



INTEGRATION GUIDE

How to Configure WatchGuard Firebox Wireless Controller to Secure your Wireless Network with Portnox CLEAR

Introduction

This document guides you step by step how to configure your WatchGuard 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 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

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 WatchGuard Wireless SSID

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

- 1) In the WatchGuard web interface, navigate to **Network > Gateway Wireless Controller > SSIDs**, and add a new SSID or edit an existing one.
- 2) In the SSID's **Security** tab, do the following:
 - a. Select **WPA/WPA2 Enterprise** as the **Security Mode**.
 - b. Select an **Encryption** type: **AES / TKIP** or **AES**.
 - c. Enter the following CLEAR RADIUS server details, which you noted in [Enabling CLEAR RADIUS Service](#), step (2)b:
 - In **RADIUS Server**, enter the Cloud RADIUS IP.
 - In **RADIUS Port**, enter the Authentication port number.
 - In **RADIUS Secret**, enter the Shared Secret.
 - d. Check the **Enable RADIUS Accounting** check box.
 - e. Enter the following CLEAR RADIUS Accounting server details, which you noted in [Enabling CLEAR RADIUS Service](#), step (2)b:
 - In **RADIUS Accounting Server**, enter the Cloud RADIUS IP.
 - In **RADIUS Accounting Port**, enter the Accounting port number.
 - In **RADIUS Accounting Secret**, enter the Shared Secret.
 - f. Click **save**.

The screenshot displays the WatchGuard Fireware Web UI interface. On the left is a dark sidebar with a navigation menu. The main content area is titled "Gateway Wireless Controller / SSID" and contains several configuration sections. A "Network Name (SSID)" field is set to "WG-CLEAR". Below this are tabs for "Settings", "Security", and "Access Points", with "Access Points" selected. The "Security Mode" is set to "WPAWPA2 Enterprise" and "Encryption" is set to "AES". The "Group Key Update Interval" is 3600. A section for RADIUS configuration includes fields for "RADIUS Server", "RADIUS Port", and "RADIUS Secret", all of which are redacted with black boxes. Below this, the "Enable RADIUS Accounting" checkbox is checked. Another RADIUS configuration section includes fields for "RADIUS Accounting Server", "RADIUS Accounting Port", and "RADIUS Accounting Secret", also redacted. The "Interim Accounting Interval" is set to 600. At the bottom, the "Enable Fast Roaming (802.11k, 802.11r)" checkbox is unchecked, with a note that it requires WPA2 authentication and only applies to supported devices. "SAVE" and "CANCEL" buttons are located at the bottom of the configuration area.

WatchGuard Fireware Web UI

Gateway Wireless Controller / SSID

Network Name (SSID) WG-CLEAR

Settings Security Access Points

Security Mode WPAWPA2 Enterprise

Encryption AES

Group Key Update Interval 3600

RADIUS Server [REDACTED]

RADIUS Port [REDACTED]

RADIUS Secret [REDACTED]

Enable RADIUS Accounting

RADIUS Accounting Server [REDACTED]

RADIUS Accounting Port [REDACTED]

RADIUS Accounting Secret [REDACTED]

Interim Accounting Interval 600

Enable Fast Roaming (802.11k, 802.11r)
Fast Roaming requires WPA2 authentication and only applies to supported devices.

SAVE CANCEL