

Ruckus SmartZone 100 and Virtual SmartZone-Essentials Hotspot WISPr Reference Guide, 5.1.2

Supporting SmartZone 5.1.2

Copyright, Trademark and Proprietary Rights Information

© 2019 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface.....	5
Document Conventions.....	5
Notes, Cautions, and Warnings.....	5
Command Syntax Conventions.....	6
Document Feedback.....	6
Ruckus Product Documentation Resources.....	6
Online Training Resources.....	7
Contacting Ruckus Customer Services and Support.....	7
What Support Do I Need?.....	7
Open a Case.....	7
Self-Service Resources.....	7
About This Guide.....	9
Overview.....	9
Terminology.....	9
Web Interface Configuration Overview.....	11
Overview.....	11
Creating Non-Proxy Authentication AAA Servers for Standby Cluster.....	12
Testing AAA Server (Auth).....	15
Creating Proxy AAA Servers for Standby Cluster.....	15
RADIUS Service Options.....	18
Testing AAA Servers.....	20
Creating Proxy Accounting AAA Servers for Standby Cluster.....	21
Creating a Hotspot (WISPr) Portal.....	22
Creating a WLAN Configuration (WISPr).....	25
Request Format.....	28
Controller Web Interface Configuration.....	29
JSON Commands - User Online Control.....	31
Overview.....	31
Request Authentication - Asynchronous Login.....	31
Using Asynchronous API.....	32
Request Authentication - Synchronous Login.....	33
Querying a User Status.....	34
Terminating a User Session.....	35
Disconnect Command.....	35
Querying Enrichment Information.....	36
JSON Responses.....	37
JSON Responses - GetConfig	37
JSON Responses Definitions.....	38
JSON Response Examples.....	39
WISPr Support for ZoneDirector Login.....	43
WISPr Support for ZoneDirector Login Overview.....	43
Web Page Setup.....	44
Captive Portal Attributes.....	47

Captive Portal Attributes Overview.....	47
The Smart Client.....	49
The Smart Client Overview.....	49
Example: Information on the redirection page.....	51
Example: Authentication Request (HTTP).....	51
Example: Authentication Reply.....	51
Example: Authentication Result (Login succeeded).....	52
Example: Authentication Result (Login failed).....	52
Example: Logoff Reply.....	52
User Defined Interface.....	53
User Defined Interface Overview.....	53
NBI and UDI.....	53
WISPr Portal Details.....	55
WISPr Portal Details Overview.....	55
Certificate Warning.....	57
Certificate Warning Overview.....	57

Preface

- Document Conventions..... 5
- Command Syntax Conventions..... 6
- Document Feedback..... 6
- Ruckus Product Documentation Resources..... 6
- Online Training Resources..... 7
- Contacting Ruckus Customer Services and Support..... 7

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	<code>device(config)# interface ethernet 1/1/6</code>
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the Start menu, click All Programs .
<i>italics</i>	Publication titles	Refer to the <i>Ruckus Small Cell Release Notes</i> for more information.

Notes, Cautions, and Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document Feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

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

For example:

- Ruckus SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

Ruckus Product Documentation Resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at <https://support.ruckuswireless.com/documents>. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a Ruckus Support Portal user account. Other technical documentation content is available without logging in to the Ruckus Support Portal.

White papers, data sheets, and other product documentation are available at <https://www.ruckuswireless.com>.

Online Training Resources

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

Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Ruckus Support Portal using <https://support.ruckuswireless.com>, or go to <https://www.ruckuswireless.com> and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The Ruckus Support Portal at <https://support.ruckuswireless.com> offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—<https://support.ruckuswireless.com/documents>

Preface

Contacting Ruckus Customer Services and Support

- Community Forums—<https://forums.ruckuswireless.com/ruckuswireless/categories>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—<https://support.ruckuswireless.com/security>

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

About This Guide

- Overview..... 9
- Terminology..... 9

Overview

This SmartZone™ (SZ) 100 and Virtual SmartZone Essentials (vSZ-E) 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 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 support web site at <https://support.ruckuswireless.com/contact-us>.

Terminology

The table lists the terms used in this guide.

TABLE 2 Terms used in this guide

Terminology	Description
AP	Access Point
CP	Captive Portal
MSP	Managed Service Provider
NBI	Northbound Interface
SZ100 / vSZ-E	The controller platform
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDI	User Define Interface
UE	User Equipment
UE-IP	User Equipment - IP Address
UE-MAC	User Equipment - MAC Address

Web Interface Configuration Overview

- Overview..... 11
- Creating Non-Proxy Authentication AAA Servers for Standby Cluster..... 12
- Creating Proxy AAA Servers for Standby Cluster..... 15
- Creating Proxy Accounting AAA Servers for Standby Cluster..... 21
- Creating a Hotspot (WISPr) Portal..... 22
- Creating a WLAN Configuration (WISPr)..... 25
- Request Format..... 28
- Controller Web Interface Configuration..... 29

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.

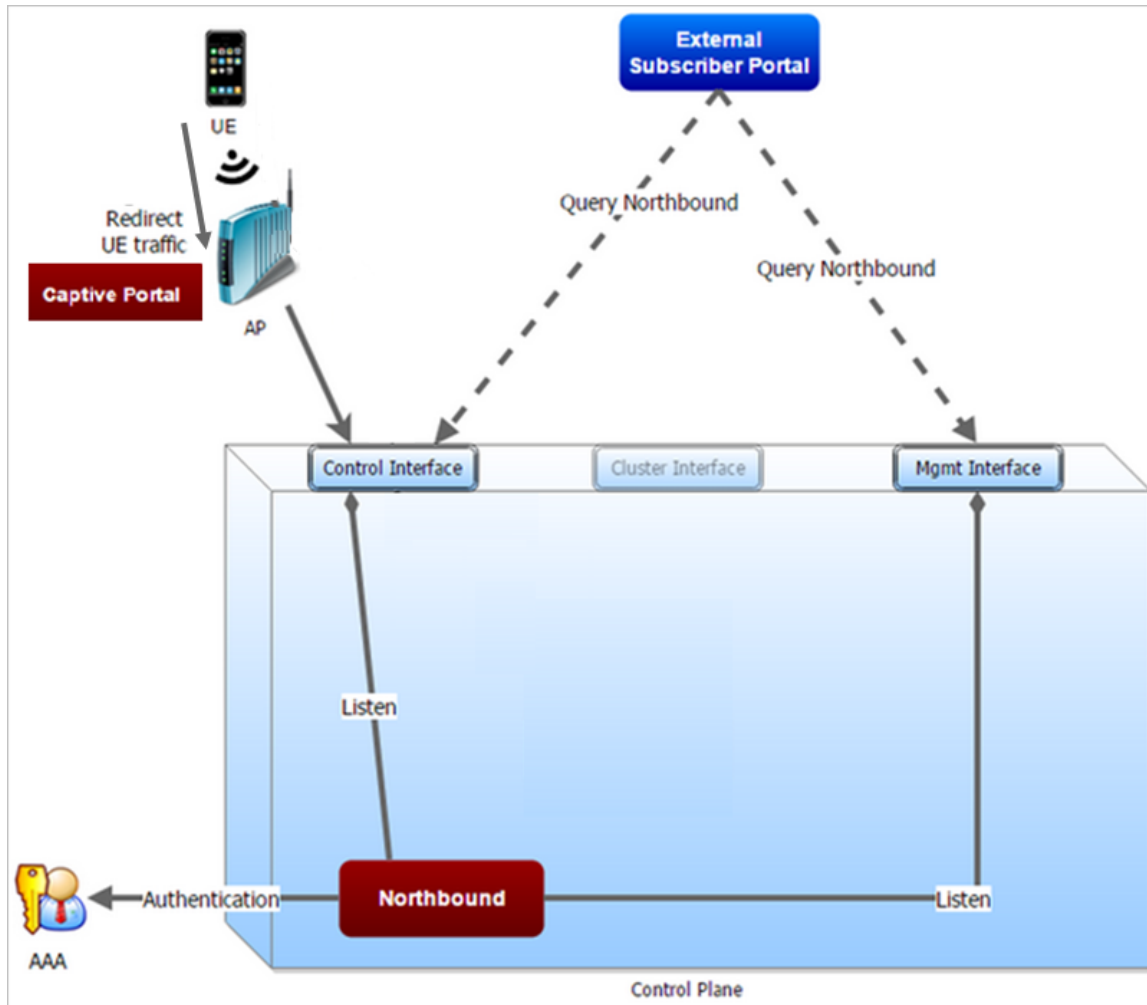
The following are the hotspot components and their roles in the hotspot portal as seen in the Figure

- 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: 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: It 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: It is responsible for authenticating the UE through the UE's login credentials (username and password).

NOTE

Refer to appendix [WISPr Portal Details Overview](#) on page 55 for IPv4 and IPv6 protocol support for GRE tunnels.

FIGURE 1 Hotspot portal components



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

NOTE

Refer to [Overview](#) on page 9 chapter for conventions used in this guide.

Creating Non-Proxy Authentication AAA Servers for Standby Cluster

A non-proxy AAA server is used when the APs connect to the external AAA server directly.

1. Go to **Services & Profiles > Authentication**.
2. Select the **Non-Proxy (AP Authenticator)** tab, and then select the zone for which you want to create the AAA server.

3. Click **Create**.
The **Create AAA Server** page is displayed.

FIGURE 2 Creating an AAA Server

Create AAA Server [Close]

General Options

Name:

Description:

Type: RADIUS Active Directory LDAP

ClusterRedundancy: OFF Enable Service for Standby Cluster

Backup RADIUS: OFF Enable Secondary Server

OK Cancel

4. Configure the following:
 - a. General Options
 - Name: Type a name for the AAA server that you are creating.
 - Description: Type a short description of the AAA server.
 - Type: Select the type of AAA server that you are creating. Options include RADIUS, Active Directory and LDAP.
 - Cluster Redundancy: Select the **Enable Service for Standby Cluster** option to enable cluster redundancy.
 - Backup RADIUS (appears if you clicked RADIUS above): Select the **Enable Secondary Server** check box if a secondary RADIUS server exists on the network.
 - Global Catalog (appears if you clicked Active Directory above): Select the **Enable Global Catalog support** if you the Active Directory server to provide a global list of all objects.
 - b. Primary Server
 - If you selected RADIUS, configure the following options in the Primary Server section:
 - IP Address: Type the IP address of the AAA server. Both IPv4 and IPv6 addressing formats are supported.
 - Port: Type the port number of the AAA server. The default RADIUS server port number is 1812.
 - Shared Secret: Type the AAA shared secret.
 - Confirm Secret: Retype the shared secret to confirm.

If you have enabled **Backup RADIUS** to the **Secondary Server**, you must provide similar information as in the primary server.

See [RADIUS Service Options](#) on page 18 for more information.
 - If you selected Active Directory, configure the following options in the Primary Server section:
 - IP Address: Type the IPv4 address of the AD server.
 - Port: Type the port number of the AD server. The default port number (389) should not be changed unless you have configured the AD server to use a different port.
 - Windows Domain Name: Type the Windows domain name assigned to the AD server (for example, domain.ruckuswireless.com).
 - If you selected LDAP, configure the following options:
 - IP Address: Type the IPv4 address of the LDAP server.
 - Port: Type the port number of the LDAP server. Default is 389.
 - Base Domain Name: Type the base DN in LDAP format for all user accounts (for example, dc=ldap,dc=com).
 - Admin Domain Name: Type the admin DN in LDAP format (for example, cn=Admin;dc=<Your Domain>,dc=com).
 - Admin Password: Type the administrator password for the LDAP server.
 - Confirm Password: Retype the administrator password to confirm.
 - Key Attribute: Type a key attribute to denote users (for example, default: uid)
 - Search Filter: Type a search filter (for example, objectClass=Person).
5. Under **User Role Mapping**, click **Create** to create a user traffic profile mapping.
 - a) In the **Group Attribute Value** field, enter the value.
 - b) Select a user role from the **User Role** list or click **+** to create a user role. For more information, refer to **Creating a User Role** section in the Administration guide.
6. Click **OK**.

You have completed creating a Non-proxy AAA server.

NOTE

You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Non-Proxy (AP Authenticator)** tab.

Testing AAA Server (Auth)

To ensure that the controller administrators will be able to authenticate successfully with the RADIUS server type that you selected, Ruckus strongly recommends testing the AAA server after you set it up.

The test queries the RADIUS server for a known authorized user and return groups associated with the user that can be used for configuring roles within the controller.

1. Go to **Services & Profiles > Authentication**.
2. Select the **Non-Proxy (AP Authenticator)** tab, and then select the zone for which you want to test the AAA server.
3. Click **Test AAA**.

The **Test AAA Server** page appears.

4. Configure the following:
 - a. Name: Select one of the AAA servers that you previous created.
 - b. User Name: Type an existing user name on the AAA server that you selected.
 - c. Password: Type the password for the user name you specified.
5. Click **Test**.

If the test was unsuccessful, there are two possible results (other than success) that will be displayed to inform you if you have entered information incorrectly: **Admin invalid** or **User name or password invalid**. These results can be used to troubleshoot the reasons for failure to authenticate administrators with an AAA server through the controller.

You have completed testing the non-proxy AAA servers that you created.

Creating Proxy AAA Servers for Standby Cluster

A proxy AAA server is used when APs send authentication/accounting messages to the controller and the controller forwards these messages to an external AAA server.

1. Go to **Services & Profiles > Authentication**.
2. Select the **Proxy (SZ Authenticator)** tab, and then select the zone for which you want to create the AAA server.

3. Click **Create**.
The **Create Authentication Service** page appears.

FIGURE 3 Creating an Authentication Service

Create Authentication Service ✕

Name:

Friendly Name:

Description:

Service Protocol: RADIUS Active Directory LDAP

ClusterRedundancy: OFF Enable Service for Standby Cluster

RADIUS Service Options

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

Primary Server

IP Address:

Port:

Shared Secret:

Confirm Secret:

Primary Server (Standby Cluster)

4. Configure the following:
 - a. Name: Type a name for the authentication service that you are adding.
 - b. Friendly Name: Type an alternative name that is easy to remember.
 - c. Description: Type a description for the authentication service.
 - d. Service Protocol: If you select
 - RADIUS, see [RADIUS Service Options](#) on page 18 for more information.
 - Active Directory, configure the following:
 1. Global Catalog: Select the **Enable Global Catalog** support if you the Active Directory server to provide a global list of all objects.
 2. Primary Server:
 - Encryption: Select the **Enable TLS Encryption** check box if you want to use the *Transport Layer Security* (TLS) protocol to secure communication with the server.

NOTE

You must also configure the Trusted CA certificates to support TLS encryption.

3. IP Address: Type the IPv4 address of the AD server.
4. Port: Type the port number of the AD server. The default port number (389) should not be changed unless you have configured the AD server to use a different port.
5. Windows Domain Name: Type the Windows domain name assigned to the AD server (for example, domain.ruckuswireless.com).
- LDAP, configure the following:
 1. Select the **Enable TLS Encryption** check box if you want to use the *Transport Layer Security* (TLS) protocol to secure communication with the server.

NOTE

You must also configure the Trusted CA certificates to support TLS encryption.

2. IP Address: Type the IPv4 address of the LDAP server.
 3. Port: Type the port number of the LDAP server.
 4. Base DN: Type the base DN in LDAP format for all user accounts (for example, dc=ldap,dc=com).
 5. Admin DN: Type the admin DN in LDAP format (for example, cn=Admin;dc=<Your Domain>,dc=com).
 6. Admin Password: Type the administrator password for the LDAP server.
 7. Confirm Password: Retype the administrator password to confirm.
 8. Key Attribute: Type a key attribute to denote users (for example, default: uid)
 9. Search Filter: Type a search filter (for example, objectClass=Person).
- e. Cluster Redundancy: Click the **Enable Service for Standby Cluster** option to enable cluster redundancy.
 - f. Advanced Options - Domain name: Type the whitelisted domain name that you want to add.
 - g. User Traffic Profile Mapping:
 1. Type a **Group Attribute Value**.
 2. Select a **User Role** from the drop-down list.
 3. Click **Add**.The mapped user profile is listed.

5. Click **OK**.

You have completed creating a Proxy AAA server.

NOTE

You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Proxy (SZ Authenticator)** tab.

RADIUS Service Options

These are the Radius service options available for the primary and secondary servers.

RFC 5580 Out of Band Location Delivery: If you want out-of-band location delivery (RFC 5580) to apply only to Ruckus APs, select the **Enable for Ruckus AP Only** check box.

Configure the primary RADIUS server settings as shown in the following table.

Configure the primary RADIUS server settings.

TABLE 3 Primary Server Options

Option	Description
IP Address	Type the IP address of the RADIUS server. IPv4 and IPv6 addressing formats are supported.
Port	Type the port number of the RADIUS server. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
Shared Secret	Type the RADIUS shared secret.
Confirm Secret	Retype the shared secret to confirm.

If you have a secondary RADIUS server on the network that you want to use as a backup, select the Enable Secondary Server check box, and then configure the settings in the following table.

TABLE 4 Secondary Server Options

Option	Description
Backup RADIUS	Select Enable Secondary Server . When a secondary RADIUS server is enabled and the primary RADIUS server becomes unavailable, the secondary Automatic Fallback Disable server takes over the handling of RADIUS requests. When the primary server becomes available again, it takes back control over RADIUS requests from the secondary server. If you want to prevent the primary server from retaking control over RADIUS requests from the secondary server, select the Automatic Fallback Disable check box.
IP Address	Type the IP address of the secondary AAA server. IPv4 and IPv6 addressing formats are supported.
Port	Type the port number of the secondary AAA server port number. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
Shared Secret	Type the AAA shared secret.
Confirm Secret	Retype the shared secret to confirm.

The following options define the health monitoring settings of the primary and secondary RADIUS servers, when the controller is configured as RADIUS proxy for RADIUS Authentication and Accounting messages.

TABLE 5 Health Check Policy

Option	Description
Response Window	<p>Set the time (in seconds) after which, if the AAA server does not respond to a request, the controller will initiate the zombie period (see below). Response Window</p> <p>If the primary AAA server does not respond to RADIUS messages sent after Response Window expires, the controller will forward the retransmitted RADIUS messages to the secondary AAA server.</p> <p>NOTE The zombie period is not started immediately after the Response Window expires, but after the configured Response Window plus $\frac{1}{4}$ of the configured Zombie Period. The default Response Window is 20 seconds</p>
Zombie Period	<p>Set the time (in seconds) after which, if the AAA server does not respond to ANY packets during the zombie period, it will be considered to inactive or unreachable.</p> <p>An AAA server that is marked zombie (inactive or unreachable) will be used to proxy with a low priority. If there are other live AAA servers, the controller will attempt to use these servers first instead of the zombie AAA server.</p> <p>The controller will only proxy requests to a zombie server only when there are no other live servers. Any request that is sent as a proxy to an AAA server will continue to be sent to that AAA server until the home server is marked inactive or unreachable. At that point, the request will fail over to another server, if a live AAA server is available. The default Zombie Period is 40 seconds.</p>
Revive Interval	<p>Set the time (in seconds) after which, if no RADIUS messages are sent as proxy to the AAA server after it has been marked as inactive or unreachable, the controller will mark the AAA server as active again (and assume that it has become reachable again). The default Revive Interval is 120 seconds.</p>
No Response Fail	<p>Click Yes to respond with a reject message to the NAS if no response is received from the RADIUS server. Click No to skip sending a response.</p>

NOTE

To ensure that the RADIUS fail-over mechanism functions correctly, either accept the default values for the Response Window, Zombie Period, and Revive Interval, or make sure that the value for Response Window is always higher than the value for RADIUS NAS request timeout multiplied by the value for RADIUS NAS max number of retries. For third party APs, you must ensure that the configured Response Window on the controller is higher than the RADIUS NAS request timeout multiplied by the RADIUS value. The maximum number of retries is configured at the 3rd party controller/AP.

Configure the following options.

TABLE 6 Rate Limiting

Options	Description
Maximum Outstanding Requests (MOR)	<p>Set the maximum outstanding requests per server. Type 0 to disable it, or set a value between 10 and 4096.</p>
Threshold (% of MOR)	<p>Set a percentage value of the MOR at which (when reached) the controller will generate an event. Threshold (% of MOR)</p> <p>For example, if the MOR is set to 1000 and the threshold is set to 50%, the controller will generate an event when the number of outstanding requests reaches 500.</p>

TABLE 6 Rate Limiting (continued)

Options	Description
Sanity Timer	Set a timer (in seconds) that will be started whenever a condition that generates an event is reached. This helps prevent conditions that trigger events which occur frequently.

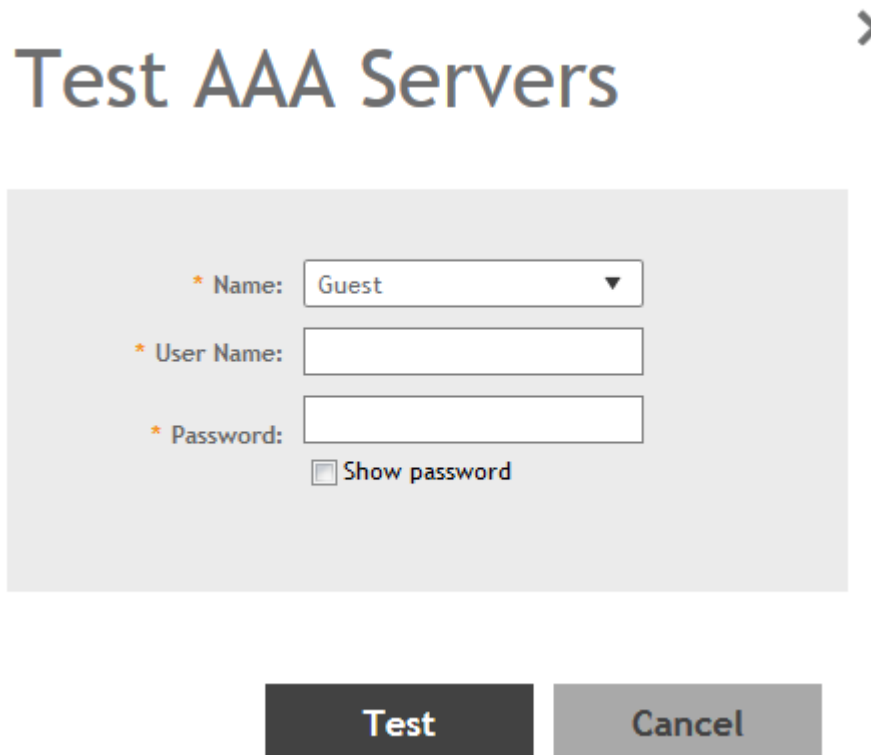
Testing AAA Servers

To ensure that the controller administrators will be able to authenticate successfully with the RADIUS server type that you selected, Ruckus strongly recommends testing the AAA server after you set it up.

1. Go to **Services & Profiles > Authentication**.
2. Select the **Proxy (SZ Authenticator)** tab, and then select the zone for which you want to test the AAA server.
3. Click **Test AAA**.

The **Test AAA Server** page appears.

FIGURE 4 Testing an AAA Server



4. Configure the following:
 - a. Name: Select one of the AAA servers that you previously created.
 - b. User Name: Type an existing user name on the AAA server that you selected.
 - c. Password: Type the password for the user name you specified.

5. Click **Test**.

If the controller was able to connect to the authentication server and retrieve the configured groups/attributes, the information appears at the bottom of the page. If the test was unsuccessful, there are two possible results (other than success) that will be displayed to inform you if you have entered information incorrectly: **Admin invalid** or **User name or password invalid**. These results can be used to troubleshoot the reasons for failure to authenticate administrators with an AAA server through the controller.

Creating Proxy Accounting AAA Servers for Standby Cluster

A proxy AAA server is used when APs send authentication/accounting messages to the controller and the controller forwards these messages to an external AAA server.

1. Go to **Services & Profiles > Accounting**.
2. Select the **Proxy** tab, and then select the zone for which you want to create the AAA server.
3. Click **Create**.

The **Create Accounting Service** page appears.

FIGURE 5 Creating an Accounting Service

The screenshot shows the 'Create Accounting Service' dialog box. At the top, there is a title bar with a close button (X). The form contains the following elements:

- Name:** A text input field.
- Description:** A text input field.
- Service Protocol:** A radio button selected for **RADIUS Accounting**.
- Cluster Redundancy:** A toggle switch set to **OFF** with the text 'Enable Service for Standby Cluster' next to it.
- RADIUS Service Options:** A section containing:
 - A dropdown menu currently showing **Primary Server**.
 - IP Address:** A text input field.
 - Port:** A text input field containing the value **1813**.
 - Shared Secret:** A text input field.
 - Confirm Secret:** A text input field.
 - A second dropdown menu at the bottom of this section showing **Primary Server (Standby Cluster)**.

At the bottom right of the dialog, there are two buttons: **OK** and **Cancel**.

4. Configure the following:
 - a. Name: Type a name for the authentication service that you are adding.
 - b. Description: Type a description for the authentication service.
 - c. Service Protocol: By default, the RADIUS Accounting selected. For more information, see [RADIUS Service Options](#) on page 18.
 - d. Cluster Redundancy: Click the **Enable Service for Standby Cluster** option to enable cluster redundancy.
5. Click **OK**.

You have completed creating a Proxy Accounting AAA server.

For information on how to test this server, see [Testing AAA Servers](#) on page 20

NOTE

You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Proxy** tab.

Creating a Hotspot (WISPr) Portal

To create a hotspot service, you must define the required basic settings.

SZ supports only one grace period, session timeout, UTP, VLAN and all UE session related configuration. These configurations for the first WLAN do not work when the UE joins the second WLAN. The configuration works only when the UE roams within the cluster node. The configurations do not work when the client roams from one zone to another zone or from one cluster to another cluster.

Before creating a hotspot, you need to create a user defined interface.

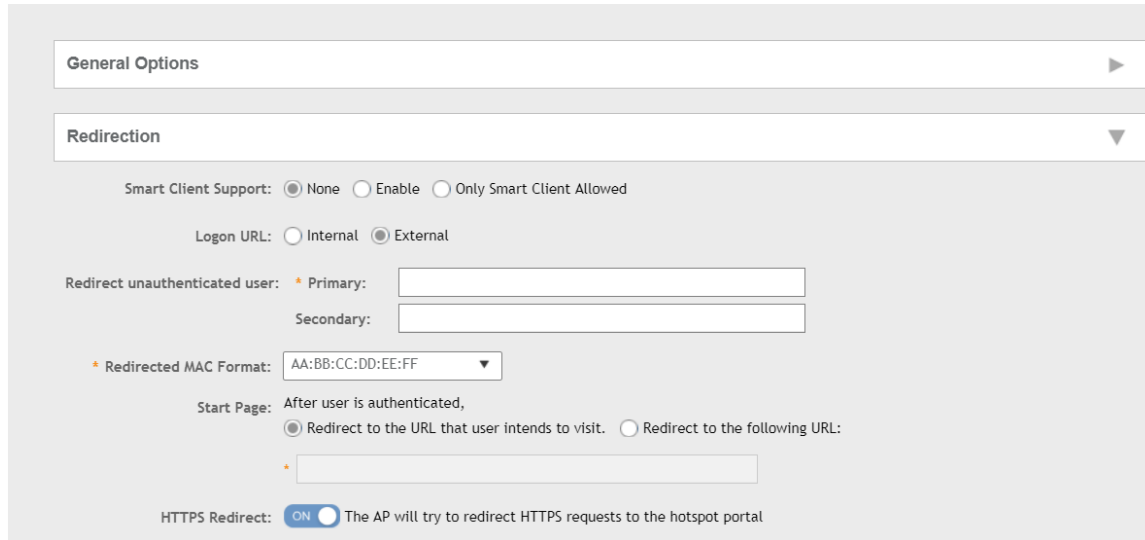
1. Go to **Services & Profiles > Hotspots & Portals**.
2. Select the **Hotspot (WISPr)** tab, and then select the zone for which you want to create the portal.

3. Click **Create**.

The **Create Hotspot (WISPr) Portal** page appears.

FIGURE 6 Creating a Hotspot (WISPr) Portal

Create Hotspot Portal



The screenshot shows the 'Create Hotspot Portal' configuration page. It features two main sections: 'General Options' and 'Redirection'. The 'Redirection' section is expanded, revealing the following settings:

- Smart Client Support:** Radio buttons for None, Enable, and Only Smart Client Allowed.
- Logon URL:** Radio buttons for Internal and External.
- Redirect unauthenticated user:** Two text input fields labeled 'Primary' and 'Secondary'.
- Redirected MAC Format:** A dropdown menu showing 'AA:BB:CC:DD:EE:FF'.
- Start Page:** A label 'After user is authenticated,' followed by radio buttons for Redirect to the URL that user intends to visit. and Redirect to the following URL: with an associated text input field.
- HTTPS Redirect:** A toggle switch labeled 'ON' with the text 'The AP will try to redirect HTTPS requests to the hotspot portal'.

4. Under **General Options**, enter portal name and portal description.

5. Under **Redirection**, select where to redirect the user after successful authentication.
 - a. For **Smart Client Support**, select one of the following options:
 - **None**: Disables Smart Client Support on the hotspot service.
 - **Enable**: Enables Smart Client Support.
 - **Only Smart Client Allowed**: Allows only Smart Clients to connect to the hotspot service.
 - b. For **Logon URL**, select one of the following options:
 - **Internal**: Indicates the internal URL of the subscriber portal (where hotspot users can log in to the service).
 - **External**: Indicates the external URL of the subscriber portal.

Selecting **External** provides an option to reroute an unauthorized user to a primary location. You can set the primary location in **Redirect unauthenticated user**. If an unauthorized user is rerouted, the AP redirects the UE to a backup portal.

The AP subscriber portal supports ZD-style API to login and logout. A customer can use AP IP address to submit the login or logout request.
 - **Redirect unauthenticated user**: APs can perform WISPr redirection. Native WISPr support is available on SZ-managed APs even if access to SZ is not available. It supports external portal redirection with survivability when APs cannot reach the centralized SZ. It also supports backup portal redirection if primary portal is down. The WISPr authentication load can be distributed to AP or use an AP as a WISPr authentication backup.

WISPr redirection and survivability is supported only on Ruckus 11AC Wave 1 and later APs. Only ZD-style external WISPr is supported. No NBI is supported for backup.

 - Primary: Redirects an unauthenticated user to a specified URL for authentication.
 - Secondary: Redirects an unauthenticated user to the backup external portal if the primary URL is down. The AP periodically accesses the primary portal URL to detect and check the availability of the primary URL.
6. Under **User Session**, set the session timeout and grace period.
 - **Session Timeout**: Sets a time limit (in minutes) after which users will be disconnected from the hotspot service and required to log in again.
 - **Grace Period**: Sets the time period (in minutes) during which disconnected users are allowed access to the hotspot service without logging in again.

NOTE

An AP and the primary portal must be in the same VLAN for the AP to access the primary portal.

- In the **Redirected MAC Format** field, enter the format of the redirection MAC address.
- For **Start Page**, select one of the following options:
 - **Redirect to the URL that the user intends to visit**: Redirects users to the page that they want to visit.
 - **Redirect to the following URL**: Sets a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address to be redirected.
- Enable **HTTPS Redirect** if you want the AP to redirect HTTPS requests to the hotspot portal. HTTPS requests are dropped if this option is disabled.

7. Under **Location Information**, set the location ID and location name.
 - a. In **Location ID**, enter the ISO and ITU country and area code that the AP includes in accounting and authentication requests. The code includes the following requirements:
 - **isocc** (ISO-country-code): The ISO country code that the AP includes in RADIUS authentication and accounting requests.
 - **cc** (country-code): The ITU country code that the AP includes in RADIUS authentication and accounting requests.
 - **ac** (area-code): The ITU area code that the AP includes in RADIUS authentication and accounting requests.
 - **network**: Name of the network.The following example illustrates a proper location ID entry: `isocc=us,cc=1,ac=408,network=Ruckus`
 - b. For **Location Name**, enter the name of the location of the hotspot service.
8. Under **Walled Garden**, click **Add** to add a user to a walled garden and provide access.
9. Click **Import CSV** to import the CSV file with the user information.
10. Select **Traffic Class Profile** and click + to create a traffic class profile. Refer to **Creating a Traffic Class Profile** section in the Administration guide.
11. Under **Advanced Options**, select the required options:
 - a. Click **Use Token Redirect URL** and enter a signature signing key.
 - b. Click **Enable Internal Node** and enter the internal node.

NOTE

If an **Internal node** is enabled, then only one IP is used and the IP domain name and IP ranges are not supported.

12. Click **OK**.

You have completed creating a Hotspot (WISPr) portal.

NOTE

If **Traffic Class Profile** or **Use Token Redirect URL** is enabled, **Smart Client Support** is set to **None**.

NOTE

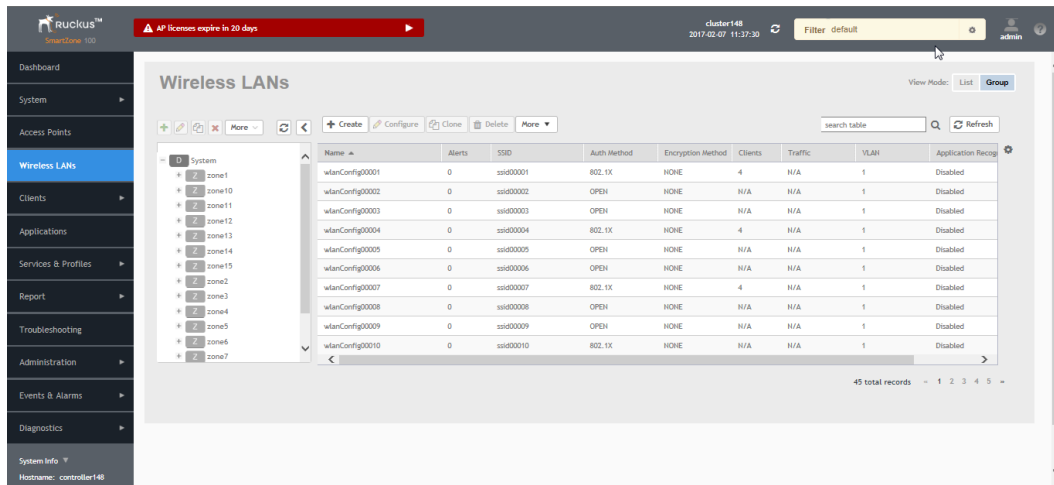
You can also edit, clone, and delete a Hotspot (WISPr) portal by selecting the **Configure**, **Clone**, and **Delete** options respectively from the **Hotspot (WISPr)** tab.

Creating a WLAN Configuration (WISPr)

To create a WLAN configuration:

1. In the Wireless LANs page, from the **System** tree hierarchy, select the **Zone** where you want to create a WLAN.

FIGURE 7 Wireless LANs



2. Click **Create**. The **Create WLAN Configuration** page is displayed.

FIGURE 8 Creating a WLAN Configuration

Create WLAN Configuration

3. Set the required configurations as explained in the below table.
4. Click **OK**.

TABLE 7 WLAN Configurations

Field	Description	Your Action
General Options		
Name	Indicates the user-friendly administrative name for the WLAN.	Enter a name.

TABLE 7 WLAN Configurations (continued)

Field	Description	Your Action
SSID	Indicates the SSID for the WLAN.	Enter the SSID
Authentication Options		
Authentication Type	<p>Defines the type of authentication flow for the WLAN.</p> <p>NOTE Authentication types such as WeChat, Web Authentication and Guest Access are not supported by APs in IPv6 mode.</p>	<p>Hotspot (WISPr)—Click this option if want to use a hotspot service (use this type for external captive portal workflows) or WISPr.</p> <p>NOTE Hotspot (WISPr) applies to WLAN traffic that is tunneled and not tunneled.</p>
Authentication Options		
Method	Specifies the authentication mechanism.	Open (Default)—No authentication mechanism is applied to connections. If WPA or WPA2 encryption is used, this implies WPA-PSK authentication.
Hotspot Portal (for WLAN Authentication Type: Hotspot (WisPr))		
Hotspot (WISPr) Portal	Defines hotspot behavior, like redirects, session timers, and location information, among others.	Select the hotspot portal profile that you want this WLAN to use.
Bypass CNA	Bypasses the Apple CNA feature on iOS and OS X devices that connect to this WLAN.	Select the Enable check box.
Authentication Server	Indicates the authentication server that you want to use for this WLAN.	<p>Choose the option. Options include Local DB, Always Accept, and any AAA servers that you previously added. Additionally, if you want the controller to proxy authentication messages to the AAA server, select the Use Controller as Proxy check box. When the SSH tunnel between the AP and the controller is down, you can enable Backup Authentication Service to back up the AP's authentication services to a secondary device.</p> <p>NOTE For WISPr survivability, the customer portal must use the AP WISPr ZD-Style API/Backup AAA authentication to continue the WISPr service.</p>
Accounting Server	Indicates the RADIUS Accounting server that you want to use for this WLAN.	<p>Choose the option. You must have added a RADIUS Accounting server previously. Additionally, if you want the controller to proxy accounting messages to the AAA server, select the Use the Controller as Proxy check box. When the SSH tunnel between the AP and the controller is down, you can enable Backup Accounting Service to back up the AP's accounting services to a secondary device.</p> <p>NOTE For WISPr survivability, the customer portal must use the AP WISPr ZD-Style API/Backup AAA authentication to continue the WISPr service.</p>
RADIUS Option		
NAS ID	Defines the ID sent to the RADIUS server, which will identify the AP.	<p>Choose the option:</p> <ul style="list-style-type: none"> • WLAN BSSID • AP MAC • User-defined

TABLE 7 WLAN Configurations (continued)

Field	Description	Your Action
NAS Request Timeout	Indicates the duration after which an expected RADIUS response message is considered to have failed.	Enter the timeout period (in seconds). NOTE It is recommended to configure the same values for NAS Request Timeout, NAS Max Number of Retries, and NAS Reconnect Primary.
NAS MAX Number of Retries	Indicates the maximum number of failed connection attempts after which the controller will fail over to the backup RADIUS server.	Enter the maximum number of failed connection attempts. NOTE It is recommended to configure the same values for NAS Request Timeout, NAS Max Number of Retries, and NAS Reconnect Primary.
NAS Reconnect Primary	Indicates the time interval after which the controller will recheck if the primary RADIUS server is available when the controller has failed over to the backup RADIUS server.	Enter the duration in minutes. <i>Range:</i> 1 through 60 minutes. The default interval is 5 minutes. NOTE It is recommended to configure the same values for NAS Request Timeout, NAS Max Number of Retries, and NAS Reconnect Primary.
Called Station ID	Indicates the format for the called station ID, which is sent to the RADIUS server as an attribute, and can be used in policy decision	Select a format: <ul style="list-style-type: none"> • WLAN BSSID • AP MAC • AP GROUP • NONE
Single Session ID Accounting	Enabling this feature allows the APs to maintain one accounting session for a client roaming between APs. If the client roams from one AP to another, the accounting session ID and stats will be carried while roaming from one AP to the other. If the feature is not enabled, the accounting session ID is re-generated and stats is also reset, essentially resetting the accounting.	Select the Enable check box to use this feature.
NAS IP	Indicates the NAS IP address.	Select the option: <ul style="list-style-type: none"> • Disabled • SZ Control IP • SZ Management IP • User-defined

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 **Diagnostics > Application Logs** as all other applications.

The table 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 8 Portal Details

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

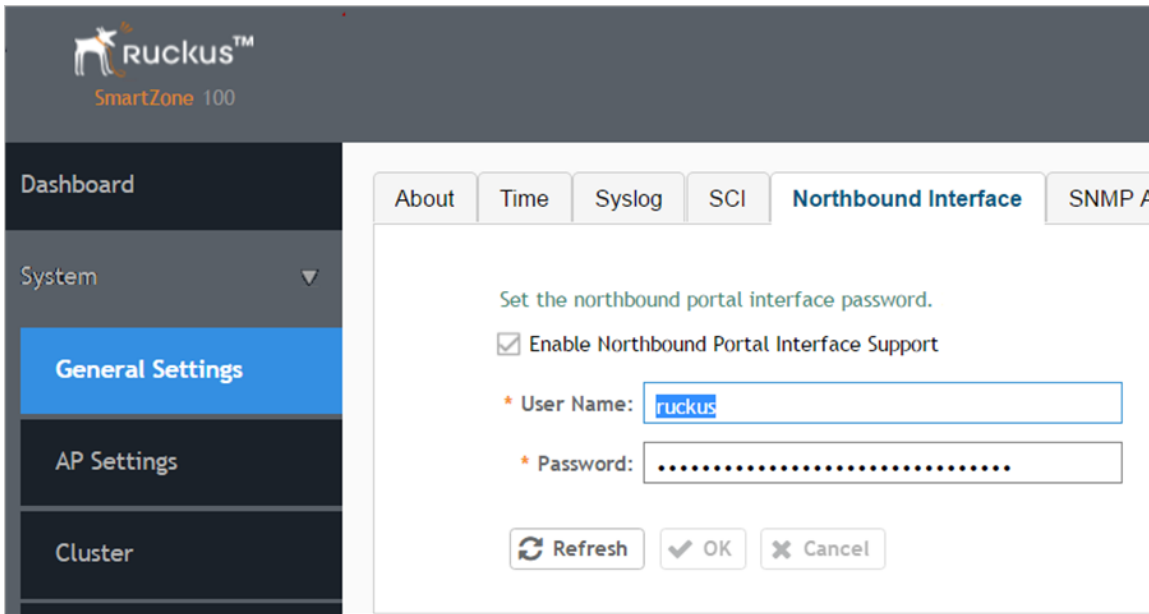
The northbound interface request password can be configured in the controller web interface by navigating to **System > General Settings > Northbound Interface**. See the figure below.

NOTE

The password in the figures is a token to ensure that the interface has the permission to get the services from the northbound 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 9 Enable Northbound Interface



JSON Commands - User Online Control

• Overview.....	31
• Request Authentication - Asynchronous Login.....	31
• Using Asynchronous API.....	32
• Request Authentication - Synchronous Login.....	33
• Querying a User Status.....	34
• Terminating a User Session.....	35
• Disconnect Command.....	35
• Querying Enrichment Information.....	36

Overview

The northbound portal interface supports the following JSON commands:

- Login
- Login Async
- Logout
- Status
- 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. 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 the table for the full list of these parameters) 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 [JSON Responses - GetConfig](#) on page 37 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 or 2001::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 authentication 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).

The following is an example of an asynchronous login request:

```
{  
  Vendor: "ruckus",  
  RequestPassword: "myPassword",  
  APIVersion: "1.0",  
  RequestCategory: "UserOnlineControl",  
  RequestType: "LoginAsync",  
  UE-IP: "ENC12bc24c4777703327f2e0aabbf6b9f9e",  
  UE-MAC: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3DBE2157",  
  UE-Proxy: "0",  
  UE-Username: "test",  
  UE-Password: "test"  
}
```

The table 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 authentication server. The hotspot portal does not provide an interface for manipulating user account information.

TABLE 9 Controller responses to authentication (asynchronous login) requests

Response Type	Possible Responses
Normal response	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.
General error	<ul style="list-style-type: none">• 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 application 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 (RequestType=Login).

In a synchronous login command, the external Web portal must wait for the authentication process to complete, which is usually processed by the authentication server. This could result in a delayed response if the controller is unable to get a response from the authentication 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: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3DBE2157",
  UE-Proxy: "0",
  UE-Username: "test",
  UE-Password: "test"
}
```

The table lists the controller responses to the synchronous login command.

TABLE 10 Controller responses to a synchronous login command

Response Type	Possible Responses
Normal response	<ul style="list-style-type: none"> 101, Client authorized: Response if the user is already authorized. 201, Login succeeded: Response if the login is accepted.
Service error	<ul style="list-style-type: none"> 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 authentication reply message is returned. 400, Internal server error: Response when an controller internal error occurs. 401, Authentication server error: Response when an authentication connection error occurs or the connection request times out.
General error	<ul style="list-style-type: none"> 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.

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: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3DBE2157"
}
```

The table lists the controller responses to these user status query commands.

TABLE 11 Controller responses to user status query

Response Type	Possible Responses
If there is a pending authentication process for this client	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 100, Client unauthorized. or 101, Client authorized.
Service error	<ul style="list-style-type: none"> 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 authentication reply message is returned 400, Internal server error: Response when an controller internal error occurs. 401, Authentication server error: Response when a authentication connection error occurs or the connection request times out.
General error	<ul style="list-style-type: none"> 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: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3DBE2157"
}
```

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: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3DBE2157"
}
```

The table lists the controller response.

TABLE 12 Controller response to a disconnect command

Response Type	Possible Responses
Normal response	<ul style="list-style-type: none"> 200, OK 100, Client unauthorized: Response if the user is already unauthorized
Service Error	<ul style="list-style-type: none"> 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.
General error	<ul style="list-style-type: none"> 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.

TABLE 12 Controller response to a disconnect command (continued)

Response Type	Possible Responses
	<ul style="list-style-type: none"> 305, Category not supported: Response if the request category not supported. 306, Wrong request password: Response if the request password is mismatched.

Querying Enrichment Information

The northbound interface provides the JSON command `EnrichmentInfo` for verifying that the enrichment information has the same content as HTML header `enrichment info` 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 wherein the AP enrichment info is not available.

NOTE

The `EnrichmentInfo` command is only applicable for UEs connected to Ruckus APs and not for third party APs.

The following is an example of an `EnrichmentInfo` request:

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

The table lists the responses for enrichment information.

TABLE 13 Query enrichment

Response Type	Possible Responses
Normal response	<ul style="list-style-type: none"> 102, Enrichment Information.
Service error	<ul style="list-style-type: none"> 300, Not found: Response if the lookup fails with given UE-MAC or UE-IP address. 400, Internal server error: Response when an controller internal error occurs.
General error	<ul style="list-style-type: none"> 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

- [JSON Responses - GetConfig](#) 37
- [JSON Responses Definitions](#).....38
- [JSON Response Examples](#).....39

JSON Responses - GetConfig

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

- Encrypt
- 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 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: "ENC1234bfdbe5y5hbfbdgh45y54ryt5y5th5"
}
```

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: "ENC1234bfdbe5y5hbfbdgh45y54ryt5y5th5"
}
```

The success response:

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

JSON Responses

JSON Responses Definitions

```
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 Definitions

The table 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)
- EI: Enrichment Info
- GC: Get Config (Encrypt and Decrypt)

NOTE

Refer to [Overview](#) on page 31 for commands related to the responses mentioned above.

TABLE 14 JSON response definitions

Category	Code	Definition	Used In				
			UA	SQ	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	•	•	•	•	•
	306	Wrong request password	•	•	•	•	•

TABLE 14 JSON response definitions (continued)

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

JSON Response Examples

This section provides the following examples of JSON responses defined in the Table (JSON Response Definitions)

Example: Client unauthorized

```
{
Vendor:"Ruckus",
APIVersion:"1.0",
ResponseCode:100,
ReplyMessage:"Client unauthorized",
UE-IP:"ENC323e79bf1bbd5ac4",
UE-MAC:"ENCf6b7f49da92a45f8978c35966b95eeafc6451102af391592",
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: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3DBE2157",
UE-Username: "user001",
AP-MAC: "04:4f:aa:32:25:f0",
SSID: "hotspot-01"
SmartClientMode: "none",
SmartClientInfo: "",
GuestUser: "0",
}
```

Example: Enrichment information

```
{
Vendor: "Ruckus",
APIVersion: "1.0",
ResponseCode: "102",
ReplyMessage: "Enrichment Information",
UE-IP: "ENC12bc24c4777703327f2e0aabbf6b9f9e",
UE-MAC: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3DBE2157",
AP-MAC: "04:4f:aa:32:25:f0",
SSID: "hotspot-01",
WLAN-ID: "1",
Location: "a location",
VLAN-ID: 1
}
```

Example: Success information

```
{
Vendor: "Ruckus",
```

JSON Responses

JSON Response Examples

```
Version: "1.0",
ResponseCode: "200",
ReplyMessage: "OK"
UE-IP: "ENC12bc24c4777703327f2e0aabbf6b9f9e",
UE-MAC: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3DBE2157",
SmartClientMode: "none",
SmartClientInfo: "",
GuestUser: "0",
}
```

Example: Login succeeded

```
{
Vendor: "Ruckus",
APIVersion: "1.0",
ResponseCode: "201",
ReplyMessage: "Login succeeded",
UE-IP: "ENC12bc24c4777703327f2e0aabbf6b9f9e",
UE-MAC: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3DBE2157",
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: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3DBE2157",
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: "ENCCDD319C6A476FA7127DF1FB80A63CD30ADC5E47C3DBE2157",
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: Authentication server error

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

Example: Encrypt for MAC address

```
{  
Vendor: "ruckus",  
RequestPassword: "myPassword",  
}
```

JSON Responses

JSON Response Examples

```
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: "ENC4782689566f8eac8aa30e276aa907f332d0bf93f9f60a7d8"
}
```

Example: Decrypt for MAC address

```
{
Vendor: "ruckus",
RequestPassword: "myPassword",
APIVersion: "1.0",
RequestCategory: "GetConfig",
RequestType: "Decrypt",
Data: "ENC4782689566f8eac8aa30e276aa907f332d0bf93f9f60a7d8"
}
The success response:
{
Vendor:"ruckus", ReplyMessage:"OK",
ResponseCode:200,
APIVersion:"1.0"
Data: "04:4f:aa:32:25:f0"
}
```

WISPr Support for ZoneDirector Login

- [WISPr Support for ZoneDirector Login Overview](#)..... 43
- [Web Page Setup](#)..... 44

WISPr Support for ZoneDirector Login Overview

The WISPr hotspot portal logon API supports the existing customer's external logon page with a ZD-style login and logout (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 AP and controller provide 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. 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 login/logout requests must include the parameters provided by controller's captive portal redirection. See [Captive Portal Attributes Overview](#) on page 47 for details.

Login: The login request path in the external portal to the controller 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. 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:9998/logout
```

To:

<https://sip:9998/SubscriberPortal/hotspotlogout?uip=10.20.30.40>

AP ZD-style Hotspot API

Customer external portal can use AP to send ZD-style login/logout requests. For logout/login examples, consult <https://apip:9998/SubscriberPortal/hotspotlogin> and <https://apip:9998/SubscriberPortal/hotspotlogout>.

Web Page Setup

This section gives details about URL parameters, UAM login URLs, and user login pages.

URL Parameters

Following are the URL parameters provided to set up a web page.

URL Parameter	Description
sip	Domain name of the Smart Zone
apip	IP address of the Ruckus AP
mac	AP MAC address
uip	Encrypted client's IP address
client_mac	Encrypted client's MAC address
sshTunnelStatus	SSH tunnel status between AP and SZ. If sshTunnelStatus is 0, it means AP cannot reach SZ.
url	Original URL which the customer tries browsing.
startUrl	The URL as per the hotspot configuration, which is to be redirected after successful login.

For details about the attributes, refer to [Captive Portal Attributes Overview](#) on page 47.

UAM login URLs

SmartZone provides the following URLs for user login:

- <http://sip:9997/SubscriberPortal/hotspotlogin>
- <https://sip:9998/SubscriberPortal/hotspotlogin>

If the authentication is successful, SmartZone redirects the user to the start page else the user is redirected to the login page.

When the Ruckus AP's SSH tunnel is up, it can use the following URLs provided by Ruckus AP for user login:

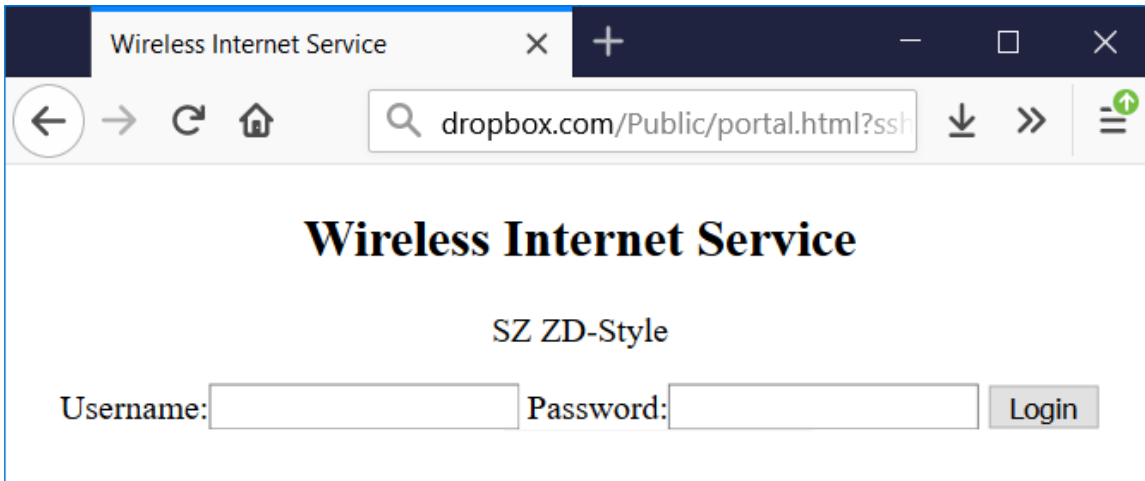
- <http://apip:9997/SubscriberPortal/hotspotlogin>
- <https://apip:9998/SubscriberPortal/hotspotlogin>

User Login page

A hotspot user uses the login page to log in to the hotspot service. The login page is provided by the hotspot service provider and is hosted on an HTTP server. A typical login page contains a form to enter the username and password. The hotspot user submits the form data to the UAM Login URL for authentication.

For example, the figure shows the HTML page with JavaScript code to generate the Smart Zone login form or Ruckus AP login form by the sshTunnelStatus.

FIGURE 10 Generating Login Form - SmartZone/Ruckus AP Login



Source Code

```
<html>
<head><title>Wireless Internet Service</title>
<script type="text/javascript">
function get_param(name) {
    if (location.href.indexOf("?") >= 0) {
        var query=location.href.split("?")[1];
        var params=query.split("&");
        for (var i = 0; i < params.length; i++) {
            value_pair=params[i].split("=");
            if (value_pair[0] == name)
                return unescape(value_pair[1]);
        }
    }
    return "";
}
</script></head>
<body>
<center>
<h2>Wireless Internet Service</h2>
<script>
if (get_param("sshTunnelStatus") == "1") {
    document.write('<p>SZ ZD-Style</p>');
    document.write('<form method=POST action="https://'+get_param("sip") + ':9998/SubscriberPortal/
hotspotlogin">');
} else {
    document.write('<p>AP ZD-Style</p>');
    document.write('<form method=POST action="https://'+get_param("apip") + ':9998/SubscriberPortal/
hotspotlogin">');
}
document.write('<input type="hidden" name="url" value="'+get_param("url")+' " />');
document.write('<input type="hidden" name="proxy" value="'+get_param("proxy")+' " />');
document.write('<input type="hidden" name="uip" value="'+get_param("uip")+' " />');
document.write('<input type="hidden" name="client_mac" value="'+get_param("client_mac")+' " />');
</script>
Username:<input type="text" name="username">
Password:<input type="password" name="password" >
<input type="submit" value="Login">
</form>
</center>
</body>
</html>
```


Captive Portal Attributes

- [Captive Portal Attributes Overview](#)..... 47

Captive Portal Attributes Overview

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.

NOTE

Apple CNA only works for HTTP redirect. It does not work if the external portal is in HTTPS.
Apple CNA does not support IPv6 addresses.

Redirection Attributes

The table lists these parameters provided by controller's captive portal redirection.

NOTE

See [WISPr Support for ZoneDirector Login Overview](#) on page 43 for login and logout details.

TABLE 15 Redirection attributes

Attributes	Description
apip	AP IP address which can be used as WISPr backup login
client_mac	Encrypted UE Mac address. NOTE The format of the MAC Address is defined at the Hotspot (WISPr) Portal configuration.
dn	The domain name.
lid	AP application identifier. For example: isocc=us, cc=1,ac=408,network=ACMEWISP_Newark_Airport
loc	AP location name. For example: ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport
mac	AP Mac address.
nbilP	The IPv4 of controller's Northbound Interface.
nbilPv6	The IPv6 of controller's Northbound Interface.
proxy	The UE browser if it is set to the Web proxy.
reason	Reason for redirecting the WLAN. The value could either be: <ul style="list-style-type: none">• Un-Auth-Captive – Regular unauthenticated UE redirected to Login Portal or <ul style="list-style-type: none">• Un-Auth-SSL-Captive – In case of HTTPS, Captive Portal is performing a “double redirect”. Adding this value to identify this flow
sip	The value could either be the: <ul style="list-style-type: none">• FQDN of the uploaded controller Web UI certificate if the uploaded certificate's common name is FQDN.• Concatenation of the controller 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 controller is packaged with, if the certificate was not uploaded at all.

TABLE 15 Redirection attributes (continued)

Attributes	Description
ssid	The broadcasted SSID name.
startUrl	The URL as per the hotspot configuration, which is to be redirected after successful login.
sshTunnelStatus	SSH tunnel status between AP and SZ. If sshTunnelStatus is 0, it means AP cannot reach SZ. If sshTunnelStatus is 1, then AP/SZ SSH tunnel is fine. The portal can check this value and decide whether to use AP IP or SZ IP to 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.
zoneld	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 controller.
zoneName	AP zone name of the UE's associated to the WLAN. The zone name is configured using the WLANs. The zone name is used for Kumo. The value is encrypted based on a special key.

The Smart Client

- [The Smart Client Overview..... 49](#)

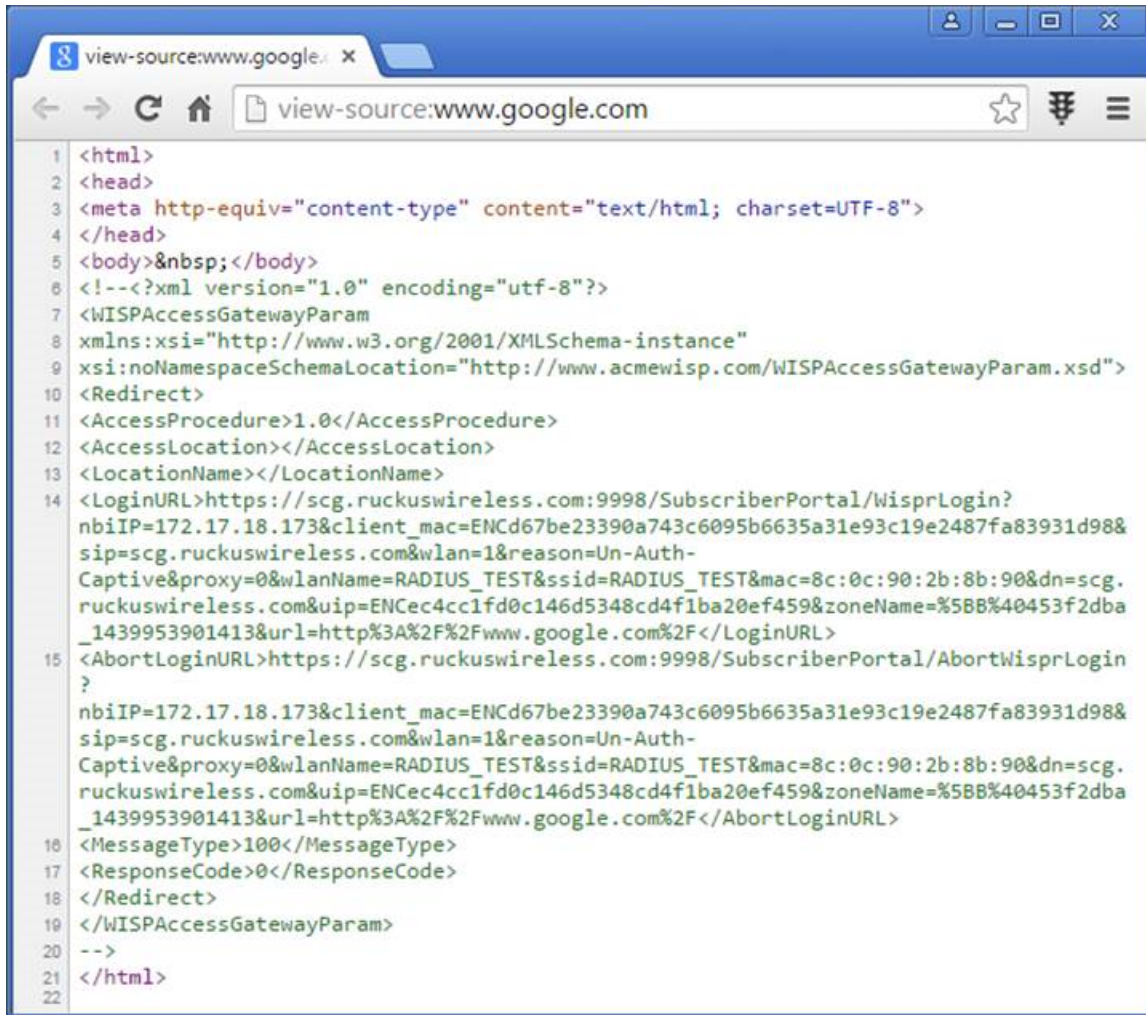
The Smart Client Overview

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 11 Smart Client Example



```
1 <html>
2 <head>
3 <meta http-equiv="content-type" content="text/html; charset=UTF-8">
4 </head>
5 <body>&nbsp;</body>
6 <!--<?xml version="1.0" encoding="utf-8"?>
7 <WISPAccessGatewayParam
8 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
9 xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGatewayParam.xsd">
10 <Redirect>
11 <AccessProcedure>1.0</AccessProcedure>
12 <AccessLocation></AccessLocation>
13 <LocationName></LocationName>
14 <LoginURL>https://scg.ruckuswireless.com:9998/SubscriberPortal/WisprLogin?
nbiIP=172.17.18.173&client_mac=ENCd67be23390a743c6095b6635a31e93c19e2487fa83931d98&
sip=scg.ruckuswireless.com&wlan=1&reason=Un-Auth-
Captive&proxy=0&wlanName=RADIUS_TEST&ssid=RADIUS_TEST&mac=8c:0c:90:2b:8b:90&dn=scg.
ruckuswireless.com&uip=ENCec4cc1fd0c146d5348cd4f1ba20ef459&zoneName=%5BB%40453f2dba
_1439953901413&url=http%3A%2F%2Fwww.google.com%2F</LoginURL>
15 <AbortLoginURL>https://scg.ruckuswireless.com:9998/SubscriberPortal/AbortWisprLogin
?
nbiIP=172.17.18.173&client_mac=ENCd67be23390a743c6095b6635a31e93c19e2487fa83931d98&
sip=scg.ruckuswireless.com&wlan=1&reason=Un-Auth-
Captive&proxy=0&wlanName=RADIUS_TEST&ssid=RADIUS_TEST&mac=8c:0c:90:2b:8b:90&dn=scg.
ruckuswireless.com&uip=ENCec4cc1fd0c146d5348cd4f1ba20ef459&zoneName=%5BB%40453f2dba
_1439953901413&url=http%3A%2F%2Fwww.google.com%2F</AbortLoginURL>
16 <MessageType>100</MessageType>
17 <ResponseCode>0</ResponseCode>
18 </Redirect>
19 </WISPAccessGatewayParam>
20 -->
21 </html>
22
```

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
=ENCd67be23390a743c6095b6635a31e93c19e2487fa83931d98&
sip=scg.ruckuswireless.com&wlan=1&reason=Un-Auth-Captive&proxy
=0&wlanName=RADIUS_TEST&ssid=RADIUS_TEST&mac
=8c:0c:90:2b:8b:90&dn=scg.ruckuswireless.com&uip
=ENCec4cc1fd0c146d5348cd4f1ba20ef459&zoneName
=%5BB%40453f2dba_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
=ENCd67be23390a743c6095b6635a31e93c19e2487fa83931d98&
sip=scg.ruckuswireless.com&wlan=1&reason=Un-Auth-Captive&proxy
```

```

=0&wlanName=RADIUS_TEST&ssid=RADIUS_TEST&mac=8c:0c:90:2b:8b:90&dn
=scg.ruckuswireless.com&uip=ENCec4cc1fd0c146d5348cd4f1ba20ef459&zoneName
=%5BB%40453f2dba_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/AbortWisprLogin?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

- User Defined Interface Overview..... 53
- NBI and UDI.....53

User Defined Interface Overview

AP uses the control interface to communicate with the controller regarding its configuration.

NBI and UDI

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 the figure) is configured, the AP uses it to DNAT unauthorized UE requests to the controller's captive portal (otherwise the AP uses the control interface).

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 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 the figure below. To define UDI on the controller's web interface, navigate to **System > Cluster > Select an existing Control Plane > Click on Configure > User Defined Interfaces**. Enter the following details. Click on **Add** to add and on **OK** to save the configuration details.

- Name of the UDI
- Physical Interface
- Service
- IP Address - (IPv4 or IPv6)
- Subnet Mask
- Gateway
- VLAN

FIGURE 12 Configuring UDI

Physical Interfaces **User Defined Interfaces** Static Routes

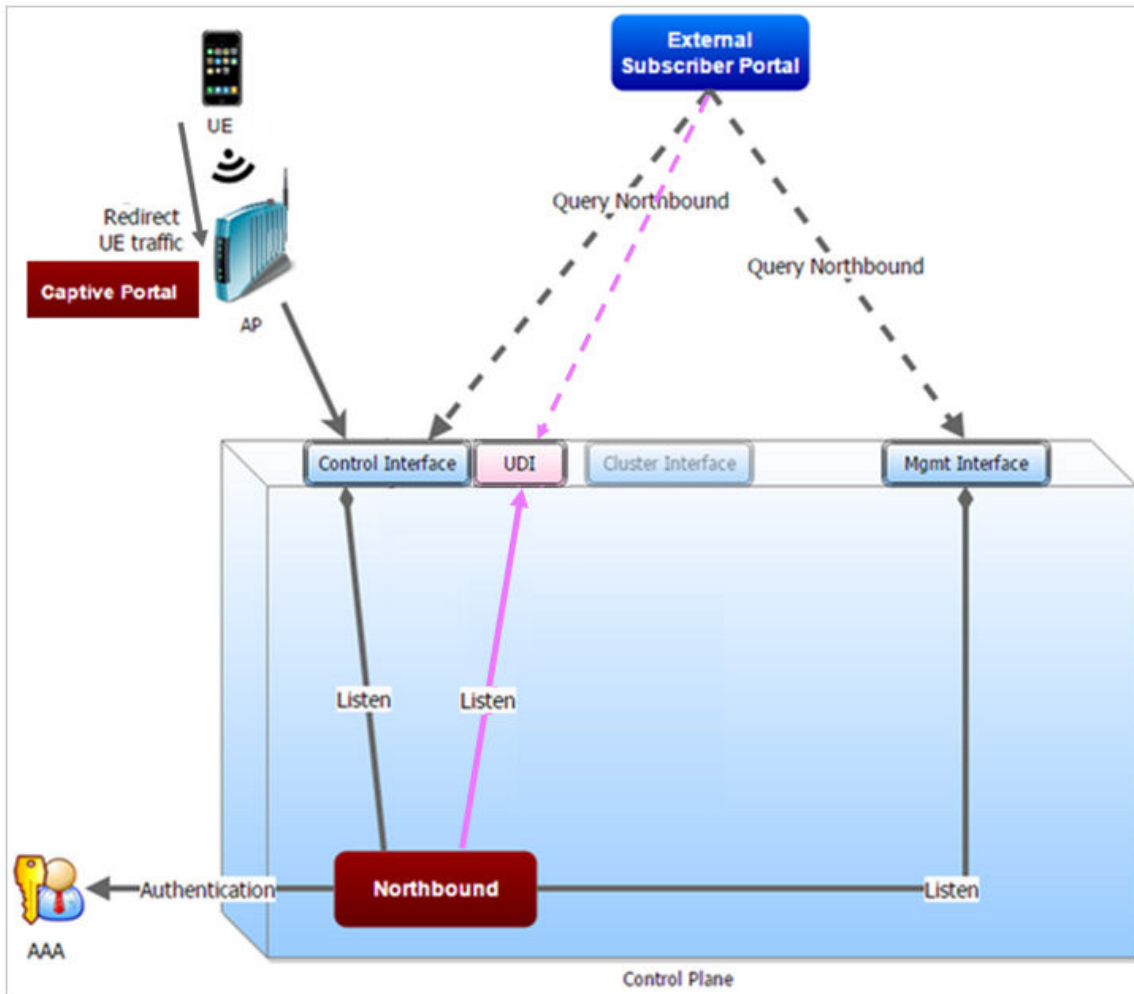
This page lists the northbound control interfaces and virtual network interfaces (VNI). At most 16 VNIs and 1 hotspot are allowed to be configured.

Name	Physical Interface	Service	IP Address	Subnet Mask	Gateway	VLAN
UDI	Control Interface	Hotspot	192.168.60.88	255.255.255.0	192.168.60.1	39
T1	Control Interface	Not Specified	192.168.2.22	255.255.255.0	N/A	55

OK Cancel

The figure below describes the request flows per interface.

FIGURE 13 Request flows per interface



WISPr Portal Details

- [WISPr Portal Details Overview..... 55](#)

WISPr Portal Details Overview

The following are the WISPr portal details for GRE tunnels.

Non GRE Tunnel

The below table lists the WISPr details for non GRE tunnel.

TABLE 16 Non GRE tunnel

Non GRE Tunnel		IPv4	IPv6
Non WISPr Client	IPv4	Supported	Supported
	IPv6	Supported	Supported

TABLE 17 Non GRE tunnel and internal portal

Non GRE Tunnel		IPv4	IPv6
WISPr Client	IPv4	Supported	Supported (This portal is IPv4)
	IPv6	Supported (This portal is IPv6. The smart zone has to enable IPv6 during the setup)	Supported (This portal is IPv6. The smart zone has to enable IPv6 during the setup)

TABLE 18 Non GRE tunnel and external portal

Non GRE Tunnel		IPv4	IPv6
WISPr Client	IPv4	Supported	Supported (This portal is IPv4)
	IPv6	Supported (This portal is IPv6)	Supported (This portal is IPv6)

Ruckus GRE Tunnel

The below table lists the WISPr details for Ruckus GRE tunnel.

TABLE 19 GRE tunnel

GRE Tunnel		IPv4	IPv6
Non WISPr Client	IPv4	Supported	Supported
	IPv6	Supported	Supported

TABLE 20 GRE tunnel and internal portal

GRE Tunnel		IPv4	IPv6
WISPr Client	IPv4	Supported	Supported (This portal is IPv4)
	IPv6	Supported (This portal is IPv6. The smart zone has to enable IPv6 during the setup)	Supported (This portal is IPv6. The smart zone has to enable IPv6 during the setup)

TABLE 21 GRE tunnel and external portal

GRE Tunnel		IPv4	IPv6
WISPr Client	IPv4	Supported	Supported (This portal is IPv4)
	IPv6	Supported (This portal is IPv6)	Supported (This portal is IPv6)

Certificate Warning

- [Certificate Warning Overview.....](#) 57

Certificate Warning Overview

Certificate warning when end users are redirecting with HTTPS request.

When a CA-signed certificate is imported to SZ certificate store and applied to Hotspot (WISPr), SZ captive portal and internal portal page use the imported certificate. However, if an end user enters a HTTPS URL through the browser manually, one certificate warning message is still expected to be seen in the UE browser.

SZ captive portal need to complete the SSL handshake before sending 302 redirect response to UE. Since the FQDN(common name) in the certificate is impossible to match the URL that UE tries to visit, the browser will display a certificate warning.

To avoid certificate warning messages, major operating systems already have built in mechanisms to detect captive network and sending HTTP requests (not HTTPS), so that users can be redirected to a portal page automatically without any certificate error.

- Apple iOS CNA (captive network assistant) sends HTTP requests to some static URLs to detect captive portal.
- Android devices detected it by sending HTTP requests to http://clients3.google.com/generate_204.
- Window 7 sends HTTP requests to <http://www.msftncsi.com/ncsi.txt> to detect captive portal.

NOTE

URL may vary based on different software releases.

In either case, user devices pop up a window and redirect users to the portal page with HTTP requests instead of HTTPS requests. No certificate warning will be shown if the UE is redirected automatically by the operating system.



© 2019 CommScope, Inc. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com