



INTEGRATION GUIDE

How to Configure Aruba 1930 (Instant-on) Switch to Secure your Wired Network with Portnox CLEAR

## Introduction

This document guides you step by step how to configure your Aruba 1930 (Instant-On) wired switch 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 WatchGuard 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

## Allow Access to Wired Networks in CLEAR

The second step is to allow, in the CLEAR portal, access to wired networks 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** check the **Enable wired access using 802.1x authentication for devices in this group** check box.

ACCESS TO WIRED NETWORKS

Manage 802.1X authenticated access to wired networks for all devices in this group.

Enable wired access using 802.1x authentication for devices in this group.

<u>Edit</u>

## Configuring the Aruba Wired Switch

In the final step, we configure the Aruba wired switch to be secured and protected based on CLEAR RADIUS authentication.

Under "Security" -> RADIUS Configuration" -> add a new "RADIUS Server":

E Orubo	Security > RADIUS Configuration	ß	ø	? ~	8~
Dashboard	Global Configuration				
Setup Network	802.1x Authentication Mode				
Spanning Tree	802.1x Accounting Mode				
VLAN	Contraction of Determined				
Neighbor Discovery	3 (1 - 19)				
Routing	Timeout Duration				
Quality of Service	3 (1 - 30) Seconds				
Security ^					
RADIUS Configuration	RADIUS Server Configuration	Add erver Priority	G Dis	əlay: 10 ∨	· ¥
Port Security					
Protected Ports	Table Is Empty				
DHCP Snooping					
ARP Attack Protection					
Denial of Service Protection					
HTTPS Certificate					
Diagnostics			-	EFRESH	APPLY

i Add RADIUS Server		×
Server IP Address		
50.95.102.5		
Authentication Port		
22564		
(0 – 65535)		
Accounting Port		
22565		
(0 – 65535)		
Server Priority		
(0 – 65535)		
Secret		
(1 – 128 characters)		
	CANCEL	APPLY

RADIUS Server details can be found in CLEAR tenant under "Settings" - > "CLEAR RADIUS SERVICE" -> "Europe and Asia" / "United States and North America"

O clear Dashboard	Alerts Devices Settings	Groups Policies	Guests Troubleshooting	Help
SERVICES         Manage Portnox <sup>TM</sup> CLEAR services         General definitions of CLEAR that are related to all of the services provided by CLEAR.				
AUTHENTICATION REPOSITORIES Connect external user repositories to CLEAR	The CLEAR RADIUS service, provid authentication of users accessing 1 CLEAR's cloud RADIUS service, CLE RADIUS information you need to c	ed through a cloud-based clu the enterprise – whether thro EAR automatically generates I configure in all your RADIUS o	uster of fully redundant RADIUS server ough wired, wireless or VPN channels. N RADIUS services for your organization, clients (network devices and equipmer	s, is used for When you enable and lists the t).
INTEGRATION SERVICES	- Europe and Asia		]	<u>Edit</u> <u>Remove</u>
with CLEAR	Cloud RADIUS IP:			0
ORGANIZATION	Authentication port:			0
Edit organization's settings	Accounting port:	**** 🕞 Show	Regenerate	0
	Enable RADIUS over TLS (F	RadSec)	Download root certifica	te 🕜
ADMINISTRATORS Manage CLEAR administrators	RESTRICT ACCESS TO CLEAR RA	ADIUS SERVICE		0
	Default rule: 🛛 🥑	Allow access from any IP ad Allow access only from the f	dress following IP addresses	
	+ United States and North Ar	merica	1	<u>Edit Remove</u>
	CUSTOM RADIUS ATTRIBUTES			
	Click to specify custom RADIUS at	tributes		
	Specify custom RADIUS attributes			0
	RADIUS ANTI-FLOOD PROTECTION			
	Click to control blocked devices			

Under "Security" -> "RADIUS Configuration" -> "Global Configuration" -> check "802.1x Authentication Mode"

	Security > RADIUS Configuration	
Dashboard	Global Configuration	
Setup Network	802.1x Authentication Mode	
Switching		
Spanning Tree	802.1x Accounting Mode	
VLAN	Max Number of Retransmits	
Neighbor Discovery	3	
Routing	Timeout Duration	
Quality of Service	3 (1 - 30) Seconds	
Security ^		
RADIUS Configuration	RADIUS Server Configuration	
Port Access Control	Current   IP Address	Authentication P
Port Security		
Protected Ports		
DHCP Snooping		
ARP Attack Protection		

Under "Security" -> "Port Access Control" -> check the "Admin Mode".

Under "Security" -> "Port Access Control" -> "Port Configuration", choose relevant 802.1X ports, mark them as "MAC Based" control mode, and click "APPLY" at the bottom of the page.

i Edit Port Configuration		×
		<b>^</b>
Interface 5		
PAE Capabilities		
Authenticator Supplicant		
Control Mode		
Force Authorized -		
Auto		- 1
Force Authorized		
Force Unauthorized		
MAC Based		
30		
(30 – 65535) Seconds		
Monitor Mode		
VLAN Assignment		
Guest VLAN		
	CANCEL	APPLY

Please note, in order to allow "Mac Based Authentication" (MAB), you will need to check "MAC Authentication" option as well.

i Edit Port Configuration	×
	•
Supplicant Timeout	
30	
(1 – 65535) Seconds	
Server Timeout	
30	
(1 – 65535) Seconds	
Maximum Requests	
2	
(1 - 10)	
MAC Authentication	
-	
Re-Authentication Period	
Never	CANCEL CANCEL