URSALINK

RG2i Groupe 2AR
Capter - Transmettre - Analyser
Interfaces pour l'informatique industrielle

UrsalinkVPN
User Guide

RG2i Groupe 2AR
Capter - Transmettre - Analyser
Interfaces pour l'informatique industrielle

Rémy GUÉDOT
Gsm: +33 (0) 662 80 65 57
guedot@rg2i.fr

Olivier BENAS
Gsm: +33 (0) 666 84 26 26
olivier.benas@rg2i.fr

14 rue Edouard Petit - F42000 Saint Etienne
Tél: +33 (0) 477 92 03 56 - Fax: +33 (0) 477 92 03 57
www.rg2i.fr

www.ursalink.com

Preface

Thanks for choosing UrsalinkVPN. As a web-based VPN monitoring and management platform, UrsalinkVPN 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 UrsalinkVPN. You can refer to it for detailed functionality and configuration.

Related Documents

Document	Description
UrsalinkVPN Datasheet	Datasheet for the UrsalinkVPN.

For assistance, please contact
Ursalink technical support:
Email: support@ursalink.com
Tel.: 86-592-5023060
Fax: 86-592-5023065

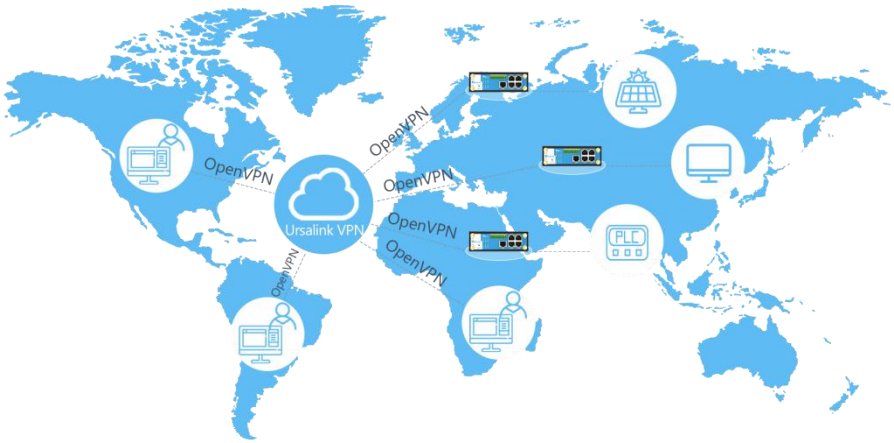
Revision History

Date	Doc Version	Description
Aug. 29, 2018	V.1.0.0	Initial version

Content

Chapter 1 Product Introduction

1.1 Overview



UrsalinkVPN, 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.

1.2 Advantage

Benefits

- Fast VPN Connection
- Security and Remote Access
- Support Multiple Control Stations Connection
- Real-time Connection Status
- Real-time Remote Configuration
- Up to 1000 Devices Connection
- Visualized Page Management

Chapter 2 Installation

2.1 Pre-installation Checklist

Ubuntu 16.04 Server

APK

Supported browsers：Chrome, Firefox

2.2 Installation Steps

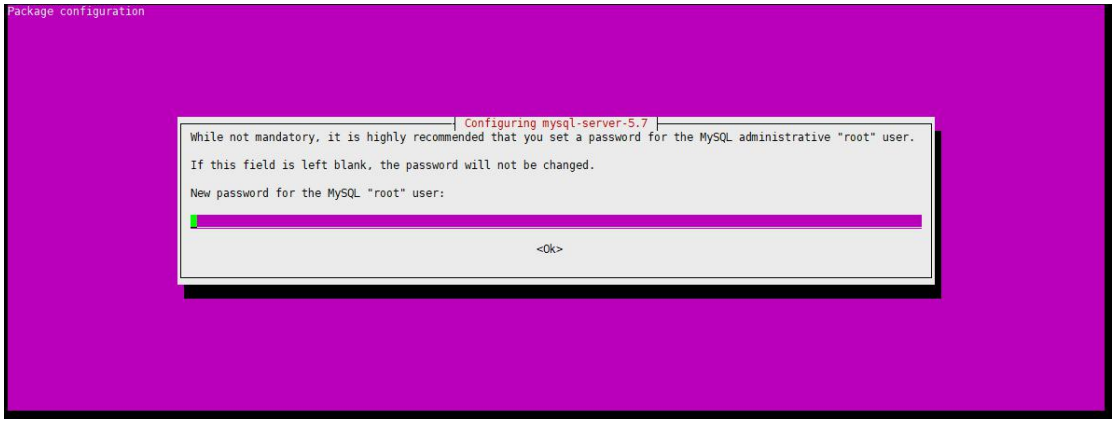
1. Download “depend_install_urvpn.sh” and “ursalink_vpn_1.0.1_amd64.deb”. Upload these two files to Ubuntu server.
   In the example below, a new path named “ursalink” is created.

```
root@ubuntu:/# mkdir ursalink
root@ubuntu:/# cd ursalink/
root@ubuntu:/ursalink# ls
depend_install_urvpn.sh  ursalink_vpn_1.0.1_amd64.deb
root@ubuntu:/ursalink#
```

2. Cd to the path where you upload the two files, and execute the shell commands
   #chmod +x depend_install_urvpn.sh
   #./depend_install_urvpn.sh

```
root@ubuntu:/ursalink# chmod +x depend_install_urvpn.sh
root@ubuntu:/ursalink# ./depend_install_urvpn.sh
```

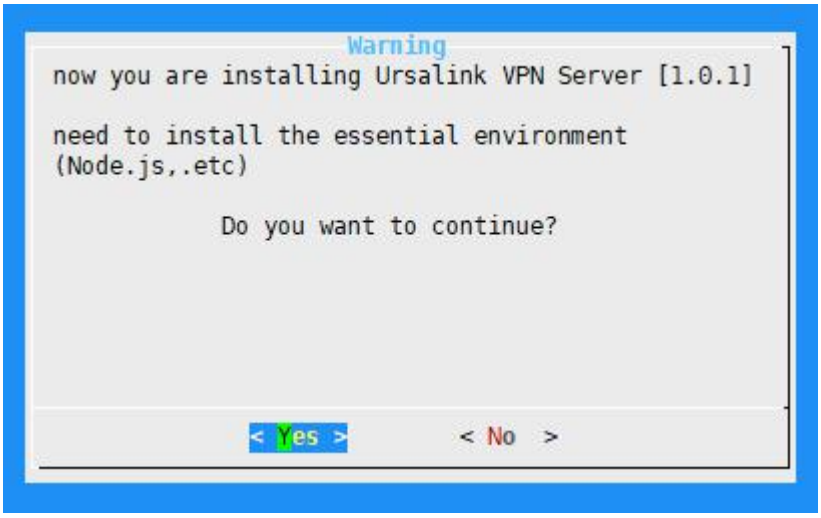
3. Set MySQL Password



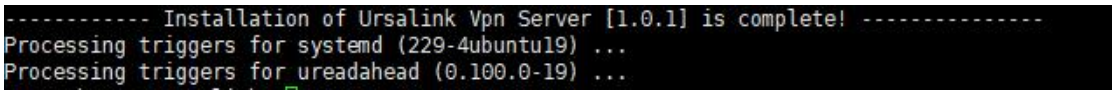
4. Execute dpkg scripts
   #dpkg -i ursalink_vpn_1.0.1_amd64.deb

```
root@ubuntu:/ursalink# dpkg -i ursalink_vpn_1.0.1_amd64.deb
Selecting previously unselected package ursalink-vpn.
(Reading database ... 74186 files and directories currently installed.)
Preparing to unpack ursalink_vpn_1.0.1_amd64.deb ...
```

5. One queries require positive responses



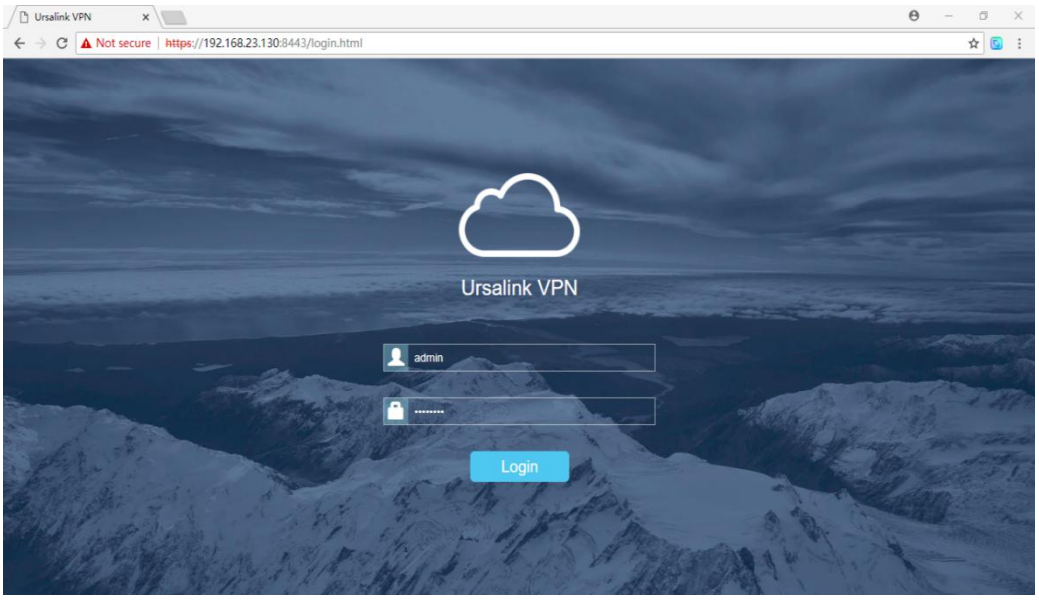
It might take about 10 minutes to complete the installation



6. Log in VPN Server

   Default username: admin

   Default password: password



Note that VPN Server is using port 18080 and 18443

Chapter 3 Configuration

3.1 Device

Display the information about devices connected to UrsalinkVPN. You can modify the Name and Remote Subnet when the subnet allocation method is manual.

Figure 3-1-1

Device Information	
Item	**Description**
Name	Show the name of device
Status	Show the status of device
Serial Number	Show the serial number of device
Virtual IP	Show the virtual IP of device
Real IP	Show the IP address of device's WAN port
Remote subnet	Show the segment and mask of the virtual IP addresses
View	Click to view historical data

Table 3-1-1 Device Information

3.2 Control

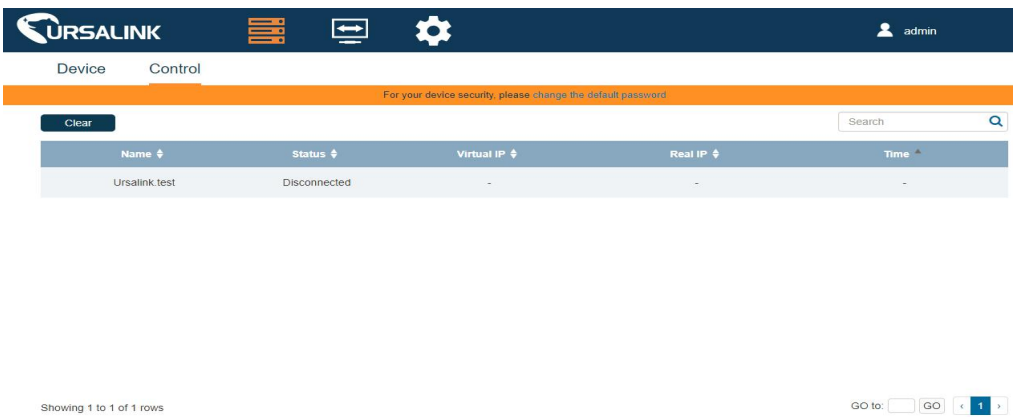


Figure 3-2-1

Control Information	
Item	**Description**
Name	Show the name of control station
Status	Show the status of control station
Virtual IP	Show the virtual IP of control station
Real IP	Show the IP address of control station's WAN port
Time	Show the connect time of the control station.

Table 3-2-1 Control Information

3.3 VPN

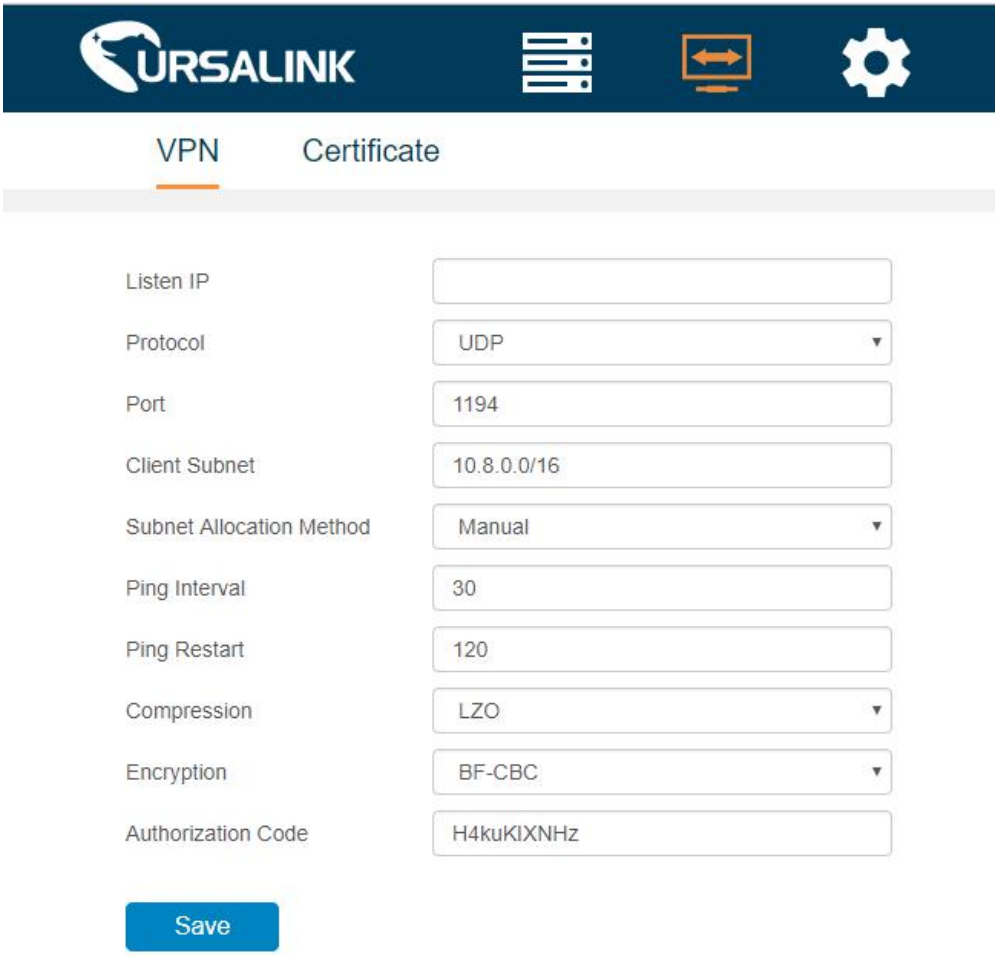


Figure 3-3-1

VPN		
Item	**Description**	**Default**
Listen	Enter the IP address of the UrsalinkVPN.	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 menu Auto: Configure router's IP address via "Subnet Behind Client"	Null
Subnet Behind Client	Configure router's DHCP Server	Null
Ping Interval	Set the Ping interval (in second)	30
Ping Restart	Reconnection interval (in second)	120
Compression	Select from: "None"and"LZO". 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 routers (5 to 31 alphanumeric combinations)	Null

Table 3-3-1 Control Information

3.4 Certificate

You can create and download a certification on this page.

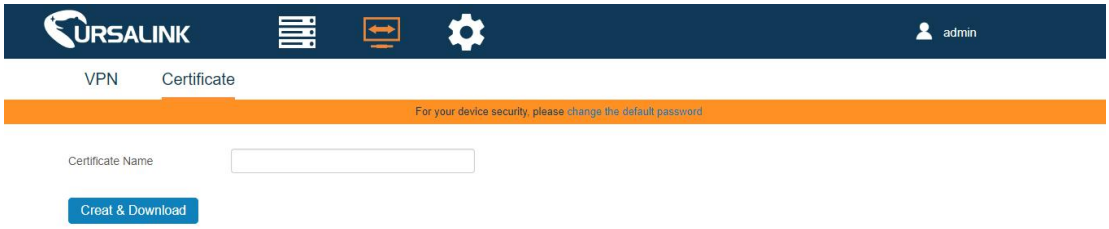


Figure 3-4-1

Certificate		
Item	**Description**	**Default**
Certificate Name	Generate a certifcate for the control station	Null

Table 3-4-1 Certificate Information

Note that always use a unique certificate name for each client.

3.5 Account

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

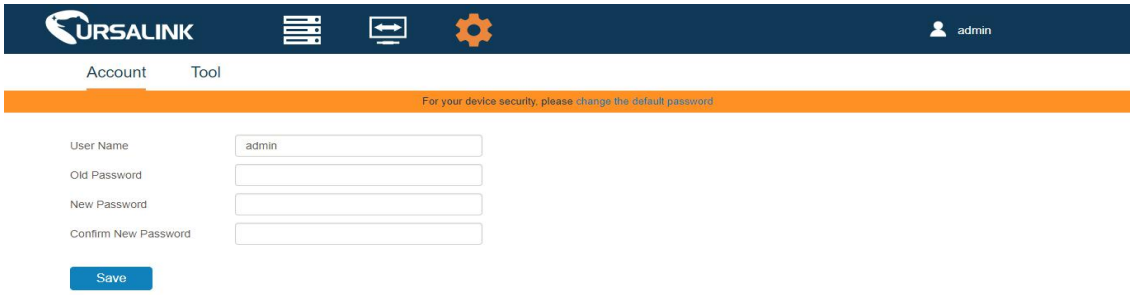


Figure 3-5-1

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.
Confirm New Password	Enter the new password again.

Table 3-5-1 Account Information

3.6 Tool

Detective tool of Ping to detect the connections between the VPN Server, routers and control stations.

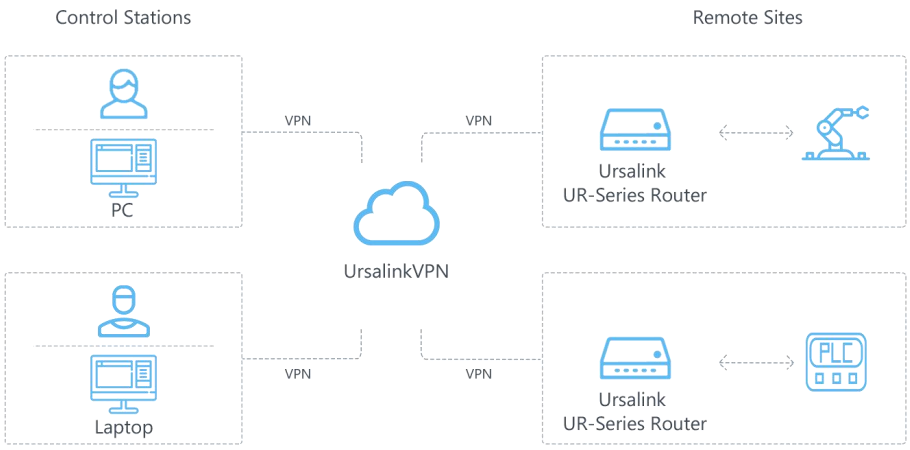
Figure 3-6-1

PING	
Item	**Description**
Ping IP Address	Destination address

Table 3-6-1 Tool Information

Chapter 4 Application Example

4.1 System Topology



1. UrsalinkVPN works as OpenVPN server.
   Note that OpenVPN server needs to have Public IP or uses DDNS.

2. The routers work as OpenVPN client and connect with UrsalinkVPN. And routers should be able to access the network.

3. The control station can be a laptop or other devices work as OpenVPN clients. After establishing connection with the UrsalinkVPN, control station can remote access to the devices that connected with the routers.

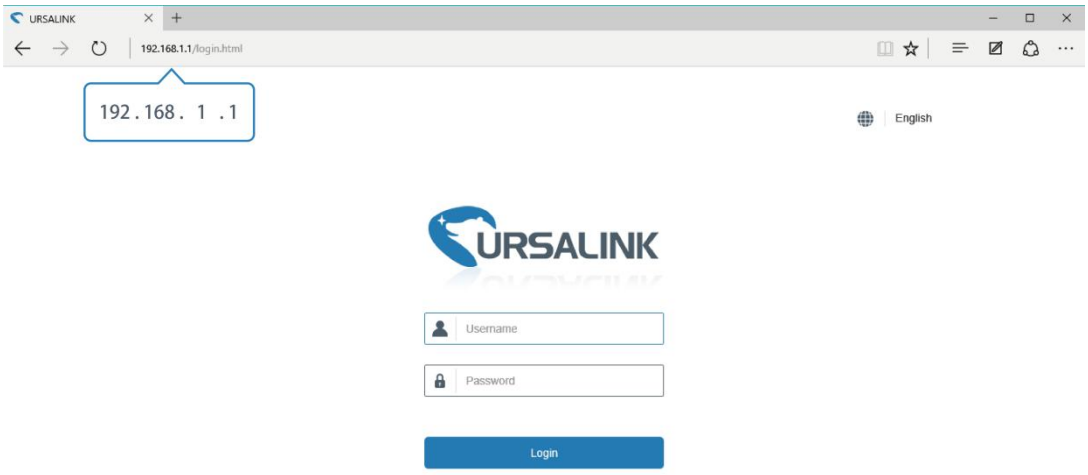
4.2 Connecting Router with UrsalinkVPN

Routers can connect to the UrsalinkVPN platform via cellular network, Wi-Fi, or Ethernet. This example mainly introduces the connection of router to the UrsalinkVPN platform via cellular network.

4.2.1 Network Access

1. Install antennas and SIM card, and then power on the router.
2. Log in to the Web GUI.

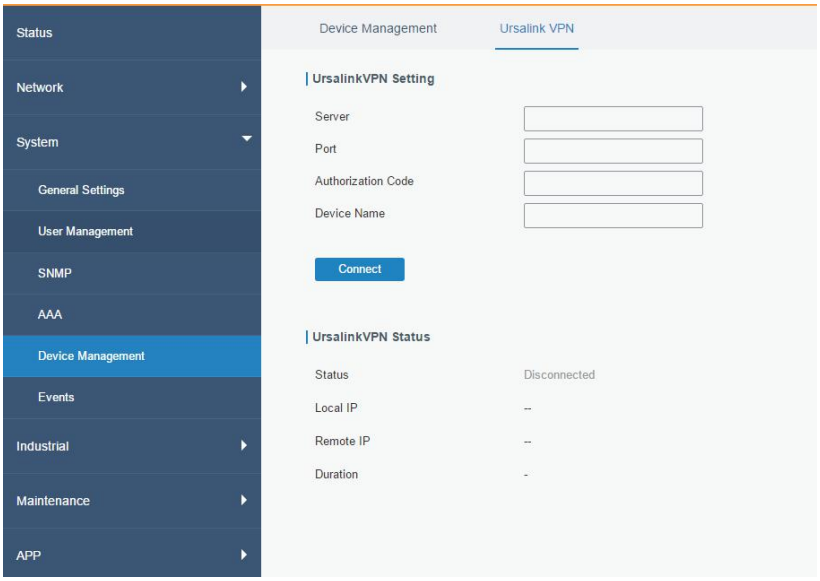
Ursalink router provides web-based configuration interface for device management. If this is the first time you configure the router, please use the default settings below:
IP Address: 192.168.1.1
Username: admin
Password: password



3. Go to “Status->Overview”， Check the current firmware version of the router.
   Note that the firmware version should be higher than x.2.0.6.
4. Go to “Network > Interface > Cellular > Cellular Setting” and configure the APN information.
5. Go to “Status/Cellular” to check the cellular network status, also you can use the network detective tool “Ping” under the menu “Maintenance/tools/Ping”
   For more details, you can refer to our online video tutorial from the below link
   https://www.ursalink.com/academy-ursalink-course-lesson-1

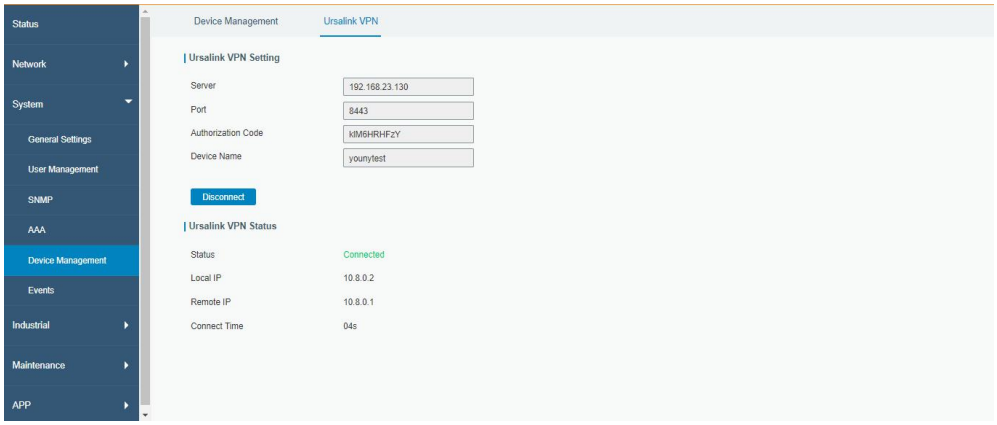
4.2.2 Router Configuration

1. Go to “System->Device Management -> UrsalinkVPN - > UrsalinkVPN Setting”. Input the IP address or Domain Name of UrsalinkVPN.



2. Input service port .
   Note that service port should be the same as the one configured on UrsalinkVPN.
3. Input the authorization code generated by UrsalinkVPN.
4. Input the device name, then click the Connect button.

5. Check the Connection Status of UrsalinkVPN, and go to “System->Device Management -> Ursalink VPN - > UrsalinkVPN Status”

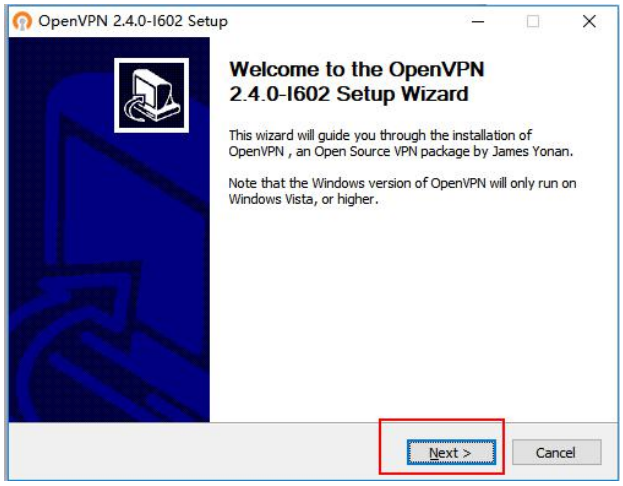


Note that time synchronization is needed between UrsalinkVPN and routers.

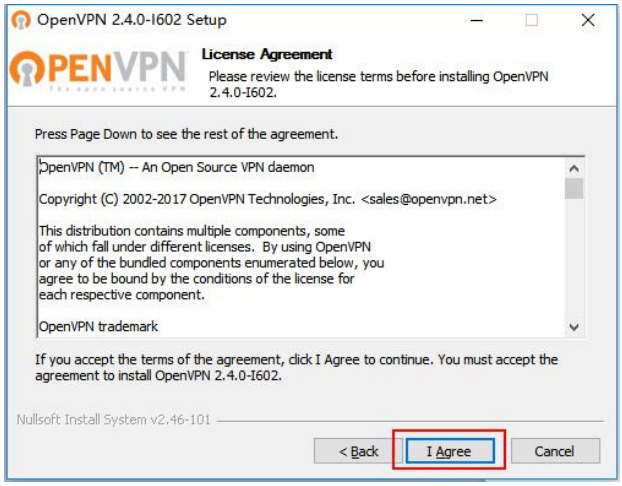
4.3 Connecting Control Station with UrsalinkVPN

4.3.1 Install OpenVPN on Windows

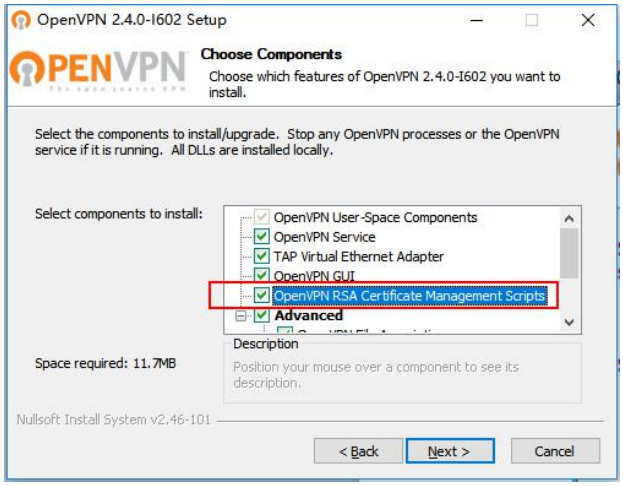
1. OpenVPN source code and Windows installers can be downloaded from the below link:
   https://openvpn.net/index.php/open-source/downloads.html



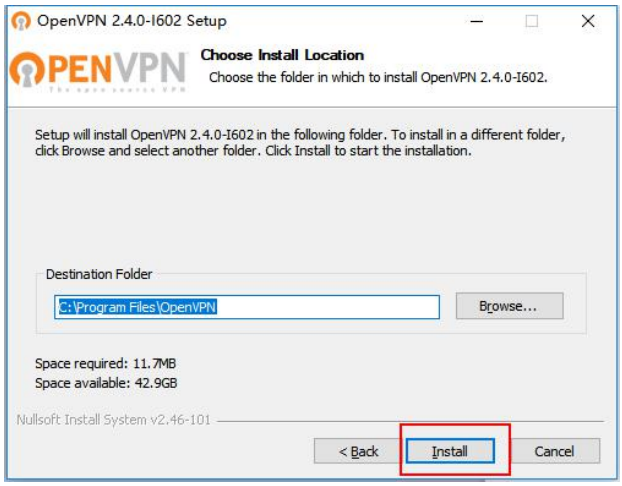
2. License Agreement.

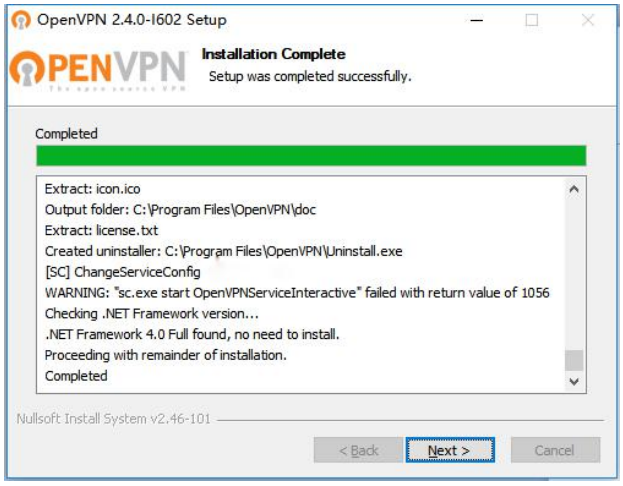


3. Make sure “OpenVPN RSA Certificate Management Scripts” has been checked.

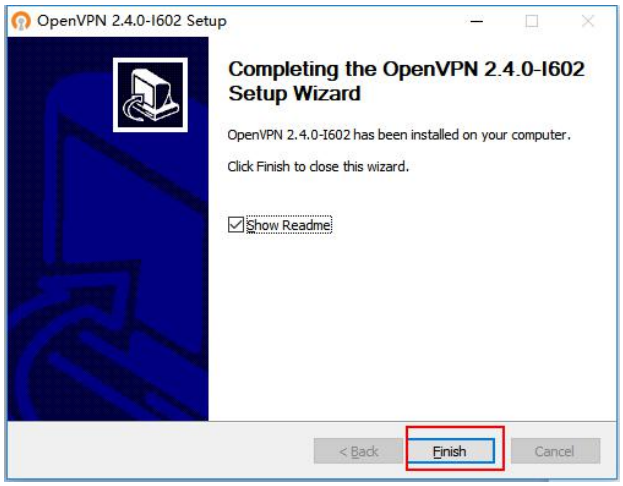


4. Choose install location and click Install. Wait for the Installation to complete.





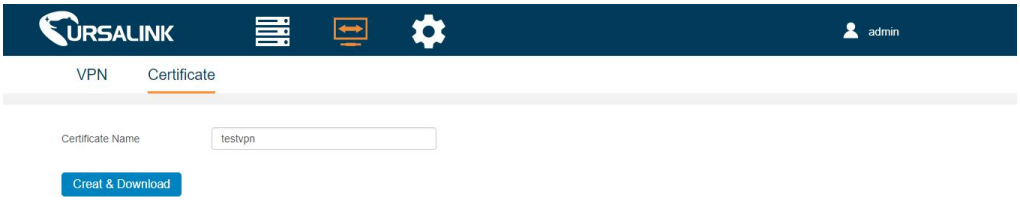
5. Click "Finish" to complete installation.



4.3.2 Generate Certificate from UrsalinkVPN

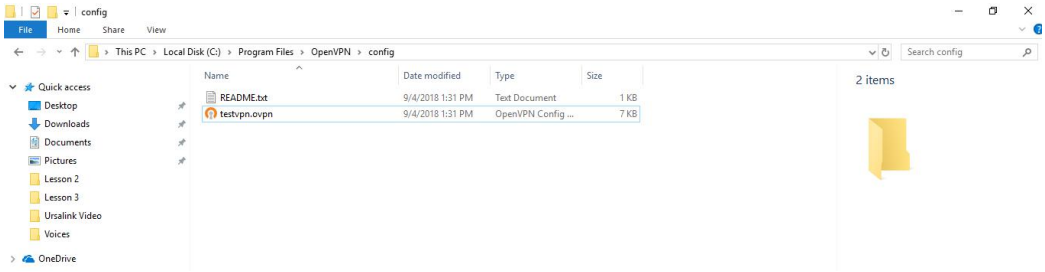
1. Log in UrsalinkVPN
2. Go to “Certificate”, input certificate name, and then click Creat & Download to Create&Download x.509 certificate.

   Note that always use a unique certificate name for each client.

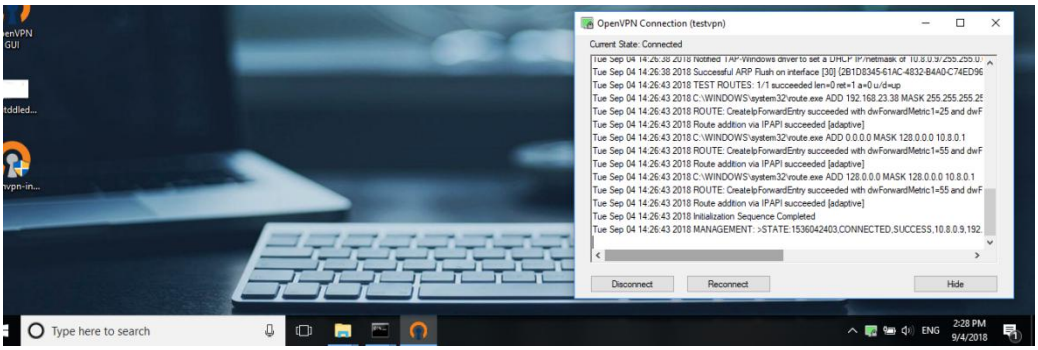


4.3.3 Running OpenVPN On Windows

1. Copy Certificate to the machine if needed and place the certificate under “OpenVPN/config” as show below.



2. Running OpenVPN



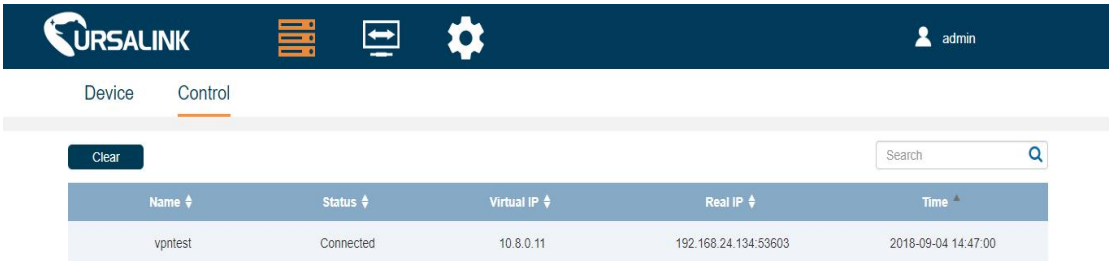
4.3.4 Communication Test

1. Router connection status

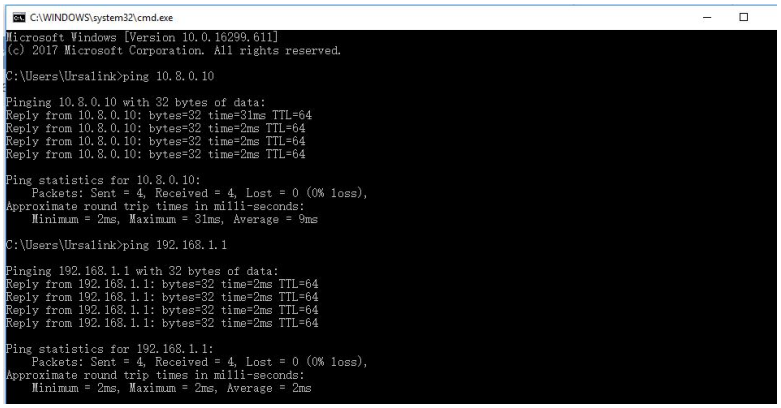
   Virtual IP : 10.8.0.10

   Subnet : 192.168.1.0

2. Control station connection status



3. Testing the communication between Control station and router


C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.611]
(c) 2017 Microsoft Corporation. All rights reserved.
C:\Users\Ursalink>ping 10.8.0.10
Pinging 10.8.0.10 with 32 bytes of data:
Reply from 10.8.0.10: bytes=32 time=31ms TTL=64
Reply from 10.8.0.10: bytes=32 time=2ms TTL=64
Reply from 10.8.0.10: bytes=32 time=2ms TTL=64
Reply from 10.8.0.10: bytes=32 time=2ms TTL=64
Ping statistics for 10.8.0.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 31ms, Average = 9ms
C:\Users\Ursalink>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 2ms, Average = 2ms

-End-