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

Hotspot 2.0 Reference Guide for SmartZone 3.4.1

Part Number 800-71362-001 Rev A
Published October 2016

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Copyright 2016. Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ruckus Wireless, Inc. (“Ruckus”), or as expressly provided by under license from Ruckus.

Destination Control Statement

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Contents

About This Guide

Document Conventions 6
Terminology 7
Related Documentation 8
Online Training Resources 9
Documentation Feedback 9

1 Hotspot 2.0 Technology Overview

Brief Overview 11
Basic Operation of Hotspot 2.0 11
Operators and Service Providers 13

2 Configuring Hotspot 2.0

Step 1: Upload Certificates 16
Step 2: Define Wi-Fi Operator Profile 18
Step 3: Define Identity Provider 20
Network Identifier 20
Online SignUp and Provisioning 23
Authentication 26
Accounting 28
Review 29
Step 4: Define Onboard WLAN 30
Define Secure Onboarding - Hotspot 2.0 OSEN 30
Step 5: Define Hotspot 2.0 Profile 31
Step 6: Define Access WLAN 34
Step 7: Create Venue Profile 35
Adding Venue Profile in AP 36
Adding Venue Profile in AP Group 37
Adding Venue Profile in AP Zone 38

3 Hotspot 2.0 R2 Device Workflow

Onboarding Flow 41
Access Hotspot 2.0 43

De-Auth 44
Remediation 44
Password Expired 45
Update Identifier 45
AAA Combinations 46

4 Configuring Legacy Devices
Authentication Services 48

A External Onboarding and Remediation Portal Integration
Overview 50
Authentication in Onboarding Flow 50
Authentication in Remediation Flow 54
OAuth 2.0 Authentication 55
MAC Encryption 56
Adding OAuth Provider URL Path to AP ACL 57
Authorization URL and Access Token 59

B OCSP Stapling Support in SCG

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

Index

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 If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

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 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

Convention	Description	Example
`monospace`	Represents information as it appears on screen	`[Device name]>`
`monospace bold`	Represents information that you enter	`[Device name]>` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	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
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

Table 3 lists the terms used in this guide.

Table 3. Terms used in this guide

Terms	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
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

Table 3. Terms used in this guide

Terms	Description
Release1 Device	Hotspot 2.0 Release1 specification compliant device
Release 2 Device	Hotspot 2.0 Release 2 compliant device
RSN	Robust Security Network
SCG	Smart Cell Gateway
SSID	Service Set Identifier
SSL	Secure Socket Layer
T&C	Terms and Conditions
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTLS	Tunneled TLS
UDI	User Define Interface
UE	User Equipment
UE-IP	User Equipment - IP Address
UE-MAC	User Equipment - MAC Address
UI	User Interface
URI	Uniform Resource Identifier
USIM	Universal Subscriber Identity Module
UTP	User Traffic Profile
UUID	Universal Unique Identifier
VSA	Vendor Specific Attributes
WAN	Wide Area Network
WFA	Wi-Fi Alliance
WLAN	Wireless Local Area Network

Related Documentation

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

Online Training Resources

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

Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

docs@ruckuswireless.com

When contacting us, please include the following information:

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

For example:

- SCG-200 and vSZ-H Hotspot 2.0 Reference Guide for SmartZone 3.4.1
- Part number: 800-71362-001
- Page 88

Hotspot 2.0 Technology Overview

1

In this chapter:

- Brief Overview
- Basic Operation of Hotspot 2.0
- Operators and Service Providers

Brief Overview

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:

- **a** Automated network discovery and selection
- **b** Secure authentication
- **c** Online sign-up
- **d** Policy management

The first release of Hotspot 2.0 focuses on components a and b, whereas release 2 goes into specification of components c and d.

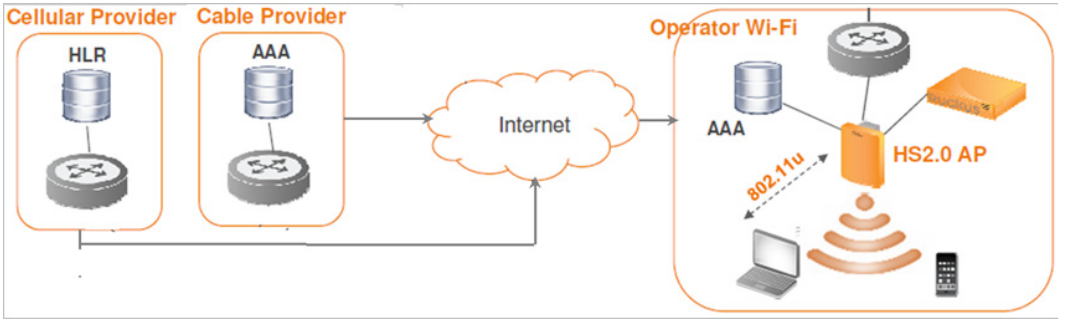
Basic Operation of Hotspot 2.0

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. After 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 the user will be directed to a sign-up portal over Hotspot 2.0 onboarding WLAN. Upon successful authentication, the user will be provisioned with Hotspot 2.0 standards-based management object known as Per-Provider Subscription Management object (PPS-MO). The 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 the provider's home Wi-Fi network and the visited Wi-Fi network in a 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 Figure 1.

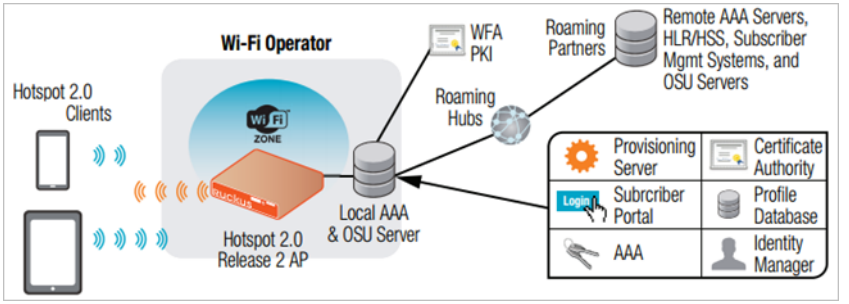
Figure 1. Working of Hotspot 2.0



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, an entity offering a Wi-Fi infrastructure may be termed as a Wi-Fi operator, while an entity owning a user database may be termed as an 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 Figure 2.

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

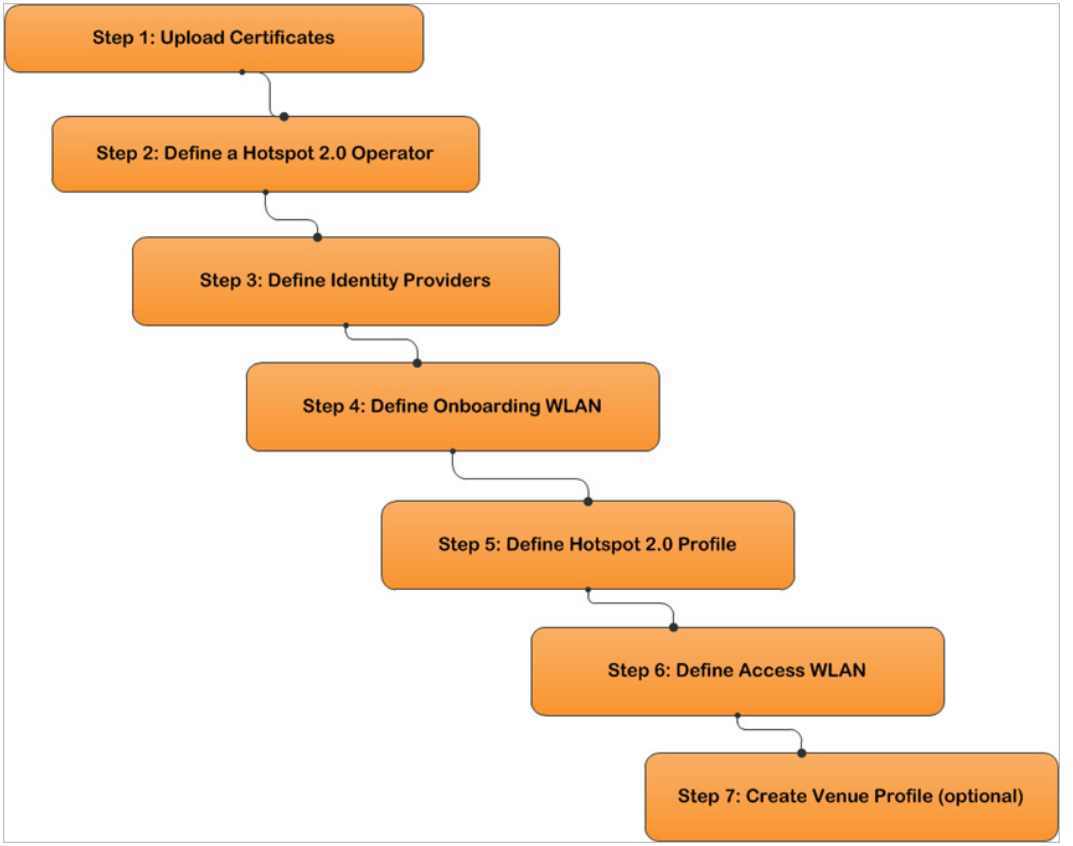
2

In this chapter:

- Step 1: Upload Certificates
- Step 2: Define Wi-Fi Operator Profile
- Step 3: Define Identity Provider
- Step 4: Define Onboard WLAN
- Step 5: Define Hotspot 2.0 Profile
- Step 6: Define Access WLAN
- Step 7: Create Venue Profile

Figure 3 shows the Hotspot 2.0 R2 devices configuration flow. To enable this flow the following are the entities that need to be configured.

Figure 3. Hotspot 2.0 Configuration Flow



NOTE: Hotspot 2.0 WLANs do not support IPv6.

Step 1: Upload Certificates

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

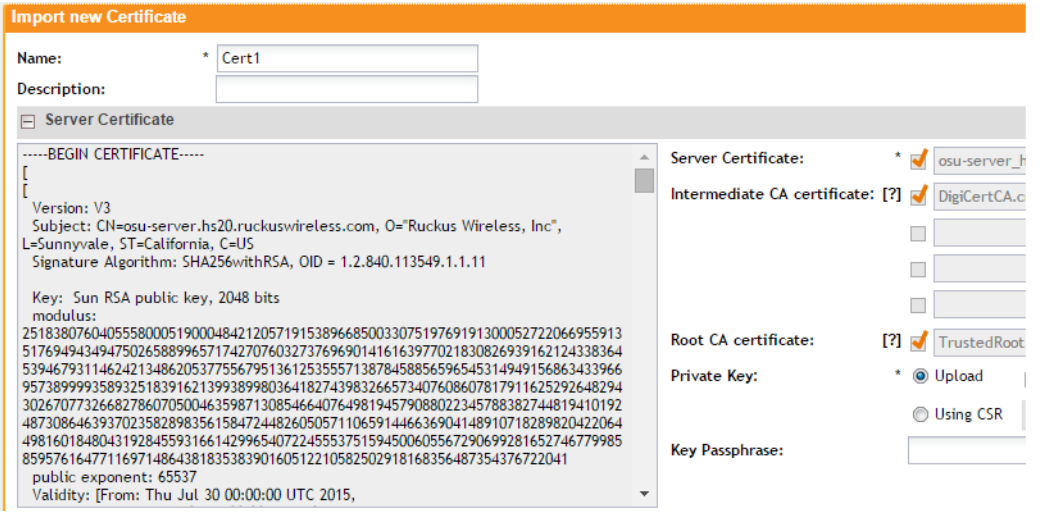
1 Click **Configuration** > **SCG Systems > Certificates > Certificate Store**
2 The *Certificate Store* page appears. Click **Import New**.
3 Use the *Browse* option to choose the root certificate file.
4 Click *Upload* to upload the root certificate.
5 Click *Apply* and review the certificate in the left pane text area.
6 Click *OK* to completing 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 completing 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 root and server certificates. You have also 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

NOTE: 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 controller Web interface.

Figure 4. Importing a Certificate



Step 2: Define Wi-Fi Operator Profile

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

1 Click **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 Table 4 to create a Hotspot 2.0 Wi-Fi operator.

Table 4. Wi-Fi operator configuration options

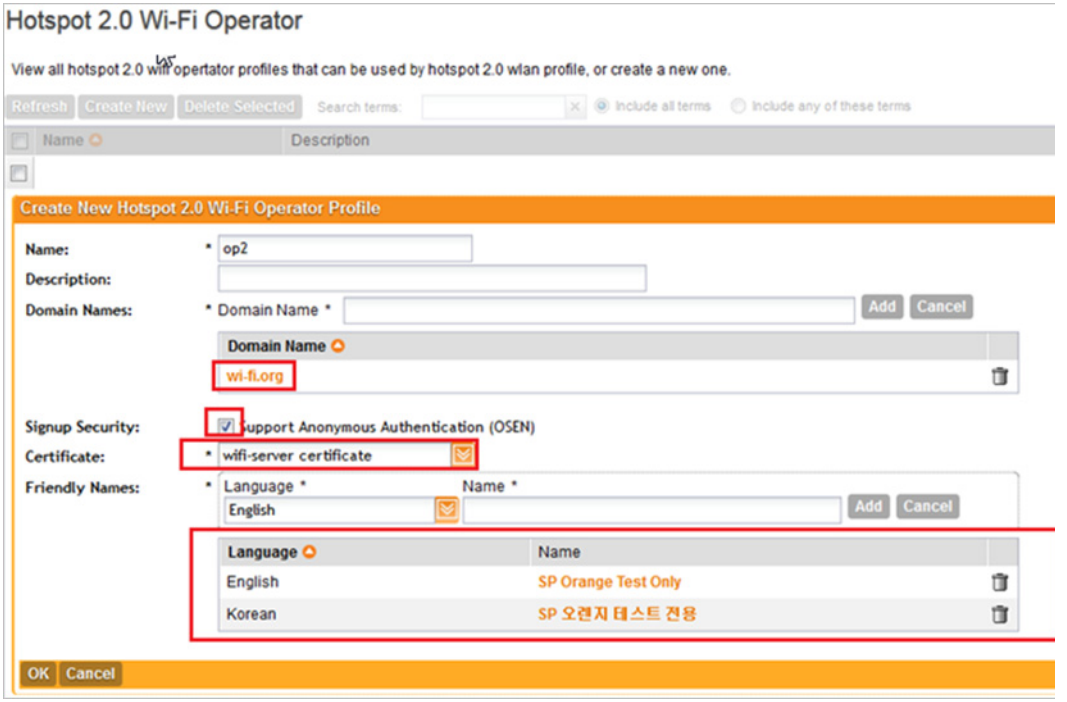
Option	Description
Name	Enter a name for this Wi-Fi operator profile.
Description (Optional)	Enter a description for the venue profile.
Domain Names	HS2.0 operator's domain name is a mandatory field, which specifies the operator's domain name. Hotspot 2.0 AP broadcasts the domain name to indicate the home Wi-Fi providers.
Signup Security	This is an optional field and is disabled by default. Enabling would mean that operator supports secure onboarding (OSEN).
Certificate	Select the certificate for the operator - AAA. This can be the same certificate as the one used with OSU service.
Friendly 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 then 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



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
- 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**.

2 The *Hotspot 2.0 Identity* page appears. Click **Create New**.

3 Configure the settings in Table 5 to create a Hotspot 2.0 Network Identifier. Alternatively, network identifier can be imported from an existing Hotspot 2.0 Wi-Fi operator.

Table 5. Network Identifier options

Option	Description
Name	Enter a name or this network identifier profile.
Description (Optional)	Enter a description for the network identifier profile.
PLMNs	Each record contains MCC and MNC. • MCC: Set the correct country code for the geographical location. This is required when the controller sends MAP authentication information. Type the mobile country code digits. Decimal digit strings with maximum length of 3 and minimum length of 2. • MNC: Set the mobile network code based on the geographical location. This is required when controller sends MAP authentication information. Type the mobile network code digits. Decimal digit strings with maximum length of 3 and minimum length of 2.

Table 5. Network Identifier options

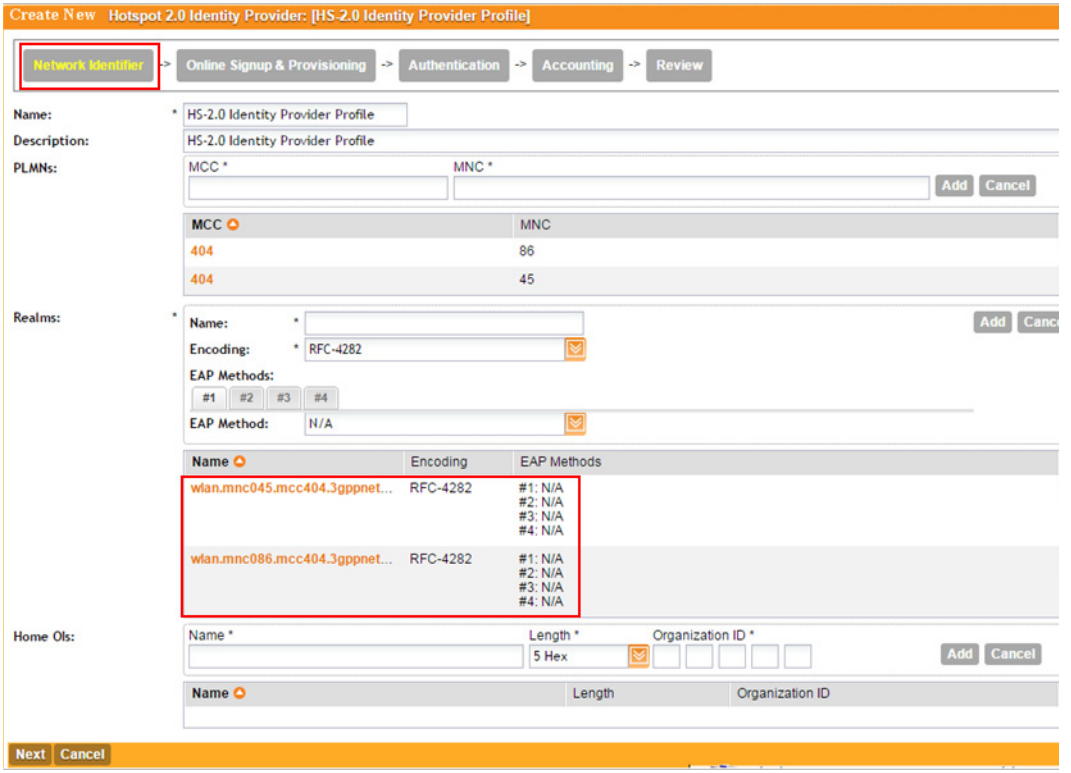
Option	Description
Realms	List of NAI realms corresponding to service providers or other entities whose networks or services are accessible via this AP. Up to five NAI realm entries can be created. Each NAI realm entry can contain up to four EAP methods. Each EAP method can contain up to four authentication 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. 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



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 Table 6 to create a Hotspot 2.0 SignUp and Provisioning.

Table 6. SignUp and Provisioning options

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. 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.

Table 6. SignUp and Provisioning options

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 with 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.
OSU NAI Realm	This configuration is only for *External Provision Service*. In case of *Internal Provisioning Service*, the NAI realm should be configured per authentication service, which is available during onboarding.

Table 6. SignUp and Provisioning options

Option	Description
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.**
Online SignUp Certificates	This option should be selected based on the certificate uploaded in the Certificate Store.
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.

Table 6. SignUp and Provisioning options

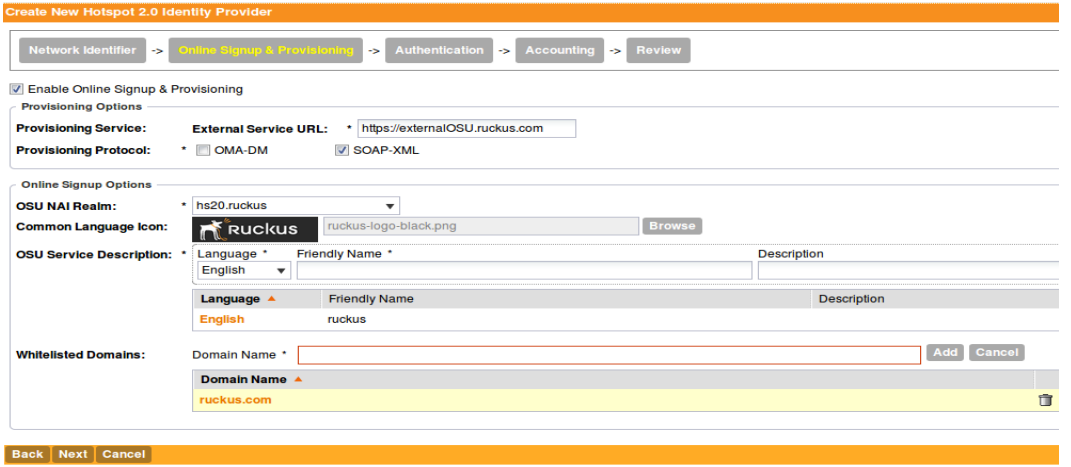
Option	Description
Whitelisted Domain	Administrator needs to add the domains of: • Remediation URL in case it is different from the external provisioning server domain • External Portal domain in case the provisioning server is external Both External Provisioning URL and External Portal URL (in case it is internal provisioning server) will automatically be pushed to AP as whitelisted domains.

4 Click **Next**.

You have completed creating a Hotspot 2.0 Identity Provider SignUp and Provisioning step.

5 Continue to Authentication.

Figure 7. Hotspot Identity Provider - Online SignUp and Provisioning



Authentication

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

1 Click on **Authentication** to configure the service for the identity provider.

2 Configure the settings in Table 7 to create a Hotspot 2.0 SignUp and Provisioning.

Table 7. Authentication options

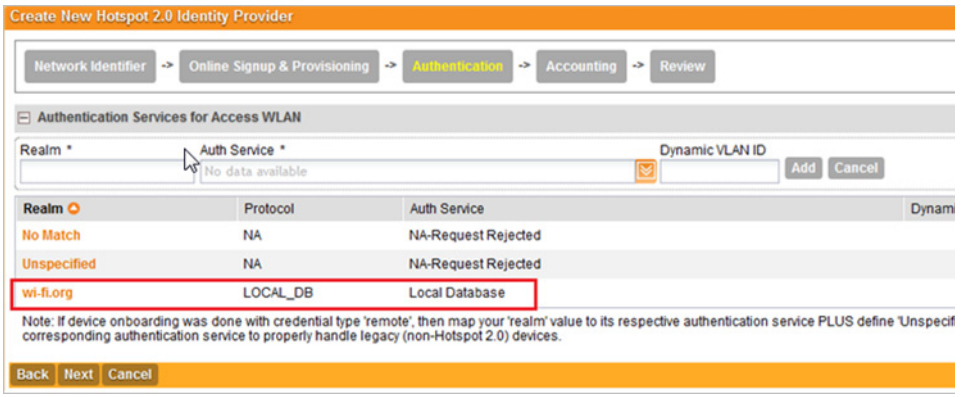
Option	Description
Realm	The administrator should configure the realm mapping to the authentication service. If the provisioned service is internal, meaning *Credential Type* is set to *Local* then the provisioning realm is bound to the Local database. For external provisioned service, meaning *Credential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



Accounting

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

1 Select the **Enable Accounting** check box to enable Accounting and configure the accounting service.

2 Configure the Accounting options in Table 7.

Table 8. Accounting options

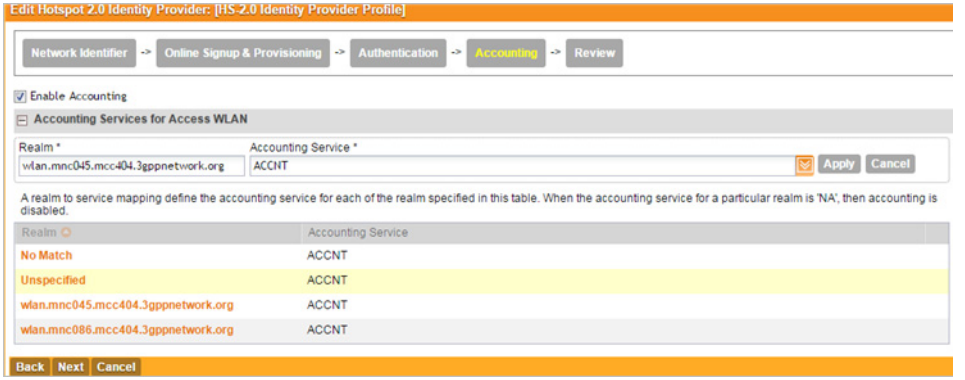
Option	Description
Realm	If the authentication's realm is set as a remote credential type, the administrator should set this realm here to the customer's external accounting server. If the authentication's realm is set as a local credential type, the access accept will include the CUI attribute and its value will be the user name 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 the Hotspot 2.0 Identity Provider - Accounting step.

4 Continue to Review.

Figure 9. Hotspot Identity Provider - Accounting



Review

Follow these steps 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 Hotspot 2.0 secure signup (OSEN) or open onboarding by selecting guest onboarding, and access WLAN which is the Hotspot 2.0 WLAN.

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

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 settings in Table 9 to create a Hotspot 2.0 WLAN profile.

Table 9. WLAN profile configuration options

Option	Description
Name	Enter a name for this WLAN profile. This name identifies the WLAN profile when assigning an HS2.0 service to a HS2.0 WLAN.
Description (Optional)	Enter a description for the WLAN profile.
Operator	Select the operator profile. This name identifies the service operator when assigning an HS2.0 service to a HS2.0 WLAN.
Identify Providers	Choose one or more identity providers. Choose the identity provider. You can configure 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.

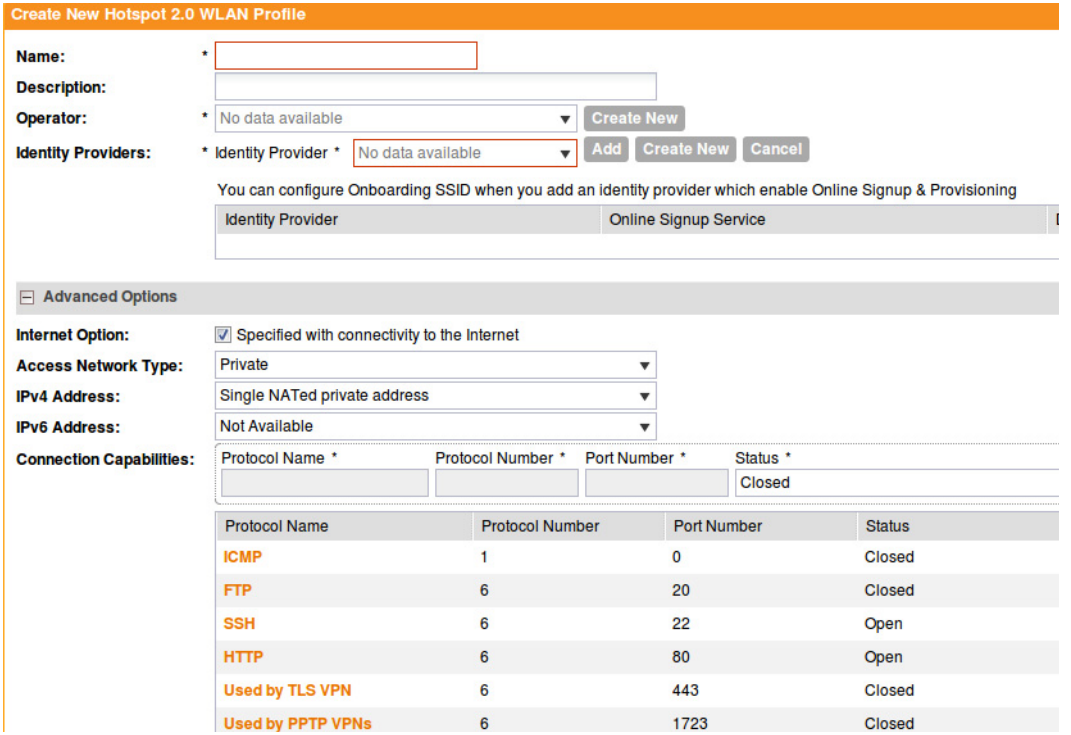
Table 9. WLAN profile configuration options

Option	Description
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 11. Hotspot 2.0 Services Profile



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

Step 6: Define Access WLAN

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

1 Click **Configuration** > **AP Zones > WLAN**.

2 On the *AP Zone List* page, select the AP zone in the WLAN Services & Group page.

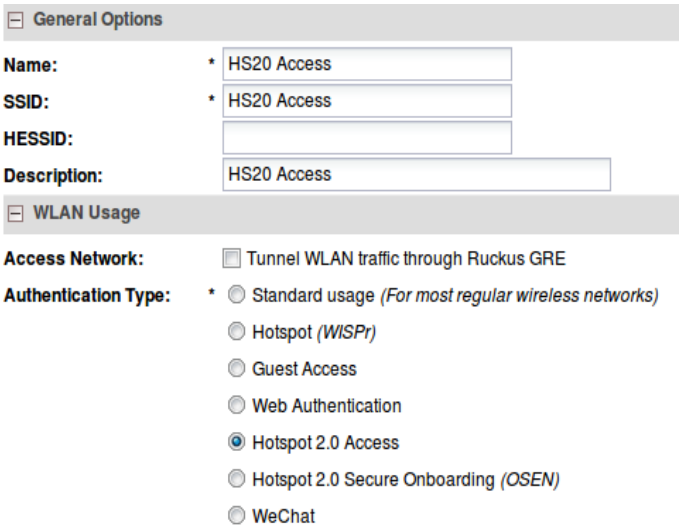
3 Navigate to **WLAN Usage**> **Authentication Type.**

4 Enable Hotspot 2.0.

5 Click **Apply**.

You have completed creating the Hotspot 2.0 authentication type.

Figure 12. Hotspot 2.0 Authentication Type



Step 7: Create Venue Profile

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

1 Click **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 settings in Table 10 to create a Hotspot 2.0 WLAN profile.

Table 10. Venue profile configuration options

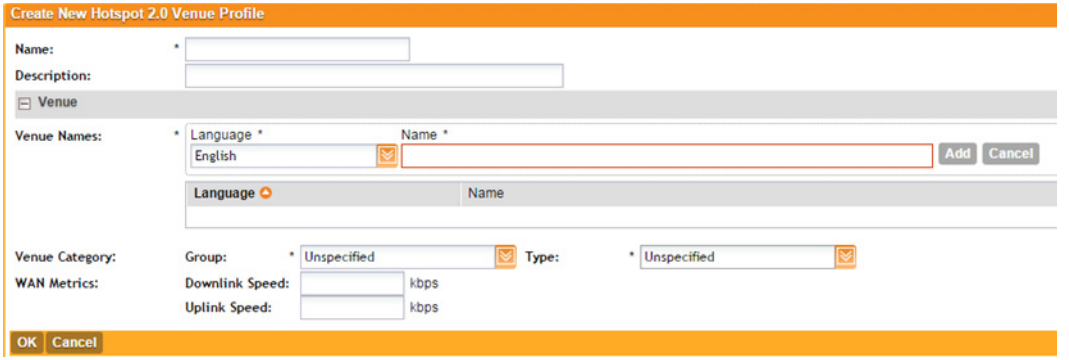
Option	Description
Name	Enter a name for this venue profile. This name identifies the venue profile when assigning an HS2.0 service to a HS2.0 venue.
Description (Optional)	Enter a description for the venue profile.
Venue Options	
Venue Names	Create a new venue name. Select the language and enter the 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 13. Hotspot 2.0 Venue Profile in AP Zone



Adding Venue Profile in AP

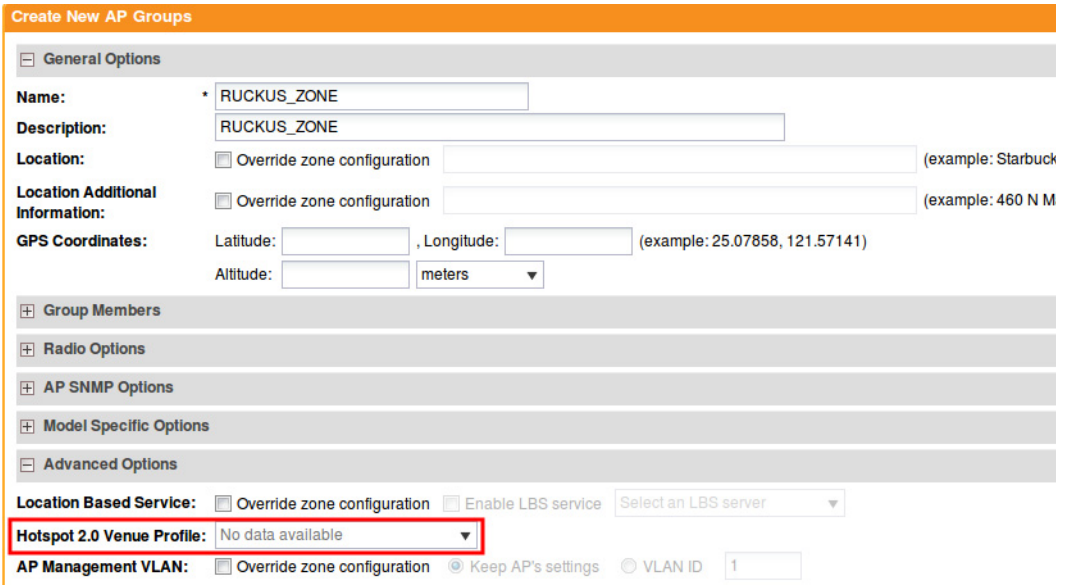
1 Click **Configuration** > **Access Points**.

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 Figure 14.

4 Click **OK**.

Figure 14. Hotspot 2.0 Venue Profile in AP



Adding Venue Profile in AP Group

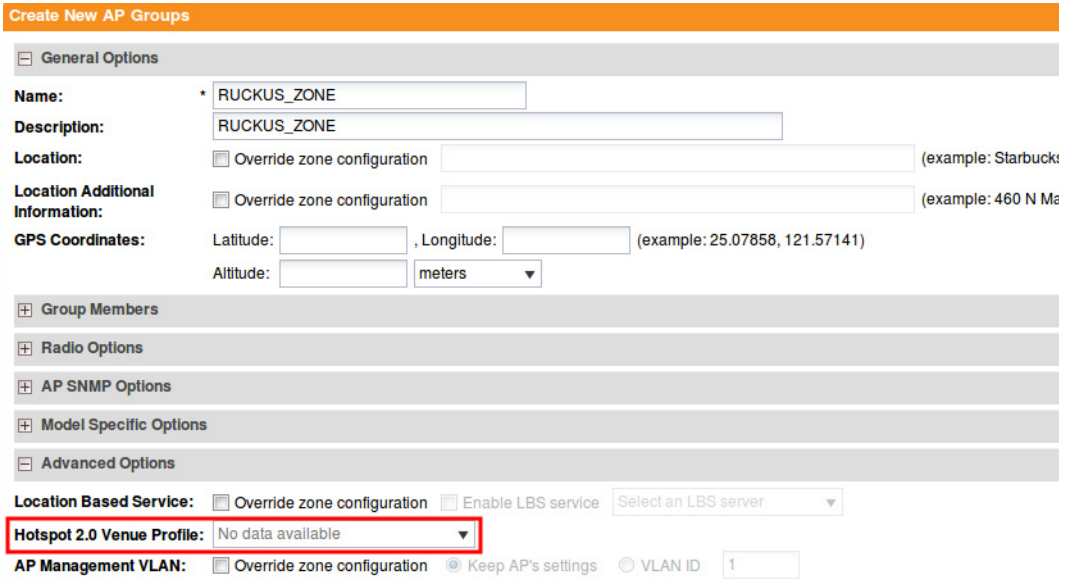
1 Click **Configuration** > **AP Zones > AP Group**.

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 Figure 15.

4 Click **OK**.

Figure 15. Hotspot 2.0 Venue Profile in AP Group



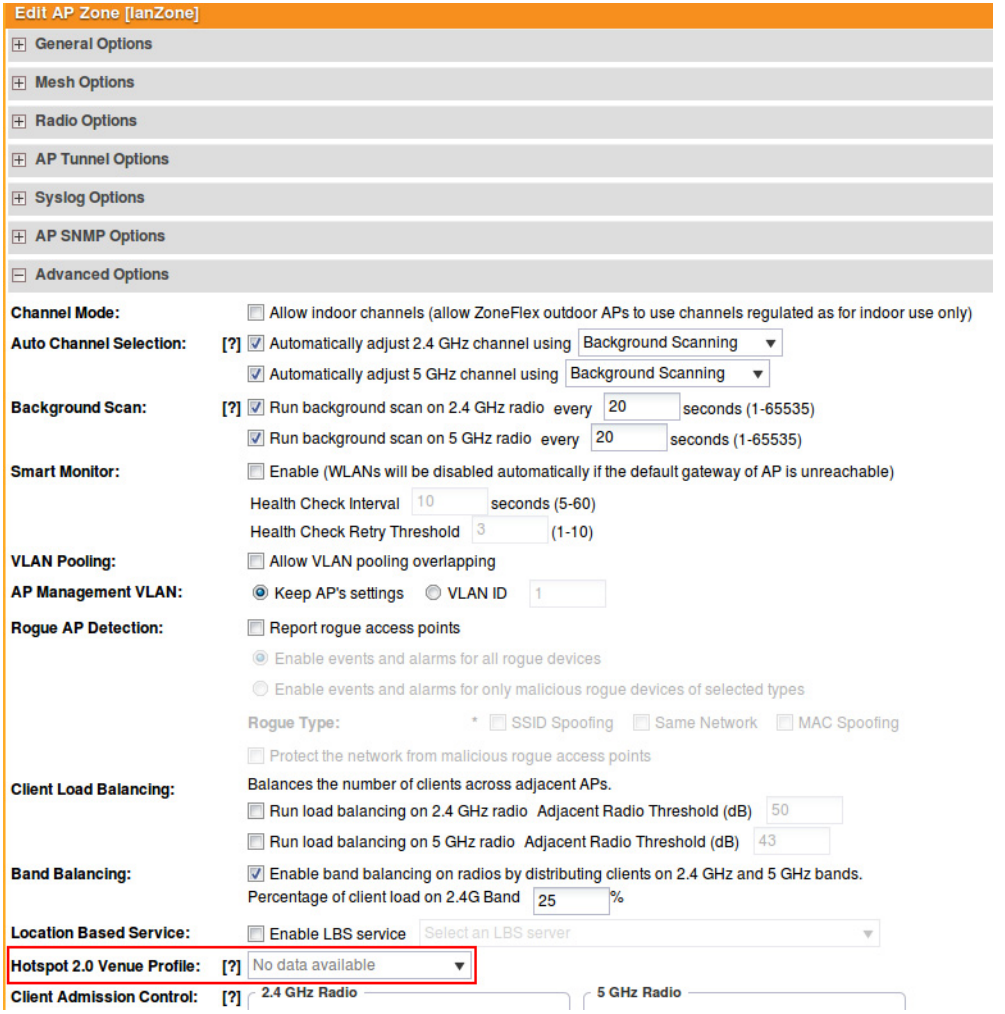
Adding Venue Profile in AP Zone

1 Click **Configuration > AP Zones > Zone Configuration > Edit.**

2 In **Advanced Options > Hotspot 2.0 Venue Profile** set the Hotspot 2.0 venue profile from the drop down list as seen in Figure 16.

3 Click **Apply**.

Figure 16. Hotspot 2.0 Venue Profile in AP Zone



Hotspot 2.0 R2 Device Workflow

3

In this chapter:

- Onboarding Flow
- Access Hotspot 2.0
- De-Auth
- Remediation
- Password Expired
- Update Identifier
- AAA Combinations

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, redirect URI, etc. 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 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). 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.

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 devices 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 in case IDM finds user's expiration has been 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 been 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 user's expiration has been 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.

AAA Combinations

In SmartZone 3.1.1 authentication server includes RADIUS, AD, LDAP, Local database, OAuth. Table 11 lists the available servers in each WLAN type.

Table 11. 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	✅					
Hotspot 2.0	Yes	✅			✅		

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

Configuring Legacy Devices

4

In this chapter:

- Authentication Services

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.

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 settings in Table 12 to create an authentication service.

Table 12. Online SignUp Portal configuration options

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

4 Click **OK**.

External Onboarding and Remediation Portal Integration

A

In this appendix:

- Overview
- Authentication in Onboarding Flow
- Authentication in Remediation Flow
- OAuth 2.0 Authentication

Overview

This appendix provides 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 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, which are referred in this appendix 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?WsgW-
lanId=1&ClientMac=98:0C:82:5E:34:10&Redirec-
tURI=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"
}
}
```

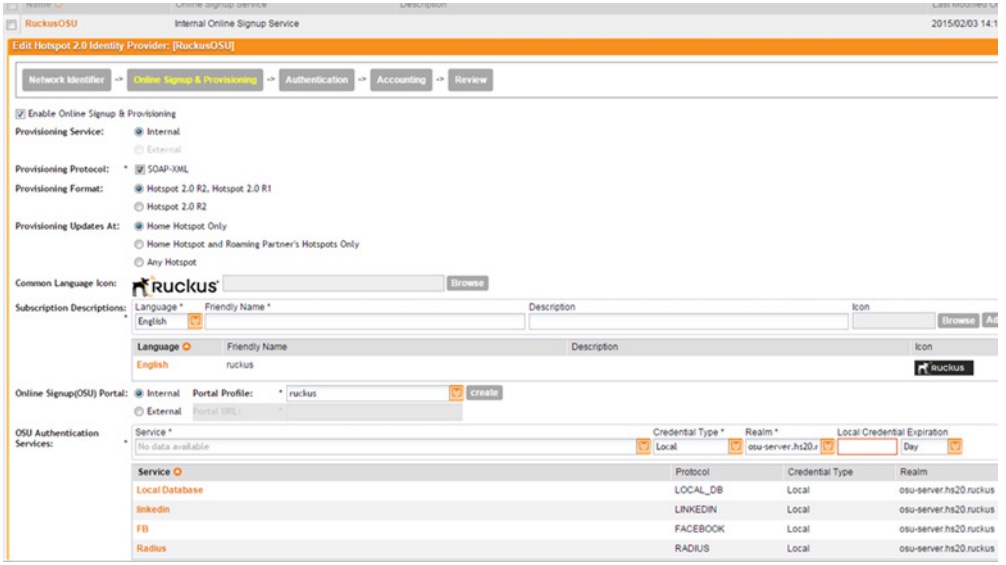
Parameters:

- *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 Figure 17. This configuration is applied to the specific Online Signup & Provisioning in **Configuration > Services&Profiles > Hotspot 2.0 Identity Provider**

Figure 17. Authentication Configuration

Figure 18. Identity Provider Configuration



Authentication in Remediation Flow

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?WsgW-
lanId=1&ClientMac=98:0C:82:5E:34:10&Redirec-
tURI=http://127.0.0.1:1234
&ExternalUsername= testuser1-uid&InternalUsername=
e552a465-1873-4d44@osuserver.hs20.ruckus&AuthServer-
Name=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

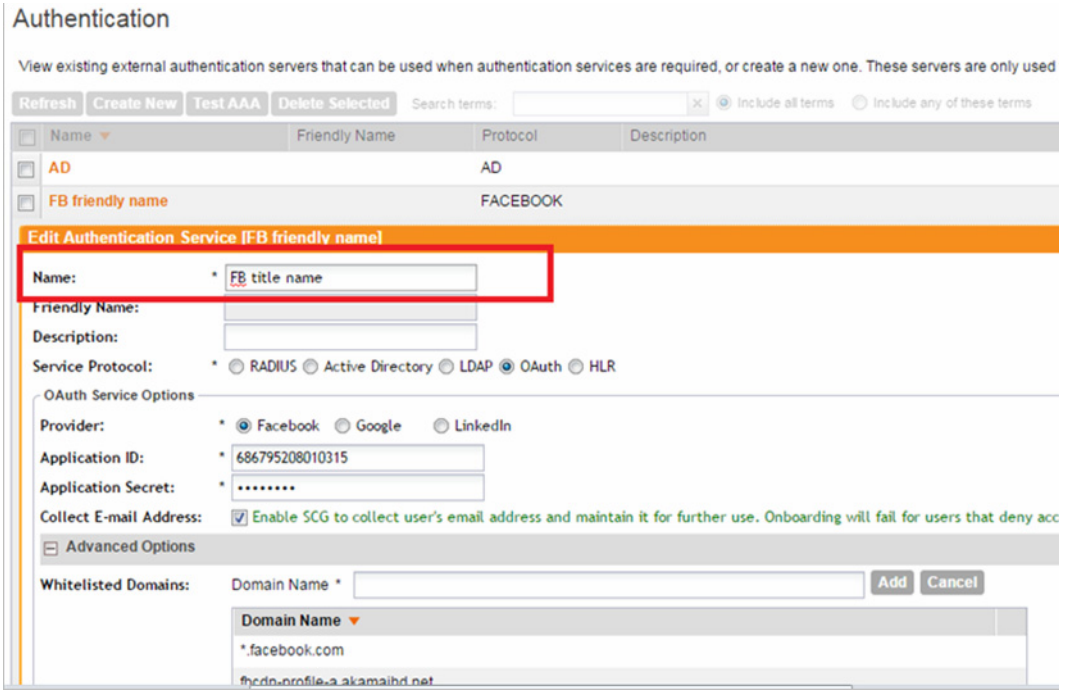
```
{
   "MSG-ID" : ":< Unique ID for the message>,
   "APIVersion" : "1.1",
   "UE-MAC" : <UE MAC>,
   "RequestType" : "ALLOW_BROWSE_OAUTH",
   "RequestCategory" : "UserOnlineControl",
   "OAuth-Provider" : <OAuth type>,
   "Vendor" : "Ruckus",
   "RequestPassword" : <NBI password as set in SCG>
}
```

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 19.

Figure 19. OAuth Provider Configuration



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}&redi-
rect_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" : {
   }
}
```

OCSP Stapling Support in SCG

B

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.
   a. During Anonymous TLS for onboarding call flow as seen in Figure 20
   b. During EAP-TTLS access flow as seen in Figure 21

   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 20. Interaction with OCSP server during Anonymous TLS

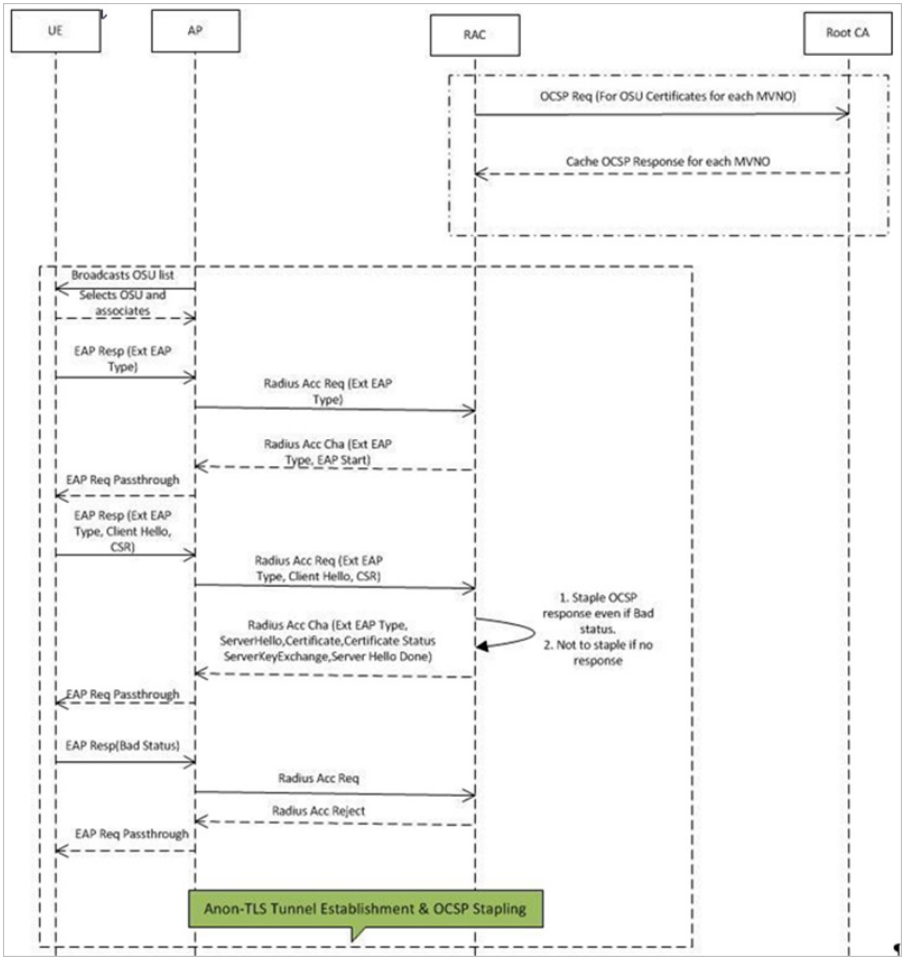


Figure 21. Interaction with OCSP server during EAP-TLS

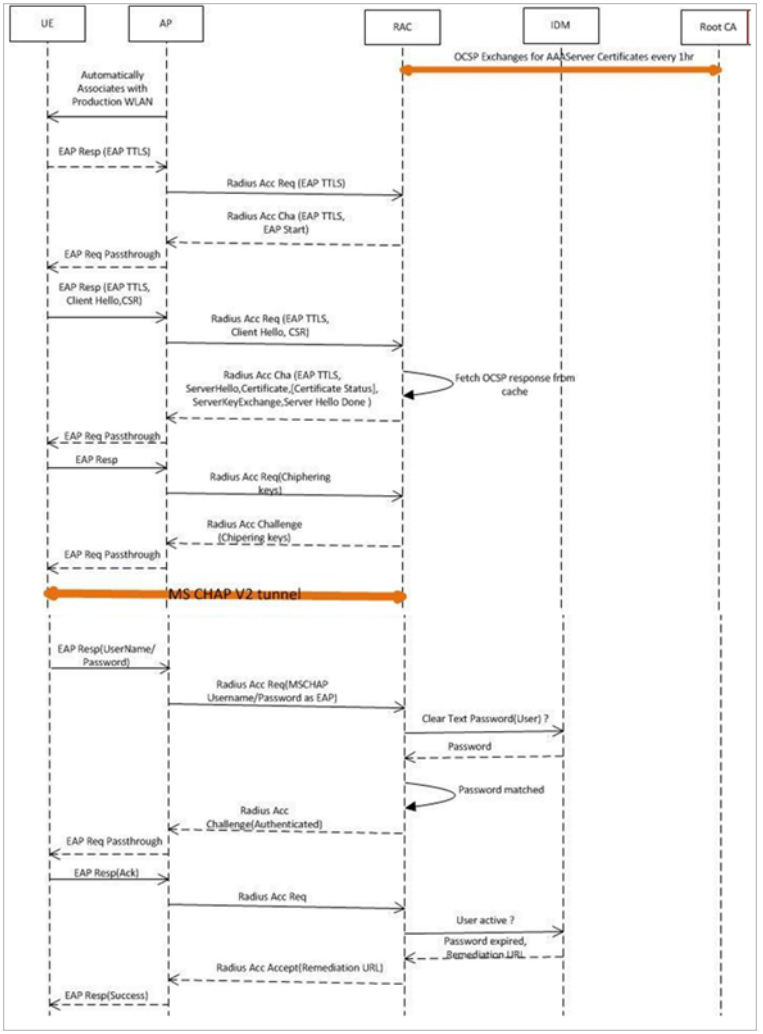


Figure 22 and Figure 23 show the important fields in the OCSP messages. These are standard message, which operators and administrators should be aware of for successful call flows. Possible values of the certificate status field is good, bad or revoked.

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 22. Important OCSP Message

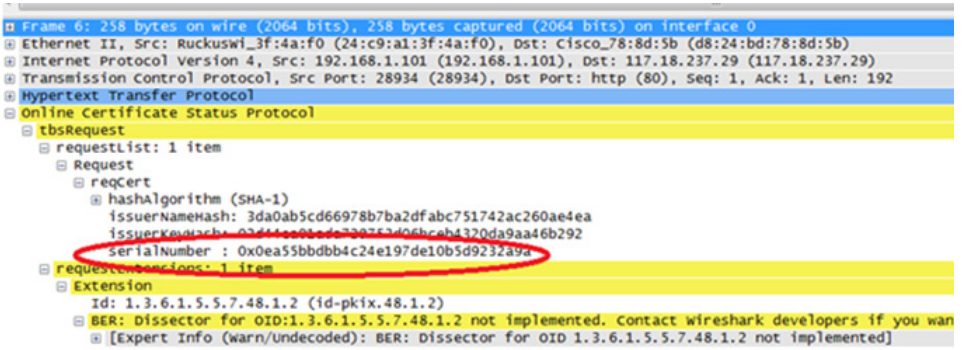


Figure 23. OCSP Response Message

Apple and Samsung Hotspot 2.0 Release 1 (Passpoint) Devices

C

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

Index

A

access network type 31
access points 13
accounting. 28
ap zone 31
authentication 26
authentication server 41, 46
authentication services 48
authentication type 34
authorization status 43

C

certificate 18
certificate store 16
common language icon 24
configured realm 43
connection capability 32
custom connection capability 32

D

de-auth 44
domain names 18

F

friendly name 18, 48

G

group attribute value 48

H

home ols 21
hotspot 2.0 wifi 18
hotspot osen 30

I

identify providers 31
identity providers 20, 43
internet option 31
ip address type 32

L

legacy devices 48

M

mobile device 11

N

network identifier 20

O

onboarding portal 48
online signup and provisioning 23
operator 31
operators 13
osu authentication services 25
osu certificates 25
osu nai realm 24
osu portal 24

P

password 45
physical network 13
plmns 20
provisioning format 24
provisioning protocol 23
provisioning service 23
provisioning updates at 24

R

read password 43
realm 27, 28
realms 21
remediation 44
review 29
root certificate 16

S

server certificate 16
service protocol 48

service providers 13
signup security 18
subscription description 25

U

update identifier 45

V

venue category 35
venue names 35
venue profile 35

W

wan metrics 35
whitelisted domain 26

Copyright © 2006-2016. Ruckus Wireless, Inc.
350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com