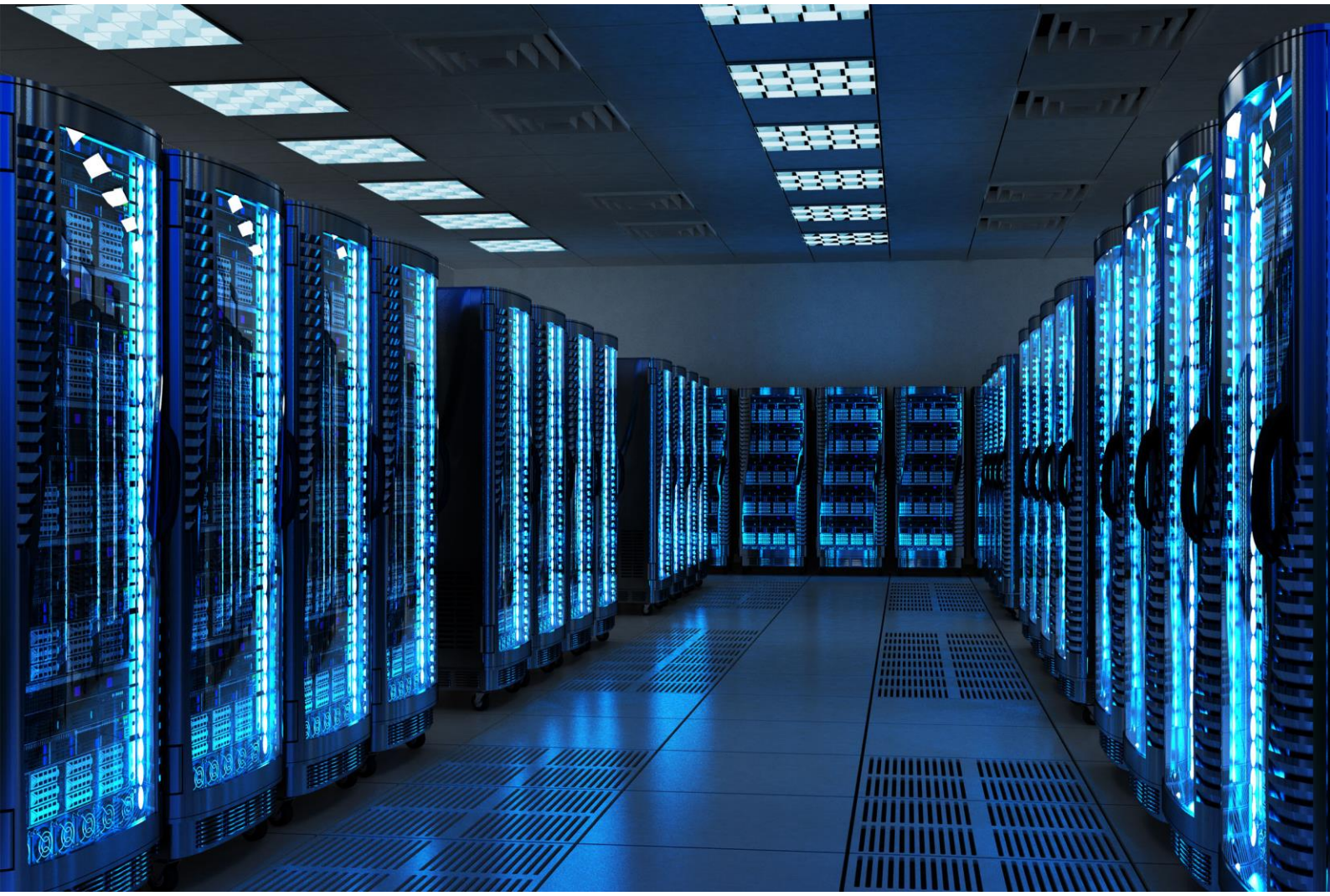
portnox™



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

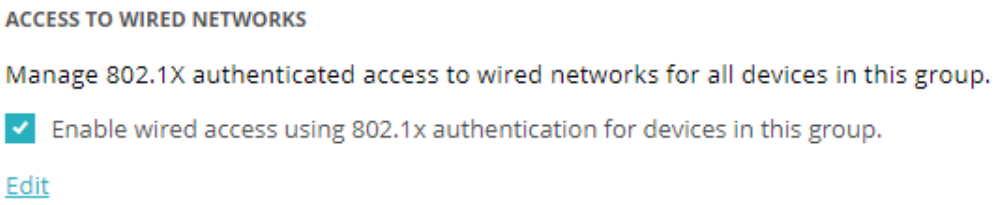
The first step is to enable the CLEAR RADIUS service:

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.

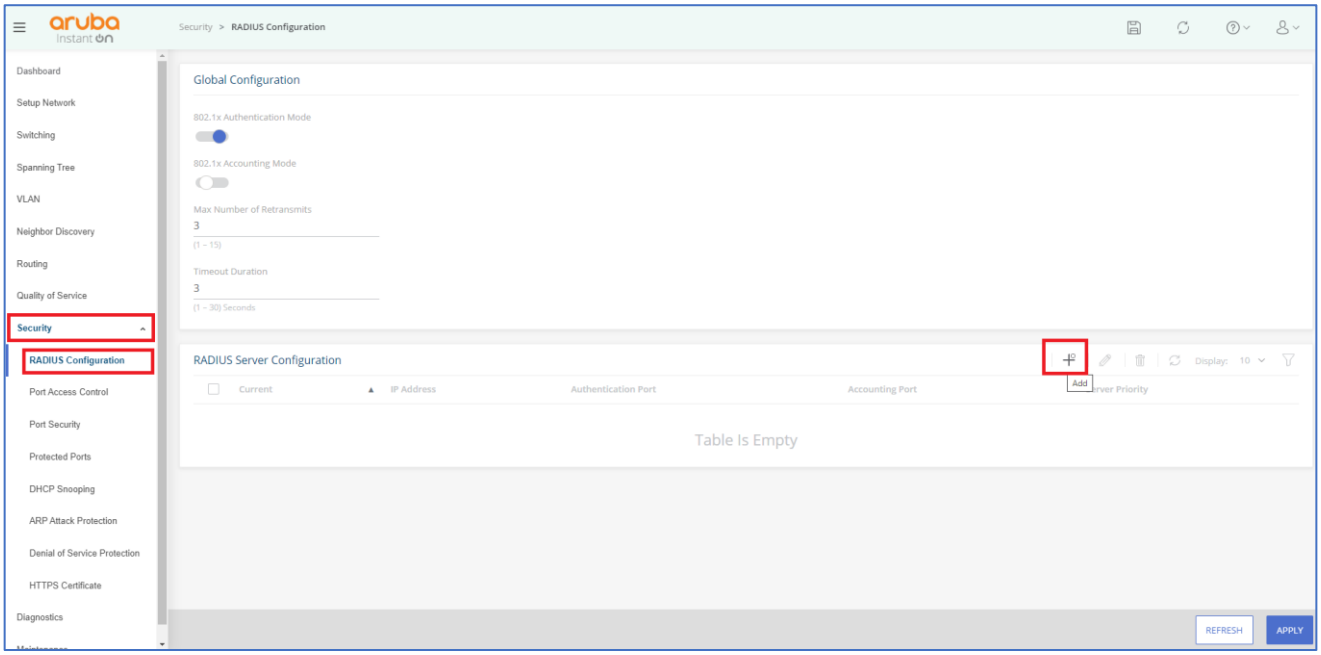
1) Navigate in the portal to **Settings** > **Groups**.
2) Edit the default “Unassigned” group or create a new security group.
3) Whether you are creating or editing a group, in **Group Settings** check the **Enable wired access using 802.1x authentication for devices in this group** check box.

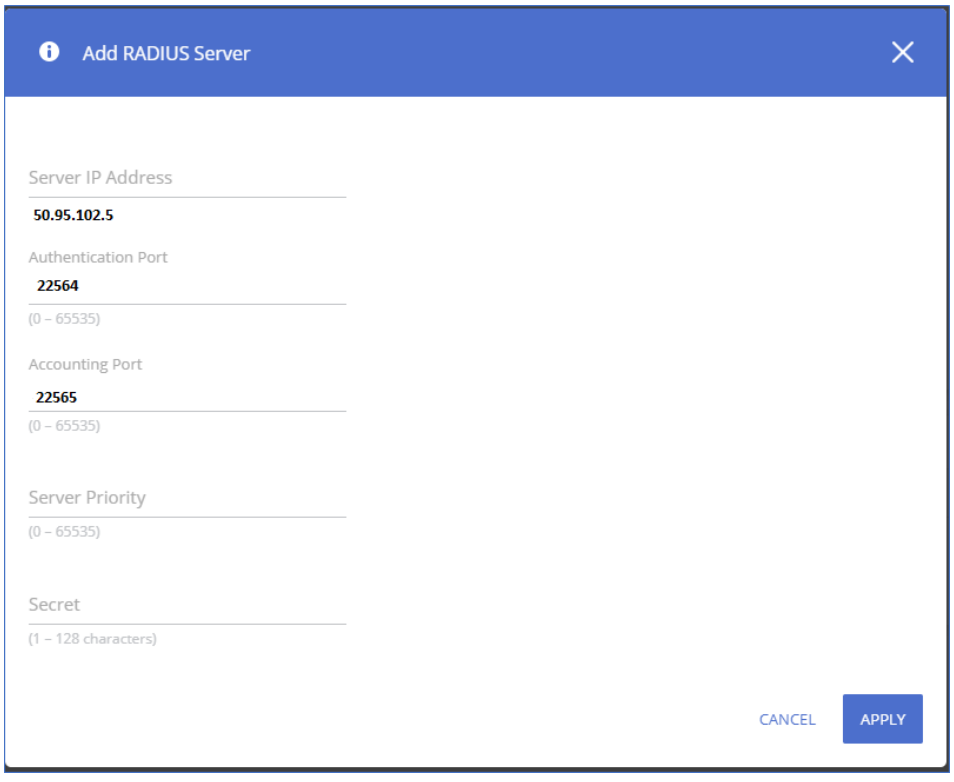


Configuring the Aruba Wired Switch

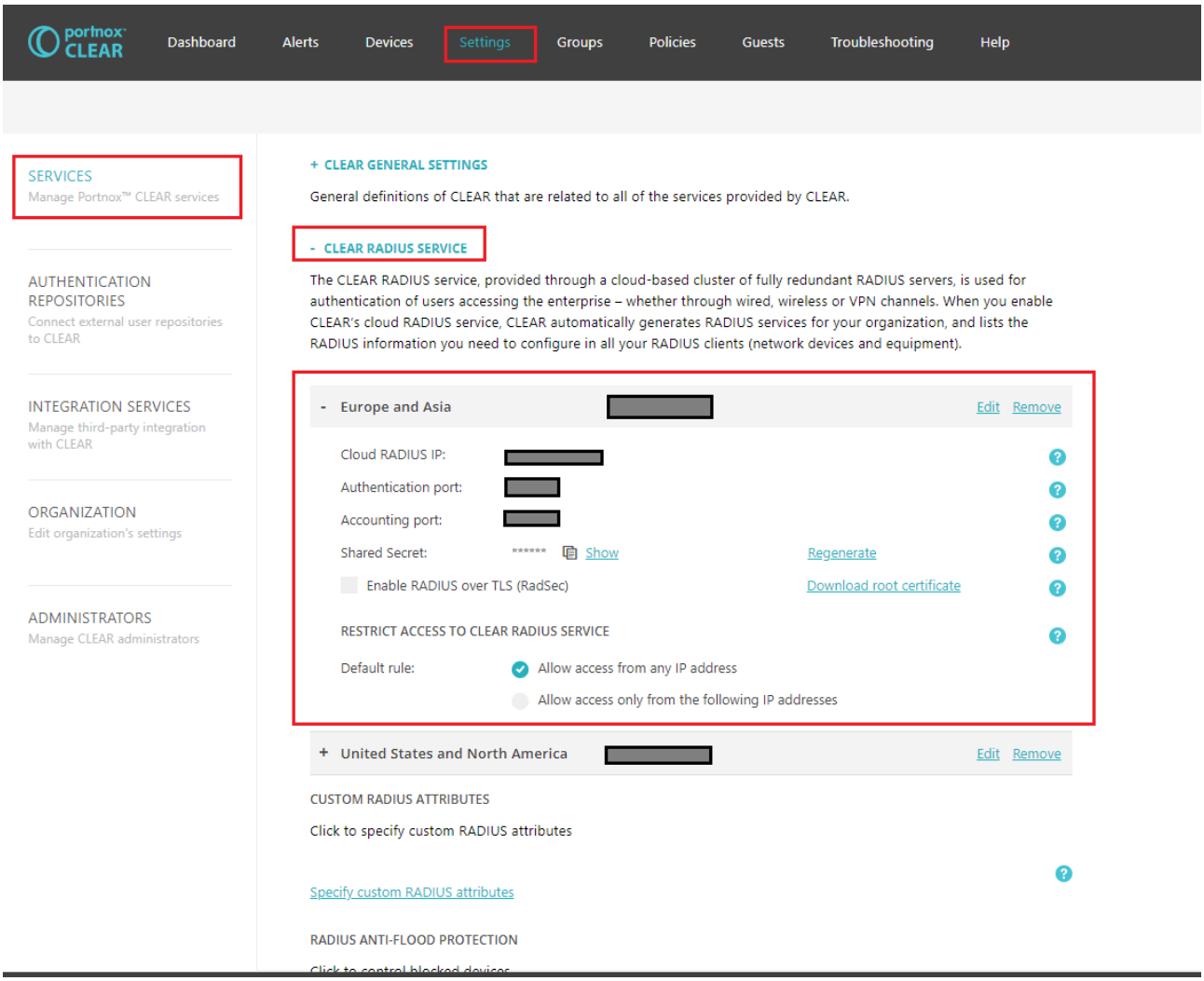
In the final step, we configure the Aruba wired switch to be secured and protected based on CLEAR RADIUS authentication.

Under “Security” - > RADIUS Configuration” -> add a new “RADIUS Server”:

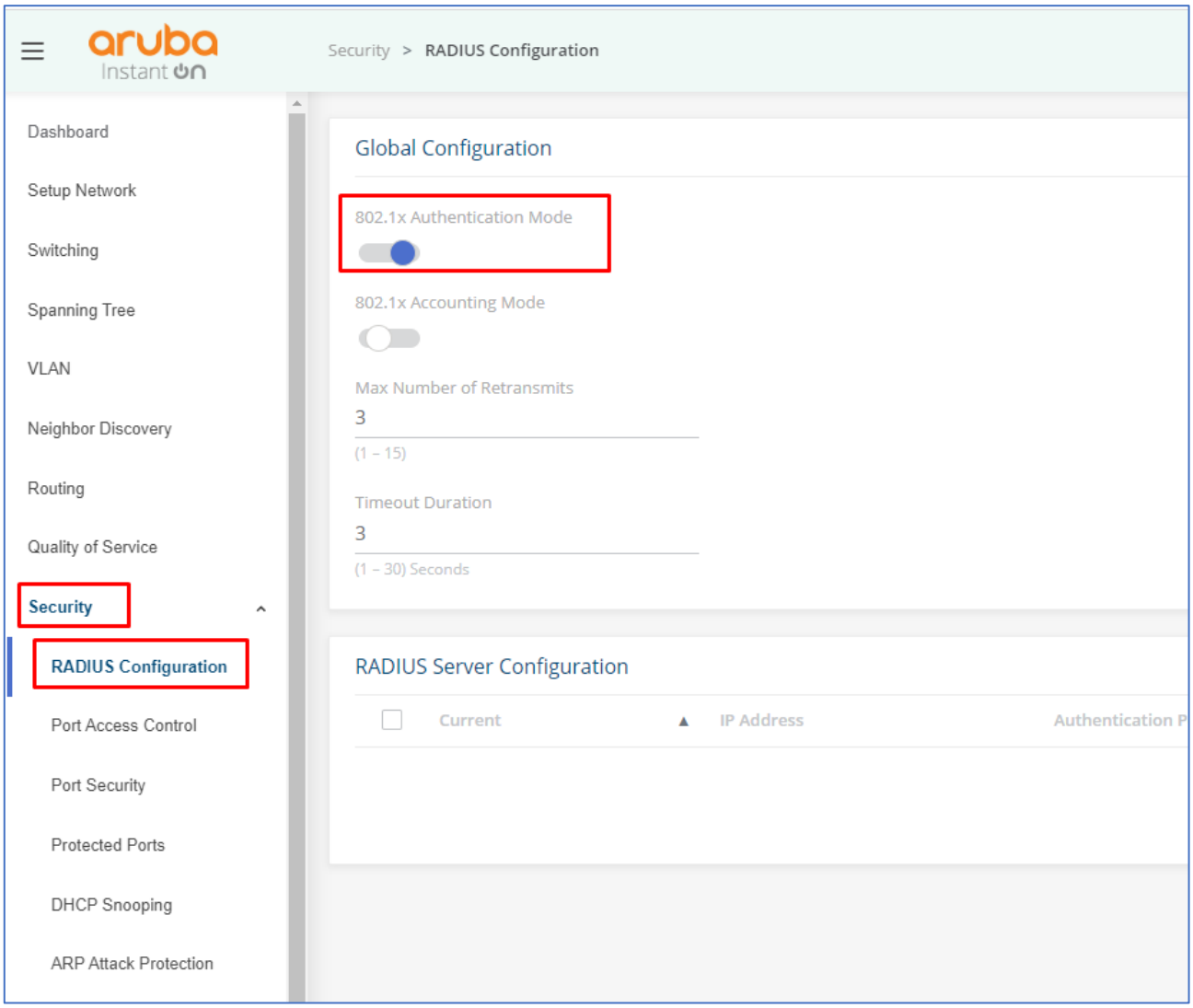




RADIUS Server details can be found in CLEAR tenant under “Settings” - > “CLEAR RADIUS SERVICE” -> “Europe and Asia” / “United States and North America”

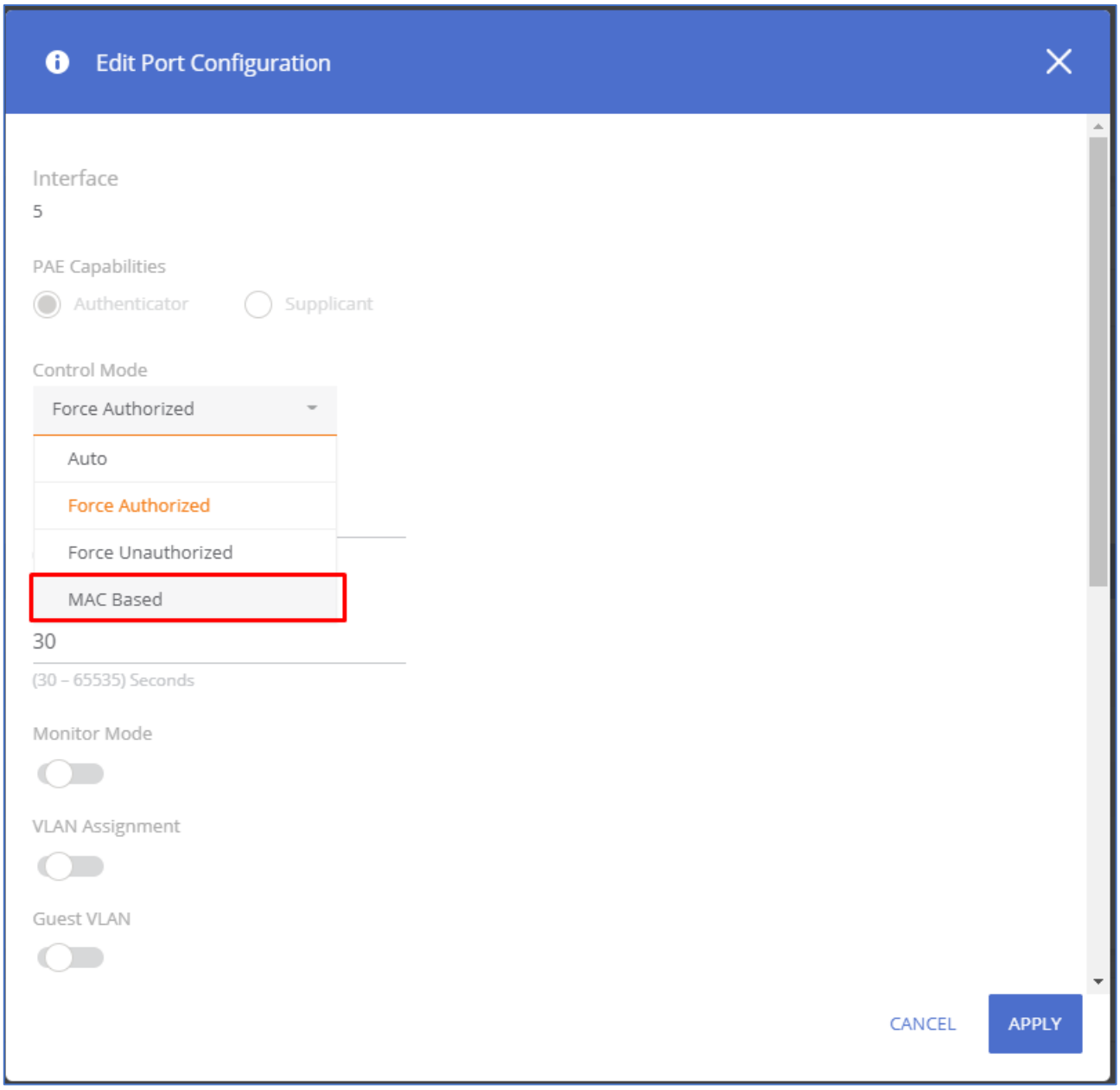


Under “Security” - > “RADIUS Configuration” - > “Global Configuration” -> check “802.1x Authentication Mode”

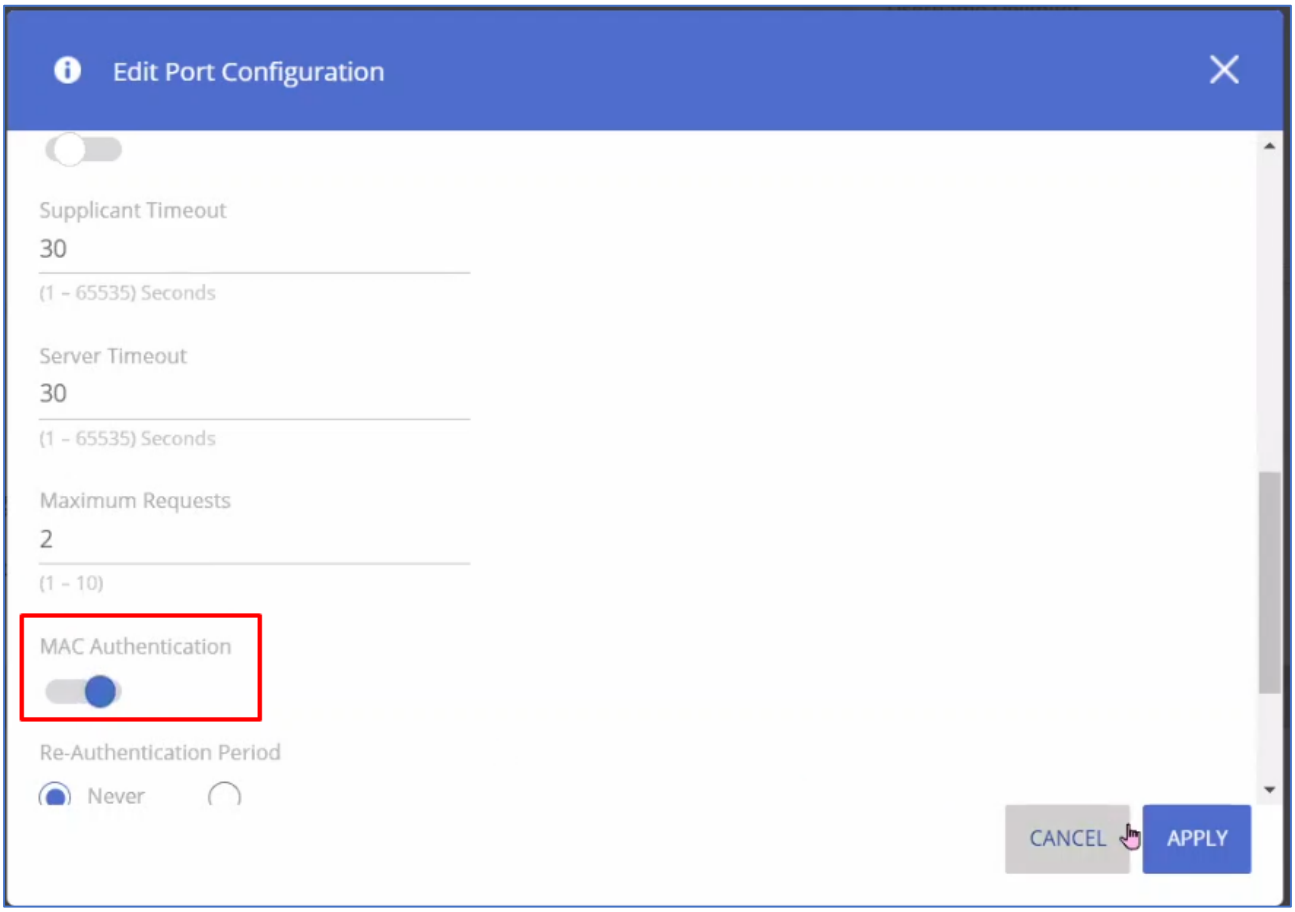


Under “Security” - > “Port Access Control” -> check the “Admin Mode”.

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.



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


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
APPLY