

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



#### LEGAL NOTICE:

Copyright © 2017 Access Layers US, Inc. (Portnox)

All rights reserved. Proprietary and confidential material.



# 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: <u>https://clear.portnox.com/</u>.
- 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 <u>Enabling CLEAR RADIUS Service</u>, 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.

	Dashboard Mo	nitor Configure	Administer			
Svstem	Authenticat	ion/Accounting	Servers			
MIL AMP	Authentication	Accounting Servers				
WLANS	This table lists all	authentication mechanisms t	hat can be used whenever authenti	ication is needed.		
Access Points	Name		Туре	Actions		
Access Control	CLEA_RAI	D_PRODUCTION	RADIUS	Edit Clone		
Mans	CLEAR_R	AD_PRIDCTION_ACC	RADIUS Accounting	Edit Clone		
	CLEAR_C	LOUD	RADIUS	Edit Clone		
Roles	CLEAR_C	LOUD_ACC	RADIUS Accounting	Edit Clone		
Users	Create New					
Guest Access	Name	CLEAR-RADIUS				
Hatcoat Consisor	Туре	Active Directo		S Accounting O TAC		
noispor services	and the second second	-				
	Encryption	TIS				
Hotspot 2.0 Services	Encryption	U TLS				
Hotspot 2.0 Services Mesh	Auth Method	TLS     PAP CHAP				
Hotspot 2.0 Services Mesh AAA Servers	Auth Method Backup RADIUS	TLS     PAP CHAP     CHAP     Enable Backu	p RADIUS support			
Hotspot 2.0 Services Mesh AAA Servers	Auth Method Backup RADIUS	TLS     PAP     CHAP     Enable Backu	p RADIUS support			
Hotspot 2.0 Services Mesh AAA Servers DHCP Relay	Auth Method Backup RADIUS IP Address* Port*	TLS     PAP     CHAP     Enable Backu	p RADIUS support			
Hotspot 2.0 Services Mesh AAA Servers DHCP Relay Alarm Settings	Auth Method Backup RADIUS IP Address* Port* Shared Secret*	TLS     PAP CHAP     Enable Backu	p RADIUS support			
Hotspot 2.0 Services Mesh AAA Servers DHCP Relay Alarm Settings Services	Auth Method Backup RADIUS IP Address* Port* Shared Secret* Confirm Secret	TLS  PAP CHAP Enable Backu	p RADIUS support			
Hotspot 2.0 Services Mesh AAA Servers DHCP Relay Alarm Settings Services WIPS	Encryption Auth Method Backup RADIUS IP Address* Port* Shared Secret* Confirm Secret* Retry Policy	TLS PAP CHAP Enable Backu	p RADIUS support			
Hotspot 2.0 Services Mesh AAA Servers DHCP Relay Alarm Settings Services WIPS Certificate	Auth Method Backup RADIUS IP Address* Port* Shared Secret* Confirm Secret* Retry Policy Request Timeou	TLS PAP CHAP Enable Backu	p RADIUS support			
Hotspot 2.0 Services Mesh AAA Servers DHCP Relay Alarm Settings Services WIPS Certificate Boniour Gateway	Auth Method Backup RADIUS IP Address* Port* Shared Secret* Confirm Secret* Retry Policy Request Timeou Max Number of	tt* 20 Retries* 2	p RADIUS support			



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.

	Dashbo	Dashboard Monitor Configure Administer						
System	Auth	entication	Accounting Sound S	ervers				
WLANs	This t	able lists all authe	ntication mechanisms th	at can be used whenever authenti	ication is needed.			
Access Points		Name		Туре	Actions			
Access Control		CLEA_RAD_PRODUCTION		RADIUS	Edit Clone			
11		CLEAR_RAD_PRIDCTION_ACC		RADIUS Accounting	Edit Clone			
maps		CLEAR_CLOUD		RADIUS	Edit Clone			
Roles		CLEAR_CLOUD_ACC		RADIUS Accounting	Edit Clone			
Users		CLEAR-RADIUS		RADIUS	Edit Clone			
Guest Access	Crea	ate New						
Hotspot Services	Name Type Encryption		CLEAR-RADIUS-ACC					
			Active Director	y 🔍 LDAP 🔍 RADIUS 🖲 RADIU:	S Accounting O TAC AC			
Hotspot 2.0 Services			TLS .					
	Enc	ryption	TLS					
Mesh	Enc	ryption kup RADIUS	Enable Backup	PADIUS Accounting support				
Mesh AAA Servers	Enc Bac	ryption kup RADIUS ddress*	Enable Backup	RADIUS Accounting support				
Mesh AAA Servers DHCP Relay	Enc Bac IP A Port	ryption kup RADIUS ddress*	Enable Backup	RADIUS Accounting support				
Mesh AAA Servers DHCP Relay Alarm Settions	Enc Bac IP A Port	ryption kup RADIUS ddress* :*	Enable Backup	RADIUS Accounting support				
Mesh AAA Servers DHCP Relay Alarm Settings	Enc Bac IP A Port Sha	ryption kup RADIUS ddress* * red Secret*	Enable Backup	RADIUS Accounting support				
Mesh AAA Servers DHCP Relay Alarm Settings Services	Enc Bac IP A Port Sha Con	ryption kup RADIUS ddress* :* red Secret* firm Secret*	Enable Backup	RADIUS Accounting support				
Mesh AAA Servers DHCP Relay Alarm Settings Services WIPS	Enc Bac IP A Port Sha Con Retu	ryption kup RADIUS ddress* * red Secret* firm Secret* ry Policy	Enable Backup	RADIUS Accounting support				
Mesh AAA Servers DHCP Relay Alarm Settings Services WIPS Certificate	Enc Bac IP A Port Sha Con Retu Req	ryption kup RADIUS ddress* ** red Secret* firm Secret* ry Policy uest Timeout*	Enable Backup	RADIUS Accounting support				
Mesh AAA Servers DHCP Relay Alarm Settings Services WIPS Certificate Boniour Gateway	Enc Bac IP A Port Sha Con Retu Req Max	ryption kup RADIUS ddress* red Secret* firm Secret* ry Policy uest Timeout*	20 22	RADIUS Accounting support				



- 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).

	Dashboard Monitor	Configure Administer							
ystem	WLANs WLANs								
VLANs	This table lists your current W	/LANs and provides basic detail	about them. Click Cr	eate New to add ar	nother WLAN,	or click Edit t			
access Points	Name	ESSID	Description	Authentication	Encryption	Actions			
ccess Control	Ruckus-CLEAR	Ruckus-CLEAR	Ruckus-CLEAR	Open	WPA2	Edit Clon			
aps	ruckus-production-gue	st ruckus-production-gues	t	Open	None	Edit Clon			
oles	Create New	Create New							
	General Options								
sers	Name/ESSID*	CLEAR-RADIUS	ESSID CLEAR-RADIUS	5					
uest Access	Description								
otspot Services	WLAN Usages								
lotspot 2.0 Services	Туре	<ul> <li>Standard Usage (For m Guest Access (Guest acc Useback Science)</li> </ul>	ost regular wireless netw ess policies and access c	ork usages.) ontrol will be applied	.)				
lesh		Hotspot 2.0	)						
AA Servers		Autonomous Social Media							
HCP Relay	Authentication Options	Authentication Options							
larm Settings	Method Open  802.1x EAP MAC Address 802.1x EAP + MAC Address								
ervices	Fast BSS Transition Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)								
/IPS	Encryption Options	Encryption Options							
ertificate	Method	thod      WPA2      WPA-Mixed      WEP-64 (40 bit)      WEP-128 (104 bit)      None							
oniour Gateway	Algorithm       ALS  Auto (TKIP+AES)								
	Options								
ocation services	Authentication Server	CLEAR-RADIUS							
	Wireless Client Isolation	Isolate wireless client	traffic from other clie	nts on the same AP.					
		Isolate wireless client traffic from all hosts on the same VLAN/subnet.							
		No WhiteList   (Requires whitelist for gateway)	v and other allowed host	s.)					
	Zero-IT Activation <sup>TM</sup>	Activation <sup>TM</sup> 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 l	nterim-Update eve	ry 10	minutes			
	Access Control	L2/MAC No ACLS V	L3/4	1/IP address No A	CLs V				
		Device Policy None V	Preo	edence Policy Def	ault 🔻				

