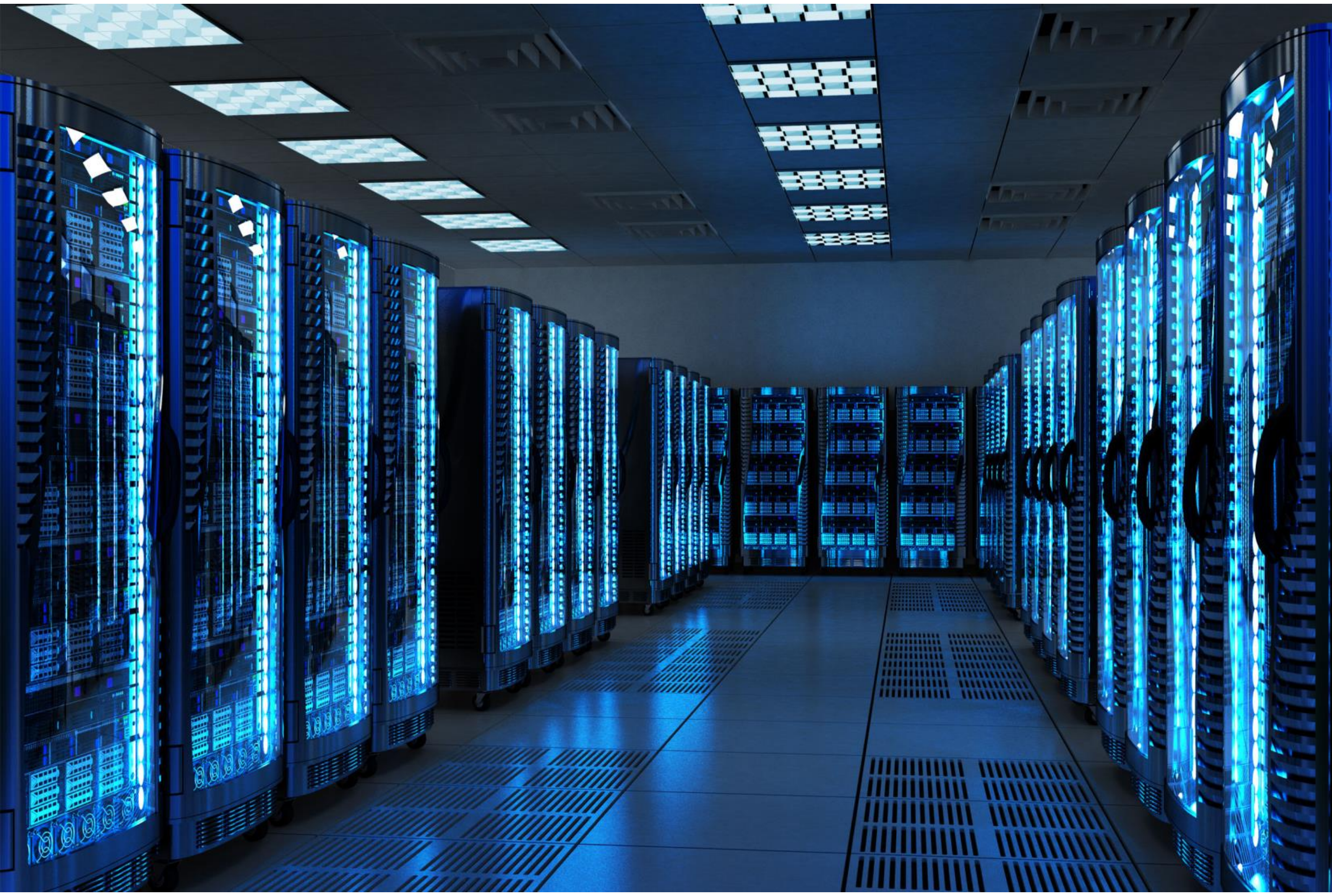
portnox™



INTEGRATION GUIDE

How to Configure OpenVPN 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:

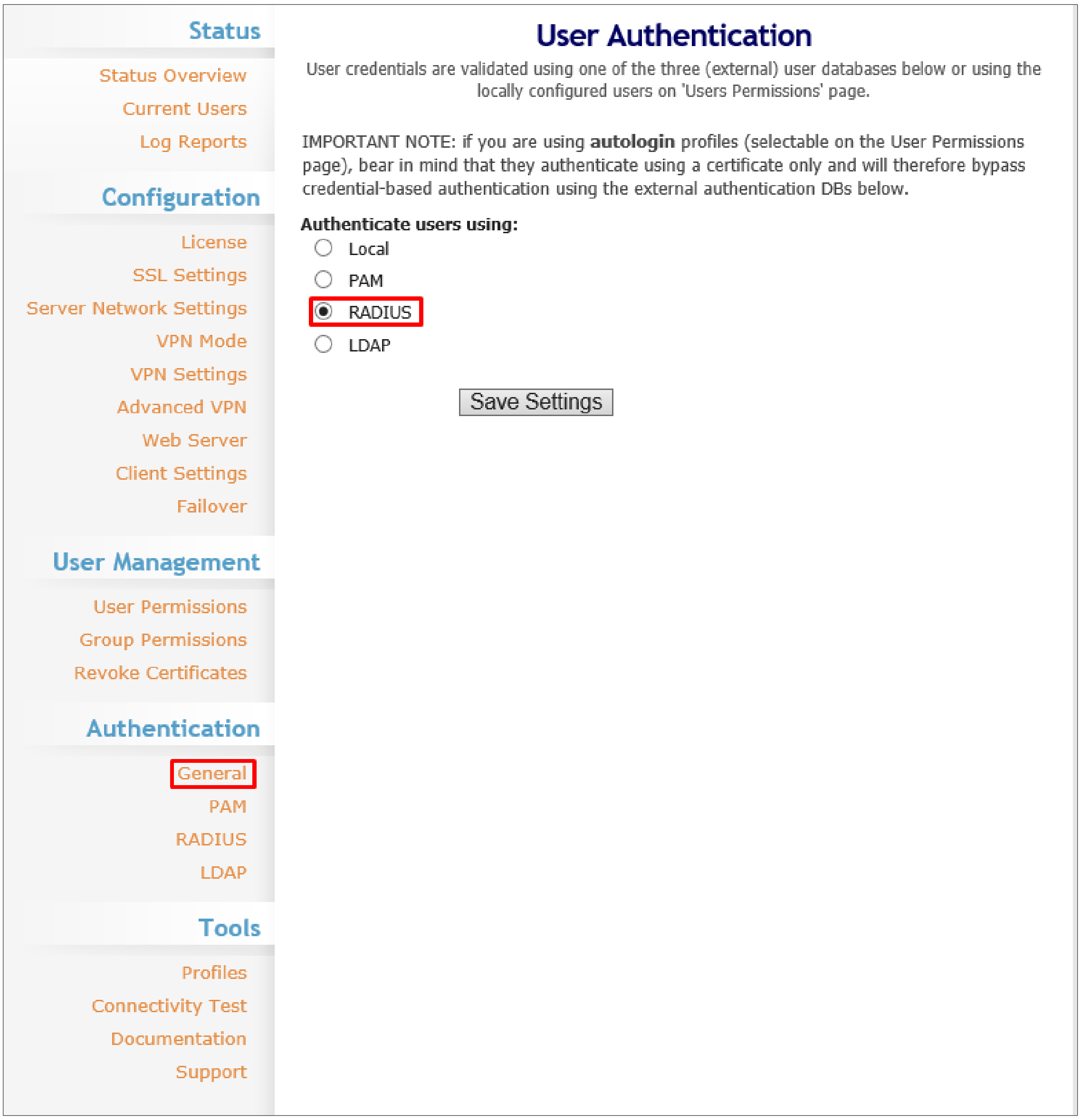
1) Verify your organization is registered on Portnox CLEAR Cloud Services: https://clear.portnox.com/
2) In the CLEAR portal, go to **Settings > Services** and expand **CLEAR RADIUS Service**. Then:
   a. If the **Enable Cloud RADIUS** checkbox is not checked, click **Edit** and check the **Enable Cloud 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**
      - **Accounting 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 OpenVPN 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 OpenVPN web interface.

1) Navigate to **Authentication > General**, select the **RADIUS** as the user authentication method, and click **Save Settings**.



User Authentication

User credentials are validated using one of the three (external) user databases below or using the locally configured users on 'Users Permissions' page.

IMPORTANT NOTE: if you are using **autologin** profiles (selectable on the User Permissions page), bear in mind that they authenticate using a certificate only and will therefore bypass credential-based authentication using the external authentication DBs below.

Authenticate users using:

○ Local

○ PAM

● RADIUS

○ LDAP

2) Navigate to **Authentication > RADIUS** and configure the following:

   a. Select **MS-CHAP v2** as the **RADIUS Authentication Method**.

   b. In **RADIUS Settings**, enter the following CLEAR RADIUS server details, which you noted in This document guides you step by step how to configure your VPN environment using Portnox

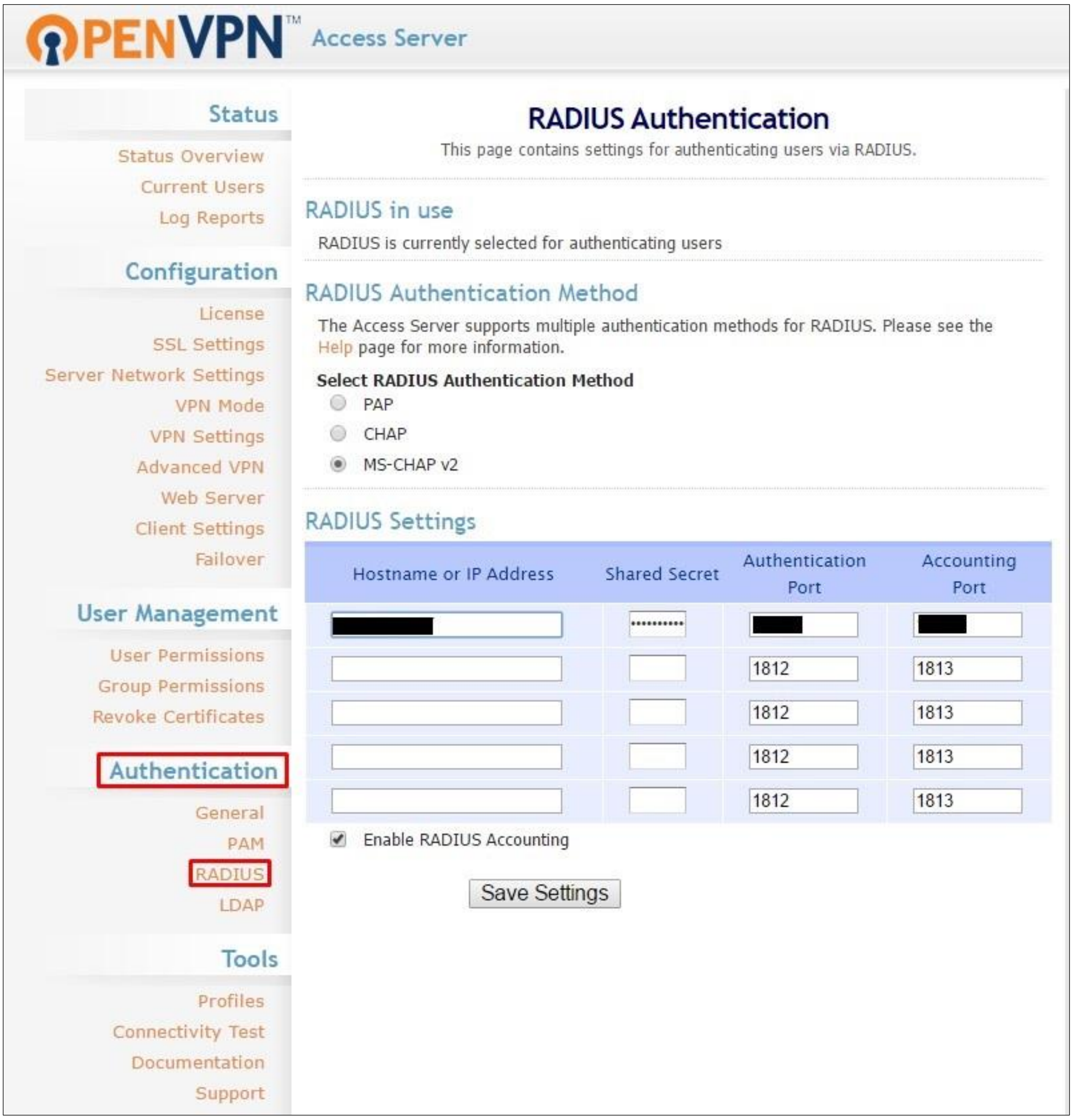
CLEAR to enable secure and trusted cloud-based RADIUS access with an optional push-to-access MFA.

c. Preliminary Actions, step 2(b):

- In **Hostname or IP Address**, enter the Cloud RADIUS IP.
- In **Shared Secret**, enter the Shared Secret.
- In **Authentication Port**, enter the Authentication port.
- In **Accounting Port**, enter the Accounting port.

d. Check the **Enable RADIUS Accounting** checkbox.

e. Click **Save Settings**.



RADIUS Authentication

This page contains settings for authenticating users via RADIUS.

RADIUS in use

RADIUS is currently selected for authenticating users

RADIUS Authentication Method

The Access Server supports multiple authentication methods for RADIUS. Please see the Help page for more information.

Select RADIUS Authentication Method

○ PAP
○ CHAP
● MS-CHAP v2

RADIUS Settings

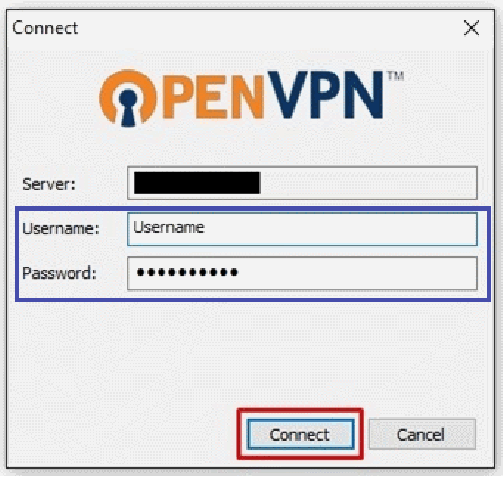
Hostname or IP Address	Shared Secret	Authentication Port	Accounting Port
[redacted]	••••••••••	[redacted]	[redacted]
		1812	1813
		1812	1813
		1812	1813
		1812	1813

☑ Enable RADIUS Accounting

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:



Connect

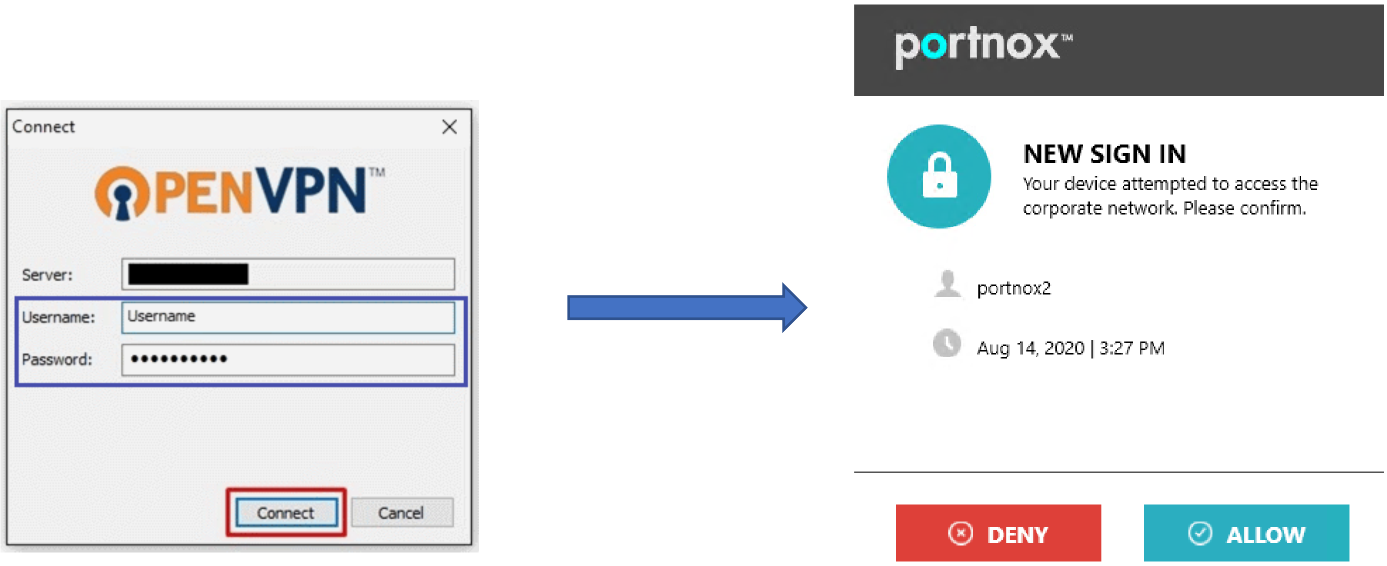
Server: [redacted]

Username: Username

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:



Connect

Server: [redacted]

Username: Username

Password: •••••••••••

NEW SIGN IN

Your device attempted to access the corporate network. Please confirm.

portnox2

Aug 14, 2020 | 3:27 PM