portnox™
boundlessly smart

How to Configure a Ruckus Wireless Controller to Secure Your Wireless Network

portnox™
CLEAR

LEGAL NOTICE:

Introduction

This document guides you step by step how to configure your Ruckus wireless environment using Portnox CLEAR to ensure secure and trusted 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 switch:
        - **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

Registering the SSID in CLEAR

The second step is to register, in the CLEAR portal, the SSID of the wireless network you will be securing.

1) Navigate in the portal to **Settings** > **Groups**.
2) Edit the default "Unassigned" group or create a new security group.
3) Whether you are creating or editing a group, in **Group Settings** click **Add Wi-Fi network** and specify the **SSID** of the network you will be securing.

Configuring the Ruckus Wireless SSID

In the following steps, we configure the Ruckus wireless SSID to be secured and protected based on CLEAR RADIUS authentication.

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

   In the window that appears:

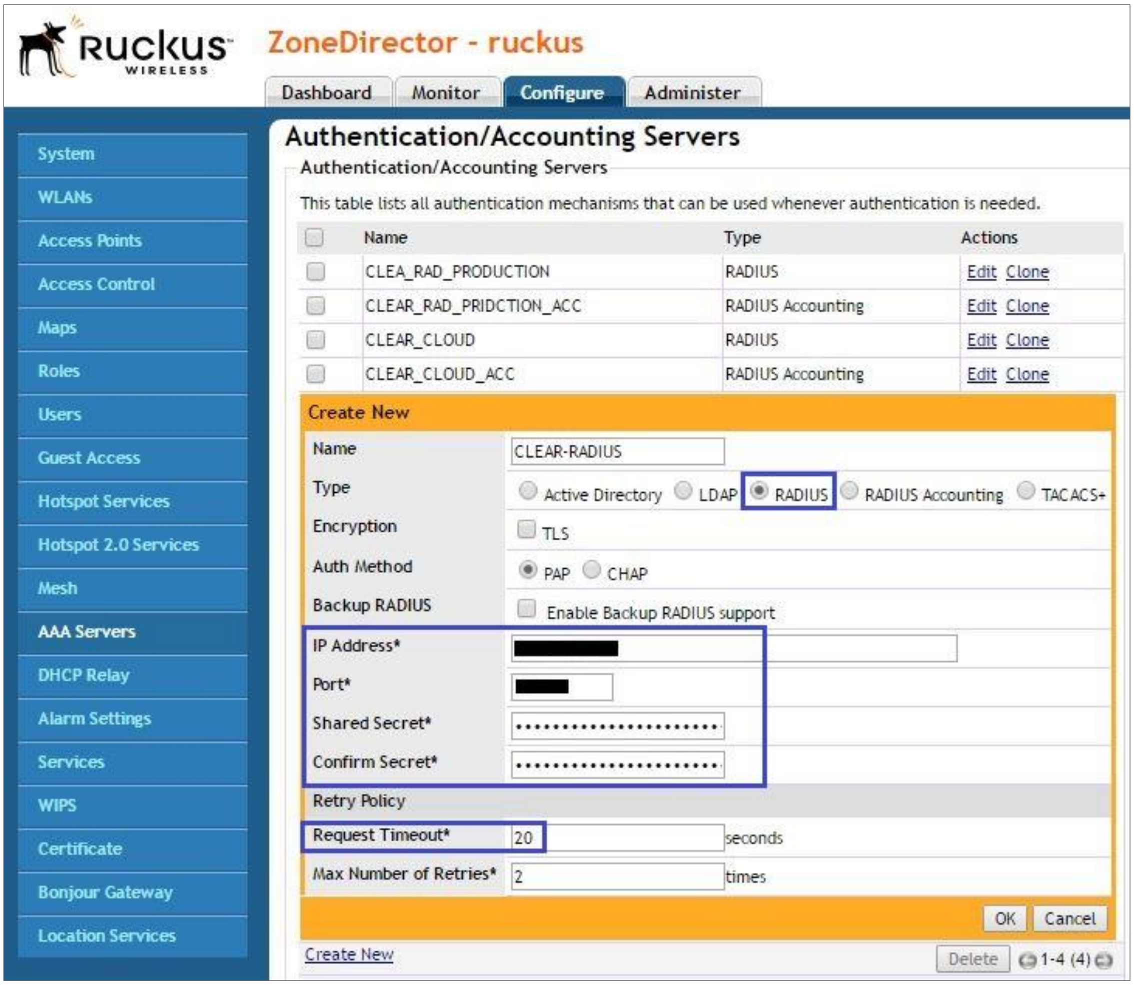
   a. Specify a **Name** for the RADIUS server.

   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:

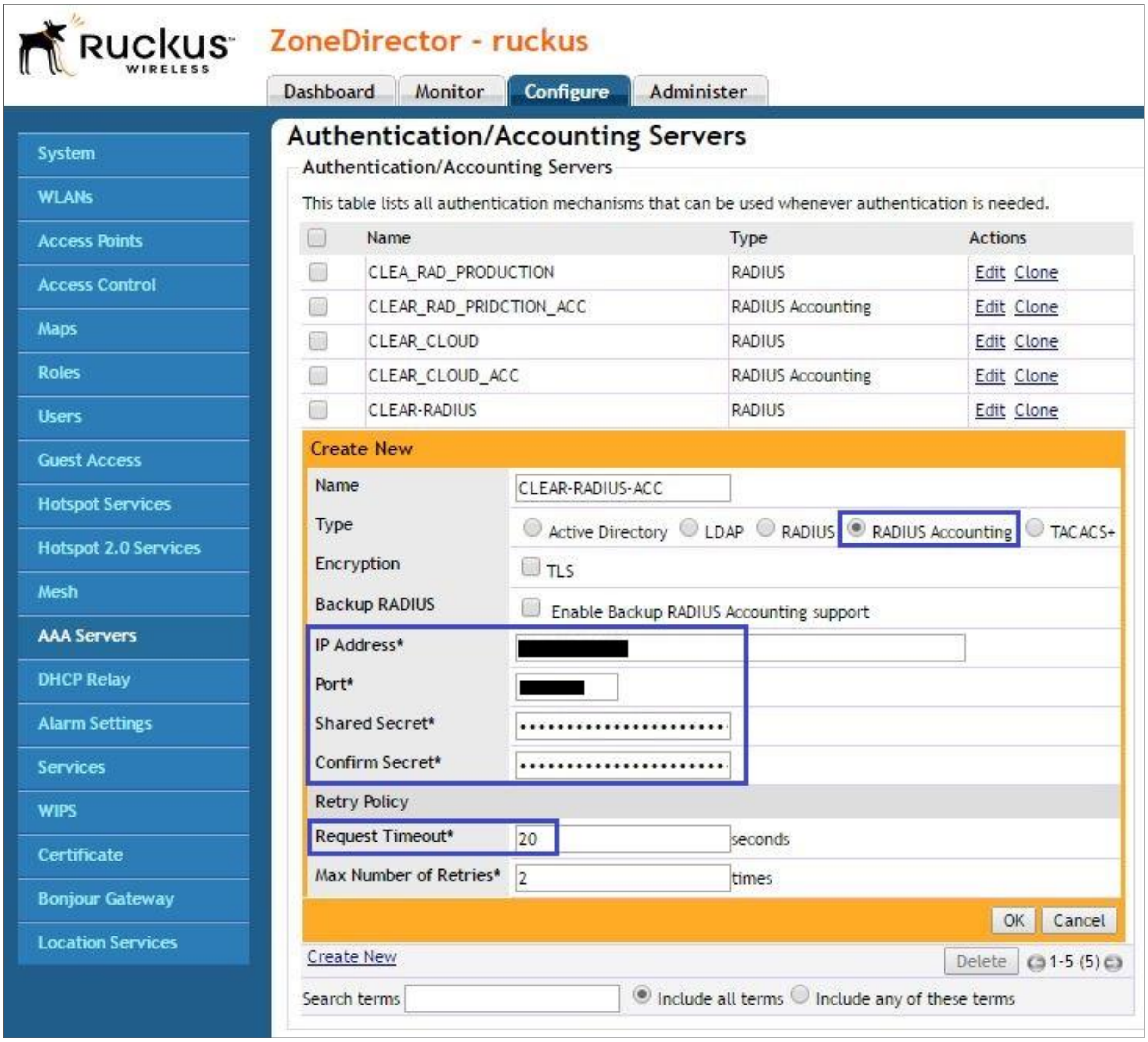
a. Specify a **Name** for the RADIUS Accounting server.

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

Search terms ● Include all terms ○ Include any of these terms

3) Add a new SSID (or edit an existing SSID) by navigating to **Configure → WLANs** and clicking **Create New**.

In the windows that appears:

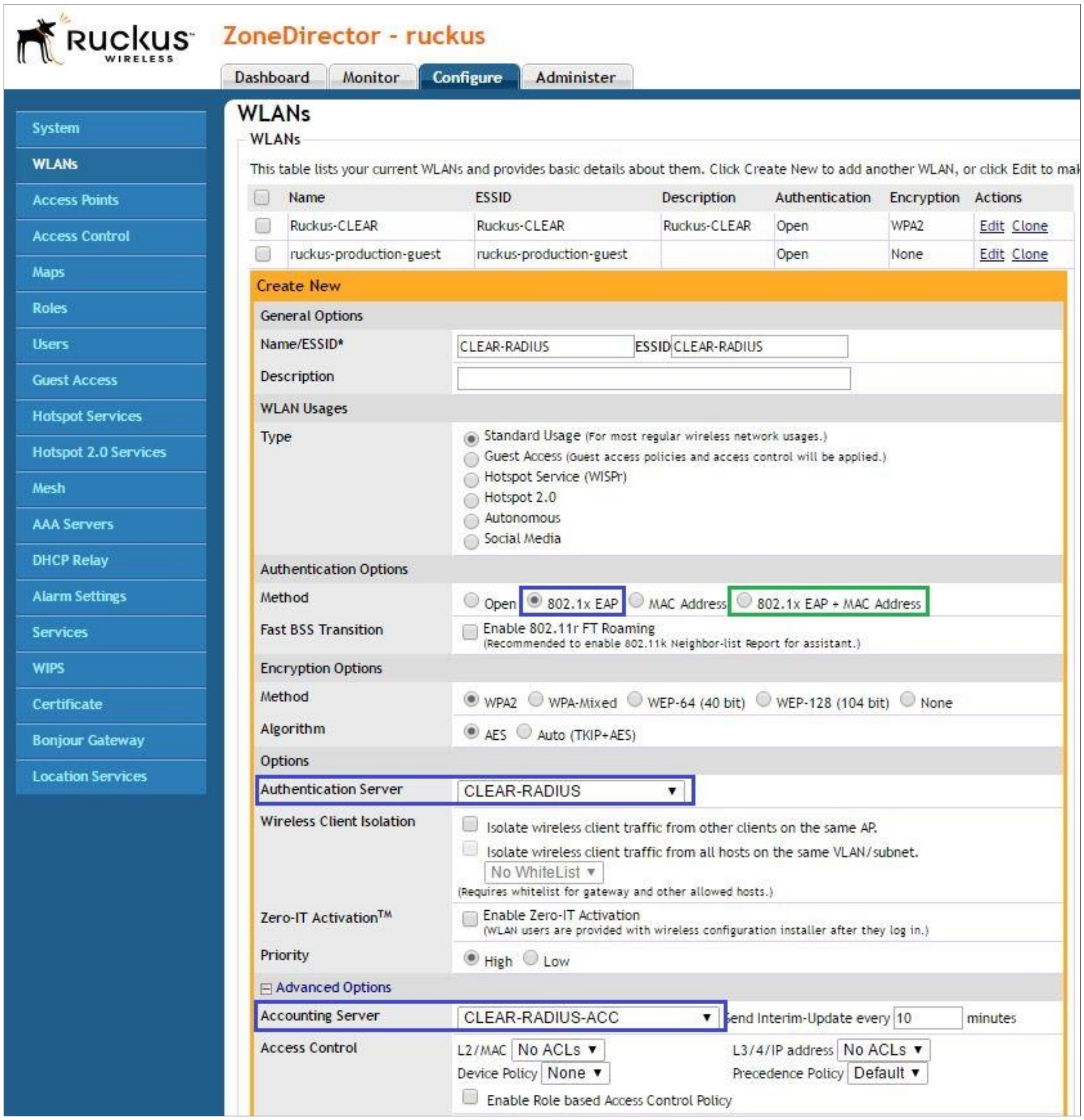
a. Specify a **Name** for the SSID.

b. In **Authentication Options**:

- If the end-point devices support 802.1x authentication, select the **802.1x EAP Method** and in **Encryption Options**, select **WPA2**.
- If the end-point devices do not support 802.1x authentication, select the **802.1x EAP + MAC Address** method.

c. In **Authentication Server**, select the RADIUS server that was created in Step (1).

d. In **Advanced Options** > **Accounting Server**, select the RADIUS Accounting server that was created in Step (2).



ZoneDirector - ruckus

WLANs

WLANs

This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN, or click Edit to mak

□	Name	ESSID	Description	Authentication	Encryption	Actions
□	Ruckus-CLEAR	Ruckus-CLEAR	Ruckus-CLEAR	Open	WPA2	Edit Clone
□	ruckus-production-guest	ruckus-production-guest		Open	None	Edit Clone

Create New

General Options

Name/ESSID* CLEAR-RADIUS ESSID CLEAR-RADIUS

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
○ Autonomous
○ Social Media

Authentication Options

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

Fast BSS Transition □ Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)

Encryption Options

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

Algorithm ● AES ○ Auto (TKIP+AES)

Options

Authentication Server CLEAR-RADIUS ▾

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.)

Zero-IT Activation™ □ Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)

Priority ● High ○ Low

⊟ Advanced Options

Accounting Server CLEAR-RADIUS-ACC ▾ Send Interim-Update every 10 minutes

Access Control
L2/MAC No ACLs ▾ L3/4/IP address No ACLs ▾
Device Policy None ▾ Precedence Policy Default ▾
□ Enable Role based Access Control Policy