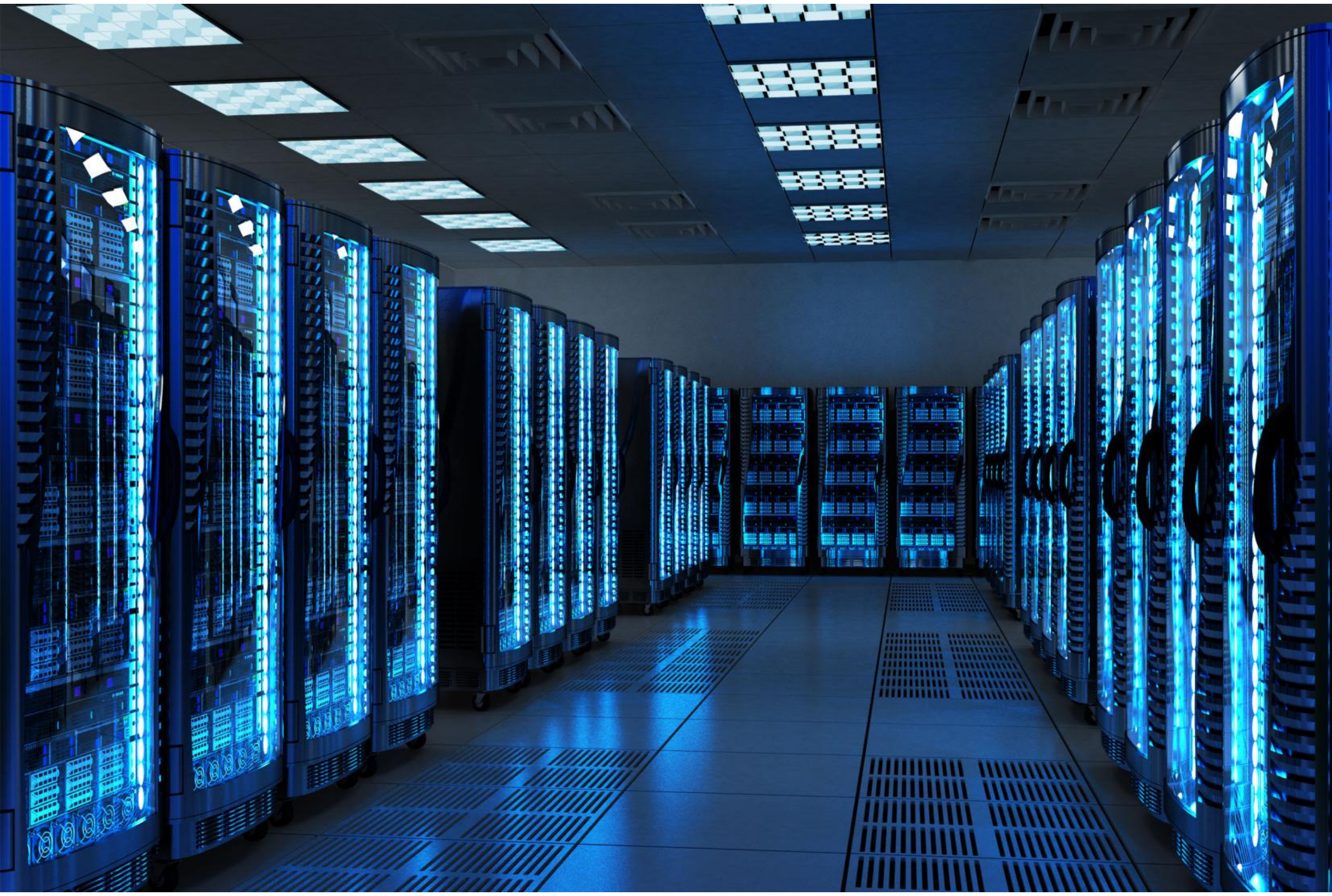


INTEGRATION GUIDE

How to Configure WatchGuard Wi-Fi Cloud to Secure your Wireless Network with Portnox CLEAR

Introduction

This document guides you step by step how to configure your WatchGuard wireless cloud 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 Wi-Fi 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 portal, navigate to **Manage** > **Configuration** > **Device Configuration** > **SSID profiles**, and add a new SSID or edit an existing one.

2) In the SSID's **Security** tab, do the following:

   a. Select **WPA and WPA2 Mixed mode** as the **Security Mode**.

   b. Select **802.1X**.

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

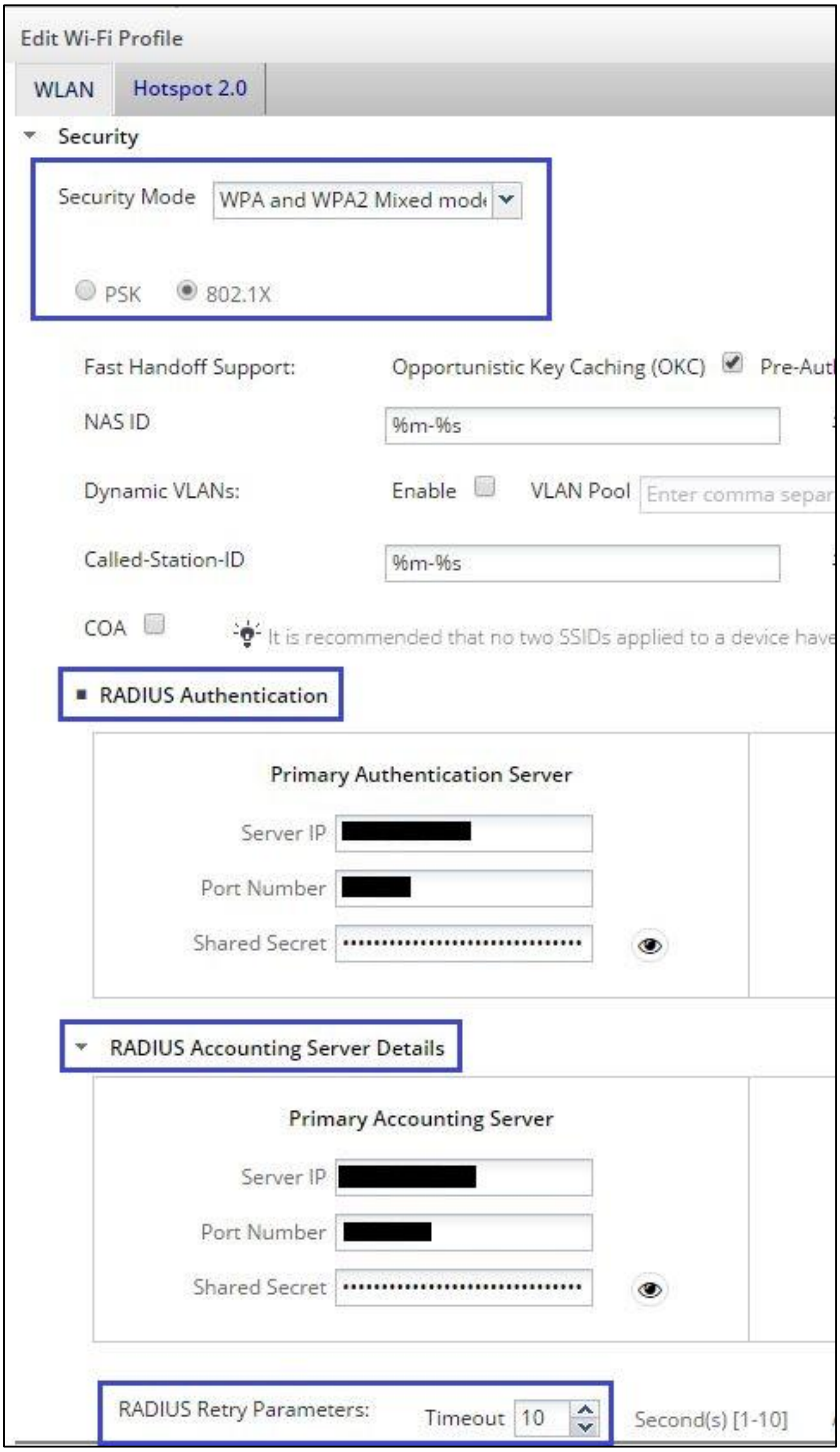
      - In **Server IP**, enter the Cloud RADIUS IP.
      - In **Port Number**, enter the Authentication port number.
      - In **Shared secret**, enter the Shared Secret.

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

      - In **Server IP**, enter the Cloud RADIUS IP.
      - In **Port Number**, enter the Accounting port number.
      - In **Shared secret**, enter the Shared Secret.

   e. Update the RADIUS **Timeout** parameter to **10** (seconds).

   f. Click **save**.



Edit Wi-Fi Profile

WLAN | Hotspot 2.0

Security

Security Mode: WPA and WPA2 Mixed mod

○ PSK ● 802.1X

Fast Handoff Support: Opportunistic Key Caching (OKC) ☑ Pre-Aut

NAS ID: %m-%s

Dynamic VLANs: Enable □ VLAN Pool: Enter comma separ

Called-Station-ID: %m-%s

COA □ It is recommended that no two SSIDs applied to a device have

RADIUS Authentication

Primary Authentication Server

Server IP: [redacted]

Port Number: [redacted]

Shared Secret: ••••••••••••••••••••••••••••••••

RADIUS Accounting Server Details

Primary Accounting Server

Server IP: [redacted]

Port Number: [redacted]

Shared Secret: ••••••••••••••••••••••••••••••••

RADIUS Retry Parameters: Timeout 10 Second(s) [1-10]