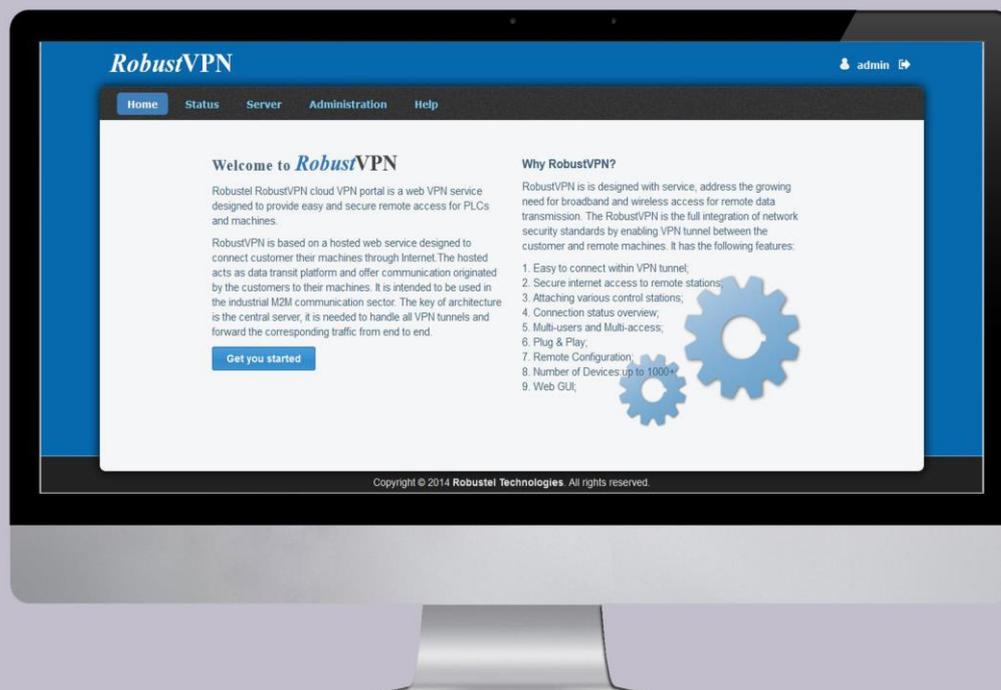


# RobustVPN Cloud VPN Portal

Easy, Secure Remote Access for PLCs and Machines

## User Guide

Document Name: **User Guide**  
Software: **1.00.00**  
Date: **2014-07-22**  
Status: **Confidential**  
Doc ID: **RT\_UG\_RobustVPN\_v.1.0.0**



# Robustel

www.robustel.com

## About This Document

This document describes the software of RobustVPN Cloud VPN Portal.

**Copyright© Guangzhou Robustel Technologies Co., Limited  
All Rights Reserved.**

## Trademarks and Permissions

Robustel are trademark of Guangzhou Robustel Technologies Co. Limited.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner. The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Robustel shall have no liability for any error or damage of any kind resulting from the use of this document.

## Technical Support Contact Information

Tel: +86-18924045664

Fax: +86-20-82321505

E-mail: [support@robustel.com](mailto:support@robustel.com)

Web: [www.robustel.com](http://www.robustel.com)

### Revision History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Release Date	RobustVPN Version	Doc Version	Details
2014-07-22	v1.00.00	v1.0.0	First release

## Contents

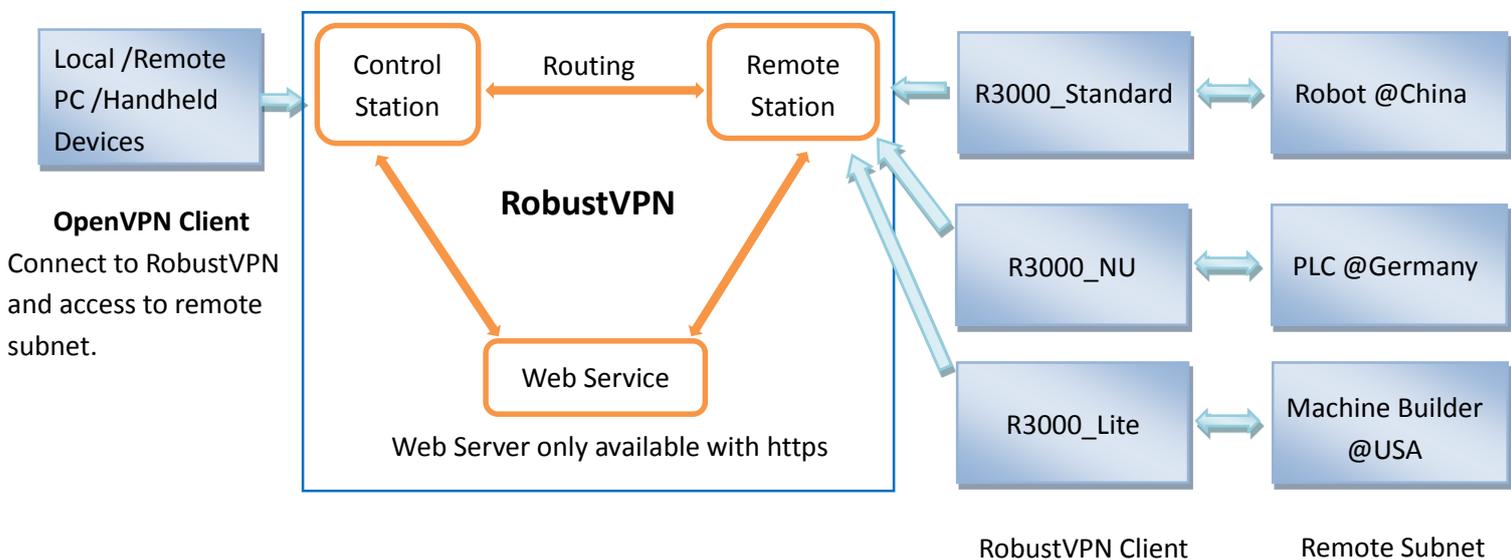
Chapter 1.	Product .....	5
1.1.	Overview .....	5
1.2.	Hardware Requirement .....	6
1.3.	Hardware Requirement .....	6
1.4.	Selection and Ordering Data .....	6
Chapter 2.	Installation and Maintain .....	7
2.1.	System requirement .....	7
2.2.	Installation steps .....	7
Chapter 3.	Configuration over web browser .....	10
3.1.	Home .....	10
3.2.	Status .....	10
3.3.	Status -> Remote Station -> Current Status .....	11
3.4.	Status -> Remote Station -> Historical Status .....	12
3.5.	Status -> Control Station -> Current Status .....	13
3.6.	Server -> Remote Station -> OpenVPN Basic .....	14
3.7.	Server ->Control Station ->OpenVPN Basic .....	16
3.8.	Server -> Control Station -> OpenVPN Certificate .....	17
3.9.	Administration -> User Management .....	18
3.10.	Administration -> Event/Log .....	19
3.11.	Administration -> Tools .....	20
3.12.	Help -> About .....	20
3.13.	Help -> Terms Of Service .....	21
3.14.	Help -> User Guide .....	22
Chapter 4.	Examples .....	23
4.1.	Application Diagram for Introduction .....	23
4.2.	Link R3000 to RobustVPN .....	23
4.2.1.	Configure Link Management .....	23
4.2.2.	Check the status of RobustVPN connection .....	25
4.3.	Settings of Control Station .....	27
4.3.1.	OpenVPN Installation on Windows .....	27
4.3.2.	Create the certificates from RobustVPN .....	30
4.3.3.	Running the OpenVPN software in Windows OS .....	31
4.3.4.	Testing from Local PC to RobustVPN Clients .....	32
Chapter 5.	Import License key of RobustVPN .....	34
5.1.	Overview of license key .....	34
5.2.	Register for RobustVPN .....	34

# Chapter 1. Product

## 1.1. Overview

RobustVPN is based on a hosted web service designed to connect customer to their machines through Internet. The hosted acts as data transit platform and offer communication originated by the customers to their machines. It is intended to be used in the industrial M2M communication sector.

The key of architecture is the central server, it is needed to handle all VPN tunnels and forward the corresponding traffic from end to end.



RobustVPN is designed with Web service, address the growing need for broadband and wireless access for remote data transmission. The RobustVPN is the full integration of network security standards by enabling VPN tunnel between the customer and remote machines.

It mainly has following features:

- Easy to connect within VPN tunnel
- Secure internet access to remote stations
- Attaching various control stations
- Connection status overview
- Multi-users and Multi-access
- Plug & Play
- Remote Configuration
- Number of Devices: up to 1000+
- Web GUI

## 1.2. Hardware Requirement

- Pentium IV or above
- 1 GHz CPU (1.5 GHz recommended)
- 1 GB RAM (2 GB recommended)
- 1 GB free disk space

## 1.3. Hardware Requirement

- O/S: Centos 6.x
- Installation Package
- Browser: IE 8.0 or above, Chrome, Firefox

## 1.4. Selection and Ordering Data

Please refer to corresponding RobusVPN datasheet.

## Chapter 2. Installation and Maintain

### 2.1. System requirement

O/S: Centos 6.x (32/64bit) or above.

### 2.2. Installation steps

1. Download RobustVPN-1.0.x-i686.install.
2. Place the **RobustVPN-1.0.x-i686.install** to Linux's any folder, e.g. "cd /tmp".

```
[root@localhost Rlink_linux32_64]# cp RobustVPN-1.0.1-i686.install /tmp
[root@localhost Rlink_linux32_64]# cd /tmp
[root@localhost tmp]# ls
keyring-HuTKQg pulse-eOXl5Czg4nje virtual-root.67jNTV virtual-root.ig88
orbit-gdm pulse-yqX6n6UKmqm0 virtual-root.AhBW7G virtual-root.pQiz
orbit-root RobustVPN-1.0.1-i686.install virtual-root.FcU5rF virtual-root.PrTo
```

3. Install the RobustVPN as root, using the following command.  
e.g. `[root@localhost tmp]# ./RobustVPN-1.0.x-i686.install -i`

```
[root@localhost tmp]# ./RobustVPN-1.0.1-i686.install -i
RobustVPN: Starting to install...
RobustVPN: Installing RobustVPN applications.....
RobustVPN: Starting to create certs for remote station: [ OK ]
RobustVPN: Starting to create certs for control station: [ OK ]
RobustVPN: Unable to get public ip, replaced by eth0: [ OK ]
RobustVPN: Starting to install database for RobustVPN: [ OK ]
RobustVPN: Starting to register system services: [ OK ]
iptables: saving firewall rules to /etc/sysconfig/iptables: [ OK ]
iptables: Flushing firewall rules: [ OK ]
iptables: setting chains to policy ACCEPT: filter [ OK ]
iptables: unloading modules: [ OK ]
iptables: Applying firewall rules: [ OK ]
RobustVPN: service iptables reload rules[-I]: [ OK ]
RobustVPN: Preparing to start RobustVPN web|openvpn process...
Starting RobustVPN for Linux 1.0.1...
RobustVPN: Starting OpenVPN for remote station: [ OK ]
RobustVPN: Starting OpenVPN for control station: [ OK ]
RobustVPN: Starting httpd: [ OK ]
RobustVPN for Linux started.
RobustVPN: Generate config for remote station: [ OK ]
RobustVPN: Generate config for control station: [ OK ]
[root@localhost tmp]#
```

4. Open the browser, such as Opera, Google Chrome or Firefox --> enter **https://IP address or Domain Name of server**.

E.g. `https://172.16.1.123`



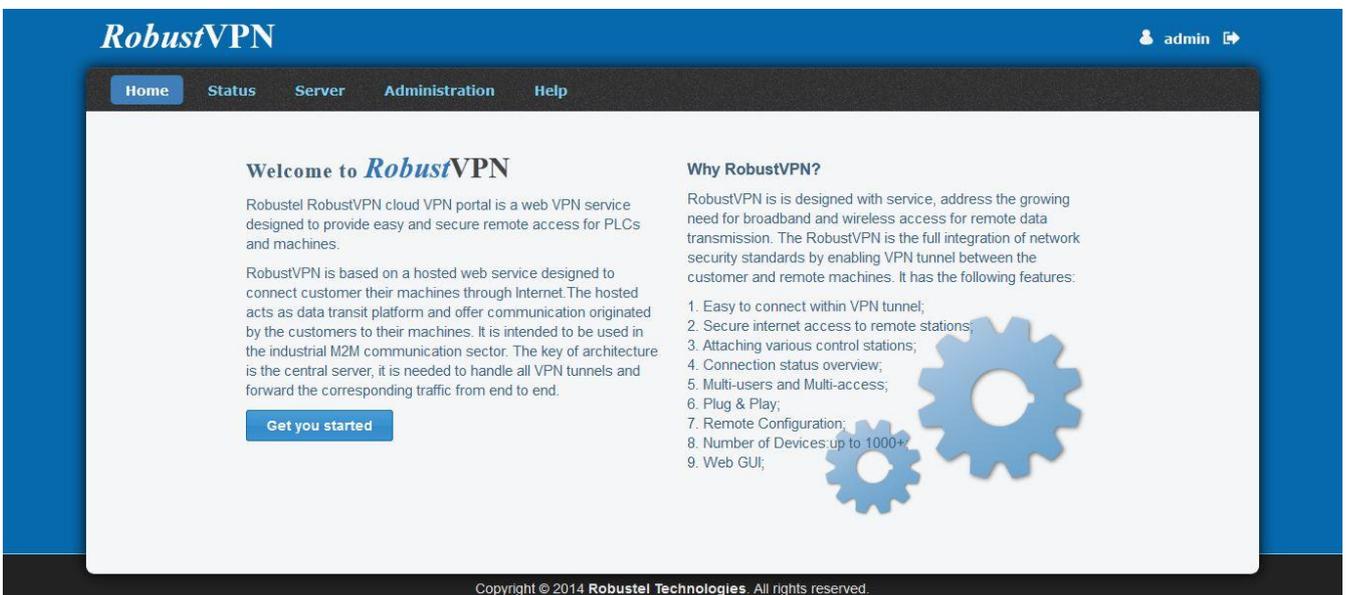
5. Enter Username & Password as **admin/admin** in the new page to enter index page. Now the RobustVPN is

installed in your Linux OS.

*Note: admin/admin is the default Username & Password for log in.*



6. After successfully login, you can see Website of RobustVPN.



7. Uninstall the **RobustVPN-1.0.x-i686.install**.

*e.g. [root@localhost tmp]# ./RobustVPN-1.0.x-i686.install -e*

```
[root@localhost tmp]# ./RobustVPN-1.0.1-i686.install -e
RobustVPN: Stopping RobustVPN process...
Stopping RobustVPN for Linux 1.0.1...
RobustVPN: Stopping OpenVPN for remote station: [ OK ]
RobustVPN: Stopping OpenVPN for control station [ OK ]
RobustVPN: Stopping httpd: [ OK ]
RobustVPN for Linux stopped.
RobustVPN: Starting to uninstall...
RobustVPN: Remove installed files: [ OK ]
RobustVPN: Remove system service: [ OK ]
iptables: Saving firewall rules to /etc/sysconfig/iptables: [ OK ]
iptables: Flushing firewall rules: [ OK ]
iptables: Setting chains to policy ACCEPT: filter [ OK ]
iptables: unloading modules: [ OK ]
iptables: Applying firewall rules: [ OK ]
RobustVPN: service iptables reload rules[-D]: [ OK ]
[root@localhost tmp]#
```

**Note:** All the RobustVPN data or services would be unavailable after software uninstallation.

8. Start/Stop RobustVPN services.

```
service RobustVPN start //Start all the services
service RobustVPN starthttpd //Start httpd web server
service RobustVPN startvpnremote //Start remote station
service RobustVPN startvpncontrol //Start control station

service RobustVPN restart //Restart all the services
service RobustVPN restarthttpd //Restart httpd web server
service RobustVPN restartvpnremote //Restart remote station
service RobustVPN restartvpncontrol //Restart control station

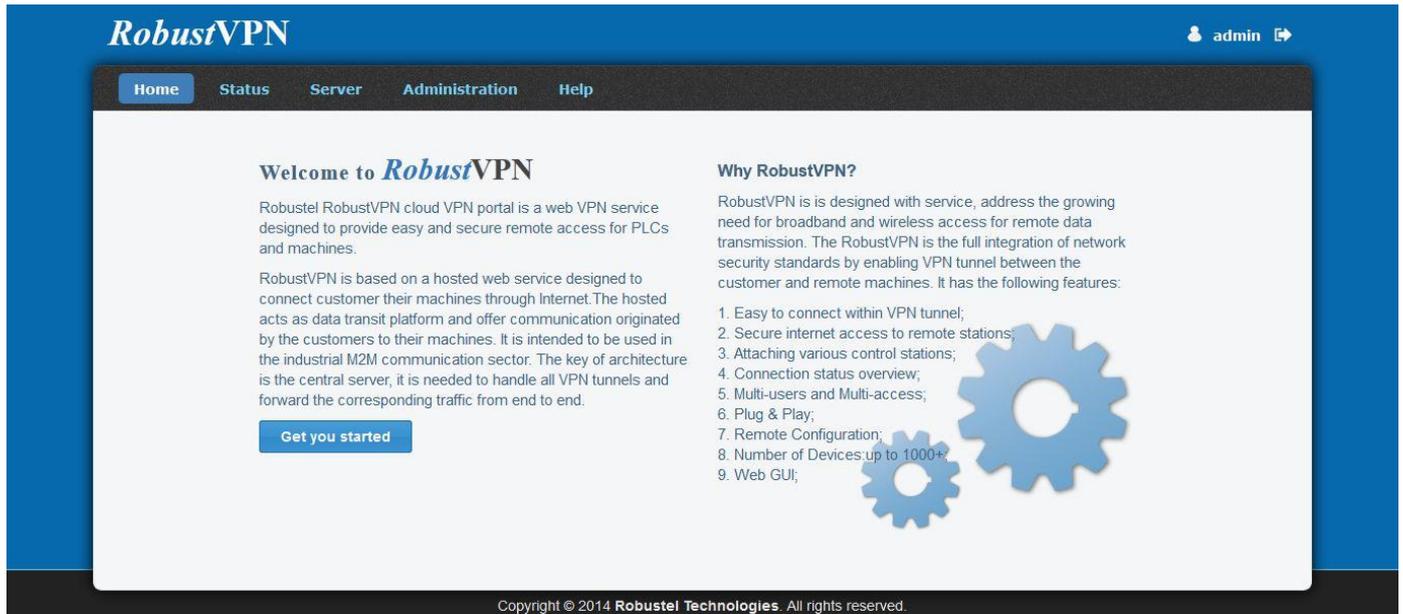
service RobustVPN stop //Stop all the services
service RobustVPN stophttpd //Stop httpd web server
service RobustVPN stopvpnremote //Stop remote station
service RobustVPN stopvpncontrol //Stop control station

service RobustVPN status //Check the status of RobustVPN
```

## Chapter 3. Configuration over web browser

### 3.1. Home

User can click “” to logout web browser of RobustVPN.



**RobustVPN** admin 

Home Status Server Administration Help

### Welcome to *RobustVPN*

Robustel RobustVPN cloud VPN portal is a web VPN service designed to provide easy and secure remote access for PLCs and machines.

RobustVPN is based on a hosted web service designed to connect customer their machines through Internet. The hosted acts as data transit platform and offer communication originated by the customers to their machines. It is intended to be used in the industrial M2M communication sector. The key of architecture is the central server, it is needed to handle all VPN tunnels and forward the corresponding traffic from end to end.

[Get you started](#)

### Why RobustVPN?

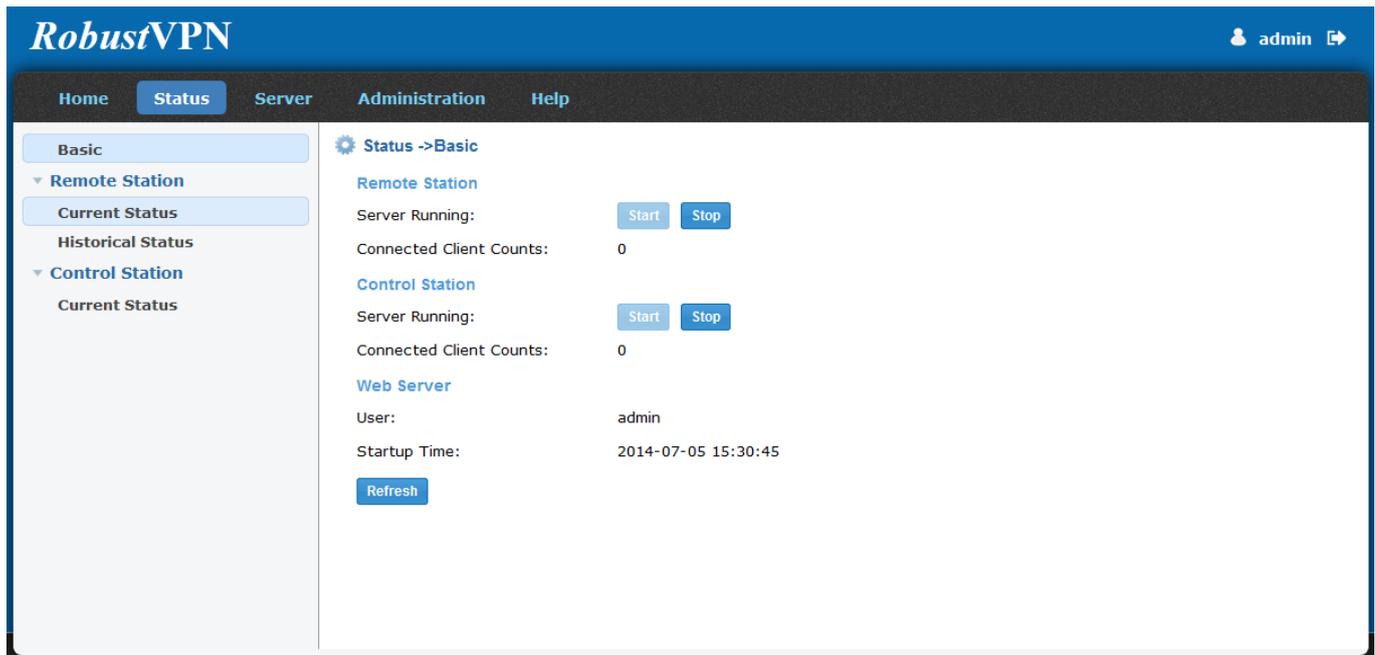
RobustVPN is designed with service, address the growing need for broadband and wireless access for remote data transmission. The RobustVPN is the full integration of network security standards by enabling VPN tunnel between the customer and remote machines. It has the following features:

1. Easy to connect within VPN tunnel;
2. Secure internet access to remote stations;
3. Attaching various control stations;
4. Connection status overview;
5. Multi-users and Multi-access;
6. Plug & Play;
7. Remote Configuration;
8. Number of Devices: up to 1000+;
9. Web GUI;

Copyright © 2014 Robustel Technologies. All rights reserved.

### 3.2. Status

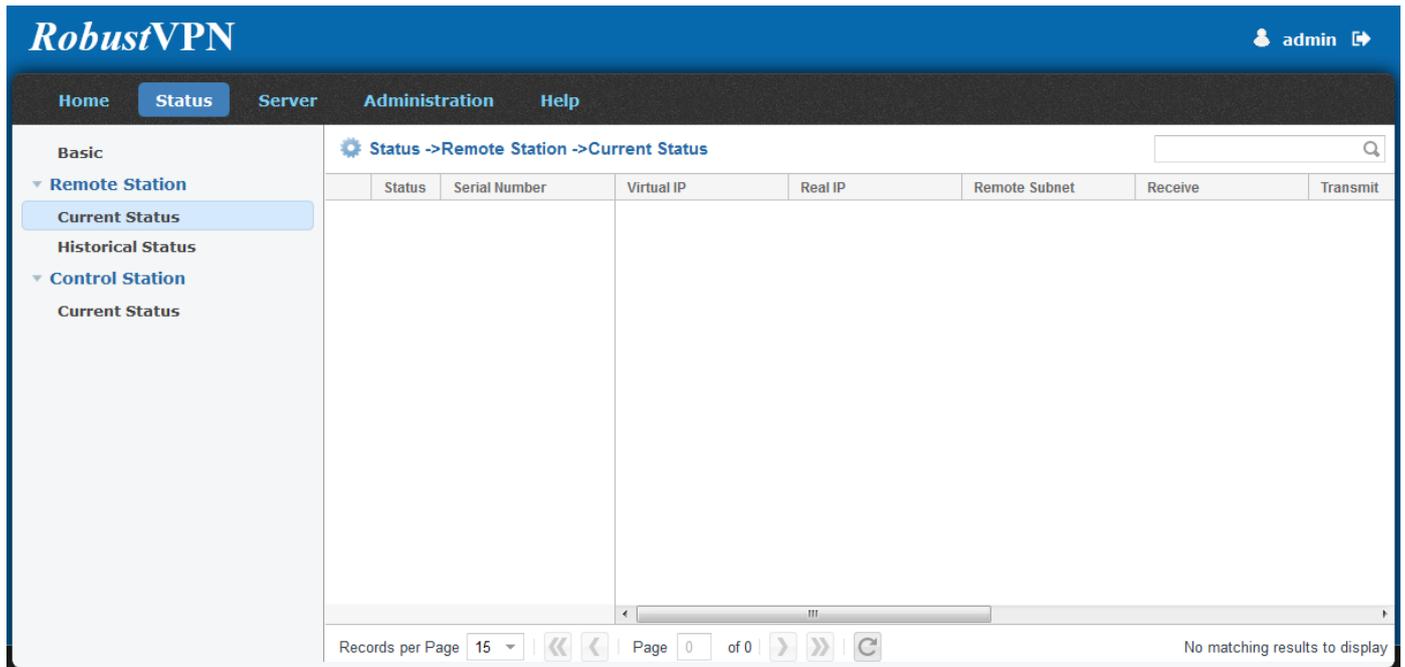
This section shows basic status of RobustVPN.



Status->Basic	
Item	Description
Start @Remote Station	Start the OpenVPN server of Remote Station.
Stop @Remote Station	Stop the OpenVPN server of Remote Station.
Connected Client Counts @Remote Station	The number of online remote routers.
Start @Control Station	Start the OpenVPN server of Control Station.
Stop @Control Station	Stop the OpenVPN server of Control Station.
Connected Client Counts @Control Station	The number of online OpenVPN client.
User	The logon name of current user.
Startup Time	The startup time of RobustVPN services.
Refresh	The button of refresh web page.

### 3.3. Status -> Remote Station -> Current Status

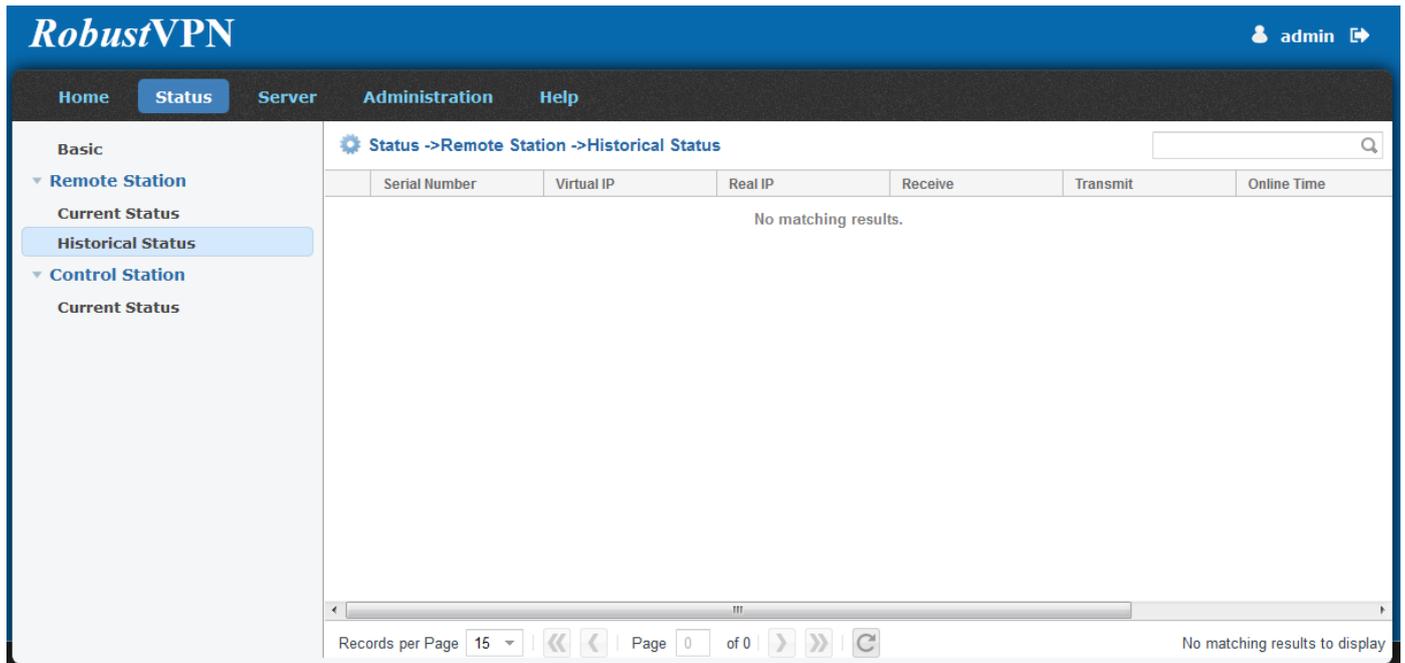
This section shows the connected status of Remote Station.



Status->Remote Station->Current Status		
Item	Description	Default
Search	User can enter characters to search specific information.	Null
Status	The status of connection.	Null
Serial Number	The serial number of routers.	Null
Virtual IP	The virtual IP address of OpenVPN subnet.	Null
Real IP	The IP address of router's WAN interface.	Null
Remote Subnet	The remote subnet of routers.	Null
Receive	The data statistics of receipt.	Null
Transmit	The data statistics of Transmission.	Null
Online Time	The online time of each connection.	Null
Description	The description of each remote router.	Null
Records per Page	Selected from "10", "20", "25", "50", user can set how many devices are wanted to show in one page.	15

### 3.4. Status -> Remote Station -> Historical Status

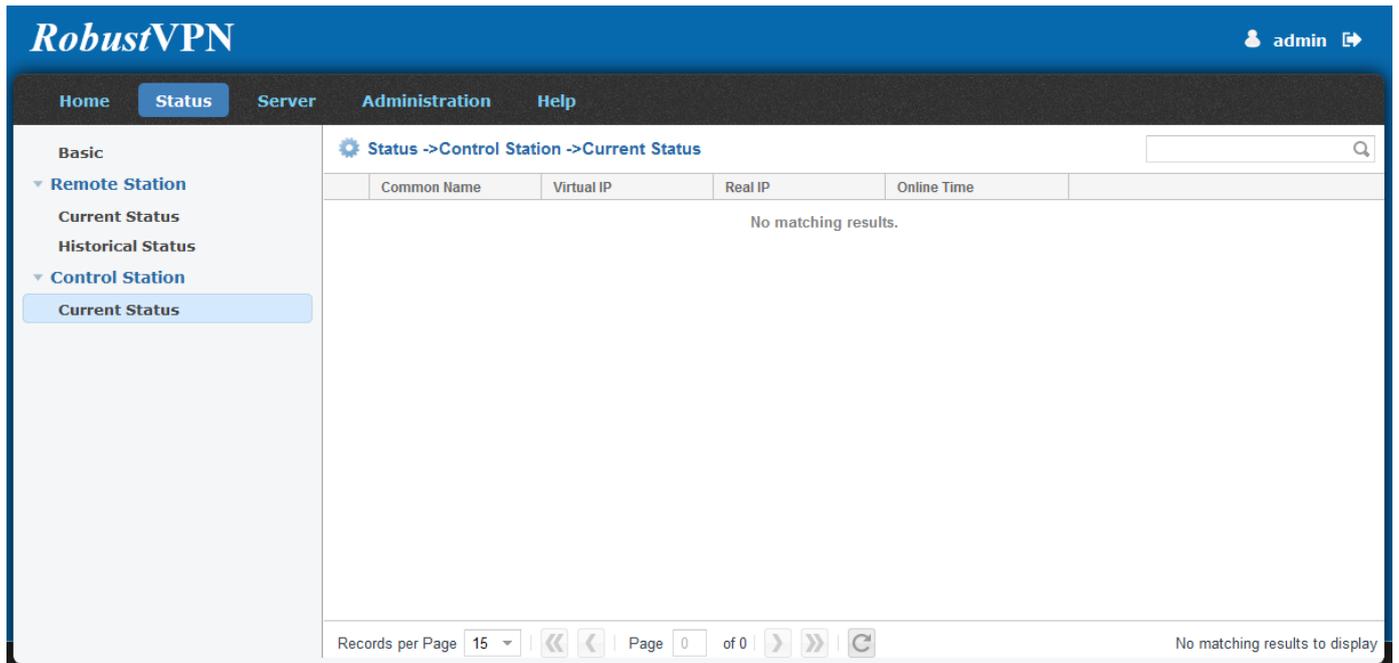
This section shows the historical connected status of Remote Station.



Status->Remote Station->Historical Status		
Item	Description	Default
Search	User can enter characters to search specific information.	Null
Serial Number	The serial number of routers.	Null
Virtual IP	The virtual IP address of OpenVPN subnet.	Null
Real IP	The IP address of router's WAN interface.	Null
Receive	The data statistics of receipt.	Null
Transmit	The data statistics of Transmission.	Null
Online Time	The online time of each connection.	Null
Offline Time	The offline time of each connection.	Null
Records per Page	Selected from "10", "20", "25", "50", user can set how many devices are wanted to show in one page.	15

### 3.5. Status -> Control Station -> Current Status

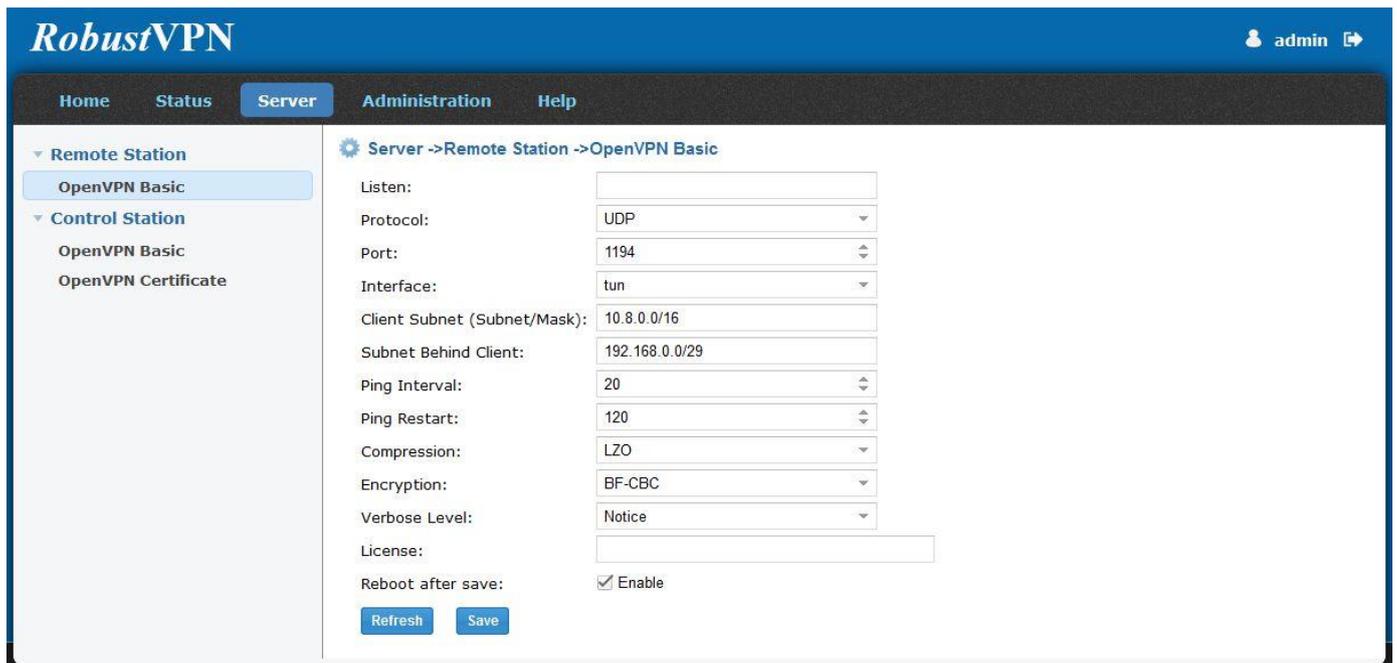
This section shows the connected status of Control Station.



Status->Control Station->Current Status		
Item	Description	Default
Search	User can enter characters to search specific information.	Null
Common Name	The common name of OpenVPN certificates.	Null
Virtual IP	The virtual IP address of OpenVPN subnet.	Null
Real IP	The IP address of control station.	Null
Online Time	The online time of each connection.	Null
Records per Page	Selected from "10", "20", "25", "50", user can set how many devices are wanted to show in one page.	15

### 3.6. Server -> Remote Station -> OpenVPN Basic

This section shows the OpenVPN settings of Remote Station.

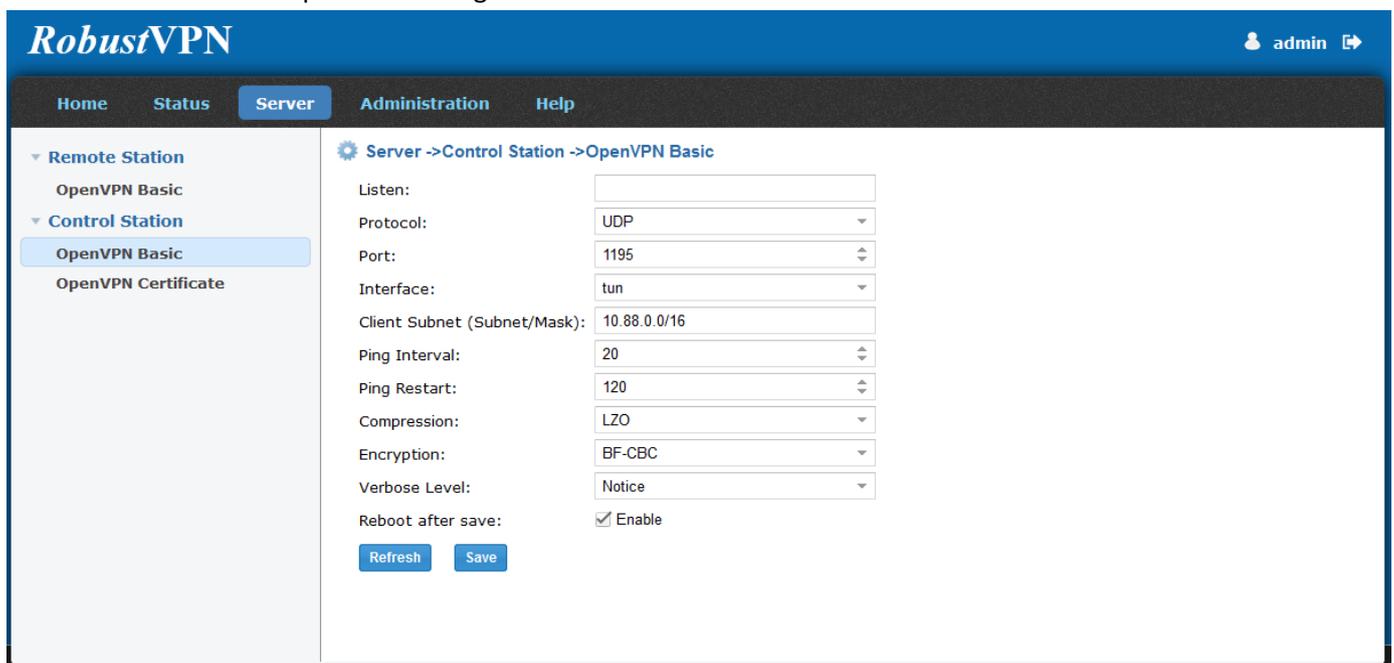


Status->Control Station->Current Status		
Item	Description	Default
Listen IP	You can enter the IP address of cellular WAN, Ethernet WAN or Ethernet LAN. Null stands for using the active WAN link currently-cellular WAN or Ethernet WAN.	Null
Protocol	Select from "UDP" and "TCP" which depends on the application.	UDP
Port	Set the local listening port.	1194
Interface	Only support "tun" type of device interface for OpenVPN.	tun
Client Subnet	Define the IP pool of OpenVPN tunnel.	10.8.0.0/16
Subnet Behind Client	Define the IP pool of R3000's DHCP server. <i>Note: After R3000 connect to RobustVPN, RobustVPN server will push the subnet to R3000. And R3000 will modify its DHCP settings and restart again.</i>	192.168.0.0/29
Ping Interval	Set ping interval to check if the tunnel is active.	20
Ping -Restart	Restart to establish the OpenVPN tunnel if ping always timeout during this time.	120
Compression	Select from "None" and "LZO", Select "LZO" to use the LZO compression library to compress the data stream.	LZO
Encryption	Select from "BF-CBC", "DES-CBC", "DES-EDE3-CBC", "AES128-CBC", "AES192-CBC" and "AES256-CBC". BF-CBC: Uses the BF algorithm in CBC mode and 128-bit key. DES-CBC: Uses the DES algorithm in CBC mode and 64-bit key. DES-EDE3-CBC: Uses the 3DES algorithm in CBC mode and 192-bit key. AES128-CBC: Uses the AES algorithm in CBC mode and 128-bit key. AES192-CBC: Uses the AES algorithm in CBC mode and 192-bit key. AES256-CBC: Uses the AES algorithm in CBC mode and 256-bit key.	BF-CBC
Verbose Level	Select the log output level which from low to high: "ERR", "WARNING",	Notice

	“NOTICE” and “DEBUG”. The DEBUG level will output more log information.	
License	The License key for paid version of RobustVPN.	Null
Reboot after save	Restart all the services of RobustVPN after modified.	Enable
Refresh	Refresh the website of RobustVPN.	Null
Save	Save the modification of RobustVPN.	Null

### 3.7. Server ->Control Station ->OpenVPN Basic

This section shows the OpenVPN settings of Control Station.

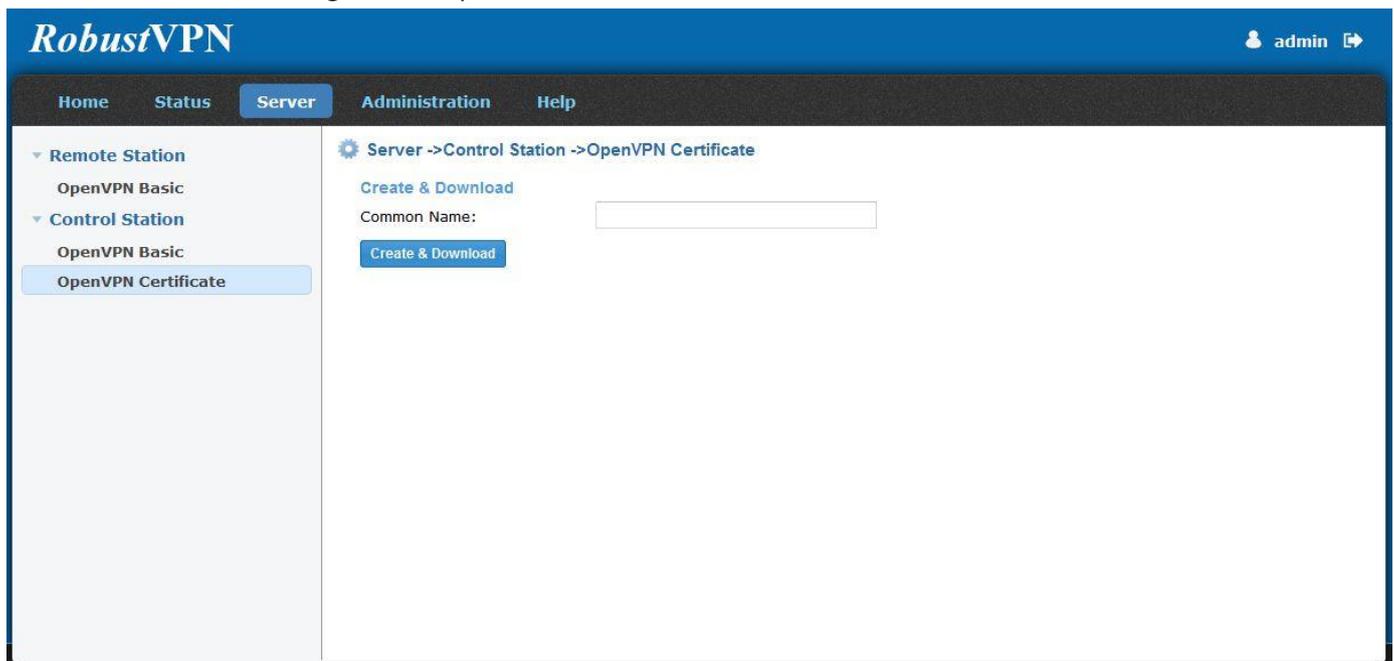


Status->Control Station->Current Status		
Item	Description	Default
Listen IP	You can enter the IP address of current WAN interface, Null means server listen all the interface of RobustVPN.	Null
Protocol	Select from “UDP” and “TCP” which depends on the application.	UDP
Port	Set the local listening port.	1195
Interface	Only support “tun” type of device interface for OpenVPN.	tun
Client Subnet	Define the IP pool of OpenVPN tunnel.	10.88.0.0/16
Ping Interval	Set ping interval to check if the tunnel is active.	20
Ping -Restart	Restart to establish the OpenVPN tunnel if ping always timeout during this time.	120
Compression	Select from “None”and”LZO”, Select “LZO” to use the LZO compression library to compress the data stream.	LZO
Encryption	Select from “BF-CBC”, “DES-CBC”, “DES-EDE3-CBC”, “AES128-CBC”, “AES192-CBC” and “AES256-CBC”.	BF-CBC

	BF-CBC: Uses the BF algorithm in CBC mode and 128-bit key. DES-CBC: Uses the DES algorithm in CBC mode and 64-bit key. DES-EDE3-CBC: Uses the 3DES algorithm in CBC mode and 192-bit key. AES128-CBC: Uses the AES algorithm in CBC mode and 128-bit key. AES192-CBC: Uses the AES algorithm in CBC mode and 192-bit key. AES256-CBC: Uses the AES algorithm in CBC mode and 256-bit key.	
Verbose Level	Select the log output level which from low to high: "ERR", "WARNING", "NOTICE" and "DEBUG". The DEBUG level will output more log information.	NOTICE
Reboot after save	Restart all the services of RobustVPN after modified.	Enable
Refresh	Refresh the website of RobustVPN.	Null
Save	Save the modification of RobustVPN.	Null

### 3.8. Server -> Control Station -> OpenVPN Certificate

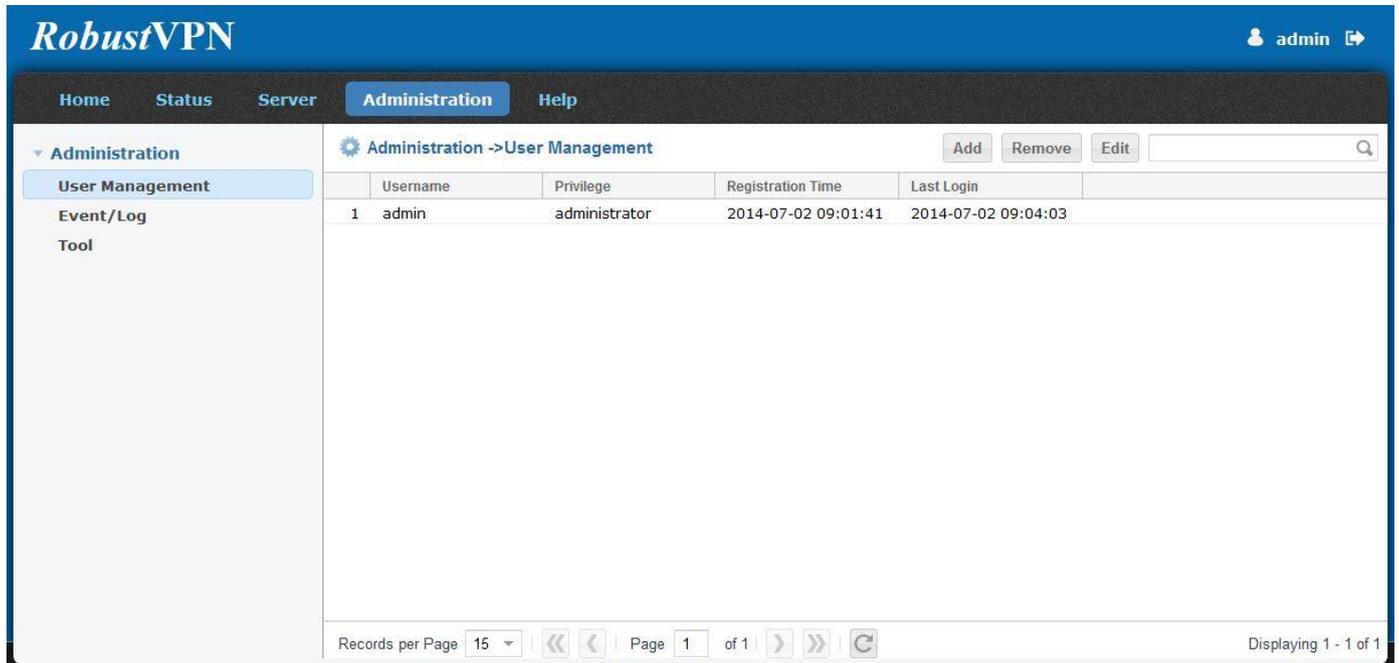
This section shows how to generate OpenVPN Certificate of Control Station.



Status->Control Station->Current Status		
Item	Description	Default
Common Name	The common name of x.509 certificates.	Null
Create & Download	Create the x.509 certificate for control station and download from RobustVPN.	Null

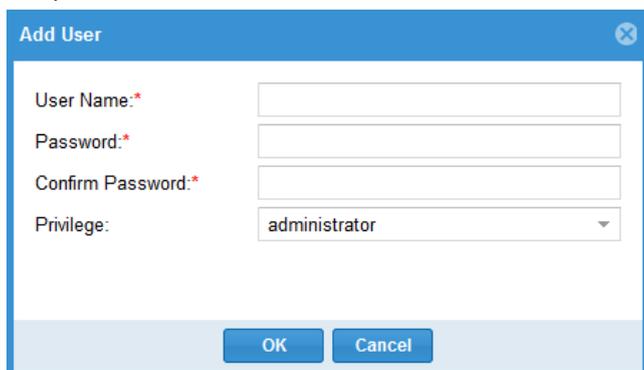
### 3.9. Administration -> User Management

This section allows user to add, remove or edit the list of user account.



Administration->User Management		
Item	Description	Default
Add	Click this button to add a new account.	Null
Remove	Click this button to delete the selected account.	Null
Edit	Click this button to edit a new account.	Null
Search	User can enter characters to search specific information.	Null
Username	The username of current account.	Null
Privilege	The privilege of current account.	Null
Registration Time	The registration of current account.	Null
Last Login	The last login time of current account.	Null
Records per Page	Selected from "10", "20", "25", "50", user can set how many devices are wanted to show in one page.	15

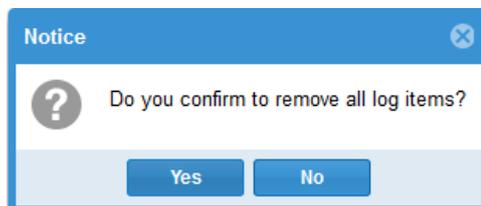
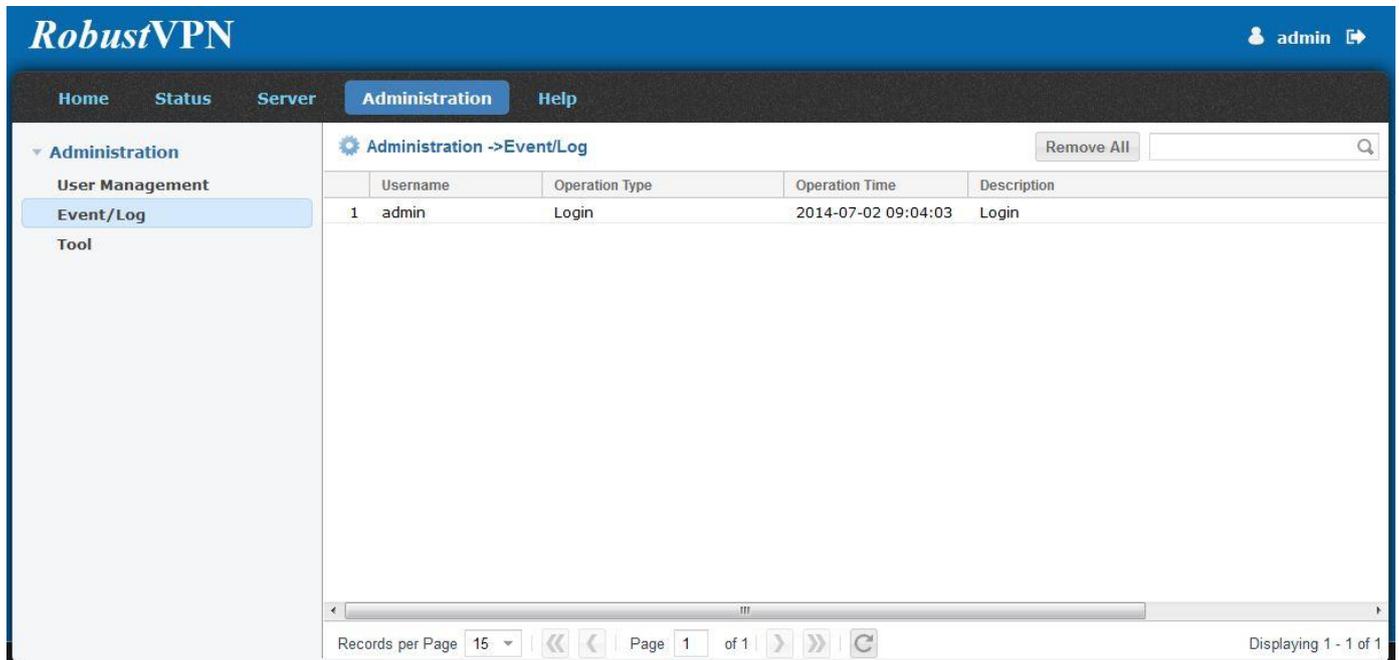
Add/Edit User account on new window.



Administration->User Management->Add/Edit		
Item	Description	Default
User Name	The username of new account.	Null
Password	Set password of new account.	Null
Confirm Password	Confirm password of new account.	Null
Privilege	There are three access level of privilege: "administrator", "user" and "readonly".	administrator

### 3.10. Administration -> Event/Log

This section allows user to check the system log.

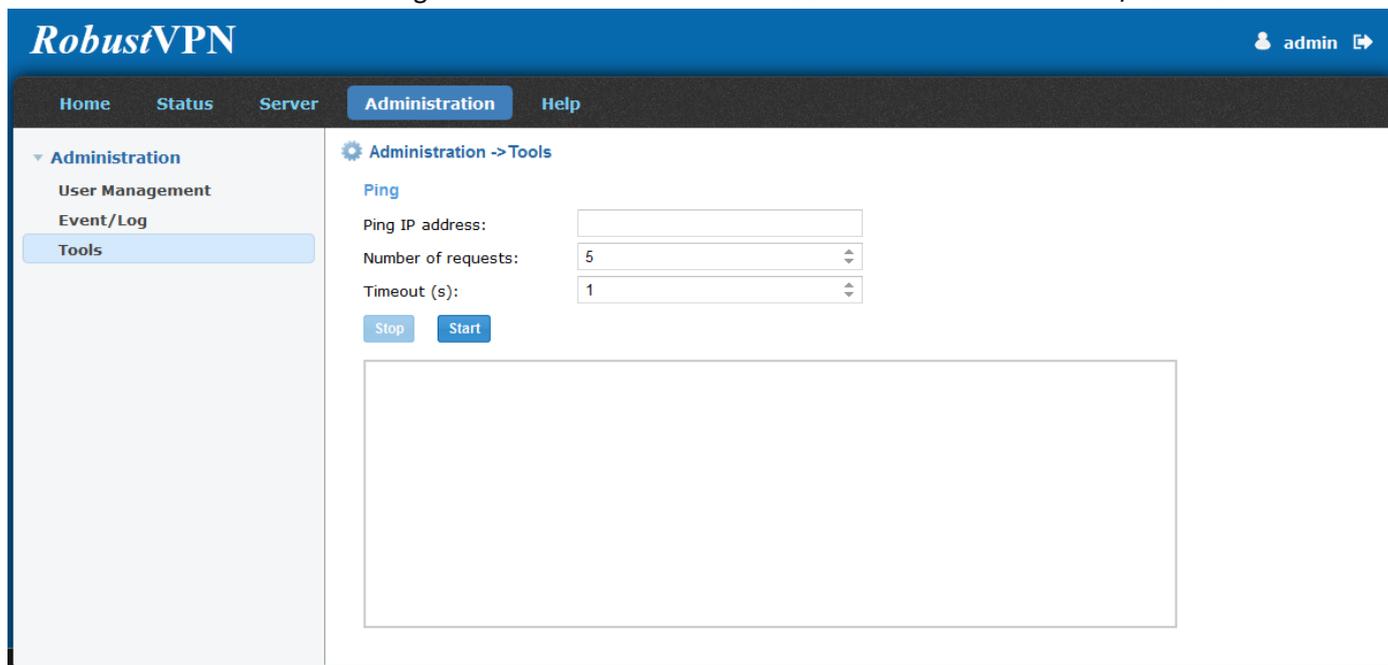


Administration->Event/Log		
Item	Description	Default
Remove All	Remove all log items.	Null
Search	User can enter characters to search specific information.	Null
Username	The username of current account.	Null
Operation Type	The type of operation with current account.	Null
Operation Time	The time of operation.	Null
Description	The description of operation.	Null

Records per Page	Selected from "10", "20", "25", "50", user can set how many devices are wanted to show in one page.	15
------------------	---	----

### 3.11. Administration -> Tools

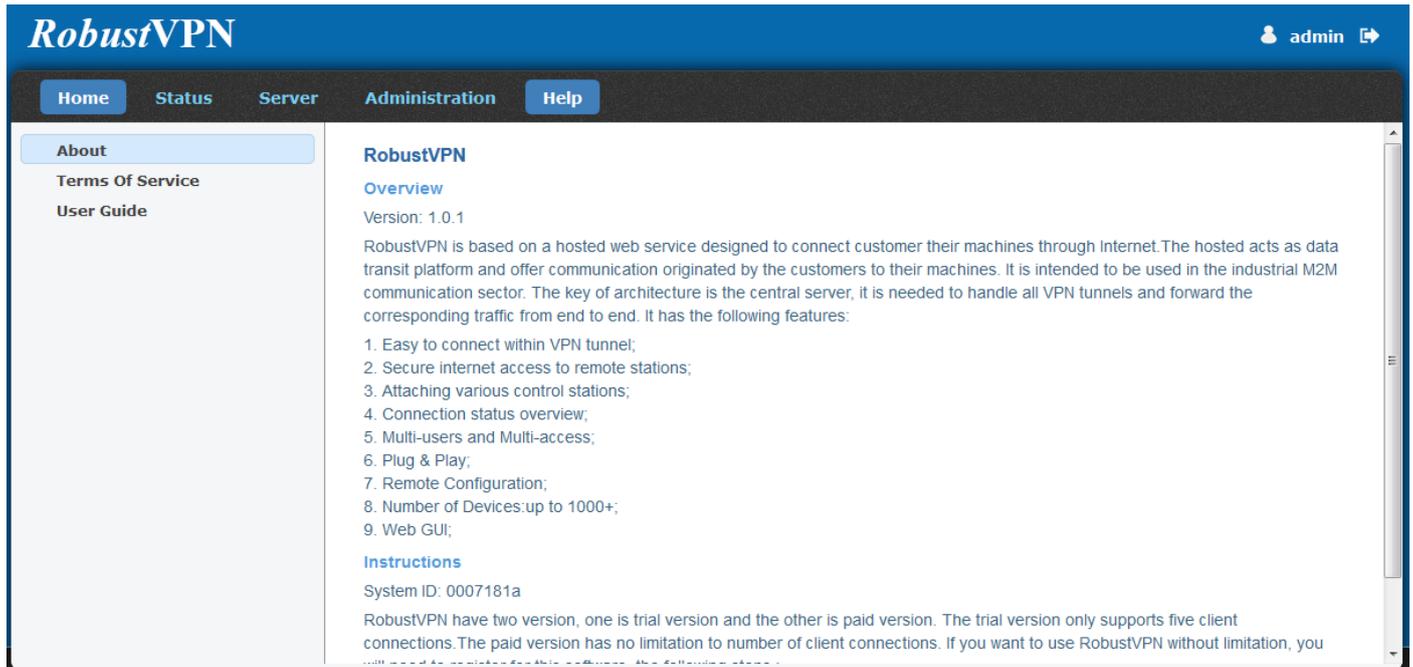
This section shows how to use Ping to check the connection between RobustVPN and Control/Remote stations.



Administration->Tools		
Item	Description	Default
Ping IP address	Enter the ping destination IP address or domain name.	Null
Number of requests	Specify the number of ping requests.	5
Timeout(s)	Specify timeout of ping request.	1
Stop	Click this button to stop ping request.	Null
Start	Click this button to start ping request, and the log will be displayed in the follow box.	Null

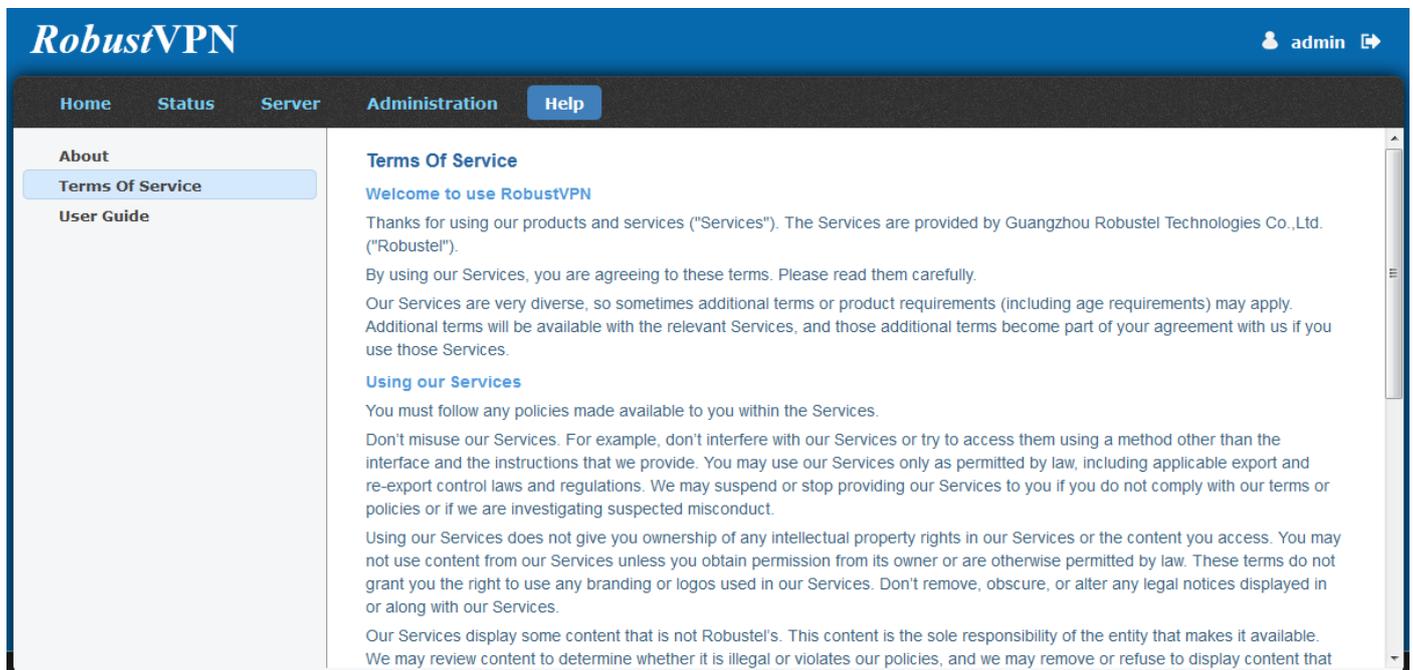
### 3.12. Help -> About

This section shows the information of RobutVPN.



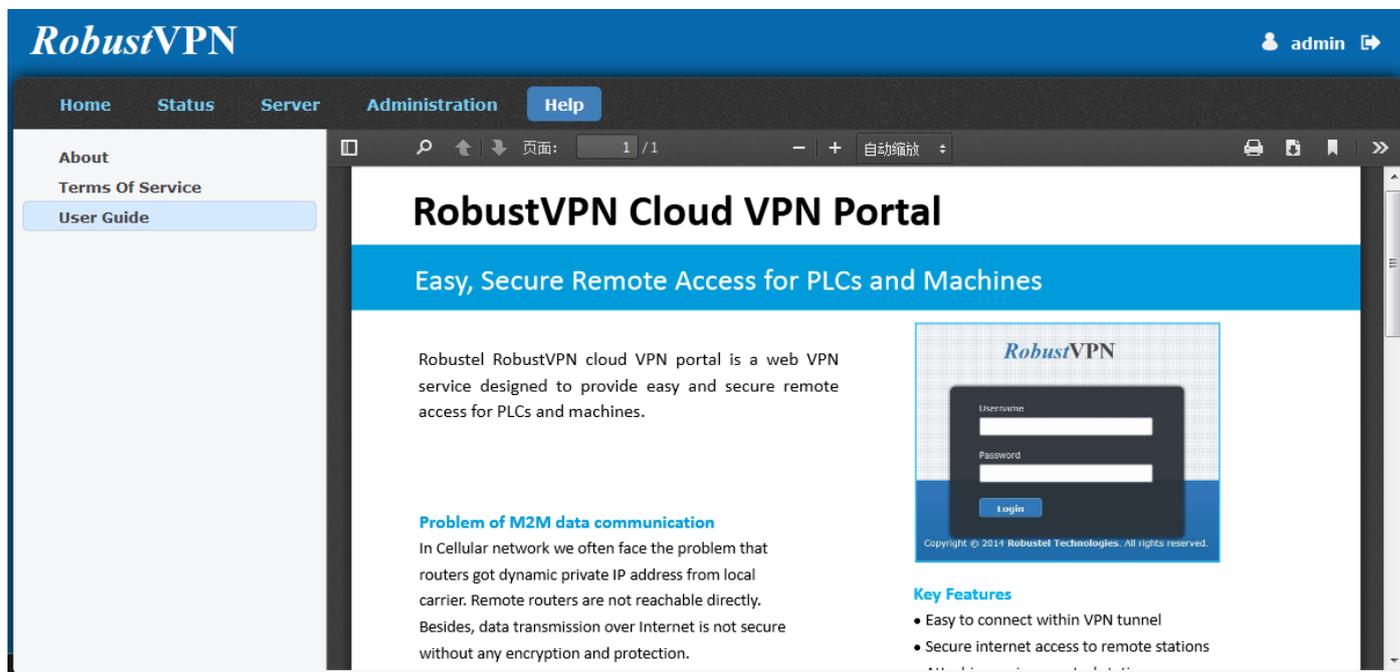
### 3.13. Help -> Terms Of Service

This section shows terms of services.



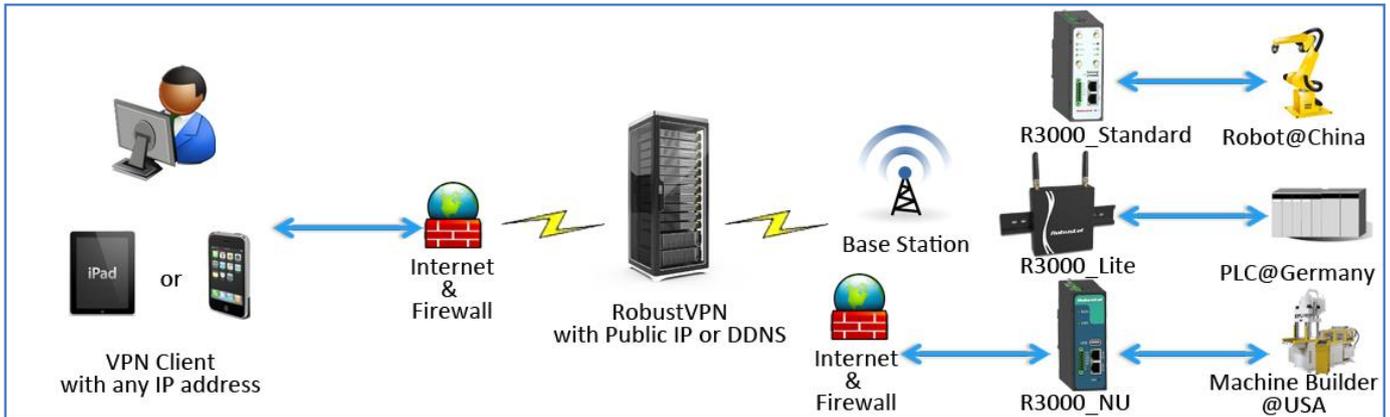
### 3.14. Help -> User Guide

This section shows the User Guide of RobustVPN.



# Chapter 4. Examples

## 4.1. Application Diagram for Introduction



1. R3000\_Standard/Lite/NU works as RobustVPN Client with any IP which can access to Internet.
2. RobustVPN works as Central VPN Server with fixed public IP or dynamic IP with domain name.
3. For Control Station site, PC or other devices which support OpenVPN client, that establish OpenVPN connection to RobustVPN and access the subnet behind R3000s via tunnel.

## 4.2. Link R3000 to RobustVPN

### 4.2.1. Configure Link Management

1. Install antenna, insert two SIM cards to R3000 -> power on R3000 and login R3000's Web GUI page.

User authentication required. Login please.

Username:

Password:

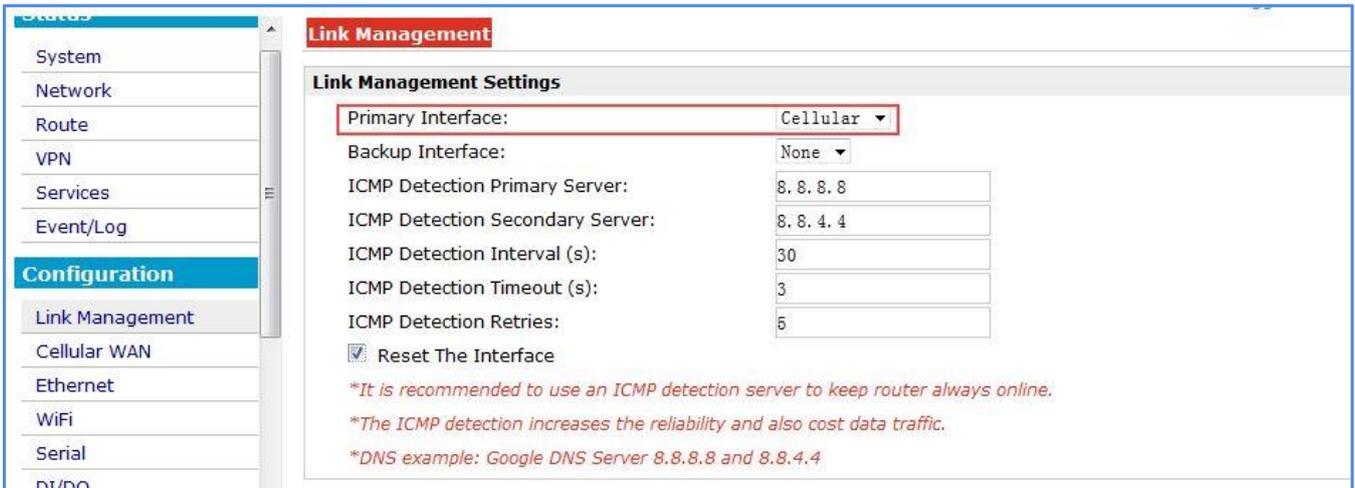
Language:  ▼

Please enter your login username and password.

2. Please check the firmware version is v1.01.16 or above. RobustVPN is available in newer firmware.

Router Information	
Device Model:	R3000-4L
Serial Number:	00300513100056
Device Name:	Cellular Router
Firmware Version:	1.01.16
Hardware Version:	1.01.02
Kernel Version:	2.6.39-6
Radio Module Type:	MC7710

3. Browse to “Configuration”-> “Link Management”.



4. Browse to “Configuration”-> “Cellular WAN”-> “ISP Profile”.

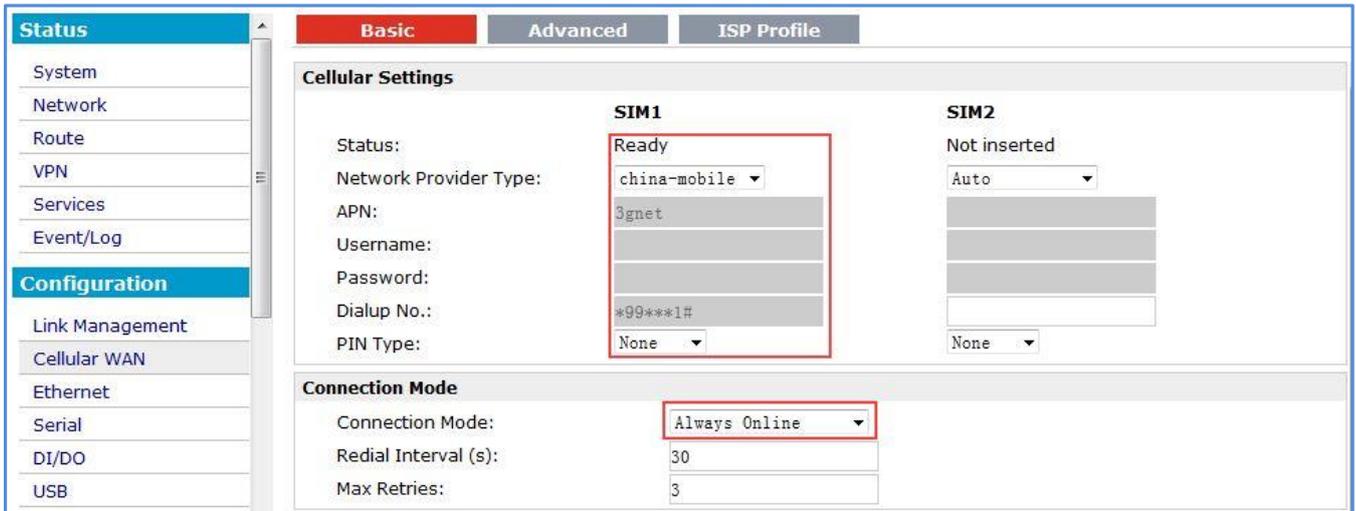
- Click “Add” to enter the APN (Access Point Name) and Dialup No. for each ISP.
- If required please enter Username and Password in the appropriate fields.
- Click “Apply”.

Note: Usually APN, Username, Password and Dialup No. are provided by ISP accordingly.



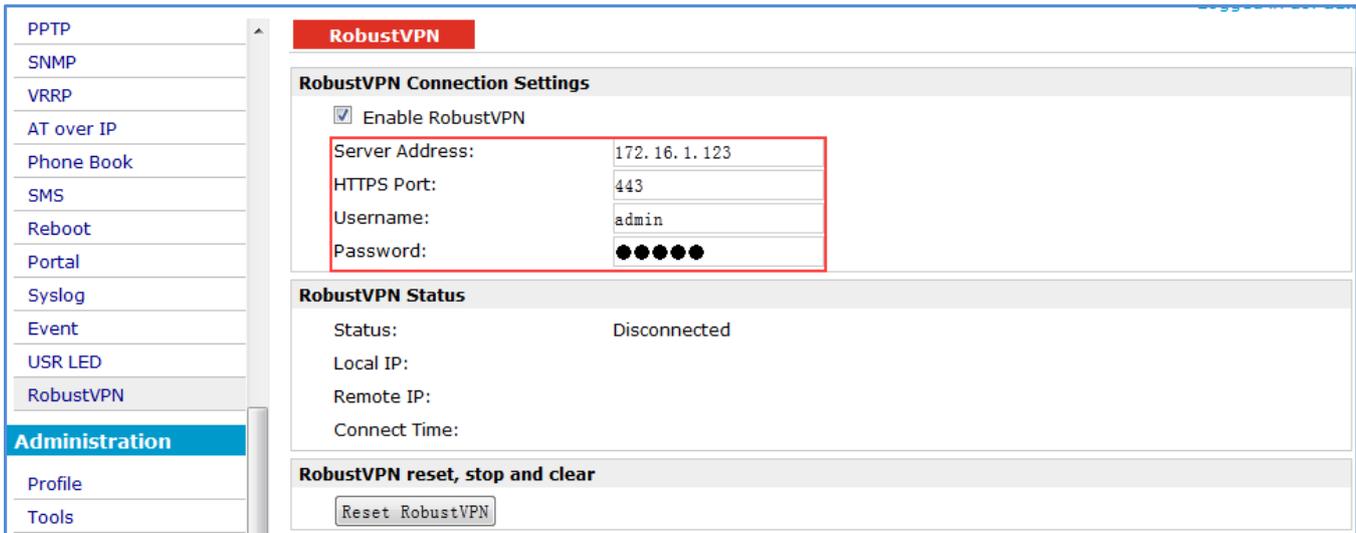
5. Browse to “Configuration”-> “Cellular WAN”-> “Basic”.

- In region “Cellular Settings”. Click the drop-down box of “Network Provider Type” of both SIM cards and select the correct “ISP” that you configure in “Configuration”-> “Cellular WAN”-> “ISP Profile”.
- If required please enter PIN number for SIM1 and SIM 2 in “PIN Type”.
- In region “Connection Mode”. Click the drop-down box of “Connection Mode” to select the connection mode accordingly. “Always Online” mode is selected in this Application Note.
- Click “Apply”.



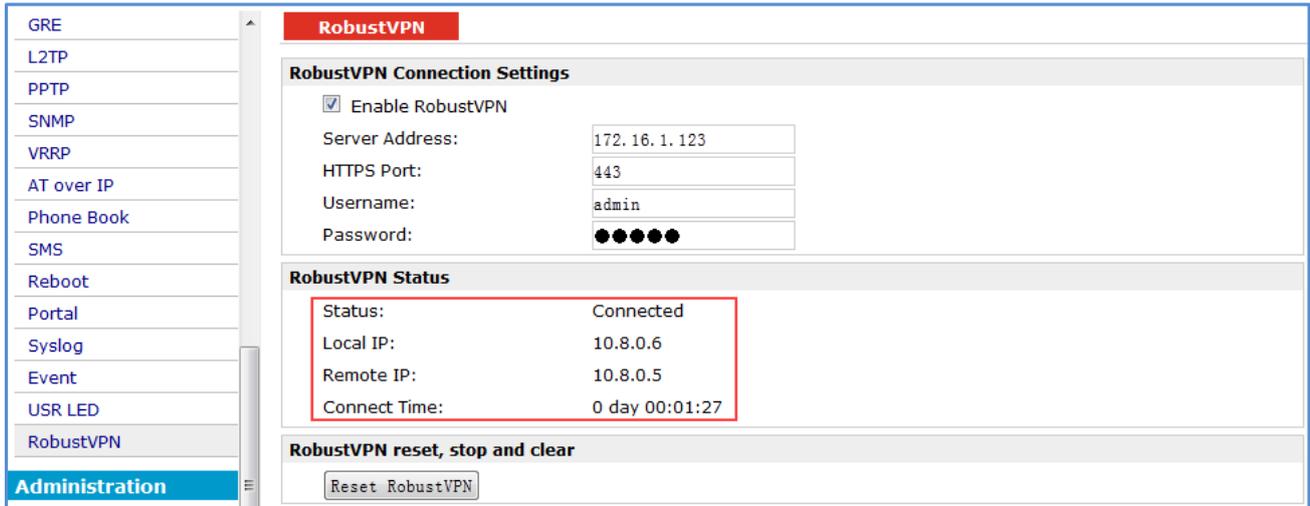
6. Browse to “Configuration”-> “RobustVPN”.

- In region “**Server Address**”, enter the IP address or Domain Name of RobustVPN server.
- 443 is the default HTTPS Port of RobustVPN.
- Username & Password is the account state of RobustVPN.
- Click “Apply”->”Save”->”Reboot”.



## 4.2.2. Check the status of RobustVPN connection

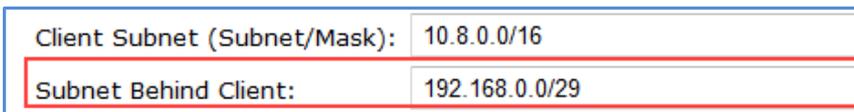
1. Browse to “Configuration”-> “RobustVPN”-> “RobustVPN Status”.



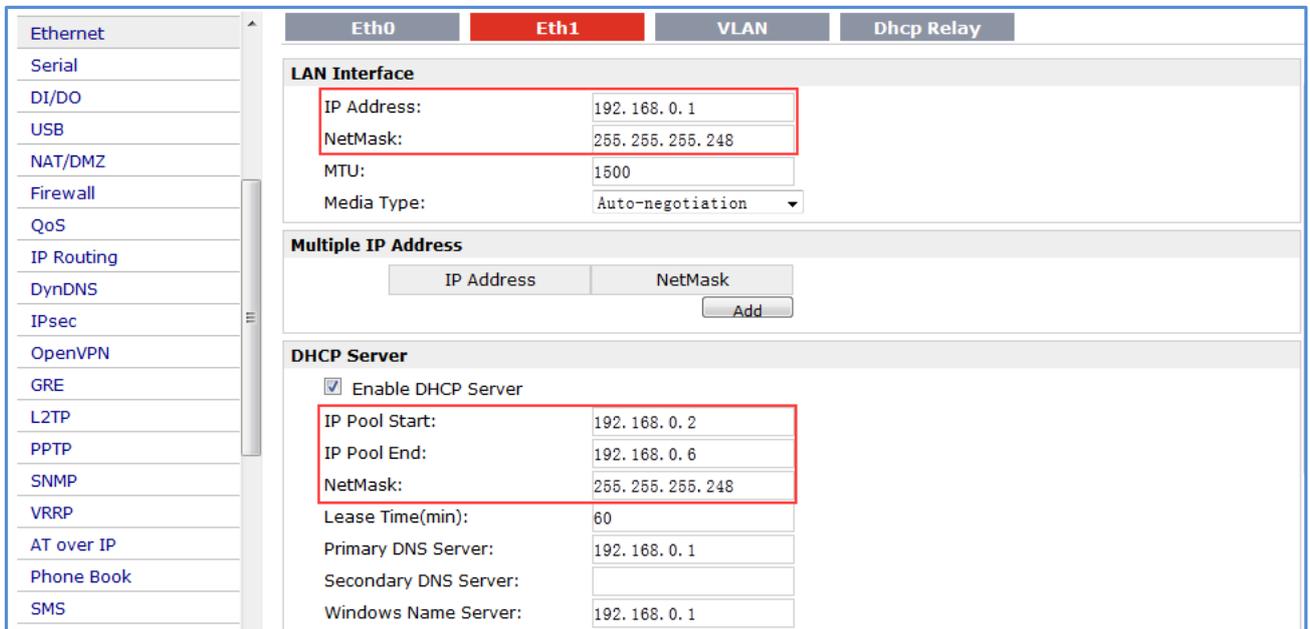
2. Browse to “Configuration”-> “Ethernet”-> “Eth1”.

- RobustVPN will push new DHCP settings to R3000 automatically, according the pre-set at RobustVPN.

*E.g. Server-> Remote Station-> OpenVPN Basic*



- /29 equal to 255.255.255.248.
- The host bits occupy 3 bit, so  $2^3=8$  IP address for each subnet, but  $8 - 2 = 6$  IP address are available for subnet.
- This R3000 start with 192.168.0.1, the next RobustVPN client would start with 192.168.0.9 and so on.



*Note: If R3000 fail to connect with RobustVPN, Please synchronize the time with RobustVPN server firstly because the validity of OpenVPN certificate is basic on RobustVPN' timestamp.*

## 4.3. Settings of Control Station

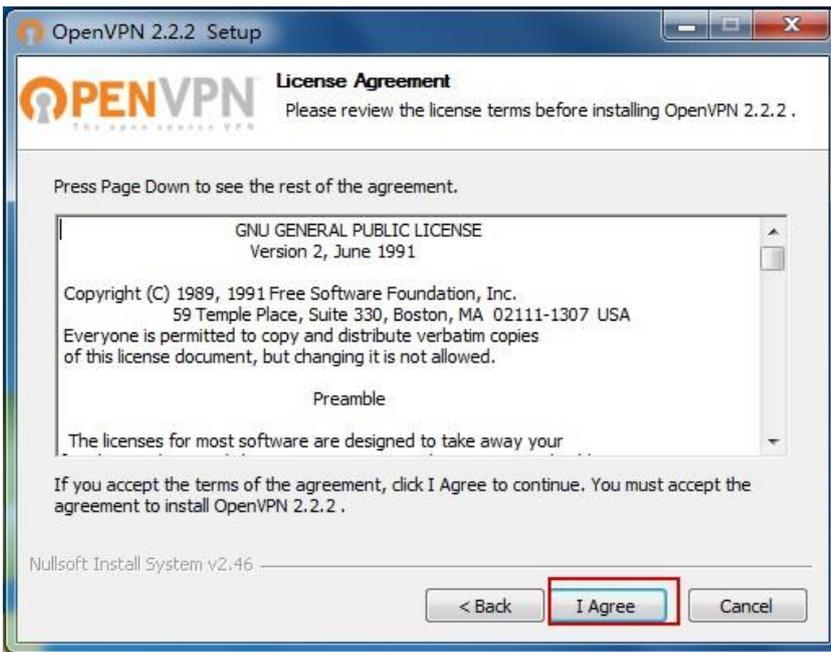
### 4.3.1. OpenVPN Installation on Windows

This step should be done on a PC that will be used to establish OpenVPN tunnel with RobustVPN server. The download is available from: <http://openvpn.net/index.php>

1. Download the release of the Windows installer. Run the installation program.



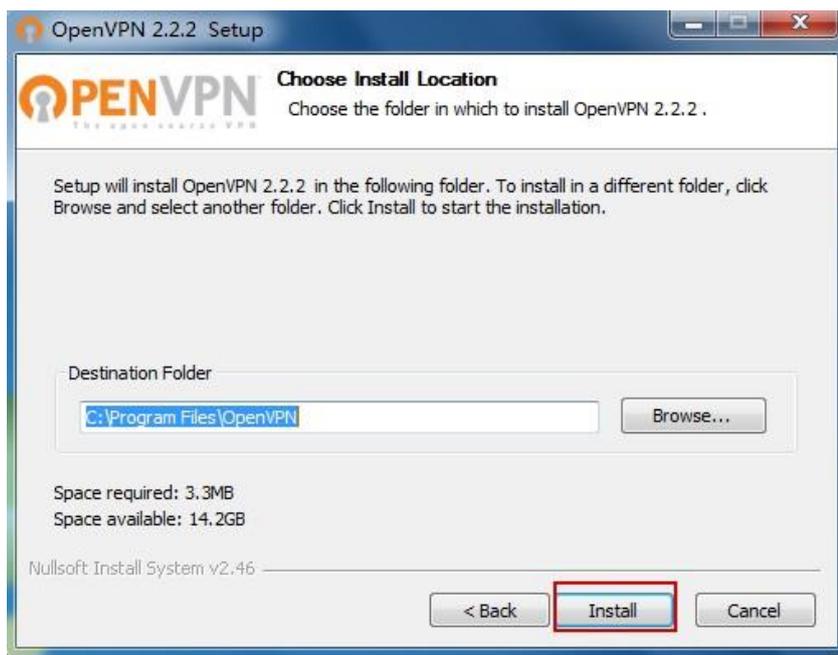
2. License Agreement.



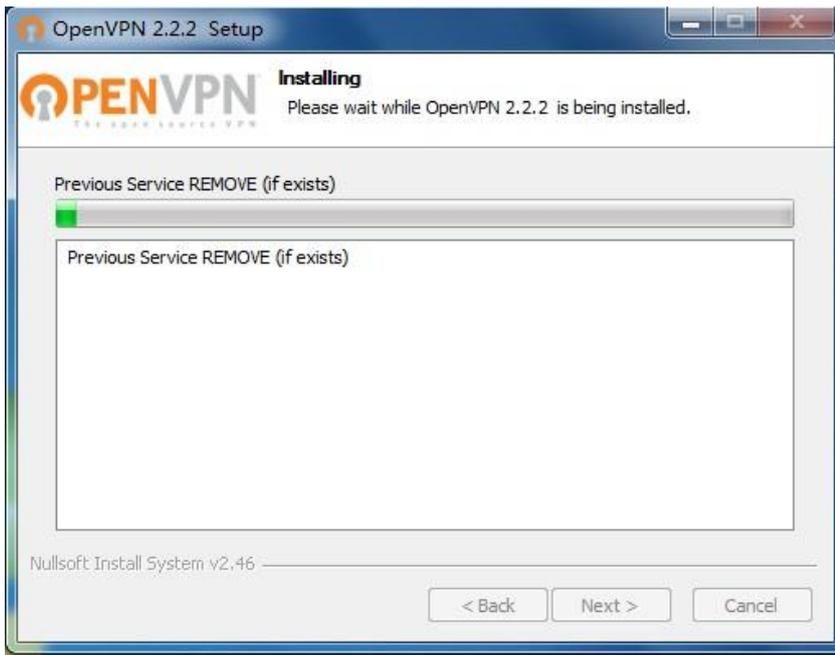
3. Select all the options by default.



4. Select the installation path. Save in default Destination Folder.



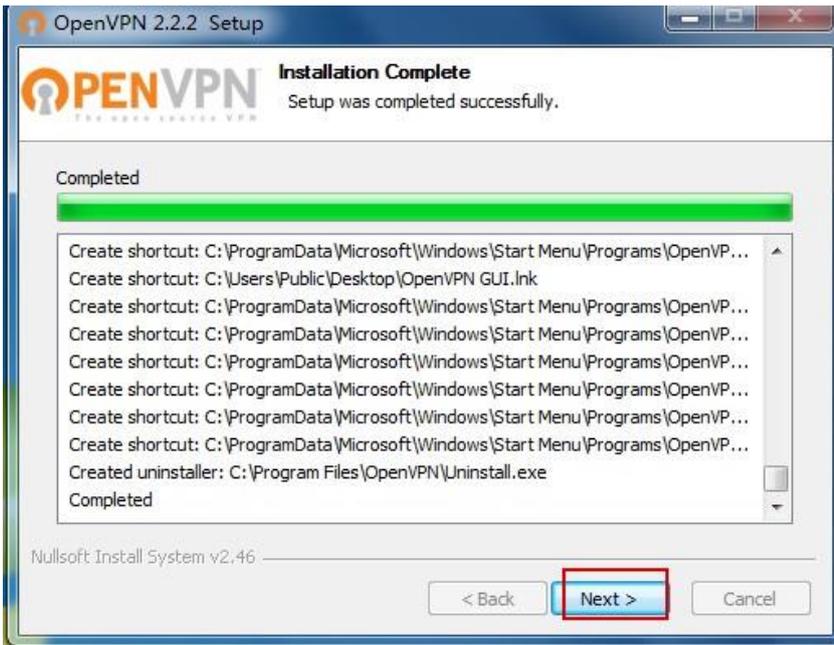
5. The installation schedule.



6. Agree to install the TAP-Win32 network adapter.



7. The installation will be completed.



8. Click "Finish" button and complete the installation.



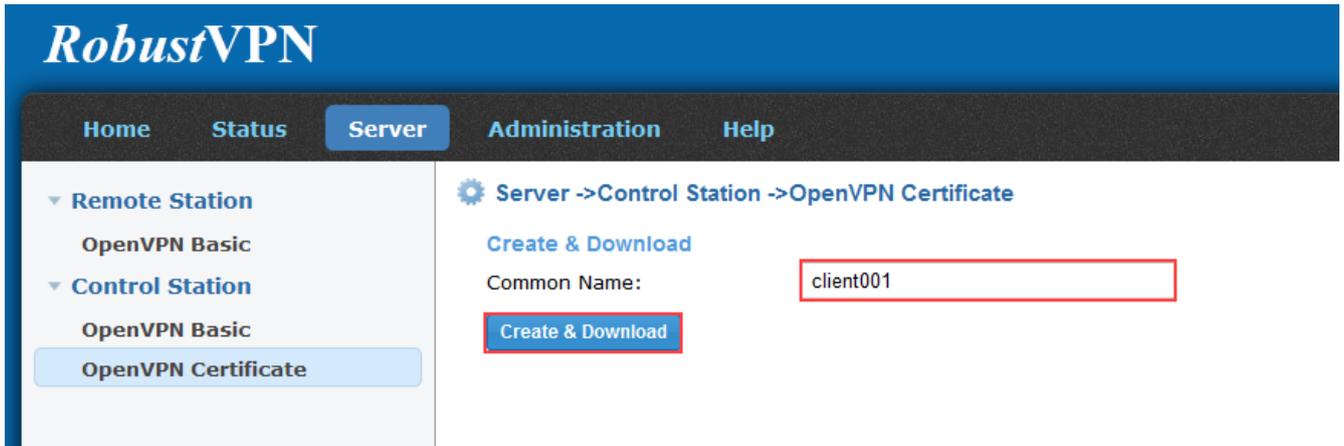
### 4.3.2. Create the certificates from RobustVPN

1. Login to RobustVPN management website.

E.g. <https://172.16.1.123>

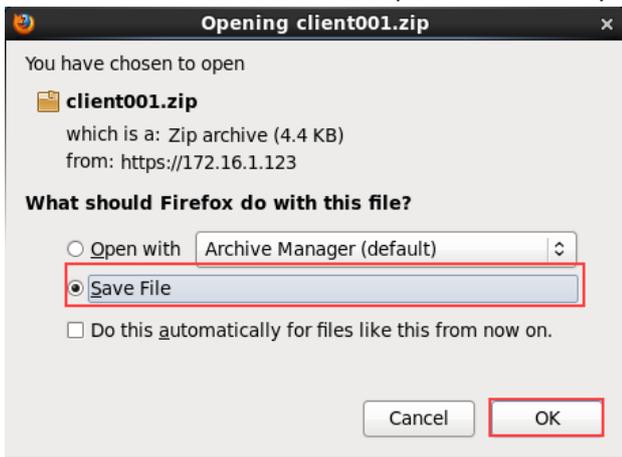


- Open page of OpenVPN certificate. Enter the common name of x.509 certificate.



*Note: Each certificate can be only used by one device at the same time, if more than one devices use the same certificate for RobustVPN, the connection is unstable and drop all the time.*

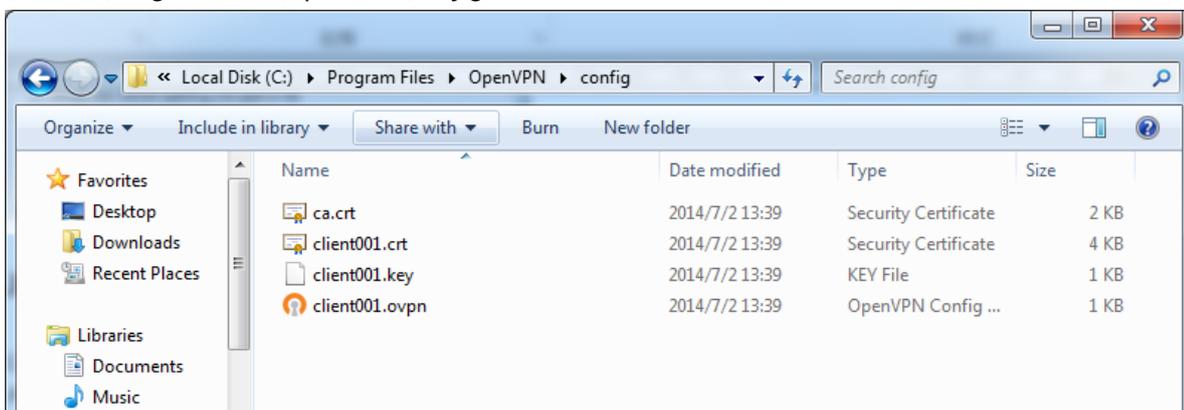
- Save the certificates and un-compress this file on your PC.



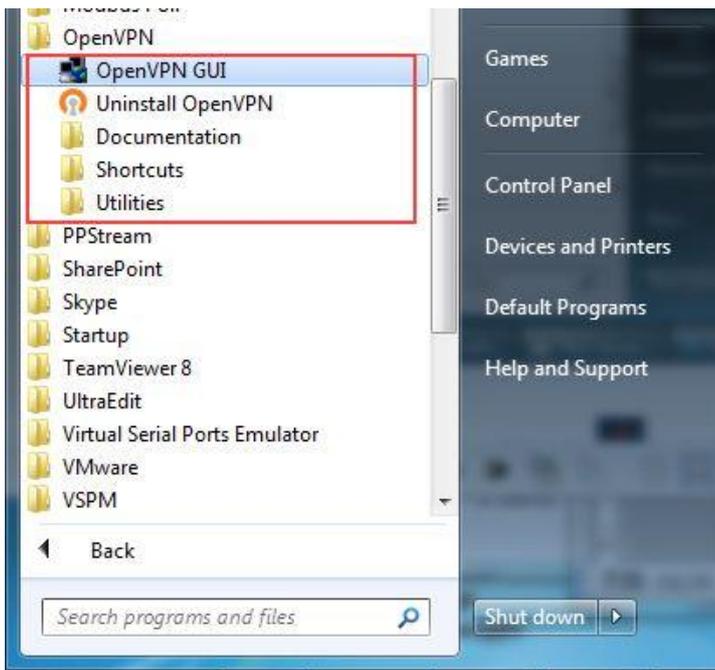
### 4.3.3. Running the OpenVPN software in Windows OS

- Copy the certificates to the OpenVPN software directory.

*Path: C:\Program Files\OpenVPN\config*



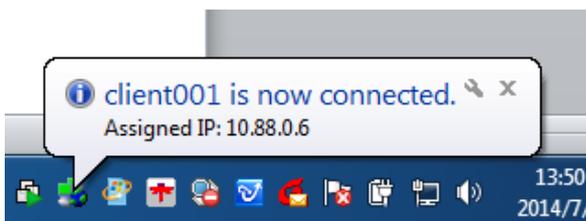
2. Run the OpenVPN software.



3. You could check the OpenVPN icon in the system tray.



4. Double click the icon, when the OpenVPN client001 has successfully started, the icon will turn green and prompt a notification with the assigned IP address.



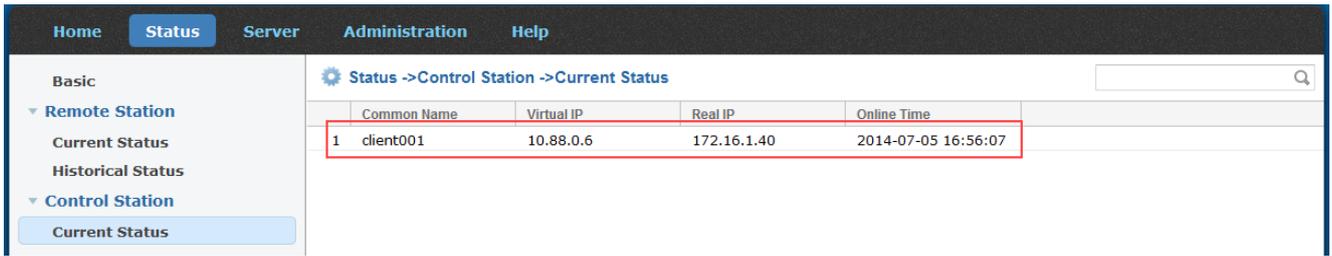
*Note: After connected to RobustVPN, RobustVPN will re-direct clients' gateway to RobustVPN. It means that default traffic (without specify routing) would forward to RobustVPN.*

### 4.3.4. Testing from Local PC to RobustVPN Clients

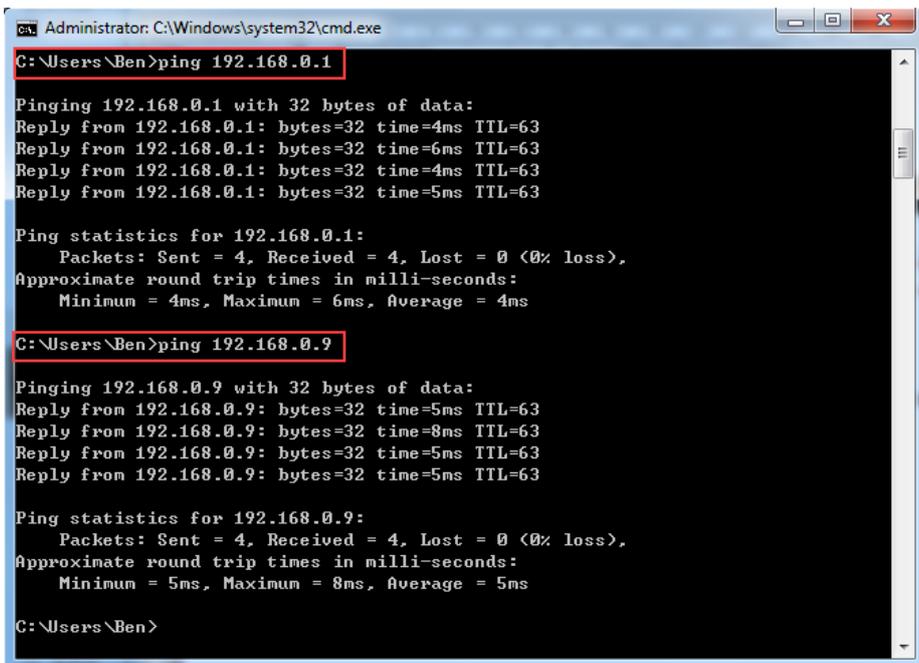
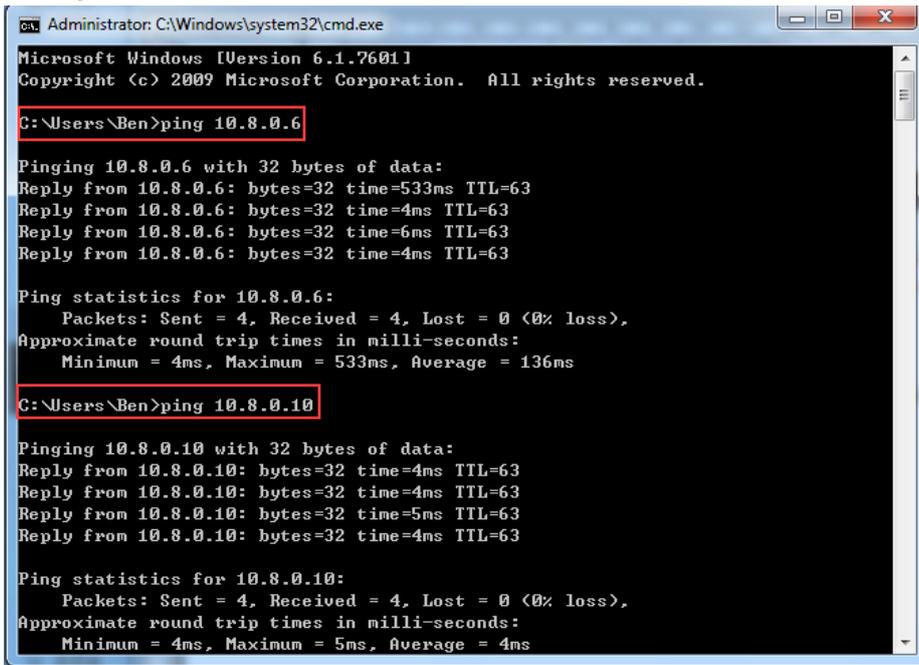
1. Check the remote connections status.

	Status	Serial Number	Virtual IP	Real IP	Remote Subnet	Receive
1	✓	00300513070020	10.8.0.10	172.16.12.4	iroute 192.168.0.8 255.255.255.248	6KB
2	✓	00300513100056	10.8.0.6	172.16.0.2	iroute 192.168.0.0 255.255.255.248	11KB

2. Check the Control Station status.



3. Testing the connection from Local PC to RobustVPN clients, make Local PC access the subnet behind R3000s.



# Chapter 5. Import License key of RobustVPN

## 5.1. Overview of license key

RobustVPN have two versions, one is trial version and the other is paid version. The trial version only supports five client connections. The paid version has no limitation to number of client connections. If you want to use RobustVPN without limitation, you will need to register for this software.

## 5.2. Register for RobustVPN

1. Check the System ID on *Help ->About*.

**Instructions**

**System ID: 0007181a**

RobustVPN have two version, one is trial version and the other is paid version. The trial version only supports five client connections. The paid version has no limitation to number of client connections. If you want to use RobustVPN without limitation, you will need to register for this software, the following steps :

1. Offer the System ID to us, we will according to your System ID to generate a License Key;
2. Enter the License Key in RobustVPN page, then save and reboot. Path: Server-> Remote Station-> OpenVPN Basic

2. Offer the System ID to our sales, we will according to your System ID to generate a License Key.

E.g.

**System ID: 0007181a**

**License key: 68BB896715913B99B8A8CE2EABA86876**

3. Enter the License Key in RobustVPN, then click "Save".

Path: Server-> Remote Station-> OpenVPN Basic

**Server ->Remote Station ->OpenVPN Basic**

Listen:

Protocol:

Port:

Interface:

Client Subnet (Subnet/Mask):

Subnet Behind Client:

Ping Interval:

Ping Restart:

Compression:

Encryption:

Verbose Level:

License:

Reboot after save:  Enable



**Server ->Remote Station ->OpenVPN Basic**

Listen:

Protocol:

Port:

Interface:

Client Subnet (Subnet/Mask):

Subnet Behind Client:

Ping Interval:

Ping Restart:

Compression:

Encryption:

Verbose Level:

License:

Reboot after save:  Enable