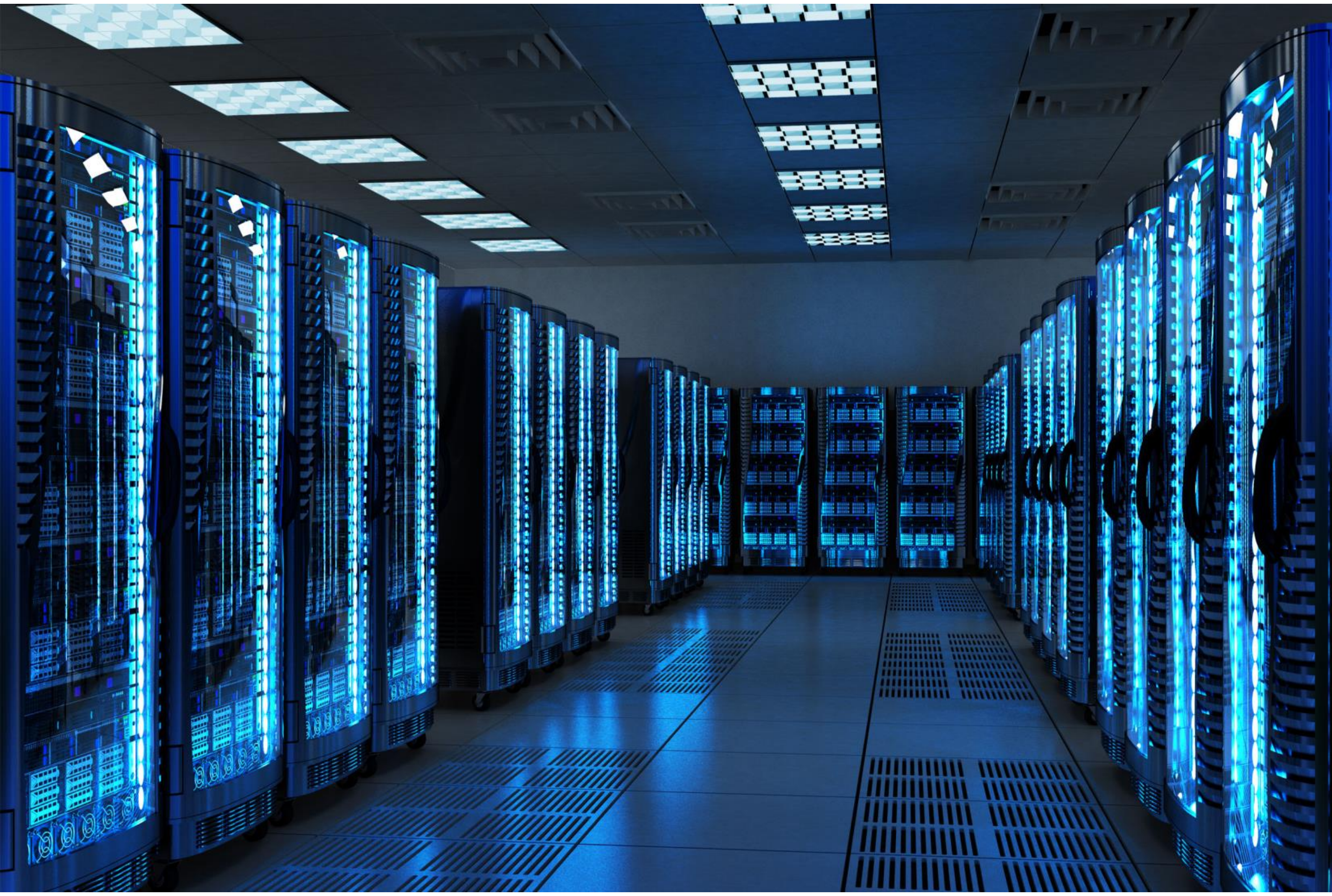


INTEGRATION GUIDE

How to Configure Ruckus Wi-Fi to Secure your Guest Wireless Network with Portnox CLEAR

Introduction

This document guides you step by step how to configure your Ruckus wireless environment using Portnox CLEAR to control guest user access.

Enabling CLEAR RADIUS Service

The first step is to enable the CLEAR RADIUS service:

1) Verify your organization is registered on Portnox CLEAR Cloud Services: https://clear.portnox.com/.

2) In the CLEAR portal, go to **Settings** > **Services** and expand **CLEAR RADIUS Service**. Then:

   a. If the **Enable Cloud RADIUS** checkbox is not checked, click **Edit** and check the **Enable Cloud RADIUS** checkbox.

   b. Note the RADIUS server details which you will need when configuring the Ruckus Controller:

      - **Cloud RADIUS IP** - this is the IP address of the CLEAR RADIUS server
      - **Authentication port**
      - **Accounting port** - needed for the RADIUS accounting server
      - **Shared Secret** - this is the RADIUS client shared secret

Enabling CLEAR Captive Portal Service

The second step is to enable the CLEAR Captive Portal (=Guest portal).

1) In the CLEAR portal, go to **Settings** > **Services** and expand **CLEAR Captive Portal Service**. Then:

   a. If the **Enable CLEAR Captive Portal** checkbox is not checked, click **Edit** and check the **Enable CLEAR Captive Portal** checkbox.

   b. Note the **URL**, the **IP (for walled garden)** and the **Shared Secret** which you will need when configuring the Ruckus controller.

Configuring the Ruckus Wi-Fi SSID

In the final step, we configure the Ruckus guest wireless SSID to control guest user access.

1) Add a Radius server by navigating to **Configure** > **AAA Servers** and clicking **Create New**.

   In the window that appears:

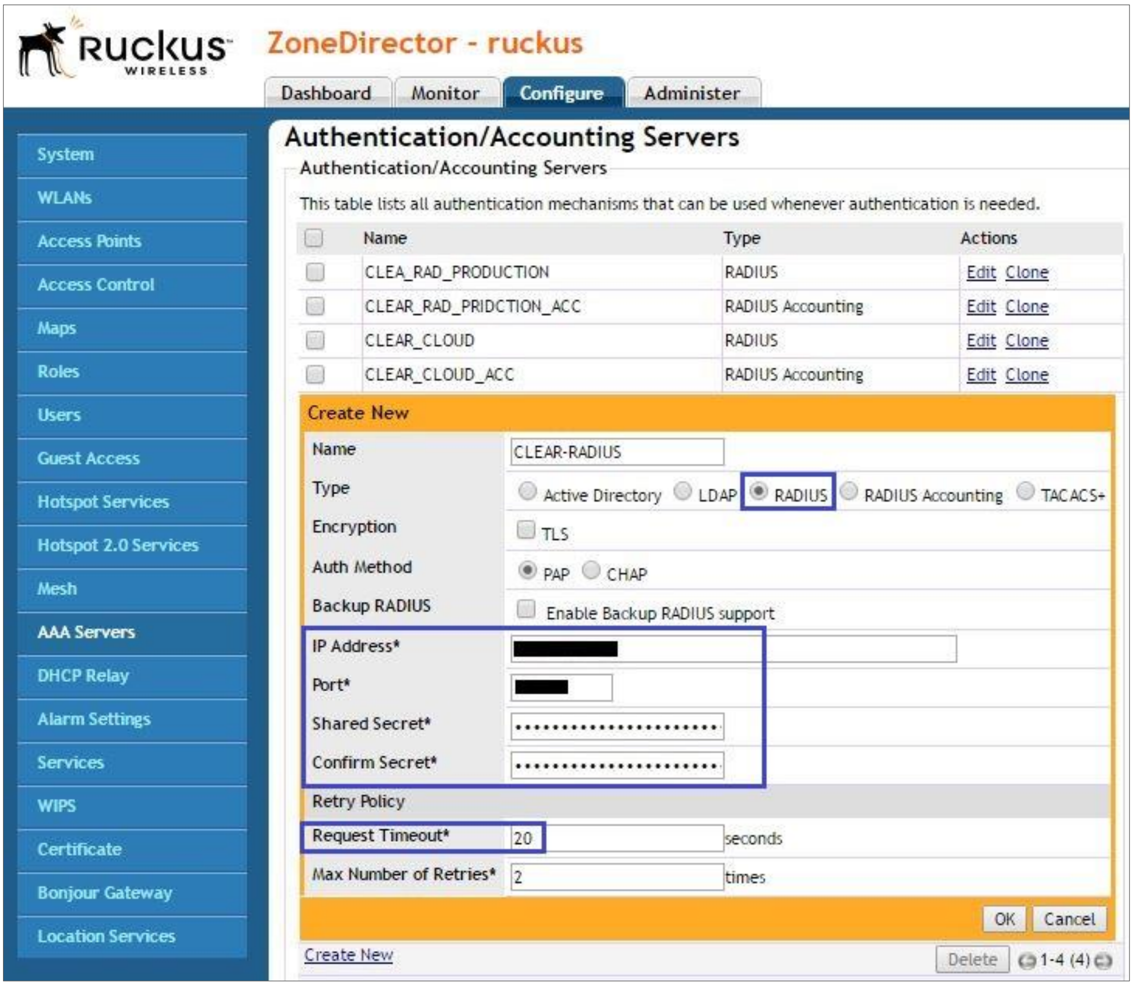
   a. Specify a **Name** for the RADIUS server.

   b. Select the **RADIUS** type.

   c. Set **Request Timeout** to **20** seconds.

   d. Enter the following CLEAR RADIUS server details, which you noted in Enabling CLEAR RADIUS Service, step (2) b:

   - In **IP Address**, enter the Cloud RADIUS IP.
   - In **Port**, enter the Authentication port number.
   - In **Shared Secret**, enter the Shared Secret and then confirm it.



Authentication/Accounting Servers

Authentication/Accounting Servers

This table lists all authentication mechanisms that can be used whenever authentication is needed.

□	Name	Type	Actions
□	CLEA_RAD_PRODUCTION	RADIUS	Edit Clone
□	CLEAR_RAD_PRIDCTION_ACC	RADIUS Accounting	Edit Clone
□	CLEAR_CLOUD	RADIUS	Edit Clone
□	CLEAR_CLOUD_ACC	RADIUS Accounting	Edit Clone

Create New

Name	CLEAR-RADIUS
Type	○ Active Directory ○ LDAP ● RADIUS ○ RADIUS Accounting ○ TACACS+
Encryption	□ TLS
Auth Method	● PAP ○ CHAP
Backup RADIUS	□ Enable Backup RADIUS support
IP Address*	[redacted]
Port*	[redacted]
Shared Secret*	••••••••••••••••••••••
Confirm Secret*	••••••••••••••••••••••
Retry Policy	
Request Timeout*	20 seconds
Max Number of Retries*	2 times

2) Add a Radius Accounting server by navigating to **Configure** > **AAA Servers** and clicking **Create New**.

   In the window that appears:

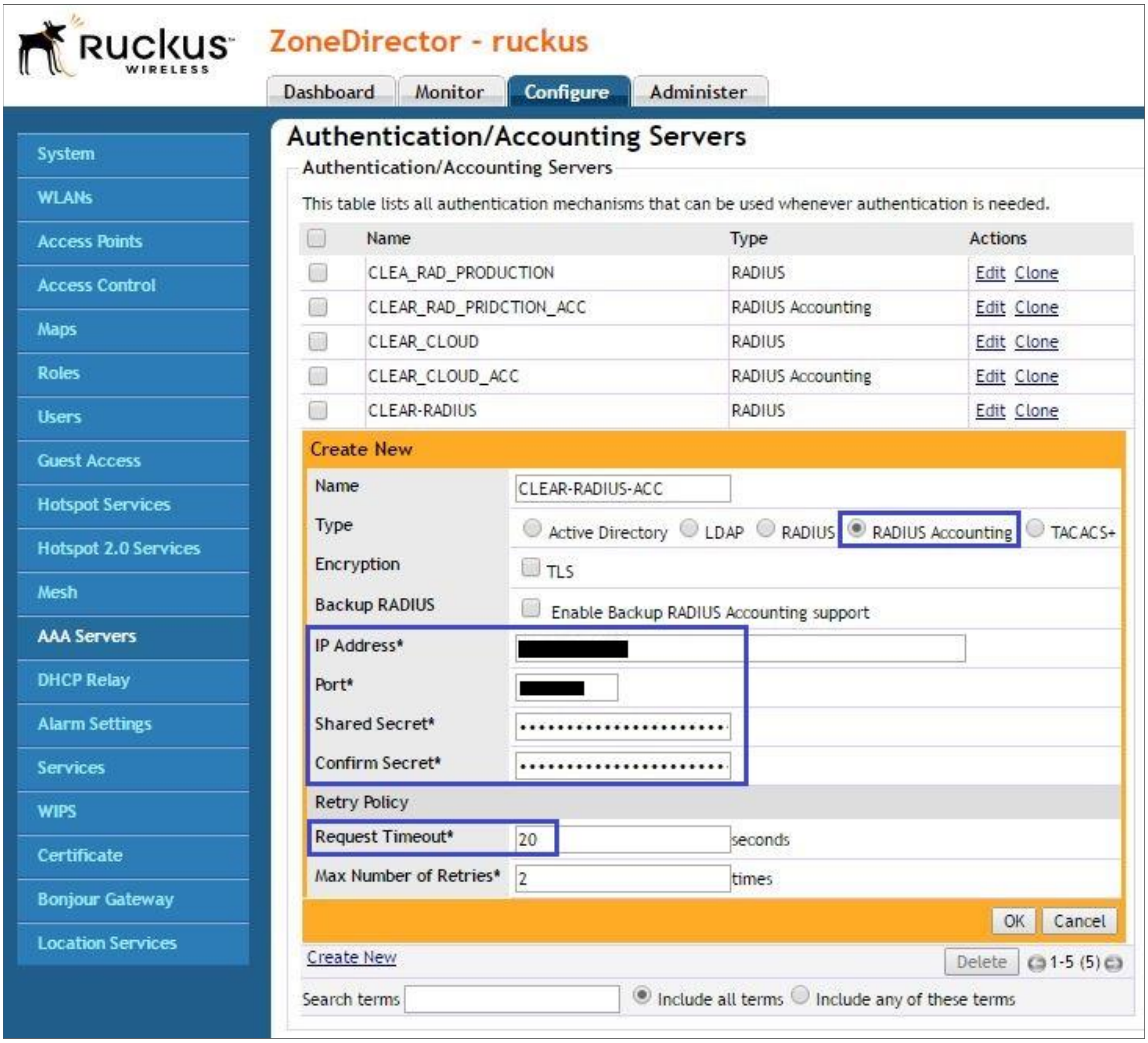
   a. Specify a **Name** for the RADIUS Accounting server.

   b. Select the **RADIUS Accounting** type.

   c. Set **Request Timeout** to **20** seconds.

   d. Enter the following CLEAR RADIUS Accounting server details, which you noted in Enabling CLEAR RADIUS Service, step (2) b:

      - In **IP Address**, enter the Cloud RADIUS IP.
      - In **Port**, enter the Accounting port number.
      - In **Shared Secret**, enter the Shared Secret and then confirm it.



Authentication/Accounting Servers

Authentication/Accounting Servers

This table lists all authentication mechanisms that can be used whenever authentication is needed.

□	Name	Type	Actions
□	CLEA_RAD_PRODUCTION	RADIUS	Edit Clone
□	CLEAR_RAD_PRIDCTION_ACC	RADIUS Accounting	Edit Clone
□	CLEAR_CLOUD	RADIUS	Edit Clone
□	CLEAR_CLOUD_ACC	RADIUS Accounting	Edit Clone
□	CLEAR-RADIUS	RADIUS	Edit Clone

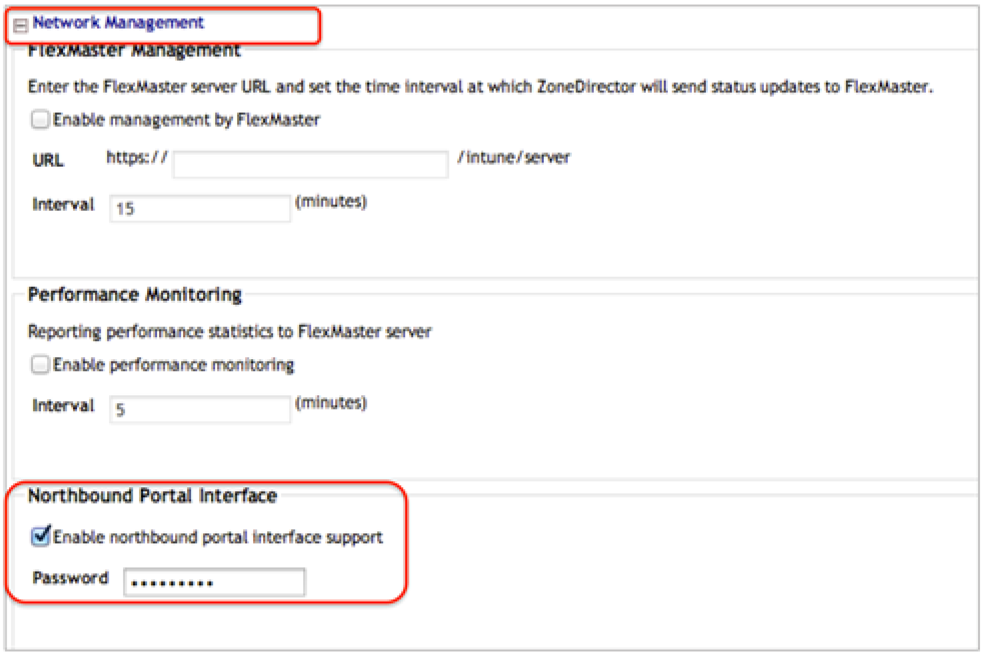
Create New

Name	CLEAR-RADIUS-ACC
Type	○ Active Directory ○ LDAP ○ RADIUS ● RADIUS Accounting ○ TACACS+
Encryption	□ TLS
Backup RADIUS	□ Enable Backup RADIUS Accounting support
IP Address*	[redacted]
Port*	[redacted]
Shared Secret*	••••••••••••••••••••••
Confirm Secret*	••••••••••••••••••••••
Retry Policy	
Request Timeout*	20 seconds
Max Number of Retries*	2 times

3) Configure Ruckus Northbound Portal Interface:

   a. Navigate to Configuration > Network Management and check the enable northbound portal interface support.

   b. In the password field enter the Shared Secret which you noted in Enable CLEAR Captive Portal Service and click apply.



Network Management

FlexMaster Management

Enter the FlexMaster server URL and set the time interval at which ZoneDirector will send status updates to FlexMaster.

□ Enable management by FlexMaster

URL https:// /intune/server

Interval 15 (minutes)

Performance Monitoring

Reporting performance statistics to FlexMaster server

□ Enable performance monitoring

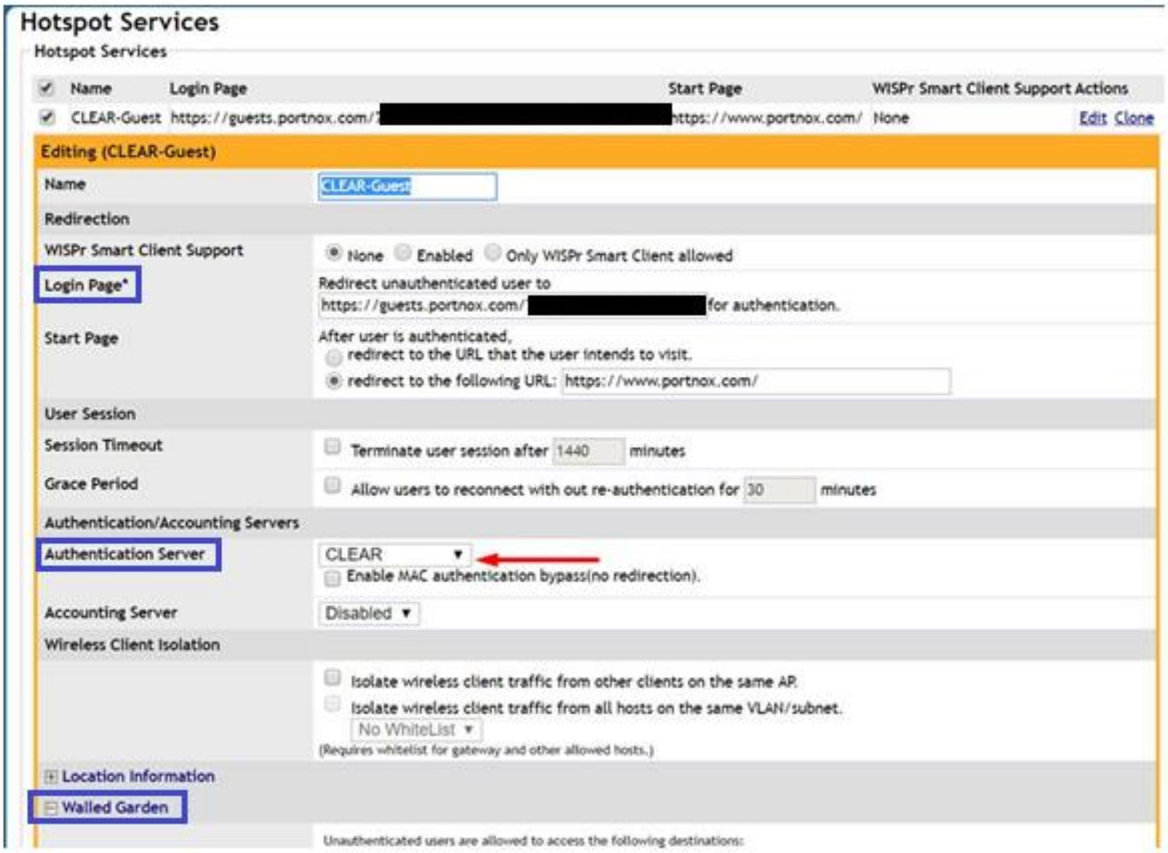
Interval 5 (minutes)

Northbound Portal Interface

☑ Enable northbound portal interface support

Password •••••••••

4) Add Ruckus Hotspot Service to control guest user access:
   Navigate to Services & Profiles > Hotspot Services and create new. In the window that appears:
   a. In **Login Page** field, enter the CLEAR Captive Portal Service URL which you noted in Enabling CLEAR Captive Portal Service.
   b. For the **Authentication Server**, select the Radius server that was created on step #1.
   c. (Optional) For the **Accounting Server**, select the Radius accounting server that was creted on step #2.
   d. In **Walled Garden** add **IP (for walled garden)** which you noted in Enabling CLEAR Captive Portal Service.



Hotspot Services

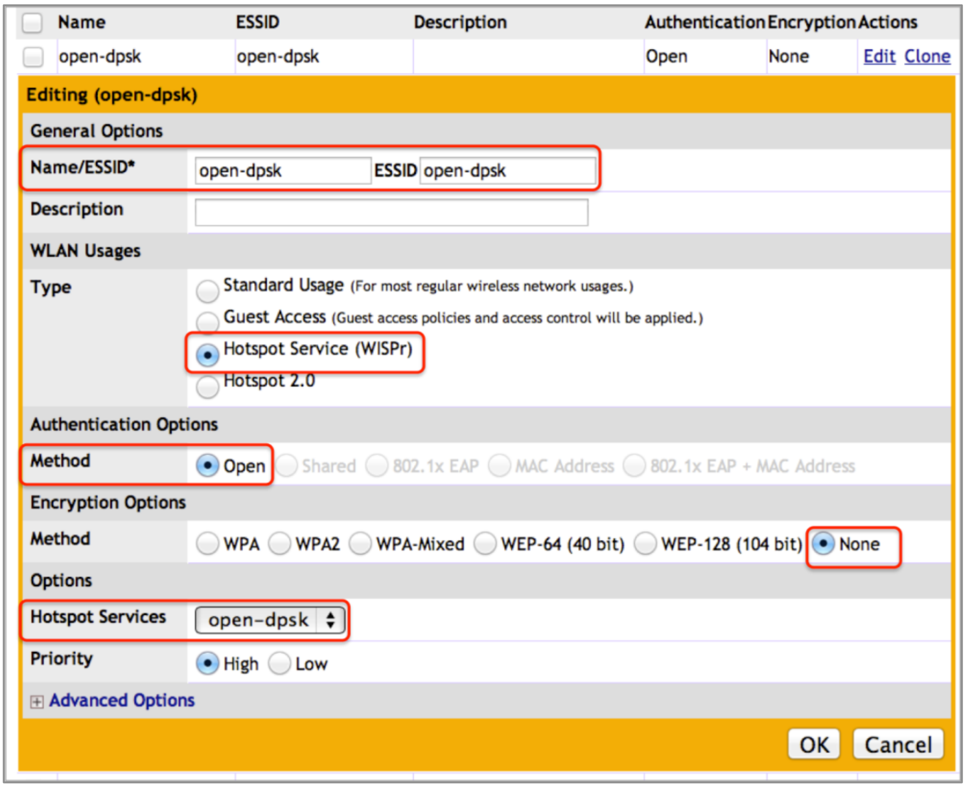
Hotspot Services

☑ Name	Login Page	Start Page	WISPr Smart Client Support	Actions
☑ CLEAR-Guest	https://guests.portnox.com/[redacted]	ttps://www.portnox.com/	None	Edit Clone

Editing (CLEAR-Guest)

Name	CLEAR-Guest
Redirection	
WISPr Smart Client Support	● None ○ Enabled ○ Only WISPr Smart Client allowed
Login Page*	Redirect unauthenticated user to https://guests.portnox.com/[redacted] for authentication.
Start Page	After user is authenticated, ○ redirect to the URL that the user intends to visit. ● redirect to the following URL: https://www.portnox.com/
User Session	
Session Timeout	□ Terminate user session after 1440 minutes
Grace Period	□ Allow users to reconnect with out re-authentication for 30 minutes
Authentication/Accounting Servers	
Authentication Server	CLEAR ▾ □ Enable MAC authentication bypass(no redirection).
Accounting Server	Disabled ▾
Wireless Client Isolation	
	□ Isolate wireless client traffic from other clients on the same AP. □ Isolate wireless client traffic from all hosts on the same VLAN/subnet. No WhiteList ▾ (Requires whitelist for gateway and other allowed hosts.)
⊞ Location Information	
⊟ Walled Garden	
	Unauthenticated users are allowed to access the following destinations:

5) configure the Ruckus guest wireless SSID to control guest user access:
Navigate to Configuration > WLANs and click on Create New. In the window that appears:
   a. Enter the guest SSID name.
   b. Select **Hotspot Service (WISPr)** as the WLAN type.
   c. Select **Open** for the Authentication and **None** for Encryption Options.
   d. Select the hotspot service created on step #4.
   e. Click Ok for save changes



□	Name	ESSID	Description	Authentication	Encryption	Actions
□	open-dpsk	open-dpsk		Open	None	Edit Clone

Editing (open-dpsk)

General Options

Name/ESSID* open-dpsk ESSID open-dpsk

Description

WLAN Usages

Type
○ Standard Usage (For most regular wireless network usages.)
○ Guest Access (Guest access policies and access control will be applied.)
● Hotspot Service (WISPr)
○ Hotspot 2.0

Authentication Options

Method ● Open ○ Shared ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address

Encryption Options

Method ○ WPA ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ● None

Options

Hotspot Services open-dpsk

Priority ● High ○ Low