

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 an optional push-to-access MFA.

## 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 > Groups** and create a group for VPN users, or edit an existing one. In the **group settings > VPN Access** select the following:
  - Allowed authentication type = credentials.
  - (optional) Multi-Factor Authentication = push-to-access on mobile only.  
Note, MFA on mobile devices require AgentP to be enrolled on the mobile device.
  - For implementation with AgentP, check the: validate risk score for all managed devices.

# 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 the 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**.

### Client VPN

Client VPN server ?

Hostname ?

Client VPN subnet   
(e.g., "192.168.1.0/24")

DNS nameservers ?

WINS ?

Secret  [Show secret](#)

Authentication

RADIUS servers

Host	Port	Secret	Actions
<input type="text" value="REDACTED"/>	<input type="text" value="REDACTED"/>	<input type="text" value="REDACTED"/>	<input type="button" value="X"/>

[Add a RADIUS server](#)

# Instructions for Supplying VPN Credentials

## Supplying VPN Credentials without MFA

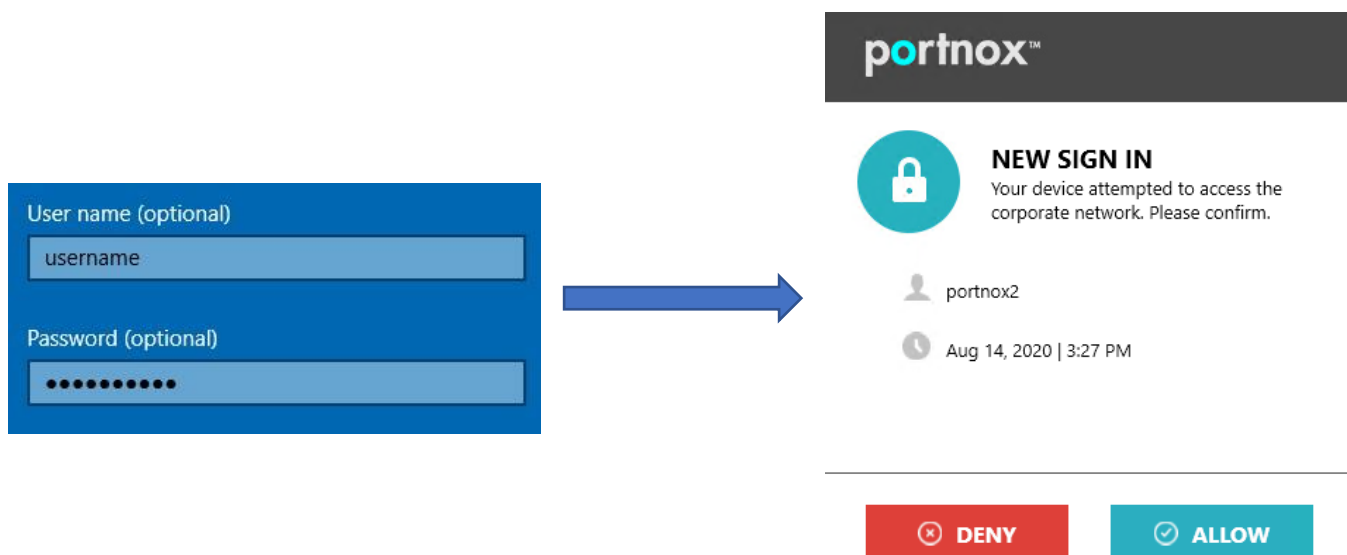
For successful VPN authentication using Portnox CLEAR RADIUS, users are required to provide their username + password:



A screenshot of a blue login form. It contains two input fields: the first is labeled 'User name (optional)' and contains the text 'username'; the second is labeled 'Password (optional)' and contains ten black dots representing a masked password.

## Supplying VPN Credentials with push-to-access MFA

For successful VPN authentication using Portnox CLEAR RADIUS and push-to-access MFA, users are required to provide their username + password and allow the push notification on their mobile device:



The diagram illustrates the process of MFA. On the left, a blue login form with 'User name (optional)' and 'Password (optional)' fields is shown. A blue arrow points from this form to a mobile notification interface on the right. The notification is from 'portnox™' and is titled 'NEW SIGN IN'. The message reads: 'Your device attempted to access the corporate network. Please confirm.' Below the message, it shows a user icon for 'portnox2' and a clock icon for 'Aug 14, 2020 | 3:27 PM'. At the bottom of the notification, there are two buttons: a red 'DENY' button with a white 'x' icon and a teal 'ALLOW' button with a white checkmark icon.