FieldServer

OpenVPN Server

Start-up Guide

APPLICABILITY & EFFECTIVITY

Effective for all systems manufactured after February 2020.

Document Revision: 1.F
T18665

Technical Support

Please call us for any technical support needs related to the FieldServer product.

MSA Safety
1991 Tarob Court
Milpitas, CA 95035

Website: www.sierramonitor.com

U.S. Support Information:

+1 408 964-4443
+1 800 727-4377

Email: smc-support@msasafety.com

EMEA Support Information:

+31 33 808 0590

Email: smc-support.emea@msasafety.com

TABLE OF CONTENTS

1 SETUP AMAZON AWS SERVER

It is recommended to use OpenVPN with Amazon AWS. Follow the linked guide to setup an Amazon AWS server: https://openvpn.net/amazon-cloud/

There are 2 options for running OpenVPN on Amazon:

- Purchase the license through Amazon and only pay for the time the OpenVPN is running. For a 5 device license the pricing is listed below:

  Starting from $0.07/hr or from $490.00/yr (20% savings) for software + AWS usage fees

- Bring your own License (BYOL): Amazon offers an unlicensed version of the EC2 instance. A license can be purchased from OpenVPN and entered into the instance. This option is cheaper for continuous usage.

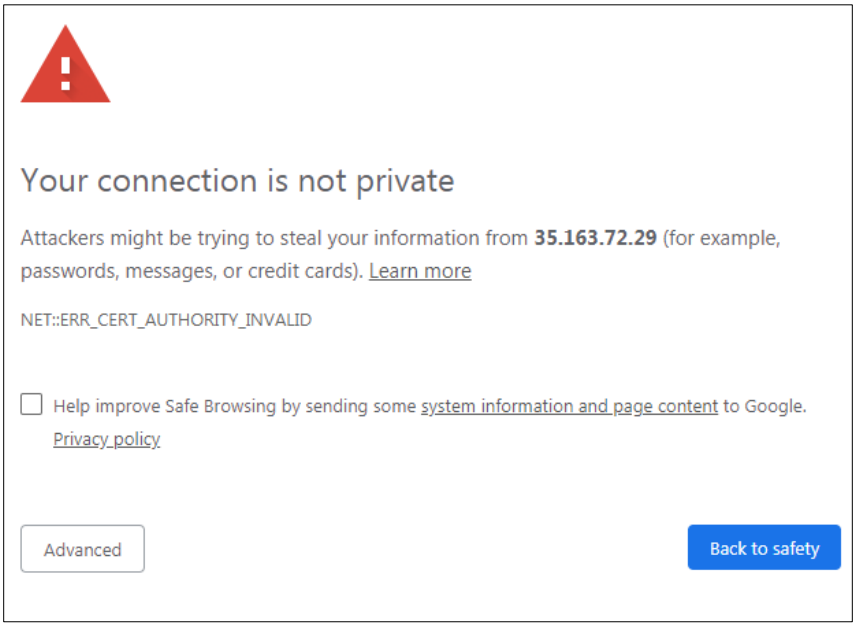
2 SETUP OPENVPN CLOUD

2.1 OpenVPN Server Configuration

- Once the server is configured, enter the server's IP Address/admin into the local device's web browser.

Example: 35.163.72.29/admin

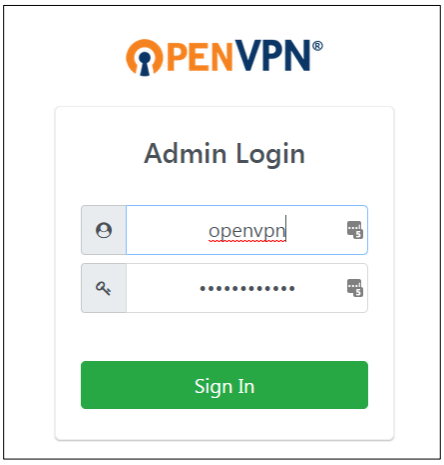
- This may generate a security warning as there is no certificate for HTTPS to verify. Click the Advanced button to proceed to the IP Address (unsafe). A domain with DNS entry can resolve this error.



NOTE: Some browsers may require adding the IP Address to the trusted IP sites list.

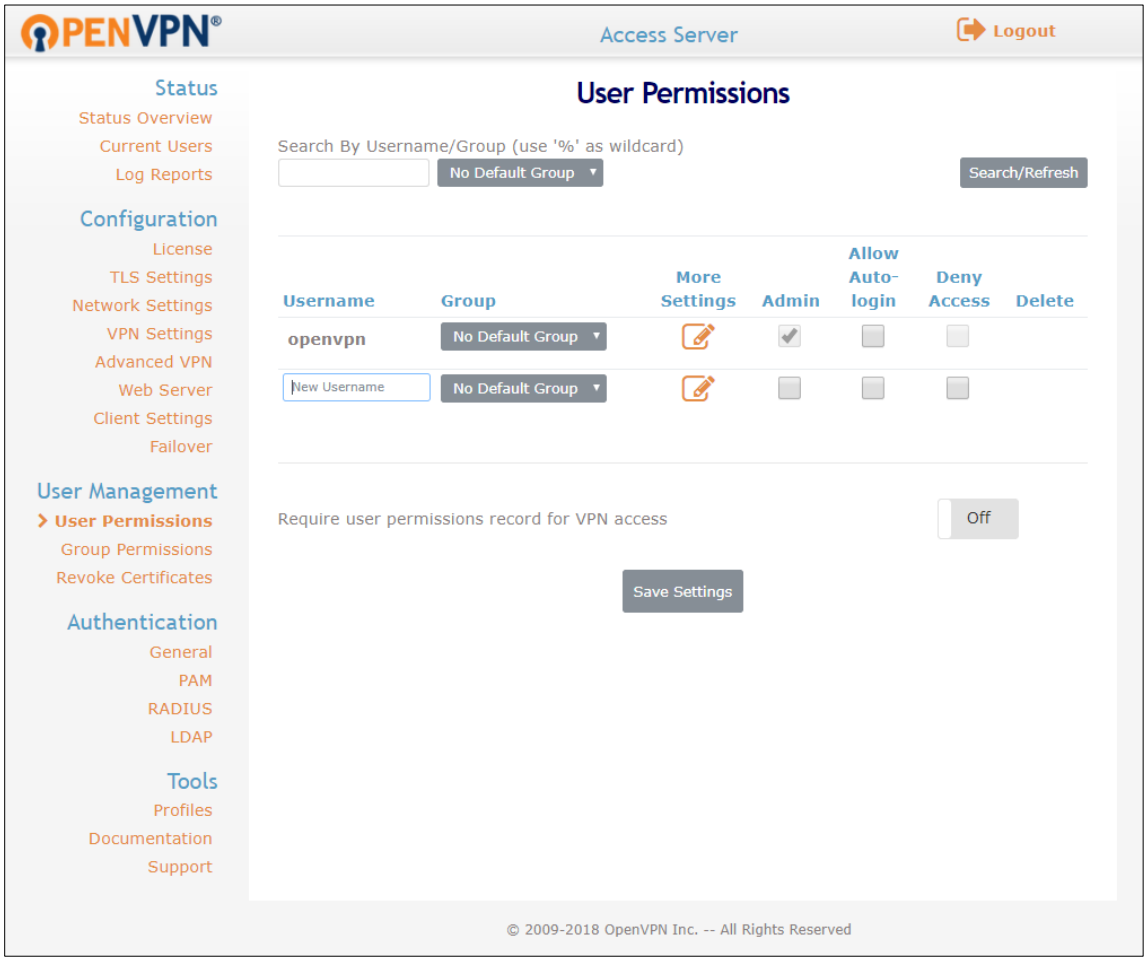
2.2 Login to the Server

- Once on the website, use Admin credentials to login.

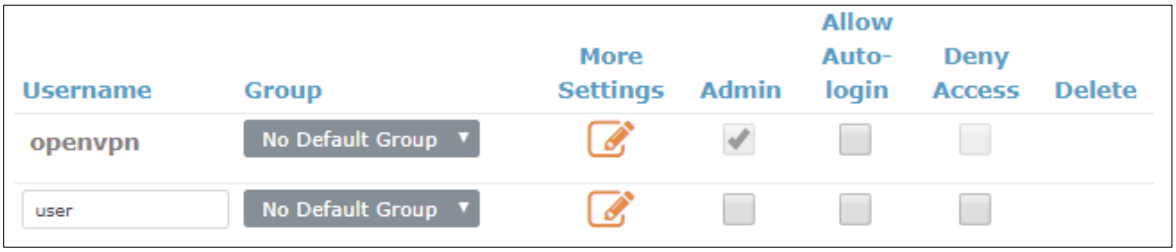


2.3 Create a New User for the PC Connection

- Find the User Management Section in the Navigation bar on the left side of the screen.
- Click on User Permissions.

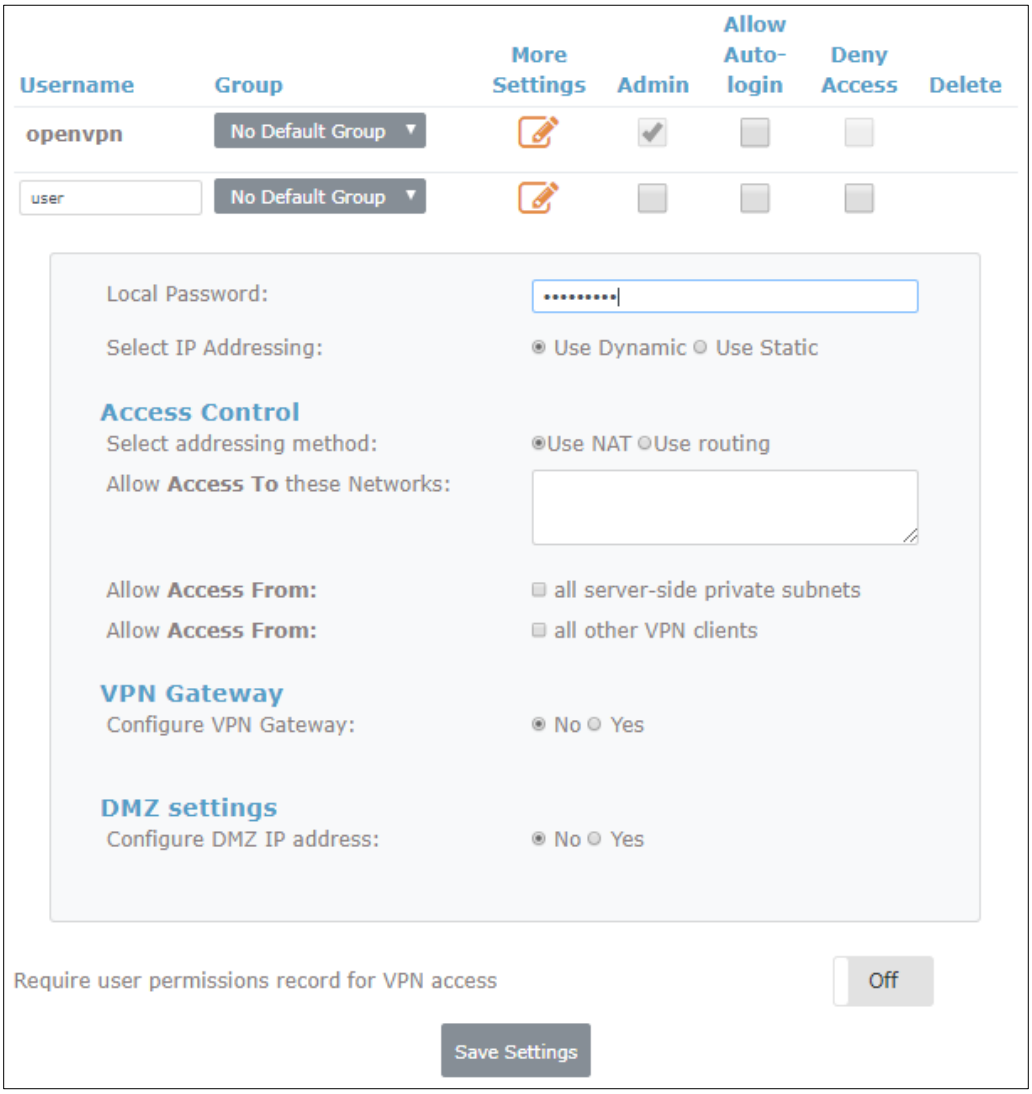


- Once the User Permissions page is open, type in a new username in the text field under the Username heading and make sure the Admin, Allow-Auto login, and Deny Access boxes are all unchecked.

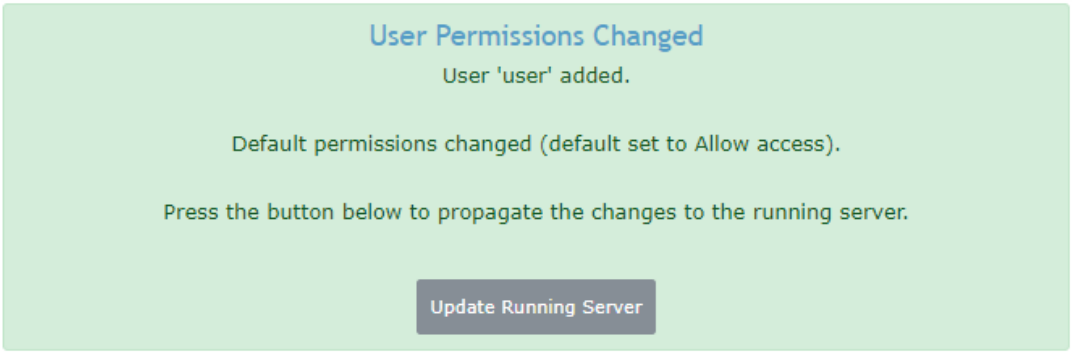


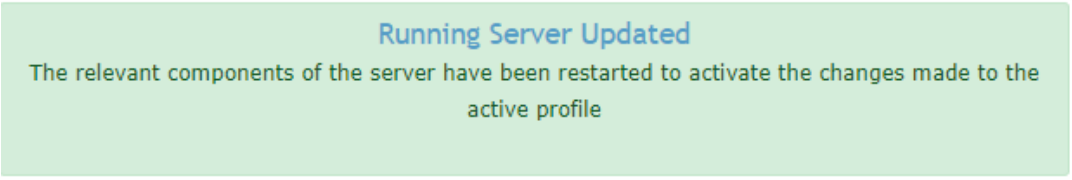
- Click the configuration button ( ) under the More Settings heading to access more configuration options.

- Enter a password for the USER profile in the Local Password field and record for future use.



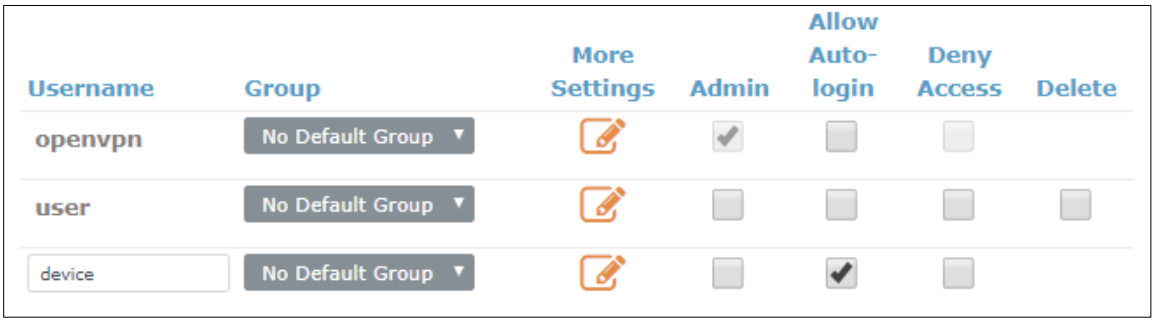
- Once configuration is complete, click the Save Settings button and then click the Update Running Server button.





2.4 Create a New User for the Device Connection

- Once the User Permissions page is open, type in a new device name in the text field under the Username heading and make sure the Allow-Auto login box is checked, and the Admin and Deny Access boxes are all unchecked.



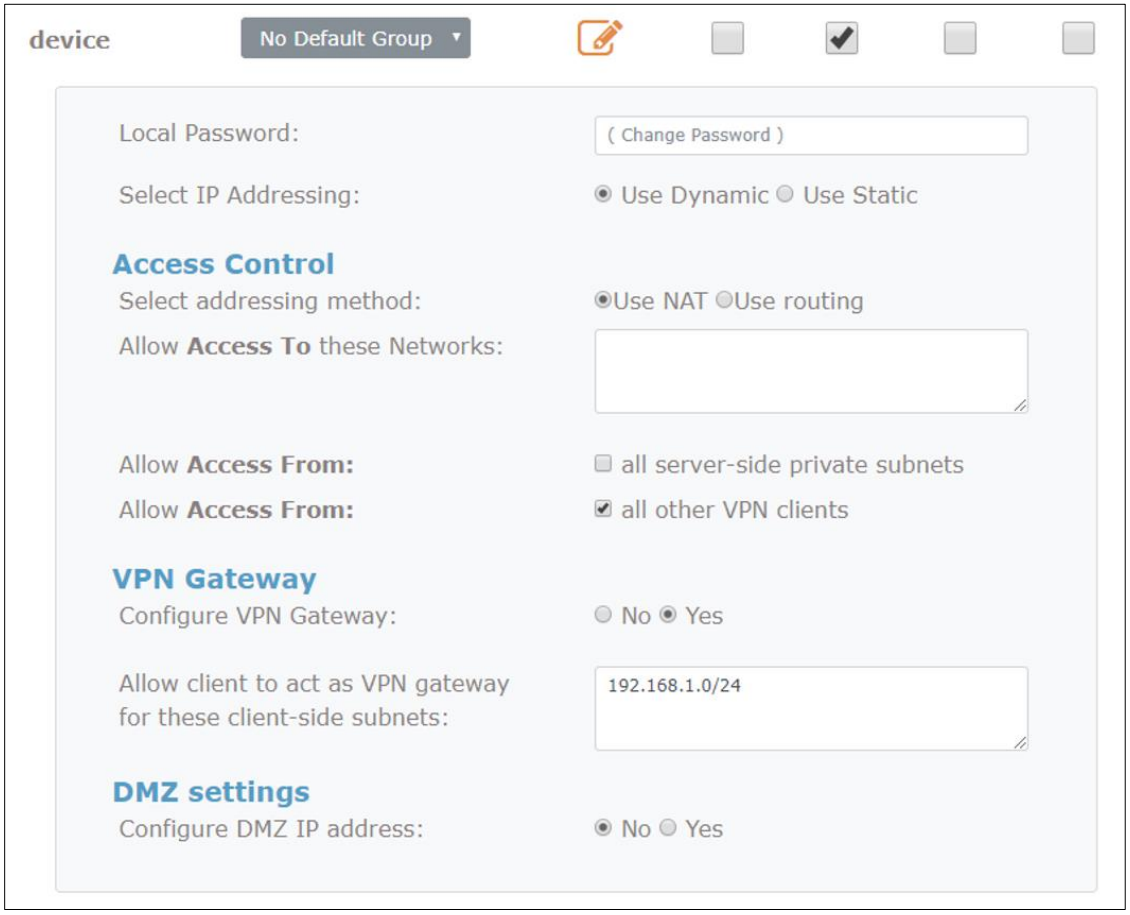
- Click the configuration button ( ) under the More Settings heading to access more configuration options.
- Enter a password for the DEVICE profile in the Local Password field and record for future use.
- Set the Configure VPN Gateway to Yes.

- If the VPN needs to access the local network, configure the VPN Gateway section. This will allow traffic through the FieldServer to the IP Addresses on the local network.

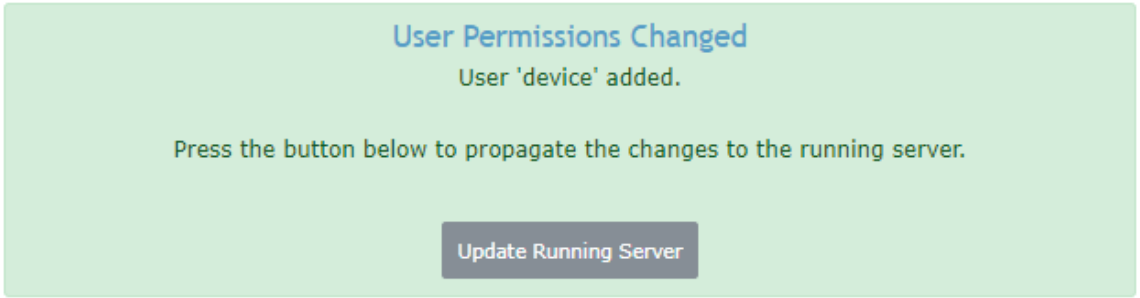
  For example:

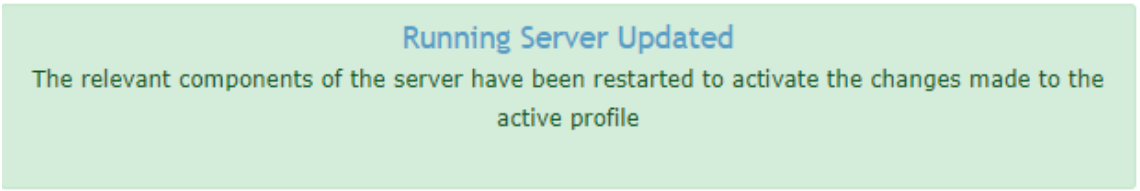
To allow access to all IP Address on 192.168.1.x subnet, type in “192.168.1.0/24”

To only allow access to 192.168.1.50, type in “192.168.1.50/32”



- Once configuration is complete, click the Save Settings button and then click the Update Running Server button.





3 CONFIGURE FIELDSERVER FOR OPENVPN

3.1 Download the DEVICE Configuration Profile

- Login with the DEVICE credentials that were created in **Section 2.4**.

- Click on “Yourself (autologin profile)”.

The DEVICE .opvn file will download to the default folder on the PC

- Click on Logout.

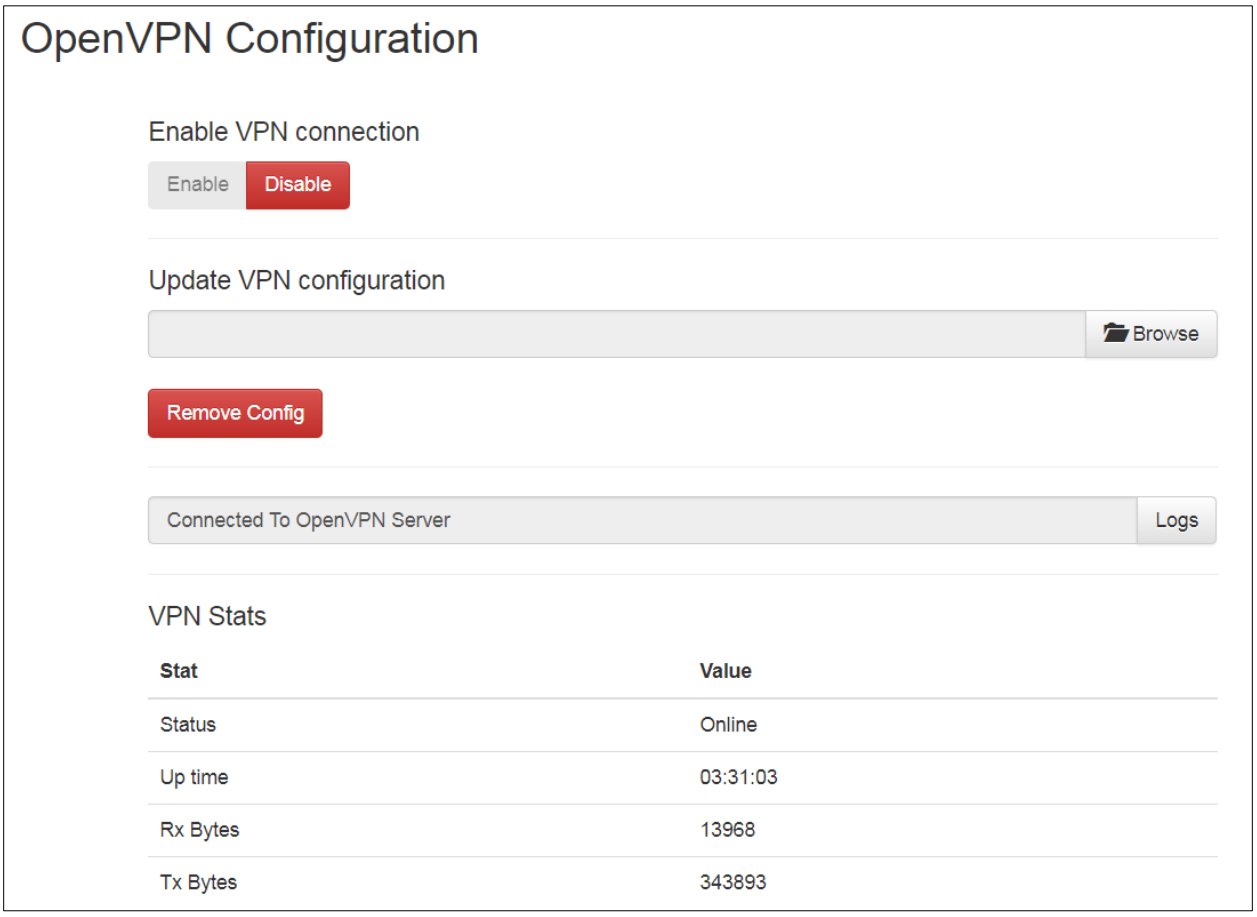
3.2 Load the DEVICE OpenVPN Connection Profile onto the FieldServer

The DEVICE .opvn file must be loaded onto the FieldServer for OpenVPN configuration.

- To do this, input the FieldServer's IP Address into the local browser followed by this text: "/openvpn/ui".

For example: http://192.168.1.24/openvpn/ui/

- This will bring up the following webpage:



- Click the Browse button under the Update VPN configuration header and select the DEVICE .opvn file to load it for OpenVPN configuration.
- Change the Enable VPN connection to Enable.

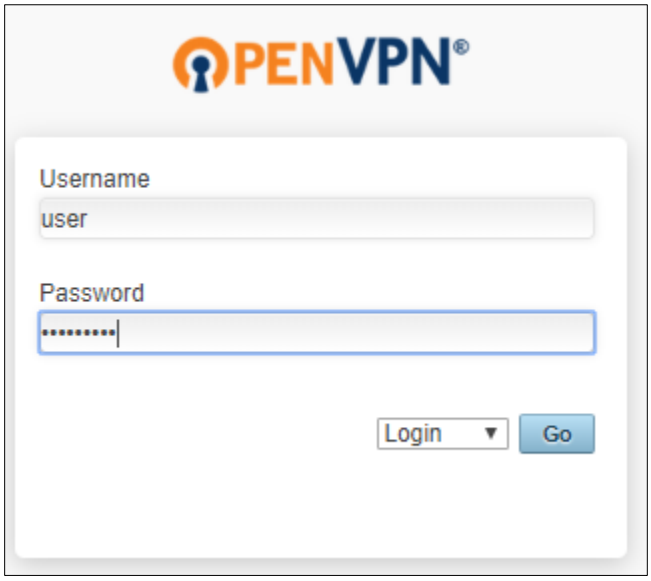
Once OpenVPN is enabled on the FieldServer, it will connect to the OpenVPN server.

NOTE: The connection statistics will be displayed in the VPN Stats section.

4 INSTALL THE OPENVPN CLIENT ONTO A LOCAL PC

4.1 Download the USER Configuration Profile

- Enter the server's IP Address into the local device's web browser.
- Go to the OpenVPN server and login with the USER credentials created in **Section 2.3**.



- Click on "Yourself (user-locked profile)".

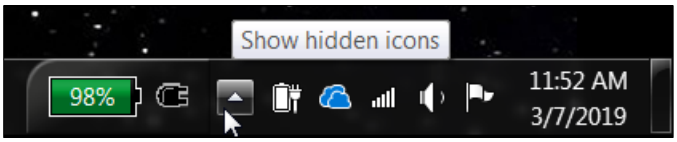
The USER .opvn file will download to the default folder on the PC

- Click on Logout.

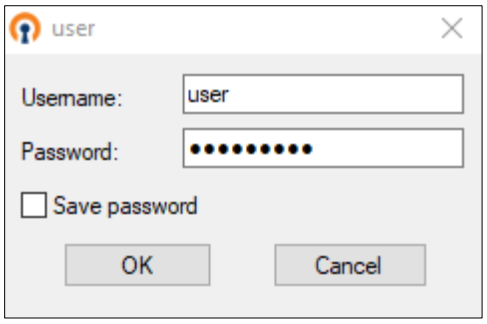
4.2 Load the USER OpenVPN Connection Profile onto the PC

- Download and install the OpenVPN client at: https://swupdate.openvpn.org/community/releases/openvpn-install-2.4.6-I602.exe
- Start the OpenVPN software by double clicking the OpenVPN GUI shortcut on the desktop.
- Right click the OpenVPN icon ( ) found in the system tray (on the right side of the taskbar).

If the icon isn't visible, click the upwards arrow in the system tray to find it



- Select the "Import file …" option in the dropdown menu.
- Find and select the USER .opvn file on the local PC.
- Right click on the OpenVPN icon ( ) again and click the new "Connect" option in the dropdown menu.
- When the login window appears, enter the USER credentials.



- A message will appear saying the OpenVPN connection has been established.

APPENDIX A. TROUBLESHOOTING

Appendix A.1. General Notes

- The VPN connection uses TCP ports 80, 443 and UDP port 1194. These ports need to be open.
- The SMC IoT VPN Gateway and the devices to connect to must be on the same subnet.
- If testing the VPN in an office setting, check with the office IT group to be sure the VPN is allowed through their firewall.
- The PC set to establish the VPN connection cannot be on the same subnet as the gateway and devices. Otherwise the VPN will not work.