Ruckus Wireless™ SmartCell Gateway™ 200

Hotspot Portal Integration Reference Guide for Release 2.1.2

Part Number 800-70518-001 Rev B
Published May 2014

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Destination Control Statement

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

Disclaimer

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

Limitation of Liability

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

Trademarks

Ruckus Wireless, Ruckus, the bark logo, 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

This *SmartCell Gateway™ (SCG) 200 Hotspot Portal Integration Reference Guide* describes the SCG RESTful-like/JSON interfaces for external web portal servers.

This guide is written for service operators and system administrators who are responsible for managing, configuring, and troubleshooting Ruckus Wireless devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

NOTE: This guide assumes that the SmartCell Gateway has already been installed as described in the *Getting Started Guide*.

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**.
italics	Screen or page names	Click **Advanced Settings**. The *Advanced Settings* page appears.

Table 2. Notice conventions

Notice Type	Description
NOTE	Information that describes important features or instructions
CAUTION!	Information that alerts you to potential loss of data or potential damage to an application, system, or device
WARNING!	Information that alerts you to potential personal injury

Terminology

Table 3 lists the terms used in this guide.

Table 3. Terms used in this guide

Terms	Description
AP	Access Point
CP	Captive Portal
NBI	Northbound Interface
RADIUS	Remote Authentication Dial-Up Service
SCG	Smart Cell Gateway
SSL	Secure Socket Layer

Table 3. Terms used in this guide

Terms	Description
TCP	Transmission Control Protocol
UE	User Equipment
UE-IP	User Equipment - IP address
UE-MAC	User Equipment - MAC address

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 2.1.2)
- Part number: 800-70516-001
- Page 88

Web Interface Configuration

1

In this chapter:

Overview

The SCG provides Wi-Fi hotspot services in conjunction with external web portal servers. In most cases, an external web portal server provides the landing web pages with Wi-Fi hotspot usage instructions, terms and conditions, etc., while the end user submits his login ID and password directly to the AP for authentication.

There are, however, some cases when an external web portal server requires total control of a user session by requesting authentication on the user's behalf as well as terminating the user sessions. JSON interface defined in this reference guide provides a standard way for an external web portal server to communicate with the SCG for this kind of usage.

This reference guide describes the SCG RESTful-like/JSON interfaces for external web portal servers.

NOTE: Refer to About This Guide chapter for conventions used in this guide.

Request Format

As defined in JSON Commands, each request issued from an external web portal server is in JSON format and the SCG URL requests are:

```
http://scg_management_ip:9080/portalintf (HTTP request)
https://scg_management_ip:9443/portalintf (HTTPS request)
```

NOTE: You can download the log for northbound portal interface from the SCG web interface by navigating to **Administration** > **Diagnostics** > **Application Logs & Status**.

SCG Web Interface Configuration

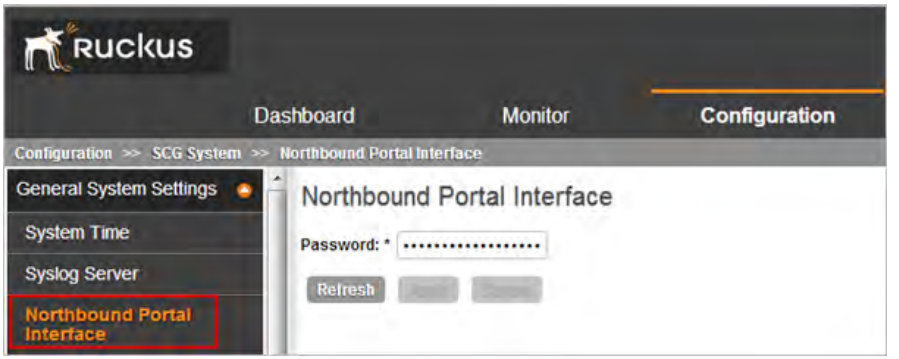
Each JSON request must be accompanied by a request password that is preconfigured on the SCG, as well as on the external web portal server. This helps to ensure that only authorized web portal servers can access the northbound portal interface.

The northbound portal interface request password can be configured in the SCG web interface by navigating to **Configuration** > **SCG System** > **General System Settings** > **Northbound Portal Interface**. See Figure 1.

If the incoming request password does not match the configured password, the SCG will silently discard the incoming requests.

A web portal server must use the POST command to issue JSON requests. The SCG will not accept requests through a regular HTTP connection.

Figure 1. Setting the password



JSON Commands

2

In this chapter:

User Online Control

The northbound portal interface supports the following JSON commands:

- Request Authorization
- Login
- Login Async
- Status
- Logout
- Disconnect
- Enrichment Info

These commands are used for user authentication, user status query, terminating user sessions and verifying that the enrichment information has the same content as that of the HTTP header enrichment information.

UE-IP (User Equipment - IP address) and UE-MAC (User Equipment - MAC address) is the IP and the MAC addresses of the end user. NBI (Northbound Interface) uses either UE-MAC or UE-IP address in all JSON requests. In case both are included in the JSON request the UE-MAC address will be used as default.

The UE-IP and UE-MAC address parameters are decrypted at the beginning of each user online control request. This is because the Captive Portal (CP) encrypts the IP and MAC address parameters in each redirection (See Table 12 for the full list of these parameters) to the subscriber portal. The SCG decrypts the UE-IP and UE-MAC address before returning the response, by using the new utility.

NOTE: Northbound Interface (NBI) expects to receive encrypted /decrypted UE-IP and UE-MAC address when the request category is user online control. In the GetConfig request category you do not need to encrypt UE-IP and UE-MAC address.

Request Authorization

Request authorization is a JSON command for authorizing a client without any authentication. It does not need a RADIUS server. The client is always authenticated, provided it is available in the SCG system.

Normally in a RADIUS authentication the login credentials such as the username and password is provided in the JSON request. The RADIUS server responds with either a success or a failed authentication (login/login async), along with a set of client session settings. Table 4 lists these client session settings.

In a request authorization command, a RADIUS authentication is not required since the client credentials are already authenticated. The client settings are passed in a JSON request from the RADIUS server.

Table 4. RADIUS and its equivalent JSON attribute

RADIUS Attribute	JSON Attribute
Session-Timeout	UE-Session-Timeout
Ruckus-Grace-Period	UE-Ruckus-Grace-Period
Idle-Timeout	UE-Idle-Timeout
WISPr-Bandwidth-Max-Up	UE-WISPr-Bandwidth-Max-Up
WISPr-Bandwidth-Max-Down	UE-WISPr-Bandwidth-Max-Down
Acct-Interim-Interval	UE-Acct-Interim-Interval
Class	UE-Class

The following is an example of request authorization.

```
{{
"Vendor":"Ruckus",
"RequestPassword":"admin!234",
"APIVersion":"1.0",
"RequestCategory":"UserOnlineControl",
"RequestType":"Authorize",
"UE-IP":"",
"UE-MAC":"ENCa13cc65-
ca57cc500bc790684ff6d6ab62d0bf93f9f60a7d8",
"UE-Proxy":"0" ,
"UE-Username":"Optional and will not be validated",
"UE-Password":"Optional and will not be validated" ,
"UE-Ruckus-Grace-Period":"600" ,
"UE-Idle-Timeout":"999" ,
"UE-WISPr-Bandwidth-Max-Up":"8888" ,
"UE-WISPr-Bandwidth-Max-Down":"22222" ,
```

```
"UE-Acct-Interim-Interval":"10" ,
"UE-Class":"1"}
}
```

Table 5 lists the responses for request authorization.

Table 5. Request authorization

Response Type	Possible Responses
Normal response	• 201, Login succeeded: Response if the login is accepted.
Service error	• 300, Not found: Response if the lookup fails with the given UE-MAC or UE-IP address. • 400, Internal server error: Response when a SCG internal error occurs.
General error	• 302, Bad request: Response if the JSON request is not well-formed. • 303, Version not supported: Response if there is a version mismatch. • 304, Command not supported: Response if the request type is not supported. • 305, Category not supported: Response if the request category not supported.

Request Authentication

In the hotspot (WISPr) WLAN use case, an unauthorized user is redirected to an external web portal server by the SCG. Using the *LoginAsync* command, the external web portal server sends a request to the SCG to authenticate the user via the RADIUS server. The following is an example of the authentication request:

```
{
 Vendor: “ruckus”
 RequestPassword: “myPassword”,
 APIVersion: “1.0”,
 RequestCategory: “UserOnlineControl”,
 RequestType: “LoginAsync”,
 UE-IP: “ENC12bc24c4777703327f2e0aabbf6b9f9e”,
 UE-MAC: “ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3D-
 BE2157”,
```

```
  UE-Proxy: “0”,
  UE-Username: “test”,
  UE-Password: “test”
}
```

NOTE: The user account *test* (UE username) mentioned in the above example, has been created as an external guest in the RADIUS server. The hotspot portal does not provide an interface for creating new user account.

UE-IP and UE-MAC is the IP address and the MAC address of the end user. Table 6 lists the SCG responses to these authentication requests.

Table 6. SCG responses to authentication requests

Response Type	Possible Responses
Normal response	• 101, Client authorized: Response if the user is already authorized. • 202, Authentication pending: Authentication is in progress, portal server needs to check the result later.
Service error	• 300, Not found: Response if the lookup fails with given UE-MAC or UE-IP address. • 400, Internal server error: Response when the SCG internal error occurs.
General error	• 302, Bad request: Response if the JSON request is not well-formed. • 303, Version not supported: Response if there is a version mismatch. • 304, Command not supported: Response if the request type is not supported. • 305, Category not supported: Response if the request category not supported.

Login Blocking Command

The SCG also provides a login blocking command. The following is an example of this command.

```
{
 Vendor: “ruckus”
 RequestPassword: “myPassword”,
 APIVersion: “1.0”,
 RequestCategory: “UserOnlineControl”,
 RequestType: “Login”,
 UE-IP: “ENC12bc24c4777703327f2e0aabbf6b9f9e”,
 UE-MAC: “ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3D-
 BE2157”,
 UE-Proxy: “0”,
 UE-Username: “test”,
 UE-Password: “test”
}
```

Table 7 lists the SCG responses to these login blocking commands until the SCG retrieves a response from the RADIUS server.

Table 7. SCG responses to a login blocking command

Response Type	Possible Responses
Normal response	• 101, Client authorized: Response if the user is already authorized. • 201, Login succeeded: Response if the login is accepted.
Service error	• 300, Not found: Response if the lookup fails with given UE-MAC or UE-IP address. • 301, Login failed: It will be replaced if the RADIUS reply message is returned. • 400, Internal server error: Response when an SCG internal error occurs. • 401, RADIUS server error: Response when a RADIUS connection error occurs or the connection request times out.

Table 7. SCG responses to a login blocking command

General error	• 302, Bad request: Response if the JSON request is not well-formed. • 303, Version not supported: Response if there is a version mismatch. • 304, Command not supported: Response if the request type is not supported. • 305, Category not supported: Response if the request category not supported.

Querying a User Status

After the authentication request is issued, the external web portal server can query the user's authentication status. The following is an example of the user status query command:

```
{
 Vendor: “ruckus”
 RequestPassword: “myPassword”,
 APIVersion: “1.0”,
 RequestCategory: “UserOnlineControl”,
 RequestType: “Status”,
 UE-IP: “ENC12bc24c4777703327f2e0aabbf6b9f9e”,
 UE-MAC: “ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3D-
BE2157”
}
```

UE-IP and UE-MAC is the IP address and the MAC address of the end user. Table 8 lists the SCG responses to these user status query commands.

Table 8. SCG responses to user status query

Response Type	Possible Responses
If there is a pending authentication process for this client	• 201, Login succeeded. • 202, Authentication pending: Authentication is in progress, portal server needs to check the result later.

Table 8. SCG responses to user status query

Response Type	Possible Responses
If there is no pending authentication process for this client	• 100, Client unauthorized. or • 101, Client authorized.
Service error	• 300, Not found: Response if the lookup fails with given UE- MAC or UE-IP address. • 301, Login failed: It will be replaced if the RADIUS reply message is returned • 400, Internal server error: Response when an SCG internal error occurs. • 401, RADIUS server error: Response when a RADIUS connection error occurs or the connection request times out.
General error	• 302, Bad request: Response if the JSON request is not well-formed. • 303, Version not supported: Response if there is a version mismatch. • 304, Command not supported: Response if the request type is not supported. • 305, Category not supported: Response if the request category not supported.

NOTE: If an authentication process has a result (not pending), the SCG responds to it only once. For example, if the SCG replies *301, Login failed* to the web portal server, and the web portal server sends the same query, the response will be *100, Unauthorized*. If the SCG replies *201, Login succeeded,* and the web portal server queries again, the response will be *101, Authorized*.

Terminating a User Session

After a user session is authorized, the external web portal server can terminate the user session by sending a JSON request to the SCG. In this case, the user will change the status from *auth* to *un-auth* for the subscriber to login again. The TCP connections to the web server portal are not terminated, as this generates a *404 Error*. The following is an example of the terminating a user session command:

```
{
 Vendor: “ruckus”
 RequestPassword: “myPassword”,
 APIVersion: “1.0”,
 RequestCategory: “UserOnlineControl”,
 RequestType: “Logout”,
 UE-IP: “ENC12bc24c4777703327f2e0aabbf6b9f9e”,
 UE-MAC: “ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3D-
BE2157”
}
```

Disconnect Command

The SCG also provides a command for terminating user TCP (Transmission Control Protocol) connections from AP (Access Point).

```
{
 Vendor: “ruckus”
 RequestPassword: “myPassword”,
 APIVersion: “1.0”,
 RequestCategory: “UserOnlineControl”,
 RequestType: “Disconnect”,
 UE-IP: “ENC12bc24c4777703327f2e0aabbf6b9f9e”,
 UE-MAC: “ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3D-
BE2157”
}
```

UE-IP and UE-MAC is the IP address and the MAC address of the end user. Table 9 lists the SCG response.

Table 9. SCG responses to a disconnect command

Response Type	Possible Responses
Normal response	• 200, OK • 101, Client unauthorized: Response if the user is already unauthorized
Service error	• 300, Not found: Response if the lookup fails with given UE- MAC or UE-IP address. • 400, Internal server error: Response when an SCG internal error occurs.
General error	• 302, Bad request: Response if the JSON request is not well-formed. • 303, Version not supported: Response if there is a version mismatch. • 304, Command not supported: Response if the request type is not supported. • 305, Category not supported: Response if the request category not supported.

Querying Enrichment Information

The northbound portal interface provides the JSON command *EnrichmentInfo* for verifying that the enrichment information has the same content as the HTML header enrichment information sent from the AP. This allows the captive portal to obtain the enriched parameters in an SSL (Secure Sockets Layer) scenario or in other cases where the AP enrichment information is not available.

The following is an example of the *EnrichmentInfo* request:

```
{
 Vendor: “ruckus”
 RequestPassword: “myPassword”,
 APIVersion: “1.0”,
 RequestCategory: “UserOnlineControl”,
 RequestType: “EnrichmentInfo”,
 UE-IP: “ENC12bc24c4777703327f2e0aabbf6b9f9e”,
}
```

Table 10 lists the responses for enrichment information.

Table 10. Query enrichment

Response Type	Possible Responses
Normal response	• 102, Enrichment Information.
Service error	• 300, Not found: Response if the lookup fails with given UE- MAC or UE-IP address. • 400, Internal server error: Response when an SCG internal error occurs.
General error	• 302, Bad request: Response if the JSON request is not well-formed. • 303, Version not supported: Response if there is a version mismatch. • 304, Command not supported: Response if the request type is not supported. • 305, Category not supported: Response if the request category not supported.

GetConfig

The northbound interface supports the following JSON commands in request category - GetConfig:

1 Control Blade IP List
2 Cluster Blade IP List
3 Management Blade IP List
4 User Interface IP List
5 Encrypt IP
6 Decrypt IP

The first four commands are used for obtaining the different blade IP address lists. The northbound portal interface responds with the control, cluster and management blade or user defined IP address list of the SCG.

The following is an example of the GetConfig command:

```
{
 Vendor: “ruckus”,
 RequestPassword: “myPassword”,
```

```
 APIVersion: “1.0”,
 RequestCategory: “GetConfig”,
 RequestType: “ControlBladeIPList”,
 UE-IP: “192.168.0.38”
}
```

The following is an example of the successful response:

```
{
   Vendor:“ruckus”,
   ReplyMessage:”OK",
   ResponseCode:200,
   APIVersion:"1.0"
  ControlBladeIPList:[“172.17.18.149”, “172.17.18.159”,
  “172.17.18.169”]
}
```

Control Blade IP address list can be replaced by Cluster Blade IP List, Management Blade IP List or User Interface IP List, depending on context of the GetConfig command.

The following is an example of an Encrypt IP address command, which returns an encrypted IP address for direct access to the subscriber portal.

```
{
 Vendor: “ruckus”,
 RequestPassword: “myPassword”,
 APIVersion: “1.0”,
 RequestCategory: “GetConfig”,
 RequestType: “EncryptIP”,
 UE-IP: “172.21.134.87”
}
```

The following is an example of the successful response:

```
{
   Vendor:“ruckus”,
   ReplyMessage:”OK",
   ResponseCode:200,
   APIVersion:”1.0”
   ENC-UE-IP: “ENC1234bfdbe5y5hbfdgh45y54ryt5y5th5”
```

```
}
```

Another example is decrypt IP address command.

```
{
Vendor: "ruckus",
RequestPassword: "myPassword", APIVersion: "1.0",
RequestCategory: "GetConfig", RequestType: "DecryptIP",
UE-IP: "ENC1234bfdbe5y5hbfdgh45y54ryt5y5th5"
}
And the success response:
{
Vendor:"ruckus", ReplyMessage:"OK", ResponseCode:200,
APIVersion:"1.0"
DEC-UE-IP: "172.21.134.87"
}
```

JSON Responses

3

In this chapter:

JSON Responses

Table 11 lists the definitions of JSON responses from the northbound portal interface. The following are the expansions for the abbreviations mentioned in the *Used In* column.

- UA: User Authenticate (includes Login and LoginAsync)
- SQ: Status Query
- TU: Terminating User (Logout and Disconnect)
- AU: Authorize the requests
- EI: Enrichment Info
- GC: Get Config (Control Blade IP, Cluster Blade IP, Management Blade IP, User Interface IP, Encrypt IP and Decrypt IP address)

NOTE: Refer to JSON Commands for commands relating to the responses mentioned above.

Table 11. JSON response definitions

Category	Code	Definition	Used In					
			UA	SQ	AU	TU	EI	GC
Informational	100	Client unauthorized		•		•		
	101	Client authorized	•	•				
	102	Enrichment Info					•	
Success	200	OK				•		•
	201	Login succeeded		•	•			
	202	Authentication pending	•	•				
Client Error	300	Not found	•	•	•	•	•	
	301	Login failed	•	•				
	302	Bad request	•	•	•	•	•	•
	303	Version not supported	•	•	•	•	•	•
	304	Command not supported						
	305	Category not supported						

Table 11. JSON response definitions (Continued)

Category	Code	Definition	Used In					
Server Error	400	Internal server error	•	•	•	•	•	•
	401	RADIUS server error	•	•				

JSON Response Examples

This section provides the following examples of JSON responses defined in Table 11.

- Example: Client unauthorized
- Example: Client authorized
- Example: Request Authorization
- Example: Enrichment information
- Example: Success information
- Example: Login succeeded
- Example: Authentication pending
- Example: Not found
- Example: Login failed
- Example: Bad request
- Example: Version not supported
- Example: Command not supported
- Example: Category not supported
- Example: Internal server error
- Example: RADIUS server error
- Example: Encrypt ID for MAC address
- Example: Decrypt ID for MAC address

Example: Client unauthorized

```
{
Vendor:"Ruckus",
APIVersion:"1.0",
ResponseCode:100,
ReplyMessage:"Client unauthorized",
UE-IP:"ENC323e79bf1bbd5ac4",
```

```
UE-MAC:"ENCf6b7f49da92a45f8978c35966b95ee-
afc6451102af391592",
AP-MAC:"00:11:22:AA:BB:CC",
SSID:" hotspot-01",
SmartClientInfo:"",
GuestUser:"0",
SmartClientMode:"none",
}
```

Example: Client authorized

```
{
Vendor: "Ruckus",
APIVersion: "1.0",
ResponseCode: "101",
ReplyMessage: "Client authorized",
UE-IP: "ENC12bc24c4777703327f2e0aabbf6b9f9e",
UE-MAC: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3D-
BE2157",
UE-Username: "user001",
AP-MAC: "04:4f:aa:32:25:f0",
SSID: "hotspot-01",
SmartClientMode: "none",
SmartClientInfo: "",
GuestUser: "0",
}
```

Example: Request Authorization

```
{
"ReplyMessage":"Login succeeded",
"AuthenticationType":"Local DB",
"UE-IP":"ENCec4cc1fd0c146d53e200ad215eec9460",
"APIVersion":"1.0",
"ResponseCode":201,
"AP-MAC":"50:A7:33:23:6E:00",
"GuestUser":"0",
"SmartClientMode":"none",
```

```
"UE-MAC":"ENCa13cc65-
ca57cc500bc790684ff6d6ab62d0bf93f9f60a7d8",
"Vendor":"Ruckus",
"SSID":"nbi-wlan-local",
"SmartClientInfo":"",
"UE-Proxy":0
}
```

Example: Enrichment information

```
{
Vendor: "Ruckus",
APIVersion: "1.0",
ResponseCode: "102",
ReplyMessage: "Enrichment Information",
UE-IP: " ENC12bc24c4777703327f2e0aabbf6b9f9e ",
UE-MAC: " ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3D-
BE2157",
AP-MAC: "04:4f:aa:32:25:f0",
SSID: "hotspot-01",
WLAN-ID: "1",
Location: "a location",
}
```

Example: Success information

```
{
Vendor: "Ruckus",
Version: "1.0",
ResponseCode: "200",
ReplyMessage: "OK"
UE-IP: "ENC12bc24c4777703327f2e0aabbf6b9f9e",
UE-MAC: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3D-
BE2157",
SmartClientMode: "none",
SmartClientInfo: "",
GuestUser: "0",
}
```

Example: Login succeeded

```
{
Vendor: "Ruckus",
APIVersion: "1.0",
ResponseCode: "201",
ReplyMessage: "Login succeeded",
UE-IP: "ENC12bc24c4777703327f2e0aabbf6b9f9e",
UE-MAC: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3D-
BE2157",
UE-Username: "user001",
AP-MAC: "04:4f:aa:32:25:f0",
SSID: "hotspot-01",
SmartClientMode: "none",
SmartClientInfo: "",
GuestUser: "0",
UE-Proxy: "0"
}
```

Example: Authentication pending

```
{
Vendor: "ruckus",
APIVersion: "1.0",
ResponseCode: "202",
ReplyMessage: "Authentication pending",
UE-IP: "ENC12bc24c4777703327f2e0aabbf6b9f9e",
UE-MAC: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3D-
BE2157",
UE-Username: "user001",
AP-MAC: "04:4f:aa:32:25:f0",
SSID: "hotspot-01",
SmartClientMode: "none",
SmartClientInfo: "",
GuestUser: "0",
}
```

Example: Not found

```
{
 Vendor: "Ruckus",
 APIVersion: "1.0",
 ResponseCode: "300",
 ReplyMessage: "Not found",
}
```

Example: Login failed

```
{
Vendor: "Ruckus",
APIVersion: "1.0",
ResponseCode: "301",
ReplyMessage: "Login failed",
UE-IP: "ENC12bc24c4777703327f2e0aabbf6b9f9e",
UE-MAC: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3D-
BE2157",
AP-MAC: "04:4f:aa:32:25:f0",
SSID: "hotspot-01",
SmartClientMode: "none",
SmartClientInfo: "",
GuestUser: "0",
}
```

Example: Bad request

```
{
Vendor: "ruckus",
APIVersion: "1.0",
ResponseCode: "302",
ReplyMessage: "Bad request",
}
```

Example: Version not supported

```
{
Vendor: "ruckus",
APIVersion: "1.0",
```

```
  ResponseCode: "303",
  ReplyMessage: "Version not supported"
  }
```

Example: Command not supported

```
  {
  Vendor: "ruckus",
  APIVersion: "1.0",
  ResponseCode: "304",
  ReplyMessage: "Command not supported",
  }
```

Example: Category not supported

```
  {
  Vendor: "ruckus",
  APIVersion: "1.0",
  ResponseCode: "305",
  ReplyMessage: "Category not supported",
  }
```

Example: Internal server error

```
  {
  Vendor: "ruckus",
  APIVersion: "1.0",
  ResponseCode: "400",
  ReplyMessage: "Internal server error",
  }
```

Example: RADIUS server error

```
  {
  Vendor: "ruckus",
  APIVersion: "1.0",
  ResponseCode: "401",ll,
  ReplyMessage: "Radius server error",
}
```

Example: Encrypt ID for MAC address

```
  {
  Vendor: “ruckus”,
  RequestPassword: “myPassword”,
  APIVersion: “1.0”,
  RequestCategory: “GetConfig”,
  RequestType: “EncryptIP”,
  UE-IP: “04:4f:aa:32:25:f0”
  }
The success response:
  {
  Vendor: “ruckus”,
  ReplyMessage:”OK",
  ResponseCode:200,
  APIVersion:”1.0”,
  ENC-UE-IP: "ENC4782689566f8-
  eac8aa30e276aa907f332d0bf93f9f60a7d8"
  }
```

NOTE: The value of the UE-IP address is the MAC address.

Example: Decrypt ID for MAC address

```
  {
  Vendor: "ruckus",
  RequestPassword: "myPassword",
  APIVersion: "1.0",
  RequestCategory: "GetConfig",
  RequestType: "DecryptIP",
  UE-IP: "ENC4782689566f8-
  eac8aa30e276aa907f332d0bf93f9f60a7d8"
  }
The success response:
  {
  Vendor:"ruckus", ReplyMessage:"OK",
  ResponseCode:200,
```

```
APIVersion:"1.0"
DEC-UE-IP: "04:4f:aa:32:25:f0"
}
```

NOTE: The value of the UE-IP is the MAC address.

WISPr Support for ZoneDirector Login

A

In this appendix:

The WISPr hotspot portal logon API supports existing customer's external logon page (working with Zone Director (ZD)). Customers, who already have a ZD deployment and have implemented their own external logon page for hotspot WLAN, can use ZD's API (provided by Ruckus) for UE authentication.

The SCG provides the same API as that of ZD for customers to use their existing logon page.

NOTE: This new API is provided since SCG's official portal integration using JSON requests does not support ZD login API. It is our recommendation that the customer works with the JSON API as documented in this guide - *Hotspot Portal Integration Interface*.

Customer Login

Customers who already have ZD deployment with their own external portal will be required to make a change to their login/logout URLs to match the new supported API.

The external portal sends the login/logout request to SCG. The requests should include the parameters provided by SCG's captive portal redirection

---

NOTE: See Captive Portal Attributes for details.

- Login: The login request path in the external portal to the SCG should be changed:

  From:

  ```
  https://sip:9998/login
  ```

  To:

  ```
  https://sip:9998/SubscriberPortal/hotspotlogin
  ```

NOTE: The login request also supports HTTP with port number 9997.

NOTE: This login request should include the customer login credentials such as the username and password parameters.

Customer Logout

The logout request path in the external portal to the SCG should be changed:

From

```
https://sip:9998/logout
```

To

```
https://sip:9998/SubscriberPortal/hotspotlo-
gout?uip=10.20.30.40
```

Captive Portal Attributes

B

In this appendix:

The UE-IP and UE-MAC address parameters are decrypted at the beginning of each user online control request. This is because the Captive Portal (CP) encrypts the IP and MAC address parameters in each redirection to the subscriber portal. The SCG decrypts the UE-IP and UE-MAC address before returning the response, by using the new utility.

Redirection Attributes

Table 12 lists these parameters provided by SCG's captive portal redirection.

NOTE: See WISPr Support for ZoneDirector Login for login and logout details.

Table 12. Redirection attributes

Attributes	Description
sip	The value could either be the: • UDI (User Defined Interface) in case of a local breakout from AP or • Internal D-Blade IP address in case of a proxy request to the SCG.
startUrl	The URL as per the hotspot configuration, which is to be redirected after successful login.
client_mac	Encrypted UE Mac address.
uip	Encrypted UE IP address.
wlan	WLAN ID of the UE's associated the WLAN.
reason	Reason for redirecting the WLAN.
mac	AP Mac address.
url	Original URL which the customer tries browsing.
loc	AP location.
proxy	The UE browser if it is set to the Web proxy.
vlan	VLAN which the customer is set to
ssid	The broadcasted SSID name.

Table 12. Redirection attributes

Attributes	Description
zoneId	In case of 3rd party AP, this attribute will be included instead of WLAN and will include the zone ID where the SSID is configured to in the SCG.
dn	The domain name.

Index