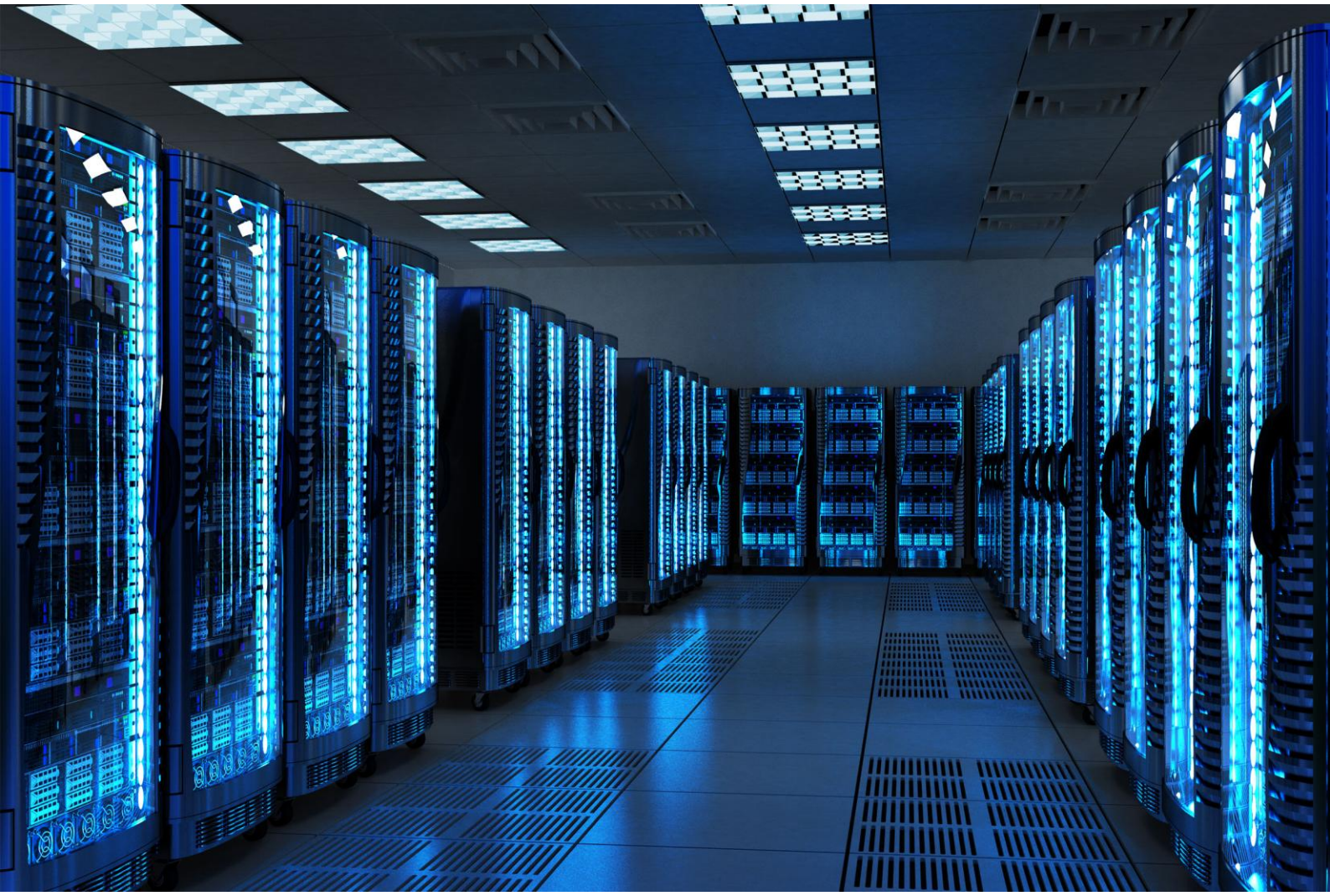
portnox™



INTEGRATION GUIDE

How to Configure Meraki Security Appliance to secure VPN access with Portnox CLEAR

Introduction

This document guides you step by step how to configure your VPN environment using Portnox CLEAR to enable secure and trusted cloud-based RADIUS access with OTP or with AgentP. Portnox CLEAR provides the additional advantages of continuous device monitoring and risk aware access control to any existing VPN implementation.

Preliminary Actions

Before configuring VPN authentication, you need to verify the following:

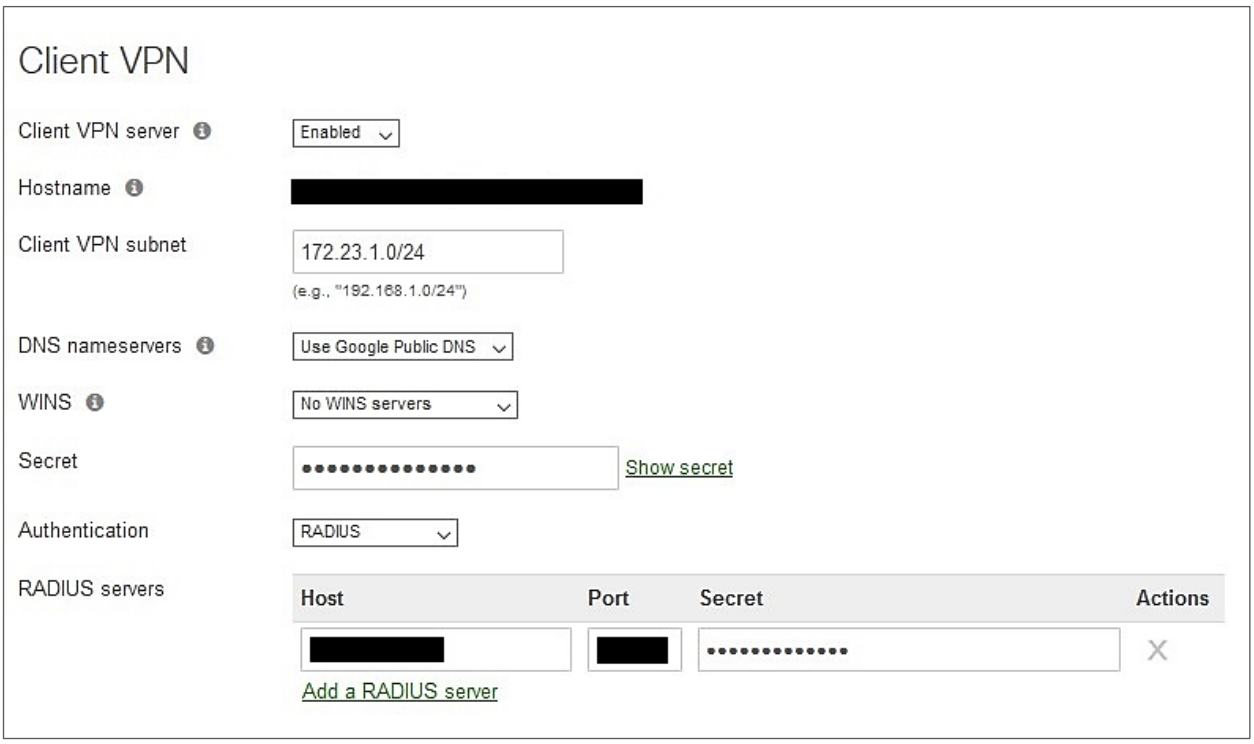
1) Verify your organization is registered on Portnox CLEAR Cloud Services: https://clear.portnox.com/
2) In the CLEAR portal, go to **Settings > Services** and expand **CLEAR RADIUS Service**. Then:
   a. If the **Enable Cloud RADIUS** checkbox is not checked, click **Edit** and check the **Enable Cloud RADIUS** checkbox.
   b. Note the RADIUS server details which you will need when configuring VPN access:
      - **Cloud RADIUS IP** – this is the IP address of the CLEAR RADIUS server
      - **Authentication port**
      - **Shared Secret** - this is the RADIUS client shared secret
3) In the CLEAR portal, go to **Settings > Services** and expand **VPN 2FA** Service. Then under **Strong Authentication Factor**, make sure that either **One-Time-Password (OTP)** or **Portnox AgentP** is selected.
4) In the CLEAR portal, go to **Settings** > **Groups** and create a group for VPN users, or record the name of an existing such group.
5) Make sure the endpoints for which you wish to secure VPN authentication, are enrolled with AgentP. You can download AgentP from here: https://clear.portnox.com/agentinstall.

Configuring Meraki Security Appliance VPN

In the following steps, we configure the VPN authentication to be secured and protected based on RADIUS authentication. The following steps should be performed in the Meraki portal.

Configure the Client VPN Server

1) Navigate to **Security Appliance** > **Client VPN** and perform the following:
   a. Set **Client VPN server** to **Enabled**.
   b. Specify the **Client VPN subnet**.
   c. Enter a **Secret** key to be used in the VPN client.
   d. In **Authentication**, select **RADIUS**.
   e. In **RADIUS servers**, enter the following CLEAR RADIUS server details, which you noted in Preliminary Actions, step 2b:
      - In **Host**, enter the Cloud RADIUS IP.
      - In **Port**, enter the Authentication port.
      - In **Secret**, enter the Shared Secret.
   f. Click **Save Changes**.

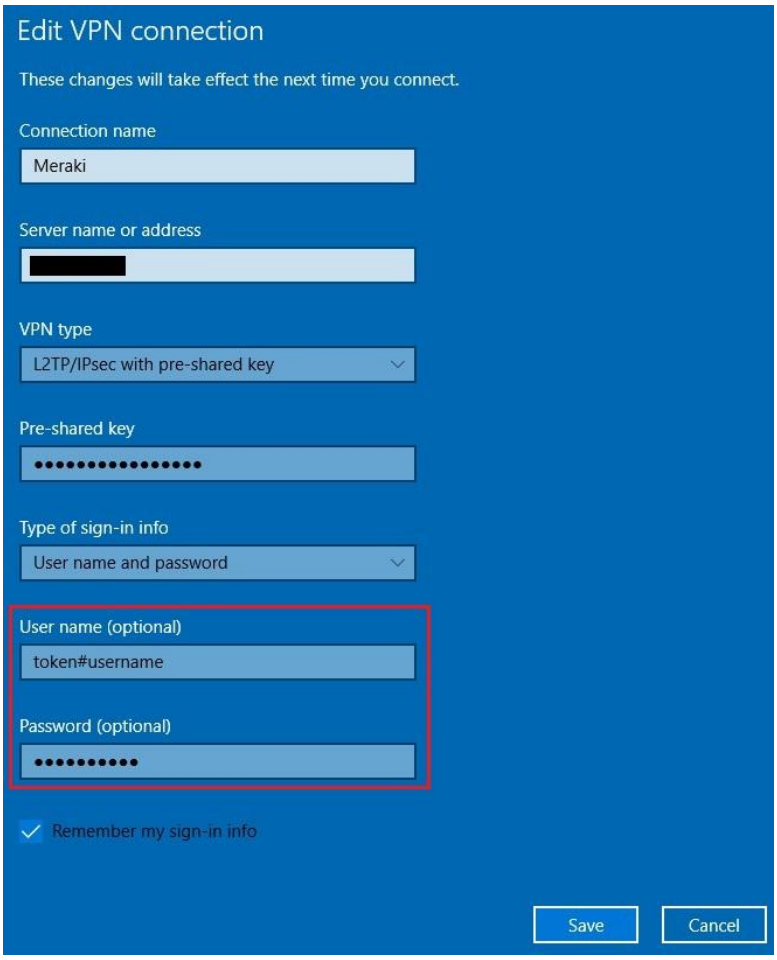


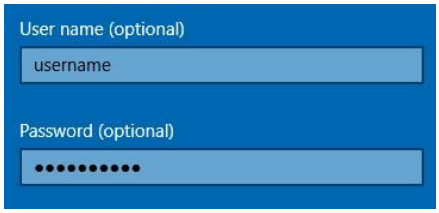
Instructions for Supplying VPN Credentials

The VPN 2FA method you selected (see Step (3) in Preliminary Actions) determines what the users need to supply to connect securely via VPN.

Supplying VPN Credentials for 2FA using OTP

For successful VPN authentication using Portnox CLEAR RADIUS and 2FA using OTP, users are required to provide their Token (OTP) generated by AgentP + username + password, in the following format:



Supplying VPN Credentials for 2FA using Portnox AgentP

For successful VPN authentication using Portnox CLEAR RADIUS and 2FA using Portnox AgentP, users are required to provide their username + password. These will be verified with the specific AgentP on the device requesting access, to confirm that the device is the one it claims to be: