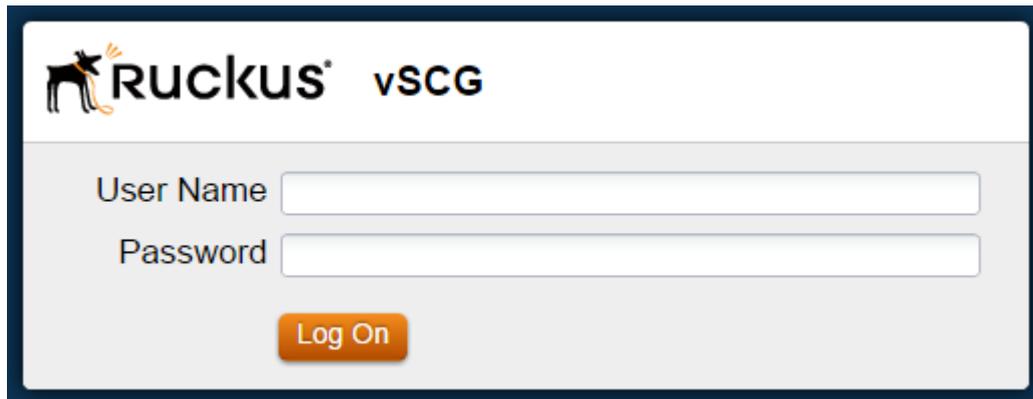


Ruckus (SCG managed)

Modified on: Thu, 19 Mar, 2015 at 11:29 AM

Open a web browser and log in to your Ruckus SCG



The screenshot shows the Ruckus vSCG login interface. At the top left is the Ruckus logo, which consists of a stylized dog icon followed by the word 'RUCKUS' in a bold, sans-serif font, and 'vSCG' in a smaller font to its right. Below the logo, there are two text input fields. The first is labeled 'User Name' and the second is labeled 'Password'. Below the password field is an orange button with the text 'Log On' in white.

Click on "**Configuration > AP Zones**" on the top menu and then "**RADIUS**" on the left.

Click on "**Create New**". Configure with the below settings:

- **Name:** Guest WiFi
- **Type:** RADIUS
- **Backup RADIUS support:** Ticked

- **Primary Server IP Address:** *insert radius_server_ip here*
- **Port:** 1812
- **Shared Secret:** *insert radius_secret here*
- **Confirm Secret:** as above

- **Secondary Server IP Address:** *insert radius_server2_ip here*
- **Port:** 1812
- **Shared Secret:** *insert radius_secret here*
- **Confirm Secret:** as above

Press **Create New** to save

General Options	
Name:	<input type="text" value="Guest WiFi"/>
Description:	<input type="text"/>
Type:	<input checked="" type="radio"/> RADIUS <input type="radio"/> RADIUS Accounting
Backup RADIUS:	<input checked="" type="checkbox"/> Enable backup RADIUS support
Health Check Policy	
Response Window:	<input type="text" value="20"/> Seconds
Zombie Period:	<input type="text" value="40"/> Seconds
Revive Interval:	<input type="text" value="120"/> Seconds
No Response Fail:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Rate Limiting	
Maximum Outstanding Requests (MOR):	<input type="text" value="0"/> Requests per Server
Threshold:	<input type="text" value="0"/> % of MOR
Sanity Timer:	<input type="text" value="10"/> Seconds
Primary Server	
IP Address:	<input type="text" value="192.168.1.1"/>
Port:	<input type="text" value="1812"/>
Shared Secret:	<input type="text" value="....."/>
Confirm Secret:	<input type="text" value="....."/>
Secondary Server	
IP Address:	<input type="text" value="172.16.1.1"/>
Port:	<input type="text" value="1812"/>
Shared Secret:	<input type="text" value="....."/>
Confirm Secret:	<input type="text" value="....."/>

Click "Create New" again and configure with the below settings:

- Name: Guest WiFi Acct
- Type: RADIUS Accounting
- Backup RADIUS Support: Ticked
- Primary Server IP Address: *insert radius_server_ip here*
- Port: 1813
- Shared Secret: *insert radius_secret here*
- Confirm Secret: as above
- Secondary Server IP Address: *insert radius_server2_ip here*

- **Port:** 1813
- **Shared Secret:** *insert radius_secret here*
- **Confirm Secret:** as above

Press **Create New** to save

General Options

Name: *

Description:

Type: RADIUS RADIUS Accounting

Backup RADIUS: Enable backup RADIUS Accounting

Health Check Policy

Response Window: * Seconds

Zombie Period: * Seconds

Revive Interval: * Seconds

Rate Limiting

Maximum Outstanding Requests (MOR): * Requests per Server

Threshold: * % of MOR

Sanity Timer: * Seconds

Primary Server

IP Address: *

Port: *

Shared Secret: *

Confirm Secret: *

Secondary Server

IP Address: *

Port: *

Shared Secret: *

Confirm Secret: *

Create New
Cancel

Click on "**Configuration > AP Zones**" at the top and then "**Create New**". Configure with the following:

- **Zone Name:** Guest WiFi

Click **Create New**

Next, click on the Zone Name you just created. This will provide a new menu down the left of the page. Click on "**WISPr (Hotspot)**" and then "**Create New**". Configure with the following:

- **Name:** Guest WiFi
- **Type:** Registered Users
- **Logon URL:** External
- **Redirect unauthenticated users to the URL for authentication:** *insert access_url here*
- **Start Page -Redirect to the following URL:** *insert redirect_url here*

Under "**Walled Garden**" click on "**Create New**" and add the following domains one by one:

*.*insert access_domain here*

www.google.com
www.google.co.uk

*.google-analytics.com

*.venuewifi.com

*.openweathermap.org

*.cloudfront.net

If you wish to support social network logins, you also need to add the domains below for each network you plan to support

Facebook	Twitter	LinkedIn	Google	Instagram
*.facebook.com *.fbcdn.net	*.twitter.com	*.linkedin.com	*.googleusercontent.com	
*.akamaihd.net	*.twimg.com	*.licdn.net *.licdn.com	*.googleapis.com *.accounts.google.com *.gstatic.com	*.instagram.com
*.connect.facebook.net				

[-] General Options

Name: *

Description:

Type: Registered Users
 Guest-Access

[-] Redirection

Smart Client Support: None
 Enable
 Only Smart Client Allowed

Logon URL: Internal
 External
Redirect unauthenticated user to the URL for authentication.

Start Page: After user is authenticated,
 Redirect to the URL that user intends to visit.
 Redirect to the following URL:

[-] User Session

Session Timeout: * Minutes (2 - 14400)

Grace Period: * Minutes (1 - 14399)

[-] Location Information

Location ID: (example: isoc=us,cc=)

Location Name: (example: ACMEWISP,

[-] Walled Garden

Unauthenticated users are allowed to access the following destinations.
Format:
- IP (e.g. 10.11.12.13)
- IP Range (e.g. 10.11.12.13-10.11.12.15)
- CIDR (e.g. 10.11.12.100/28)
- IP and mask (e.g. 10.11.12.13 255.255.255.0)
- Precise web site (e.g. www.ruckus.com)
- Web site with special regular expression like
- *.amazon.com
- *.com
- *

Press "**Apply**" to Save

Click on "**WLAN**" on the left menu and then "**Create New**".

Configure with the below settings:

- **Name:** Guest Wi-Fi

- **SSID:** Whatever you want to broadcast as your wireless network name (SSID)
- **Type:** Hotspot Service (WISPr)
- **Authentication Method:** Open
- **Encryption Method:** Open
- **Hotspot Service:** Guest Wi-Fi
- **Authentication Service:** Use SCG as Proxy - Guest WiFi
- **Accounting Service:** Use SCG as Proxy - Guest WiFi Acct

Under "**RADIUS Options**" set:

- **Called STA ID:** AP MAC

General Options

Name: *

SSID: *

Description:

WLAN Usage

Authentication Type: Standard usage (For most regular wireless networks)
 Hotspot service (WISPr)
 Hotspot 2.0
 Guest Access

Authentication Options

Method: * Open 802.1x EAP MAC Address

Encryption Options

Method: WPA WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None

Hotspot Service

Hotspot(WISPr) Service: * 

Authentication & Accounting Service

Authentication Service: * Use SCG as Proxy 

Accounting Service: Use SCG as Proxy  Send interim update every

Options

Acct Delay Time: Enable

Wireless Client Isolation: Disable
 Enable (Wireless clients associated with the same AP will be unable to communicate with

Priority: High Low

RADIUS Options

RADIUS NAS ID: * WLAN BSSID AP MAC User-defined:

RADIUS NAS Request Timeout: * Seconds

RADIUS NAS Max Number of Retries: * Times

RADIUS NAS Reconnect Primary: * Minute(1-60)

Called STA ID: WLAN BSSID AP MAC

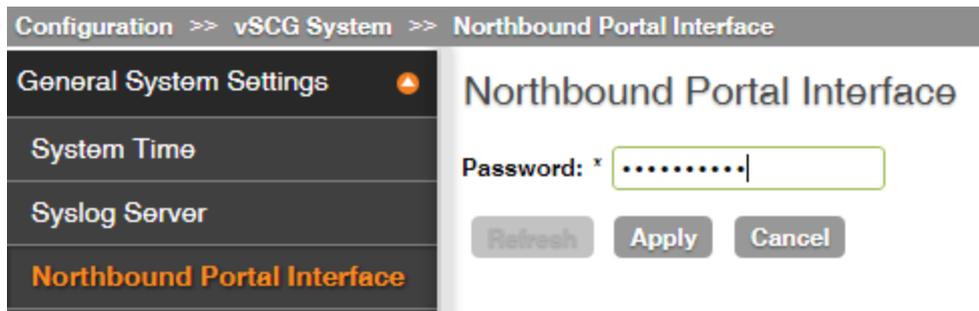
Advanced Options

Apply **Cancel**

Click on "Create New / Apply" to save

Next, click on **Configuration > (v)SCG system**" and on the left select "**Northbound Portal Interface**".

If you already use a custom password, you do not need to modify this, however if you have not yet set a password, please enter one now. This password will need to be entered in to the Portal later.



To complete the set up you will need to log in to your portal, and under "Management > Venues > Edit Venue > Options" you will need to enter your SCG Public IP and the Password from above. This allows our system to talk to the SCG for authenticating users etc.

Ruckus SCG (UDI) IP



Ruckus SCG (UDI) Password

