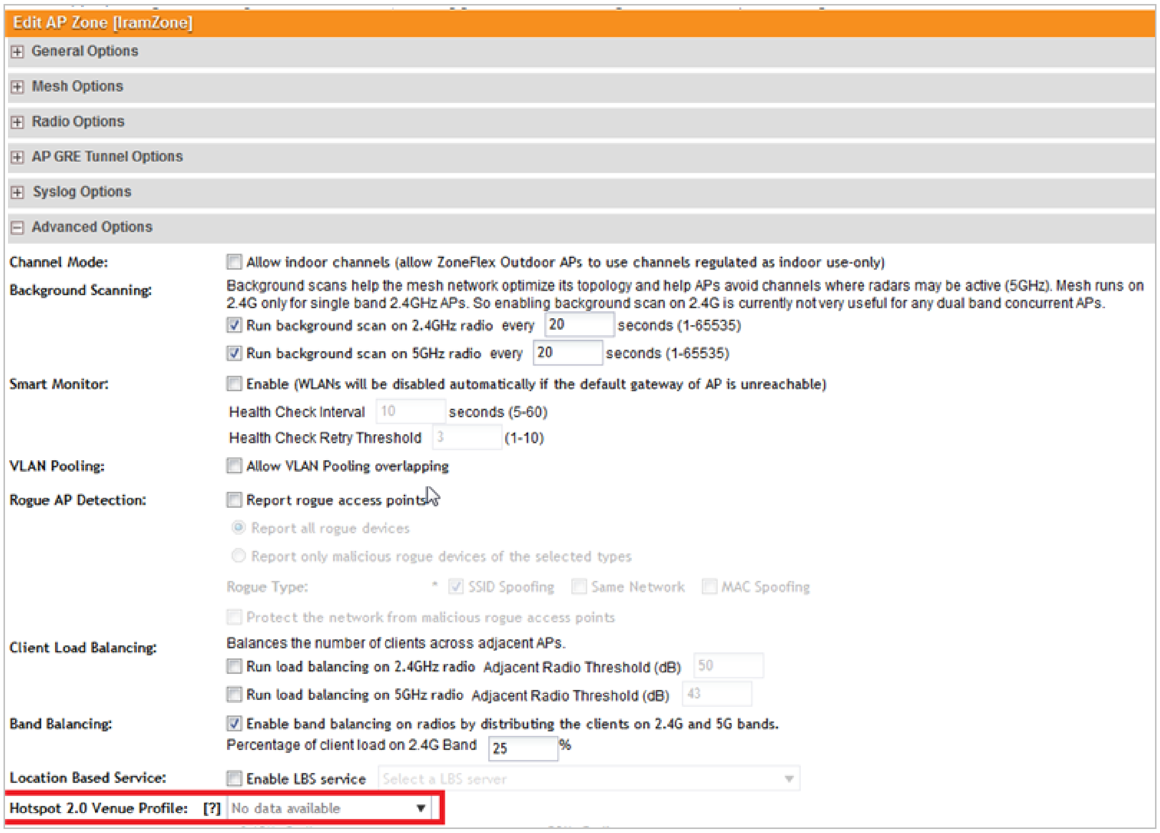
2.4GHz Radio

5GHz Radio

Adding Venue Profile in AP Zone

1. Click **Configuration** > **AP Zones** > **Zone Configuration** > **Edit**.
2. In **Advanced Options** > **Hotspot 2.0 Venue Profile** to set the Hotspot 2.0 venue profile from the drop down list as seen in the figure below.
3. Click **Apply**.

Figure 18: Hotspot 2.0 Venue Profile in AP Zone



Channel Mode: □ Allow indoor channels (allow ZoneFlex Outdoor APs to use channels regulated as indoor use-only)

Background Scanning: Background scans help the mesh network optimize its topology and help APs avoid channels where radars may be active (5GHz). Mesh runs on 2.4G only for single band 2.4GHz APs. So enabling background scan on 2.4G is currently not very useful for any dual band concurrent APs.
☑ Run background scan on 2.4GHz radio every 20 seconds (1-65535)
☑ Run background scan on 5GHz radio every 20 seconds (1-65535)

Smart Monitor: □ Enable (WLANs will be disabled automatically if the default gateway of AP is unreachable)
Health Check Interval 10 seconds (5-60)
Health Check Retry Threshold 3 (1-10)

VLAN Pooling: □ Allow VLAN Pooling overlapping

Rogue AP Detection: □ Report rogue access points
● Report all rogue devices
○ Report only malicious rogue devices of the selected types
Rogue Type: * ☑ SSID Spoofing □ Same Network □ MAC Spoofing
□ Protect the network from malicious rogue access points

Client Load Balancing: Balances the number of clients across adjacent APs.
□ Run load balancing on 2.4GHz radio Adjacent Radio Threshold (dB) 50
□ Run load balancing on 5GHz radio Adjacent Radio Threshold (dB) 43

Band Balancing: ☑ Enable band balancing on radios by distributing the clients on 2.4G and 5G bands.
Percentage of client load on 2.4G Band 25 %

Location Based Service: □ Enable LBS service Select a LBS server

Hotspot 2.0 Venue Profile: [?] No data available

Hotspot 2.0 R2 Device Workflow

3

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.

The UE initiates request to the portal URL (which also includes request for OCSP Stapling). In case of the controller's internal OSU portal, the identity provider's information is retrieved (as per the internal provisioning service). As per the configured OSU authentication services the portal presents a list for user selection. If Facebook, Google+ or Linked-In is included the portal will include the corresponding icons.

In case a non OAuth provider is selected the user should provide his username/password at the portal and select the *Sign In* button. If the authentication server is *Local database*, the portal sends a JSON authentication request to the controllers subscriber management (also called IDM) application. IDM independently authenticates the user.

If the authentication server is RADIUS/LDAP/AD, IDM uses the Java library for remote authentication services (RAS). Only for RADIUS authentication RAS uses the controller’s RAC module but for others (LDAP/AD) it uses the direct method of authentication.

In case the OAuth provider icon is selected, the portal executes a command to NBI, which in turn executes the remote CLI command to AP to let the UE browse the OAuth web site for authentication. This is termed as time bound whitelist, which is 5 minutes and it is not configurable. In case the time is exceeded the user is redirected to the onboarding portal again.

The portal redirects the UE to the OAuth provider's specific URL for authentication. The portal also provides a callback URL for the OAuth provider to respond after authentication. The user provides his OAuth credentials and the OAuth provider responds to callback URL. This OAuth response includes some code required by the IDM for sending another request to the OAuth provider for the user's profile.

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.

The default EAP type, which the controller's RAC module responds is EAP-TTLS. For Hotspot 2.0 R2 device it matches but for other legacy or R1 devices configured with Zero-IT file it does not match and the RAC module will fall back to authenticate according to their requested EAP type (EAP-PEAP).

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.

In case the original onboarding authentication server is an OAuth provider, the portal automatically redirects the user to the OAuth provider's authentication page where the user needs to provide his OAuth credential. In case of successful OAuth credential authentication the process flow is the same as onboarding. After successful authentication, IDM generates a new user password and responds back to the portal. The portal sends a response to the UE initiating the final request to the OSU server to fetch the updated PPS-MO. 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

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

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

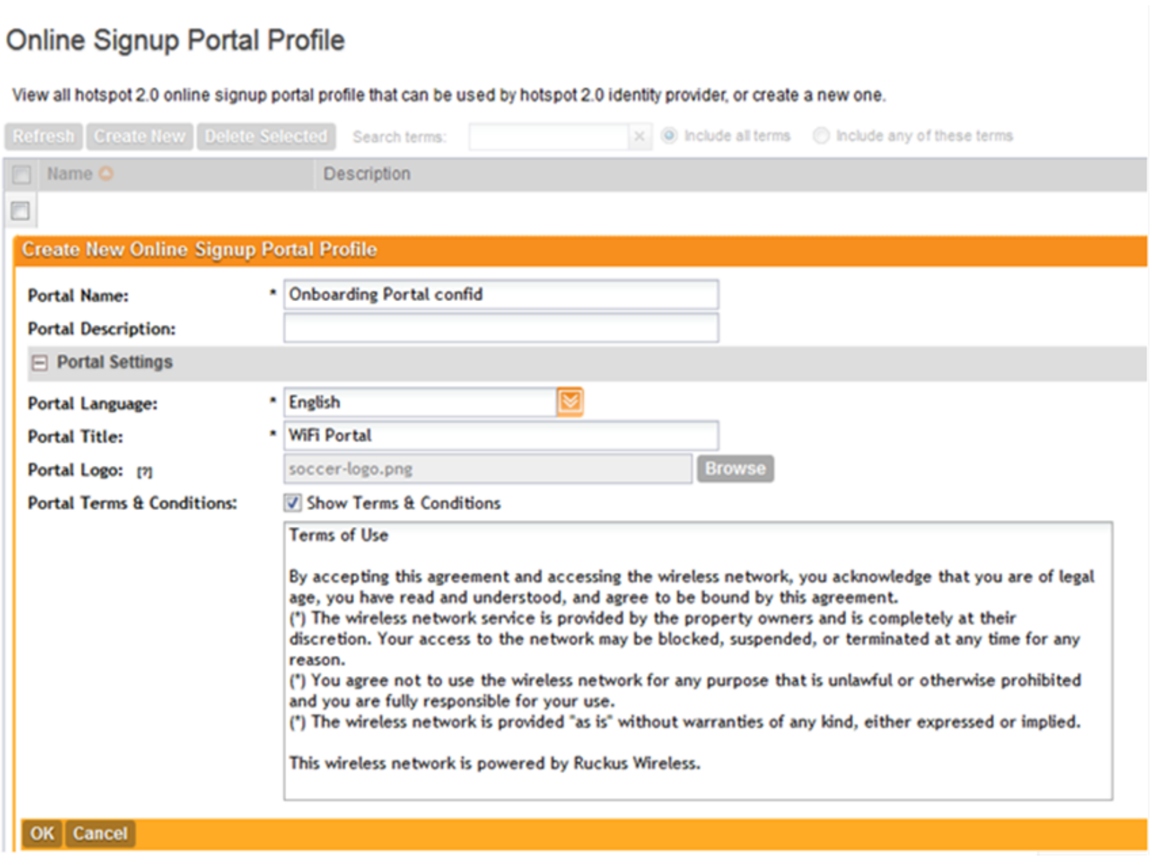
Follow these steps to define the look and feel of the Online Signup Portal.

1. Click **Configuration > Services&Profiles > Online SignUp Portal**.
2. The *Hotspot 2.0 Wi-Fi* page appears. Click **Create New**.
3. Configure the Online SignUp Portal configuration options in the table to create a Hotspot 2.0 OSU portal profile:

Option	Description
Portal Name	Enter the portal name.
Description (Optional)	Enter a description for the portal profile.
Portal Language	This option allows the administrator to choose the language that the portal will be displayed to the user.
Portal Title	The title as seen by the user.
Portal Logo	Choose the logo as seen by the user.
Terms and Conditions	The terms and conditions that will be accepted by the user.

4. Click **OK**. You have completed creating a Hotspot 2.0 online signup portal.
5. Continue to Authentication Services.

Figure 19: Online SignUp Portal form



Online Signup Portal Profile

View all hotspot 2.0 online signup portal profile that can be used by hotspot 2.0 identity provider, or create a new one.

Create New Online Signup Portal Profile

Portal Name: * Onboarding Portal confid

Portal Description:

Portal Settings

Portal Language: * English

Portal Title: * WiFi Portal

Portal Logo: [?] soccer-logo.png

Portal Terms & Conditions: ☑ Show Terms & Conditions

Terms of Use

By accepting this agreement and accessing the wireless network, you acknowledge that you are of legal age, you have read and understood, and agree to be bound by this agreement.
(*) The wireless network service is provided by the property owners and is completely at their discretion. Your access to the network may be blocked, suspended, or terminated at any time for any reason.
(*) You agree not to use the wireless network for any purpose that is unlawful or otherwise prohibited and you are fully responsible for your use.
(*) The wireless network is provided "as is" without warranties of any kind, either expressed or implied.

This wireless network is powered by Ruckus Wireless.

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 **Configuration > Services&Profiles > Services > Authentication**.
2. The *Authentication Service* page appears. Click **Create New**.
3. 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”).

Option	Description
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.

4. Click **OK**.

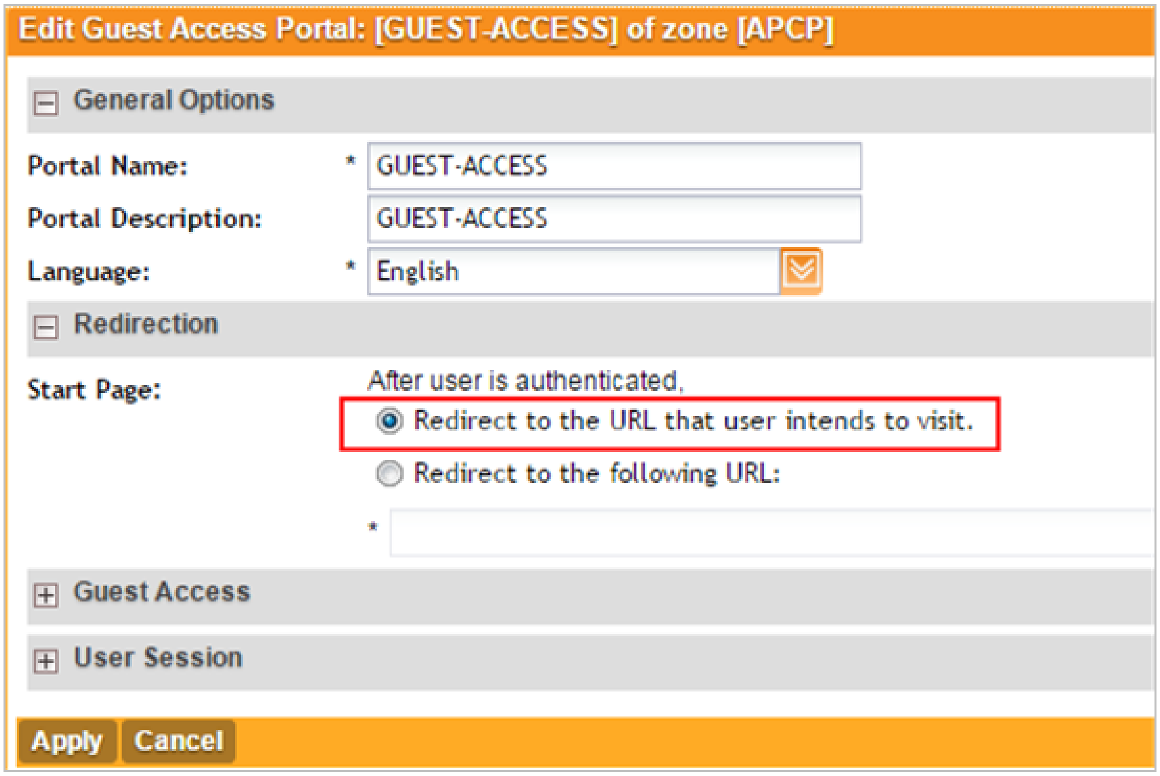
AP Zone - Guest Access

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 **Configuration > AP Zone> Guest Access**.
2. The *Guest Access Portal* page appears. Click **Create New**.
3. The related configuration options are language (labels on the URL page), title, logo and terms and conditions.
4. Click OK. You have completed creating / enabling guest access portal window.

Figure 20: Guest Access Redirection



Edit Guest Access Portal: [GUEST-ACCESS] of zone [APCP]

⊟ General Options

Portal Name: * GUEST-ACCESS

Portal Description: GUEST-ACCESS

Language: * English

⊟ Redirection

Start Page: After user is authenticated,

● Redirect to the URL that user intends to visit.

○ Redirect to the following URL:

*

⊞ Guest Access

⊞ User Session

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 **Configuration > AP Zones > WLAN**.
2. On the *AP Zone List* page, select the AP zone in the *WLAN Services & Group* page.
3. In **WLAN Usage> Authentication Type** enable Guest Access + Hotspot 2.0 Online Signup.
4. In *Online SignUp/Onboarding Service* enable the Zero-IT Onboarding option.
   a. Onboarding Portal - This is as per the Online SignUp Portal Profile configuration.
   b. Authentication Services - Select the authentication services, which a user will use during onboarding. Define:
      a. Service - Option to choose all authentication services (Local database RADIUS, LDAP, AD and OAuth)
      b. Credential Type - Local -All authentication types are available for this selection. After successful onboarding authentication using the credentials the user provides in the onboarding portal, IDM generates new credentials for this user

which is used in the Zero-IT configuration file. The username is composed of UUID@Realm. The UUID is randomly generated and the realm is taken from the “Realm” text box.

Remote – Only RADIUS authentication type is available and the credentials used in the Zero-IT configuration file is the same user name and password that the user fills in the onboarding portal.

c. Realm value is leveraged only for provisioning Hotspot 2.0 Rel 1 capable for Apple/Samsung devices (See: Apple and Samsung Hotspot 2.0 Release 1 (Passpoint) Devices) and legacy for non-Hotspot 2.0 devices (if credential type is set to 'Local'). If the credential type is set to Remote, then this realm value is not utilized for provisioning legacy devices. As a result, while configuring authentication profile for access WLAN, the administrator must appropriately map different realms to their respective authentication services. If device onboarding is with credential type:

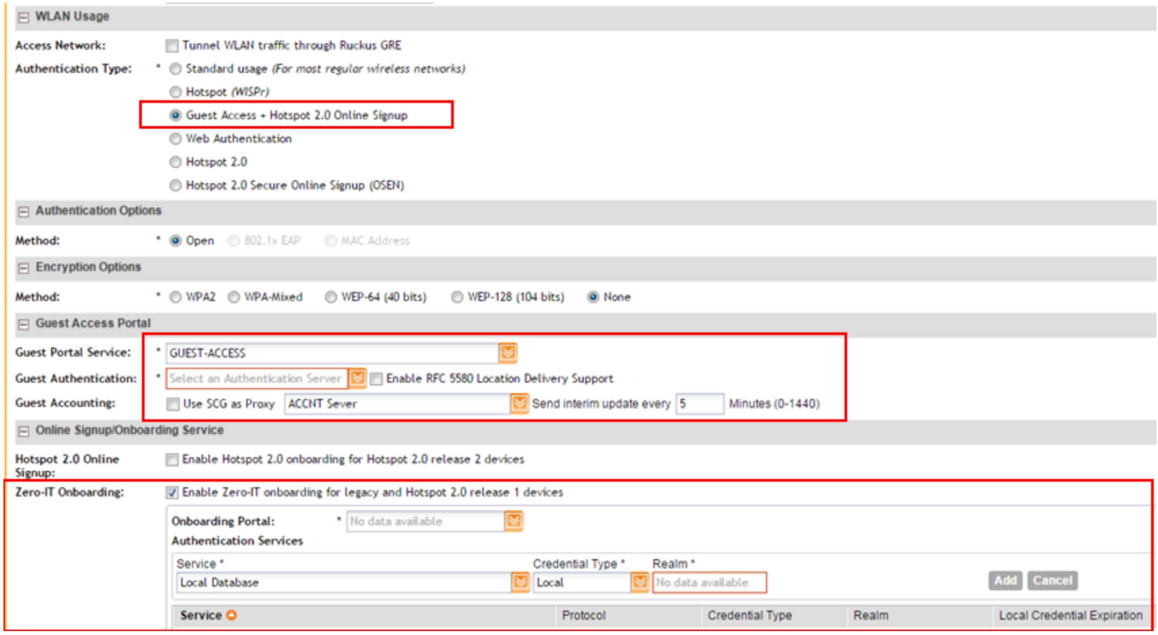
Local, then map 'realm' to Local Database

Remote, then map realm value to its respective authentication service and also define Unspecified realm and map it to the corresponding authentication service for handling legacy devices.

d. Local Credential Expiration - In case this option and the selected authentication service is not Local database, the administrator is required to set the expiration value. In case Local database is selected, the expiration value is taken from the existing credential of the users.

5. Click **Apply**. You have completed enabling guest access for legacy devices.

Figure 21: Configuring Guest Access for Legacy Devices



⊟ WLAN Usage

Access Network: □ Tunnel WLAN traffic through Ruckus GRE

Authentication Type: *
○ Standard usage *(For most regular wireless networks)*
○ Hotspot *(WISPr)*
● Guest Access + Hotspot 2.0 Online Signup
○ Web Authentication
○ Hotspot 2.0
○ Hotspot 2.0 Secure Online Signup (OSEN)

⊟ Authentication Options

Method: * ● Open ○ 802.1x EAP ○ MAC Address

⊟ Encryption Options

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

⊟ Guest Access Portal

Guest Portal Service: * GUEST-ACCESS

Guest Authentication: * Select an Authentication Server □ Enable RFC 5580 Location Delivery Support

Guest Accounting: □ Use SCG as Proxy ACCNT Sever Send interim update every 5 Minutes (0-1440)

⊟ Online Signup/Onboarding Service

Hotspot 2.0 Online Signup: □ Enable Hotspot 2.0 onboarding for Hotspot 2.0 release 2 devices

Zero-IT Onboarding: ☑ Enable Zero-IT onboarding for legacy and Hotspot 2.0 release 1 devices

Onboarding Portal: * No data available

Authentication Services

Service * Local Database
Credential Type * Local
Realm * No data available

Service	Protocol	Credential Type	Realm	Local Credential Expiration

A
External Onboarding and Remediation Portal Integration

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 **Configuration > SCG Systems > Northbound Portal 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.

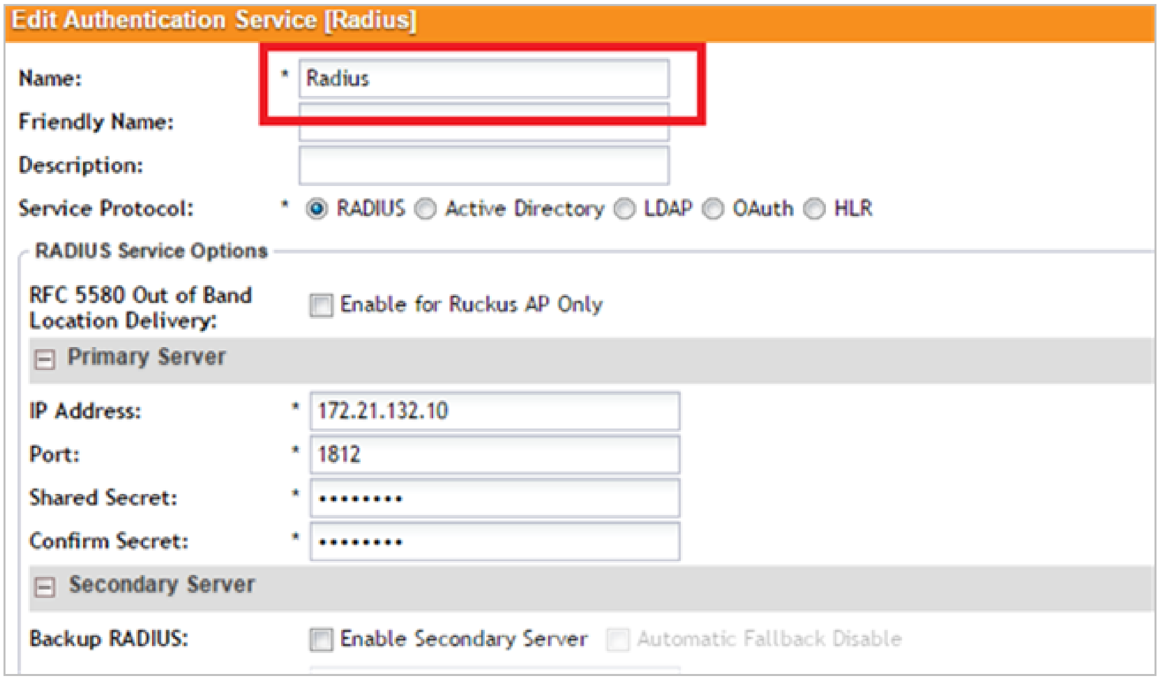
Request Content

```
{
"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 **Configuration > Services&Profiles > Authentication** in the controller web interface as seen in the figure. This configuration is applied to the specific Online Signup & Provisioning in **Configuration > Services&Profiles > Hotspot 2.0 Identity Provider**

Figure 22: Authentication Configuration



Edit Authentication Service [Radius]

Name:	* Radius
Friendly Name:	
Description:	
Service Protocol:	* ● RADIUS ○ Active Directory ○ LDAP ○ OAuth ○ HLR

RADIUS Service Options

RFC 5580 Out of Band Location Delivery:	□ Enable for Ruckus AP Only

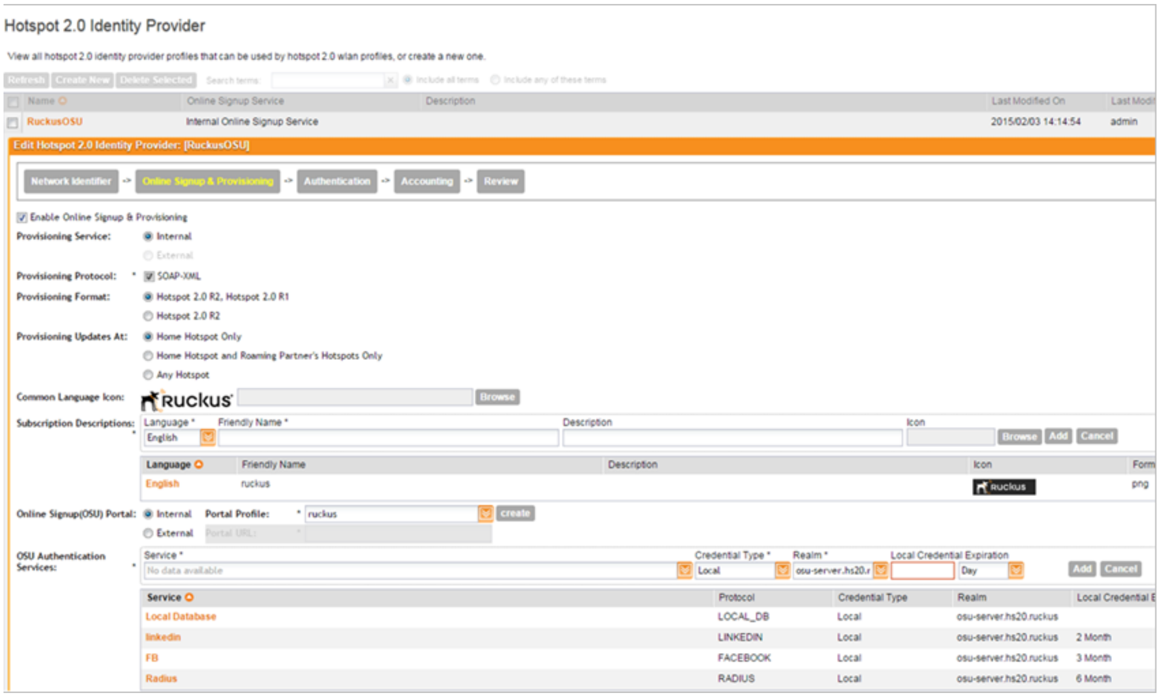
⊟ Primary Server

IP Address:	* 172.21.132.10
Port:	* 1812
Shared Secret:	* ••••••••
Confirm Secret:	* ••••••••

⊟ Secondary Server

Backup RADIUS:	□ Enable Secondary Server □ Automatic Fallback Disable

Figure 23: Identity Provider Configuration



Hotspot 2.0 Identity Provider

View all hotspot 2.0 identity provider profiles that can be used by hotspot 2.0 wlan profiles, or create a new one.

Refresh
Create New
Delete Selected
Search terms:
Include all terms
Include any of these terms

Name	Online Signup Service	Description	Last Modified On	Last Modi
RuckusOSU	Internal Online Signup Service		2015/02/03 14:14:54	admin

Edit Hotspot 2.0 Identity Provider: [RuckusOSU]

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

☑ Enable Online Signup & Provisioning

Provisioning Service:	● Internal ○ External
Provisioning Protocol: *	☑ SOAP-XML
Provisioning Format:	● Hotspot 2.0 R2, Hotspot 2.0 R1 ○ Hotspot 2.0 R2
Provisioning Updates At:	● Home Hotspot Only ○ Home Hotspot and Roaming Partner's Hotspots Only ○ Any Hotspot
Common Language Icon:	Ruckus

Subscription Descriptions: *

Language *	Friendly Name *	Description	Icon
English			

Language	Friendly Name	Description	Icon	Form
English	ruckus		Ruckus	png

Online Signup(OSU) Portal:	● Internal Portal Profile: * ruckus ○ External Portal URL: *

OSU Authentication Services: *

Service *	Credential Type *	Realm *	Local Credential Expiration
No data available	Local	osu-server.hs20.r	Day

Service	Protocol	Credential Type	Realm	Local Credential E
Local Database	LOCAL_DB	Local	osu-server.hs20.ruckus	
linkedin	LINKEDIN	Local	osu-server.hs20.ruckus	2 Month
FB	FACEBOOK	Local	osu-server.hs20.ruckus	3 Month
Radius	RADIUS	Local	osu-server.hs20.ruckus	6 Month

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 - **Configuration > Services&Profiles > 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

OAuth 2.0 Authentication

The following requests are sent to NBI when a user clicks on the OAuth provider icon.

- MAC encryption
- Request to open access to OAuth authorization URL
- Request authorization URL
- Register onboarding request

MAC Encryption

An encrypted request is sent to NBI to receive an encrypted response.

Request content

```
{
"Vendor": "Ruckus",
"RequestPassword": <NBI password as set in SCG>,
   "APIVersion": "1.1",
   "RequestCategory": "GetConfig",
   "RequestType": "Encrypt",
   "Data": <UE MAC>
}
```

Response content

```
{
"APIVersion":"1.1",
"Data":<Encrypted UE MAC>,
"ReplyMessage": "OK",
"ResponseCode": "200 ",
"Vendor":"Ruckus"
}
```

Use the following controller CLI commands to enable sending requests without the need to encrypt the UE-MAC address.

```
en
<cli password>
no encrypt-mac-ip
```

```
To enable encrypted UE-MAC address again:
en
<cli password>
encrypt-mac-ip
```

NOTE Executing this CLI command will affect WISPr configuration settings.

Adding OAuth Provider URL Path to AP ACL

To gain access to the OAuth login page, *ALLOW_BROWSE_OAUTH* request should be sent to NBI. The URL path, which the external onboarding portal sends as HTTP request to NBI is:

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

The following example indicates a successful request and response from NBI.

Request content

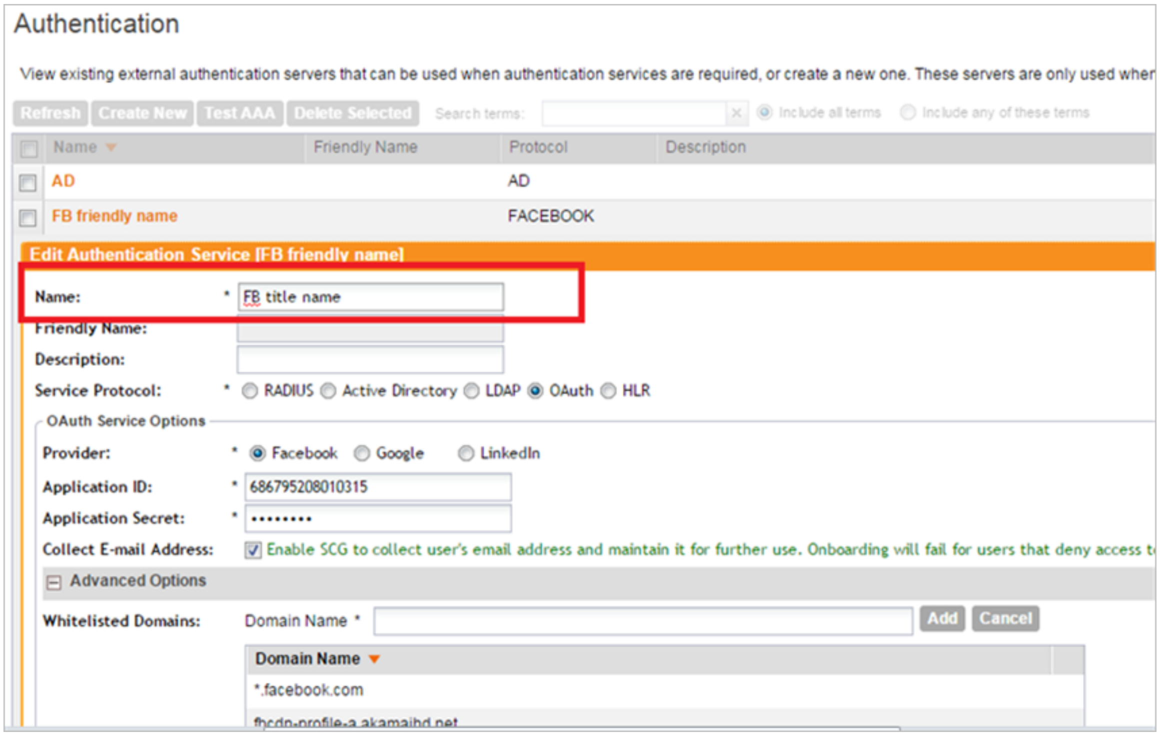
```
{
"MSG-ID" : ":< Unique ID for the message>,
"APIVersion" : "1.1",
"UE-MAC" : <UE MAC>,
"RequestType" : "ALLOW_BROWSE_OAUTH",
"RequestCategory" : "UserOnlineControl",
"OAuth-Provider" : <OAuth type>,
"Vendor" : "Ruckus",
"RequestPassword" : <NBI password as set in SCG>
}
```

Parameter

- *MSG-ID* identifies the related request and response

NOTE The parameter - OAuth-Provider is the name configured in the controller web interface - Configuration > Services&Profiles > Authentication. See figure.

Figure 24: OAuth Provider Configuration



Authentication

View existing external authentication servers that can be used when authentication services are required, or create a new one. These servers are only used wher

□	Name	Friendly Name	Protocol	Description
□	AD		AD	
□	FB friendly name		FACEBOOK	

Edit Authentication Service [FB friendly name]

Name: * FB title name
Friendly Name:
Description:
Service Protocol: * ○ RADIUS ○ Active Directory ○ LDAP ● OAuth ○ HLR

OAuth Service Options

Provider: * ● Facebook ○ Google ○ LinkedIn
Application ID: * 686795208010315
Application Secret: * ••••••••
Collect E-mail Address: ☑ Enable SCG to collect user's email address and maintain it for further use. Onboarding will fail for users that deny access t

⊟ Advanced Options

Whitelisted Domains: Domain Name *

Domain Name
*.facebook.com
fbcdn-profile-a.akamaihd.net

Response content

```
{
"APIVersion" : "1.1",
"UE-MAC" : "ENC32D7046A0C3F5EA9",
"ReplyMessage" : "OK",
"ResponseCode" : 200,
"Output" : {
}
}
```

Authorization URL and Access Token

Upon successful *ALLOW_BROWSE_OAUTH* response the portal sends the *BuildOauthUrl* request to NBI. This is required to get the URL which the portal redirects the user to remote OAuth provider login page based on OAuth provider configuration in the controller web interface. After the user is logged in, OAuth Provider redirects the UE to a callback URL, which is specified in *redirectUrl* parameter. In the callback side, the access code is returned and passed to IDM to retrieve the access token by access code. The returned URL response of *BuildOauthUrl* is the URL which is executed when the user clicks on the OAuth login icon, right after successful *ALLOW_BROWSE_OAUTH* response.

BuildOAuth URL Request Content

UE-MAC address is retrieved from the URL request.

```
{
"MSG-ID" : < Unique ID for the message different than
the one in ALLOW_BROWSE_OAUTH >,
"Vendor" : "Ruckus",
"RequestPassword" : <NBI password as set in SCG>,
"APIVersion" : "3.1.0",
"UE-MAC" : <Device MAC>,
"RequestType" : "BuildOauthUrl",
"RequestCategory" : "UserManagement",
"Input" : {
"authenticationServerName" : <authentication sever name>,
"sessionId" : "954316EDC578BD1AF464F3FCFCAF568B",
"redirectUrl" : <redirect Url that appear in the OAuth app>
}
}
```

Parameter

UE-MAC can be retrieved from the URL request

BuildOAuth URL Response Content

```
{
"MSG-ID" : < Unique ID for the message - same as in the request
 >,
"APIVersion" : "3.1.0",
"UE-MAC" : <Device MAC>,
"ReplyMessage" : "OK",
"ResponseCode" : 200,
"Output" : {
"url" : <a URL to redirect the user for login>
}
```

Parameter

- *MSG-ID* identifies the related request and response

Registration Request Content to NBI from OAuth

The portal redirects the user to the URL path that appears in *BuildOauthUrl* response under *Output.url*. For example:

```
www.facebook/V1.0/dialog/aouth?client_id =
{app-id}&redirect_uri={redirectUrl}
```

The user is now asked to login with his/her OAuth credentials. On successful login, the OAuth redirects the UE to the callback path configured in the OAuth app, which is actually the value of “*redirectUrl*" as seen in the above request content. An external web service / handler is required by the customer to implement as well handle the post request from OAuth provider to *redirectUrl* and sends a registration request to the NBI.

Request Content

```
{
"MSG-ID" : < Unique ID for the message different than the
one in the previous request >,
"Vendor" : "Ruckus",
"RequestPassword" : <NBI password as set in SCG>,
"APIVersion" : "3.1.0",
"UE-MAC" : <Device MAC>,
"RequestType" : "RegistrationOnboarding",
"RequestCategory" : "UserManagement",
"Input" : {
"userAgent" : <user agent>
"hsReleaseVersion" : "0",
"wlanId" : "3",
"credentials" : {
"codeForAccessToken" : <code token to access OAuth
retrieved from request parameters (parameter value will be
“code”)>,
"redirectUrl" :  <redirect Url that appears in the OAuth app>
"authenticationServerName" : <authentication sever name>,
},
"remediation" : <boolean value true for remediation
flow and false otherwise>
}
}
}
```

Successful IDM Response Content

On a successful response from the NBI, the portal redirects the client to the *RedirectUri* passed as one of the parameters in the URL. The `redirectUri` parameter is passed by the UE in the initial registration request. The value of this parameter invokes the connection manager within the client to continue with the registration flow. The following is the successful response from the NBI.

Response Content

```
{
"MSG-ID" : <Unique ID of the message -
Same as the one in the request>,
"APIVersion" : "3.1.0",
"UE-MAC" : <Device MAC - Same as the one in the request >,
"ReplyMessage" : "Registration Succeeded",
"ResponseCode" : 203,
"Output" : {
"user" : {
"replyMessage" : "OK",
"responseCode" : 200,
"credentialsList" : [ {
"authenticationMethod" : "USERNAME_PASSWORD",
"key" : "9cf3c104-9893-46ec-a161-191064a95cad",
"serviceProviderId" : "839f87c6-d116-497e-afce-aa8157abd30c",
"creationDate" : 1423649934734,
"expirationDate" : 32503672800330,
"loginName" : <user login name- Same as the one in the request
 >,
"loginPassword" : "",
"authenticationServerId" :
"6403d050-b1c6-11e4-a90f-000c29e52e92",
"authenticationServerName" : "raduis",
"authenticationServerType" : "RADIUS",
"passwordCreation" : 1423649934734,
"passwordExpiration" : 32503672800330
}, {
"authenticationMethod" : "MO",
"key" : "db978393-d87b-475f-a054-8569b762bbc7",
"serviceProviderId" : "839f87c6-d116-497e-afce-aa8157abd30c",
"creationDate" : 1424258217340,
"expirationDate" : 32503672800330,
"loginName" : "db978393-d87b-475f-a054-8569b762bbc7",
"loginPassword" : "",
"machineManaged" : true,
"ableToShare" : false,
"deviceId" : "<Device MAC - Same as the one in the request >,",
"realm" : "osu-server.hs20.ruckus ",
"updateIdentifer" : 7,
"hsReleaseVersion" : "0",
"onboardingWlanId" : "1",
"passwordCreation" : 1424258217340,
"passwordExpiration" : 32503672800330
}, {
"authenticationMethod" : "MO",
"key" : "53f30919-6f68-4cee-b5ec-c657d6ec4add",
"serviceProviderId" : "839f87c6-d116-497e-afce-aa8157abd30c",
"creationDate" : 1424167256743,
"expirationDate" : 32503672800330,
"loginName" : "53f30919-6f68-4cee-b5ec-c657d6ec4add",
"loginPassword" : "",
"machineManaged" : true,
"ableToShare" : false,
"deviceId" : "00:24:D7:F1:B8:04",
"realm" : "osu-server.hs20.ruckus ",
"updateIdentifer" : 8,
"hsReleaseVersion" : "0",
"onboardingWlanId" : "1",
"passwordCreation" : 1424167256743,
"passwordExpiration" : 32503672800330
}, {
"authenticationMethod" : "MO",
"key" : "9ef43dbe-2139-4c80-b002-71bd1174968c",
"serviceProviderId" : "839f87c6-d116-497e-afce-aa8157abd30c",
"creationDate" : 1424258339186,
"expirationDate" : 1432034339186,
"loginName" : "9ef43dbe-2139-4c80-b002-71bd1174968c",
"loginPassword" : "",
"machineManaged" : true,
"ableToShare" : false,
"deviceId" : "98:0C:82:5E:34:10",
"realm" : "osu-server.hs20.ruckus",
"updateIdentifer" : 7,
"hsReleaseVersion" : "2",
"onboardingWlanId" : "1",
"passwordCreation" : 1424258339186,
"passwordExpiration" : 1432034339186
} ],
"uniqueId" : "0c21c61e-00d1-4b63-8b75-7026637eed6f",
"selectedPackage" : "839f87c6-d116-497e-afce-aa8157abd30c",
"serviceProviderId" : "839f87c6-d116-497e-afce-aa8157abd30c",
"creatorUUID" : "92cc1b65-c3cd-4f26-8c9b-3e7b055c7c25",
"primaryUser" : true,
"userStatus" : "ENABLED",
"subscriberType" : "REMOTE",
"subscriberId" : "5168c8e0-ed0d-4566-a720-f39b5a988e30",
"userName" : "user1-in-group",
"displayName" : "user1-in-group",
"aaaId" : "6403d050-b1c6-11e4-a90f-000c29e52e92",
"aaaName" : "raduis",
"subscriptionDto" : {
"replyMessage" : "OK",
"responseCode" : 200,
"key" : "0825fc09-8ebb-46e9-a104-c5a76a2206b9",
"activationDate" : 1423649934627,
"expirationDate" : 1486808334628,
"creationDate" : 1423649934627,
"businessPackage" : {
"replyMessage" : "OK",
"responseCode" : 200,
"name" : "RemoteUserPackage",
"key" : "839f87c6-d116-497e-afce-aa8157abd30c",
"expirationInterval" : "YEAR",
"expirationValue" : 2,
"serviceProviderId" : "839f87c6-d116-497e-afce-aa8157abd30c",
"creatorUUID" : "92cc1b65-c3cd-4f26-8c9b-3e7b055c7c25",
"state" : "ACTIVE"
},
"status" : "AVAILABLE"
},
"createDateTime" : 1423649934411,
"userSource" : "raduis",
"userRole" : "Default",
"tenantUUID" : "839f87c6-d116-497e-afce-aa8157abd30c"
},
"UE-UserUniqueId" : "0c21c61e-00d1-4b63-8b75-7026637eed6f"
}
}
```

Failure Response Content

In case of failure an error message is sent by the IDM and the user is allowed reauthentication of user credentials.

Response Content

```
{
"MSG-ID" : <Unique ID of the message -
Same as the one in the request>,
"APIVersion" : "3.1.0",
"UE-MAC" : <Device MAC - Same as the one in the request >,
"ReplyMessage" : <reason of failure >,
"ResponseCode" : <error code>,
"Output" : {
}
}
```

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 25: Interaction with OCSP server during Anonymous TLS

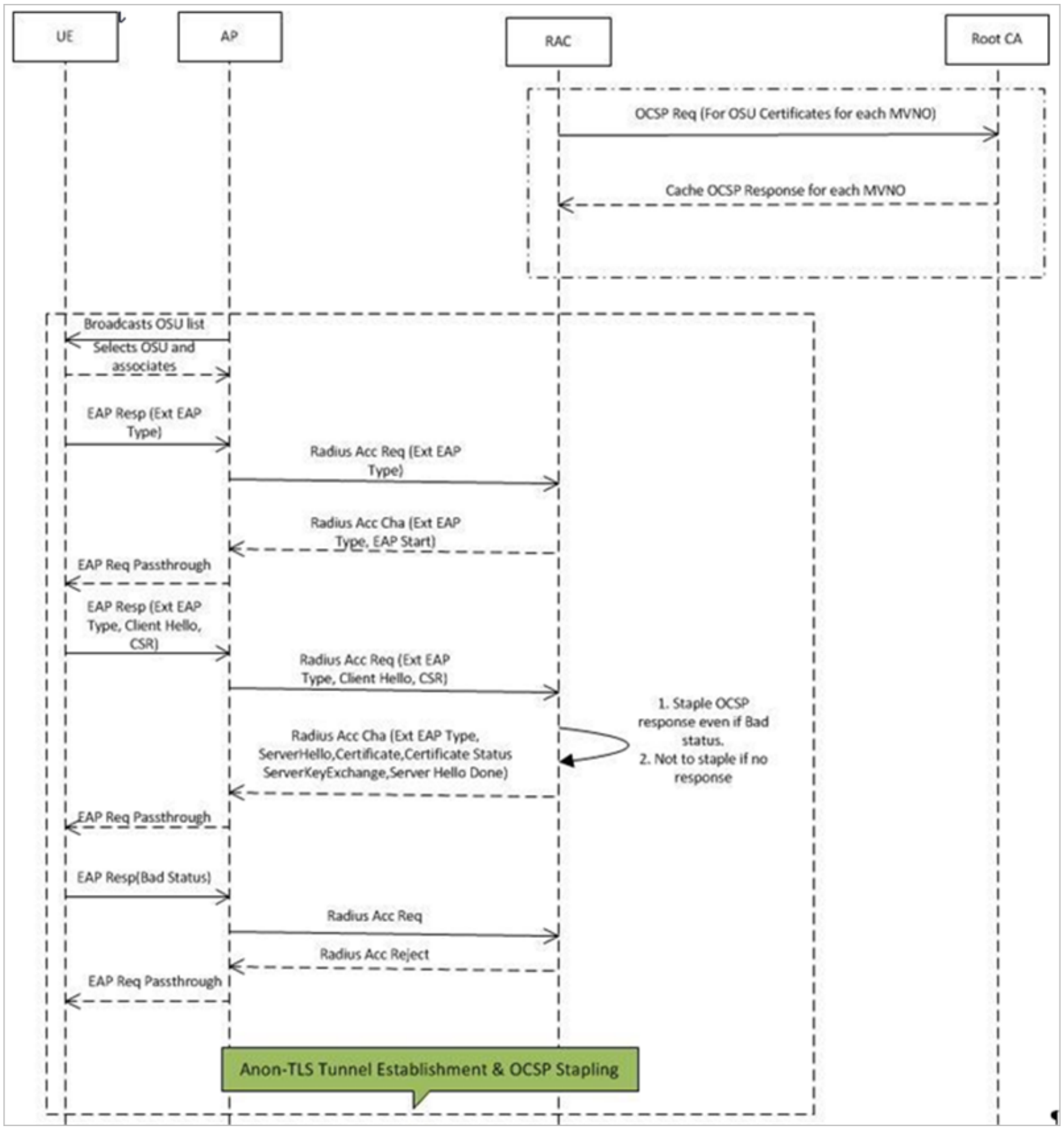
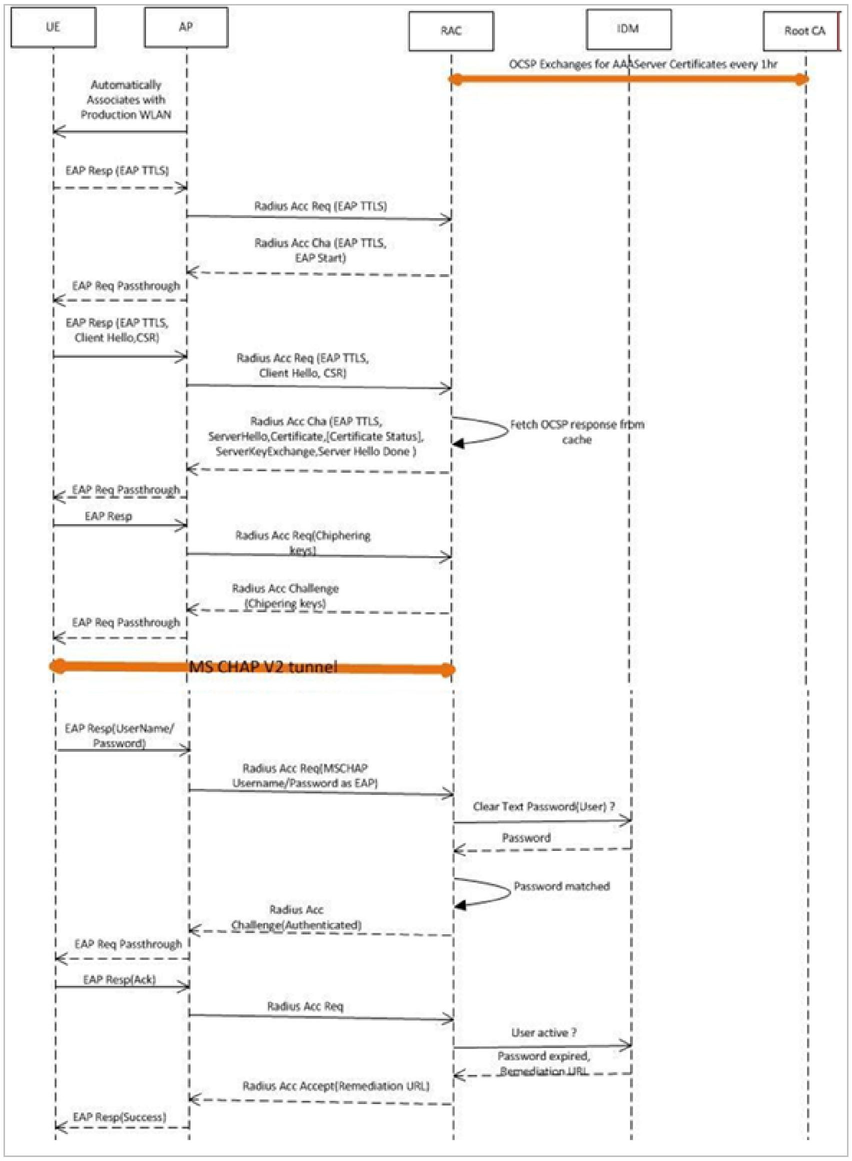

UE
AP
RAC
Root CA
OCSP Req (For OSU Certificates for each MVNO)
Cache OCSP Response for each MVNO
Broadcasts OSU list
Selects OSU and associates
EAP Resp (Ext EAP Type)
Radius Acc Req (Ext EAP Type)
Radius Acc Cha (Ext EAP Type, EAP Start)
EAP Req Passthrough
EAP Resp (Ext EAP Type, Client Hello, CSR)
Radius Acc Req (Ext EAP Type, Client Hello, CSR)
1. Staple OCSP response even if Bad status.
2. Not to staple if no response
Radius Acc Cha (Ext EAP Type, ServerHello,Certificate,Certificate Status ServerKeyExchange,Server Hello Done)
EAP Req Passthrough
EAP Resp(Bad Status)
Radius Acc Req
Radius Acc Reject
EAP Req Passthrough
Anon-TLS Tunnel Establishment & OCSP Stapling

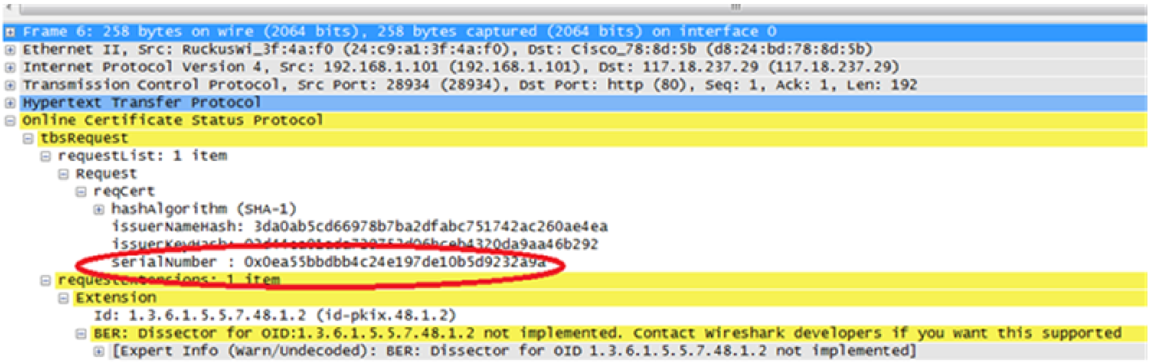
Figure 26: Interaction with OCSP server during EAP-TLS


UE
AP
RAC
IDM
Root CA
OCSP Exchanges for AAAServer Certificates every 1hr
Automatically Associates with Production WLAN
EAP Resp (EAP TTLS)
Radius Acc Req (EAP TTLS)
Radius Acc Cha (EAP TTLS, EAP Start)
EAP Req Passthrough
EAP Resp (EAP TTLS, Client Hello,CSR)
Radius Acc Req (EAP TTLS, Client Hello, CSR)
Radius Acc Cha (EAP TTLS, ServerHello,Certificate,[Certificate Status], ServerKeyExchange,Server Hello Done)
Fetch OCSP response from cache
EAP Req Passthrough
EAP Resp
Radius Acc Req(Chiphering keys)
Radius Acc Challenge (Chipering keys)
EAP Req Passthrough
MS CHAP V2 tunnel
EAP Resp(UserName/ Password)
Radius Acc Req(MSCHAP Username/Password as EAP)
Clear Text Password(User) ?
Password
Password matched
Radius Acc Challenge(Authenticated)
EAP Req Passthrough
EAP Resp(Ack)
Radius Acc Req
User active ?
Password expired, Remediation URL
Radius Acc Accept(Remediation URL)
EAP Resp(Success)

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.

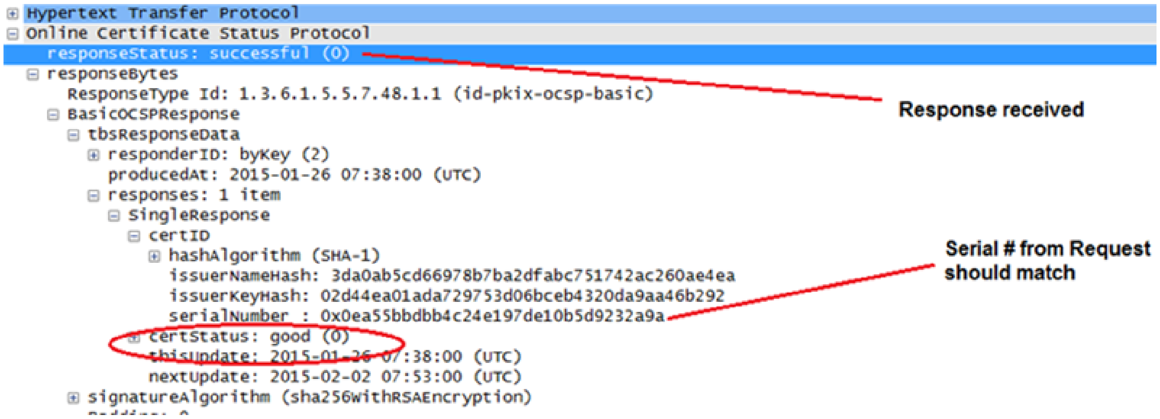
NOTE If the client (mobile device) requests for Certificate Status request, RAC provides the status if it is available. In case the certificate status is not provided it is up to the client if it wants to continue or abort the call.

Figure 27: Important OCSP Message



```
⊞ Frame 6: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits) on interface 0
⊞ Ethernet II, Src: RuckusWi_3f:4a:f0 (24:c9:a1:3f:4a:f0), Dst: Cisco_78:8d:5b (d8:24:bd:78:8d:5b)
⊞ Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: 117.18.237.29 (117.18.237.29)
⊞ Transmission Control Protocol, Src Port: 28934 (28934), Dst Port: http (80), Seq: 1, Ack: 1, Len: 192
⊞ Hypertext Transfer Protocol
⊟ Online Certificate Status Protocol
  ⊟ tbsRequest
    ⊟ requestList: 1 item
      ⊟ Request
        ⊟ reqCert
          ⊞ hashAlgorithm (SHA-1)
            issuerNameHash: 3da0ab5cd66978b7ba2dfabc751742ac260ae4ea
            issuerKeyHash: 02d44ea01ada729753d06bceb4320da9aa46b292
            serialNumber : 0x0ea55bbdbb4c24e197de10b5d9232a9a
    ⊟ requestExtensions: 1 item
      ⊟ Extension
          Id: 1.3.6.1.5.5.7.48.1.2 (id-pkix.48.1.2)
        ⊟ BER: Dissector for OID:1.3.6.1.5.5.7.48.1.2 not implemented. Contact Wireshark developers if you want this supported
          ⊞ [Expert Info (Warn/Undecoded): BER: Dissector for OID 1.3.6.1.5.5.7.48.1.2 not implemented]
```

Figure 28: OCSP Response Message



```
⊞ Hypertext Transfer Protocol
⊟ Online Certificate Status Protocol
    responseStatus: successful (0)
  ⊟ responseBytes
      ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
    ⊟ BasicOCSPResponse
      ⊟ tbsResponseData
        ⊞ responderID: byKey (2)
          producedAt: 2015-01-26 07:38:00 (UTC)
        ⊟ responses: 1 item
          ⊟ SingleResponse
            ⊟ certID
              ⊞ hashAlgorithm (SHA-1)
                issuerNameHash: 3da0ab5cd66978b7ba2dfabc751742ac260ae4ea
                issuerKeyHash: 02d44ea01ada729753d06bceb4320da9aa46b292
                serialNumber : 0x0ea55bbdbb4c24e197de10b5d9232a9a
            ⊞ certStatus: good (0)
              thisUpdate: 2015-01-26 07:38:00 (UTC)
              nextUpdate: 2015-02-02 07:53:00 (UTC)
      ⊞ signatureAlgorithm (sha256WithRSAEncryption)
```

Response received

Serial # from Request should match

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
```

Simply Better Wireless.

350 West Java Drive, Sunnyvale, CA

www.ruckuswireless.com