



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.

The screenshot shows the Fortinet FortiWLC configuration interface for adding a RADIUS profile. The left sidebar shows the navigation menu with 'RADIUS' selected under the 'Security' section. The main content area is titled 'RADIUS Profiles - Add'. The form contains the following fields and values:

- RADIUS Profile Name ***: CLEAR-RADIUS (Valid range: Enter 1-16 chars.)
- Description**: (Empty) (Valid range: Enter 0-128 chars.)
- RADIUS IP ***: (Redacted IP address)
- RADIUS Secret ***: (Redacted secret) (Valid range: Enter 1- 64 chars.)
- RADIUS Port**: (Redacted port) (Valid range: [1024-65535])
- Remote RADIUS Server**: Off
- RADIUS Relay AP-ID**: No Relay AP
- MAC Address Delimiter**: Hyphen (-)
- Password Type**: Shared Key
- Called-Station-ID Type**: Default
- COA**: On
- RADIUS Server Timeout**: 20 (Valid range: [1-20])
- RADIUS Server Retries**: 3 (Valid range: [1-10])

- 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.

The screenshot shows the Fortinet FortiWLC configuration interface. The left sidebar contains a navigation menu with the following items: Monitor, Configuration, System Config, Security (expanded), Profile, **RADIUS** (highlighted), Captive Portal, Guest Users, MAC Filtering, WAPI Server, VPN Client, VPN Server, Certificates, and Rogue APs. The main content area is titled "RADIUS Profiles - Add" and contains the following fields:

RADIUS Profile Name *	RADIUS-ACCT	Enter 1-16 chars.
Description		Enter 0-128 chars.
RADIUS IP *	████.████.████.████	
RADIUS Secret *	Enter 1- 64 chars.
RADIUS Port	████	Valid range: [1024-65535]
Remote RADIUS Server	Off	
RADIUS Relay AP-ID	No Relay AP	
MAC Address Delimiter	Hyphen (-)	
Password Type	Shared Key	
Called-Station-ID Type	Default	
COA	On	
RADIUS Server Timeout	20	Valid range: [1-20]
RADIUS Server Retries	3	Valid range: [1-10]

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

In the windows that appears:

- Specify Security Profile Name for the **Security Profile**.
- In Security Mode, select **WPA2/CCMP-AES**.
- In Primary Radius Profile Name, select the Radius server that was created in step (1).

The screenshot shows the Fortinet FortiWLC configuration interface. The left sidebar is expanded to 'Security' > 'Profile'. The main content area is titled 'Security Profiles - Add'. The form includes the following fields and settings:

- Security Profile Name ***: CLEARProfile (with a note 'Enter 1-32 chars.')
- SECURITY SETTINGS** section:
 - Security Mode ***: WPA2/CCMP-AES
 - Primary RADIUS Profile Name**: CLEAR-RADIUS
 - Secondary RADIUS Profile Name**: No RADIUS
 - 802.1X Network Initiation**: On
 - Tunnel Termination**: PEAP and TTLS (both unchecked)
 - PMK Caching**: On
 - Reauthentication**: On
 - 802.11W - Management Frame Protection**: disable

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

In the windows that appears:

- Specify a name for the **ESS Profile**.
- Specify a name for the **SSID**.
- In **Security profile**, select the profile that was created in Step (3).
- In **Primary Radius Accounting Server** select the accounting server that was created in Step (2).

The screenshot shows the Fortinet FortiWLC configuration interface. The left sidebar is expanded to 'Wireless' > 'ESS'. The main content area is titled 'ESS Profiles - Add'. The form includes the following fields and settings:

- ESS Profile ***: CLEAR-SSID (with a note 'Enter 1-32 chars.')
- Enable/Disable**: Enable
- SSID ***: CLEAR-SSID (with a note 'Enter 0-32 chars.')
- Security Profile**: CLEARProfile
- ESSID TYPE** section:
 - Essid Type**: Regular
 - Backup ESS Profile**: No Backup ESS
 - Timer Profile**: No Data for Timer Profile
 - Primary RADIUS Accounting Server**: CLEAR-Accounting
 - Secondary RADIUS Accounting Server**: No RADIUS
 - Accounting Interim Interval (seconds)**: 3600 (Valid range: [60-36000])
 - Reconnect Primary Server (minutes)**: 10 (Valid range: [5-60])