

# Ruckus Virtual SmartZone (High Scale)

For firmware versions 3.0 - 3.4

## *Setup Guide*



## Disclaimer

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

## Limitation of Liability

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

**VERSION 1.0 PUBLISHED OCTOBER 2016**

## IMPORTANT - BEFORE YOU START

Before attempting to integrate your hardware controller in to Odysys, please ensure that **ALL** of the following requirements are in place;

- You have a controller installed in an environment where compatible Access Points are configured to work with the controller, i.e - DNS, DHCP options configured correctly
- Access points must be able to successfully obtain the configuration from controller

Your client environment is configured to allow network clients to;

- Associate to an Access Point
- Obtain an IP address
- Access to the internet

The following components are required to be configured and working in your environment before attempting integration with Odysys;

- DHCP Server
- DNS Server
- Firewall NAT
- Firewall Rules
  - Allow incoming and outgoing on ports 9080/443/80/Primary RADIUS port/Secondary RADIUS port to the below addresses

54.246.86.107 – TCP + UDP

54.246.87.64 – TCP + UDP

54.243.42.241 – TCP + UDP

52.31.81.51 – TCP + UDP

54.75.232.45 – TCP

54.247.65.132 – TCP

54.75.236.90 – TCP

**PLEASE NOTE** - Odysys does not use standard RADIUS ports, therefore please make sure you allow the ports in your firewall, defined in your manage.odysys.net Captive Portal settings.

**This is a technical document and as such, integration of your hardware with Odysys should only be handled by trained individuals.**

## GETTING STARTED WITH ODYSYS

Before configuring the Ruckus SZ for use with Odysys, you will first need to create a Captive Portal to obtain key settings for your Ruckus SZ.

1. Within your Internet browser, navigate to <http://manage.odysys.net>
2. Log in to Odysys using your Customer ID, Username and Password



### Login to Odysys

CustomerID

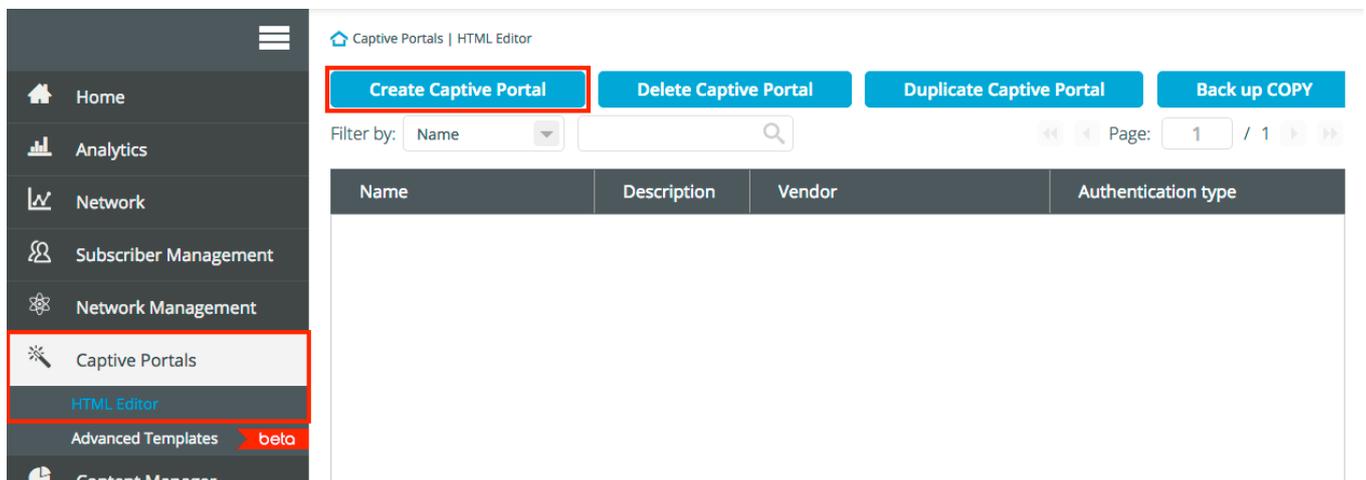
Username

Password

By clicking 'Login' you accept our [Terms & Conditions](#)

[Forgotten password?](#)

3. Using the navigation panel on the left hand side of the Odysys Dashboard, select **Captive Portals** then **HTML Editor**. Then click the **Create Captive Portal** button.



The screenshot shows the Odysys dashboard with a navigation sidebar on the left. The sidebar includes options like Home, Analytics, Network, Subscriber Management, Network Management, Captive Portals (highlighted with a red box), HTML Editor, Advanced Templates (beta), and Content Manager. The main content area is titled 'Captive Portals | HTML Editor' and features four buttons: 'Create Captive Portal' (highlighted with a red box), 'Delete Captive Portal', 'Duplicate Captive Portal', and 'Back up COPY'. Below the buttons is a search filter for 'Name' and a table with columns for Name, Description, Vendor, and Authentication type. The table is currently empty.

4. Enter in the following details for your Captive Portal

**Name:** <Enter a name for your captive portal>

**Description:** <Enter a description for your captive portal>

**RADIUS Shared Secret:** <Either keep the random-generated shared secret or create your own>

**Hardware Vendor:** **Ruckus Wireless SmartCell Gateway**

**SCG MGMT Primary IP Address:** <IP address of your primary SmartZone controller – if you are using a 3-interface setup, then this should be the CONTROL INTERFACE IP address>

**NOTE:** This needs to be a public IP address so that Odysseys can establish communication with the SmartZone controller.

**SCG MGMT Secondary IP Address:** <<IP address of your secondary SmartZone controller – if you are using a 3-interface setup, then this should be the CONTROL INTERFACE IP address >

**NOTE:** This can be the same as the primary IP if you do not have a secondary SZ.

**Northbound Portal Interface Password:** <Your SmartZone Northbound Portal Password>

Create Cloud Captive Portal ✕

Set Cloud Captive portal Name, Secret and choose hardware vendor.

**Name:** \*

**Description:**

**RADIUS Shared Secret:** \*

Import Portal from existing file

**Hardware Vendor:**

**Advanced Template:**

**SCG MGMT Primary IP Address** \*

**SCG MGMT Secondary IP Address** \*

**Northbound Portal Interface Password:** \*

Click the **Create** button to save the settings and complete initial setup of the Captive Portal.

5. Select the newly created Captive Portal and it will display the information required to configure the Ruckus SmartZone.  
**NOTE: You may need to scroll down to see the information.**

### Cloud Captive Portal: Ruckus vSZ 3.2

General Info | Pages | Terms & Conditions | Auth Providers

General info:

Name: Ruckus vSZ 3.2

Description:

Portal Status: Staging

|                             |               |
|-----------------------------|---------------|
| RADIUS Primary Server IP:   | 54.246.86.107 |
| RADIUS Secondary Server IP: | 54.246.87.64  |
| RADIUS Authentication Port: | 3262          |
| RADIUS Accounting Port:     | 3263          |
| RADIUS Shared Secret:       | [REDACTED]    |

Hardware Vendor: Ruckus Wireless SmartCell Gateway

SCG MGMT Primary IP Address: [REDACTED]

SCG MGMT Secondary IP Address: [REDACTED]

Northbound Portal Interface Password: ..... Show

|                   |   |
|-------------------|---|
| Splash Page URL:  | <a href="https://portals.odyssey.net/captivePortal/189203381">https://portals.odyssey.net/captivePortal/189203381</a>                         |
| Success Page URL: | <a href="https://portals.odyssey.net/captivePortal/successpage/189203381">https://portals.odyssey.net/captivePortal/successpage/189203381</a> |

Enable HotSpot 2.0 support

Require to accept receiving promotions

Show Walled Garden IPs Download files info

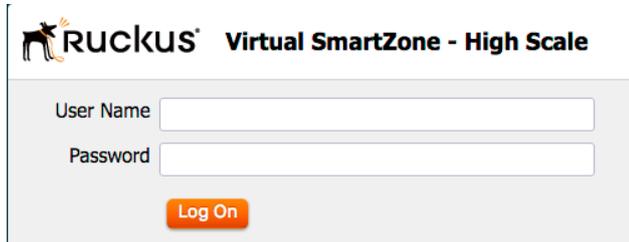
Edit Restore

**TECH NOTE**  
The information will differ for each Captive Portal created and is unique to each Captive Portal.

# CONFIGURING ODYSYS WITHIN THE RUCKUS SMARTZONE

Please ensure you have an AP Zone preconfigured before attempting this guide.

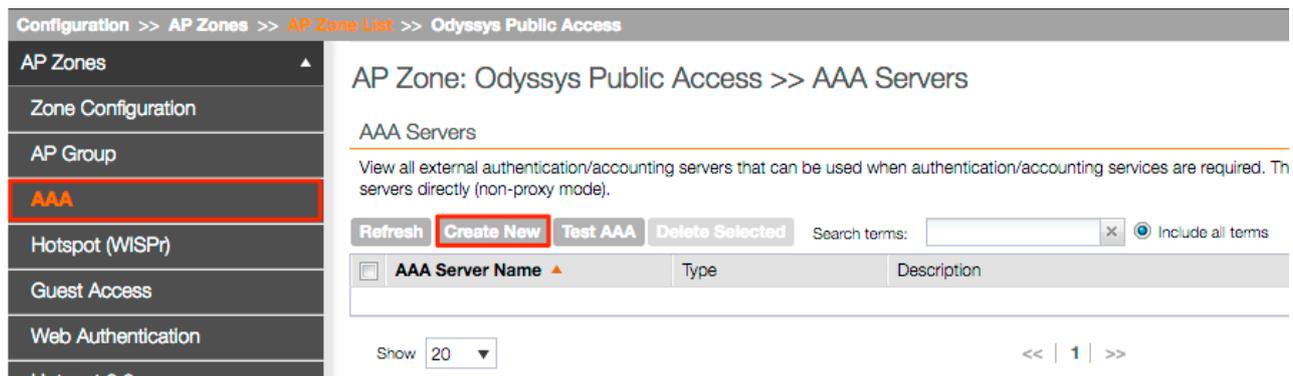
1. Log in to your Ruckus SmartZone controller.



2. Click **Configuration** and then **AP Zones**



3. Select you AP Zone and navigate the **AAA** page of your AP Zone. Click **Create New**.



4. To configure the RADIUS Authentication server, enter in the settings below and click **OK** once completed

**Name:** <Name of your RADIUS Authentication service i.e Odysys - Auth>

**Type:** RADIUS

**Backup RADIUS:** Tick

**Primary Server**

**IP Address:** <IP address of Odysys Primary RADIUS Server>

**Port:** <RADIUS Authentication Port>

**Shared Secret:** <Shared Secret Password>

**Confirm Secret:** <Shared Secret Password>

**Secondary Server**

**IP Address:** <IP address of Odysys Secondary RADIUS Server>

**Port:** <RADIUS Authentication Port>

**Shared Secret:** <Shared Secret Password>

**Confirm Secret:** <Shared Secret Password>

**Create New AAA Server**

General Options

Name: \*

Description:

Type: \*  RADIUS  RADIUS Accounting  Active Directory  LDAP

Backup RADIUS:  Enable Secondary Server

Primary Server

IP Address: \*

Port: \*

Shared Secret: \*

Confirm Secret: \*

Secondary Server

IP Address: \*

Port: \*

Shared Secret: \*

Confirm Secret: \*

OK Cancel

5. Whilst still on the **AAA** page, click **Create New** again.

Configuration >> AP Zones >> AP Zone List >> Odysys Public Access

AP Zones

Zone Configuration

AP Group

**AAA**

Hotspot (WISPr)

Guest Access

Web Authentication

Hotspot 2.0

AP Zone: Odysys Public Access >> AAA Servers

AAA Servers

View all external authentication/accounting servers that can be used when authentication/accounting services are required. These servers directly (non-proxy mode).

Refresh Create New Test AAA Delete Selected Search terms:   Include all terms  Inc

| AAA Server Name | Type   | Description |
|-----------------|--------|-------------|
| Odysys - Auth   | RADIUS |             |

Show 20 << | 1 | >>

6. This time you should configure the RADIUS Accounting settings. Complete the below settings and click **OK** once completed.

**Name:** <Name of your RADIUS Accounting service i.e Odysys - Acc>

**Type:** RADIUS Accounting

**Backup RADIUS:** Tick

**Primary Server**

**IP Address:** <IP address of Odysys Primary RADIUS Server>

**Port:** <RADIUS Accounting Port>

**Shared Secret:** <Shared Secret Password>

**Confirm Secret:** <Shared Secret Password>

**Secondary Server**

**IP Address:** <IP address of Odysys Secondary RADIUS Server>

**Port:** <RADIUS Accounting Port>

**Shared Secret:** <Shared Secret Password>

**Confirm Secret:** <Shared Secret Password>

**Create New AAA Server**

General Options

**Name:** \*

**Description:**

**Type:** \*  RADIUS  RADIUS Accounting  Active Directory  LDAP

**Backup RADIUS:**  Enable Secondary Server

Primary Server

**IP Address:** \*

**Port:** \*

**Shared Secret:** \*

**Confirm Secret:** \*

Secondary Server

**IP Address:** \*

**Port:** \*

**Shared Secret:** \*

**Confirm Secret:** \*

**OK** **Cancel**

7. Select **Hotspot (WISPr)** from the left-hand side menu and then click **Create New**



8. Enter in the below settings

**Name:** <Name of your hotspot (not the SSID)>

**Logon URL:** External

**Redirect unauthenticated user to URL for authentication:** <Splash Page URL from Odysseys>

**Redirect to the following URL:** <Success Page from Odysseys>

**Walled Garden:** <Expand this section, and enter the Walled Garden IPs obtained from your Odysseys Captive Portal configuration>

Click **OK** to save your settings.

The screenshot shows the 'Create New Hotspot Portal' configuration form. The form is divided into several sections: 'General Options', 'Redirection', 'User Session', 'Location Information', and 'Walled Garden'. The 'General Options' section includes 'Portal Name' (set to 'Odysseys Public Access Hotspot'), 'Portal Description', and 'Smart Client Support' (set to 'None'). The 'Redirection' section includes 'Logon URL' (set to 'External'), 'Redirect unauthenticated user to the URL for authentication.' (with a text input field), 'Redirected MAC Format' (set to 'AA:BB:CC:DD:EE:FF'), and 'Start Page' (set to 'Redirect to the following URL:' with a text input field). The 'User Session' section includes 'Session Timeout' (set to '1440' minutes) and 'Grace Period' (set to '60' minutes). The 'Location Information' section includes 'Location ID' and 'Location Name' (both with text input fields). The 'Walled Garden' section includes a 'Walled Garden Entry' field (with a text input field) and buttons for 'Add', 'Import CSV', 'Cancel', and 'Delete'. At the bottom of the form, there are 'OK' and 'Cancel' buttons.

9. Click on **WLAN** from the left-hand side menu and **Create New**

The screenshot shows a web-based configuration interface. On the left, a sidebar menu lists various configuration options, with 'WLAN' highlighted in red. The main content area is titled 'AP Zone: Odysseys Public Access >> WLAN Services & Groups'. Under 'WLAN Configuration', there are buttons for 'Refresh', 'Create New' (highlighted in red), 'Extract WLAN Template', 'Apply WLAN Template', and 'Delete Selected'. Below these buttons is a table with columns for 'WLAN Name', 'SSID', 'Description', and 'Auth'. A 'Show 20' dropdown and pagination controls are also visible. The 'WLAN Group Configuration' section below is partially visible.

10. Enter in the below settings:

**Name:** <Name of your WLAN>

**SSID:** <SSID you want to broadcast>

**Authentication Type:** <Hotspot (WISPr)>

**Hotspot (WISPr) Service:** <Select previously created Hotspot service from the drop down>

**Authentication Service:** <Select previously created Authentication service from the drop down >

**Accounting Service:** <Select previously created Accounting service from the drop down >

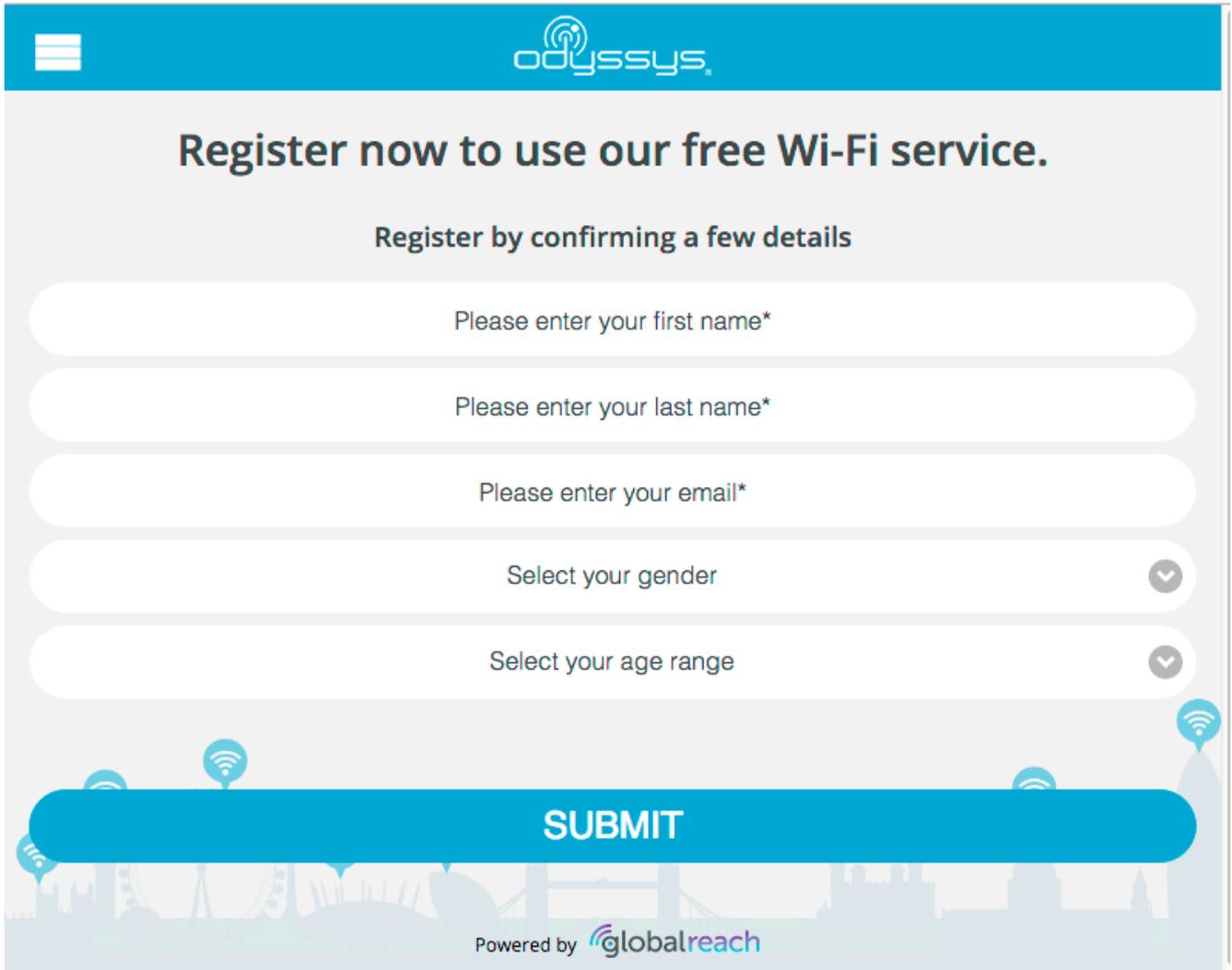
Click the **OK** button once completed.

The screenshot shows the 'Create New WLAN Configuration' dialog box. The 'General Options' section has 'Name' set to 'Odysseys Free Wi-Fi' and 'SSID' set to 'Free Wi-Fi'. The 'WLAN Usage' section has 'Authentication Type' set to 'Hotspot (WISPr)'. The 'Authentication Options' section has 'Method' set to 'Open'. The 'Encryption Options' section has 'Method' set to 'None'. The 'Hotspot Portal' section has 'Hotspot (WISPr) Portal' set to 'Odysseys Public Access Hotspot'. The 'Authentication Service' is set to 'Odysseys - Auth' and the 'Accounting Service' is set to 'Odysseys - Acc'. The 'Options' section has 'Priority' set to 'High'. The 'RADIUS Options' and 'Advanced Options' sections are collapsed. The 'OK' button is highlighted in red.

Page 11 of 16

This concludes the basic configuration process. You should now set your WLAN to broadcast and test to ensure:

- You are redirected to the Odysys Splash Page URL upon connecting to the SSID.
- You are able to authenticate and gain internet access successfully by completing and submitting the form on the Splash Page (assuming you have not made any modifications to the default splash page template).



The image shows a screenshot of a web registration form for a free Wi-Fi service. The form is titled "Register now to use our free Wi-Fi service." and includes a sub-heading "Register by confirming a few details". The form contains five input fields: "Please enter your first name\*", "Please enter your last name\*", "Please enter your email\*", "Select your gender", and "Select your age range". A large blue "SUBMIT" button is positioned below the fields. The form is powered by "globalreach" and features a background illustration of a city skyline with Wi-Fi signal icons.

**Odysys**

## Register now to use our free Wi-Fi service.

Register by confirming a few details

Please enter your first name\*

Please enter your last name\*

Please enter your email\*

Select your gender

Select your age range

**SUBMIT**

Powered by **globalreach**

## ACCESS CONTROL LIST ADDRESSES

### Odyssys

54.246.86.107  
54.246.87.64  
54.243.42.241  
52.31.81.51  
54.75.232.45  
54.247.65.132  
54.75.236.90

### Twitter

api.twitter.com  
\*.twimg.com

### Google

74.125.29.84  
74.125.226.243  
74.125.228.10  
74.125.228.74  
74.125.228.111  
130.111.19.240  
173.194.74.95

### Facebook

\*.facebook.com  
\*.akamaihd.net  
\*.fbcdn.net  
connect.facebook.com

### LinkedIn

8.247.88.225  
23.202.203.120  
64.94.107.57  
138.108.7.20  
216.52.242.80  
216.52.242.86

### PayPal Express Checkout

173.0.82.77/32  
92.122.246.85/32  
66.117.29.34/32  
216.113.188.89/32  
66.235.147.113/32

**If you wish to disable Apple's Captive Assistant please add the following to your walled garden**

www.apple.com  
www.airport.us  
www.ibook.info  
www.thinkdifferent.us  
www.itools.info  
www.appleiphonecell.com  
captive.apple.com

## FREQUENTLY ASKED QUESTIONS

**Q.** Where do I find my Northbound Portal Interface Password?

**A.** This can be found in Configuration -> System ->Northbound Portal Interface in your SmartZone Web GUI

**Q.** I want to add different authentication provider types, how do I do this?

**A.** Please see our Odysys Authentication guide for further information.

**Q.** I need more information on how to setup Odysys

**A.** Please see our Odysys setup guide.

## GLOSSARY

**AAA** - Authentication, Authorization, and Accounting

**ACL** - Access Control List

**AP** - Access Point

**DHCP** - Dynamic Host Configuration Protocol

**DNS** - Domain Name Service

**NAT** - Network Address Translation

**PORT** - A process-specific or an application-specific software construct serving as a communication endpoint, which is used by the Transport Layer protocols of Internet Protocol suite, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP)

**RADIUS** - Remote Authentication Dial In User Service (RADIUS)

**SZ** - Ruckus Wireless SmartZone

**SHARED SECRET** - A single password shared between two devices

**SSID** - Service Set Identifier - A unique identifier for your Wi-Fi service

**WALLED GARDEN** - List of addresses that are allowed for unauthenticated users

**WISPr** - Wireless Internet Service Provider roaming

**WLAN** - Wireless Local Area Network

**WLC** - Wireless Local Area Network Controller

Global Reach Technology Ltd  
Craven House, 121 Kingsway  
London WC2B 6PA  
T +44 (0) 20 7831 5630  
[info@globalreachtch.com](mailto:info@globalreachtch.com)

Copyright © Global Reach Technology Limited  
All rights reserved.  
Global Reach and the Global Reach logo  
are registered trademarks.