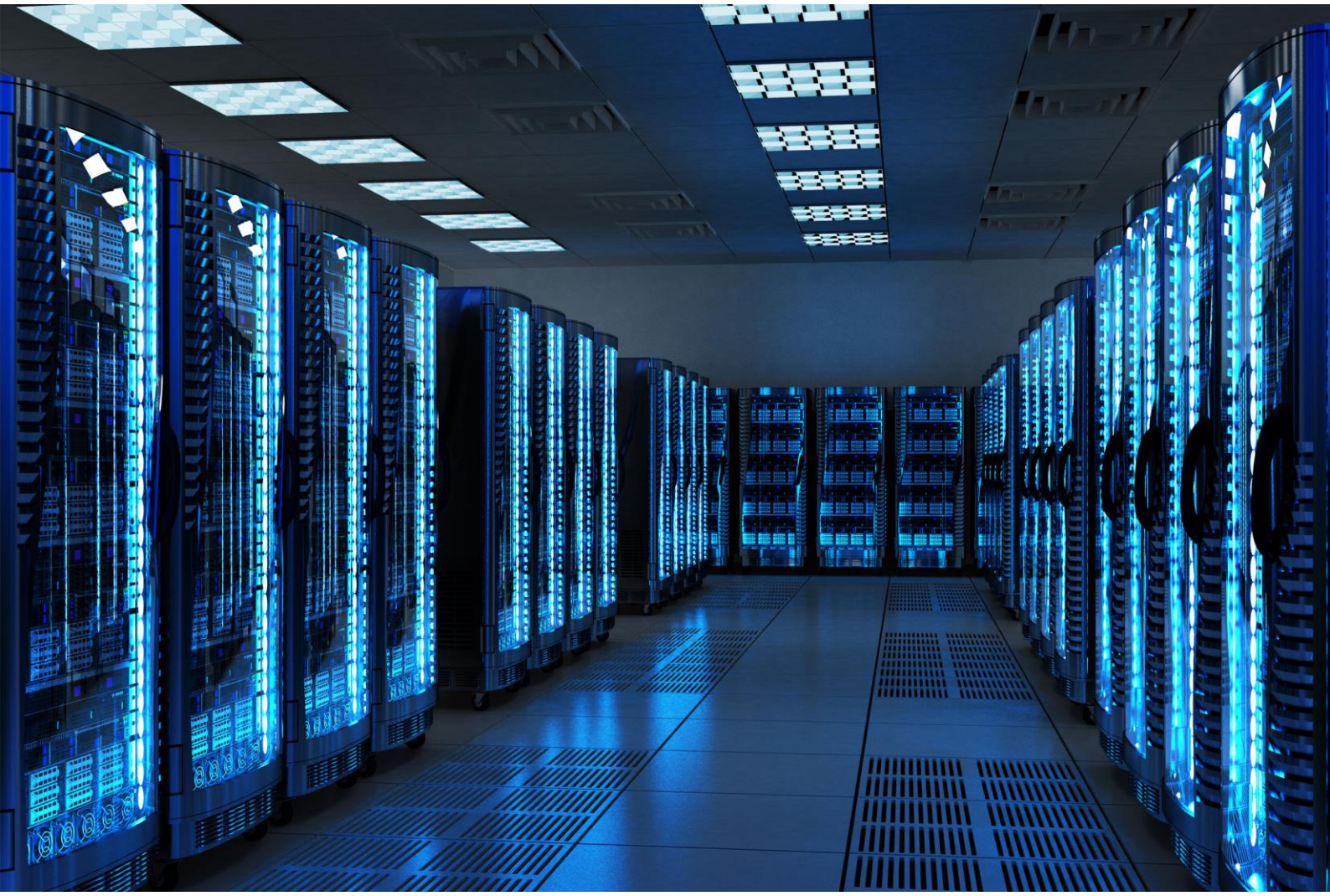
portnox™



INTEGRATION GUIDE

How to Configure Fortinet Wireless Controller to Secure your Wireless Network with Portnox CLEAR

Introduction

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

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

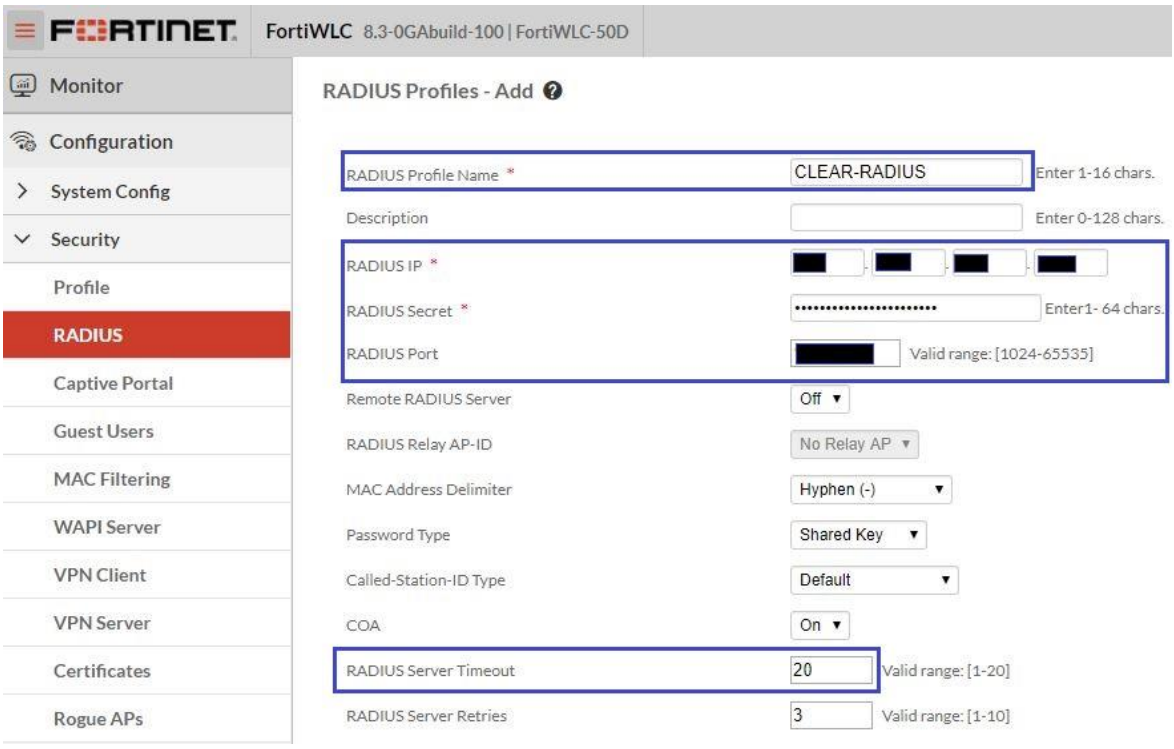
1) Add a radius server by navigating to **Configuration > Security > Radius**, and clicking **add**.

   In the window that appears:

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

   b. Enter the following CLEAR RADIUS server details, which you noted in Enabling CLEAR RADIUS Service in step (2) b:

      - In **Radius IP**, enter the Cloud RADIUS IP.
      - In **Radius Secret**, enter the Shared Secret and then confirm it.
      - In **Radius Port**, enter the Authentication port number.
      - Set **Radius Server Timeout** to **20** seconds.



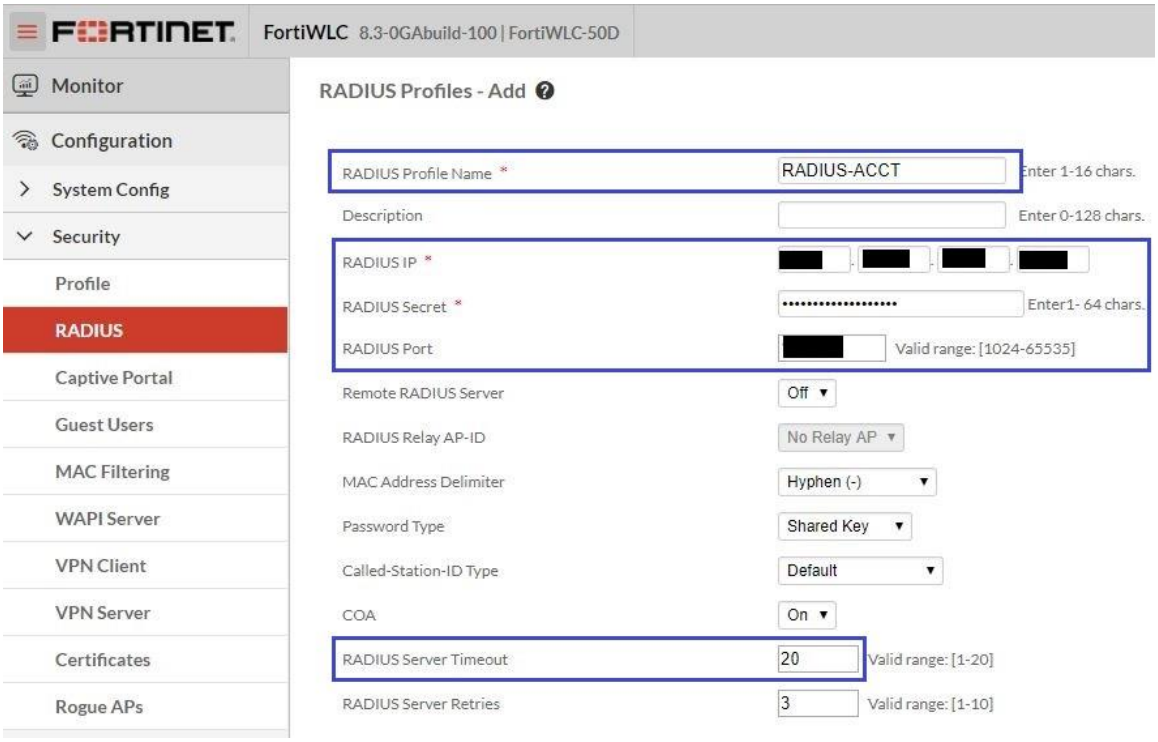
2) Add a Radius Accounting server by navigating to **Configuration > Security > Radius**, and clicking **Add**.

   In the window that appears:

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

   b. Enter the following CLEAR RADIUS server details, which you noted in Enabling CLEAR RADIUS Service in step (2) b:

      - In **Radius IP**, enter the Cloud RADIUS IP.
      - In **Radius Secret**, enter the Shared Secret and then confirm it.
      - In **Radius Port**, enter the Accounting port number.
      - Set **Radius Server Timeout** to **20** seconds.



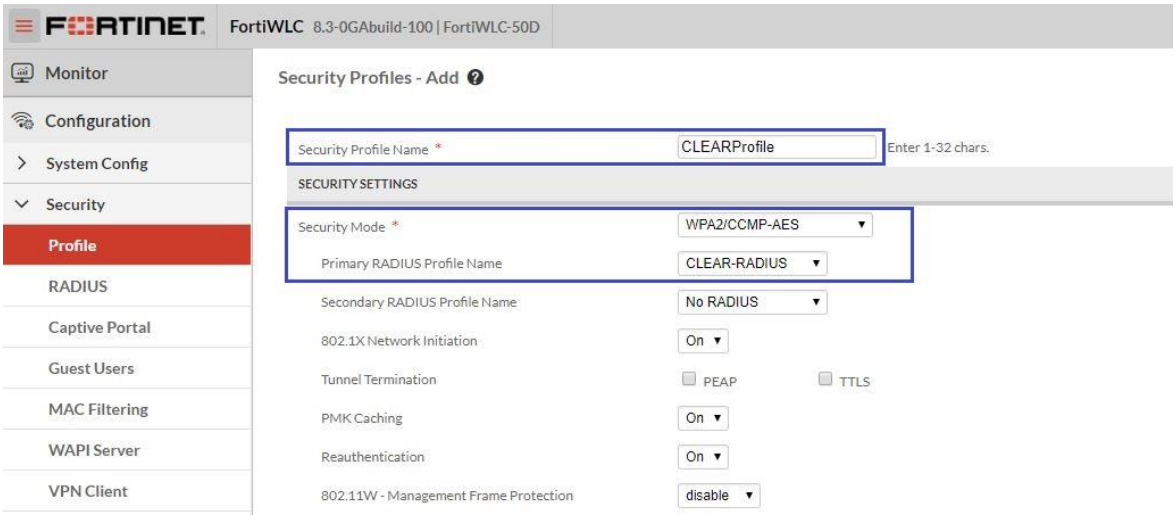
3) Add a Security Profile by navigating to Configuration > Security > profile, and clicking add.

In the windows that appears:

a. Specify Security Profile Name for the **Security Profile**.

b. In Security Mode, select **WPA2/CCMP-AES**.

c. In Primary Radius Profile Name, select the Radius server that was created instep (1).



4) Add a new SSID (or edit an existing SSID) by navigating to **Configuration > Wireless > ESS** and clicking **Add**.

In the windows that appears:

c. Specify a name for the **ESS Profile**.

d. Specify a name for the **SSID**.

e. In **Security profile**, select the profile that was created in Step (3).

f. In **Primary Radius Accounting Server** select the accounting server that was created in Step (2).