

INTEGRATION GUIDE

How to Configure an Aruba Wireless Controller to Secure your Wireless Network with Portnox CLEAR

Introduction

This document guides you step by step how to configure your Aruba 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 SSID:
 - **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

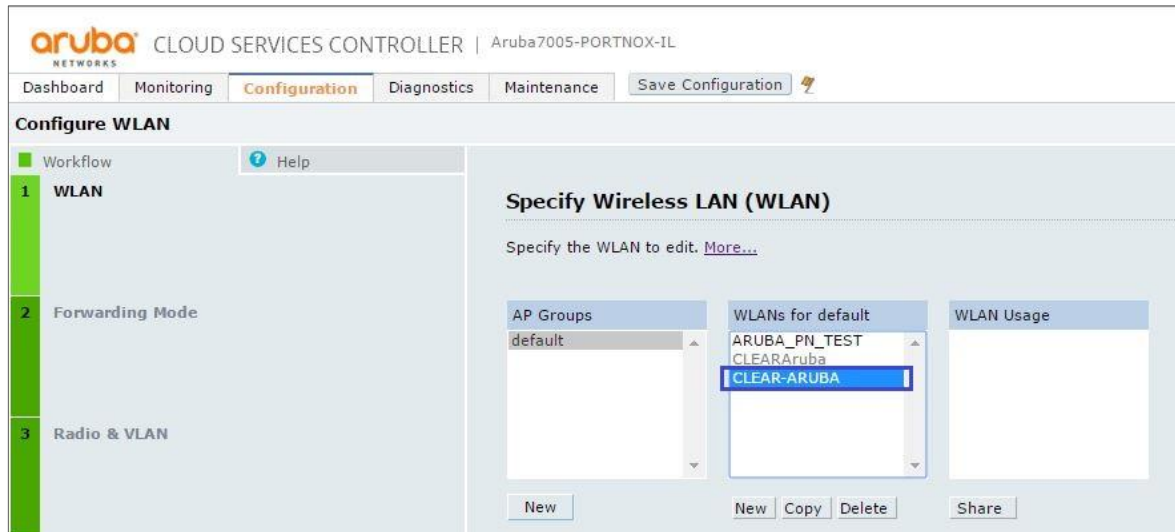
The second step is to register, in the CLEAR portal, the SSID of the wireless network you will be securing.

- 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 Aruba Wireless SSID

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

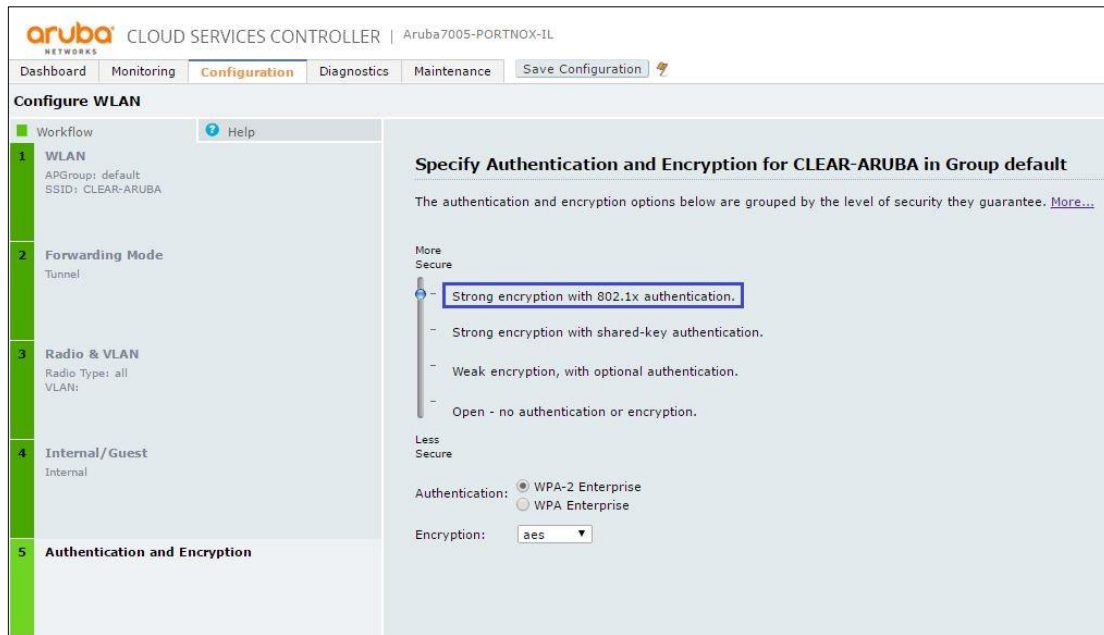
- 1) In the Aruba web interface, navigate to **Configuration > Wizards > Campus WLAN**, and add a new SSID or select an existing one.



- 2) In the **Internal/Guest** section, select **Internal**.



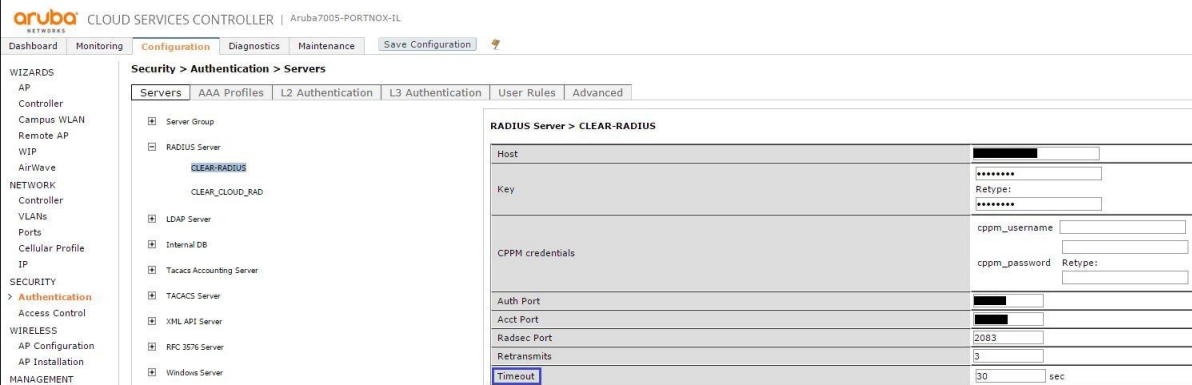
- 3) In the **Authentication and Encryption** section, select **Strong encryption with 802.1x authentication.**



- 4) In the **Authentication Server** section, add a new server.
 - a. In **Server type**, select **RADIUS**.
 - b. 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 **Auth port**, enter the Authentication port.
 - In **Acct port**, enter the Accounting port.
 - In **Shared key**, enter the Shared Secret.

The screenshot displays the Aruba Cloud Services Controller configuration interface. The top navigation bar includes 'Dashboard', 'Monitoring', 'Configuration', 'Diagnostics', and 'Maintenance'. The main content area is titled 'Configure WLAN' and shows a workflow with seven steps: 1. WLAN, 2. Forwarding Mode, 3. Radio & VLAN, 4. Internal/Guest, 5. Authentication and Encryption, 6. Captive Portal, and 7. Authentication Server. The 'Authentication Server' step is currently selected. A dialog box titled 'Specify Authentication Server for CLEAR-ARUBA in Group default' is open, showing an 'Ordered list of Authentication servers' and a form to 'Specify new server'. The form includes fields for Name (CLEAR-RADIUS), IP address, Auth port, Acct port, Shared key, and Retype key. The 'Server type' is set to RADIUS.

- 5) Navigate to **configuration > Security > Authentication > servers**, select the RADIUS server that was created in the previous step, and update the **Timeout** to **30** seconds.



The screenshot displays the Aruba Cloud Services Controller configuration interface. The navigation path is **Configuration > Security > Authentication > Servers**. The left sidebar shows the navigation menu with **Authentication** selected. The main content area shows the configuration for a RADIUS server named **CLEAR-RADIUS**. The **Timeout** field is highlighted in blue and set to **30** seconds.

| RADIUS Server > CLEAR-RADIUS | |
|------------------------------|------------------------------------------------------------------------------|
| Host | [Redacted] |
| Key | ***** Retype: ***** |
| CPPM credentials | cppm_username: [Redacted] cppm_password: [Redacted] Retype: [Redacted] |
| Auth Port | [Redacted] |
| Acct Port | [Redacted] |
| Radsec Port | 2083 |
| Retransmits | 3 |
| Timeout | 30 sec |

- 6) Click **Save Configuration**.