Ruckus Wireless™
SmartZone™ 100 and Virtual SmartZone Essentials

Hotspot WISPr Reference Guide for SmartZone 3.4.1

Copyright Notice and Proprietary Information

Contents

About This Guide

This *SmartZone™ (SZ) 100 and vSZ-H Hotspot WISPr Reference Guide* describes the SZ-100/vSZ-E (collectively referred to as "the controller" throughout this guide) 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 If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

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

Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1.   Text conventions

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

Table 2.   Notice conventions

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

Terminology

Table 3 lists the terms used in this guide.

Table 3.   Terms used in this guide

Terms	Description
AP	Access Point
CP	Captive Portal
NBI	Northbound Interface
RADIUS	Remote Access Dial In User Service
SZ	Smart Zone
SSL	Secure Socket Layer

Table 3.   Terms used in this guide

Terms	Description
TCP	Transmission Control Protocol
UDI	User Define Interface
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.

Online Training Resources

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

Documentation Feedback

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

docs@ruckuswireless.com

When contacting us, please include the following information:

• Document title

• Document part number (on the cover page)

• Page number (if appropriate)

For example:

• SmartZone 100 and vSZ-E Hotspot WISPr Reference Guide for SmartZone 3.4.1

• Part number: 800-71148-001

• Page 88

Web Interface Configuration

1

In this chapter:

-
-
-

Overview

The controller 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 user sessions. JSON interface defined in this reference guide provides a standard way for an external web portal server to communicate with the controller for this kind of usage.

The following are the hotspot components and its role in the hotspot portal as seen in Figure 1.

- Northbound: Listens on the control and management interface. It is responsible for handling requests from external subscriber portal and authenticates with the AAA server.

- Captive portal: Listens on the control interface or UDI. It is responsible for providing a wall garden for web-proxy UE. It blocks UEs, which uses user agents that are listed in the configured black-list and mainly handles high scalable redirecting UEs to the external subscriber portal.

- External subscriber portal: Is a Web service. The user sends his/her login credentials (username and password) through this portal. The authentication is performed through the northbound by user input credential. The external subscriber portal can reach the northbound depending on the type of interface it can reach such as control interface, management interface or both.

- AAA server: Is responsible for authenticating the UE through the UE's login credentials (username and password).

Figure 1. Hotspot portal components
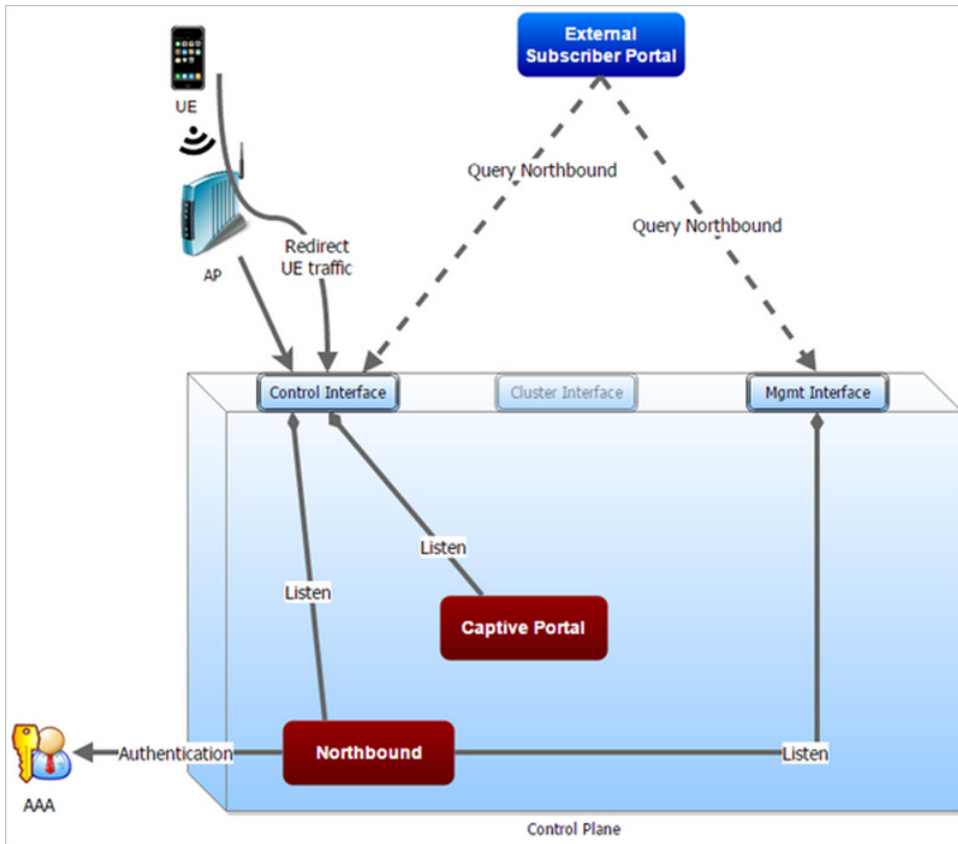
This reference guide describes the controller RESTful-like/JSON interfaces for external web portal servers.

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. NBI is only accessible via the management, control and user defined interfaces. The following are the request formats.

HTTP Request

```
http://{sz_management_ip}:9080/portalintf
```

HTTPS Request

```
https://{sz_management_ip}:9443/portalintf
```

NOTE: The above URI is a fixed value and cannot be modified.

NOTE: You can download the log for northbound portal interface from the controller web interface by navigating to **Administration** > **Diagnostics** > **Application Logs & Status**, as all other applications.

Table 4 lists the ports that must be opened on the network firewall to ensure that the controller and NBI can communicate with each other successfully.

Table 4.   Portal details

Port Number	Layer 4 Protocol	Source	Destination	Configurable from Web Interface?	Purpose
9080	HTTP	Any	Controller	No	Northbound Portal Interface for Hotspot
9443	HTTPS	Any	Controller	No	Northbound Portal Interface for Hotspot

Controller Web Interface Configuration

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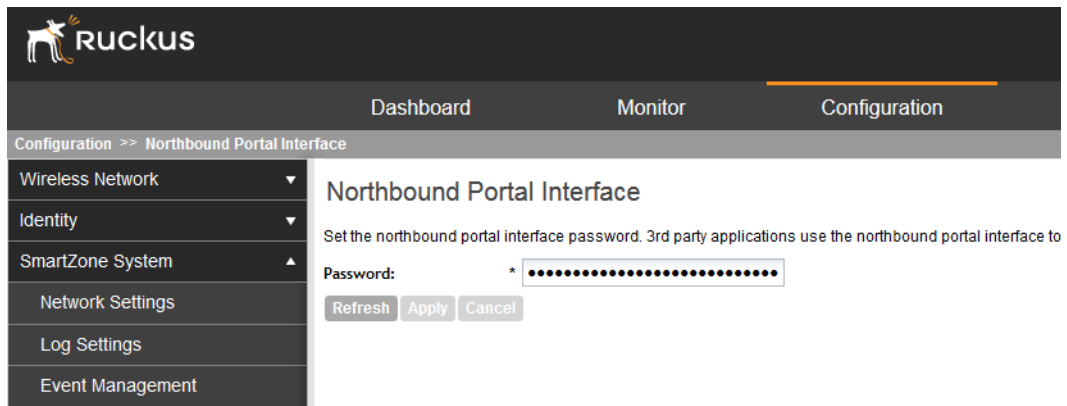
The northbound portal interface request password can be configured in the controller web interface by navigating to:

- For SZ 100: **Configuration** > **SmartZone System** > **General System Settings** > **Northbound Portal Interface**. See Figure 2.

- For vSZ-H: **Configuration** > **Virtual SmartZone System** > **General System Settings** > **Northbound Portal Interface**. See Figure 3.

The password in Figure 2 or in Figure 3 is a token to ensure that a portal has the permission to get the services from the northbound portal interface. It must be included in all JSON request as *RequestPassword* sent to NBI.

A web portal server must use the POST command to issue JSON requests. The controller will not accept a request with the GET request command.

Figure 2. Setting the password for SZ

Figure 3. Setting the password for vSZ-H

JSON Commands

2

In this chapter:

User Online Control

The northbound portal interface supports the following JSON commands:

- Login
- Login Async
- Status
- Logout
- Disconnect

These commands are used for user authentication, user status query, and terminating user sessions. For each command (JSON POST), both the UE-IP and UE-MAC may be included. Where both are present, the UE-MAC will be preferred.

The NBI decrypts the strings and returns the decrypted version within the response message. This is because the Captive Portal (CP) encrypts the IP and MAC address parameters in each redirection (See Table 10 for the full list of these pa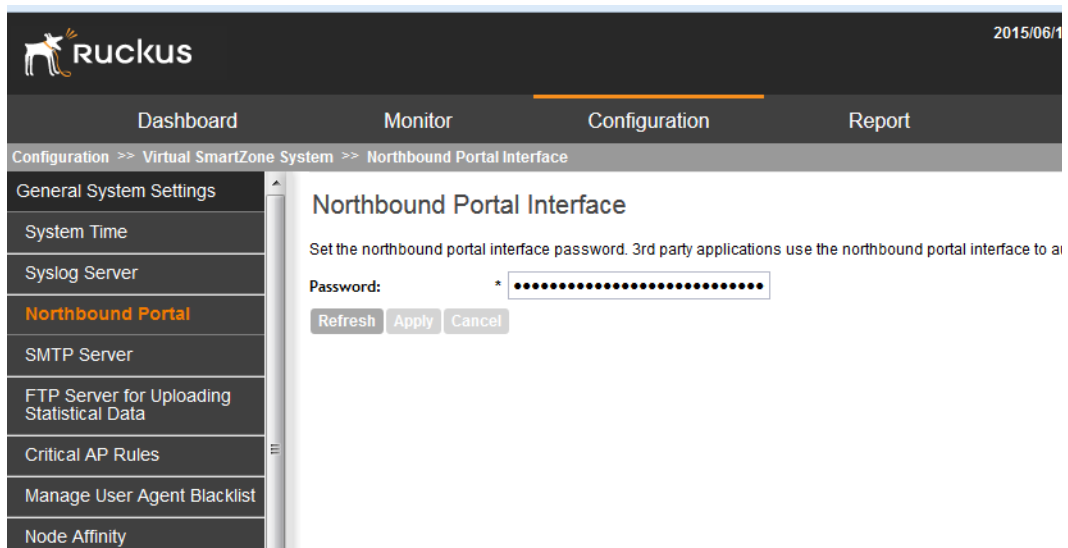rameters) to the subscriber portal. The controller decrypts the UE-IP and UE-MAC address before returning the response, by using the Encrypt and Decrypt API described in GetConfig section.

NOTE: Northbound Interface (NBI) expects to receive encrypted UE-IP and UE-MAC address (For example, ENC12bc24c4777703327f2e0aabbf6b9f9e) when the request category is UserOnlineControl. In the GetConfig request category you do not need to encrypt UE-IP and UE-MAC address (For example: 172.21.134.87)

Request Authentication - Asynchronous Login

In the hotspot (WISPr) WLAN use case, an unauthorized user is redirected to an external web portal server by the controller. Using the *asynchronous login* command (RequestType=LoginAsync), the external web portal server sends a request to the controller to authenticate the user using the RADIUS server. The external Web portal server receives the response - *202 Authentication pending,* while the controller performs the authentication in the background. It is the responsibility of the Web portal to poll the controller and fetch the authentication result. This action is performed using the status command (RequestType=Status).

NOTE: To use asynchronous APIs refer to Using Asynchronous API

The following is an example of the asynchronous login 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"
}
```

Table 5 lists the controller responses to these authentication requests.

NOTE: The user account *test* (UE username) mentioned in the above example, is created as an external user in the RADIUS server. The hotspot portal does not provide an interface for manipulating user account information.

Table 5.   Controller responses to authentication (asynchronous login) 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 controller internal error occurs.

Table 5.   Controller responses to authentication (asynchronous login) requests

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.
	• 306, Wrong request password: Response if the request password is mismatched.

Using Asynchronous API

When using the asynchronous API (RequestType = LoginAsync), NBI will always return a response as pending authentication. The client must send a status request (each X seconds/milliseconds) to check for the authentication result.

This is useful when using a smart device. The App in a smart device can query the login status periodically. It stores the user credentials in the background thereby reducing the user driven actions.

Request Authentication - Synchronous Login

The controller also provides a synchronous login blocking command (Request-Type=Login). In synchronous login command the external Web portal must wait for the authentication process to complete, which is usually processed by the RADIUS server. This could result in a delayed response if the controller is unable to get a response from the RADIUS server. 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 6 lists the controller responses to the synchronous login command.

Table 6.   Controller responses to a synchronous login 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 controller 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. • 306, Wrong request password: Response if the request password is mismatched.

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"
 }
```

Table 7 lists the controller responses to these user status query commands.

Table 7.   Controller 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.
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 controller internal error occurs. • 401, Radius server error: Response when a RADIUS connection error occurs or the connection request times out.

Table 7.   Controller responses to user status query

Response Type	Possible Responses
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. • 306, Wrong request password: Response if the request password is mismatched.

NOTE: If an authentication process has a result (not pending), the controller responds to it only once. For example, if the controller 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 controller 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 controller. In this case, the Web portal changes the status of the client from authenticated, to unauthenticated, forcing the user to login again. When un-authenticating a user, existing TCP sessions are not terminated and the UE is not disassociated from the AP. It only changes the status of the UE from authorized to unauthorized. The following is an example of 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 controller also provides a command for terminating user TCP (Transmission Control Protocol) connections from the AP (Access Point)). In other words, the disconnect command (RequestType=Disconnect) changes the status of the UE from authorized to unauthorized and also disassociates the UE from the AP.

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

Table 8 lists the controller response.

Table 8.   Controller responses to a disconnect command

Response Type	Possible Responses
Normal response	• 200, OK
	• 100, Client unauthorized: Response if the user is already unauthorized
Service error	• 300, Not found: Response if the lookup fails with given UE- MAC or the UE-IP address.
	• 400, Internal server error: Response when an controller internal error occurs.

Table 8.   Controller responses to a disconnect command

Response Type	Possible Responses
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. • 306, Wrong request password: Response if the request password is mismatched.

JSON Responses

3

In this chapter:

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

6 Decrypt

NOTE: It is recommended for new users to implement and use the new APIs - Encrypt and Decrypt. Existing users can continue using the legacy APIs - EncryptIP and DecryptIP provided; you have not made any changes to it during implementation on your portal server.

The first four commands are used for obtaining the different blade IP lists. The northbound portal interface simply responds with the control, cluster, management blade or user defined IP list of the controller. The following is an example of the GetConfig command:

```
{
 Vendor: "ruckus",
 RequestPassword: "myPassword",
 APIVersion: "1.0",
 RequestCategory: "GetConfig",
 RequestType: "ControlBladeIPList",
```

The following is an example of the success 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. By default, the encryption is enabled. To disable the encryption, use the CLI command:

```
ruckus(config)# [no] encrypt-mac-ip
```

NOTE: Refer to the CLI examples given below for enabling and disabling the IP and MAC address encryption.

```
{
 Vendor: "ruckus",
 RequestPassword: "myPassword",
 APIVersion: "1.0",
 RequestCategory: "GetConfig",
 RequestType: "Encrypt",
 Data: "172.21.134.87"
}
```

The following is an example of the success response:

```
{
    Vendor: "ruckus",
    ReplyMessage:"OK",
    ResponseCode:200,
    APIVersion:"1.0"
    Data: "ENC1234bfdbe5y5hbfdgh45y54ryt5y5th5"
}
```

Another example is the decrypt command, which returns a decrypted value of IP address.

```
{
    Vendor: "ruckus",
    RequestPassword: "myPassword", APIVersion: "1.0",
    RequestCategory: "GetConfig", RequestType: "Decrypt",
    Data: "ENC1234bfdbe5y5hbfdgh45y54ryt5y5th5"
}
```

The success response:

```
{
  Vendor:"ruckus", ReplyMessage:"OK", ResponseCode:200,
  APIVersion:"1.0"
  Data: "172.21.134.87"
}
```

The following are examples of using the CLI command for enabling and disabling the IP address and MAC address encryptions.

Enabling the IP address and MAC address encryption:

```
# show running-config encrypt-mac-ip
```

Disabling the IP address and MAC address encryption:

```
# config
(config)# no encrypt-mac-ip
Do you want to continue to disable (or input 'no' to
cancel)? [yes/no] yes
Successful operation
```

Confirming that the IP address and MAC address encryption is disabled:

```
(config)# do show running-config encrypt-mac-ip
Encryption MAC and IP: Disabled
```

JSON Responses

Table 9 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 LoginSync and LoginAsync)
- SQ: Status Query
- TU: Terminating User (Logout and Disconnect)
- GC: Get Config (Control Blade IP, Cluster Blade IP, Management Blade IP, User Interface IP, Encrypt and Decrypt)

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

Table 9.   JSON response definitions

Category	Code	Definition	Used In				
			UA	SQ	TU	EI	GC
Informational	100	Client unauthorized		•	•		
	101	Client authorized	•	•			
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					
	306	Wrong request password	•	•	•	•	•
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 9.

- Example: Client unauthorized
- Example: Client authorized
- 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: Wrong request password
- Example: Internal server error
- Example: RADIUS server error
- Example: Encrypt for MAC address
- Example: Decrypt 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: 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: Wrong request password

```
{
Vendor: "ruckus",
APIVersion: "1.0",
ResponseCode: "306",
ReplyMessage: "Wrong request password",
}
```

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",
ReplyMessage: "Radius server error",
}
```

Example: Encrypt for MAC address

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

Example: Decrypt for MAC address

```
{
Vendor: "ruckus",
RequestPassword: "myPassword",
APIVersion: "1.0",
RequestCategory: "GetConfig",
RequestType: "Decrypt",
Data: "ENC4782689566f8-
eac8aa30e276aa907f332d0bf93f9f60a7d8"
}
```

The success response:

```
{
Vendor:"ruckus", ReplyMessage:"OK",
ResponseCode:200,
APIVersion:"1.0"
Data: "04:4f:aa:32:25:f0"
}
```

WISPr Support for ZoneDirector Login

A

In this appendix:

- Customer Login
- Customer Logout

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

NOTE: This new API is provided since controller's official portal integration using JSON requests does not support ZD login API. Ruckus Wireless recommends 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 must change their login/logout URLs to match the new supported API.

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

NOTE: See Captive Portal Attributes for details.

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

  ```
  https://{sip-server-ip-address}:9998/login
  ```

  To:

  ```
  https://{sip-server-ip-address}:9998/Subscriber-
  Portal/hotspotlogin
  ```

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

NOTE: This login request should include the customer's login credentials such as the user name and password parameters. It is expected that the customer's portal also sends the following parameters from Captive Portal's redirection -

- url - the original URL which the user tried to browse
- proxy - if the UE browser is set to Web proxy
- uip - UE IP address
- client_mac - UE MAC IP address

Customer Logout

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

From:

```
https://{sip-server-ip-address}:9998/logout
```

To:

```
https://{sip-server-ip-address}:9998/Subscriber-
Portal/
hotspotlogout?uip=10.20.30.40
```

Captive Portal Attributes

B

In this appendix:

- Redirection Attributes

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 controller decrypts the UE-IP and UE-MAC address before returning the response, by using the Encrypt and Decrypt API described in the GetConfig section.

NOTE: Apple CNA works only for HTTP redirect. It will not work if the external portal is in HTTPS.

Redirection Attributes

Table 10 lists these parameters provided by the controller's captive portal redirection.

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

Table 10.   Redirection attributes

Attributes	Description
client_mac	Encrypted UE Mac address. NOTE: The format of the MAC Address is defined in the Hotspot (WISPr) Portal configuration.
dn	The domain name.
loc	AP location.
mac	AP Mac address.
proxy	The UE browser if it is set to the Web proxy.

Table 10.   Redirection attributes

Attributes	Description
reason	Reason for redirecting the WLAN. The value could either be: • Un-Auth-Captive – Regular unauthenticated UE redirected to Login Portal or • Un-Auth-SSL-Captive – In case of HTTPS, Captive Portal is performing a "double redirect". Adding this value to identify this flow.
nbilp	The IP of SCG/SZs Northbound Interface.
sip	The value could either be the: • FQDN of the uploaded SCG/SZ Web UI certificate if the uploaded certificate's common name is FQDN. • Concatenation of the SCG/SZ cluster name with the common name value after the wild card, if the uploaded certificate's common name is not FQDN (meaning if it includes wild card). For example, if the common name is "*.ruckuswireless.com" and the cluster name is "Cluster_Node1", then the sip will be "cluster_node1.ruckuswireless.com." • "scg.ruckuswireless.com", which is the FQDN of the self-signed certificate which SCG/SZ is packaged with, if the certificate was not uploaded at all.
ssid	The broadcasted SSID name.
startUrl	The URL as per the Hotspot configuration, which is to be redirected after successful login.
uip	Encrypted UE IP address.
url	Original URL which the customer tries browsing.
vlan	VLAN which the customer is set to
wlan	WLAN ID of the UE's associated the WLAN.
wlanName	SSIDs configured WLAN name

Table 10.   Redirection attributes

Attributes	Description
zoneId	In case of third party AP, this attribute will be included instead of WLAN and will include the zone ID where the SSID is configured in the controller.
zoneName	AP zone name of the UE's associated with the WLAN. WLANs configured Zone name. This name is used for Kumo. The value is encrypted based on a special key.

The Smart Client

C

In this appendix:

- The Smart Client

The Smart Client

The Smart Client is a software solution which resides on the user's access device that facilitates the user's connection to Public Access Networks, whether via a browser, signaling protocol or other proprietary method of access.

The XML is embedded in the HTML source code as a comment block as the following:

```
<html>
< head>
< meta http-equiv="content-type" content="text/html; charset=UTF-8">
< /head>
< body></body>
<!--<?xml version="1.0" encoding="utf-8"?>
{{{ The Embedded XML }}}
-->
</html>
```

Figure 4. Smart Client Example

Extract the embedded XML as the following.

<?xml version="1.0" encoding="utf-8"?>

<WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"xsi:noNamespaceSchemaLocation="http://
www.acmewisp.com/WISPAccessGatewayParam.xsd">

   <Redirect>

      <AccessProcedure>1.0</AccessProcedure>

      <AccessLocation></AccessLocation>

      <LocationName></LocationName>

      <LoginURL>https://scg.ruckuswireless.com:9998/SubscriberPortal/
WisprLogin?nbiIP=172.17.18.173&client_mac=ENCd67be23390a743c6095b
6635a31e93c19e2487fa83931d98&sip=scg.ruckuswire-
less.com&wlan=1&reason=Un-Auth-Captive&proxy=0&wlanName=RADI-
US_TEST&ssid=RADIUS_TEST&mac=8c:0c:90:2b:8b:90&dn=scg.ruckuswirel

ess.com&uip=ENCec4cc1fd0c146d5348cd4f1-
ba20ef459&zoneName=%5BB%40453f2d-
ba_1439953901413&url=http%3A%2F%2Fwww.google.com%2F</
LoginURL>

    <AbortLoginURL>https://scg.ruckuswireless.com:9998/SubscriberPortal/
AbortWisprLogin?nbiIP=172.17.18.173&client_mac=ENCd67be23390a743c6
095b6635a31e93c19e2487fa83931d98&sip=scg.ruckuswire-
less.com&wlan=1&reason=Un-Auth-Captive&proxy=0&wlanName=RADI-
US_TEST&ssid=RADIUS_TEST&mac=8c:0c:90:2b:8b:90&dn=scg.ruckuswirel
ess.com&uip=ENCec4cc1fd0c146d5348cd4f1-
ba20ef459&zoneName=%5BB%40453f2d-
ba_1439953901413&url=http%3A%2F%2Fwww.google.com%2F</
AbortLoginURL>

    <MessageType>100</MessageType>

    <ResponseCode>0</ResponseCode>

  </Redirect>

Example: Information on the redirection page

```
<?xml version="1.0" encoding="utf-8"?>
<WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:noNamespaceSchemaLocation="http://
www.acmewisp.com/WISPAccessGatewayParam.xsd">
<Redirect>
<AccessProcedure>1.0</AccessProcedure>
<AccessLocation></AccessLocation>
<LocationName></LocationName>
<LoginURL>https://sip:9998/SubscriberPortal/WisprLogin?nbiIP=<nbiIP>{& ...
other Redirection attributes in Table 11}</LoginURL>
<AbortLoginURL>https://sip:9998/SubscriberPortal/AbortWispr-
Login?nbiIP=<nbiIP>></AbortLoginURL>
<MessageType>100</MessageType>
<ResponseCode>0</ResponseCode>
</Redirect>
</WISPAccessGatewayParam>
```

NOTE: To do authentication. An HTTP POST request must be sent to the
<LoginURL> with the `UserName` and `Password` fields.

NOTE: The content type of request must be "application/x-www-form-
urlencoded".

Example: Authentication Request (HTTP)

```
POST /SubscriberPortal/WisprLogin?nbiIP=<nbiIP>
HTTP/1.1
Host: sip:9998
Content-Type: application/x-www-form-urlencoded
UserName=<UserName>&Password=<Password>
```

Example: Authentication Reply

```
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:noNamespaceSchemaLocation="http://
www.acmewisp.com/WISPAccessGatewayParam.xsd">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>201</ResponseCode>
<ReplyMessage>Authentication pending</ReplyMessage>
<LoginResultsURL>https://sip:9998/SubscriberPortal/
WisprStatus?nbiIP=<nbiIP></LoginResultsURL>
</AuthenticationReply>
</WISPAccessGatewayParam>
```

Example: Authentication Result (Login succeeded)

```
<?xml version="1.0"encoding="UTF-8"?>
<WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:noNamespaceSchemaLocation="http://
www.acmewisp.com/WISPAccessGatewayParam.xsd">
<AuthenticationPollReply>
<MessageType>140</MessageType>
<ResponseCode>50</ResponseCode>
<ReplyMessage>Login succeeded</ReplyMessage>
<LogoffURL>https://sip:9998/SubscriberPortal/WisprLogout?nbiIP=<nbiIP>
&UserName=<UserName>&Password=<Password></LogoffURL>
</AuthenticationPollReply>
</WISPAccessGatewayParam>
```

Example: Authentication Result (Login failed)

```
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:noNamespaceSchemaLocation="http://
www.acmewisp.com/WISPAccessGatewayParam.xsd">
```

```
<AuthenticationPollReply>
<MessageType>140</MessageType>
<ResponseCode>100</ResponseCode>
<ReplyMessage>Login failed</ReplyMessage>
</AuthenticationPollReply>
</WISPAccessGatewayParam>
```

Example: Logoff Reply

```
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:noNamespaceSchemaLocation="http://
www.acmewisp.com/WISPAccessGatewayParam.xsd">
<LogoffReply>
<MessageType>130</MessageType>
<ResponseCode>150</ResponseCode>
</LogoffReply>
</WISPAccessGatewayParam>
```

User Defined Interface

D

In this appendix:

- NBI and UDI

NBI and UDI

AP uses the control interface to communicate with the controller regarding its configuration. To have a logical separation of UE traffic from the AP control traffic the administrator can create an UDI (User Defined Interface).

In case the UDI (using control interface, physical interface and hotspot service as shown in Figure 5) is configured, the AP uses it to DNAT unauthorized UE requests to the controller's captive portal (otherwise the AP uses the control interface).

Figure 5. Using UDI

	Name	Physical Interface	Service
☐	UDI	Control Interface	Hotspot

The controller's captive portal redirects the UE to the configured portal login page URL. When the UE triggers this portal URL request, the AP will let it go through (it will not DNAT to the controller's captive portal), as it is configured as ACL in the AP, direct to the external portal server.

The external portal communicates with the controller's NBI for status/login/logout requests. The interfaces external portal can communicate are the interfaces NBI listens to. NBI is bound by default to the controller's control and management interfaces.

In addition, the administrator can configure the UDI interface, which NBI will bind as well. This UDI for NBI can be the same UDI which AP DNAT to the controller's captive portal, or others using control or management physical interfaces and whatever service (hotspot/not specified) as in Figure 6. To define UDI on the controller web interface, navigate to:

- For SZ 100: **Configuration** > **SmartZone System** > **Network Settings** > **existing Cluster Node > User Defined Interface.**

- For vSZ-H: **Configuration** > **Virtual SmartZone System** > **Cluster & Planes** > **Cluster Plane > existing Control Plane > User Defined Interface.**

Figure 6. UDI Physical Interface

Name	Physical Interface		Service
UDI1	Management Interface	⌄	Not Specified
UDI2	Control Interface	⌄	Hotspot

Figure 7 describes the request flows per interface.

Figure 7.   .Request flows per interface
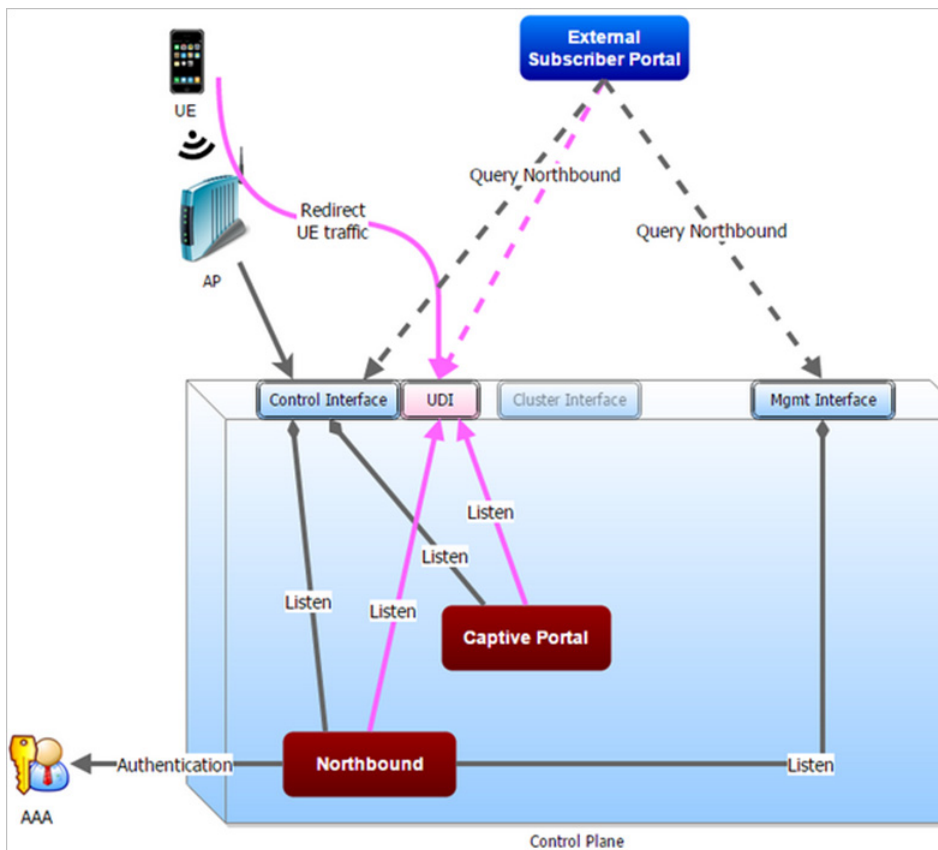
Index

A

aPI 37
asynchronous login 15
authentication 9
authentication pending 31
authentication request 19
authorized 20

B

bad request 32
blocking command 17

C

category not supported 33
client authorized 29
client error 27
client unauthorized 29
client_mac 40
cluster blade IP list 24
cluster management blade 24
command not supported 33
control 24
control blade IP list 24

D

decrypt 24, 25
decrypt for MAC address 35
disconnect command 21
dn 40

E

encrypt 24
encrypt for MAC address 34
external portal 37

G

general error 18, 20, 22
get config 24, 26

H

hotspot 37
hotspot services 9

I

informational 27
internal server error 34

J

jSON response examples 27
jSON responses 26

L

loc 40
login 37
login failed 20, 32
login succeeded 20, 31
logout 38

M

mac 40
management blade IP list 24

N

nbilp 41
normal response 18, 21
northbound portal interface 11
not found 32

O

overview 9

P

password 11
pending authentication 19
portal logon 37
pOST 12
proxy 40

Q

querying a user status 18