

Operating Manual
OpenVPN Server Start-up Guide



Revision: 2.E

Document No.: T18665

Print Spec: 10000005389 (F)



fieldserver

MSA Safety
1000 Cranberry Woods Drive
Cranberry Township, PA 16066 USA

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

For your local MSA contacts, please go to our website www.MSAsafety.com

Contents

1	Setup Amazon AWS Server	4
2	Setup OpenVPN Cloud	5
2.1	OpenVPN Server Configuration	5
2.2	Login to the Server	5
2.3	Create a New User for the PC Connection	6
2.4	Create a New User for the Device Connection	8
3	Configure FieldServer for OpenVPN	9
3.1	Download the DEVICE Configuration Profile	9
3.2	Load the DEVICE OpenVPN Connection Profile onto the FieldServer	10
4	Install the OpenVPN Client onto a Local PC	11
4.1	Download the USER Configuration Profile	11
4.2	Load the USER OpenVPN Connection Profile onto the PC	12
5	Troubleshooting	13
5.1	General Notes	13

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.

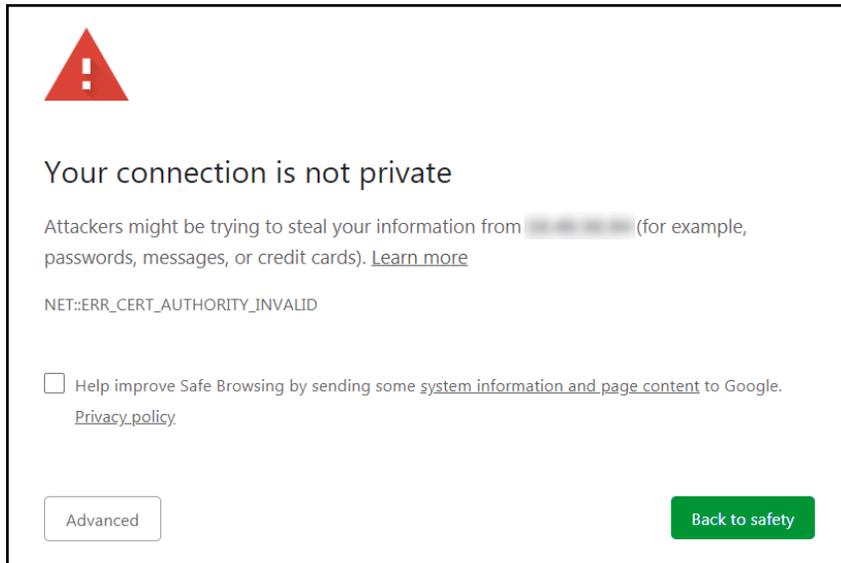
2 Setup OpenVPN Cloud

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

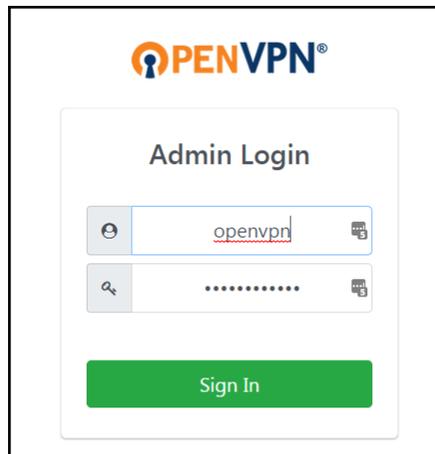
- This may generate a security warning as there is no certificate for HTTPS to verify. Click the Advanced button to proceed to the IP Address (unsafe). A domain with DNS entry can resolve this error.



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

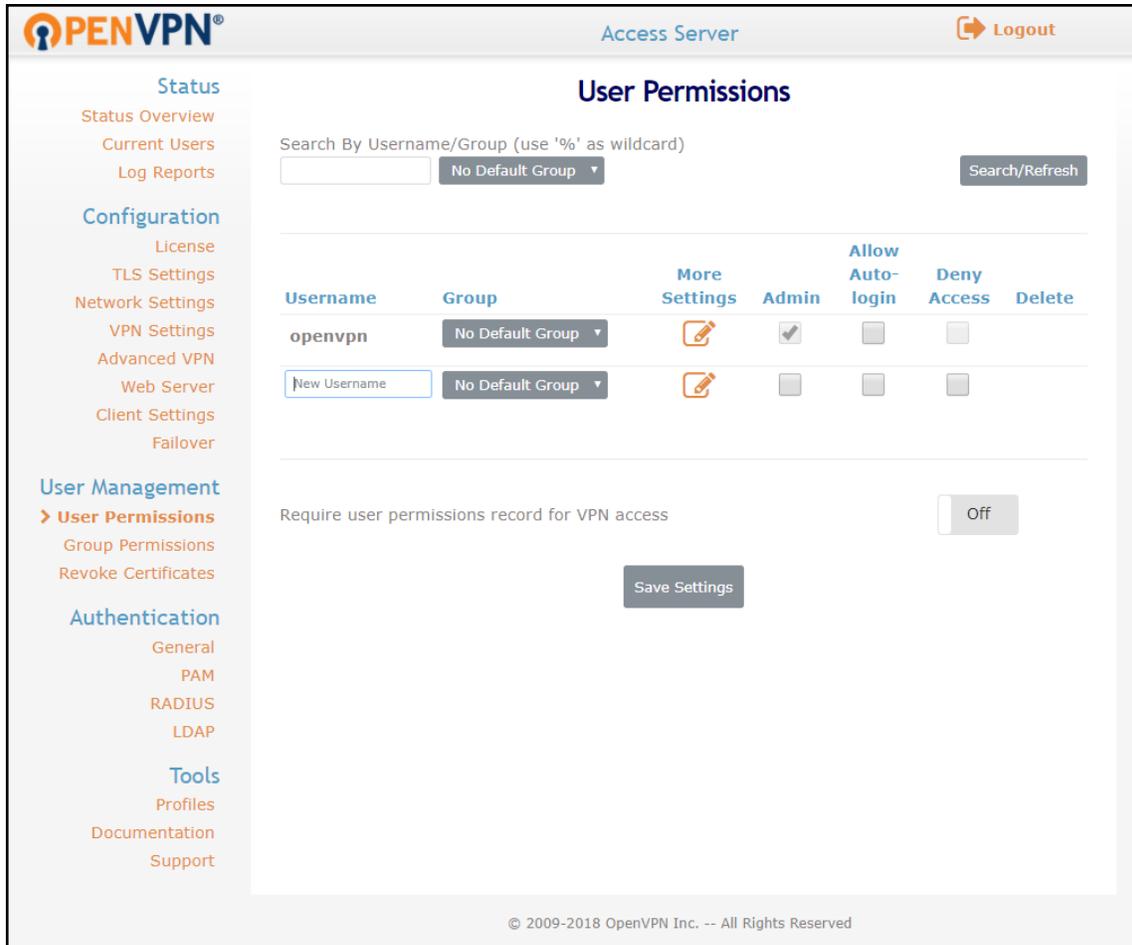
2.2 Login to the Server

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

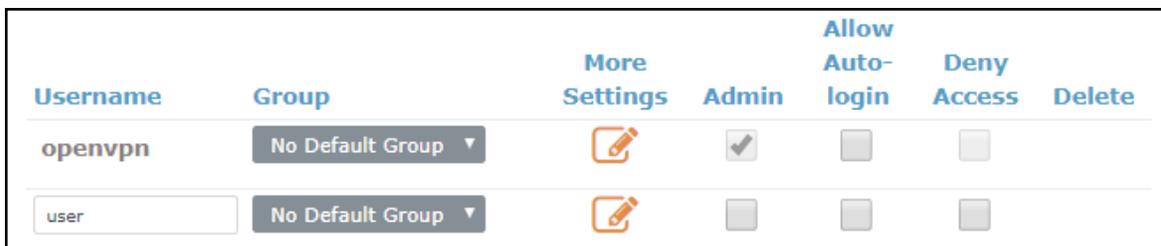


2.3 Create a New User for the PC Connection

- 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.

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
user	No Default Group		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Local Password:

Select IP Addressing: Use Dynamic Use Static

Access Control

Select addressing method: Use NAT Use routing

Allow **Access To** these Networks:

Allow **Access From**: all server-side private subnets

Allow **Access From**: all other VPN clients

VPN Gateway

Configure VPN Gateway: No Yes

DMZ settings

Configure DMZ IP address: No Yes

Require user permissions record for VPN access Off

Save Settings

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

User Permissions Changed

User 'user' added.

Default permissions changed (default set to Allow access).

Press the button below to propagate the changes to the running server.

Update Running Server

Running Server Updated

The relevant components of the server have been restarted to activate the changes made to the active profile

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.

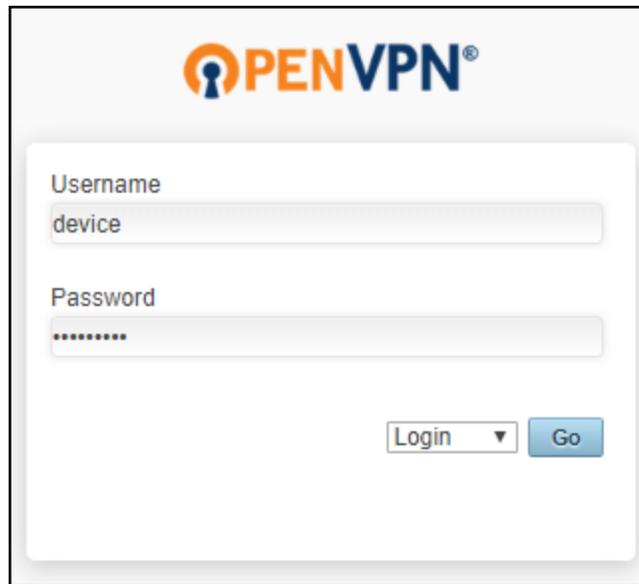
Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
user	No Default Group		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="device"/>	No Default Group		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

- 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.

3 Configure FieldServer for OpenVPN

3.1 Download the DEVICE Configuration Profile

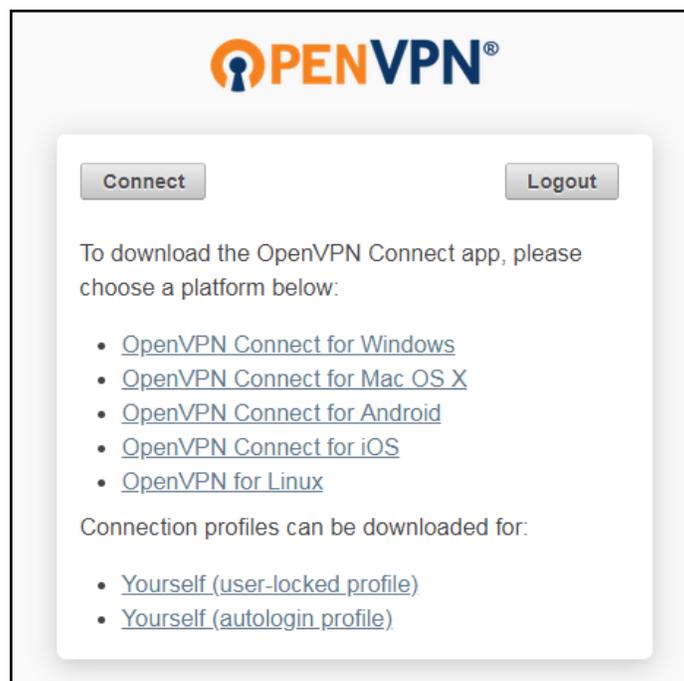
- Login with the DEVICE credentials that were created in [Section 2.4 Create a New User for the Device Connection](#).



The image shows the OpenVPN login interface. At the top is the OpenVPN logo. Below it is a form with two input fields: 'Username' containing the text 'device' and 'Password' containing a series of dots. At the bottom right of the form are two buttons: 'Login' with a dropdown arrow and a blue 'Go' button.

- Click on “Yourself (autologin profile)”.

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



The image shows the OpenVPN post-login screen. At the top is the OpenVPN logo. Below it are two buttons: 'Connect' and 'Logout'. The main content area contains the text: 'To download the OpenVPN Connect app, please choose a platform below:' followed by a list of links: 'OpenVPN Connect for Windows', 'OpenVPN Connect for Mac OS X', 'OpenVPN Connect for Android', 'OpenVPN Connect for iOS', and 'OpenVPN for Linux'. Below this is the text: 'Connection profiles can be downloaded for:' followed by a list of links: 'Yourself (user-locked profile)' and 'Yourself (autologin profile)'.

- 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:

Stat	Value
Status	Online
Up time	03:31:03
Rx Bytes	13968
Tx Bytes	343893

- 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.

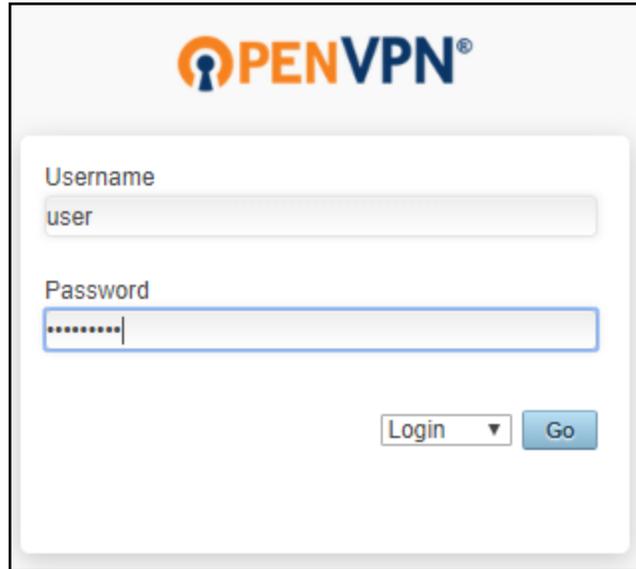
Once OpenVPN is enabled on the FieldServer, it will connect to the OpenVPN server.

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 Create a New User for the PC Connection](#).



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

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

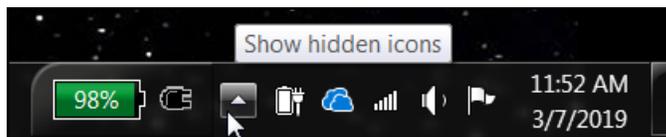


- Click on Logout.

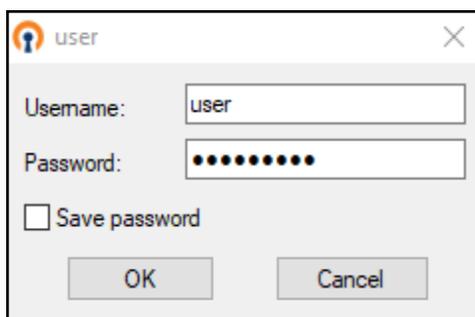
4.2 Load the USER OpenVPN Connection Profile onto the PC

- Download and install the OpenVPN client at:
<https://swupdate.openvpn.org/community/releases/openvpn-install-2.4.6-l602.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.

5 Troubleshooting

5.1 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.