



Ruckus Wireless™ SmartZone™ 100

Hotspot 2.0 Reference Guide for RuckOS 3.1

Part Number 800-70902-001 Rev A
Published May 2015

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Copyright 2015. 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	4
Terminology	5
Related Documentation	6
Documentation Feedback	7
Online Training Resources	7

1 Hotspot 2.0 Technology Overview

Brief Overview	9
Basic Operation of Hotspot 2.0	9
Operators and Service Providers	11

2 Configuring Hotspot 2.0

Configuring Wi-Fi Operators	13
Defining the Identity Provider	15
Network Identifier	15
Online Signup and Provisioning	18
Defining the Online Signup Portal Profile	22
OSU Authentication Services	24
Authentication	25
Accounting	26
Review	27
Defining the Hotspot 2.0 WLAN Profile	28
Defining the Hotspot 2.0 Venue Profile	30
Adding a Venue Profile in an AP	31
Adding a Venue Profile in an AP Group	33
Adding a Venue Profile in the AP Common Settings	34

3 Hotspot 2.0 R2 Device Workflow

Onboarding Flow	36
Access Hotspot 2.0	38
De-Auth	39
Remediation	39

Password Expired.	40
Update Identifier	40
AAA Combinations	41
4 Configuring Legacy Devices	
Online Signup Portal Profile.	43
Authentication Services.	44
Guest Access Portal	45
WLAN Guest Access	46
5 Legacy Devices and R1 Onboarding Workflow	
Onboarding Flow	50
Remediation for Legacy and R1 Devices.	55
6 Configuration and Workflow of Hotspot 2.0 for R1 Devices	
Configuring Hotspot 2.0 for R1 Devices	58
Onboarding Flow	59
A External Onboarding and Remediation Portal Integration	
Overview.	61
Authentication in Onboarding Flow	61
Authentication in Remediation Flow.	64
OAuth 2.0 Authentication	65
MAC Encryption.	66
Adding OAuth Provider URL Path to AP ACL	67
Authorization URL and Access Token	69
B OCSP Stapling Support in SZ	
C Apple and Samsung Hotspot 2.0 Release 1 (Passpoint) Devices	
Index	

About This Guide

This *SmartZone™ 100 Hotspot 2.0 Reference Guide* describes the Hotspot 2.0 technology and provides configuration guidelines for enabling Hotspot 2.0 based features on the RuckOS 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 For caveats, limitations, and known issues that you must be aware of before upgrading to this release, refer to 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/documents>.

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 .
<i>italics</i>	Screen or page names	Click Advanced Settings . The <i>Advanced Settings</i> 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
NAI	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.

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:

- Ruckus Wireless SmartCell Gateway 200 Administrator Guide (Release 3.1)
- Part number: 800-70826-001
- Page 88

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>

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 Hotspot 2.0 Release 1 focuses on components a and b, whereas Release 2 goes into specifications of components c and d.

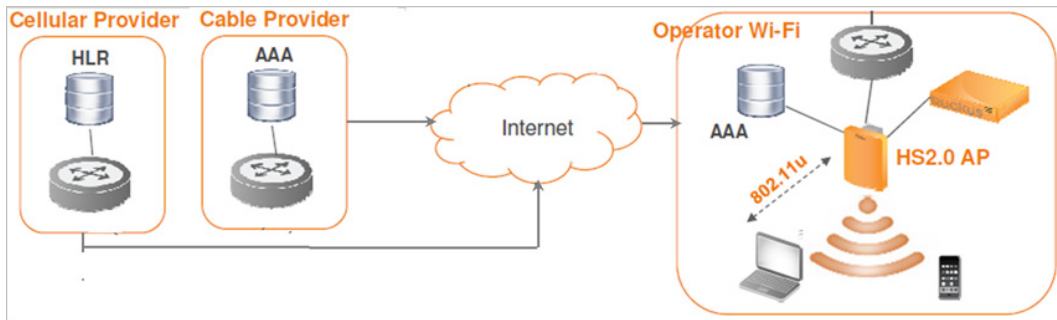
Basic Operation of Hotspot 2.0

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. 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 a Hotspot 2.0 onboarding WLAN. Upon successful authentication, the user will be provisioned with Hotspot 2.0 standards-based management object, known as a Per-Provider Subscription Management object (PPS-MO). The user will then be disconnected from the 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](#).

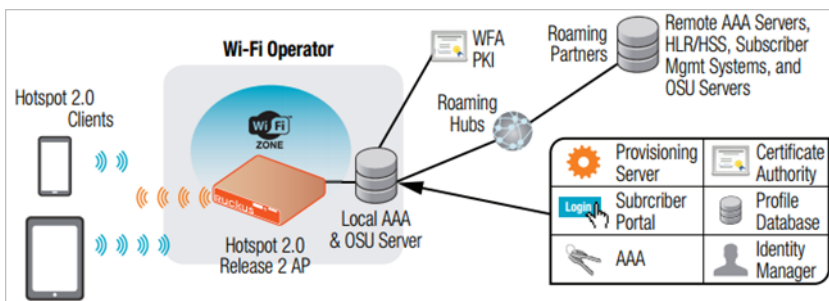
Figure 1. How Hotspot 2.0 works



The onboarding WLAN for Hotspot 2.0 may be an 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, and data usage limit.

In a Hotspot 2.0 based network topology, the entity offering a Wi-Fi infrastructure may be termed as Wi-Fi operator, while the entity owning the 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 [Figure 2](#).

Figure 2. Hotspot 2.0 components



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 Hotspot 2.0 services to a number of service providers. Operators deal mostly with physical network elements, while 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 like a 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:

- [Configuring Wi-Fi Operators](#)
- [Defining the Identity Provider](#)
- [Defining the Online Signup Portal Profile](#)
- [Defining the Hotspot 2.0 WLAN Profile](#)
- [Defining the Hotspot 2.0 Venue Profile](#)

The following are the entities that need to be configured for the Hotspot 2.0 R2 devices configuration flow.

NOTE: Hotspot 2.0 WLANs do not support IPv6.

Configuring Wi-Fi Operators

Follow these steps to configure Wi-Fi operators.

- 1 Click **Configuration > Hotspot 2.0 > Wi-Fi Operators**.
- 2 The *Hotspot 2.0 Wi-Fi Operator* 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). Select the display language from the drop down list.

NOTE In the 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**.

Figure 3. .Hotspot Wi-Fi Operator Profile

Hotspot 2.0 Wi-Fi Operator

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

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

Name	Description

Create New Hotspot 2.0 Wi-Fi Operator Profile

Name: *

Description:

Domain Names: * Domain Name * Add Cancel

Domain Name
wi-fi.org

Signup Security: ☒ Support Anonymous Authentication (OSEN)

Certificate: *

Friendly Names: * Language * Name * Add Cancel

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

OK Cancel

Defining the Identity Provider

The 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.

The 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 > Identity Providers**.
- 2 The *Hotspot 2.0 Identity Provider* 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.

Table 5. Network Identifier options

Option	Description
PLMNs	<p>Each record contains MCC and MNC.</p> <ul style="list-style-type: none"> • 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	<p>List of NAI realms corresponding to service providers or other entities whose networks or services are accessible via this AP. Up to 16 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.</p>
Home Ols	<p>Organization Identifier (OI) is a unique value assigned to the organization. User can configure a maximum of 12 OI values and can adjust the order since the AP takes only 3 OIs in the beacon.</p>

4 Click **Next**.

You have completed creating a Hotspot 2.0 Identity Provider - Network Identifier.

5 Continue to [Online Signup and Provisioning](#).

Figure 4. Hotspot Identity Provider - Network Identifier

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

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

Name: * HS-2.0 Identity Provider Profile

Description: HS-2.0 Identity Provider Profile

PLMNs:

MCC * MNC *

Add Cancel

MCC	MNC
404	86
404	45

Realms:

Name: * Encoding: * RFC-4282

EAP Methods:

#1 #2 #3 #4

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 * Organization ID *

5 Hex

Add Cancel

Name	Length	Organization ID
------	--------	-----------------

Next Cancel

Online Signup and Provisioning

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

- 1 Click to enable **Online Signup & Provisioning** after **Network Identifier** to configure the service for the identity provider.
Alternatively, you can skip this step to move to [Authentication](#)
- 2 Select the check box to enable Online Signup & Provisioning. Configure the settings in [Table 6](#) to set the Hotspot 2.0 Signup and Provisioning options.

Table 6. Signup and Provisioning options

Option	Description
Provisioning Service	<p>The provisioning service is responsible for any subscription provisioning process in which messages are communicated between the UE and the SZ 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.</p> <p>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.</p> <p>Administrator can select <i>Internal Provisioning Service</i> or <i>External</i>. By default it is internal, meaning SZ's online signup service provides this capability. In case external is selected, the administrator is required to fill the external OSU server URL.</p> <p>In this release only username/password credential are supported to be provisioned using SZ's Internal OSU. Policy and subscription parameters in the PPS-MO are not supported using SZ's internal OSU.</p> <p>Note: There can be only one identity provider configured for internal provisioning service.</p>
Provisioning Protocol	<p>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.</p>

Table 6. Signup and Provisioning options

Option	Description
Provisioning Format	<p>This options allows the administrator to choose:</p> <ul style="list-style-type: none"> Hotspot 2.0 R2, Hotspot 2.0 R1 - in case the Release 1 device is doing the onboarding the configuration file downloaded should be a Release 1 configuration file. Hotspot 2.0 Release2. <p>Note: This option is available when the provisioning service is internal.</p>
Provisioning Updates At	<p>This option is available when the provisioning service is internal. Select the provisioning updates to be sent to the user:</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> 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	<p>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.</p>
OSU Portal	<p>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.</p>
OSU NAI Realm	<p>This configuration is only for <i>External Provision Service</i>. In case of <i>Internal Provisioning Service</i>, the NAI realm should be configured per authentication service, which is available during onboarding.</p>

Table 6. Signup and Provisioning options

Option	Description
OSU Authentication Services	<p>The administrator can select the authentication services the user is able to choose for onboarding.</p> <p>Local means that SZ's identity management generates local random credentials and the OSU provisions it to the device.</p> <p>Remote means that same credentials used for onboarding with external RADIUS is provisioned to the device.</p> <p>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.</p> <p>Additional attribute per selected authentication service is <i>Local Credential Expiration</i> available (only if the <i>Local Credential</i> 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.</p> <p>This configuration is available in Configuration > Services & Profiles > Services > Authentication.</p> <p>Note: For further details see: OSU Authentication Services</p>
Online Signup Certificates	<p>This option should be selected based on the certificate uploaded in the Certificate Store.</p>
Subscription Description	<p>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.</p> <p>Administrators are required to set the matched icon per language as included in the OSU certificate.</p>

Table 6. Signup and Provisioning options

Option	Description
Whitelisted Domain	<p>Administrator needs to add the domains of:</p> <ul style="list-style-type: none"> Remediation URL in case it is different from the external provisioning server domain External Portal domain in case the provisioning server is external <p>Both External Provisioning URL and External Portal URL (in case it is internal provisioning server) will automatically be pushed to AP as whitelisted domains.</p>

3 Click **Next**.

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

4 Continue to [Authentication](#).

5 Refer to [Defining the Online Signup Portal Profile](#) to define the look and feel of the Online Signup Portal.

Figure 5. Hotspot Identity Provider - Online Signup and Provisioning

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

Online Signup(OSU) Portal: ☒ Internal Portal Profiles: * Onboarding Portal confid ☐ External Portal URL: *

Service *	Credential Type *	Realm *	Local Credential Expiration
No data available	Local	wifi.org	Day

Service	Protocol	Credential Type	Realm
radius	RADIUS	Local	wifi.org

Online Signup Certificates: * wifi-server certificate

Common Language Icons: * icon_orange_zoo.png

Subscription Descriptions: Language *	Friendly Name *	Description	Icon
English			

Defining the Online Signup Portal Profile

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

- 1 Click **Configuration > Hotspot 2.0 > Online Signup Portal Profile**.
- 2 The *Hotspot 2.0 Online Signup Portal Profile* page appears. Click **Create New**.
- 3 Configure the settings in [Table 7](#) to create a Hotspot 2.0 OSU portal profile.

Table 7. Online Signup Portal Profile configuration options

Option	Description
Portal Name	Enter the portal name.

Table 7. Online Signup Portal Profile configuration options

Option	Description
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	Enter the portal title as seen by the user.
Portal Logo	Choose the logo as seen by the user.
Terms and Conditions	Enter the terms and conditions that a user will accept on OSU. Note: Portal title and T&C will NOT be presented in the selected language but in the same language as written in the Title and T&C text boxes.

4 Click **OK**.

You have completed creating a Hotspot 2.0 online signup portal profile.

Figure 6. 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.

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


Name	Description

Create New Online Signup Portal Profile

Portal Name: *

Portal Description:

☐ Portal Settings

Portal Language: * 

Portal Title: *

Portal Logo: [?]

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.

OSU Authentication Services

In case the credential type is set to *Remote*, for successful authentication in the HS2.0 access SSID, customer needs to ensure:

- To use the OSU server certificate as the external AAA server certificate deployed on the external AAA server.

OR

- In case OSU and AAA server certificates are different ensure that the:
 - AAA trust root in the external AAA server is same as the OSU server trust root
 - AAA server certificate has SAN value, which matches the rule of FQDN in the PPS-MO (taken from the common name of the OSU server certificate) is at least the suffix of one of the SAN in the AAA server certificate.

In case the credential type is set to *Remote*, RuckOS OSU server does not support any remediation flows, which are elaborated in [Hotspot 2.0 R2 Device Workflow](#).

Authentication

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

- 1 Click on **Configuration > AAA Servers > Proxy AAA > Authentication** to configure the service for the identity provider.
- 2 Configure the settings in [Table 8](#) to set the Hotspot 2.0 Signup and Provisioning Authentication options.

Table 8. Authentication options

Option	Description
Realm	<p>The administrator should configure the realm mapping to the authentication service. If the provisioned service is internal, meaning <i>Credential Type</i> is set to <i>Local</i> then the provisioning realm is bound to the Local database.</p> <p>For external provisioned service, meaning <i>Credential Type</i> is set to <i>Remote</i>, the administrator should map the realm to an external RADIUS server which should be preconfigured in Configuration > Authentication.</p> <p>The default EAP method which the SZ responds to is EAP-TTLS. In case the client is using other EAP methods (for example EAP-PEAP in legacy on-board devices) the SZ falls back to the required EAP method.</p>

- 3 Click **Next**.

You have completed creating a Hotspot 2.0 Identity Provider - Authentication step.

- 4 Continue to [Accounting](#).

Figure 7. Hotspot Identity Provider - Authentication

Create New Hotspot 2.0 Identity Provider

Network Identifier → Online Signup & Provisioning → **Authentication** → Accounting → Review

Authentication Services for Access WLAN

Realm * Auth Service * Dynamic VLAN ID

No data available Add Cancel

Realm	Protocol	Auth Service	Dynam
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 'Unspecif' corresponding authentication service to properly handle legacy (non-Hotspot 2.0) devices.

Back Next Cancel

Accounting

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

- 1 Click to enable **Accounting** and configure the accounting service.
- 2 Select the Enable Accounting check box to configure the settings in [Table 8](#) and create Hotspot 2.0 Accounting.

Table 9. Accounting options

Option	Description
Realm	<p>In case the authentication's realm is set as remote credential type, administrator should set this realm here to the customer's external accounting server.</p> <p>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 user name which the user used for onboarding. This way, even if the access authentication is done with the SZ's local database, accounting can still be proxy to the external accounting server based on CUI value. The SZ's local database does not support accounting.</p> <p>The actual external accounting server should be preconfigured in Configuration > Services & Profiles > Services > Accounting.</p>

- 3 Click **Next**.

You have completed creating a Hotspot 2.0 Identity Provider - Accounting step.

4 Continue to [Review](#).

Figure 8. Hotspot Identity Provider - Accounting

Enable Accounting

Accounting Services for Access WLAN

Realm * Accounting Service *

wlan.mnc045.mcc404.3gppnetwork.org 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

Back Next Cancel

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 SZ web interface back to the corresponding section.
- 2 Click **Submit** to create the Hotspot 2.0 Identity Provider.

Defining the Hotspot 2.0 WLAN Profile

Follow these steps to create a Hotspot 2.0 WLAN profile.

- 1 Click **Configuration > Hotspot 2.0 > Hotspot 2.0 WLAN Profiles**.
- 2 In the *Hotspot 2.0 WLAN Profiles* section, click **Create New**.
- 3 Configure the settings in [Table 10](#) to create a Hotspot 2.0 WLAN profile.

Table 10. 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	<p>Choose one or more identity providers. Choose the identity provider. You can configure an OSU SSID when you add an <i>Identity Provider</i> 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 <i>No Match</i> and <i>Unspecified</i> mapping could be duplicated. To avoid duplication, the default identity provider is taken as the correct configuration for <i>No Match</i> and <i>Unspecified</i> mapping. OSUSSID can be OSEN or OPEN [Guest].</p> <p>Note: To create a new identity provider refer to Defining the Identity Provider</p>
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.

Table 10. WLAN profile configuration options

Option	Description
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.

4 Click **OK**.

You have completed creating a Hotspot 2.0 services profile.

Figure 9. Hotspot 2.0 Services Profile

Create New Hotspot 2.0 WLAN Profile

Name: *

Description:

Operator: * No data available create

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

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 *
FTP	6	20	Closed

Apply Cancel

Protocol Name	Protocol Number	Port Number	Status
ICMP	1	0	Closed
FTP	6	20	Closed
SSH	6	22	Closed
HTTP	6	80	Closed

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

Defining the Hotspot 2.0 Venue Profile

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

- 1 Click **Configuration > Hotspot 2.0 > Hotspot 2.0 Venue Profiles**.
- 2 In the *Hotspot 2.0 Venue Profiles* section, click **Create New**.
- 3 Configure the settings in [Table 11](#) to create a Hotspot 2.0 Venue profile.

Table 11. 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

- 4 Click **OK**.

You have completed creating a Hotspot 2.0 venue profile.

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 10. Hotspot 2.0 Venue Profile

Create New Hotspot 2.0 Venue Profile

Name: *

Description:

☐ Venue

Venue Names: *

Language *	Name *
English	<input type="text"/>

Language	Name
----------	------

Venue Category: Group: * Type: *

WAN Metrics: Downlink Speed: kbps
Uplink Speed: kbps

Adding a Venue Profile in an AP

- 1 Click **Configuration** > **Access Points** > **APs**.
- 2 Click to select one of the APs. 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 11](#).
- 4 Click **OK**.

Figure 11. Hotspot 2.0 Venue Profile in the AP

Edit AP: [84:18:3A:21:08:70]

AP Configuration | Swap Configuration

General Options

AP Name: * RuckusAP

Description:

Location: * ☐ Override zone config (example: Starbucks)

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

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

Country Code: United States

User Location Information (ULI): Area Code: [255] , Cell Identifier: []

AP Admin Logon: ☐ Override zone configuration Logon ID: Password:

Radio Options

Radio Options b/g/n (2.4GHz)

Channelization: ☐ Override zone configuration Auto

Channel: ☐ Override zone configuration Auto

TX Power Adjustment: ☐ Override zone configuration Full

WLAN Group: ☐ Override zone configuration default

WLAN Service: ☒ Enable the WLAN service on this radio

Advanced Options

Network Settings: IP Settings: * ☐ Static ☐ Dynamic ☒ Keep the AP's settings

Device IP Mode: * ☒ IPv4 only ☐ IPv6 only

Smart Monitor: ☐ Override zone configuration ☐ Enable (WLANs will be disabled automatically if the default gateway of AP is unreachable)

Syslog Options: ☐ Override zone configuration ☐ Enable external syslog server

Bonjour Gateway: ☐ Enable to broadcast gateway with Bonjour No data available

Hotspot 2.0 Venue Profile: No data available

Client Admission Control: ☐ Override zone configuration [?] 2.4GHz Radio

Adding a Venue Profile in an AP Group

- 1 Click **Configuration > Access Points > APs > AP Groups**.
- 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 12](#).
- 4 Click **OK**.

Figure 12. Hotspot 2.0 Venue Profile section on the AP Group page

The screenshot shows the 'Edit AP: [84:18:3A:21:08:70]' configuration page. The 'General Options' tab is active, showing fields for AP Name, Description, Location, and GPS Coordinates. The 'Radio Options' tab is also visible, showing settings for Channelization, Channel, TX Power Adjustment, WLAN Group, and WLAN Service. The 'Advanced Options' tab is selected, showing network settings, smart monitor, syslog options, and the Hotspot 2.0 Venue Profile section. The 'Hotspot 2.0 Venue Profile' dropdown is highlighted with a red box, showing 'No data available' as the selected option. Below it, the 'Client Admission Control' section is visible, with a checkbox for 'Override zone configuration' and a radio button for '2.4GHz Radio'.

AP Configuration Swap Configuration

General Options

AP Name: * RuckusAP

Description:

Location: * ☐ Override zone config (example: Starbucks)

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

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

Country Code: United States

User Location Information (ULI): Area Code: 255 Cell Identifier: 1

AP Admin Login: ☐ Override zone configuration Login ID: Password:

Radio Options

Radio Options begin (2.4GHz)

Channelization: ☐ Override zone configuration Auto

Channel: ☐ Override zone configuration Auto

TX Power Adjustment: ☐ Override zone configuration Full

WLAN Group: ☐ Override zone configuration default

WLAN Service: ☒ Enable the WLAN service on this radio

Advanced Options

Network Settings: IP Settings: * Static Dynamic Keep the AP's settings

Device IP Mode: * IPv4 only IPv6 only

Smart Monitor: ☐ Override zone configuration ☐ Enable (WLANs will be disabled automatically if the default gateway of AP is unreachable)

Syslog Options: ☐ Override zone configuration ☐ Enable external syslog server

Hotspot 2.0 Venue Profile: No data available

Client Admission Control: ☐ Override zone configuration

[?] 2.4GHz Radio

Adding a Venue Profile in the AP Common Settings

- 1 Click **Configuration > Access Points > Common Settings**.
- 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 [Figure 13](#).
- 3 Click **Apply**.

Figure 13. Hotspot 2.0 Venue Profile in Common Settings

The screenshot displays the 'Common Settings' page for Access Points in RuckOS. The left sidebar shows the navigation menu with 'Common Settings' highlighted. The main content area is titled 'Common Settings' and contains several sections: General Options, Mesh Options, Radio Options, Syslog Options, and Advanced Options. The 'Advanced Options' section is expanded, showing various configuration options. The 'Hotspot 2.0 Venue Profile' is set to 'No data available'. The 'Client Admission Control' is set to '2-WIRE RADIO'.

Configuration >> Common Settings

Wireless Network

WLANs

Access Points

Common Settings

APs

Model Based Settings

AP Tunnel Settings

Critical AP Rules

Access Control

Guest Access

Web Authentication

Hotspot (WISPr)

Hotspot 2.0

AAA Servers

Location Services

Bonjour Gateway Policies

Forwarding Service

Identity

SmartZone System

Common Settings

These configuration applies to all access points unless they are modified at the AP group level or AP level.

Refresh

General Options

Mesh Options

Radio Options

Syslog Options

Advanced Options

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

Auto Channel Selection: [?] ☒ Automatically adjust 2.4GHz channel using Background Scanning

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 Location LBS server

Hotspot 2.0 Venue Profile: [?] No data available

Client Admission Control: [?] 2-WIRE RADIO 5GHz Radio

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 SZ, handled by the RAC module. Anonymous TLS is between UE and SZ. 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 SZ 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). In case of SZ'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 SCG 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 SCG 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 SZ has in its configuration group attribute mapping to the SZ 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 **Configuration > Identity Providers > Network Identifier > Authentication > Accounting > Review configuration**).

At this point the UE disconnects from the on-boarding 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], and SSID of on-boarding.

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 SZ'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 SZ'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 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 Online Signup & Provisioning. The 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 the 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 user name 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 an access rejection is sent back to UE.
- 2 Authorization Status - RAC sends the user name again and the IDM tries to authorize 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 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 user name 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 user name which the user used for on-boarding.

De-Auth

De-Auth occurs when the IDM detects that a user session has expired. The IDM sends a special response to RAC and the RAC responds to the access accept with the new De-Auth attribute, which includes the De-Auth URL. This indicates that the UE has not yet been 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 SZs portal, which displays the message that the user is disabled.

Remediation

If the IDM finds the user's session 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*, RuckOS OSU server does not support any remediation flows, as elaborated in this section.

Password Expired

In case the IDM finds that the user session has expired, the OSU server redirects the UE to a specific path into the SZ portal.

In case the original on-boarding authentication server is not an OAuth provider, the portal presents the regular user name and password page, with the user name already prepopulated. The user would need to provide the password used during on-boarding. The portal sends the authentication request to the IDM similar to the on-boarding process.

In case the original on-boarding 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 on-boarding. 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, it generates an updated PPS-MO with the updated identifier. It responds to the UE, which initiates the new access request along with the new updated PPS-MO information.

AAA Combinations

In RuckOS 3.1, authentication server includes RADIUS, AD, LDAP, local database, and OAuth. [Table 12](#) lists the available servers in each WLAN type.

Table 12. AAA Combinations

WLAN Type	Enable Proxy to SZ	RADIUS	AD	LDAP	Local Database	Always Accept	OAuth
802.1X	No	✓			✓ when proxy to SZ is enabled.		
	Yes	✓					
MAC Auth	No	✓					
	Yes	✓					
Hotspot (WISPr)	Yes	✓			✓	✓	
Guest Access	Yes				✓	✓	
On-boarding	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:

- [Online Signup Portal Profile](#)
- [Authentication Services](#)
- [Guest Access Portal](#)
- [WLAN Guest Access](#)

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

- The onboarding portal is hosted at the SZ instead of at the AP.
- New authentication service configuration. In addition to RADIUS, AD, and LDAP users can on-board using the local database credential and their personal Facebook or Google+ or LinkedIn account.
- Group attribute mapping to user role has been updated.

Online Signup Portal Profile

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

- 1 Click **Configuration > Hotspot 2.0 > Online Signup Portal**.
- 2 The *Hotspot 2.0 Online Signup Portal* page appears. Click **Create New**.
- 3 Configure the settings in [Table 13](#) to create a Hotspot 2.0 OSU portal profile.

Table 13. Online Signup Portal configuration options

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 14. 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.

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

Name	Description

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 Browse

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.

OK Cancel

Authentication Services

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

- 1 Click **Configuration > AAA Servers > Proxy AAA**.
- 2 The *Authentication Service* page appears. Click **Create New**.

3 Configure the settings in [Table 13](#) to create an authentication service.

Table 14. Authentication service 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 SZ uses it map the <i>User Role</i> (with all its attributes) to the user entity.

4 Click **OK**.

Guest Access Portal

Users with legacy devices will have to manually select the on-board WLAN, the administrator will need to configure the guest access profile on the SZ to facilitate the SZ on-board in **WLAN > Guest Access**. 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 > 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 the guest access portal window.

Figure 15. 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

Apply **Cancel**

WLAN Guest Access

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

- 1 Click **Configuration > WLANs**.
- 2 On the *WLAN Groups* page, select the WLAN List and select the specific WLAN.
- 3 In **WLAN Configuration > WLAN Usage** to enable Guest Access + Hotspot 2.0 Online Signup.
- 4 In the **Online Signup/Onboarding Service** to enable **Hotspot 2.0 Online Signup** and the **Zero-IT On-boarding** options.
 - 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 on-boarding. Define:
 - i. Service - Option to choose all authentication services (Local database RADIUS, LDAP, AD and OAuth)
 - ii. Credential Type - Local -All authentication types are available for this selection. After successful on-boarding authentication using the credentials the user provides in the on-boarding portal, IDM generates new

credentials for this user which is used in the Zero-IT configuration file. The user name 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.

- iii. 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 on-boarding 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.

- iv. 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 16. 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

☒ Send interim update every 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:

Authentication Services

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

Add

Cancel

Service	Protocol	Credential Type	Realm	Local Credential Expiration
---------	----------	-----------------	-------	-----------------------------

Legacy Devices and R1 Onboarding Workflow

5

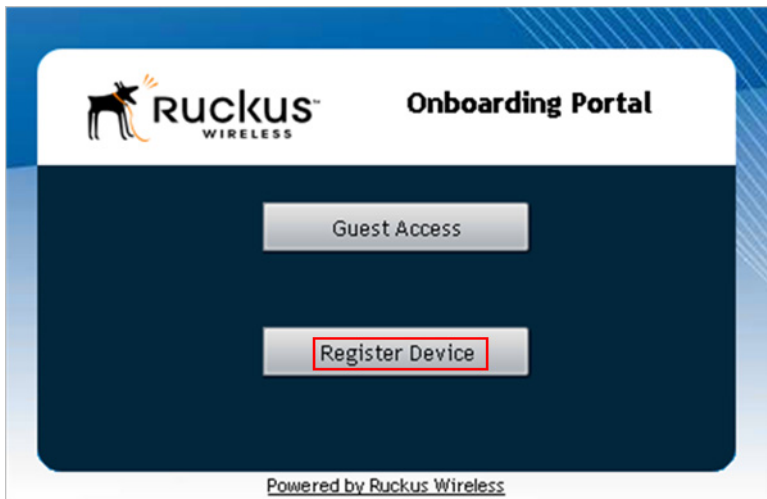
In this chapter:

- [Onboarding Flow](#)
- [Remediation for Legacy and R1 Devices](#)

Onboarding Flow

Users with legacy devices will have to manually select the onboarding SSID. The user will need to open a browser and initiate a connection to a remote website in order to be redirected to the onboarding portal. While attempting to browse, the AP portal is displayed (as seen in [Figure 17](#)). For onboarding, the user is required to click the *Register Device* option, which navigates to the SZ portal (as seen in [Figure 18](#)).

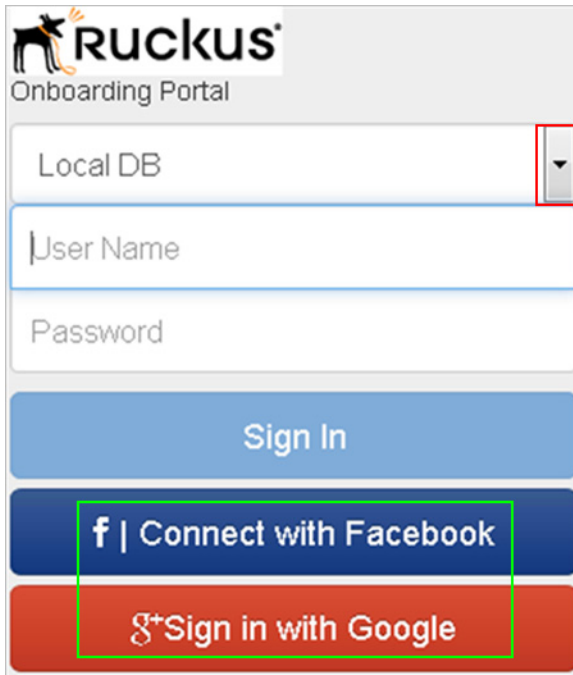
Figure 17. AP Onboarding Portal



For redirecting, AP uses the following process:

- If the OSU server certificate is uploaded, AP will redirect to the FQDN of the OSU server certificate
- If OSU server is not configured, AP will redirect to the FQDN of the hotspot interface certificate. In case the common name of the hotspot certificate includes '*', AP will replace it with the SZ cluster name.
- In case hotspot certificate is not configured, AP will redirect to the SZ's self-signed certificate FQDN.

Figure 18. SZ Portal for User Login with Local Database



The screenshot shows the Ruckus Onboarding Portal. At the top is the Ruckus logo and the text 'Onboarding Portal'. Below this is a dropdown menu labeled 'Local DB' with a downward arrow icon. Underneath the dropdown are two input fields: 'User Name' and 'Password'. Below the input fields is a blue 'Sign In' button. At the bottom are two social login buttons: 'f | Connect with Facebook' and 'g+ Sign in with Google'. A red box highlights the 'Local DB' dropdown menu, and a green box highlights the social login buttons.

The authentication services (in the drop-down list) is taken from the Zero-IT onboarding configuration (refer to [WLAN Guest Access](#)) and is listed in the list box. If Facebook or Google+ or Linked-In is included, the SZ portal will include their corresponding icons ([Figure 18](#)). The SZ OSU portal look and feel will differ based on the following configuration options.

- In case only one non OAuth authentication service is selected in the on-boarding WLAN (or in the Identity Provider configuration), the drop down list will not be present at all.
- In case only OAuth providers are selected in the on-boarding WLAN (or in the Identity Provider configuration), only their icons will be presented and the user credentials (login name and password) will be hidden.
- In case non OAuth provider is selected (usage of user credentials) for authentication, the user provides his user name and password and selects the Sign-in button.

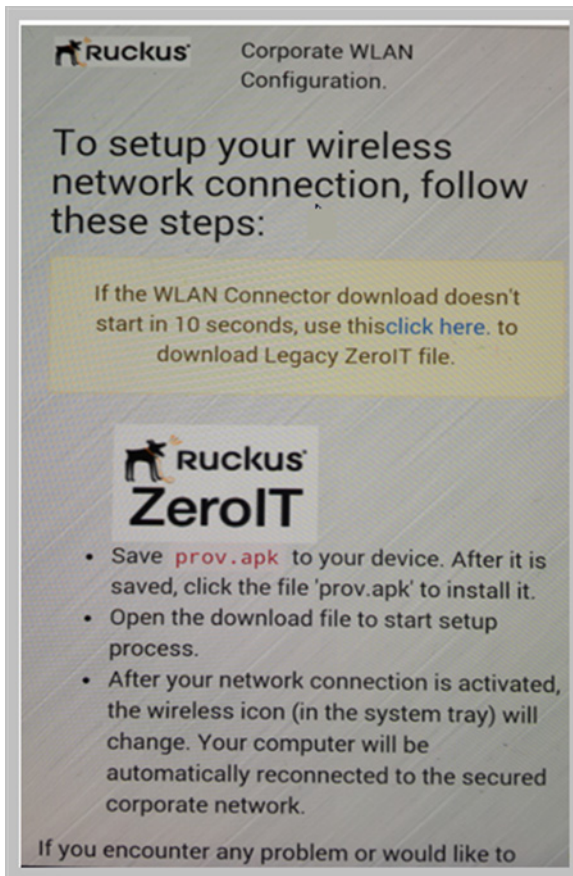
In case the authentication server is Local database, the portal sends a JSON authentication request to the SZ subscriber management (also called IDM) application. The IDM independently authenticates the user.

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 SZ 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 white list. 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.

After successful authentication (regardless of the authentication service used), the IDM uses the group attribute returned from the authentication service (uses the default service in case the service is not configured) for the best match map to the user role. From the user role (in addition to validating the maximum devices to use) IDM retrieves all authorized WLANs and provides it to Zero-IT module for generating the Zero-IT file. IDM also provides the required credentials to the Zero-IT module for including it in the file. When the IDM receives the file it save it in Cassandra and responds the SZ portal with the relative file path. With this the user sees the corporate WLAN configuration page ([Figure 19](#)) and the Zero-IT file is automatically downloaded.

Figure 19. WLAN Configuration

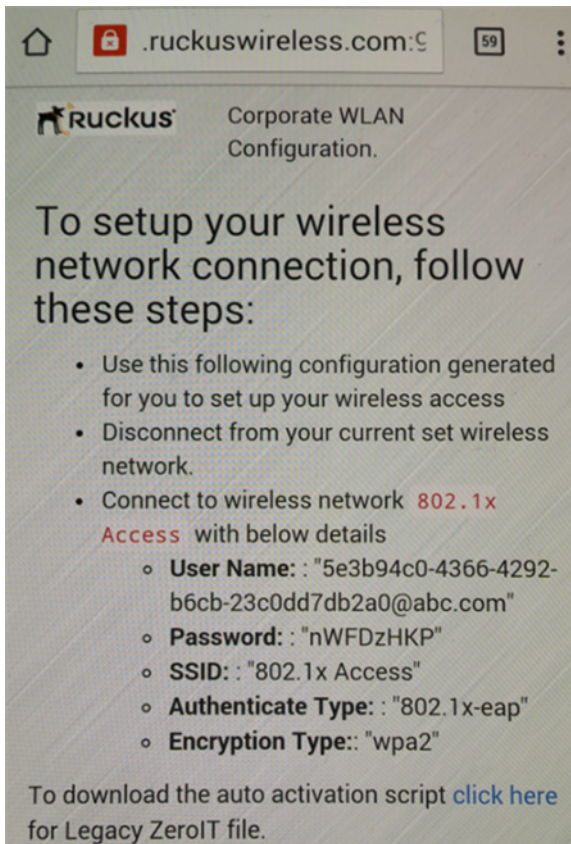


The portal also provides an icon to download the file manually. After installing the file, all Zero-IT WLANs are automatically configured.

NOTE: Some legacy devices will automatically switch to the first WLAN of the new provisioned WLAN list but some need a manual switch. Refer to [Table 15](#).

Detailed WLAN configuration information is also provided for manual setup ([Figure 20](#)) in case the Zero-IT module identifies the device as not supported for Zero-IT onboarding or the user has problems executing the file.

Figure 20. Connecting to Wi-Fi Network



NOTE: Each operating system /platform has various limitations to downloading and installing the Zero-IT file and automatically connecting to the appropriate SSID.

Table 15. Zero-IT Details

Operating System	Zero-IT			
	WPA/WPA2 WLAN		802.1x EAP (external RADIUS server)	
	Step 1	Step 2	Step 1	Step 2
IOS 5.1.1	Y	N (ZF-2888)	Y	N (ZF-2888)
IOS 6.1.3	Y	N (ZF-2888)	Y	N (ZF-2888)
IOS7 beta3	Y	N (ZF-2888)	Y	N (ZF-2888)
Mac OS (10.6.8)	Y	Y	Y	Y
Mac OS (10.8.3)	Y	Y	Y	N(ZF-4699)
Android(4.1.1,4.2.2)	Y	Y	Y	Y
Windows XP	Y	Y	Y	Y
Windows 7	Y	Y	Y	partial support (ZF-2366)
Windows 8	Y	Y	Y	partial support (ZF-2366)
Windows phone 7.	N	N	N	N
Windows phone 8	N	N	N	N
Blackberry OS 10	N	N	N	N

Remediation for Legacy and R1 Devices

SZ generates local credentials (if configured) and sets an expiration based on which the credentials will expire. In order to provide renewal of expiration (similar to R2 device) specific parameters are defined between several components.

When the RAC receives the expired password response from IDM for authorization status request (non R2 device) it adds a new VSA in the access accept response to AP instead of access reject response. Based on the RAC response the AP lets the UE get the IP address.

The user is required to initiate an access attempt to a remote website. The AP will intercept this access attempt and DNAT the request to the SZ captive portal, which in turn redirects the user to the internal on-boarding portal. The user types in his credentials, which are used in the on-boarding phase and is provisioned with the new Zero-IT file.

Configuration and Workflow of Hotspot 2.0 for R1 Devices

6

In this chapter:

- [Configuring Hotspot 2.0 for R1 Devices](#)
- [Onboarding Flow](#)

Certain devices support Hotspot 2.0 on R1 but not R2. In such circumstances, these devices can select the appropriate network based on Hotspot 2.0 configuration of the connection manager, but are not capable of provisioning the PPS-MO through the OSU server.

In order to support the provisioning of Hotspot 2.0 configuration file into such devices, the SCG uses the existing onboarding with Zero-IT procedure. The Zero-IT file contains the required Hotspot 2.0 parameter usually included in the PPS-MO.

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.

Configuring Hotspot 2.0 for R1 Devices

To enable an R1 device to download the appropriate R1 file, the administrator should follow [Configuring Hotspot 2.0](#) with the following exceptions.

- 1 In **Configuration > Hotspot 2.0 > Identity Providers > Network Identifier > Online Signup and Provisioning** select the option as Hotspot 2.0 R2, Hotspot 2.0 R1 ([Figure 21](#)).
- 1 Configure the WLAN guest access as in [WLAN Guest Access](#).
- 2 In **Configuration > WLAN:**
 - a In **WLAN Usage > Authentication Type** enable Guest Access + Hotspot 2.0 Online Signup.
 - b Authentication services for R1 devices should be defined in the **Configuration > Wireless Network > Guest Access**.

Figure 21. WLAN Usage form

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

Encryption Options

Guest Access Portal

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

Select the Guest Access - Hotspot 2.0.0 Online Signup radio button under WLAN Usage, and select the Zero-IT Onboarding checkbox for Release 1 devices.

Onboarding Flow

The onboarding flow is the same as [Legacy Devices and R1 Onboarding Workflow](#). The SZ portal identifies the device as R1 and provides this to IDM in the authentication request. The available files will be downloaded automatically and the user will be able to install them.

External Onboarding and Remediation Portal Integration



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 on-boarding and remediation.

The external portal communicates through the SZ's NBI. The NBI IP address (`nbiIp`) is the same as SZ 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 SZ web interface. Navigate to **Configuration > SmartZone System > 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 on-boarding 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&Redirect-
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

- The authentication server name is taken from the authentication service configuration specified in **Configuration > AAA Servers** in the SZ web interface as seen in [Figure 22](#). This configuration is applied to the specific Online Signup & Provisioning in **Configuration > 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

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: Browse

Subscription Descriptions: Language * English Friendly Name * ruckus Description Icon

Online Signup(OSU) Portal: ☒ Internal Portal Profile: * ruckus Create

OSU Authentication Services:

Service *	Credential Type *	Realm *	Local Credential Expiration
No data available	Local	osu-server.hs20.r	Day
Local Database	LOCAL_DB	Local	osu-server.hs20.ruckus
linkedin	LINKEDIN	Local	osu-server.hs20.ruckus
FB	FACEBOOK	Local	osu-server.hs20.ruckus
Radius	RADIUS	Local	osu-server.hs20.ruckus

Authentication in Remediation Flow

In remediation, OSU module in SZ 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 - User name used for remote authentication
- InternalUsername - User name sent for digest authentication
- AuthServerName- Authentication name as seen in the SZ web interface -
Configuration > Hotspot 2.0 > Identity Providers > 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= test-
user1-uid&InternalUsername= e552a465-1873-4d44@osu-
server.hs20.ruckus&AuthServerName=radius
```

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 on-boarding 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 SZ 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 SZ web interface - **Configuration > AAA Servers > Proxy AAA > Authentication Service**. See [Figure 24](#).

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

Refresh Create New Test AAA Delete Selected Search terms: ☒ Include all terms ☐ Include any of these terms

<input type="checkbox"/>	Name ▾	Friendly Name	Protocol	Description
<input type="checkbox"/>	AD		AD	
<input type="checkbox"/>	FB friendly name		FACEBOOK	

Edit Authentication Service [FB friendly name]

Name: *

Friendly Name:

Description:

Service Protocol: * ☐ RADIUS ☐ Active Directory ☐ LDAP ☒ OAuth ☐ HLR

OAuth Service Options

Provider: * ☒ Facebook ☐ Google ☐ LinkedIn

Application ID: *

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 acc

Advanced Options

Whitelisted Domains: Domain Name * Add Cancel

Domain Name ▾

*.facebook.com

fhcdnprofile.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 SZ 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" : "954316EDC578BD1AF464F3FCFCFAF568B",
    "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/oauth?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 ",
"updateIdentifier" : 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 ",
"updateIdentifier" : 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",
  "updateIdentifier" : 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 re-authentication 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 SZ

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 the AAA server (for Anon-TLS or EAP-TTLS) certificates or the OSU server certificates have not been revoked using OCSP within the TLS connection.

RuckOS 3.1 has 2 different modules which handle this requirement:

- 1** NGINX - Provisioning and remediation servers in the SZ 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 SZ RAC module interacts with the OCSP server.
 - a** During Anonymous TLS for on-boarding call flow as seen in [Figure 25](#)
 - b** During EAP-TTLS access flow as seen in [Figure 26](#)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

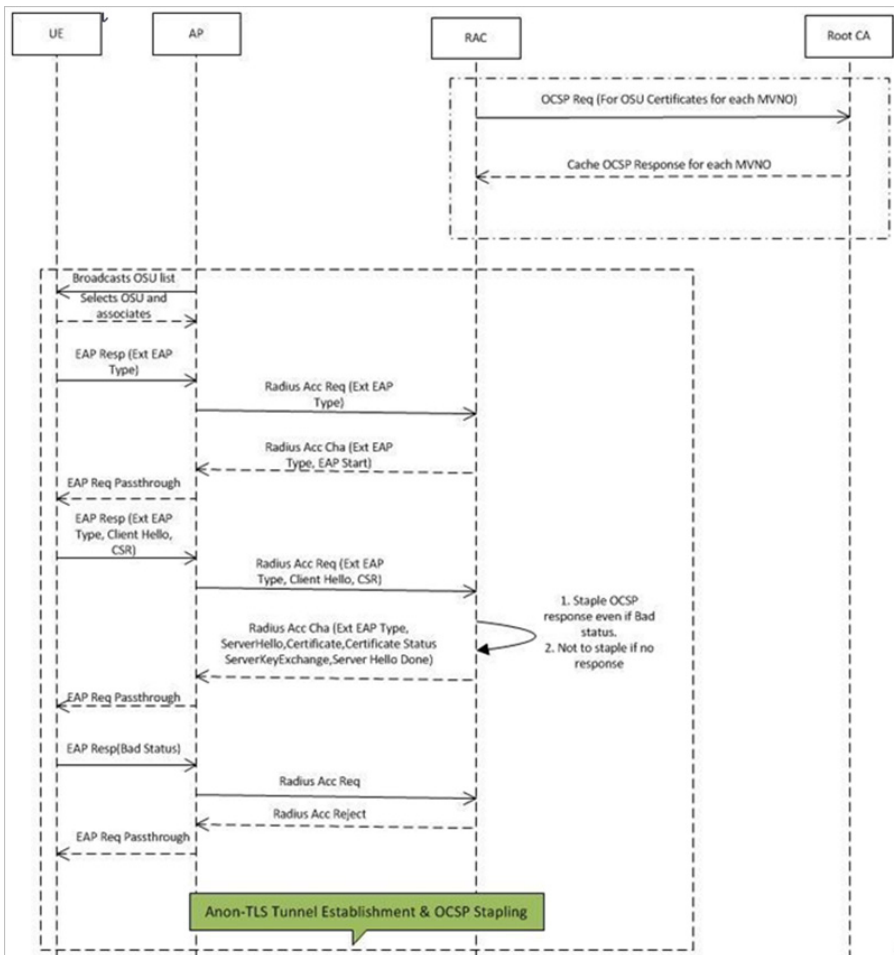


Figure 26. Interaction with OCSP server during EAP-TLS

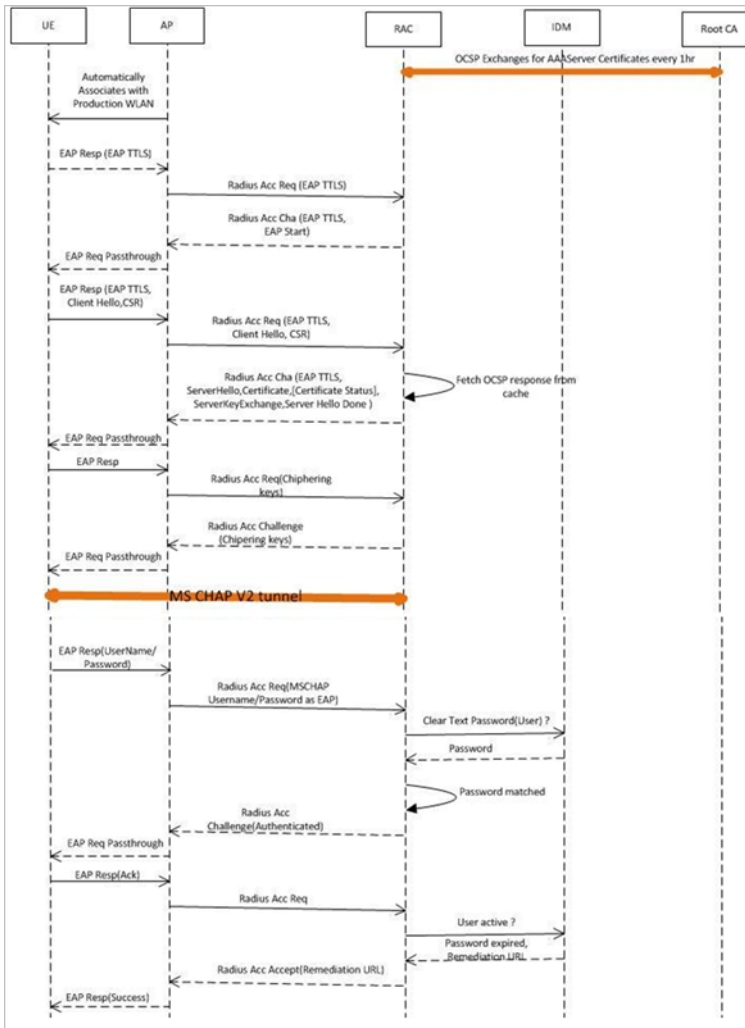


Figure 27 and Figure 28 show the important fields in the OSCP messages. These are standard message, which operators and administrators should be aware of for successful call flows. Possible values of the certificate status field is good, bad or revoked.

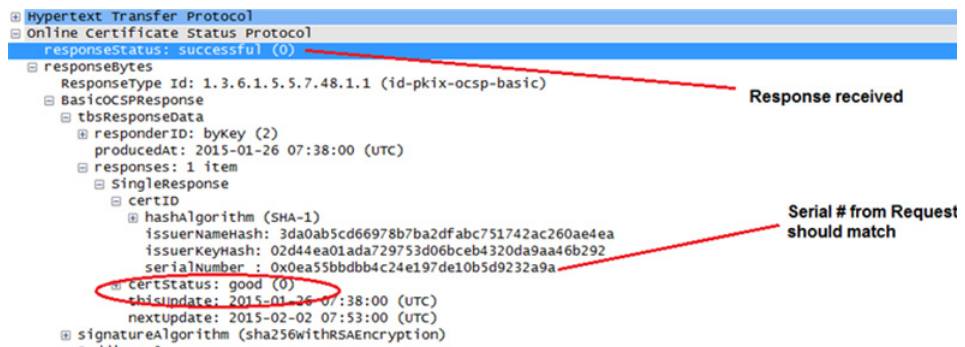
NOTE: If the client (mobile device) requests for *Certificate Status* request, RAC provides the status if it is available. In case the certificate status is not provided it is up to the client if it wants to continue or abort the call.

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
                [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

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

Index

A

- access network type 28
- access points 11
- accounting. 26
- ap zone 28
- authentication 25
- authentication server 36, 41
- authentication services 44, 46
- authorization status 38

C

- certificate 13
- common language icon 19
- configured realm 38
- connection capability 29
- credential type 46, 47
- custom connection capability 29

D

- de-auth 39
- domain names 13

F

- facebook 51
- friendly name 13, 45

G

- google 51
- group attribute 52
- group attribute value 45
- guest access 45, 46, 58

H

- home ols 16
- hotspot 2.0 wifi 13

I

- identify providers 28
- identity providers 15, 38

- internet option 28
- ip address type 28

L

- legacy devices 43
- local credential expiration 47

M

- mobile device 9

N

- network identifier 15

O

- oauth authentication 51
- oauth providers 51
- onboarding 50
- onboarding flow 59
- onboarding portal 43, 46
- online signup and provisioning 18
- online signUp portal 22
- online signup portal 43
- operator 28
- operators 11
- osu authentication services 20
- osu certificates 20
- osu nai realm 19
- osu portal 19
- osu server certificate 50

P

- password 40
- physical network 11
- plmns 16
- portal language 23, 43
- portal logo 23, 43
- portal name 22, 43
- portal title 23, 43
- provisioning format 19
- provisioning protocol 18

provisioning service 18
provisioning updates at 19

R

read password 38
realm 25, 26
realm value 47
realms 16
register device 50
remediation 39
remote 47
renewal of expiration 55
review 27

S

service 46
service protocol 45
service providers 11
signup security 13
subscription description 20

T

terms and conditions 23
time bound whitelist 52

U

update identifier 40
user role 52

V

venue category 30
venue names 30
venue profile 30

W

wan metrics 30
whitelisted domain 21

Z

zero-it onboarding 51



Copyright © 2006-2015. Ruckus Wireless, Inc.
350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com