MilesightVPN

User Guide

Preface

Thanks for choosing MilesightVPN. As a web-based VPN monitoring and management platform, MilesightVPN establishes a virtual private network for communications between users and devices to offer a highly reliable, efficient and secure solution for connecting to machines remotely.
This guide teaches you how to configure and operate the MilesightVPN. You can refer to it for detailed functionality and configuration.

Readers

This guide is intended for the following users:

- Distributors
- Network Planners
- On-site technical support and maintenance personnel
- Network administrators responsible for network configuration and maintenance

For assistance, please contact
Milesight technical support:
Email: iot.support@milesight.com
Tel: 86-592-5085280
Fax: 86-592-5023065
Address: Building C09, Software Park III, Xiamen 361024, China

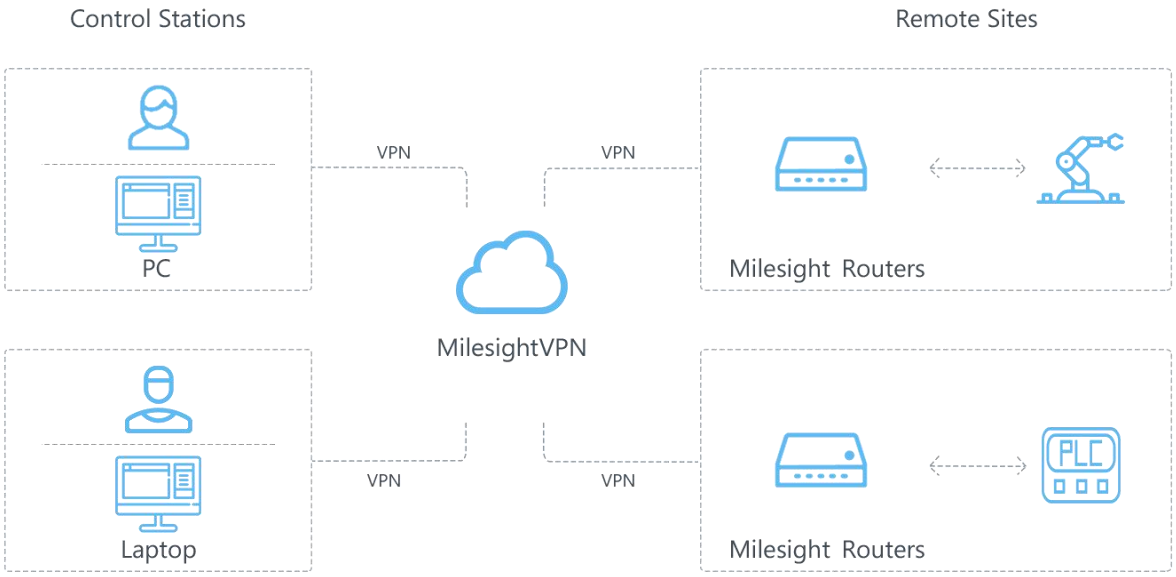
Revision History

Date	Doc Version	Description
Aug. 29, 2018	V.1.0	Initial version
Mar. 25, 2020	V.1.1	Optimize the installation steps
Jun. 3, 2021	V 2.0	Replace Brand to MilesightVPN
Sept. 2, 2021	V 2.1	Support Ubuntu 20.04
Dec. 9, 2021	V 2.2	1. Logo Change 2. Add uninstall commands and network tool detection

Contents

Introduction

MilesightVPN, based on WEB service design, addresses the increasing demand for bandwidth and wireless remote data access and establishes a secure and reliable VPN tunnel for users and remote devices to ensure the security of data transmission. It also solves the problem of the lack of public network IP for routers in mobile cellular network, and implements local direct access to remote devices. Basic usage of MilesightVPN are as follows:



1. MilesightVPN works as OpenVPN server. **Note** that OpenVPN server needs to have public IP.
2. Milesight routers or CPEs work as OpenVPN client and connect with MilesightVPN.
3. The control station can be a laptop or other devices also working as OpenVPN clients. After establishing connection with the MilesightVPN, control station can remotely access to the devices that connected with Milesight routers or CPEs.

Compatibility

The following Milesight IoT products support connection and management with MilesightVPN:

- UR Series Router
- UF51 5G CPE

System Requirements

Hardware

It' s suggested to use the server which suit following requirements:
For 500 devices

- CPU: 2 Cores, 2.0 GHz
- RAM: 16 GB
- Disk: 512 GB
- Bandwidth: ≥100MBps

For 1000 devices

- CPU: 8 Cores, 3.2 GHz
- RAM: 32 GB
- Disk: 1 TB
- Bandwidth: ≥100MBps

Software

- Operating System: Ubuntu Server 20.04
- Browser: Chrome, Firefox

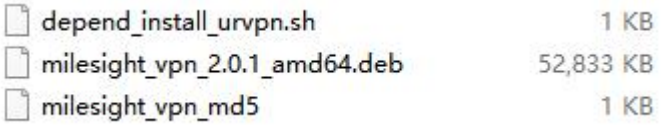
Installation

Requirements

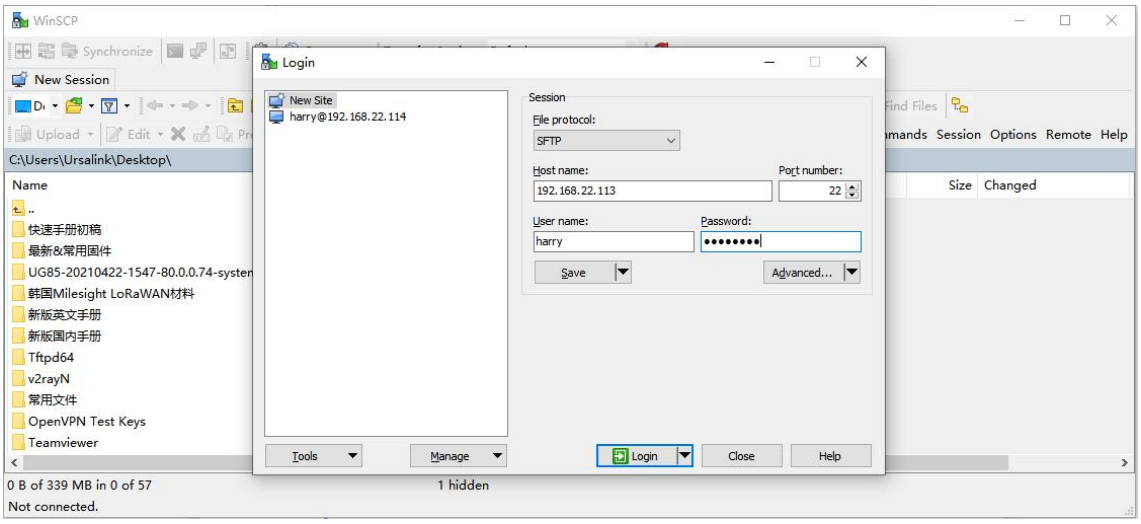
- Ubuntu Server
- MilesightVPN Software Package
- WinSCP
- Putty (or other SSH tool)

Package Upload

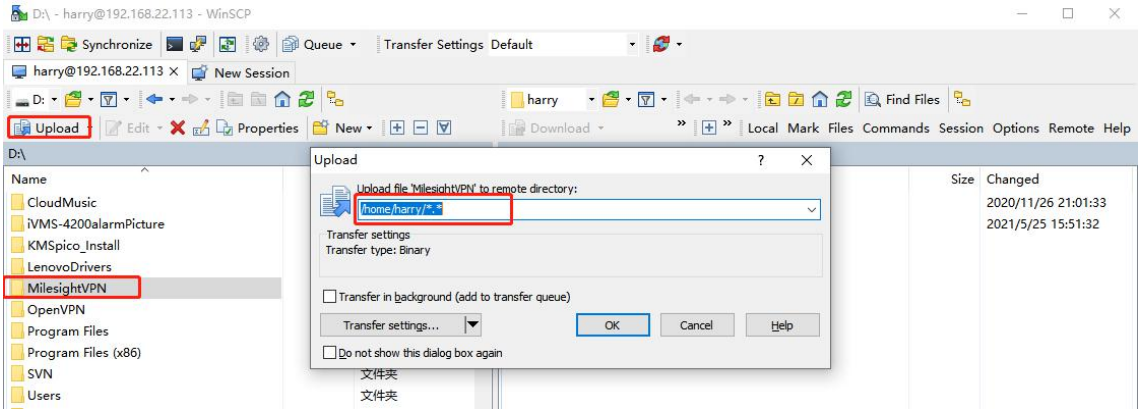
Following steps are based on WinSCP tool. You can also use other tools to upload packages.
1. Download the MilesightVPN package from Milesight IoT website, then extract and check files:

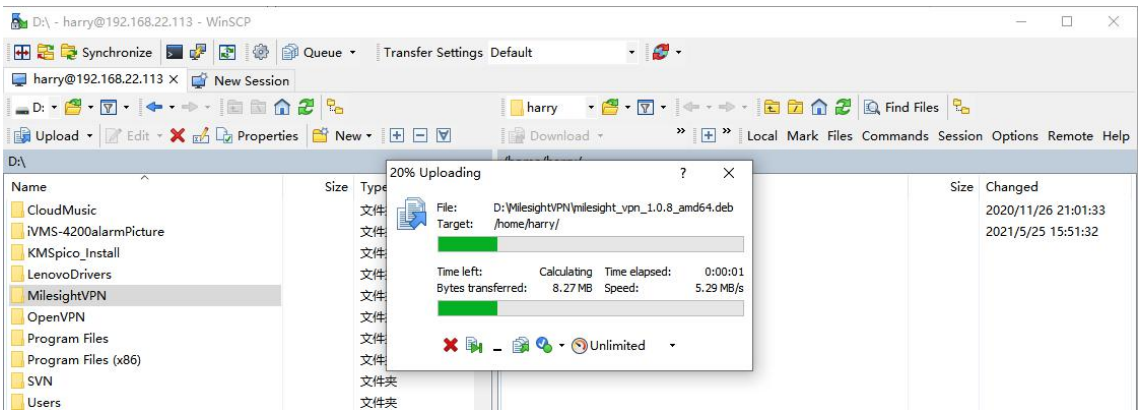


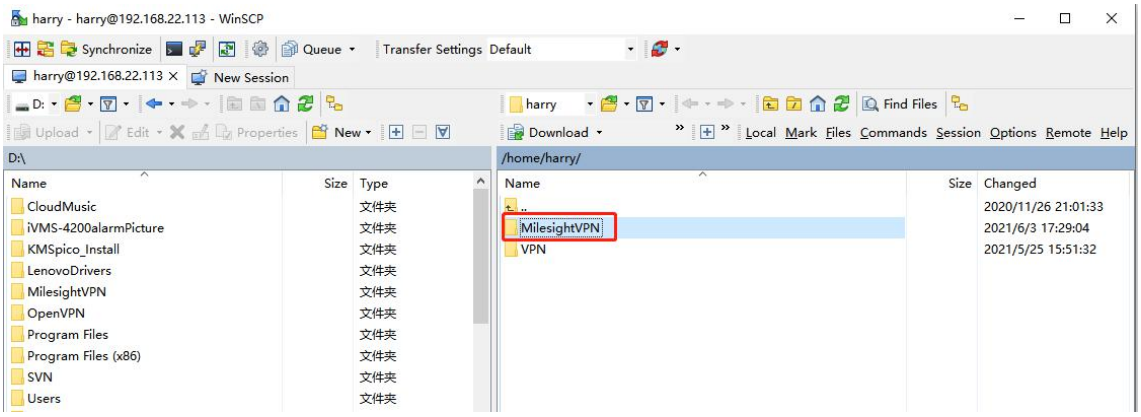
2. Open WinSCP and set up a session between WinSCP and server.



3. Select the MilesightVPN folder and click “Upload”, select the server path and click “OK” to upload.

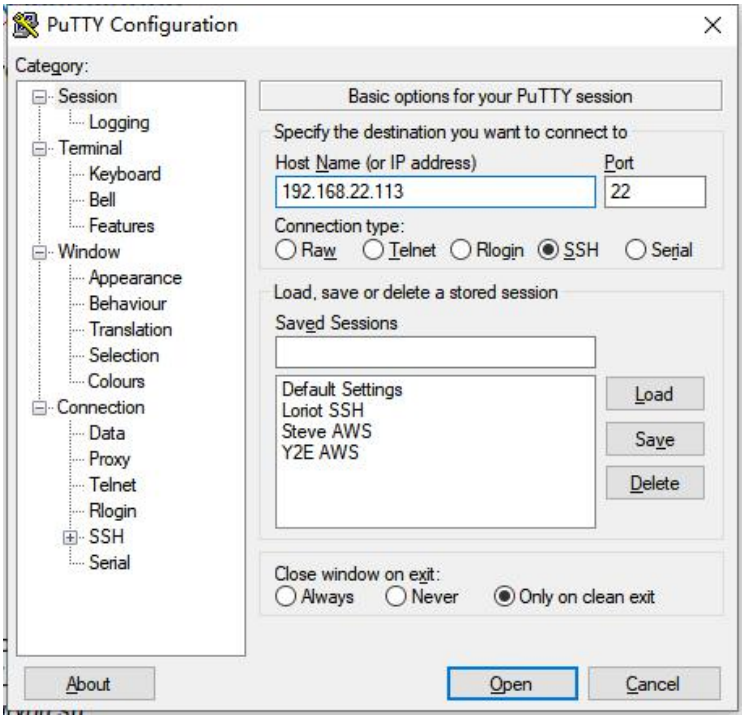






MilesightVPN Installation

1. Log in the server via Putty. You can also use other SSH tools.

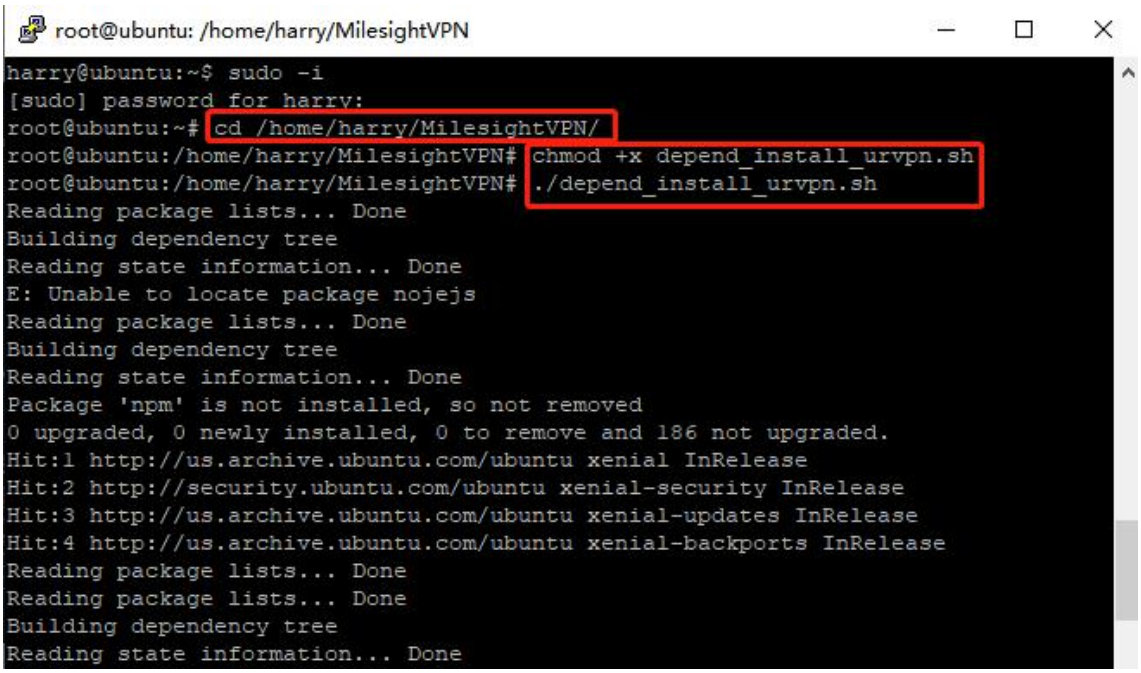


2. Ensure the netwrok tool is installed in the server. You can type *ifconfig* to check it. If not found, excute *apt install net-tools* to install it.

```
root@yuxy:/etc/netplan# ifconfig

Command 'ifconfig' not found, but can be installed with:

apt install net-tools

root@yuxy:/etc/netplan#
```

3. Run following commands under MilesightVPN directory.

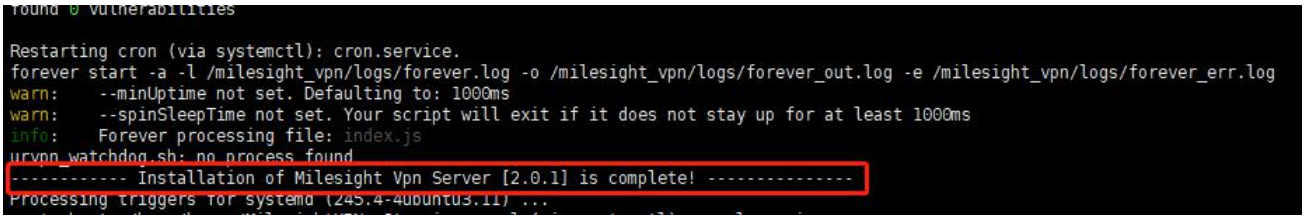
```
chmod +x depend_install_urvpn.sh
./depend_install_urvpn.sh
```



4. Install DeviceHub software. Take the 2.0.1 version as example, please type following command:

```
dpkg -i milesight_vpn_2.0.1_amd64.deb
```

It will take about 10 minutes to complete the installation and there will show following message when the installation complete.



Note:

If you need to upgrade to V2.0.1 from V1.0.19, please backup the VPN database and uninstall the old version program, then install new version. More details about backup and restore please contact Milesight technical support.

MilesightVPN Uninstallation

If you need to uninstall the MilesightVPN, run following commands:

```
sudo rm /etc/init.d/milesight_vpn.sh /etc/init.d/urvpn-server.sh
/etc/init.d/urvpn_watchdog_start.sh
sudo rm -rf /milesight_vpn
sudo dpkg -P milesight-vpn
sudo apt-get remove mysql*
```

Services and Ports

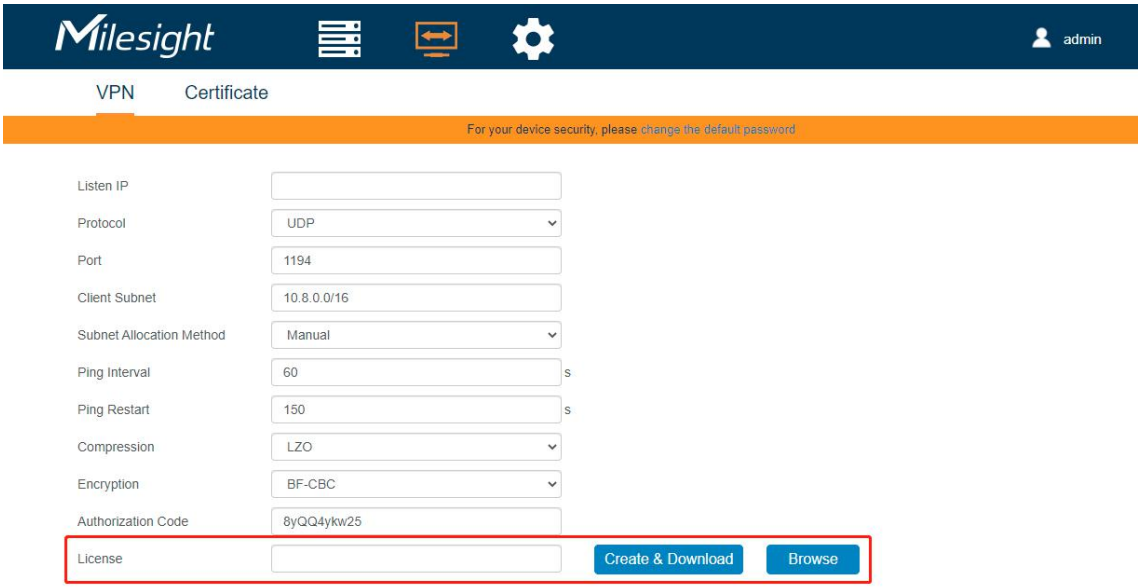
In order to ensure the security and unblocked communication, here are ports for services:

Port	Protocol	Description
18080	TCP	HTTP Service
18443	TCP	HTTPS Service
1194	TCP	OpenVPN Service

Expand Manage Devices

The number of available managing devices can be checked in “Device” tab. Maximum number of managing devices is 25 by default. Please refer to following steps to expand manage devices.

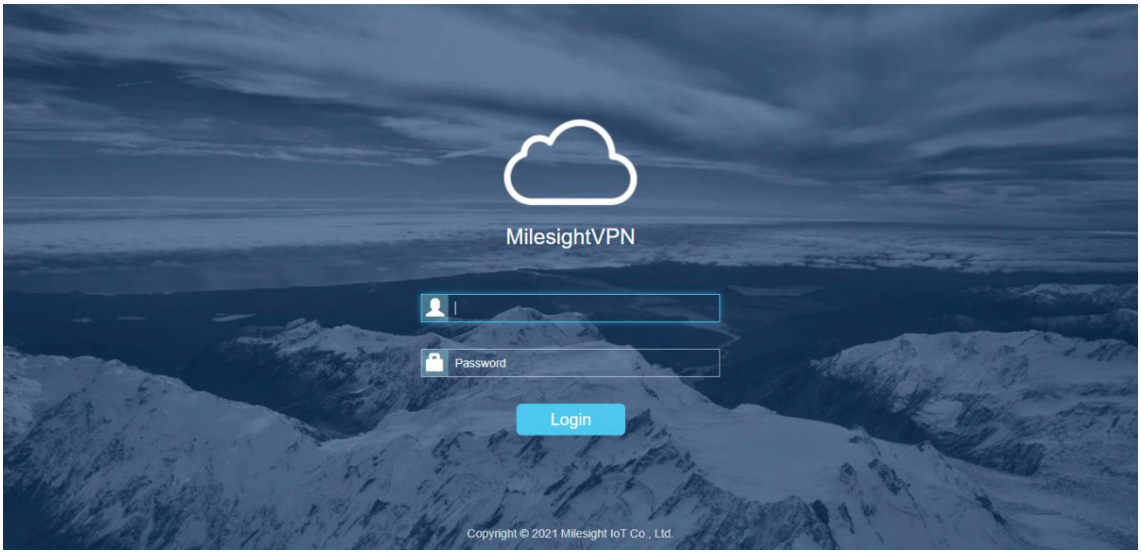
1. Log in MilesightVPN and go to “VPN” tab, then click “Create&Download” to download license info file.
2. Contact Milesight sales or technical support and send the license info file.
3. Get expand license from Milesight and click “Browse” to import the license.
4. Click “save” to save the settings and the max manageable devices will change.



General Settings

Login MilesightVPN

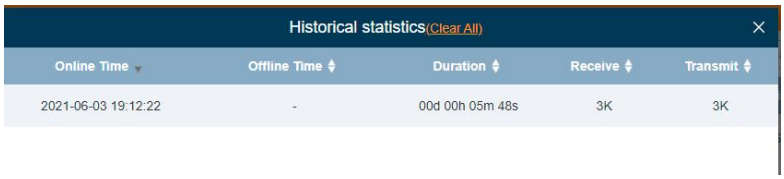
After installation, type https://server ip:18443 or http://server ip:18080 to visit the login page.
Default username: admin
Default password: password



Device

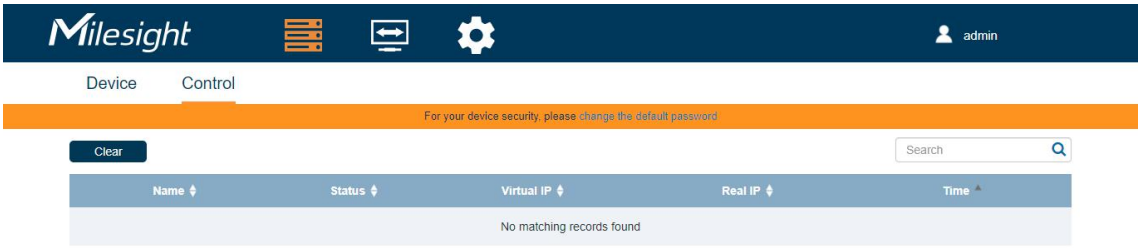
Display the information about Milesight devices connected to MilesightVPN. You can modify the "Name" and "Remote Subnet" when the subnet allocation method is "Manual".

Device Information	
Item	**Description**
Name	Show the name of device. Users can click it to change the name.
Status	Show the connection status of device.
Serial Number	Show the serial number of device.
Virtual IP	Show the virtual IP of device.
Real IP	Show the real IP address of device's WAN port/cellular.

Remote subnet	Show the subnet segment and mask of devices. Users can click it to change it.
Time	Show the connected time of the control device.
View	Click to view historical statistics record. 
Clear	Click to clear disconnect device records.

Control

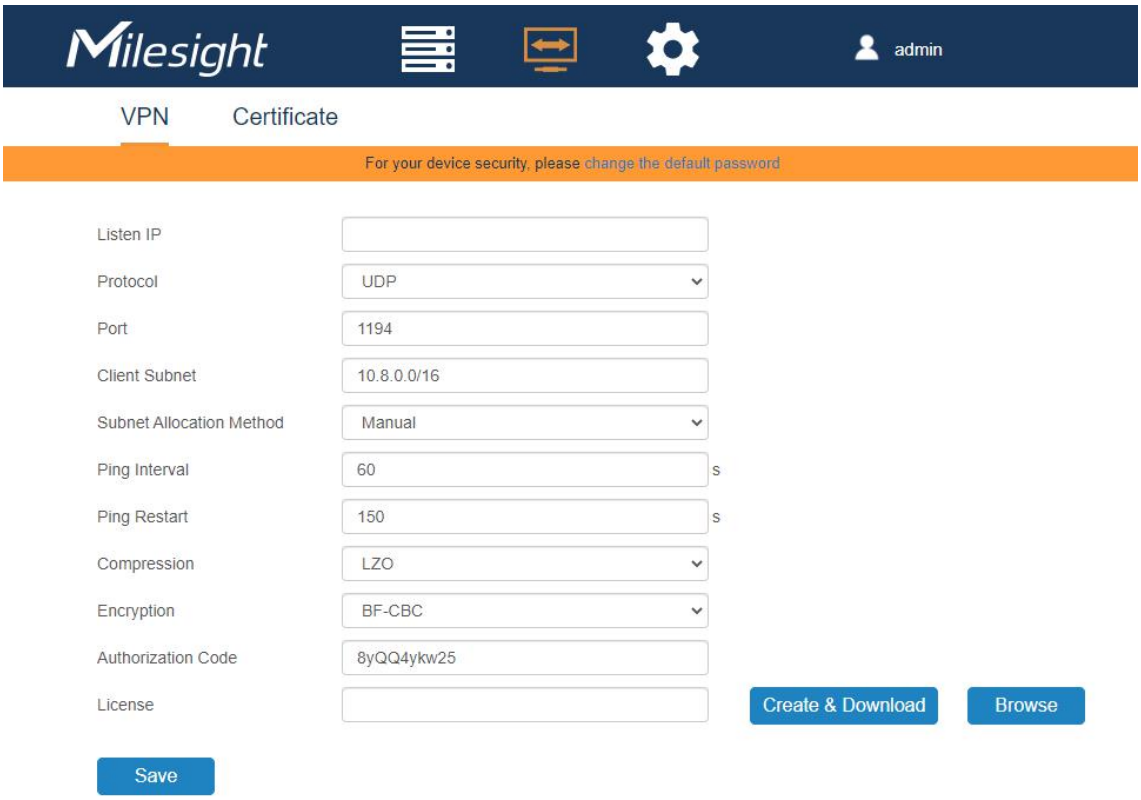
Display the information about control devices (PC, laptop, etc.) connected to MilesightVPN. You can modify the “Name” and “Remote Subnet” when the subnet allocation method is “Manual”.



Control Information	
Item	**Description**
Name	Show the name of the control device.
Status	Show the connection status of control device.
Virtual IP	Show the virtual IP of device.
Real IP	Show the real IP address of control device.
Time	Show the connected time of the control device.
Clear	Click to clear disconnect device records.

VPN

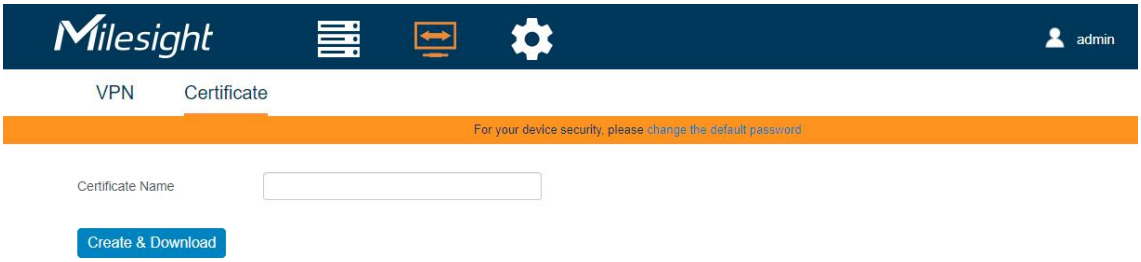
Configure basic VPN settings and import expand license. After changing VPN settings, please re-connect the Milesight devices to make it take effect.



VPN		
Item	**Description**	**Default**
Listen IP	Enter the IP address of the MilesightVPN.	Null
Protocol	Select communication protocol (TCP/UDP).	UDP
Port	Service port	1194
Client Subnet	Set the segment and the mask of the virtual addresses pool.	10.8.0.0/16
Subnet Allocation Method	Select from “Manual” or “Auto” options. Manual: Modify remote subnet manually from the Device page Auto: Configure remote subnet automatically via “Subnet Behind Client”.	Manual
Subnet Behind Client	Configure Milesight device subnet.	Null
Ping Interval	Set the Ping interval (in second)	60
Ping Restart	Reconnection interval (in second)	150
Compression	Select from “None” or “LZO” options. LZO: Lempel-Ziv-Oberhumer (or LZO) is a lossless algorithm that compresses data to ensure high decompression speed.	LZO
Encryption	Select from “NONE”, “BF-CBC”, “DES-EDE3-CBC”, “AES-128-CBC”, “AES-192-CBC” and “AES-256-CBC”.	BF-CBC
Authorization Code	Input the Authorization Code for Milesight device connection (5 to 31 alphanumeric combinations) .	Random
License	Import the license for expanding manage devices.	/

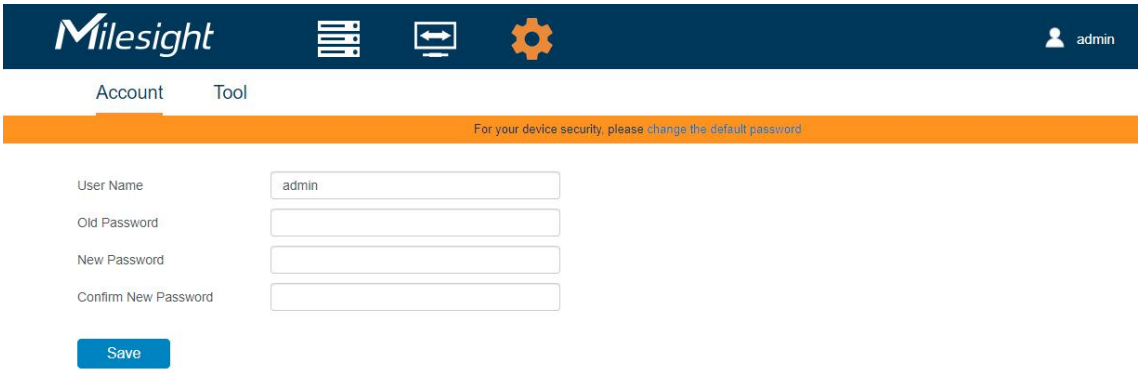
Certificate

After clicking “Create & Download”, it will generate a unique ovpn file with certificate for control devices to connect to MilesightVPN.



Account

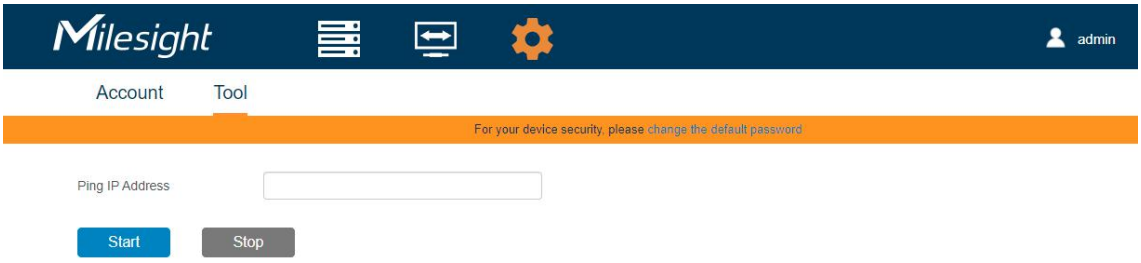
You can edit the information about user account on this page.



Account	
Item	**Description**
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-", "$". The first character can't be a number.
Old Password	Enter the old password.
New Password	Enter a new password to change the password.
Confirm New Password	Enter the new password again.

Ping Tool

Ping tool is used for checking network connection between MilesightVPN and other devices.

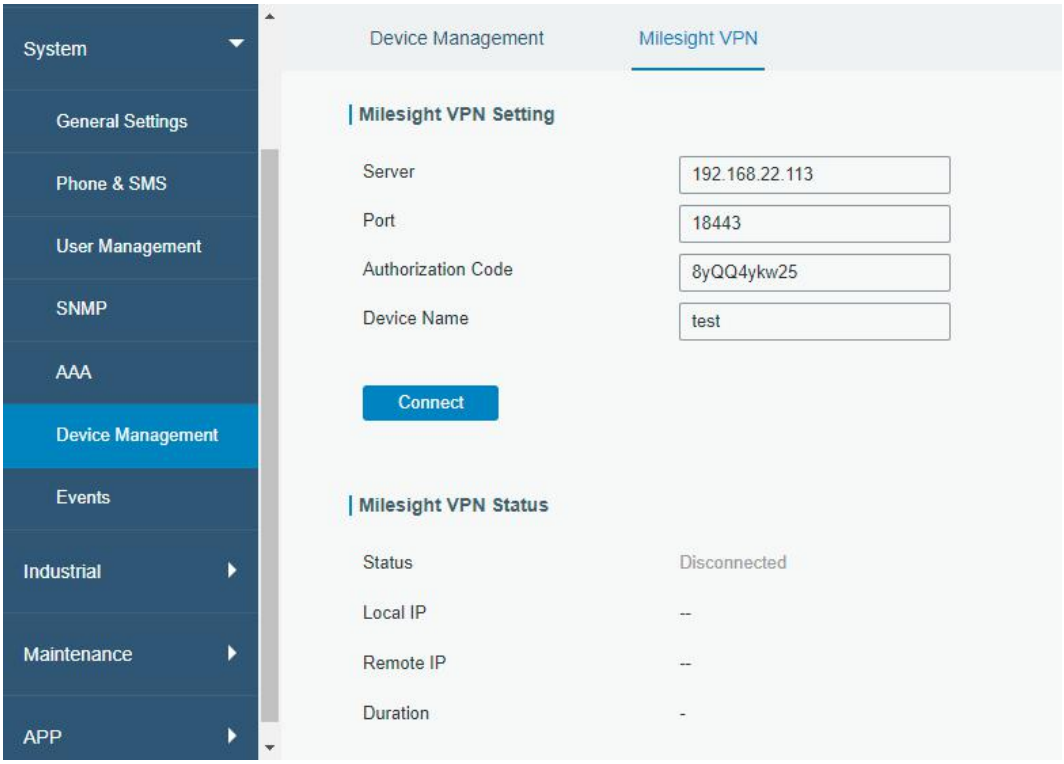


Application Example

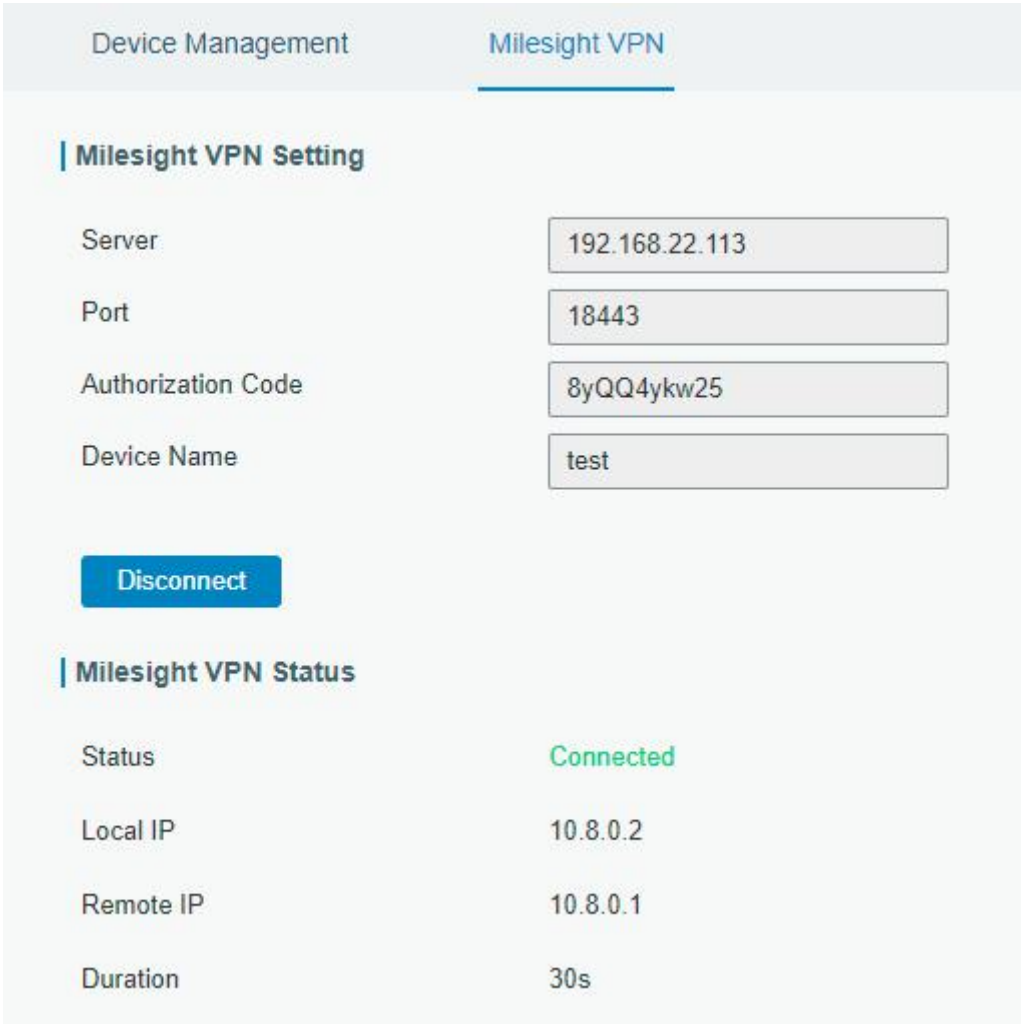
Connect Milesight Devices to MilesightVPN

1. Ensure the network between routers and MilesightVPN platform is normal.
2. Go to "System -> Device Management -> MilesightVPN" page to fill in MilesightVPN server information.

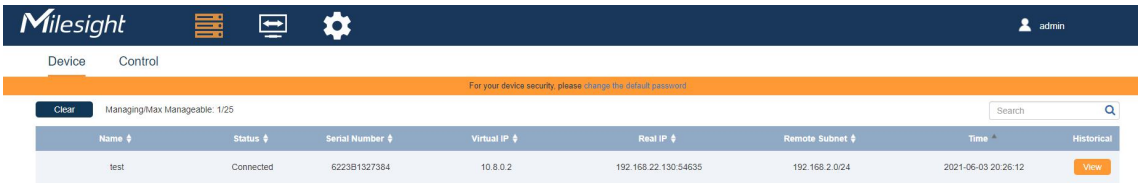
- **Server:** MilesightVPN server address or domain name
- **Port:** 18443 (Fixed)
- **Authorization Code:** this code can be found on VPN page of MilesightVPN server
- **Device Name:** user-define name



3. Click "Connect" and after a while, you can check it shows "connected".

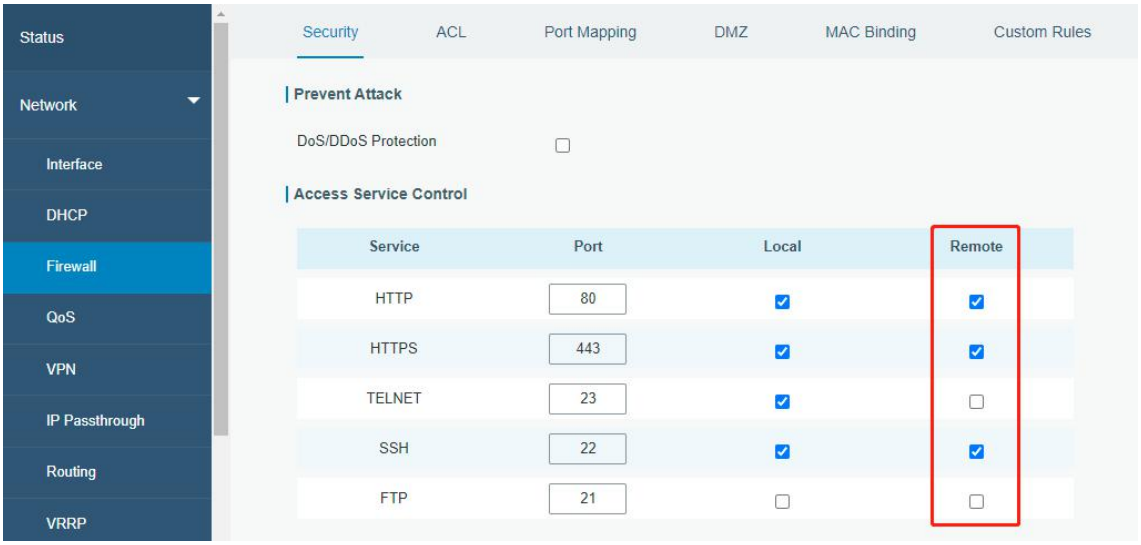


Router connection status can also be checked on MilesightVPN web GUI.



Note: time synchronization is needed between MilesightVPN and routers.

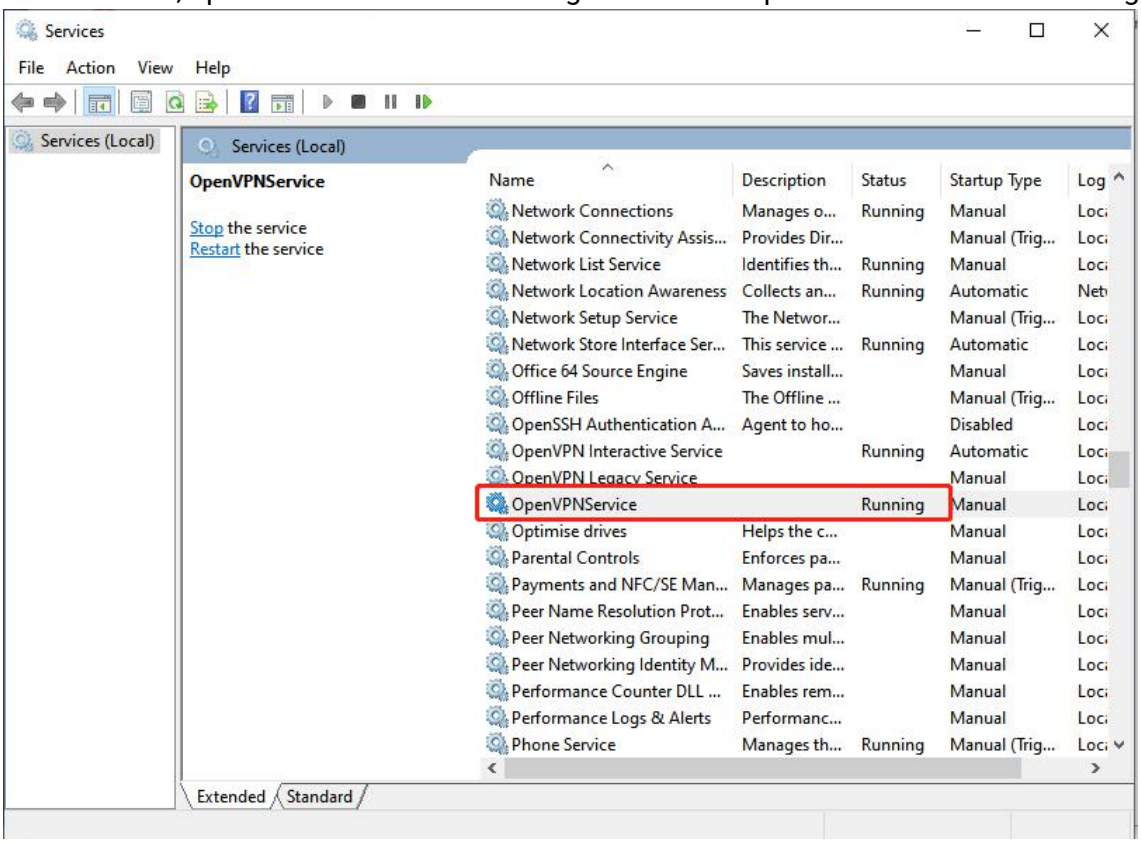
4. Go to “Network -> Firewall -> Security” to enable remote access services if you need to remotely access routers. You can also change service ports here.



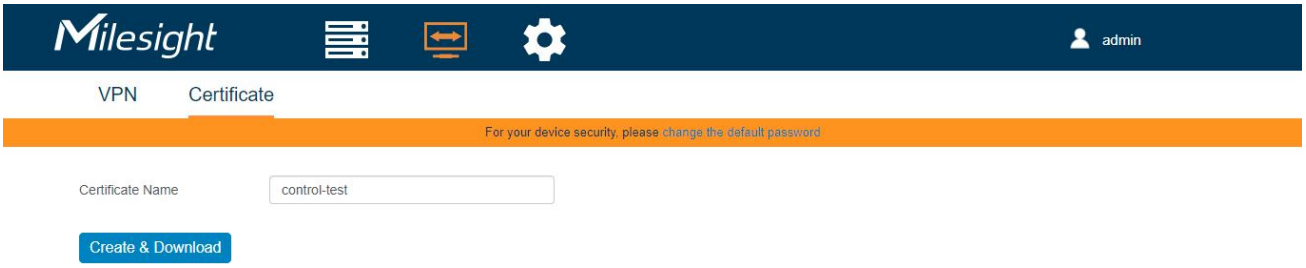
Connect Control Device to MilesightVPN

This example mainly introduces how to connect a Windows10 laptop to the MilesightVPN platform.

1. Install OpenVPN software. You can select either OpenVPN Connect or Community OpenVPN as OpenVPN client.
2. After installation, open Windows Service Manager to ensure OpenVPN services are running.



3. Go to “Certificate” page of MilesightVPN, fill in a certificate name, click “Create & Download” to download the certificate.



Note:

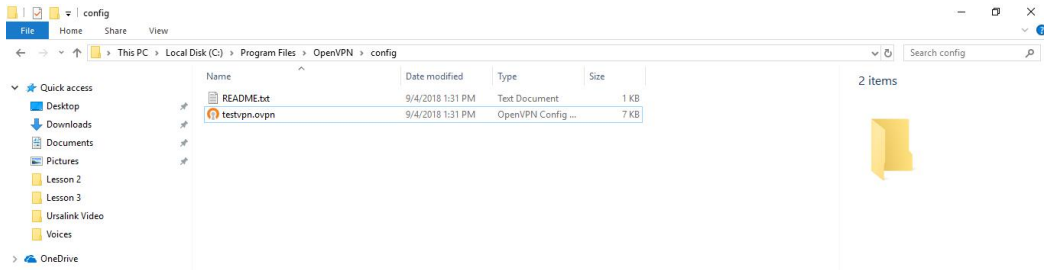
1) If there is not Milesight VPN server IP address in the certificate, check if you fill in Listen IP in VPN page of MilesightVPN.

2) If you use default certificate, all traffic will pass VPN tunnels and the laptop may not access the Internet. In order to define a specific tunnel and not affect normal Internet access, please open the certificate and change “redirect-gateway defl” to “route 192.168.0.0 255.255.0.0” (192.168.0.0 is the subnet of Milesight routers).

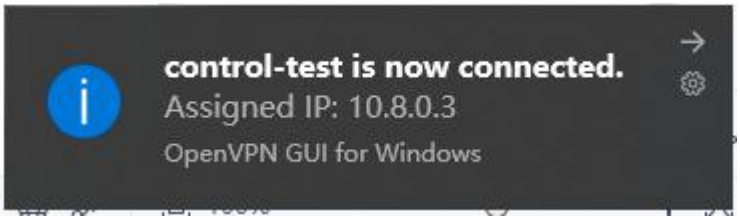
```
comp-lzo
cipher BF-CBC
dev tun100
remote 192.168.22.113 1194
proto udp
resolv-retry 0
nobind
up-delay
verb 3
keepalive 60 150
topology subnet
client
redirect-gateway defl
<ca>
```

4. Run OpenVPN software with the certificate.

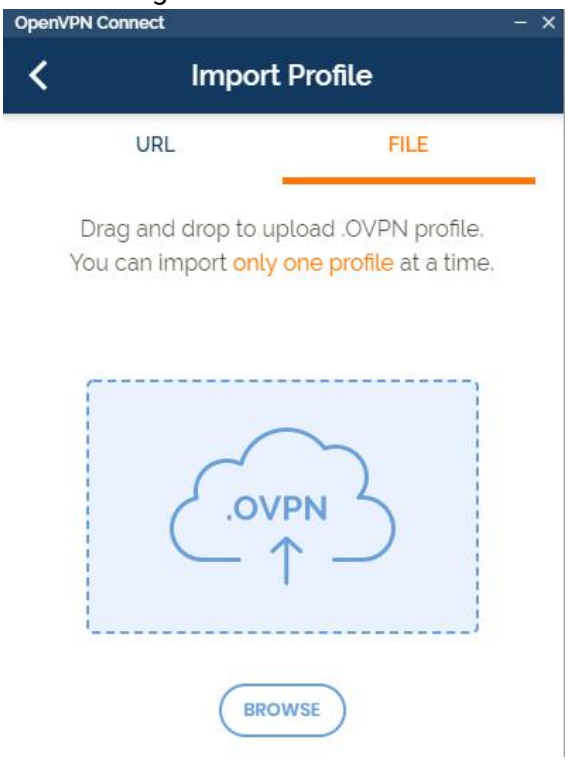
1) If you use Community OpenVPN, put the certificate under “OpenVPN/config” folder.

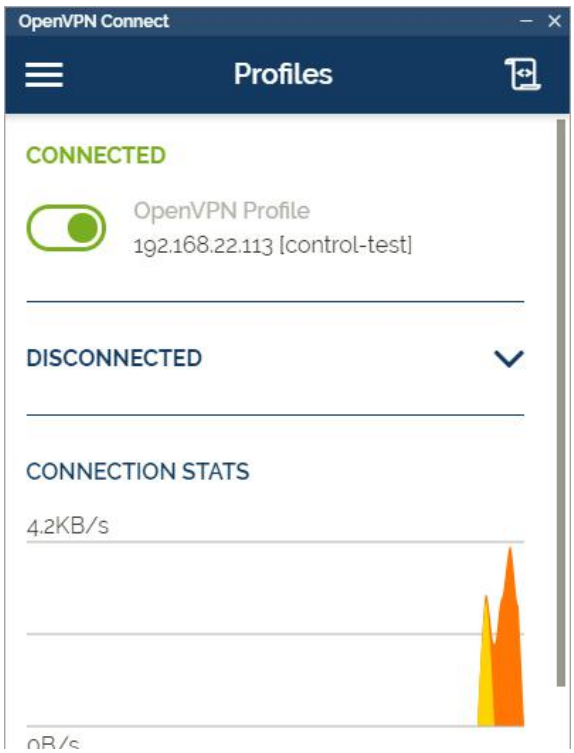


then run OpenVPN GUI, select this file to click Connect.



2) If you use OpenVPN Connect, run the software and import the certificate, then connect device to MilesightVPN.

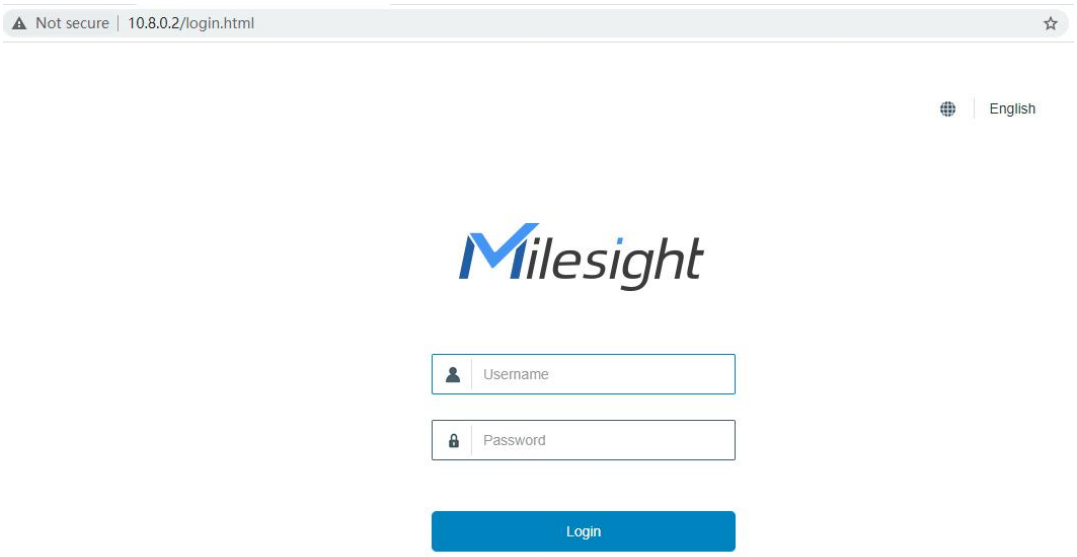




Devices Communication

Method 1: Virtual IP Access

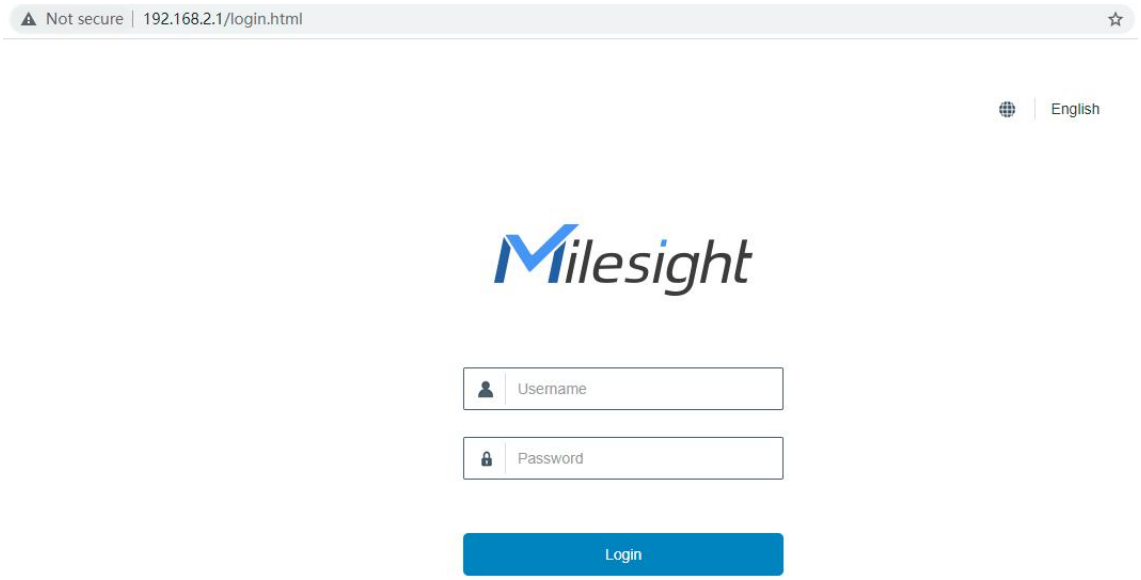
Users can use virtual IP: http port to access router from laptop.



If you need to access the devices under router subnet, you can add a port mapping rule in router web GUI and use virtual IP: port to access the device.

Method 2: Real IP Access

Users can use real subnet IP (bridge0) to access router from laptop. For that ensure the subnet is different from your laptop and laptop routing table should include the subnet.



–END–