WoMaster

User Manual

COVER

WA512G Series

Industrial IEEE 802.11a/b/g/n/ac Wireless Mesh AP/Client

WA512G/GM-D-M2 Series

Industrial Din-Rail IIoT Router with M2 expansion slot, 802.11ac Wave 2 + 802.11b/g/n WLAN AP/MESH, 2GE, 2SIM, M2+4SMA, 24VDC

Nov.2021 V.1.4

www.womaster.eu

WoMaster

WA512G
Industrial Dual Radio 2.4G+5GHz Concurrent Wireless Mesh AP/Client
WA512G/GM-D-M2
Industrial Din-Rail IIoT Router with M2 expansion slot

User Manual

About This Manual

This user manual is intended to guide a professional installer to install and to configure the WoMaster Industrial Wireless MESH AP/Client. It includes procedures to assist you in avoiding unforeseen problems.

NOTE:

Only qualified and trained personnel should be involved with installation, inspection, and repairs of this router.

Disclaimer

WoMaster reserves the right to make changes to this Manual or to the product hardware at any time without notice. Information provided here is intended to be accurate and reliable. However, it might not cover all details and variations in the equipment and does not claim to provide for every possible contingency met in the process of installation, operation, or maintenance. Should further information be required or should particular problem arise which are not covered sufficiently for the user's purposes, the matter should be referred to WoMaster. Users must be aware that updates and amendments will be made from time to time to add new information and/or correct possible unintentional technical or typographical mistakes. It is the user's responsibility to determine whether there have been any such updates or amendments of the Manual. WoMaster assumes no responsibility for its use by the third parties.

WoMaster Online Technical Services

At WoMaster, you can use the online service forms to request the support. The submitted forms are stored in server for WoMaster team member to assign tasks and monitor the status of your service. Please feel free to write to help@womaster.eu if you encounter any problems.

TABLE OF CONTENTS

Declaration of Conformity

CE RED (Radio Device Directive)

While you see the CE Marking print in our product, it indicates the product comfort to the requirement of the CE RED.
We provide the CE RED Declaration of Conformity (DoC) for our Wireless Router, WLAN AP products in our web site. The DoC includes the Brand Name, Product Name, Model Name, Description, compliant standards and Manufacture information. Different product may comfort to different standards of Safety, Health, EMC, Radio and other specific standard. You can download the formal document of the product in our Web site or apply from our Sales/Technical people.

The DoC in this product manual applied to below models:
Brand Name: **WoMaster**
Product Name: **Industrial Din-Rail /Waterproof IP67 2.4+5GHz 802.11ac Wave 2 MESH WLAN AP/outer**
Model Name: **WA512GM-D/IP67, WA512G-D/IP67**
Compliant Standard:
Safety: UL62368-1
RF: EN300328, EN301893 B1, EN62311
EMC: EN301489-1/17, EN55032/35, EN61000-3-2/3
Also Complaint with FCC Standard:
RF: Part 15C 2.4G, FCC Part 15E 5G B1/B4, CFR 2.1091
EMC: FCC Part 15B

The declaration of CE RED is authorized at the following company and address.

WoM Asia.
(Manufacturer Name)
4F, No.86-2, Yiwen 1st St., Taoyuan Dist., Taoyuan 330, Taiwan
(Manufacturer Address)

FCC

Federal Communications Commission Statement

This device complies with FCC Rules Part 15. Operation is subject to the following two conditions:

• This device may not cause harmful interference.

• This device must accept any interference received, including interference that may cause undesired operation.

FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC exposure compliance requirement, please follow operation instruction as documented in this manual.

Radiation Exposure Statement:

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter

Installer Compliance Responsibility

Devices must be professionally installed and it is the professional installer’s responsibility to make sure the device is operated within local country regulatory requirements.

The device is compliance with IEC62368-1, EN62368-1, UL62368-1 Safety Request. Please read the safety precaution in user manual.

SAFETY PRECAUTION

- **Statement regarding restricted access:** The equipment is intended to be used in a restricted access location. Access should only be given to skilled person or instructed person who has been instructed in the operation of the equipment.
- **Only operate the device at the specified ambient temperature and humidity.**

- **High temperature warning:** When the router is operating, it must be **Noted** that the temperature of the metal surface is very hot.
- **Power Specification:** Follow the power installing instruction of the user manual, it indicates the available input voltage range, V+/V- pin assignment, power consumption and other notice.

> Connecting power with reverse polarity or using the wrong type of power supply may damage the equipment. Make sure that the power supply is connected correctly and of the recommended type.

- **Switch ON Notice:** Only switch on the supply voltage while the housing is closed, the input voltage is correct and the terminal blocks are wired correctly.
- **Wiring:** The connection cables used are permitted for the specified electronic voltage, current, wire diameter and temperature range. The quality of the RJ45 connector is also very important. In harsh environment, inferior quality RJ45 plug may also cause damage, short or even machine/PD damage.
- **Grounding:** The well grounding is important for EMC protection and make sure everything is done correctly before power on the system. **To avoid system damage, the equipment should be connected to ground.**
- **NOT allow to open the housing:** Only technicians authorized by the manufacturer are permitted to open the housing. *Note: When installing the M2 type cellular module, please shut down the router, install it according to the instruction guide. After installed, please close the housing before power on the router.
- **Mounting:** The equipment is only suitable for mounting at height ≦2m.
- **SIM:** Disconnect power before ejecting the SIM tray. Eject SIM tray carefully and Ensure that the SIM card is installed correctly.

1. Introduction

1.1 Overview

WA512G series is designed for IIoT application by dual band concurrent Wireless LAN Radio. WA512G is equipped with high performance Quad core ARM processor with 5GHz IEEE 802.11ac Wave 2 and 2.4G 802.11n WLAN radio, up to 866M+300Mbps high throughput, 2 Gigabit Ethernet port are able to support Bridge/Router mode and powered by 802.3af PoE switch. It supports MESH self-healing wireless network, DHCP Server, NAT and secure VPN connectivity can reach 150Mbps IPsec performance in 256-bit encryption.

Model Name	Description
IP67 Series	
WA512GM-IP67-E	Industrial 802.11ac Din-Rail Dual Radio 2.4+5GHz Concurrent Wireless Mesh AP, 802.11ac Wave 2 + 802.11b/g/n WLAN, 2GE, USB, IP67 Enclosure, EU-plug
WA512GM-IP67-U	Industrial 802.11ac Din-Rail Dual Radio 2.4+5GHz Concurrent Wireless Mesh AP, 802.11ac Wave 2 + 802.11b/g/n WLAN, 2GE, USB, IP67 Enclosure, US-plug
WA512G-IP67-E	Industrial 802.11ac Din-Rail Dual Radio 2.4+5GHz Concurrent Wireless AP/Client, 802.11ac Wave 2 + 802.11b/g/n WLAN, 2GE, USB, IP67 Enclosure, EU-plug
WA512G-IP67-U	Industrial 802.11ac Din-Rail Dual Radio 2.4+5GHz Concurrent Wireless AP/Client, 802.11ac Wave 2 + 802.11b/g/n WLAN, 2GE, USB, IP67 Enclosure, US-plug
DIN-Rail Series	
WA512GM-D	Industrial 802.11ac Din-Rail Dual Radio 2.4+5GHz Concurrent Wireless Mesh AP, 802.11ac+802.11b/g/n WLAN, 2GE, Din-Rail, 24VDC Terminal Block
WA512G-D	Industrial 802.11ac Din-Rail Dual Radio 2.4+5GHz Concurrent Wireless AP/Client, 802.11ac+802.11b/g/n WLAN, 2GE, Din-Rail, 24VDC Terminal Block
WA512G-D-M2	Industrial 802.11ac Din-Rail Dual Radio 2.4+5GHz Concurrent Wireless AP/Client, 802.11ac+802.11b/g/n WLAN, 2GE,LTE,NR5G,Din-Rail, 24VDC Terminal Block

1.2 Major Features

Below are the major features of WA512G Series:

- Quad-Core ARM Processor
- IEEE 802.11ac Wave 2, compatible with 802.11a/b/g/n
- Concurrent dual-band 2.4 G+5GHz radio, up to 866Mbps + 300Mbps Bandwidth
- 2x SMA/N-type Antenna socket for 2.4GHz + 5GHz DBDC (Dual Band Dual Concurrent)
- Dual Gigabit Ethernet ports in Router mode for WLAN/LAN to Eth-WAN routing
- Support IEEE 802.3af PoE P.D. Input
- **Qualcomm® Wi-Fi SON MESH Technology** (WA512GM Series)
  - Self-Healing auto rerouting through multi-hop (up to 4 hops and 10 nodes)
  - Self-Configuring Plug-and-play via Wireless network with ViewMaster utility
- **Enhanced Cyber Security & Redundancy**
  - Support Firewall for inbound/outbound traffic
  - OpenVPN (server/client), IPsec for secure remote connection
  - IPSec Performance >150Mbps @256-bit encryption
  - Support L2TP with PPP, PAP, CHAP(LCP, IPCP)
  - HTTPs/SSH secure login
  - Support TACACS+ multi-user authentication for privileged user management
- Support Industrial IoT Cloud Server, AWS, Azure, Private IoT and communication protocol
- Support Network management utility ViewMaster and NetMaster NMS
- Support Private cloud management server ThingMaster, ThingMaster OTA for Remote Management
- Slim size 110x106x40mm Din-Rail mounting design (WA512GM/WA512G-D)
- Support 24V(9-50V) DC Input (WA512GM/WA512G-D)
- Support IP67 enclosure for industrial application (WA512GM/WA512G-IP67)
- Wide range operating temperature -40~70˚C
- **Expandable M2 Slot in WA512G/WA512GM-D-M2**
  - Industrial Din-Rail IIoT Router with one additional M2 socket, available for M2 type 5GNR/4G LTE module
  - Dual SIM Tray to support Redundant SIM
  - 5GNR module kit with 5GNR module, screw, heat pad, 5GNR antennas and ready to use firmware

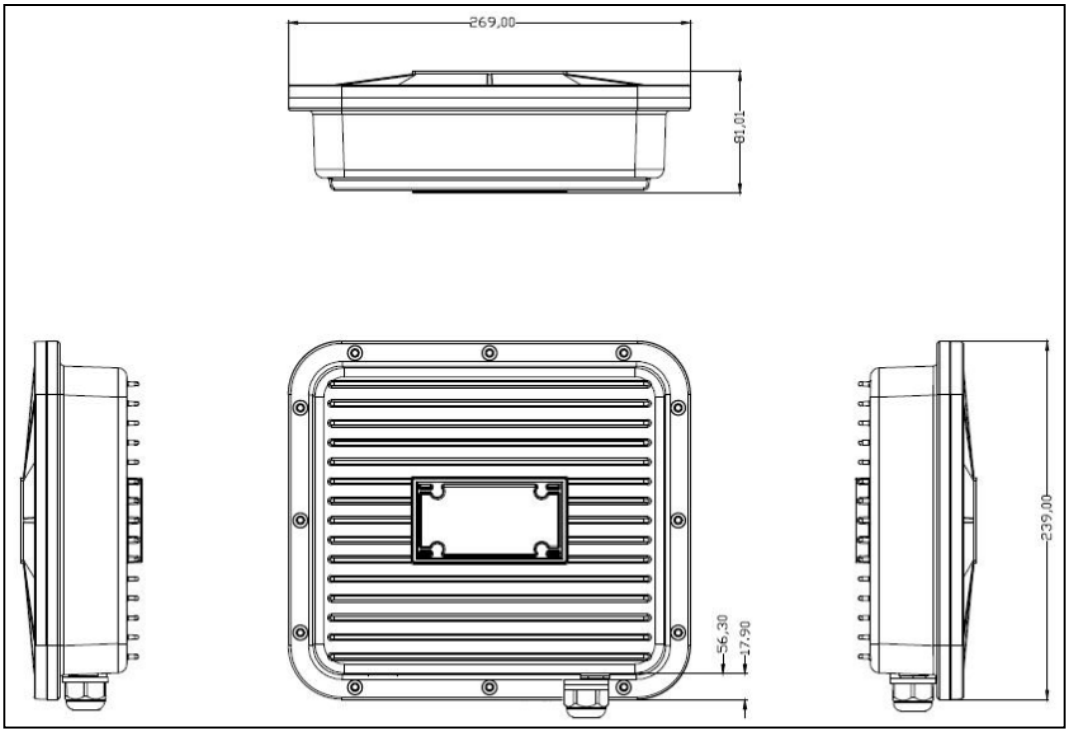
2. Installation

This chapter introduces mechanical and contains information on installation and configuration procedures.

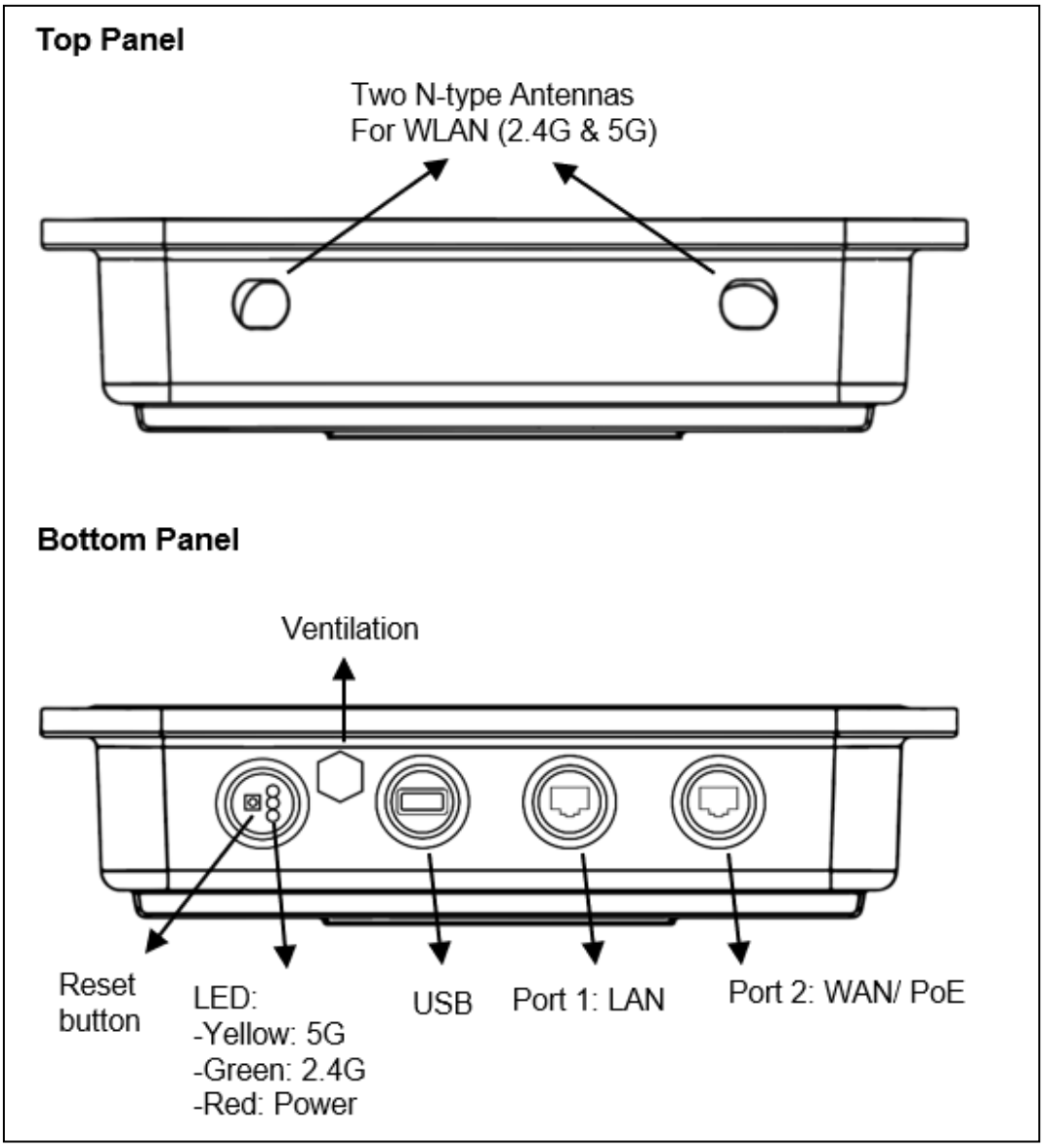
2.1 WA512G (IP67 Housing)

2.1.1 Dimension

Dimensions of WA512G-IP67: 239mm(H) x 269mm(H) x 68mm (D) / without mounting clip



2.1.2 Product Appearance



2.2.3 Product Package

Standard package includes:

1x Product Unit
1x Quick Installation Guide
1x PoE Injector with AC Plug
3x Cable Gland
1x Mounting kit

*Note: Antenna not included

2.2.4 Interface Installation

After unpacking the box, follow the steps below in order to properly connect the device.

2.2.4.1 Wiring Power Input

Standard package includes a PoE injector to power on WA512G-IP67 series. WA512G is a standard IEEE 802.3 PoE P.D. device and can also be power by PoE switch (P.S.E).

Wiring the Power Input through PoE Injector

1) Install PoE injector power cord.

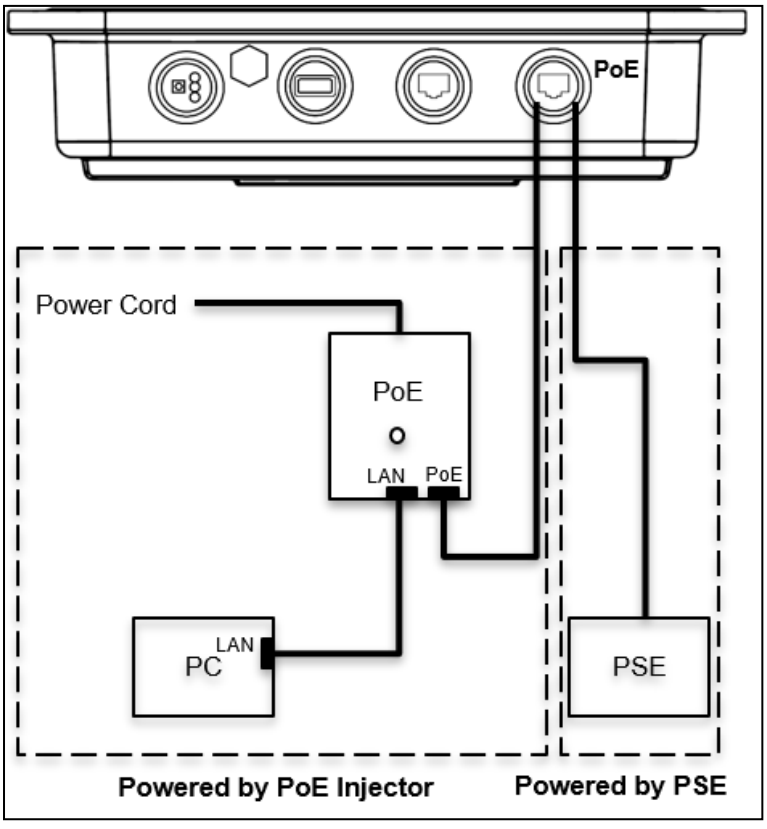
2) Install Ethernet cable between PoE ports of WA512G and PoE injector.

3) Install Ethernet cable between LAN ports of WA512G and PC/NB whenever proceeding WebGUI configuration.

Wiring the Power Input through PSE switch

1) Install Ethernet cable between PoE ports of WA512G and PSE switch

2) Install Ethernet cable between LAN ports of WA512G and PSE switch whenever proceeding WebGUI configuration.



2.2.4.2 Wiring Antenna

Antenna Socket on device - N-type female

The antenna socket is N-type female and located on the top of the device. The antenna is usually installed in the upper/upward position. You can install the external antennas or you can install an antenna cables to connect to a long-distance antenna.

Antenna/Antenna Cable - N-type male

You can wire the waterproof antenna with N-type Male connector directly to the N-female socket on the top of the device. For safely installation, it is usually applied for short length, lower gain omni-antenna.

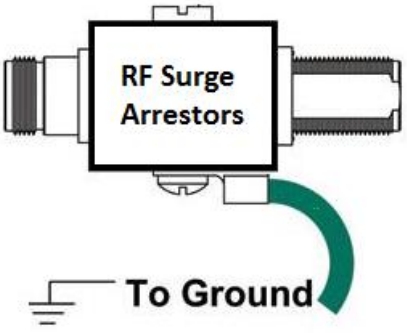
You can also Wire extended antenna cable with N-type Male connector to connect the external antenna.

Please noted that the longer RF cable must cause more signal lost, the shorter the more suitable. The RF cable quality is also important for the extended antenna installation. We recommend the high quality RF cable, for example the **RF400 50ohm LOW LOSS COAXIAL CABLE with UV RESISTANCE.**

Note: In field installation, the RF Surge Arrestor is also important for product safety.

RF Surge Arrestors

RF surge arrester is also known as cable free coaxial lightning arrestors/suppressors. It is used for antenna feeder equipment, it can protect the communication device from the lightning strike. The arrestor features an N-type male and an N-type female connector to connect the extended RF cable. An earth bond connection must be created using the shortest path to the ground.



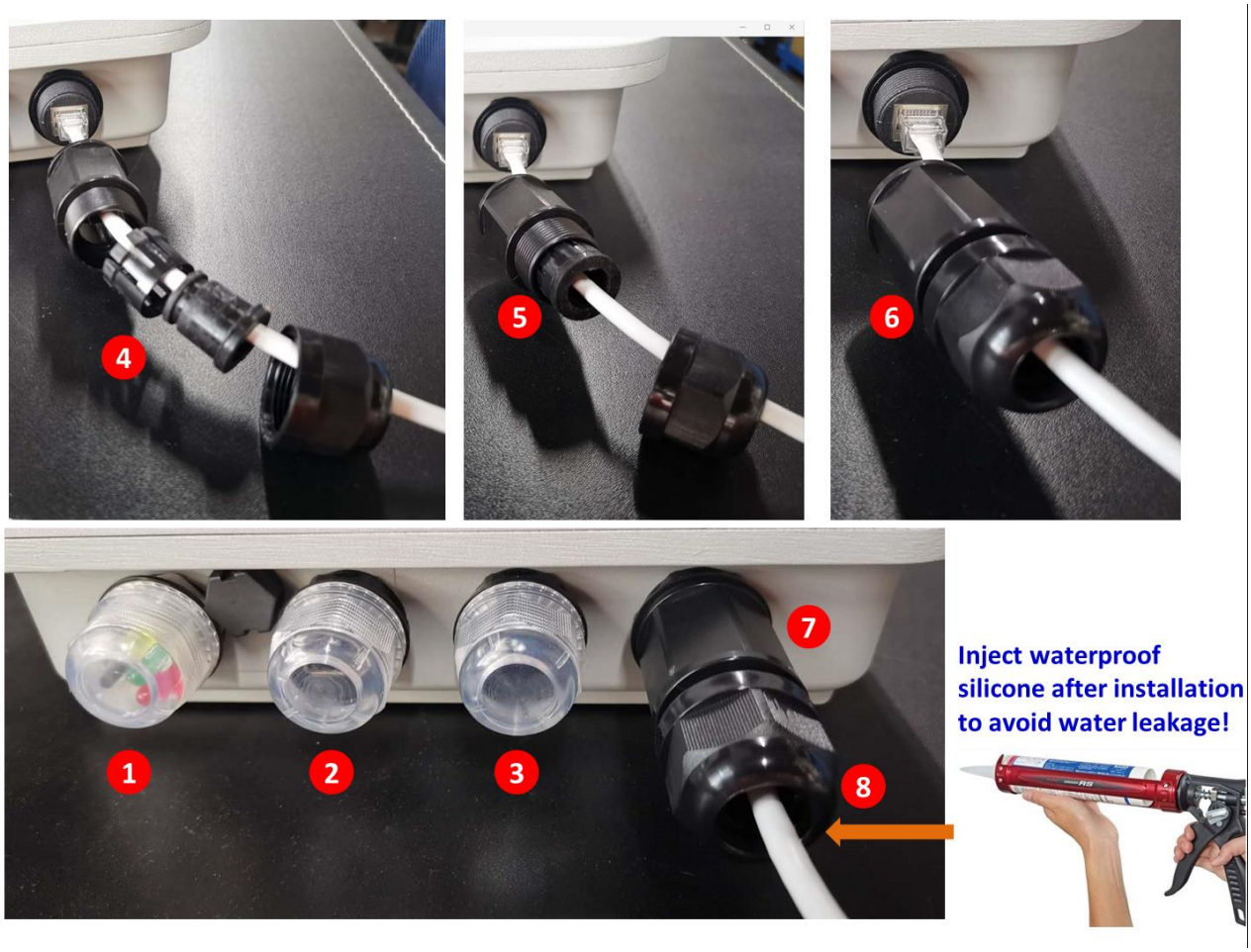
2.2.4.3 Wiring Waterproof Connector

As shown in the figure, there are some steps to wire the waterproof connectors.

Step 1~3: **Lock the waterproof cover** for the unused RJ45, USB and LED light connectors. The steps can be done before go to the field.

Step 4~7: Wiring Ethernet cable. Since the Ethernet cable length is not fixed in every site, the steps are usually done in the field. Connect the Ethernet cable to the waterproof cable gland in sequence. If your RJ45 crystal connector is larger than the aperture, you must thread the cable before pressing the RJ45 crystal connector. Lock the Ethernet connector with cable gland finally.

Step 8: After completing the installation of the connector, please check whether the Ethernet cable and the waterproof cable gland are fastened, and **inject waterproof silicone to avoid water leakage.**



2.2.5 Mounting the AP

Mount the AP on a Pole/Wall

1) Screw up the attached mounting plate and the Access Point by screw A (M5, 15mm).

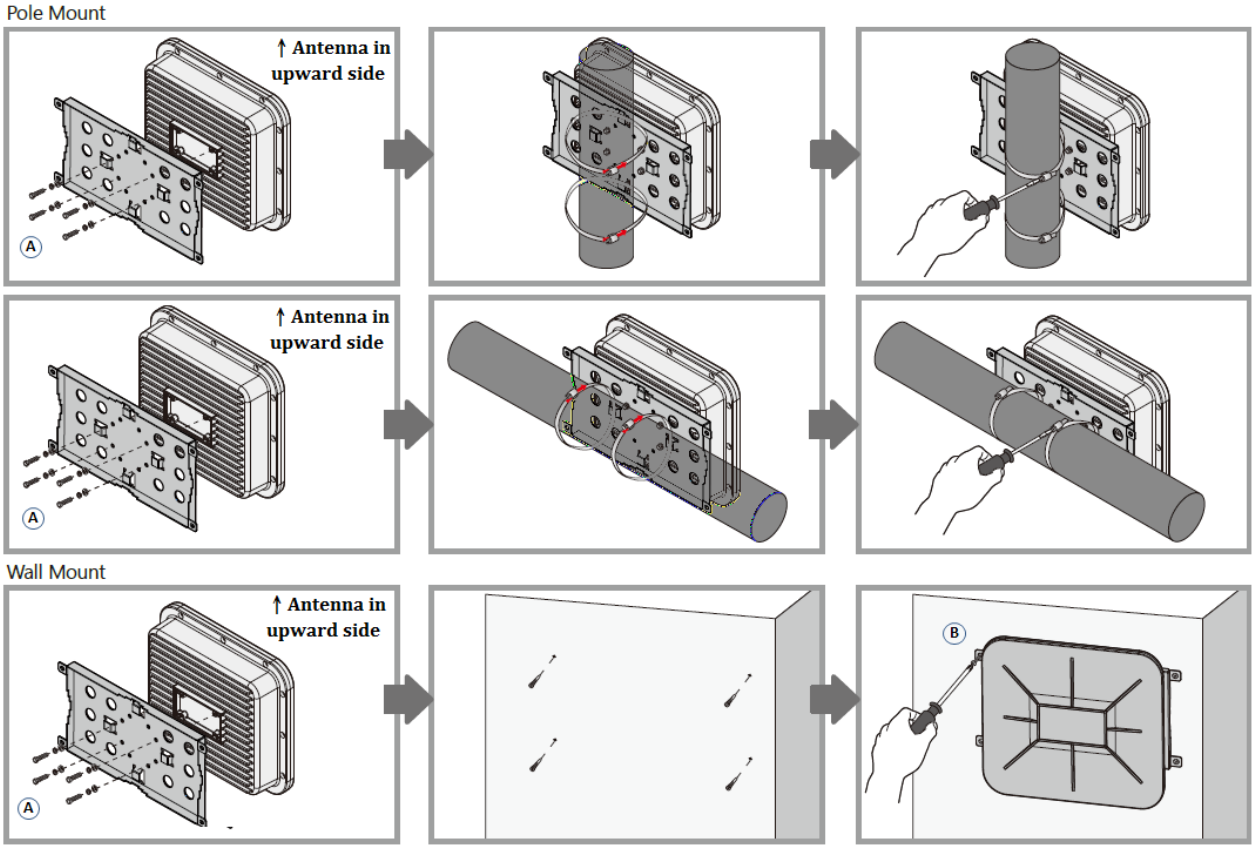
2) Screw up the mounting kit between pole and Access Point.

3) Mount the Access Point steadily to the pole by locking the pole mounting kit tightly. The antenna is installed in the upper/upward position. While installed the AP in high tall factory, the AP is also available by pole mounting on the ceiling.

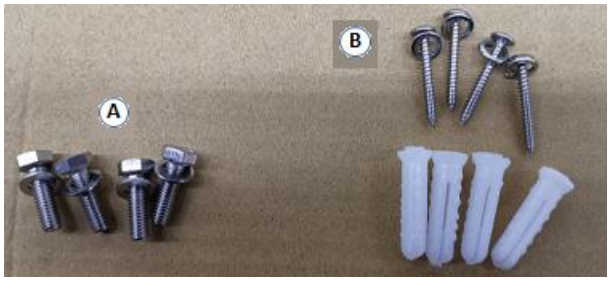
4) You can also mount the Access Point steadily to the wall by locking the wall mounting plate tightly. The antenna is installed in the upper/upward position. You can use the attached screw B and its expansion screw. While using other type screw for wall-mounting, make sure the device is fixed well.

5)The mount plate can be installed in Horizontal or Vertical direction, refer to the below steps.

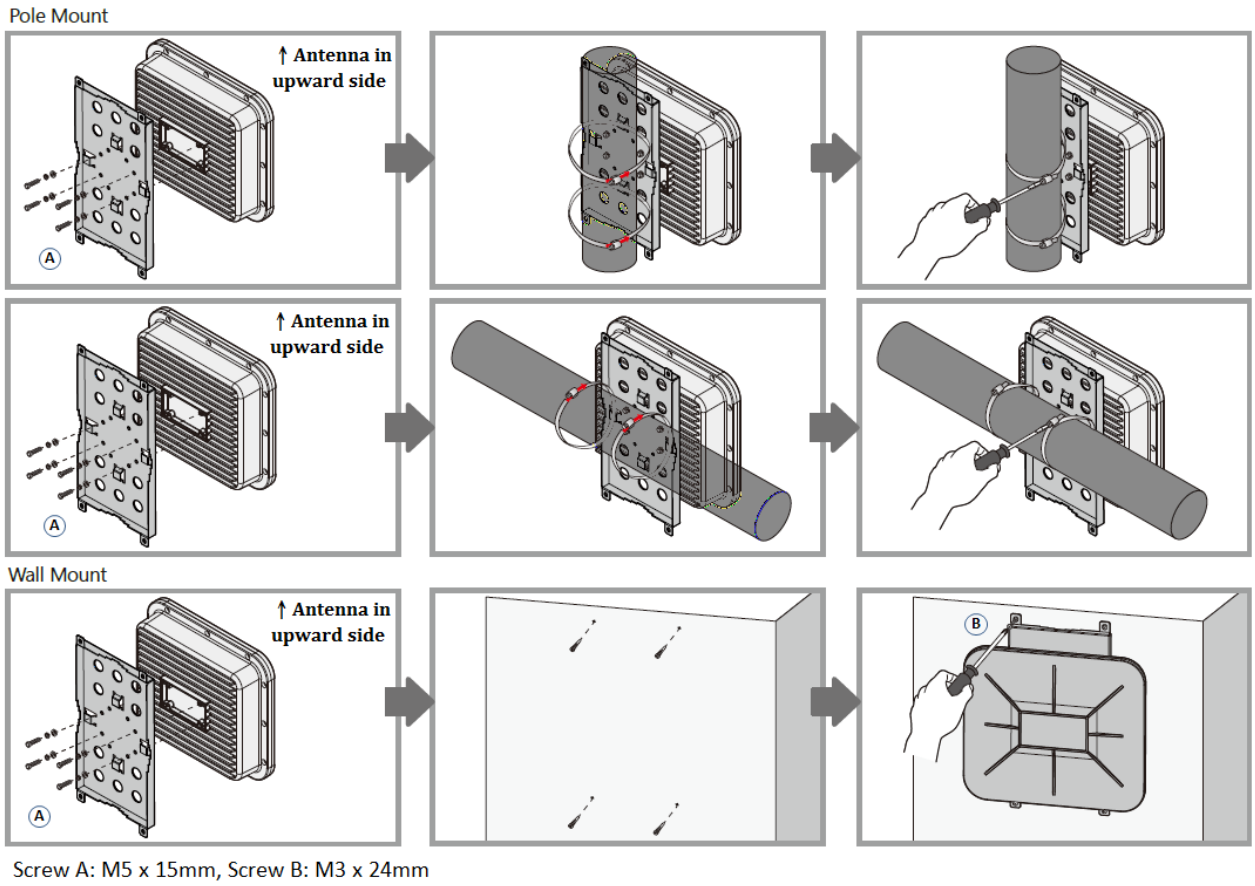
Mounting plate in Horizontal installation (The N-Type Antenna socket is in upper/upward side.)



Screw A: M5 x 15mm, Screw B: M3 x 24mm



Mounting plate in Vertical installation (The N-Type Antenna socket is in upper/upward side.)



Screw A: M5 x 15mm, Screw B: M3 x 24mm

2.2.6 LED

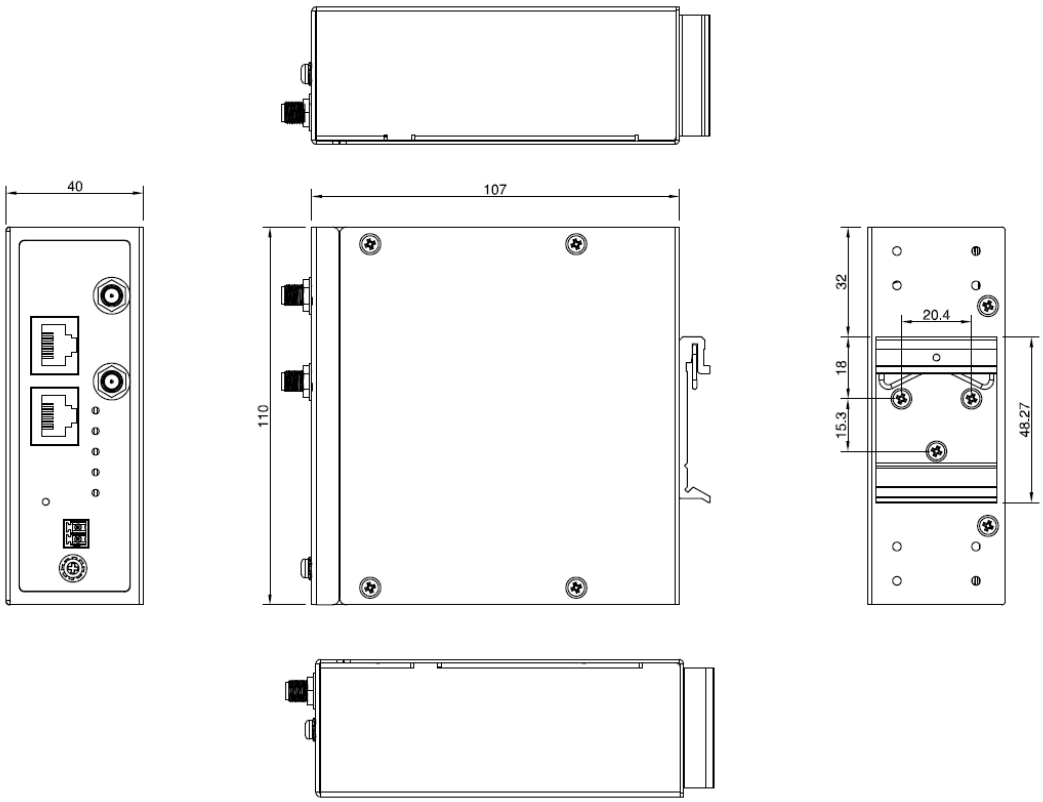
Check system status through LED connector.

WA512G-IP67 series

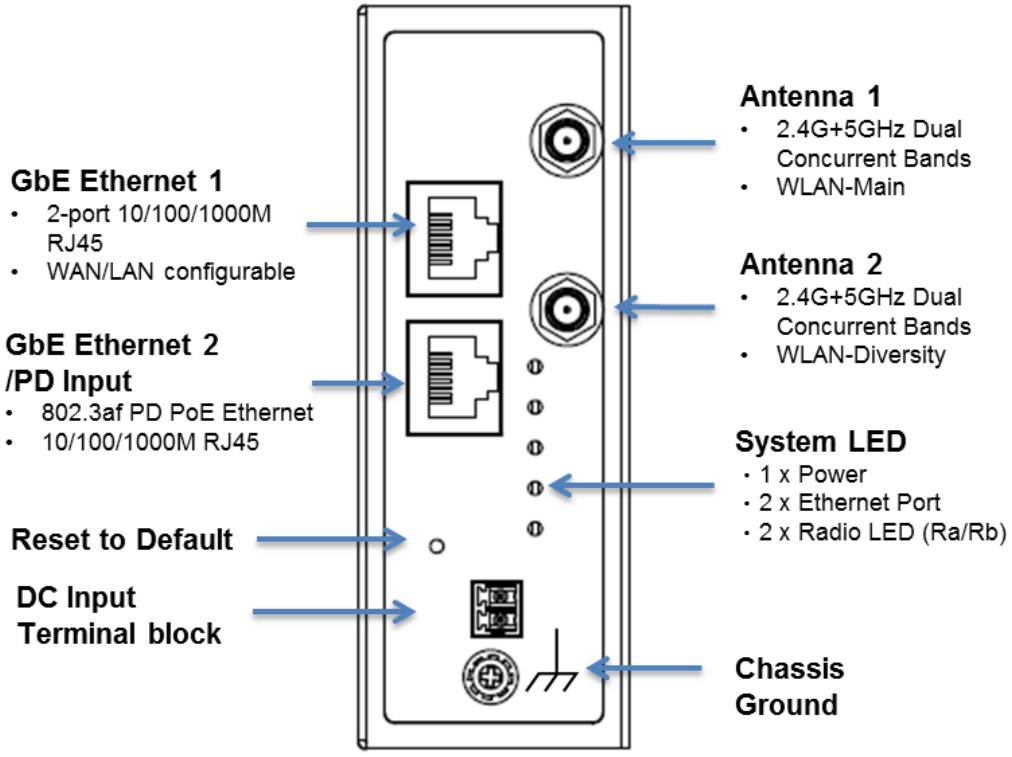
	LED	Status	Description
	5GHz	Amber On	AP mode
		Amber Blinking	Station mode client connected
		Off	Station mode/radio disabled
	2.4GHz	Green On	AP mode
		Green Blinking	Station mode client connected
		Off	Station mode/radio disabled
	Power	Red On	Power On
		Off	Not Receiving Power

2.2 WA512G-D (DIN-Rail)

2.2.1 Dimension



2.2.2 Product Appearance



2.2.3 Product Package (WA512G-D)

Standard package includes:

1x Product Unit
1x Quick Installation Guide
2x WLAN Antenna, White The Antenna supports 2.4G/5G wide range. Attached them to ANT1 and ANT2 sockets.
1 x Attached Din Clip

Note: The model doesn't offer PoE injector. If you need additional PoE injector or PoE switch, check with our sales contact window.

2.2.4 Interface Installation

After unpacking the box, follow the steps below in order to properly connect the device.

2.2.4.1 Wiring Power Input

The WA512G-D supports DC terminal block with 24V(9~50V) DC input. The typical power input voltage is 24VDC. Wire the power positive(+) and native(-) correctly before turn on the power supply.

WA512G supports standard IEEE 802.3af PoE Power Device (PD), it can be powered by PoE switch (P.S.E) or PoE injector. WA512G equips with gigabit Ethernet ports and dual WLAN radio, it's MUST to choose full gigabit PoE Switch with higher Ethernet bandwidth, for example the DP208, DP412, DP612.

The standard package in WA512G-D does NOT have PoE injector inside. You can buy our passive 48V (not standard 802.3af/at PoE), you can also choose standard IEEE 802.3af/af PoE Injector for powering. You can aslo buy our PoE Switch.

Wiring the Power Input through DC Terminal Block

1) Insert the positive and negative wires into the V+ and V- contact on the terminal block connector.

2) Tighten the wire-clamp screws.

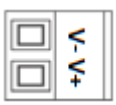
3) Connect the power wires to suitable DC Switching type power supply. The input DC voltage should be in the range of the spec.

Wiring the Power Input through PoE Injector

1) Install PoE injector power cord.

2) Install Ethernet cable between PoE ports of WA512G and PoE injector.

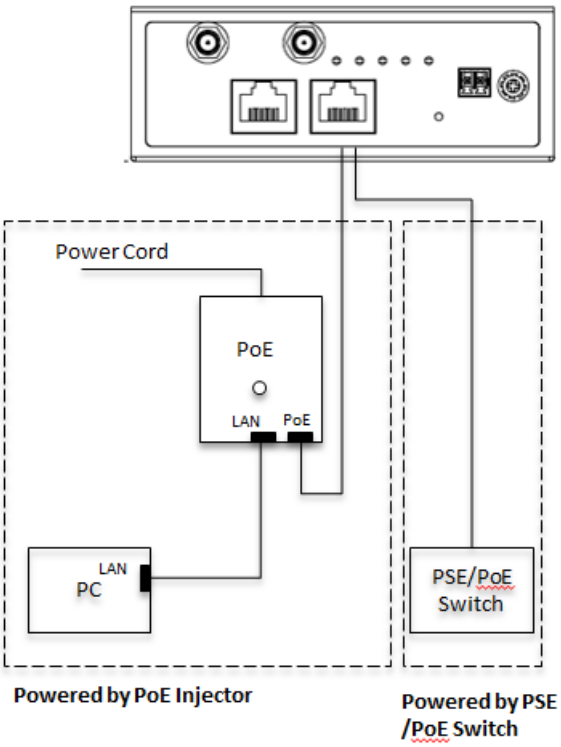
3) Install Ethernet cable between LAN ports of WA512G and PC/NB whenever proceeding WebGUI configuration.



Wiring the Power Input through PSE switch

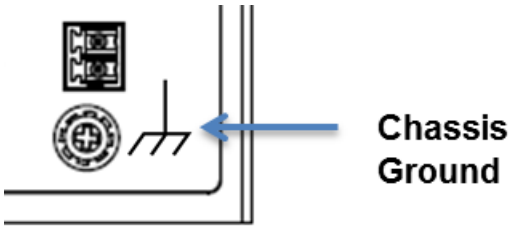
1) Install Ethernet cable between PoE ports of WA512G and PSE switch

2) Install Ethernet cable between LAN ports of WA512G and PSE switch whenever proceeding WebGUI configuration.



2.2.4.2 Wiring the Ground

The chassis grounding screw is located on the bottom side of the router. For avoiding system damage by noise or electric shock, establish a direct connection between the ground screw and the grounding surface prior to connecting devices.

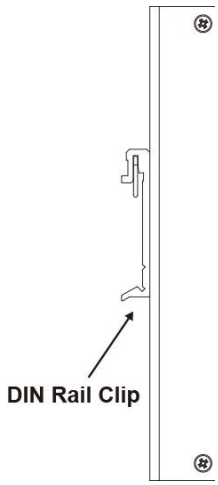


2.2.5 Mounting the AP

You can mount the AP by attached Din-Rail Clip or Wall-mount by optional wall-mount plate.

2.2.5.1 DIN-Rail Mounting

The EN50022 DIN-Rail plate should be already attached to the back panel of the device screwed tightly. If user needs to reattach the DIN-Rail attachment plate to the device, make sure the plate is situated towards the top, as shown by the following figures.



To mount the router on DIN Rail track, do the following instruction:

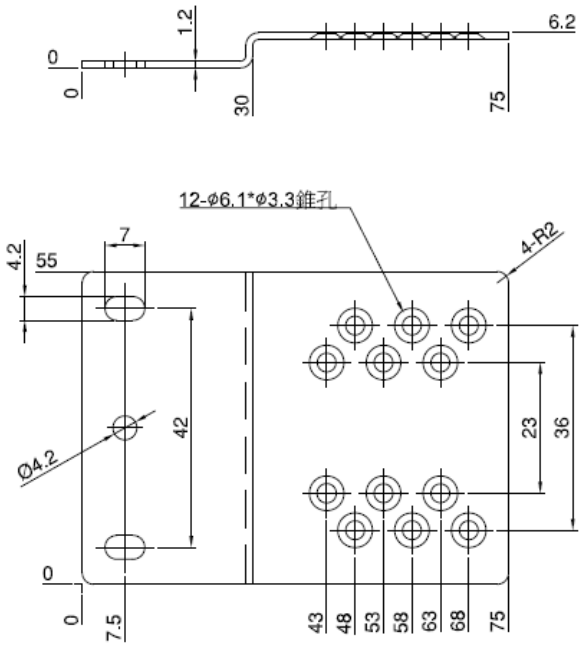
1. Insert the top side of DIN Rail track into the slot of DIN Rail clip.
2. Lightly clip the bottom of DIN-Rail to the track and make sure it attached well.
3. To remove the device from the track, reverse the steps.

2.2.5.2 WALL Mounting

Optional Wall-mount Plate, MK-D1-2:

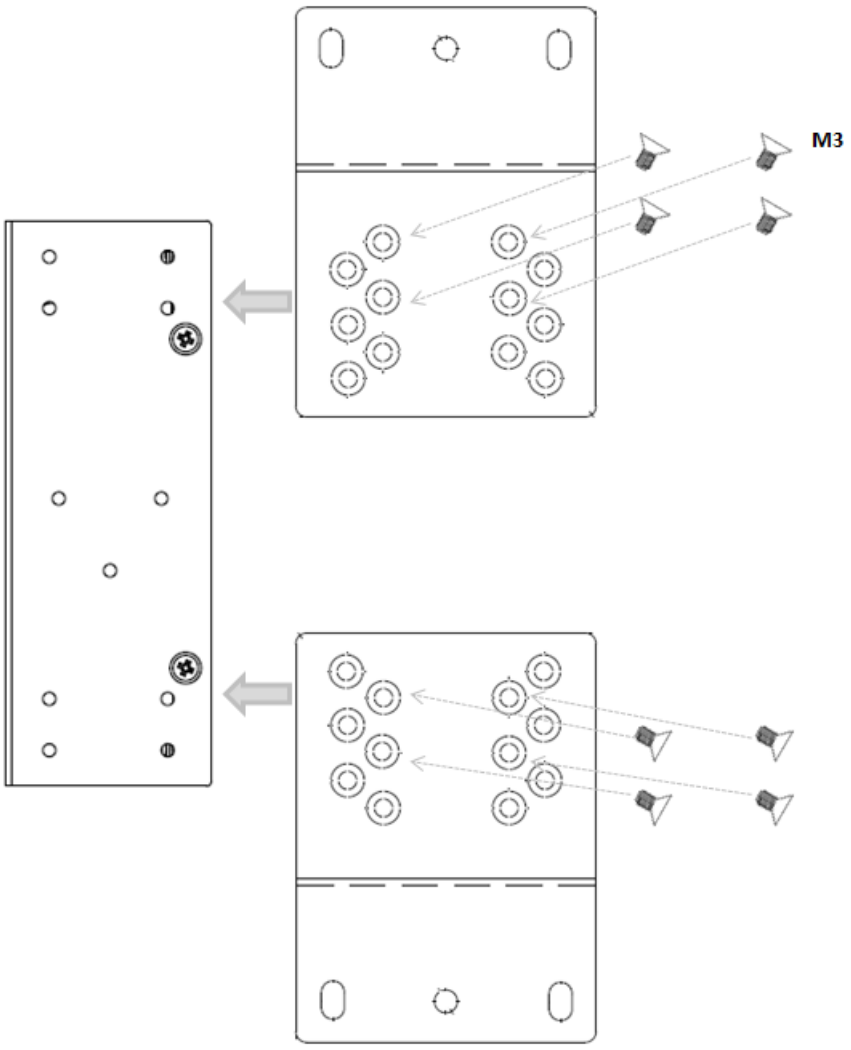
Name	Specification
MK-D1-2	WALL-MOUNTING KIT WITH 2 PLATES AND 8 SCREWS
DP210 WALL MOUNT PLATE	2pc DP210 WALL MOUNT PLATE, PANTON BLACK (Or other color by request)
Flat head M3 screw	8pcs Flat head screw, M3, length 6MM, nickel plated
Packing material, zipper bag No3	Packing material, zipper bag No.3, 70(W)x100(L)MM for SCREW
Packing material, zipper bag No.6	Packing material, zipper bag No.6, 120(W)x170(L)MM for All

MK-D1-2 Dimension:



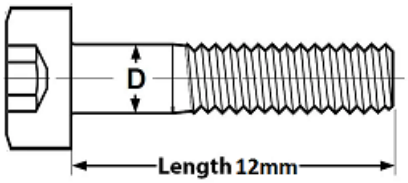
To mount the AP to the WALL/BOX, do the following instruction:

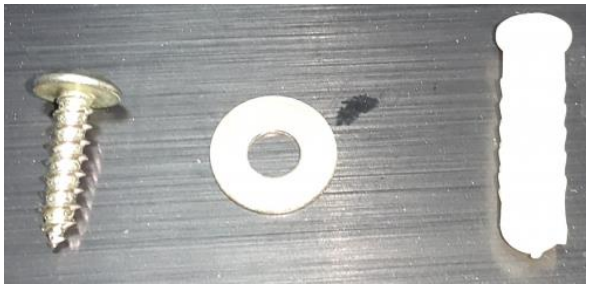
1. Remove the attached DIN Rail Clip first.
2. This wall-mount plate can be shared with our switch or router. For WA512GM-D, please use the 6 screw holes near the inside.
3. Lock the wall-mount plate by the attached “M3” 6mm length screw to the device.



4. Lock the wall-mount plate to the WALL. The suggested screw size for wall-mount is M6 12mm length. (This screw varies from site to site, we do not attach it.)

   Reference Wall-mount screw: M6 12mm





2.2.6 ANTENNA & LED

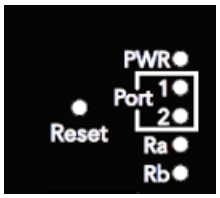
WiFi Antenna

WA512GM-D Series supports Dual Band in One Antenna socket design. It means one antenna can transmit dual band dual radio signal, you should choose Dual Band antenna. Connect the attached dual band antenna to the SMA connector on the front panel. Alternatively, you can connect the antenna through extended RF cable with antenna holder to SMA on the front panel and screwing the antenna holder on the field box. The magnet holder is also popular for metal box installation.

Major Specification of attached antenna:

Frequency	2400 ~ 2500 MHz 5150 ~ 5850 MHz
S.W.R	<= 2.0 @ 2400 ~ 2500 MHz <= 2.0 @ 5150 ~ 5850 MHz The data is tested with 1M cable
Peak Gain (Max.)	1.92 dBi @ 2450 MHz 3.4 dBi @ 5150 MHz
Efficiency	70 % @ 2400 ~ 2500 MHz 85 % @ 5150 ~ 5850 MHz
Polarization	Linear
Impedance	50 Ohm
Connector Type	SMA Male Reverse
Operational Temperature	- 40 °C ~ +65 °C

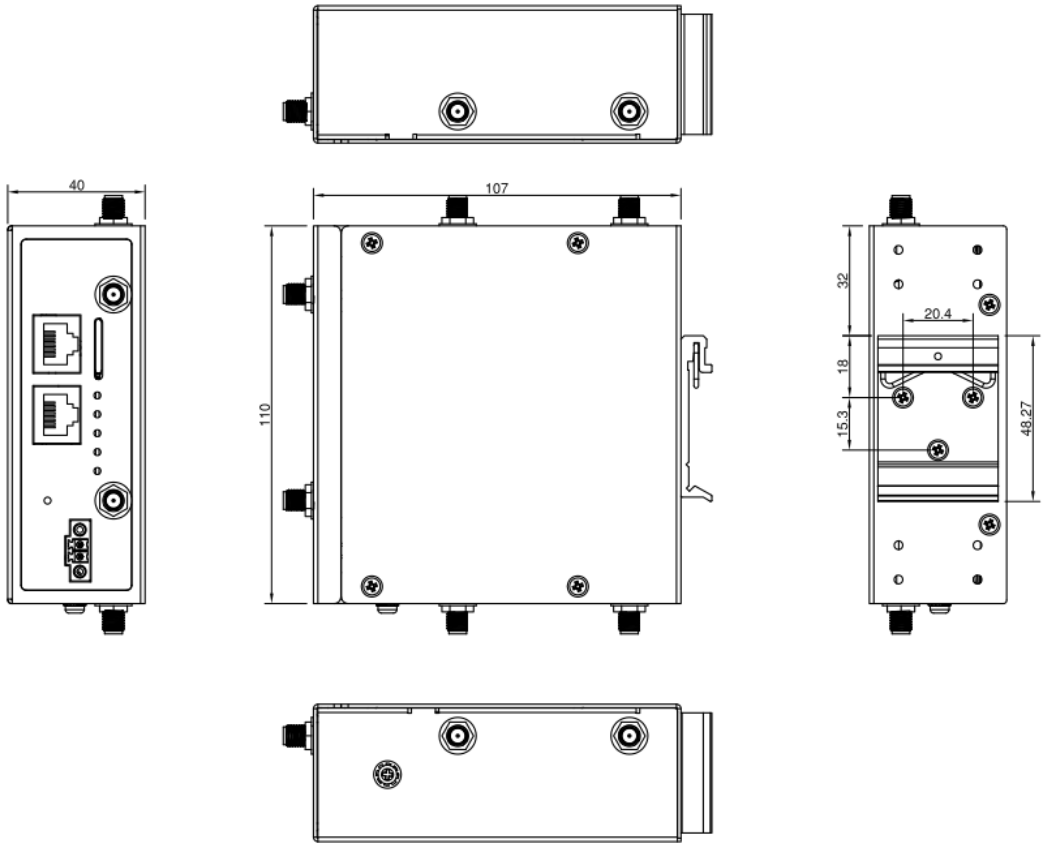
WA512GM/WA512G-D LED:

	LED	Status	Description
	**Power**	Green On	Power On
		Off	Not Receiving Power
	Port 1/2	Green On	Link
		Green Blinking	Activity
	Ra (2.4GHz) **Rb (5GHz)**	Green On	AP mode
		Green Blinking	Station mode client connected
		Off	Station mode/radio disabled

2.3 WA512G-D-M2 (DIN-Rail)

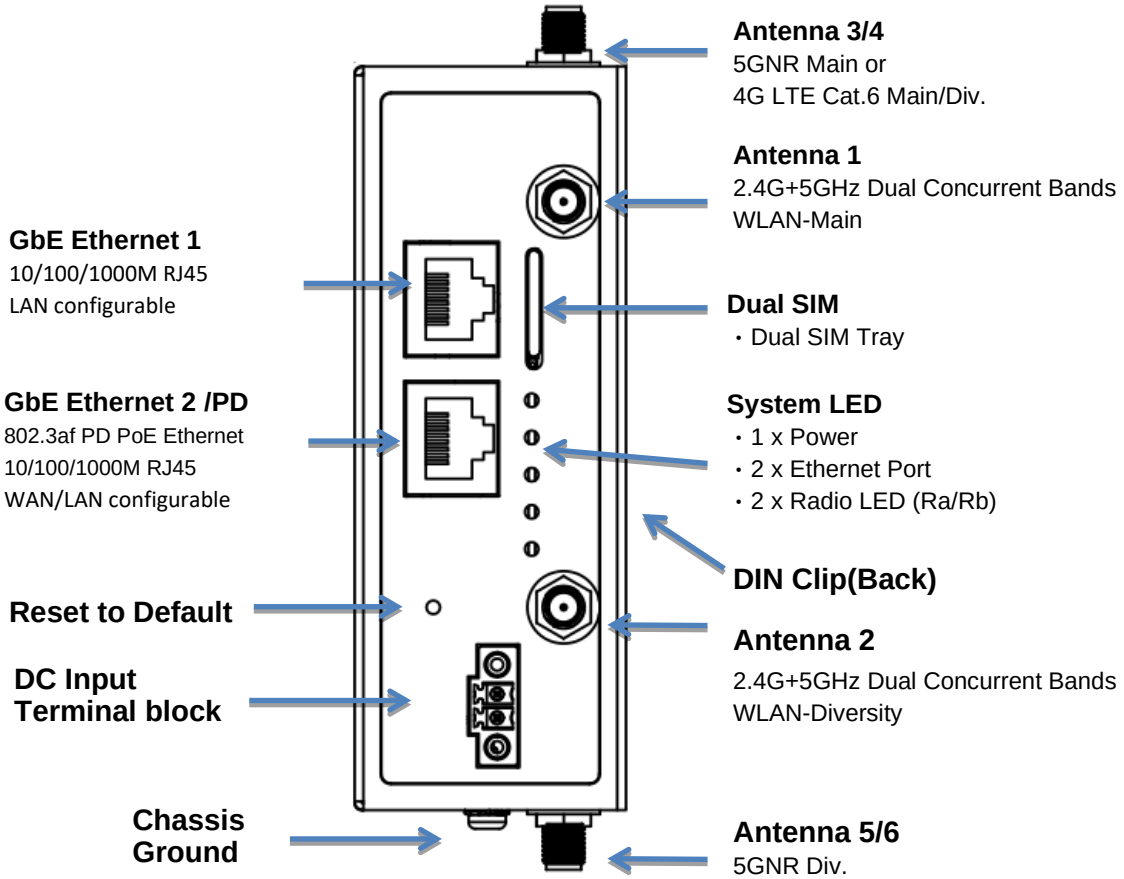
2.3.1 Dimension (WA512G-D-M2)

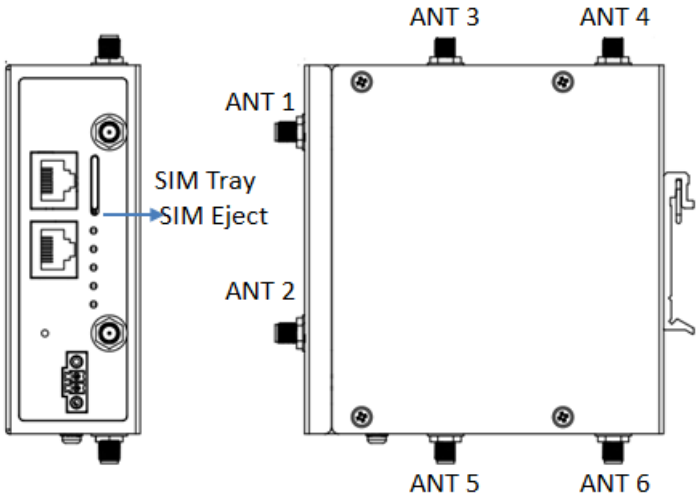
40 x 110 x 107 mm(W x H x D) / without DIN Rail Clip



2.3.2 Product Appearance (WA512G-D-M2)

WA512G/WA512GM-D-M2 (5GNR/4G LTE Cat.6)





Ant	WA512G-D-M2
1	WLAN-Main 2.4/5G Dual Band
2	WLAN-Diversity 2.4/5G Dual Band
3	5GNR Main /4G Main
4	5GNR Main /4G Div.
5	5GNR Div.
6	5GNR Div.

Note: Ant. 3/4/5/6 SMA and RF Cable are pre-assembled.

User must connect to the correct antenna pin-count on the 5GNR/LTE module.

2.3.3 Product Package (WA512G-D-M2)

Standard package:

Model Name	Package
WA512G-D-M2/ WA512GM-D-M2	1x Product Unit
	1x Quick Installation Guide
	2x WLAN Antenna, White The Antenna supports 2.4G/5G wide range. Attached them to ANT1 and ANT2 sockets.
	1 x SIM Eject Pin Pack
Expansion Module	**Package**
WM-5GNR-M2Q-E Kit	1x 5GNR M2 Module and Screw (EU Bands)
	1x Quick Installation Guide
	4x 5GNR Antennas
	Heat Pad/Sink
WM-LTE6-M2Q-E Kit	1x 4G_LTE Cat6 M2 Module and Screw (EU Bands or Other)
	1x Quick Installation Guide
	2x LTE Antennas
	Heat Pad/Sink

Note: The model doesn't offer PoE injector. If you need additional PoE injector or PoE switch, check with our sales contact window.

2.3.4 Interface Installation (WA512G-D-M2)

After unpacking the box, follow the steps below in order to properly connect the device.

2.3.4.1 Wiring Power Input

The WA512G-D-M2 supports DC terminal block with 24V(9~50V) DC input. The typical power input voltage is 24VDC. Wire the power positive(+) and native(-) correctly before turn on the power supply.

WA512G-D-M2 also supports standard IEEE 802.3af PoE Power Device (PD), it can be powered by PoE switch (P.S.E) or PoE injector. However, considering the high power consumption of Cellular M2 module, the power capacity of PoE input may not be enough to boot up the Cellular M2 module. We request using DC terminal input instead of the PD input.

Wiring the Power Input through DC Terminal Block

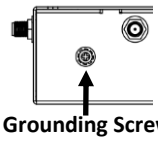
1) Insert the positive and negative wires into the V+ and V- contact on the terminal block connector.

2) Tighten the wire-clamp screws.

3) Connect the power wires to suitable DC Switching type power supply. The input DC voltage should be in the range of the spec.

2.3.4.2 Wiring the Ground

The chassis grounding screw is located on the bottom side of the router. For avoiding system damage by noise or electric shock, establish a direct connection between the ground screw and the grounding surface prior to connecting devices.



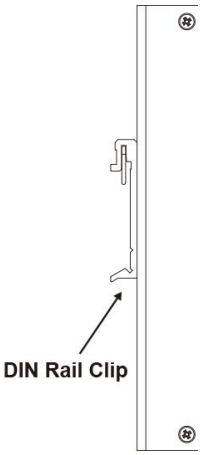
Grounding Screw on the bottom

2.3.5 Mounting the AP

You can mount the AP by attached Din-Rail Clip or Wall-mount by optional wall-mount plate.

2.3.5.1 DIN-Rail Mounting

The EN50022 DIN-Rail plate should be already attached to the back panel of the device screwed tightly. If user needs to reattach the DIN-Rail attachment plate to the device, make sure the plate is situated towards the top, as shown by the following figures.



To mount the router on DIN Rail track, do the following instruction:

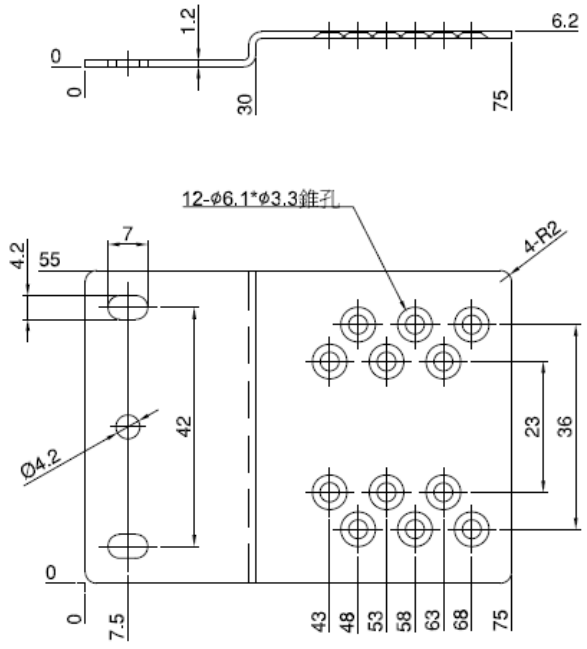
1. Insert the top side of DIN Rail track into the slot of DIN Rail clip.
2. Lightly clip the bottom of DIN-Rail to the track and make sure it attached well.
3. To remove the device from the track, reverse the steps.

2.3.5.2 WALL Mounting

Optional Wall-mount Plate, MK-D1-2:

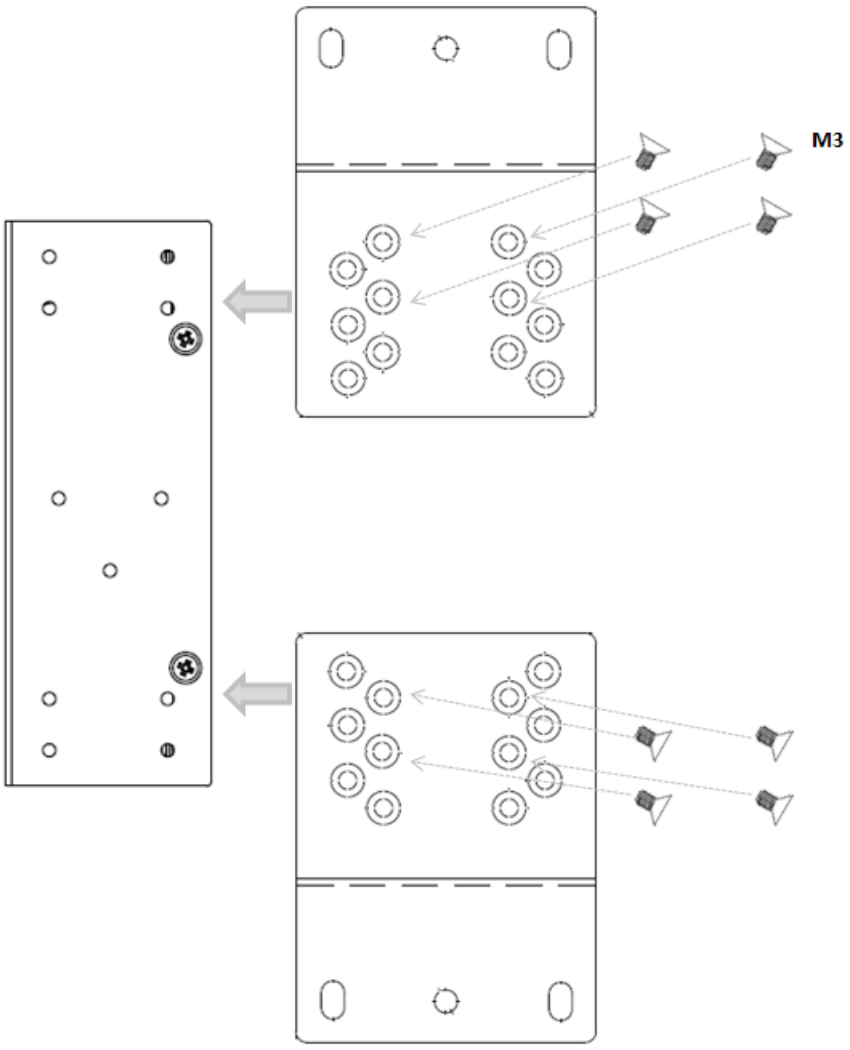
Name	Specification
MK-D1-2	WALL-MOUNTING KIT WITH 2 PLATES AND 8 SCREWS
DP210 WALL MOUNT PLATE	2pc DP210 WALL MOUNT PLATE, PANTON BLACK (Or other color by request)
Flat head M3 screw	8pcs Flat head screw, M3, length 6MM, nickel plated
Packing material, zipper bag No3	Packing material, zipper bag No.3, 70(W)x100(L)MM for SCREW
Packing material, zipper bag No.6	Packing material, zipper bag No.6, 120(W)x170(L)MM for All

MK-D1-2 Dimension:



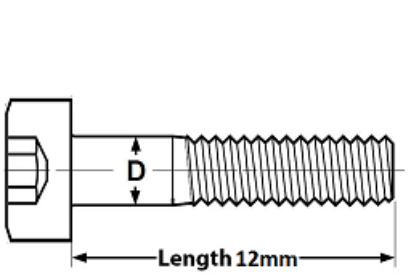
To mount the AP to the WALL/BOX, do the following instruction:

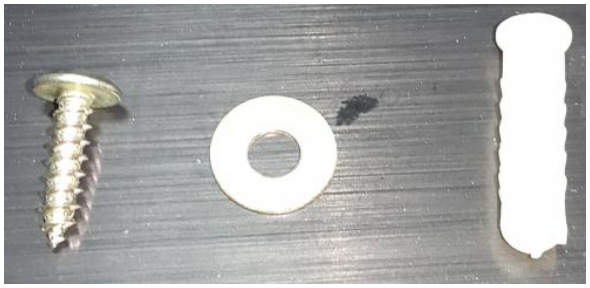
1. Remove the attached DIN Rail Clip first.
2. This wall-mount plate can be shared with our switch or router. For WA512GM-D, please use the 6 screw holes near the inside.
3. Lock the wall-mount plate by the attached “M3” 6mm length screw to the device.



4. Lock the wall-mount plate to the WALL. The suggested screw size for wall-mount is M6 12mm length. (This screw varies from site to site, we do not attach it.)

Reference Wall-mount screw: M6 12mm





2.3.6 ANTENNA & LED (WA512G-D-M2)

WA512GM/WA512G-D-M2 Antenna:

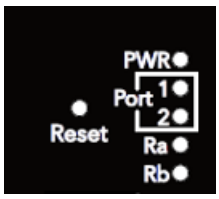
The router supports 2 antenna sockets for WLAN. ANT1 is primary antenna and should be installed when only 1 antenna installed. Install ANT1/2 for the best performance.

The router supports up to 4 antenna sockets for 5GNR/4G cellular. The antenna 3/4/5/6 SMA connectors with Cable are pre-assembled. User must connect to the correct antenna pin of the 5GNR/LTE module. The definition of the antenna is listed in below table.

	WA512GM-D	WA512GM-D-M2
ANT 1	WLAN-Main 2.4G+5GHz Dual Band	WLAN-Main 2.4G+5GHz Dual Band
ANT 2	WLAN-Diversity 2.4G+5GHz Dual Band	WLAN-Diversity 2.4G+5GHz Dual Band
ANT 3	-	5GNR Main /4G Main
ANT 4	-	5GNR Main /4G Div.
ANT 5	-	5GNR Div.
ANT 6	-	5GNR Div.

The attached 5GNR / 4G LTE antenna specification is listed in next page.

WA512GM/WA512G-D-M2 LED:



LED	Status	Description
Power	Green On	Power On
	Off	Not Receiving Power
Port 1/2	Green On	Link
	Green Blinking	Activity
Ra(WLAN)	Green On	Dual WLAN Enabled, 2.4GHz + 5GHz
	Green Blinking	Single WLAN Enabled, 2.4GHz or 5GHz
	Off	Disabled
Rb(Cellular)	Green On	Cellular Turn On/ Capable of Transmitting
	Off	Cellular Turn Off/ Incapable of Transmitting

WiFi Antenna

WA512GM-D-M2 Series supports Dual Band in One Antenna socket design, it is the same as WA512GM-D series.

It means one antenna can transmit dual band dual radio signal, you should choose Dual Band antenna. Connect the attached dual band antenna to the SMA connector on the front panel. Alternatively, you can connect the antenna through extended RF cable with antenna holder to SMA on the front panel and screwing the antenna holder on the field box. The magnet holder is also popular for metal box installation.

Major Specification of attached antenna:

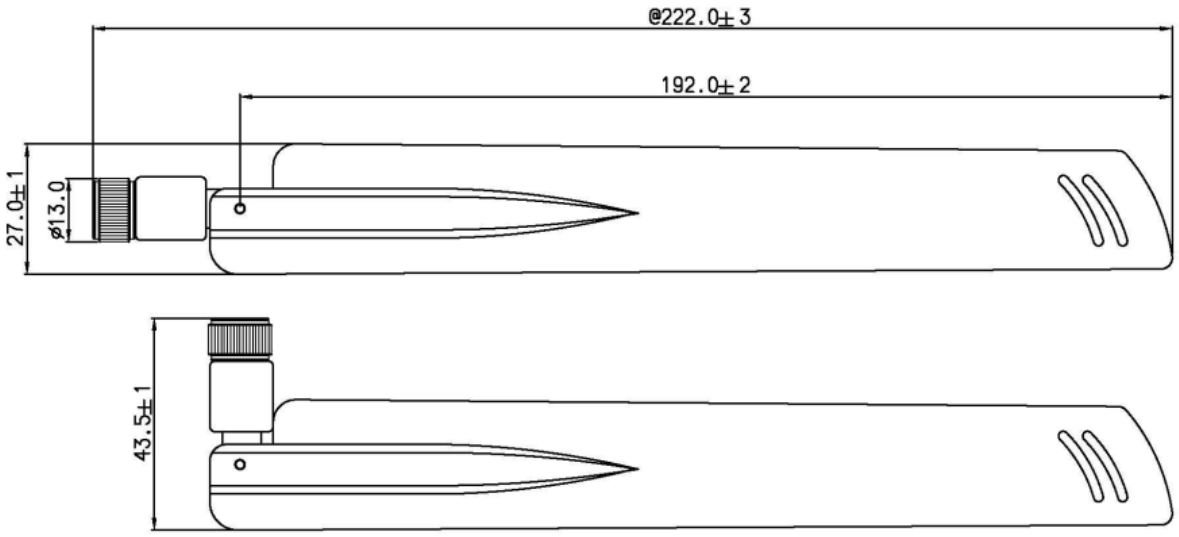
Frequency	2400 ~ 2500 MHz 5150 ~ 5850 MHz
S.W.R	<= 2.0 @ 2400 ~ 2500 MHz <= 2.0 @ 5150 ~ 5850 MHz The data is tested with 1M cable
Peak Gain (Max.)	1.92 dBi @ 2450 MHz 3.4 dBi @ 5150 MHz
Efficiency	70 % @ 2400 ~ 2500 MHz 85 % @ 5150 ~ 5850 MHz
Polarization	Linear
Impedance	50 Ohm
Connector Type	SMA Male Reverse
Operational Temperature	- 40 °C ~ +65 °C

Cellular Antenna

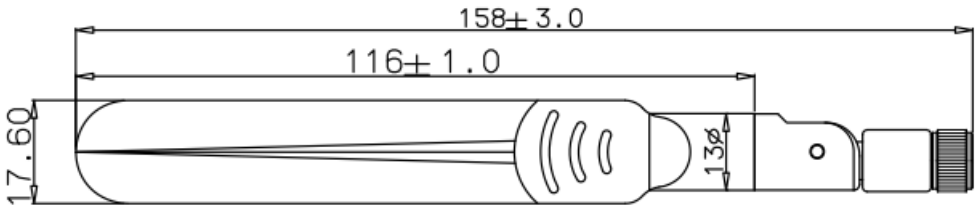
WA512GM-D-M2 Series supports optional 5GNR/ 4G LTE Module kit. There are 2~4 attached antennas within the module kit. The 5GNR antenna support wide frequencies. It includes 3.3G~5GHz which is not used in 4G connectivity, so that it can backward compatible with 4G connectivity. Below table shows the detail specification.

Cellular 5GNR Antenna	
Cellular 5GNR Default Antenna	**Frequency:** 700~5000 MHz
	Peak Gain: 4.12dBi @ 3500MHz 690~960MHz: 0.73~3.04dBi, 1700~1900MHz: 2.2~3.11dbi, 3300~3800MHz: 4.12~5.95dBi, 4000~5000MHz: 3.16~5.97dbi
	Direction: Omni
	Connector: SMA Male
	Dimension: 220x27mm Φ13mm

Dimension:



Cellular 4G LTE Antenna	
Cellular 4G LTE **Default Antenna**	**Frequency:** 690~960/1710~2700 MHz
	Peak Gain: 3.15dBi 690/960MHz: 1.36/1.37dBi, 1700/1800/1900MHz: 3.12/1.29/2.63dbi, 2100/2170MHz: 1.47/1.14dBi, 2500/2600/2700MHz: 3.15/2.46/1.89dbi
	Direction: Omni
	Connector: SMA Male
	Dimension: 158x17.6mm Φ13 mm



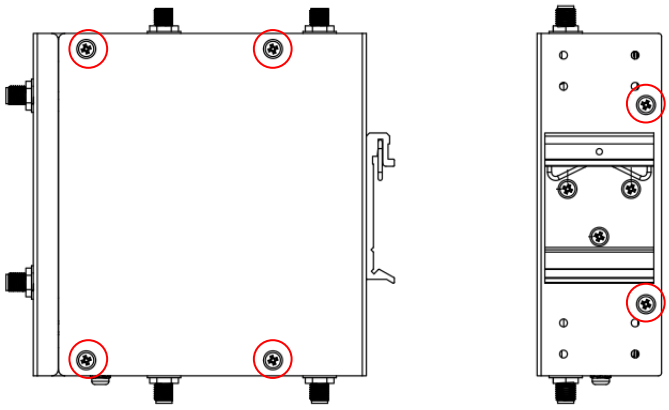
Note: If the alternate antenna are used due to shortage, please refer to the actual antenna specifications.

2.3.7 Install M2 Module (WA512G-D-M2)

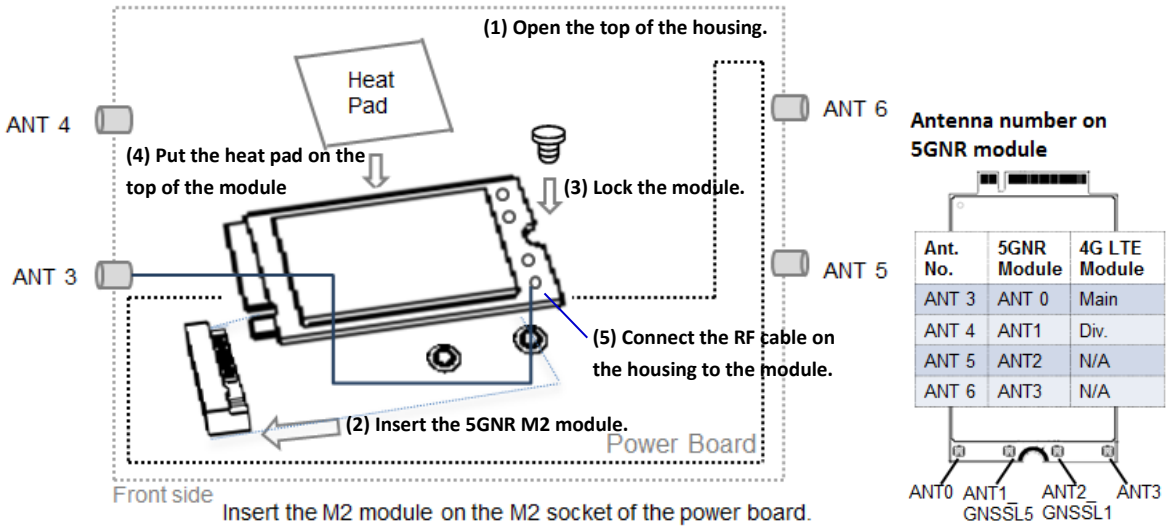
The router allows you to install Cellular M2 module to have 5GNR/4G LTE connectivity. However, the router does Not support all kinds of 5GNR/4G LTE M2 module, the firmware version and dual SIM design may not the same. And you also need screw, antenna pin map, heat sink/pad for installation. **Please purchase the Module Kit from us, it provides cellular module, screw, heat pad/sink and antennas.**

Install the M2 Module and RF cables

1) Open the housing & prepare the M2 module.
   Remove the below 6 screws to open the housing.

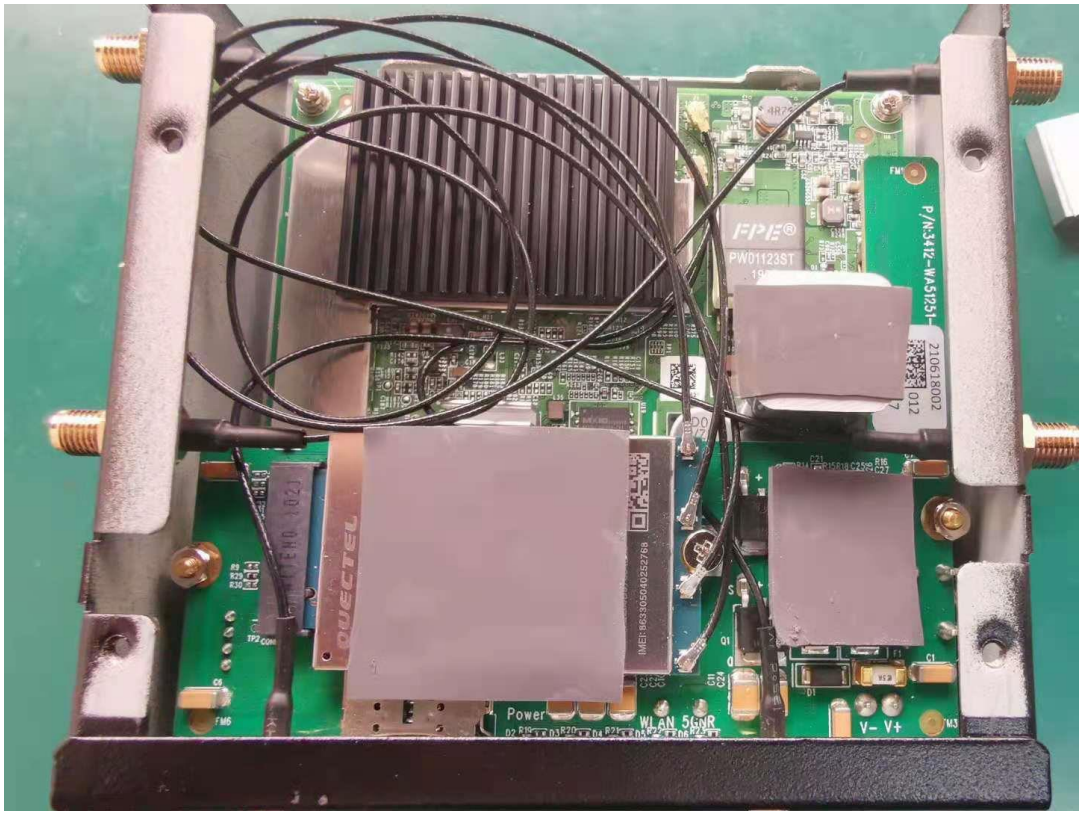


2) Insert the 5GNR module into the M2 socket which is located on the power board.
3) Lock the module with the attached screws.
4) Put the attached heat pad (30x30mm) on the top of the 5GNR/LTE Cat.6 module.
5) Connect the Radio cable on the housing to the cellular module. Ex: ANT 3 on the housing to the Ant 0 of the 5GNR module.
6) Close the housing and please notice the heat pad on the module/board must correctly touch the heat sink of the housing.

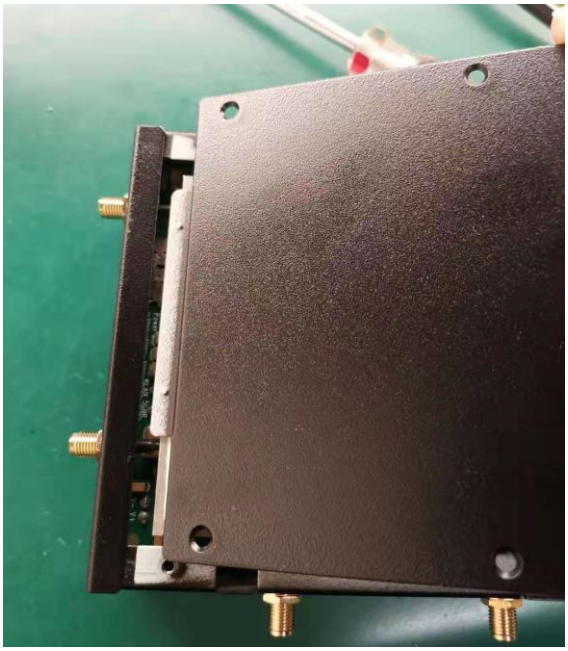


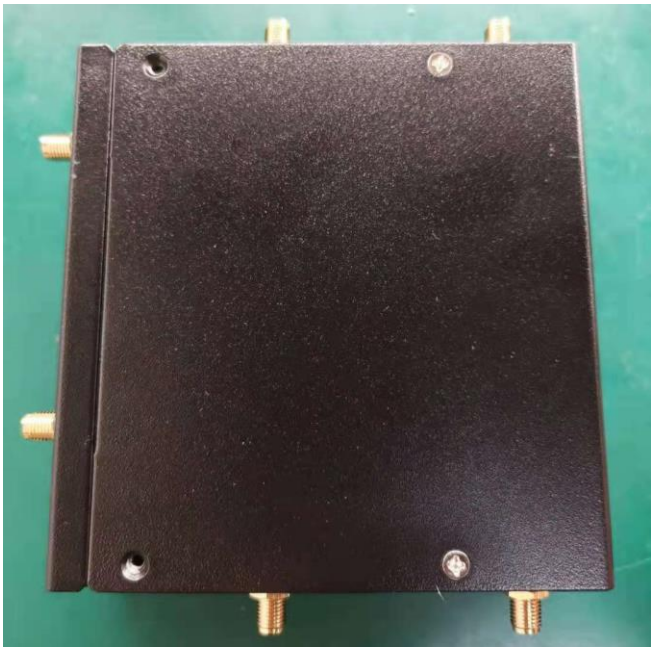
Ant. No.	5GNR Module	4G LTE Module
ANT 3	ANT 0	Main
ANT 4	ANT1	Div.
ANT 5	ANT2	N/A
ANT 6	ANT3	N/A

Below photo shows the Cellular M2 module, heat pad and antenna cables are well assembled.



Close the housing after assembled. Please note the heat sink on the back and top of the housing must properly contact the heat pad on the main device. Then it can have better heat dissipation capability.





2.3.8 SIM (WA512G-D-M2)

Insert SIM

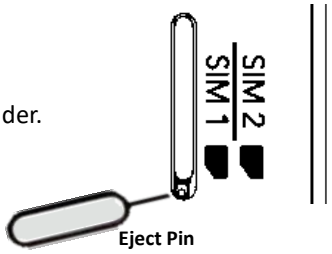
The router equips a dual SIM tray holder for Nano SIM (4FF) cards.

1) Remove the SIM tray holder by the attached SIM eject pin carefully.

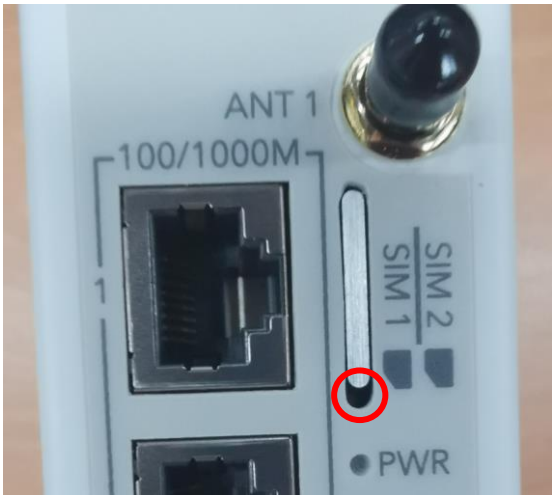
2) The default SIM is SIM 1, put the main carrier's SIM card on SIM 1 of the tray holder.

If the module doesn't support dual SIM, please insert the SIM card on SIM 1.

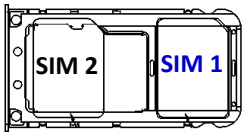
3) Pull the SIM tray holder carefully inside the router again.



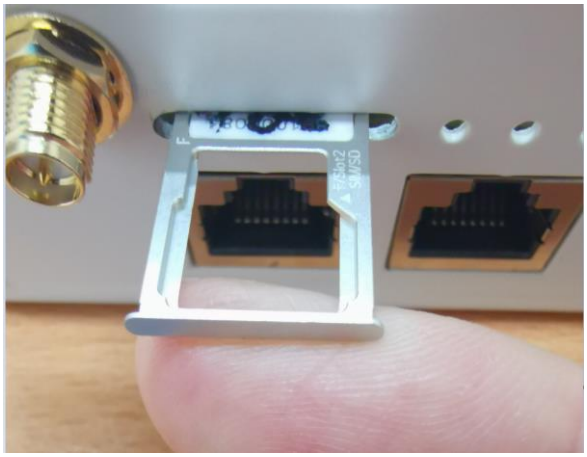
SIM Slot & Attached SIM Pin



SIM Tray Holder



SIM Tray holder



⚠ **Caution:** Disconnect power before ejecting the SIM tray.

Eject SIM tray carefully and Ensure that the SIM card is installed correctly.

Note: The router does Not support all kinds of 5GNR/4G LTE M2 module, the firmware and dual SIM design may not the same. Some of the cellular modules do not support dual SIM. If the cellular doesn't support dual SIM, please insert your SIM card on SIM 1. Please check the available 5GNR/4G LTE module with dual SIM with our sales.

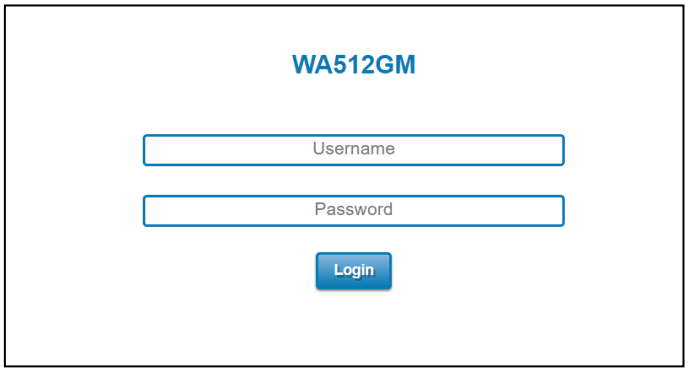
3. Web Management Configuration

To access the management interface, WoMaster router has two ways access mode through a network; they are web management and telnet management. Web interface management is the most common way and the easiest way to manage a network, through web interface management, a router interface offering status information and a subset of device commands through a standard web browser. If the network is down, another alternative to access the management interface can be used. The alternative way is by using telnet management which is offer configuration way through CLI Interface. This manual describes the procedures for Web Interface and how to configure and monitor the managed router only.

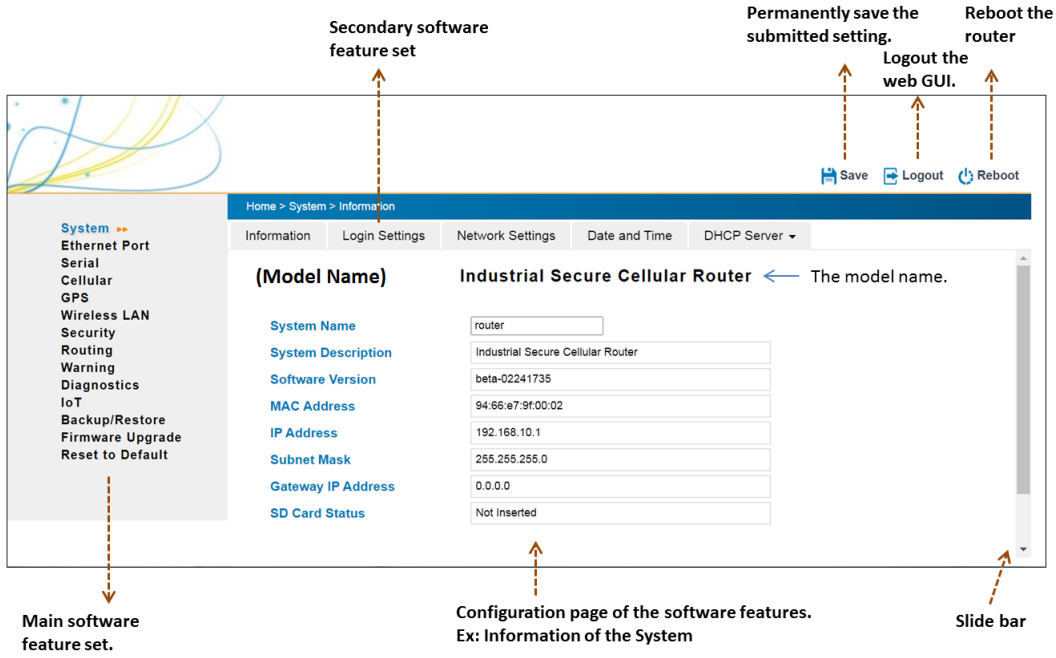
PREPARATION FOR WEB INTERFACE MANAGEMENT

WoMaster provides Web interface management that allows user through standard web-browser such as Microsoft Internet Explorer, or Mozilla, or Google Chrome, to access and configure the router management on the network.

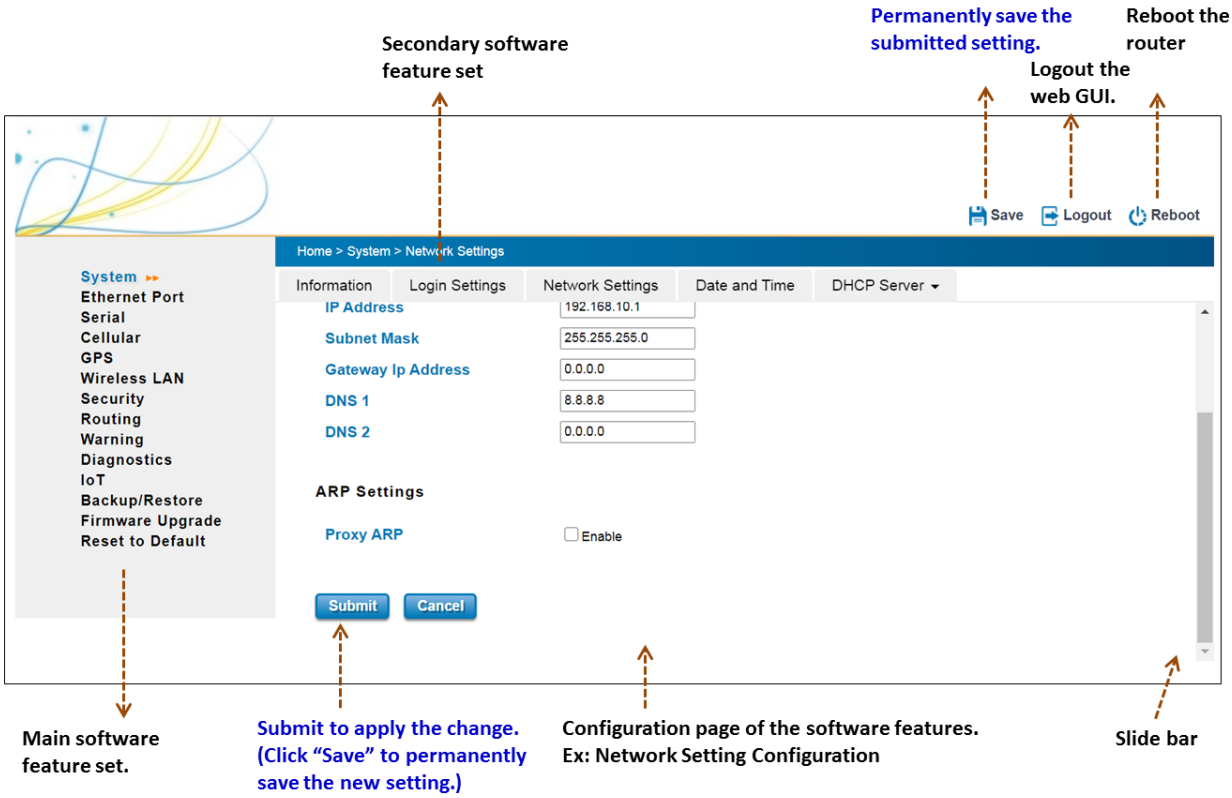
1. Plug the DC power to the router and connect router to computer.
2. Make sure that the router default IP address is **192.168.10.1**.
3. Check that PC has an IP address on the same subnet as the router. For example, the PC and the router are on the same subnet if they both have addresses that start 192.168.10.x (Ex: **192.168.10.2)**. The subnet mask is 255.255.255.0.
4. Open command prompt and ping **192.168.10.1** to verify that the router is reachable.
5. Launch the web browser (Internet Explorer or Mozilla Firefox or Google Chrome) on the PC.
6. Type **http://192.168.10.1** (or the IP address of the router). And then press **Enter** and the login page will appear.
7. Key in the **NEW User name and Password** in login screen while first Login. (There is no default user name and password for Security concern)
8. After you click OK, the Welcome page of the web-based management interface will appear.
9. On the left side you can see the list of software features, on the right side – available settings.



Web GUI Console Example 1: System Information



Web GUI Console Example 2: Network Setting Configuration. Click "Submit" to apply the change. **Click "Save" to save the new setting permanently, the setting will be remained after reboot.**



In this Web management for Featured Configuration, user will see all of WoMaster Router's various configuration menus at the left side from the interface. Through this web management interface, user can configure, monitoring, and set the administration functions. The whole information used web management interface to introduce the featured functions. User can use all of the standard web-browser to configure and access the router on the network.

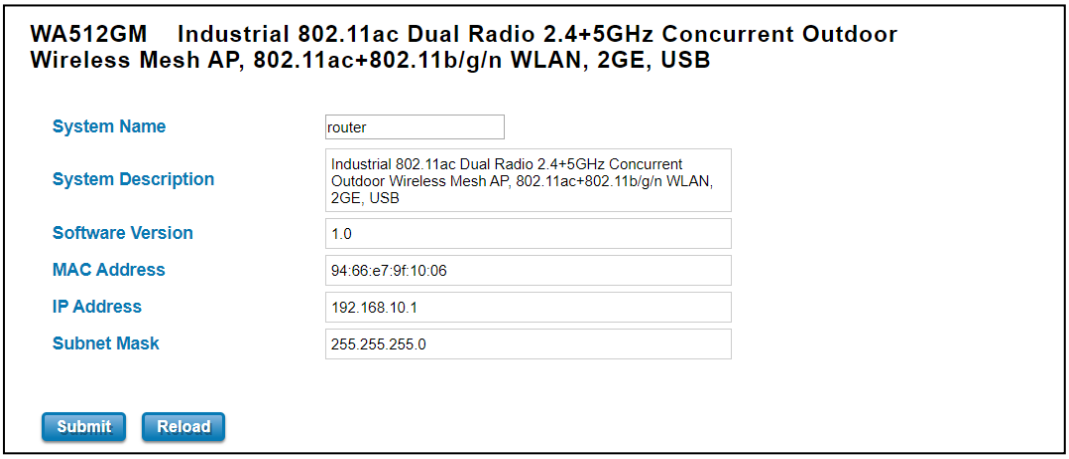
Following topics are covered in this chapter:

3.1 System

When the user login to the router, user will see the system section appear. This section provides all the basic setting and information or common setting from the router that can be configured by the administrator.
Following topics are included:

3.1.1 Information

Information section, this section shows the basic information from the router to make it easier to identify different router that is connected to User network and also it shows LAN Settings information. The figure below shows the interface of the Information section.

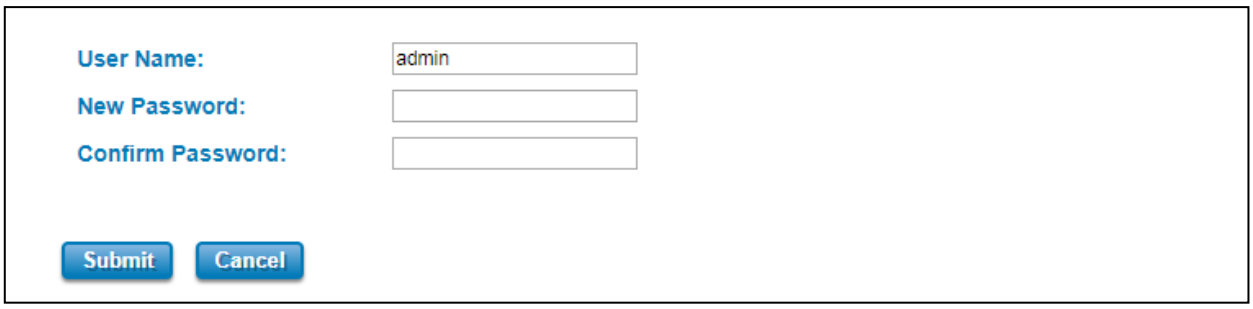


The description of the Information's interface is as below:

TERMS	DESCRIPTION
System Name	**Default: router** Set up a name to the device.
System Description	Display the name of the product.
Software Version	Display the firmware latest version that installed in the device.
MAC Address	Display the hardware's MAC address that assigned by the manufacturer.
IP Address	Display the IP Address of the device
Subnet Mask	Display the subnet mask of the device

3.1.2 Login Settings

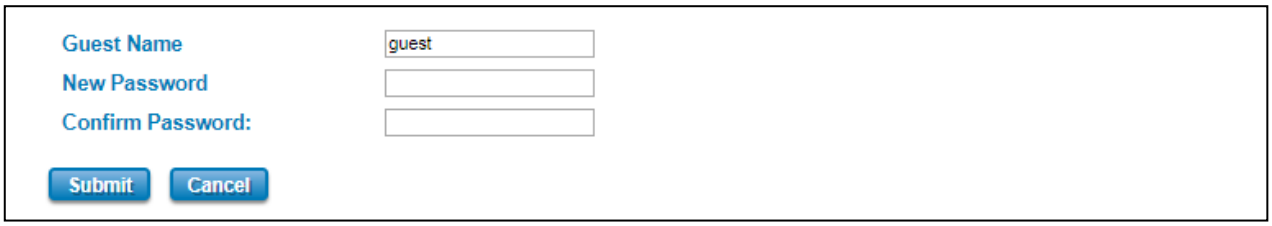
WoMaster' router supports Login Setting that has several authentication methods. It is supported with TACACS+, Radius, and Multi-User Authentication. This Login Setting consists of two level, admin and guest. Where the admin level, it has the privilege to read and write and for the guest level the privilege is read only. Below is the **Login Setting** section for **admin level**.



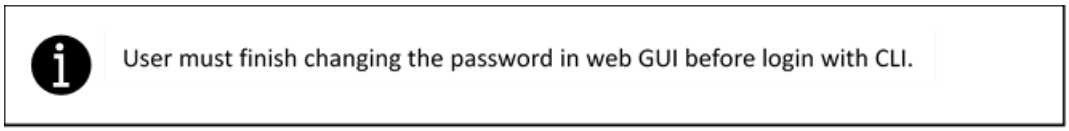
With the Name first login setting is administrator user name level and the authority allow user to configure all of configuration parameters.

The Login Setting interface describes how to configure the system username and password for the web management login. To change the Name and Password, user just needs to input a new Name and New Password then confirm the new password in this section. Try to re-login with the new username and password.

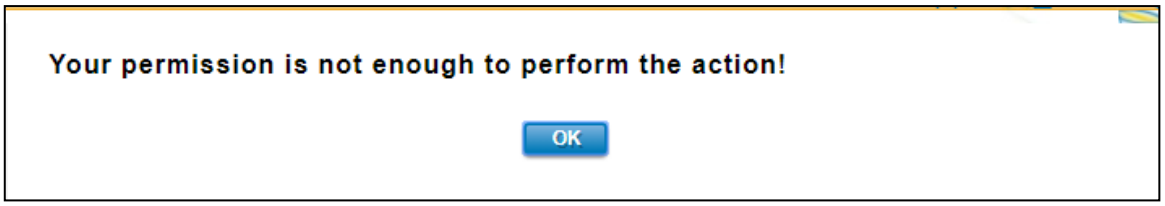
Below is the interface for **guest level**.



With the Name default setting is **guest** and the authority allow user to read only all of configuration parameters.



When user try to change the configuration, message will appear if user is not permitted to configure the configuration. Below is the interface.



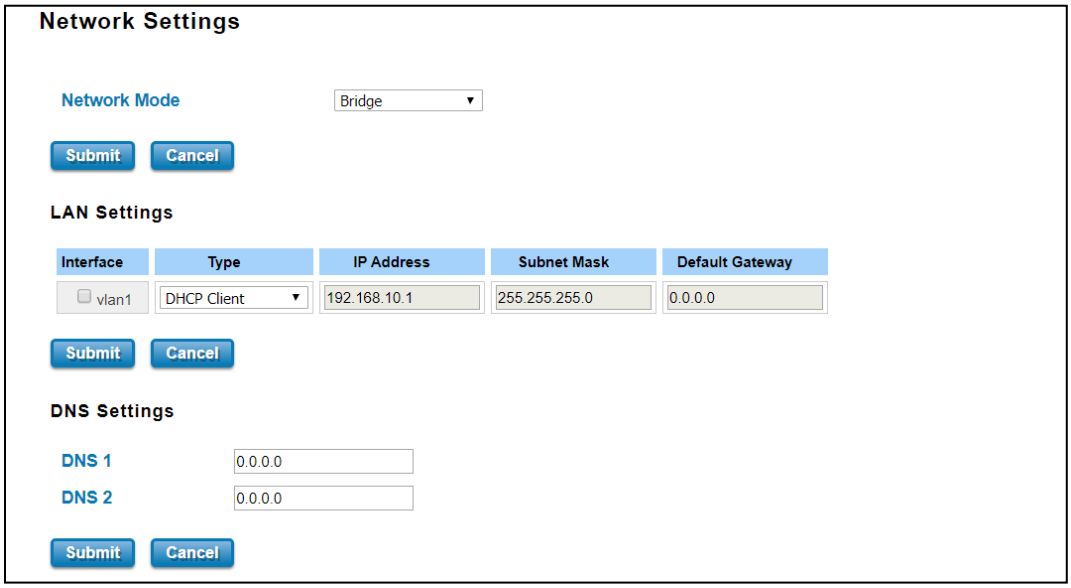
The description of the Login Setting interface is as below:

TERMS	DESCRIPTION
User Name/ Guest Name	**Default: admin/guest** Key in new username here.
New Password	Key in new password here.
Confirm Password	Re-type the new password again to confirm it.

After finishing configure the Username and Password, click on **Submit** to apply the configuration. Don't forget to **Save** the configuration.

3.1.3 Network Settings

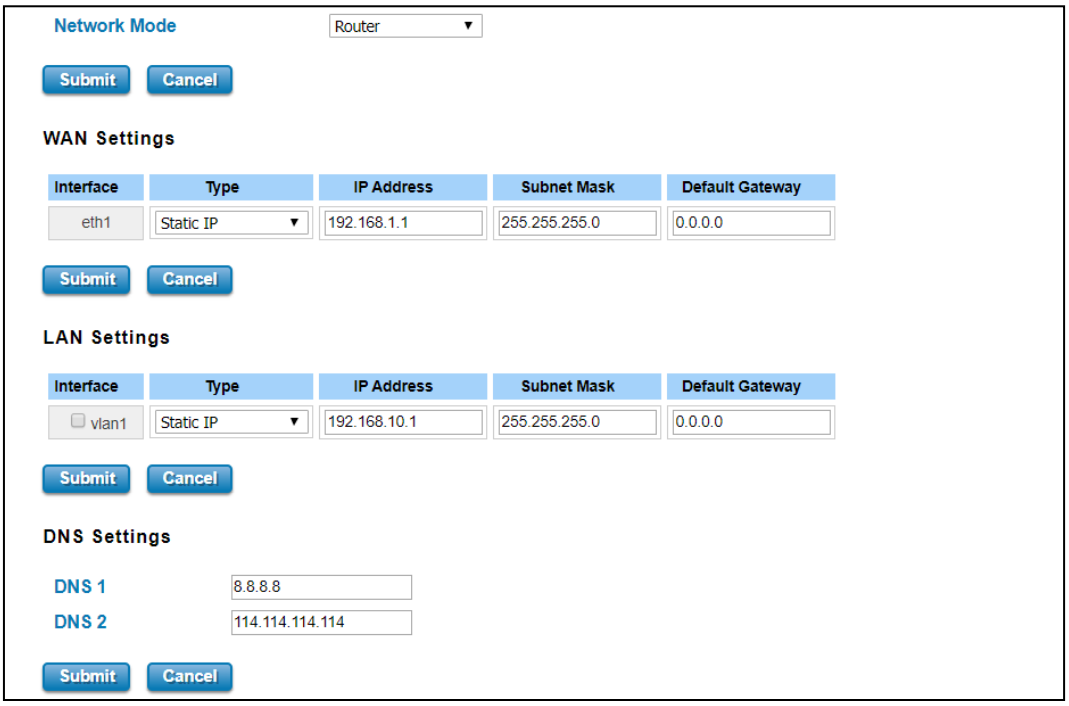
The Network Setting section allows users to configure both IPv4 values for management access over the network. WoMaster' router supports IPv4 and can be managed through either of these address types. Below is the IP Setting interface for **Bridge Mode**.



The description of the columns is as below:

TERMS	DESCRIPTION
Type	User can select to DHCP or Static IP to activate the function. **DHCP:** Select DHCP to activate DHCP Client Function, no need to assign IP Address and received IP Address from DHCP Server. **Static IP:** Select Static IP to configure the IP configuration manually
IP Address	**Default: 192.168.10.1** Set up the IP address reserved by User network for User device. If DHCP Client function is enabled, no need to assign an IP address to device as it will be overwritten by DHCP server and shown here.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here. If DHCP Client function is enabled, no needs to assign the subnet mask.
Gateway IP Address	**Default: 0.0.0.0.** Assign the gateway for the device here.
DNS 1	Specifies the IP address of the DNS server 1 that used in user network.
DNS 2	Specifies the IP address of the DNS server 2 that used in user network.

And below is the IP Setting interface for the **Router Mode w**here it supports with the WAN port on port 2. User can configure the WAN Settings.



The description of the columns is as below:

TERMS	DESCRIPTION
Type	User can select to DHCP Client or Static IP to activate the function. **DHCP Client:** Select DCHP Client to activate DHCP Client Function, no need to assign IP Address and received IP Address from DHCP Server. **Static IP:** Select Static IP to configure the IP configuration manually
IP Address	**Default: 192.168.1.1** Set up the IP address reserved by User network for User device. If DHCP Client function is enabled, no need to assign an IP address to device as it will be overwritten by DHCP server and shown here.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here. If DHCP Client function is enabled, no needs to assign the subnet mask.
Gateway IP Address	**Default: 0.0.0.0.** Assign the gateway for the device here.
DNS 1	Specifies the IP address of the DNS server 1 that used in user network.
DNS 2	Specifies the IP address of the DNS server 2 that used in user network.

3.1.4 Date and Time

The WoMaster router has a time calibration function based on information from an NTP server or user specified time and date, allowing functions such as automatic warning emails to include a time and date stamp.

The description of the columns is as below:

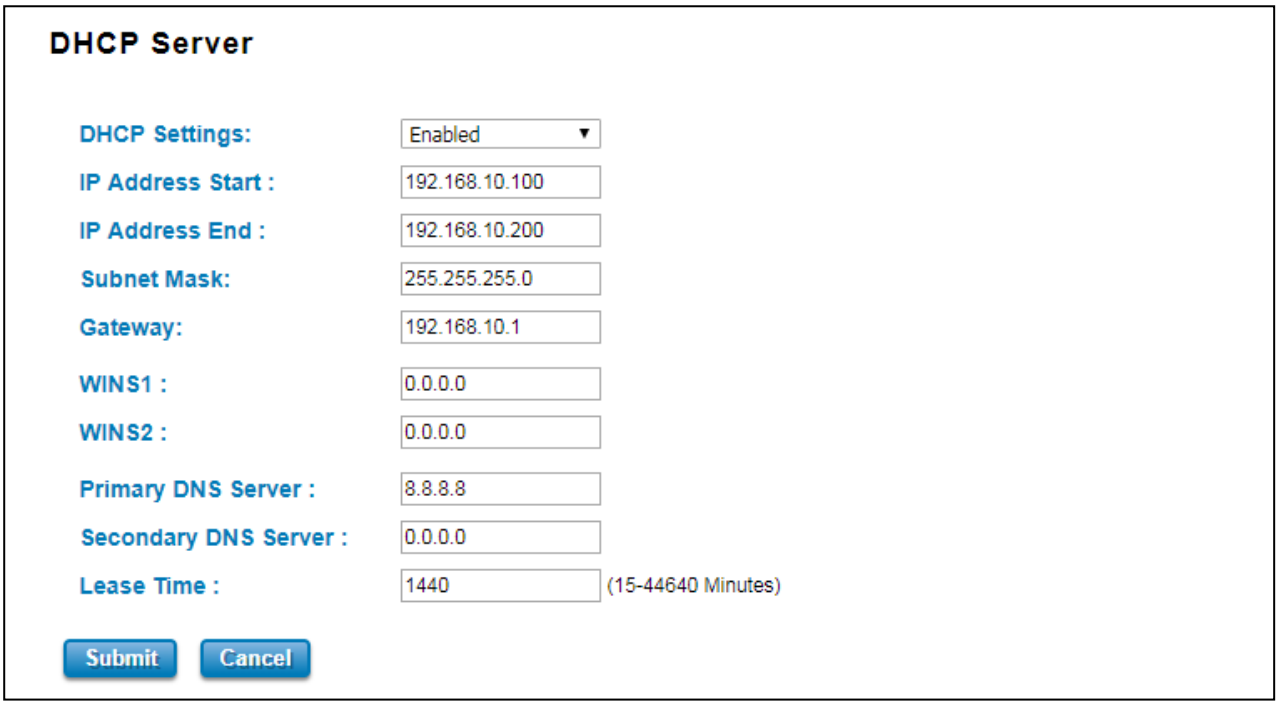
TERMS	DESCRIPTION
Current Time	User can configure time by input it manually. Get PC Time: get the time the PC
Time Zone	Choose the Time Zone section to adjust the time zone based on the user area.
NTP	**Enable NTP Client update** by checking this box. Select the time server from the **NTP Serve**r dropdown list or select **Manual IP** to manually input the IP address of available time server. ***Make sure that the device also has the internet connection.**

After finished configuring, click on **Submit** to activate the configuration.

3.1.5 DHCP Server

DHCP Server Setting

WoMaster router has DHCP Server Function that will provide a new IP address to DHCP Client. After enabling DHCP Server function, set up the Network IP address for the DHCP server IP address, Subnet Mask, Default Gateway address and Lease Time for client. Below is the DHCP Server Setting interface



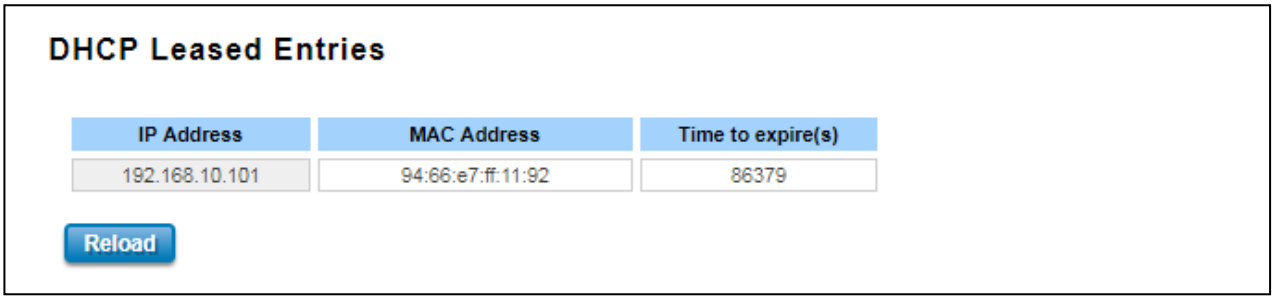
The description of the columns is as below:

TERMS	DESCRIPTION
DHCP Setting	Select to **Enable** or **Disable** to activate and deactivate DHCP Server function.
IP Address Start	Assign the IP Address Start range.
IP Address End	Assign the IP Address End range.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here for DHCP Server.
Gateway	Assign the gateway for the router here for DHCP Server.
WIN S1	Enter WINS Server 1 IP address
WIN S2	Enter WINS Server 2 IP address
Primary DNS Server	Enter Primary DNS Server that used in user network.
Secondary DNS Server	Enter Secondary DNS Server that used in user network.
Lease Time	**Default: 1440** The maximum length of time for the IP address lease. Enter the Lease time in minutes. (Lease Time range: 15-44640 minutes)

The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set user computers to be DHCP clients by setting their TCP/IP settings to “Obtain an IP Address Automatically.” When user turns the computers on, they will automatically load the proper TCP/IP settings provided by the router. If User manually assigns IP addresses to User computers or devices, make sure the IP addresses are outside of this range or User may have an IP conflict. After finished configuring, click on **Submit** to activate the configuration.

DHCP Leased Entries

The figure below shows the **DHCP Leased Entries.** It will show the MAC and IP address that was assigned by router. Click the **Reload** button to refresh the list.



The description of the columns is as below:

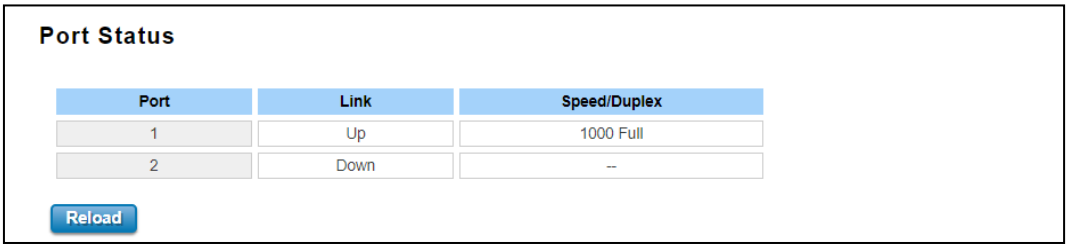
TERMS	DESCRIPTION
IP Address	IP address that was assigned by router.
MAC Address	The MAC Address of the network interface that was used to acquire the lease.
Time to expire(s)	Remains time for the IP address from DHCP Server leased.

3.2 Ethernet Port

Ethernet Port section is used to access the port configuration and rate limit control. It also allows User to view port status and port trunk information.

3.2.1 Port Status

Port Status section allows users to see the current status from the Ethernet.



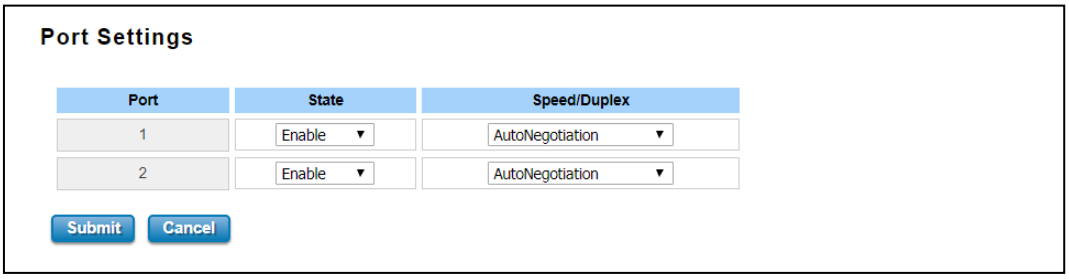
The description of the columns is as below:

TERMS	DESCRIPTION
Link	Display the Ethernet status, whether it is Link Up or Link Down.
Speed/Duplex	**Default: N/A** Show the Speed/Duplex for each port, such as 10 full,10 half,100 full,100 half mode for **Giga Ethernet Port 1~2**

Click on **Reload** to update the information.

3.2.2 Ethernet Setting

Use this page to configure the Ethernet setting.



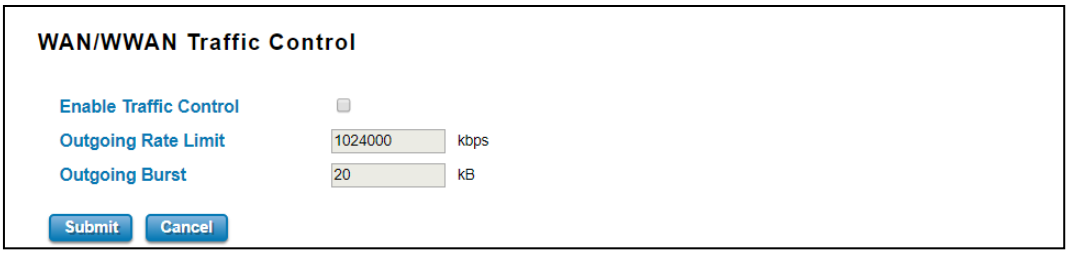
The description of the Ethernet Setting page is as below:

TERMS	DESCRIPTION
State	Enable or disable the port.
Speed/Duplex	**Default: Auto / Auto-Negotiation** Configure the Speed/Duplex of the port Ethernet 1. Users can set the bandwidth of each port as Auto-negotiation, 100 full, 100 half, 10 full, 10 half mode.

Click **Submit** to apply the configuration that just made.

3.2.3 Traffic Control

Traffic control is a form of flow control used to enforce a strict bandwidth limit at a port. User can configure separate Incoming Outgoing rate limits and burst



The description of the columns is as below:

TERMS	DESCRIPTION
Enable Traffic Control	Check the box to activate the function
Outgoing Rate Limit	**Default: 1024000 kbit/s** Set the maximum outgoing rate.
Outgoing Burst	**Default: 20 kBytes** Set the maximum outgoing burst.

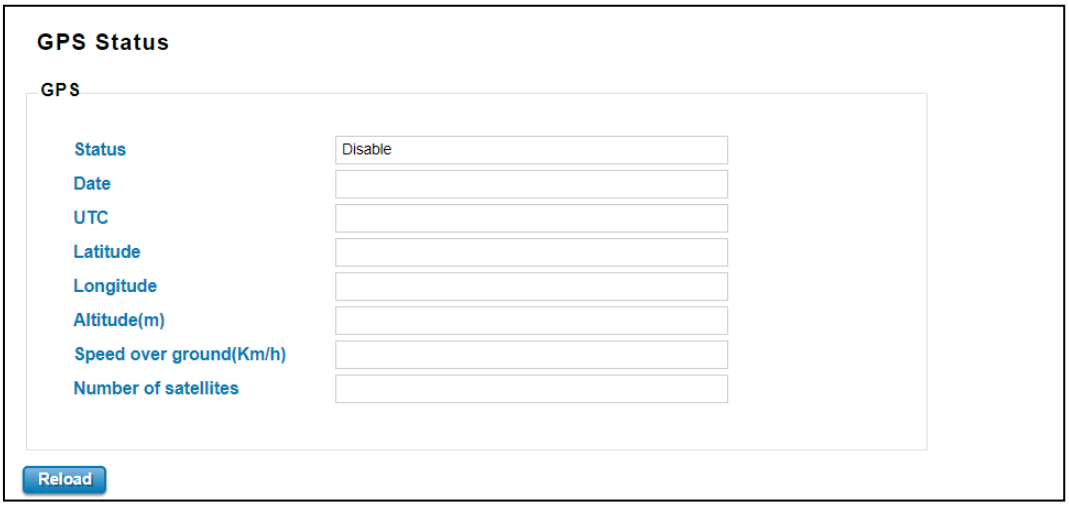
Click on **Submit** to apply the configuration.

3.3 GPS

This GPS section has the function to show the current position of the device. It could help the technician to track the device location.

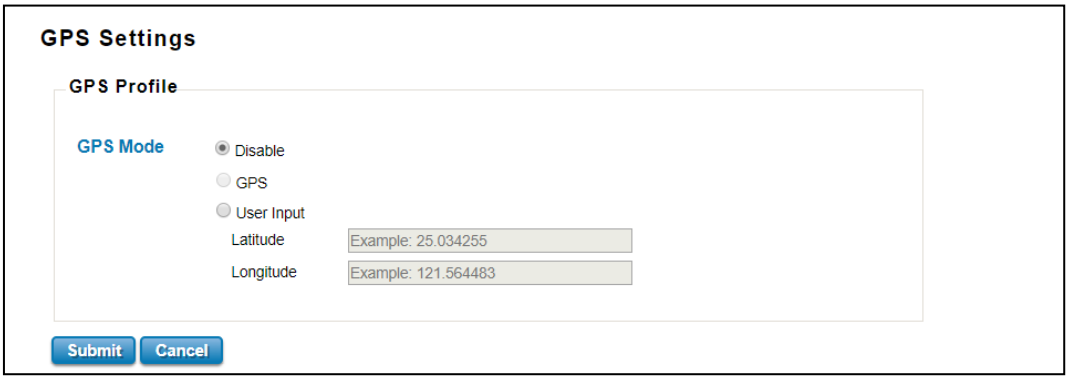
3.3.1 GPS Status

GPS status is always disable since user need to manually input GPS coordinates in GPS settings page.



3.3.2 GPS Settings

In this GPS Setting section, user can manually input GPS coordinates. The coordinates can be used to report to cloud or specific server.



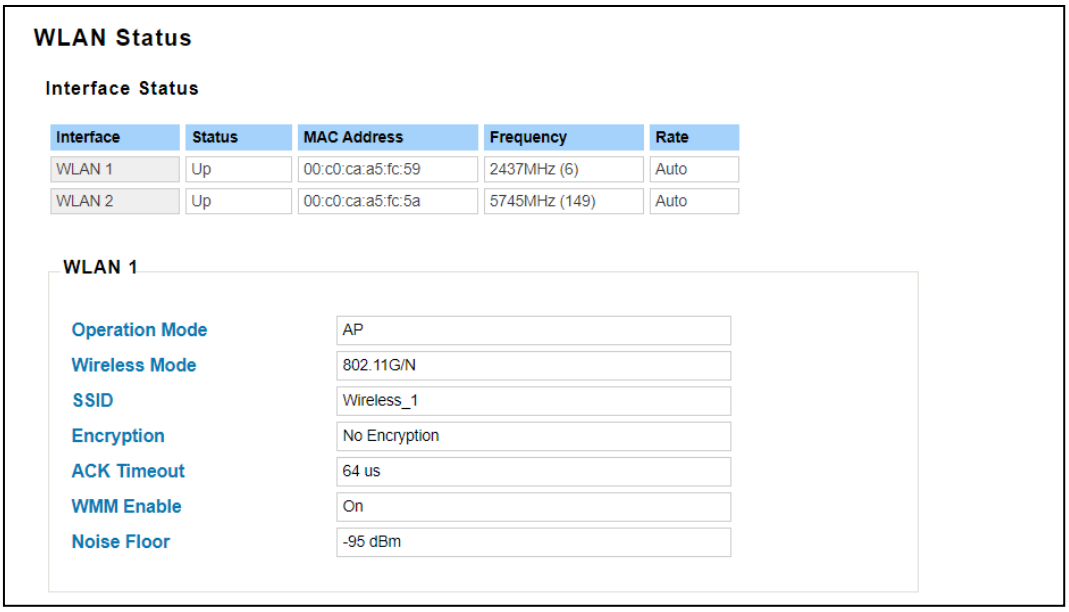
TERMS	DESCRIPTION
GPS mode	**Default: Disable** **Disable**: Disable GPS function. **GPS**: Enable GPS function. WA512G WLAN AP series does not support GPS feature. You can just type Latitude/Longitude through User Input. WA512G-D-M2 with Cellular Module may support GPS features. It depend on the cellular module you install. Contact our salesperson for GPS support. **User Input**: Input Latitude and Longitude. The coordinates can be used to report to cloud or specific server.

3.4 Wireless LAN

This Wireless LAN configuration pages only support the device that supported with Wi-Fi feature. This configuration page allows users to configure the Wireless LAN configuration.

3.4.1 WLAN Status

The figure below shows the WLAN status.



The description of the columns is as below:

TERMS	DESCRIPTION
Operation Mode	Display the current operating modes on the device
Wireless Mode	Display the current wireless mode
SSID	Display the primary name of the SSID
Encryption	Display the encryption mode.
ACK Timeout	The ACK time of wireless beacon packet
WMM Enable	Display the status of the WMM support.
Noise Floor	Display the background noise level.
Description when MESH AP Enabled	
TERMS	**DESCRIPTION**
Mode	MESH AP or RE (Range Extender) mode
SSID	The current SSID of MESH network
WLAN 1 Signal Strength	WLAN 1 Signal in dBm unit
WLAN 1 Status	Connected or Disconnected Status
WLAN 1 Signal Strength	WLAN 2 Signal in dBm unit
WLAN 1 Status	Connected or Disconnected Status

3.4.2 WLAN Settings

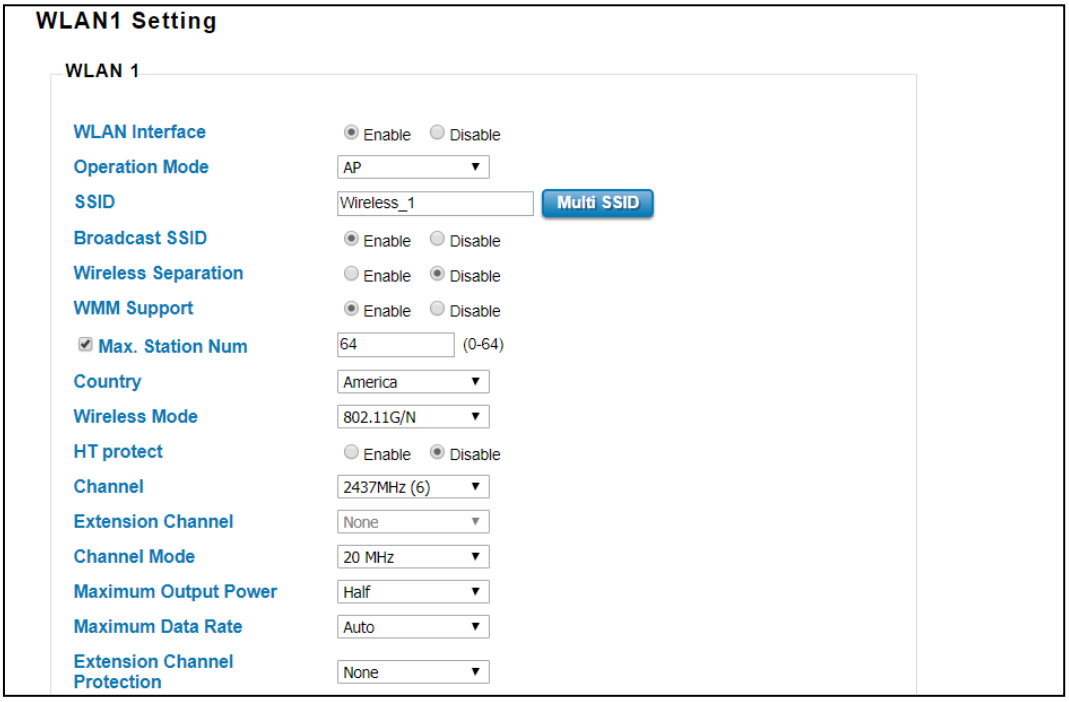
WLAN Setting page, on this page user may configure the parameters for Wireless LAN Interface includes change wireless interface modes and all of the related parameters for each operation mode.

There are 2 WLAN interfaces supported in WA512G series. WLAN1 for 2.4GHz and WLAN2 for 5GHz in AP mode can be configured in the same time. Only one radio can be configured to client mode in the same time.

> Pop up window will be displayed to indicate only one radio can be configured in client mode

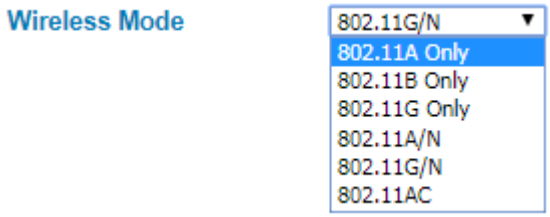
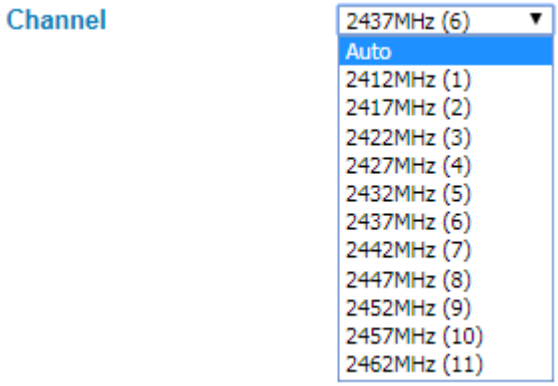
3.4.2.1 AP mode

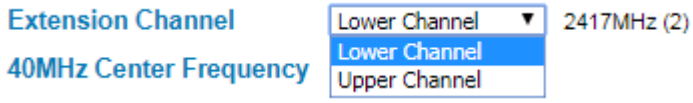
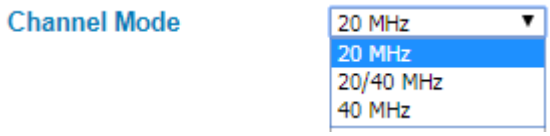
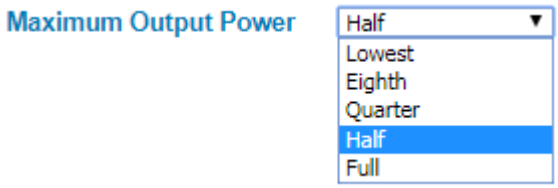
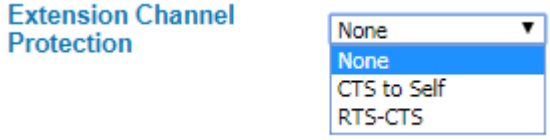
The Access Point mode, it establishes a wireless connection, receive from wireless clients and provide connection for wireless client devices, the client can search and connect to several the access points.



The description of the columns is as below:

TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	**Default: AP** Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: WR322_1** Input the primary name of the access point.
Broadcast SSID	**Default: Enabled.**

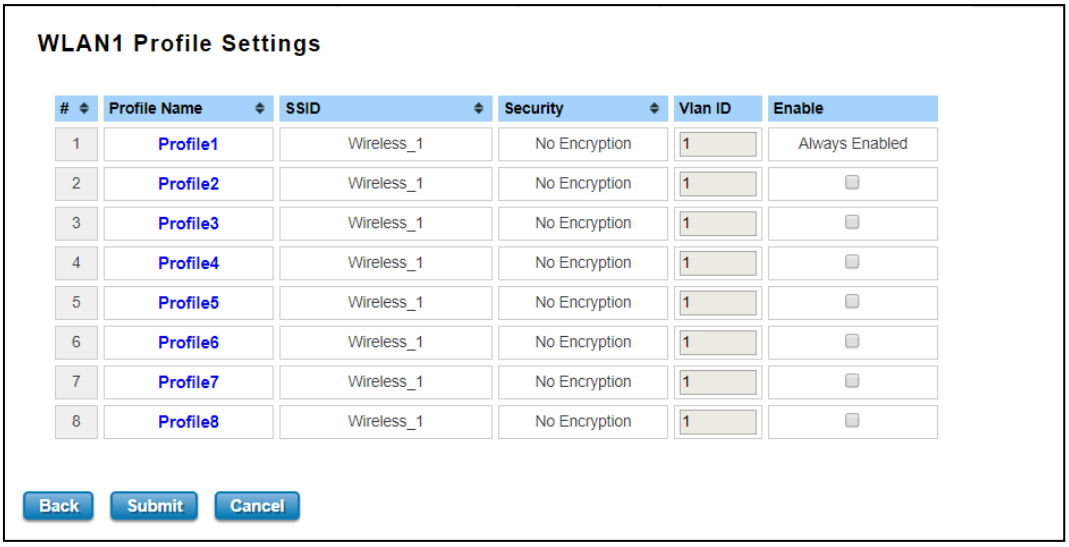
	By enabling the broadcast SSID, it makes the AP can be accessed and searched by the clients, and for the security concern by disabling this broadcast SSID, the network will be hidden in order to prevent any malicious attack.
Wireless Separation	**Default: Disable** By enabling the function, connected clients will be separated and can reach each other (ex: can't ping each other)
WMM support	**Default: Enable** To enable or disable WIFI multi-media QoS.
Max. Station Num	**Default: 64** Specify the maximum number of connected clients
Country	Select your country code for band regulation.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has different configuration. For each wireless mode, it has the specific frequency and it has different basic settings. 
HT Protect	**Default: Disabled** Select Enabled to activate the High Throughput protect to ensure HT transmission with MAC mechanism. (Note: The setting is not support in/after V1.5.x firmware version)
Channel	**Default: 2437MHz (6)** Select the proper channel, each country has different band user may select the channel based on the situation. Or select auto to automatically set the channel. 
Extension Channel	**Default: Lower Channel 2417MHz (2)**

	 This option would be appeared when user select the Channel Mode to 20/40MHz or 40MHz. To put range for the frequency, it provides the Lower Channel (2417MHz (2)) with the 40MHz center frequency is 2427MHz (4) and Upper Channel (2457MHz (10)) with the 40MHz center frequency is 2447MHz (8).
Channel Mode	**Default: 20MHz**  There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequency, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna. 
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate, the access point will automatically select the highest available rate to transmit. User may select the low rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	 Select from the dropdown list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activating this

	function, it may decrease wireless network performance.

Click **Submit** to apply the configuration

At the SSID section, there is a **Multi SSID** button appeared. This AP mode supports the multiple SSID or multiple access point connections. So user may separate the connection into several access points and it is supported with 8 profiles for multiple SSID. Click the button then another form will appear, see the figure below.

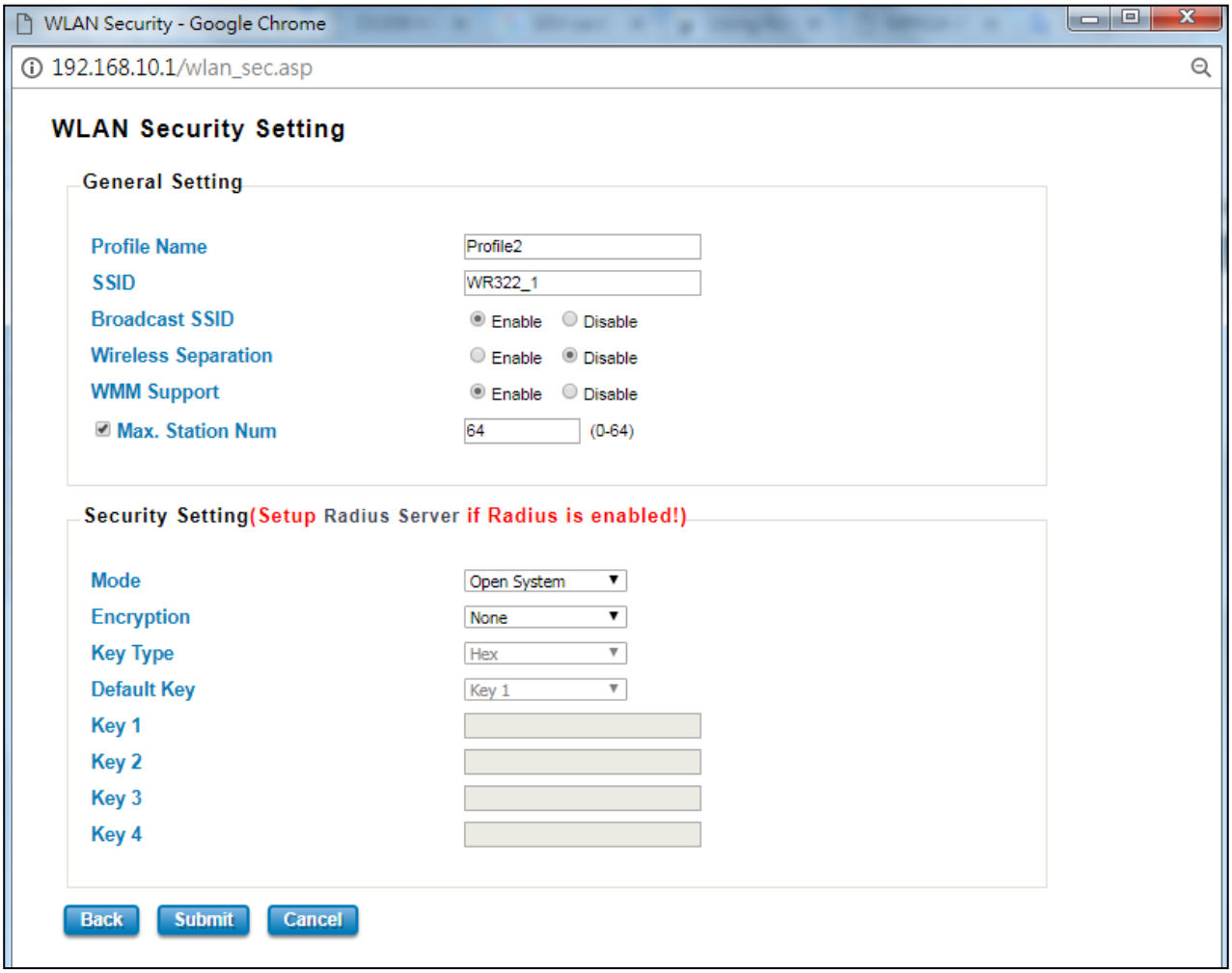


The description of the column is as below:

TERMS	DESCRIPTION
Profile Name	Display the available WLAN Profile name
SSID	Display the SSID Name.
Security	Display the current security mode for the Wireless network
VLAN ID	Display the VLAN ID
Enable	Check the box to enable the WLAN Profile. When user enabled the Profile, user may configure the WLAN Setting by click the Profile name.

Click **Submit** to apply the configuration

The Multi SSID section shows the configuration page where the Profile1 always enabled. In this section, user may configure each Profile by check the box to enable the Profile and then click the profile name to open the configuration page for specific Profile. The figure below is the pop-up WLAN Security configuration page for each Profile. In this configuration page, user can configure the AP profile, divide the AP connection and set the security setting by put the encryption mode and set the key or password to access the AP. Refers to the WLAN Security Section for more description (3.7.3).

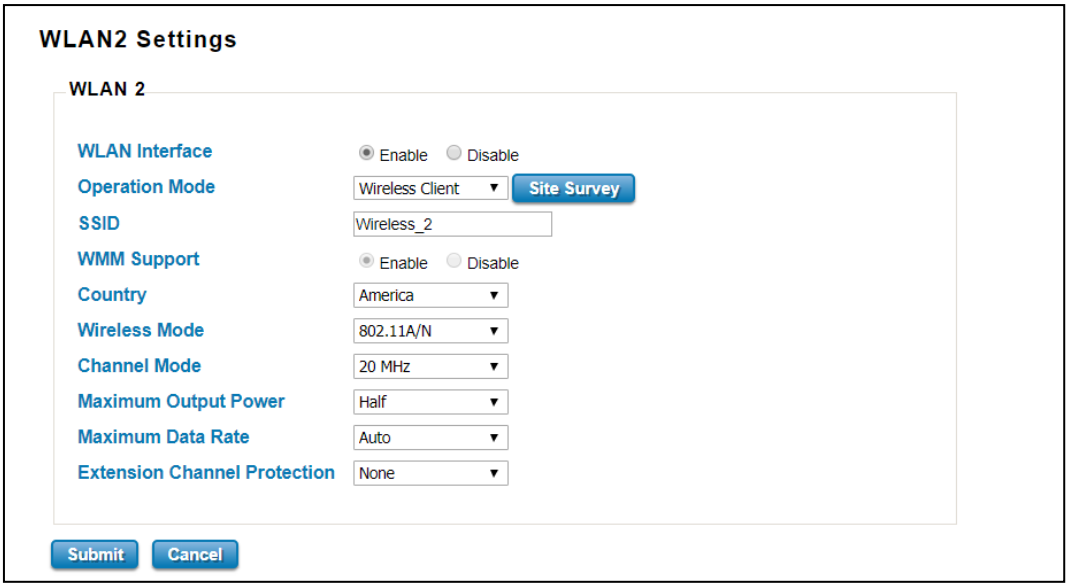


Click **Submit** to apply the configuration

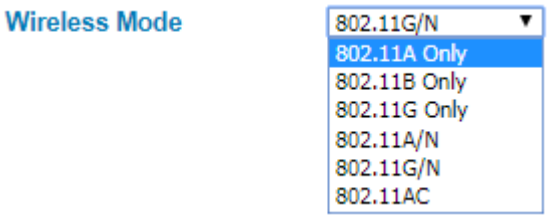
Pop up window may be blocked by browser. Change browser settings to allow pop-up window to configure multi-SSID.

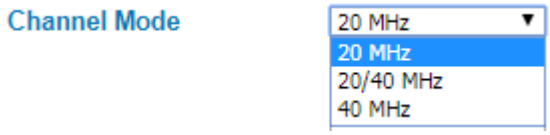
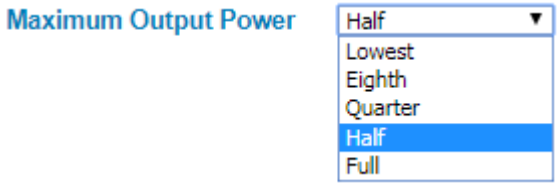
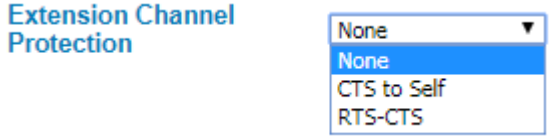
3.4.2.2 Client mode

Wireless Client mode, in this mode the device is able to connect to the Access Point and join the wireless network around the device that opens the connection. User can find the best connection for the AP by click the **Site Survey** and the AP list will appear.



The description of the columns is as below:

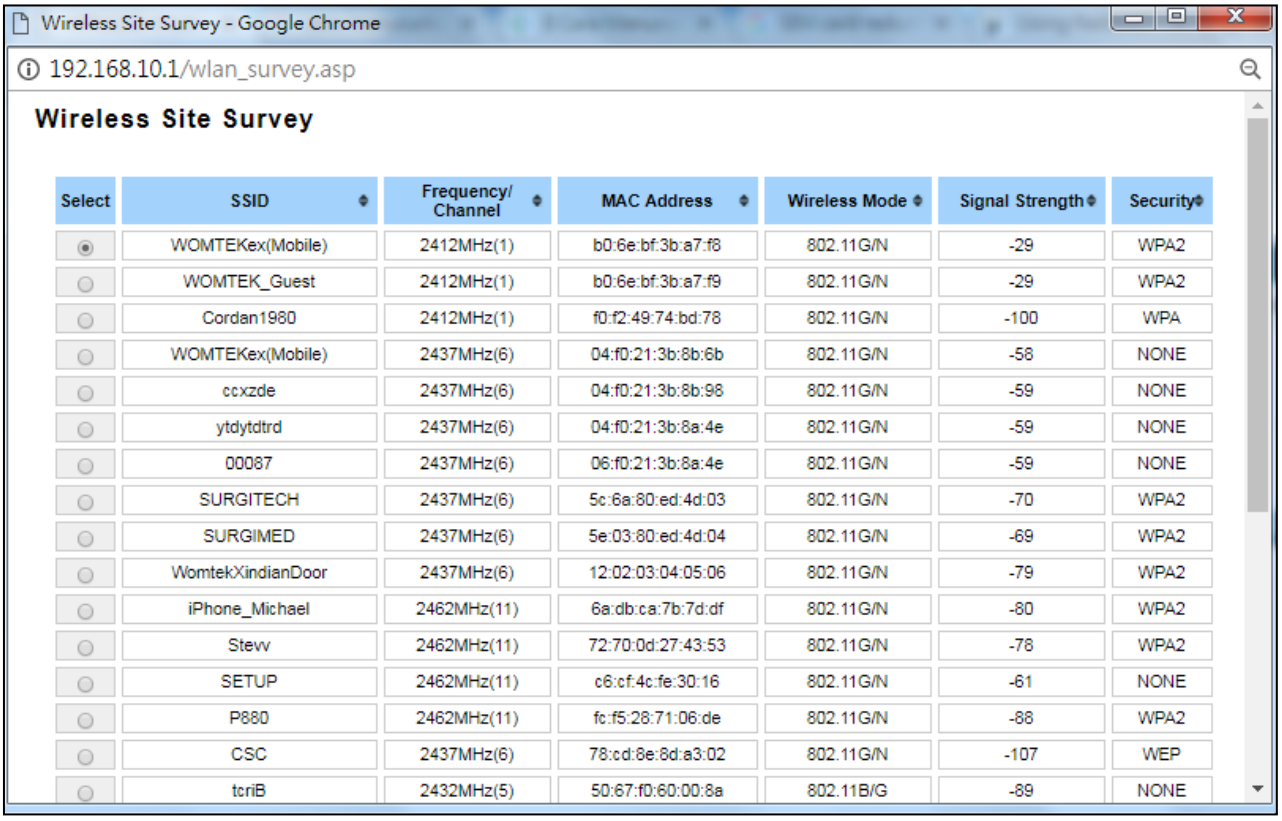
TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	Input the primary name of the access point.
WMM support	**Default: Enable** To enable or disable WIFI multi-media QoS.
Country	Select your country code for band regulation.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has a different configuration. For each wireless mode, it has a specific frequency and it has different basic setting. 
Channel Mode	**Default: 20MHz**

	 There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequency, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna. 
Maximum Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate; the access point will automatically select the highest available rate to transmit. User may select lower rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	 Select from the drop down list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activating this function, it may decrease wireless network performance.

Click **Submit** to apply the configuration

Wireless Site Survey (Wireless Client & WDS-Client)

Click the Site Survey button to open the Wireless Site Survey page. On this page user may choose the Access Point that appeared on the list. After selects the specific AP, then click **Selected** to apply the choice. Click **Scan** to refresh the list.



Select	SSID	Frequency/ Channel	MAC Address	Wireless Mode	Signal Strength	Security
◉	WOMTEKex(Mobile)	2412MHz(1)	b0:6e:bf:3b:a7:f8	802.11G/N	-29	WPA2
○	WOMTEK_Guest	2412MHz(1)	b0:6e:bf:3b:a7:f9	802.11G/N	-29	WPA2
○	Cordan1980	2412MHz(1)	f0:f2:49:74:bd:78	802.11G/N	-100	WPA
○	WOMTEKex(Mobile)	2437MHz(6)	04:f0:21:3b:8b:6b	802.11G/N	-58	NONE
○	ccxzde	2437MHz(6)	04:f0:21:3b:8b:98	802.11G/N	-59	NONE
○	ytdytdtrd	2437MHz(6)	04:f0:21:3b:8a:4e	802.11G/N	-59	NONE
○	00087	2437MHz(6)	06:f0:21:3b:8a:4e	802.11G/N	-59	NONE
○	SURGITECH	2437MHz(6)	5c:6a:80:ed:4d:03	802.11G/N	-70	WPA2
○	SURGIMED	2437MHz(6)	5e:03:80:ed:4d:04	802.11G/N	-69	WPA2
○	WomtekXindianDoor	2437MHz(6)	12:02:03:04:05:06	802.11G/N	-79	WPA2
○	iPhone_Michael	2462MHz(11)	6a:db:ca:7b:7d:df	802.11G/N	-80	WPA2
○	Stevv	2462MHz(11)	72:70:0d:27:43:53	802.11G/N	-78	WPA2
○	SETUP	2462MHz(11)	c6:cf:4c:fe:30:16	802.11G/N	-61	NONE
○	P880	2462MHz(11)	fc:f5:28:71:06:de	802.11G/N	-88	WPA2
○	CSC	2437MHz(6)	78:cd:8e:8d:a3:02	802.11G/N	-107	WEP
○	tcriB	2432MHz(5)	50:67:f0:60:00:8a	802.11B/G	-89	NONE

The description of the columns is as below:

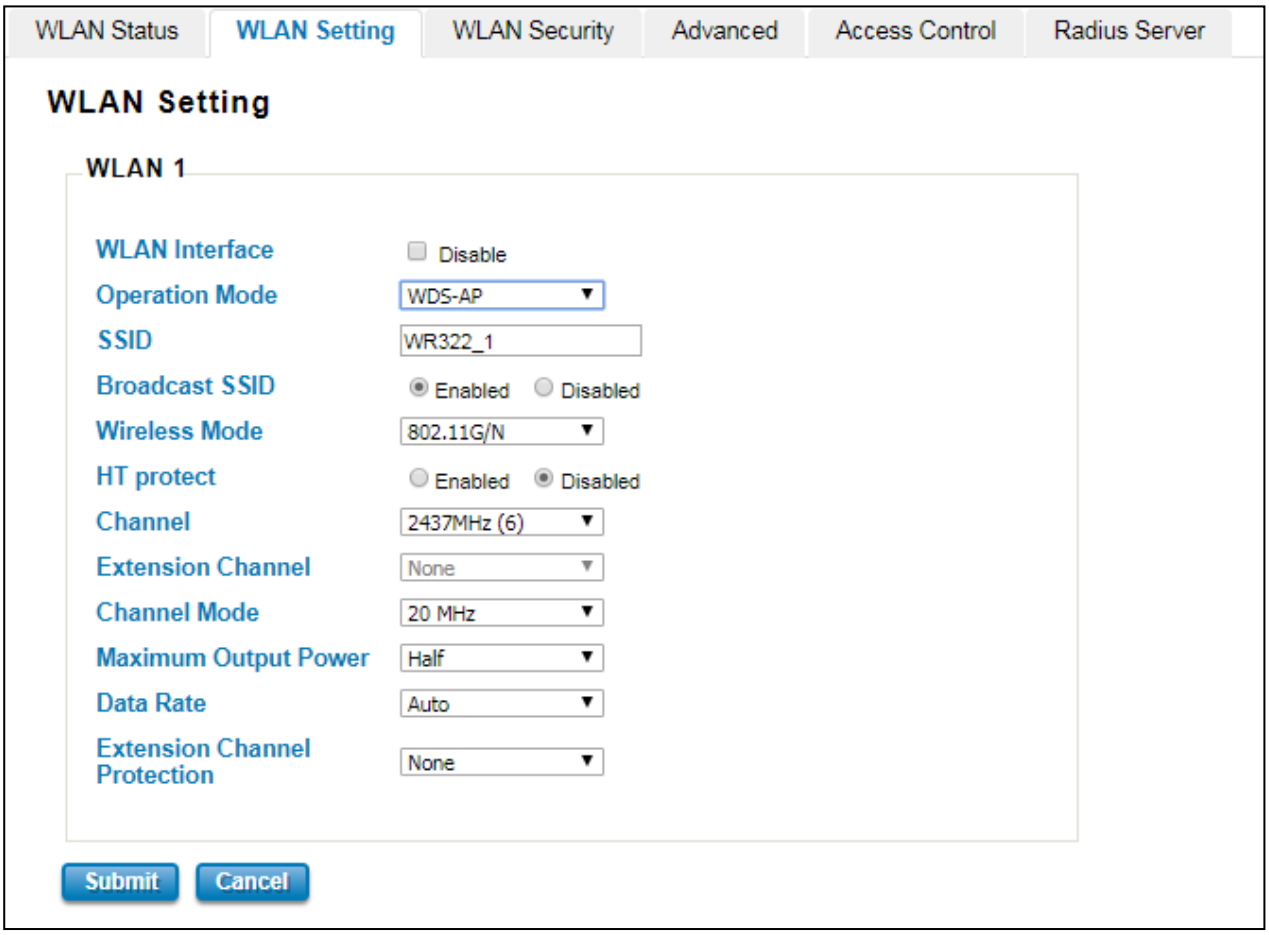
TERMS	DESCRIPTION
Select	Select the SSID.
SSID	Display the detected SSID's name
Frequency/Channel	Display the current frequency of the AP.
MAC Address	Display the listed AP MAC Address.
Wireless Mode	Display the Wireless mode.
Signal Strength	Display the signal strength
Security	The security mode of the Access Point.

Click **Selected** to connect to the specific SSID.

Pop up window may be blocked by browser. Change browser settings to allow pop-up window to configure multi-SSID.

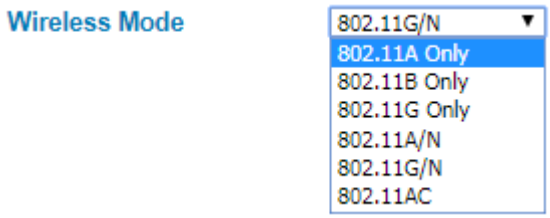
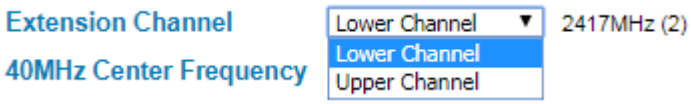
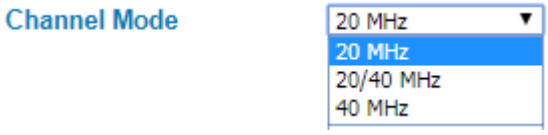
3.4.2.3 WDS AP Mode

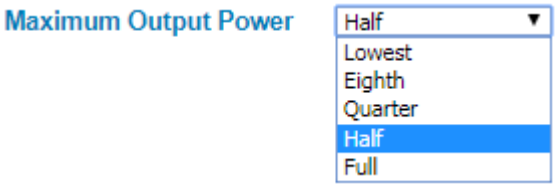
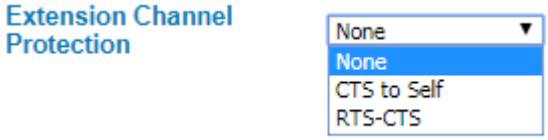
The WDS-AP mode usually implements the Point to Point (P2P) connection, so the access point should be WDS-AP and the wireless client should be WDS-Client. In this case, the AP just can share the connection to the specific wireless client that has its MAC Address. But WDS-AP can be a repeater to provide network access to general clients.



The description of the columns is as below:

TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless function.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: WR322_1** Input the primary name of the access point.
Broadcast SSID	**Default: Enabled.** By enabling the broadcast SSID, it makes the AP can be accessed and searched by the clients, and for the security concern by disabling this broadcaset SSID, the network will be hidden in order to prevent any malicious attack.

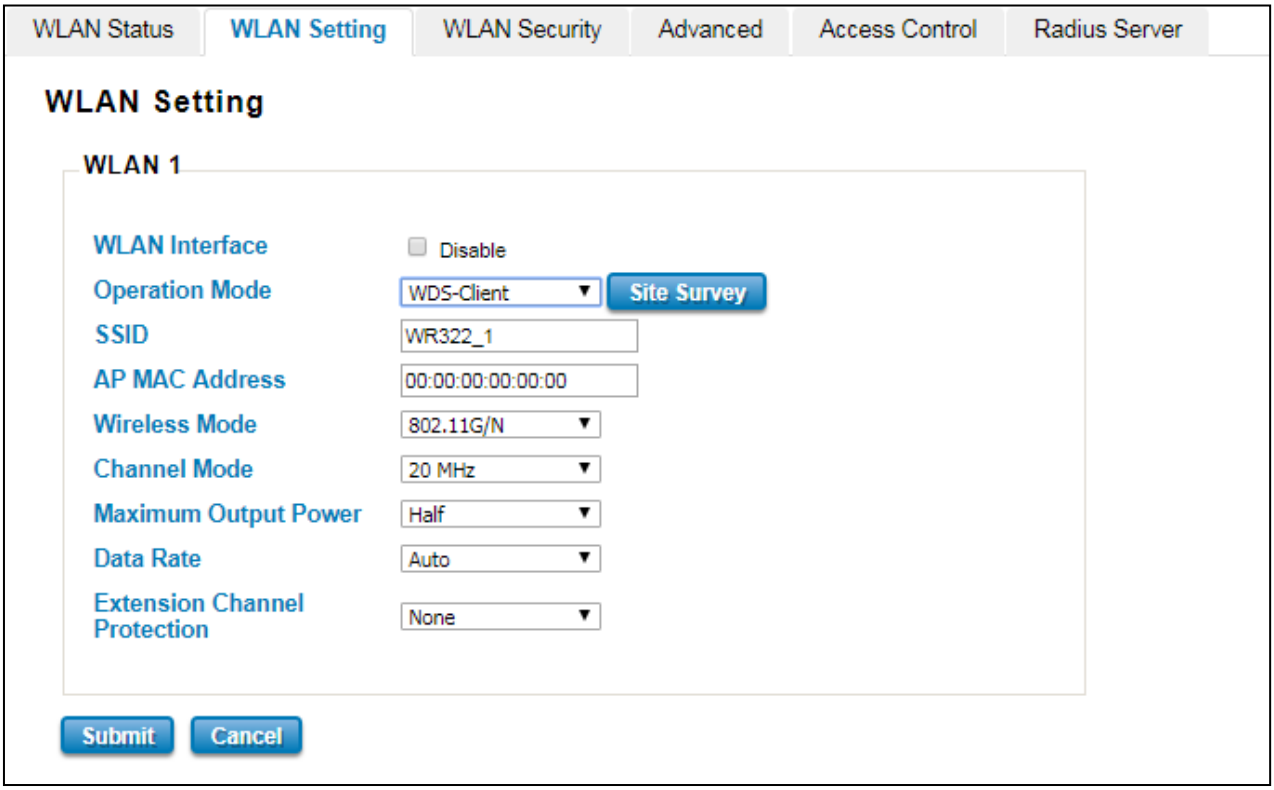
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has different configuration. For each wireless mode, it has specific frequency and it has different basic setting. 
HT Protect	**Default: Disabled** Select Enabled to activate the High Throughput protect to ensure HT transmission with MAC mechanism.
Channel	**Default: 2437MHz (6)** Select the proper channel, each country has different band user may select the channel based on the situation. Or select auto to automatically set the channel. 
Extension Channel	**Default: Lower Channel 2417MHz (2)**  This option would be appeared when user select the Channel Mode to 20/40MHz or 40MHz. To put range for the frequency, it provides the Lower Channel (2417MHz (2)) with the 40MHz center frequency is 2427MHz (4) and Upper Channel (2457MHz (10)) with the 40MHz center frequency is 2447MHz (8).
Channel Mode	**Default: 20MHz**  There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user

	select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequencies, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna. 
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate; the access point will automatically select the highest available rate to transmit. User may select the low rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	 Select from the dropdown list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activating this function it may decrease wireless network performance.

Click **Submit** to apply the configuration

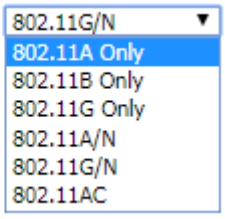
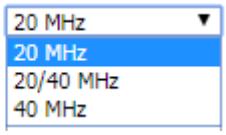
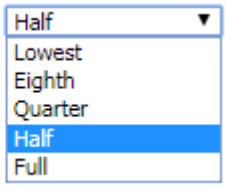
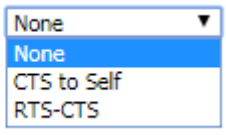
3.4.2.4 WDS Client Mode

In WDS-Client mode, user must specify the specific WDS-AP's SSID and MAC address. So WDS-Client just do the transmission to the WDS-AP only. In this mode, please make sure that the configuration should be the same as the WDS-AP as well.



The description of the columns is as below:

TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: WR322_1** Input the primary name of the access point.
AP MAC Address	**Default: 00:00:00:00:00:00** Set the specific AP MAC Address of the WDS-AP.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has a different configuration. For each wireless mode, it has a specific frequency and it has different basic setting.

	Wireless Mode 
Channel Mode	**Default: 20MHz** Channel Mode  There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequencies, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna. Maximum Output Power 
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate, the access point will automatically select the highest available rate to transmit. User may select the low rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	Extension Channel Protection  Select from the dropdown list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activate this function it may decrease wireless network performance.

3.4.2.5 Mesh Settings

WA512GM series support mesh network. Click checkbox and submit button to enable mesh network. SSID will be used as connections for both mesh links and wireless clients. Mesh link will be connected automatically to form adaptive mesh network. There are 2 roles in mesh network:

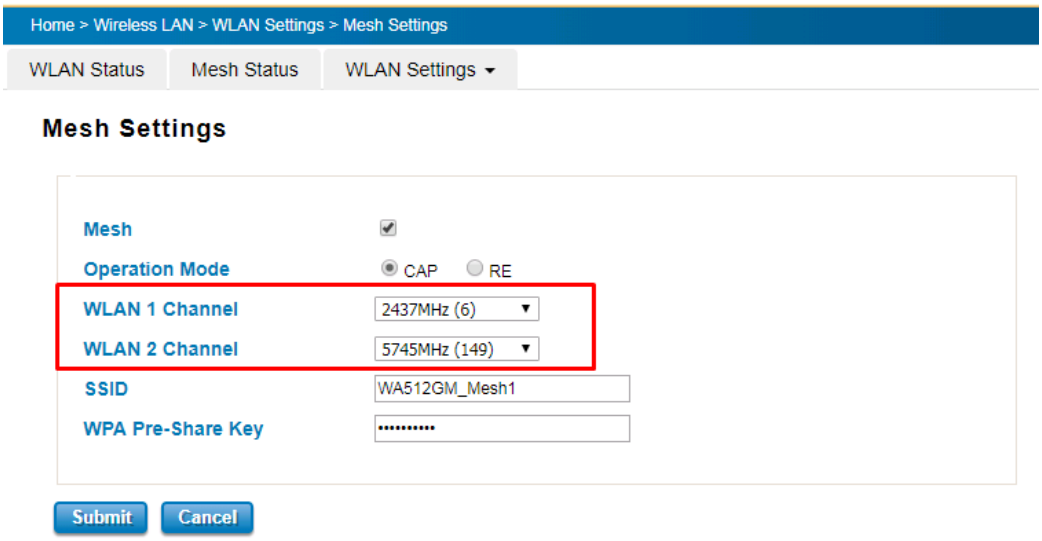
CAP: Central AP, also known as root AP, with a wired data connection that can be configured to relay data to and from mesh APs. In CAP, you can enable MESH in 2.4GHz or 5GHz frequency, define SSID and Key for the MESH network. The DHCP server feature is enabled automatically in CAP, it can assign IP address to MESH RE devices and connected clients.

RE: Range Extender, to form a mesh network by uplink to other RE or CAP. In MESH RE device, the MESH SSID and Key setting must follow CAP settings.

Note that other wireless modes including AP/client/WDS AP/WDS client modes will be dismissed and can't be configured. Disable mesh to go back to AP/client/WDS AP/WDS client mode.

> AP/client/WDS AP/WDS client modes will be dismissed when mesh enabled. Disable mesh to enable AP/client/WDS AP/WDS client modes again.

MESH Settings



TERMS	DESCRIPTION
Mesh	Check the box to enable mesh network
Operation Mode	Select the Operation Mode in mesh network. CAP: Central AP, node with WAN uplink for outside network. RE: Node has only uplink to other RE nodes or CAP nodes, functions as range extender.
WLAN 1 Channel	Select the channel of WLAN 1 (CAP only)
WLAN 2 Channel	Select the channel of WLAN 2 (CAP only)

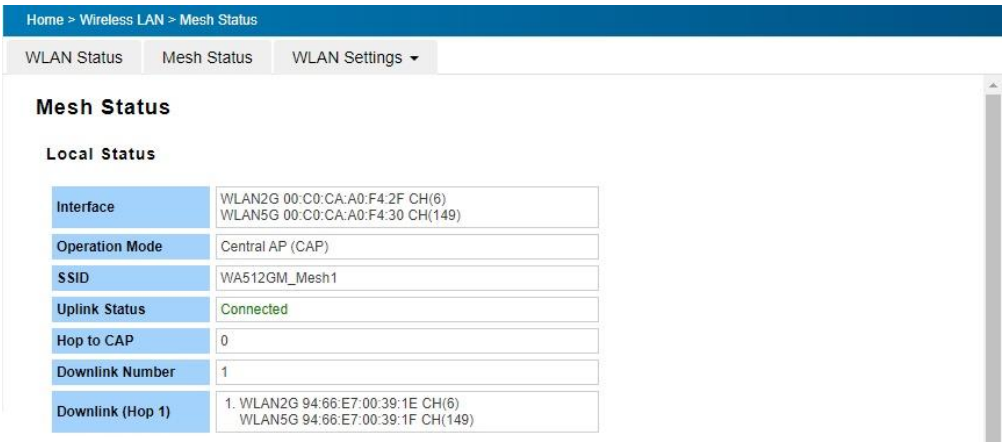
SSID	The SSID will be used for both mesh links and wireless clients. The setting within the MESH network must be the same.
WPA Pre-Share Key	Passphrase used to connect to SSID. The setting within the MESH network must be the same.

MESH Status

Click MESH Status, you can find the MESH status of the connected AP in this page.

The MESH Status in CAP:

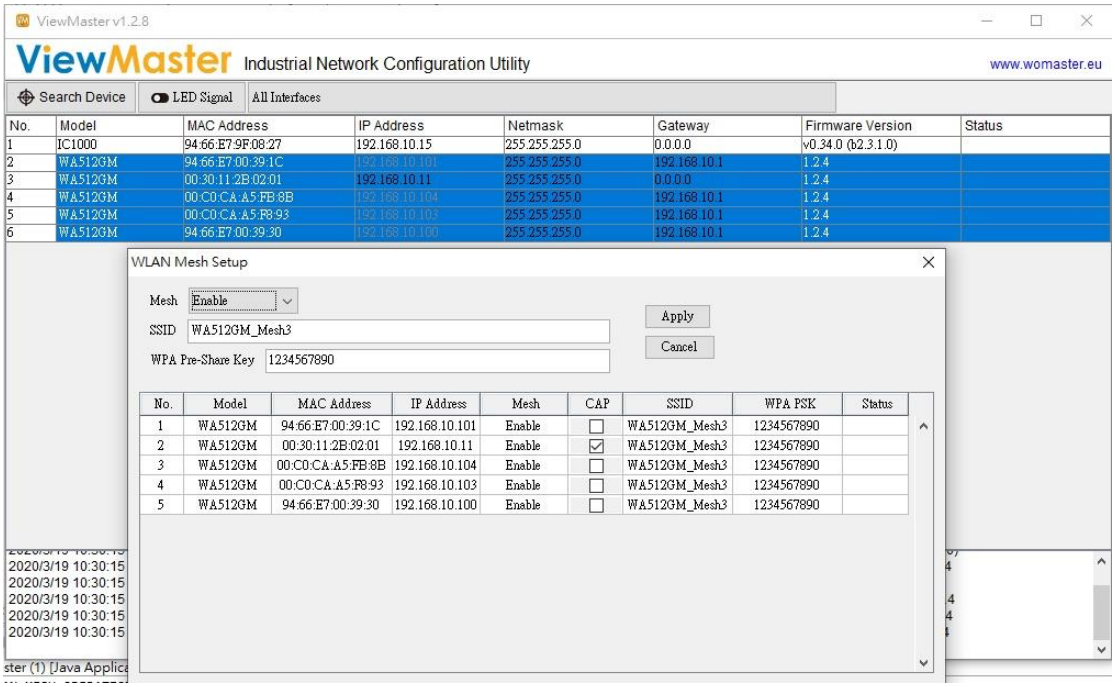
In **Local Status,** you can find the information of the WLAN interface, Operation mode, MESH SSID, Uplink Status, Hop to CAP(0 in CAP), Downlink number and Hops.



In **Device,** you can find all the APs' role and information. It helps you to monitor the MESH network. You can draw your MESH network architecture according to the information. The first column you see is "ME", the role of your connected AP. While check RE, the first column will be 1(ME): RE mode.

Quick MESH configuraiton in ViewMaster

ViewMaster allows user to group assign and change WLAN MESH Setting. Scan and select all the MESH APs, you can assign/change SSID, Key and enable CAP. Once you change the settings, please reboot all the MESH device to activate the new seting.



ViewMaster Configuration Utility Download:

- Go to the **Support/Software & Literature/Software** page of the WoMaster web site. Apply the member account and login, then you can download the ViewMaster software.
- The link is as following: https://www.womaster.eu/download_83_84.htm
- If you can't find the link, search key word **"WoMaster ViewMaster**" to find it through searching machine.
- Install the ViewMaster and run **"Search Device"**. You can find your device through network, you can configure basic setting, for example the IP address, WLAN/MESH settings, configuration file backup/restore and firmware upgrade.

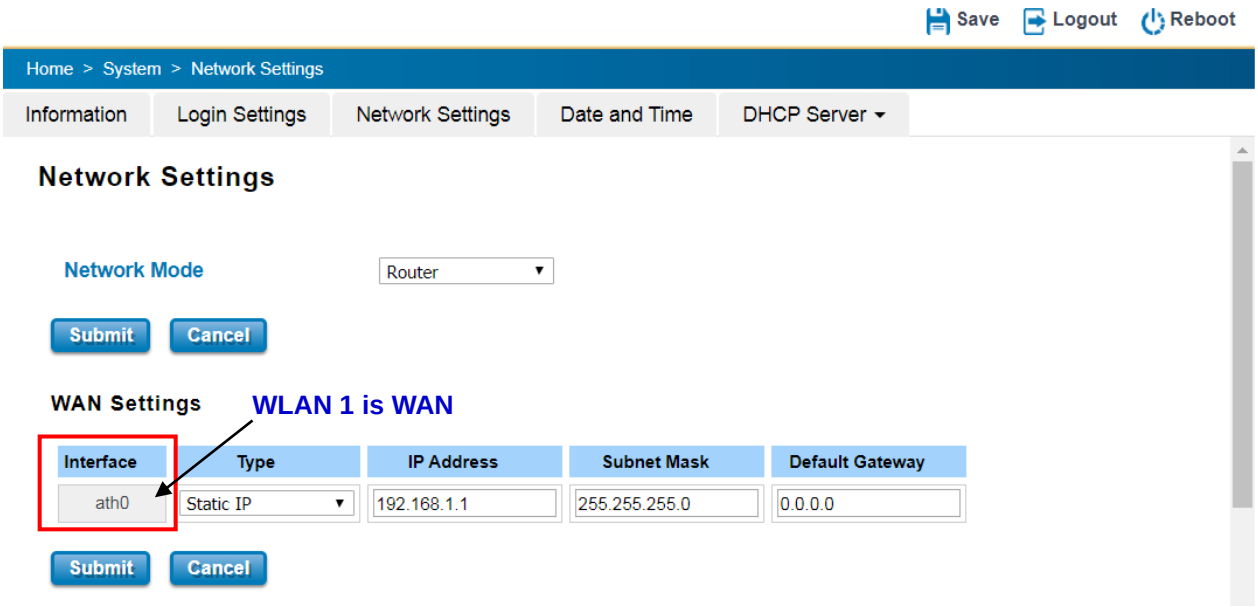
3.4.2.6 Client Router (Wireless WAN NAT) Mode

Some of the specific firmware supports the “Client Router” operation mode, also known as WLAN NAT or Wireless WAN mode. The configured WLAN 1 or WLAN 2 interface acts as WAN interface instead of other Ethernet or WLAN interfaces. Refer to the below comparison table of WALN/Ethernet interface to Router operation mode.

	RJ45 Interface		WLAN Interface		
Interface\ Operation Mode	**Eth 1**	**Eth 2/PD**	**WLAN 1**	**WLAN 2**	**Note**
WLAN 1- Clinet Router	LAN	LAN	**WAN (ath0)**	LAN	LAN to Wireless WAN NAT Routing.
WLAN 2- Clinet Router	LAN	LAN	LAN	**WAN (ath16)**	LAN to Wireless WAN NAT Routing.
Ethernet - Router	LAN	**WAN (Eth1)**	LAN	LAN	
Ethernet - Bridge (Default Setting)	LAN	LAN	LAN	LAN	Default: All interfaces work as LAN segment

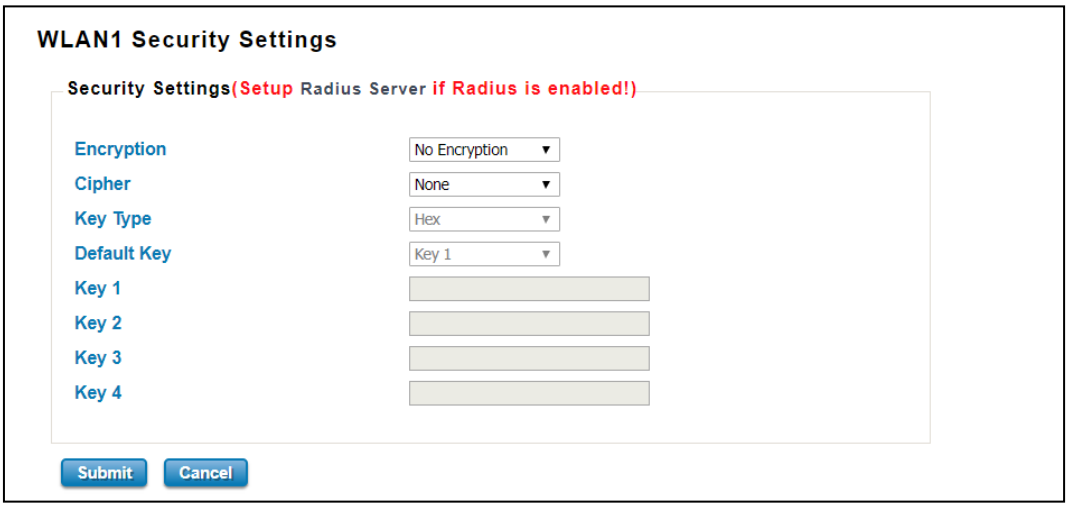
Note: Only one Radio can be enabled as Client/Client Router mode.

After enabled the WLAN Client Router mode, the interface of WLAN 1 in WAN Settings of Network settings is “ath0”. The interface of WLAN 2 in WAN Settings of Network settings is “ath16”. You can select Static IP or DHCP Client, and assign the IP address for your Wireless WAN interface. The system will run the LAN to Wireless WAN NAT Routing.



3.4.3 WLAN Security

On this configuration page, user can configure the WLAN Security feature.

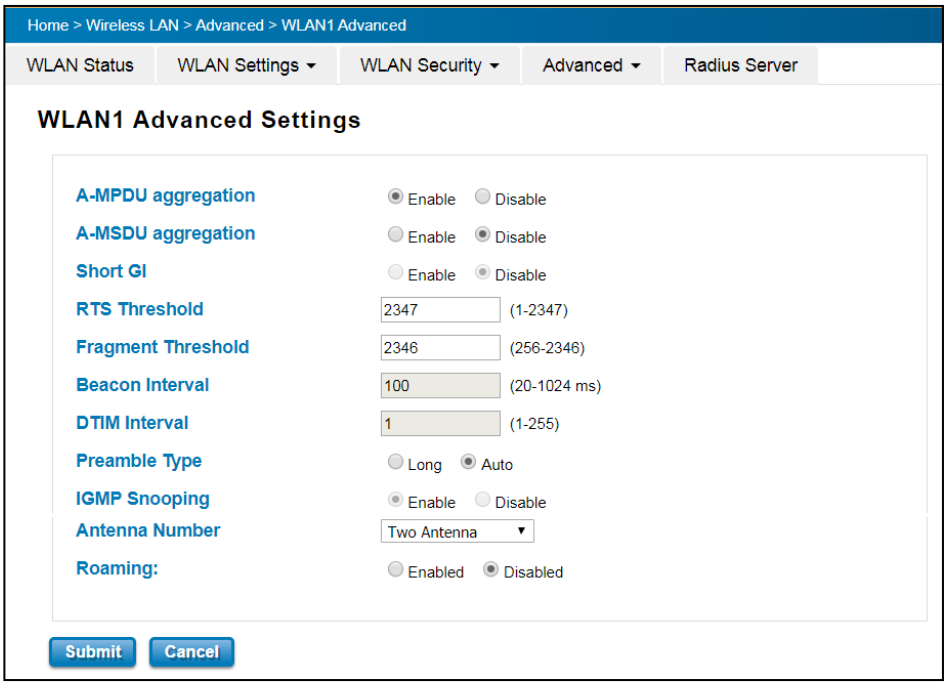


The description of the columns is as below:

TERMS	DESCRIPTION
Encryption	Configure the data encryption mode. ● **None**: Available only when the authentication type is an open system. ● **64 bits WEP**: It is made up of 10 hexadecimal numbers. ● **128 bits WEP**: It is made up of 26 hexadecimal numbers. ● **TKIP**: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK. ● **AES**: Advanced Encryption Standard, it is usually co-used with WPA2-PSK.
Key Type	**Default: Hex** WEP can be configured with a 64-bit or 128-bit Shared Key (hexadecimal or ASCII). As defined, hexadecimal number is represented by 0-9, A-F or a-f; ASCII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.
Default Key	**Default: Key 1** Set the specific default key.
Key 1~4	Enter the specific encryption key.

3.4.4 Advanced

The page allows the advanced user to configure advanced wireless setting with more experience about the WLAN. If user doesn't have any qualified knowledge about WLAN, we suggest not to change the default setting except user know the effects when the setting is changed. The wrong configuration may impact the performance of wireless network.



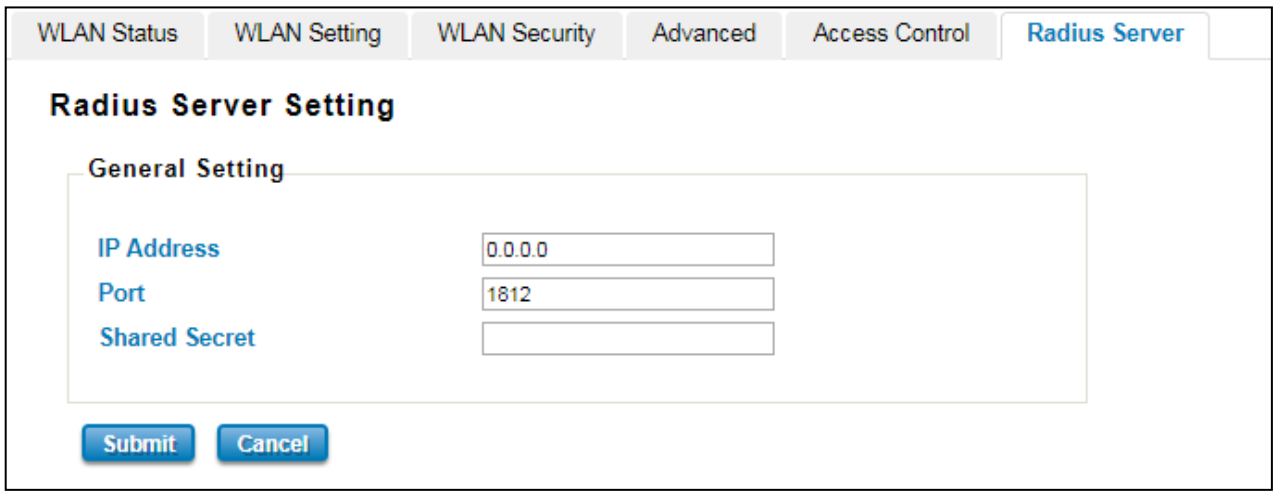
The description of the columns is as below:

TERMS	DESCRIPTION
A-MPDU/A-MSDU aggregation	For the AP mode, the data rate of the AP could be enhanced greatly. Do not enable this function if the wireless clients don't support A-MPDU/A-MSDU aggregation.
Short GI	Enable this function to obtain better data rate. (careful with compatibility issue)
RTS Threshold	**Default: 2347 (1-2347)** Basically, it is about the transmission process between the AP and the end station. When the AP sends Request to Send frames to station and it will do the negotiation process about sending the data frame. When the station receives an RTS frame, the station will respond with send back Clear to Send frame to confirm the right to start transmission.
Fragment Threshold	**Default: 2346 (256-2436)** Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance.
Beacon Interval	**Default: 100ms (20-1024 ms)**

	Specify the interval to broadcast packets.
DTIM Interval	**Default: 1 (1-255)** Delivery Traffic Indication Message interval is an additional message added after the beacon interval broadcast by access point. It is for enhancing the wireless transmission efficiency. The more intervals we added, the more power that we need. By setting a low value of DTIM, user can effectively keep the devices awake indefinitely so they never go into sleep mode when idling.
Preamble Type	**Default: Long** Preamble Type setting means that it adds some additional data header strings to help check the Wi-Fi data transmission errors. Basically, preamble type divided into two, long and short. Short is for shorter data strings that adds less data to transmit the error redundancy check which means that it is much faster. Long Preamble Type uses longer data strings which allow for better error checking capability. Auto Preamble Type the device can set the Preamble Type Automatically according to the need, which is can be long or can be short.
IGMP Snooping	**Default: Enable** By enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the AP. IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic.
Antenna Number	**Default: Two Antenna** The Antenna Number setting allows user to choose the antenna that used in the wireless connection. Basically, the default setting is set to Two antennas, because the device itself provide two antenna sockets. User can configure One Antenna or Two Antenna. Please refer to the Antenna Placement table to connect the antenna correctly.
Roaming	**Client Based Fast Roaming** The feature is available in WLAN Client mode. The client can check better AP by itself and start the Fast Roaming mechanism without AP controller. Select “Enable” to configure the Fast Roaming feature, you will find more advanced settings. Check the Fast Roaming description in below. (**Note:** This is proprietary fast roaming design for specific application, the feature is not available in/after V1.5.x firmware version.)

3.4.5 RADIUS Server (AP Mode)

The Remote Authentication Dial In User Service (RADIUS) mechanism is a centralized “AAA” (Authentication, Authorization, and Accounting) system for connecting to network services. The fundamental purpose of RADIUS is to provide an efficient and secure mechanism for user account management. The RADIUS server system allows you to access the router through secure networks against unauthorized access.



How to set up a RADIUS server:

a. Enter the IP address of the RADIUS server in **Server IP Address**
b. Enter the **Shared Secret** of the RADIUS server
c. Enter the **Server port** if necessary, by default RADIUS server listens to port 1812
d. Click **Submit**

The description of the RADIUS Authentication interface is as below:

TERMS	DESCRIPTION
IP Address	Radius Server IP Address
Server Port	Set communication port on an external RADIUS server as the authentication database. The default value is 1812
Shared Key	Shared key is used to verify that RADIUS messages, with the exception of the Access-Request message, are sent by a RADIUS-enabled device that is configured with the same shared key. Shared key also verifies that the RADIUS message has not been modified in transit (message integrity).

3.4.6 Certificate File (Client Mode)

Using digital certificates for authentication method through the RADIUS that provided by the AP. User needs to upload the specific certificate file, so then the client can access the Wi-Fi connection.

The description of the columns is as below:

TERMS	DESCRIPTION
Delete User Key	Delete the selected certificate
Upload User Key	Upload a certificate file from a specified file location

3.5 Security

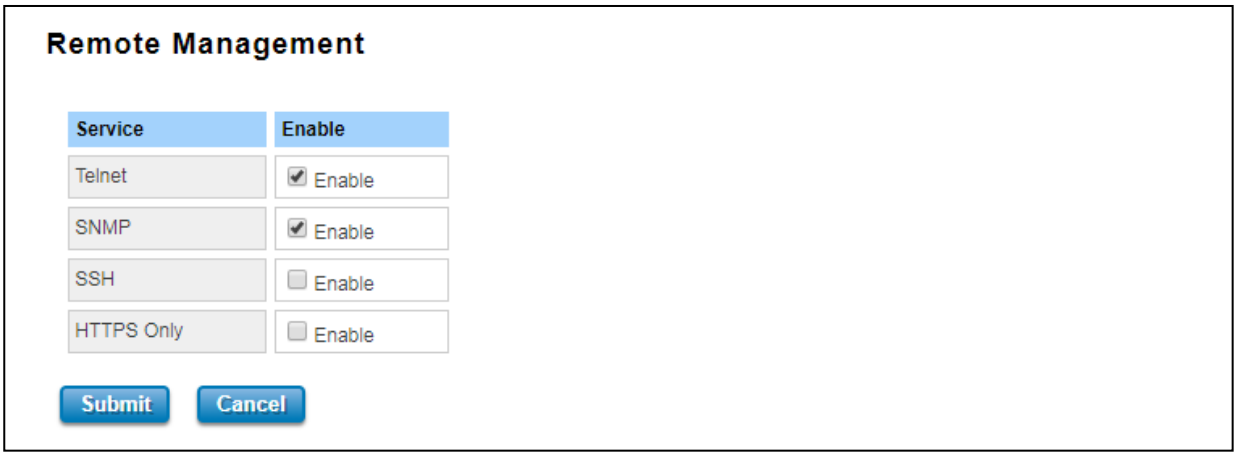
WoMaster Router provides several security features for User to secure access to its management functions and it can be remotely managed (monitored and configured).

3.5.1 Access Control

WoMaster router provides access control mode in several ways, such as Remote Management, WAN Service Access Control and Custom Exception. By configuring this configuration, user can enhance the security access to the device.

Remote Management

Remote management function: open the Remote Management, that would allow the user via the local access (WAN Port) Remote Management the router.



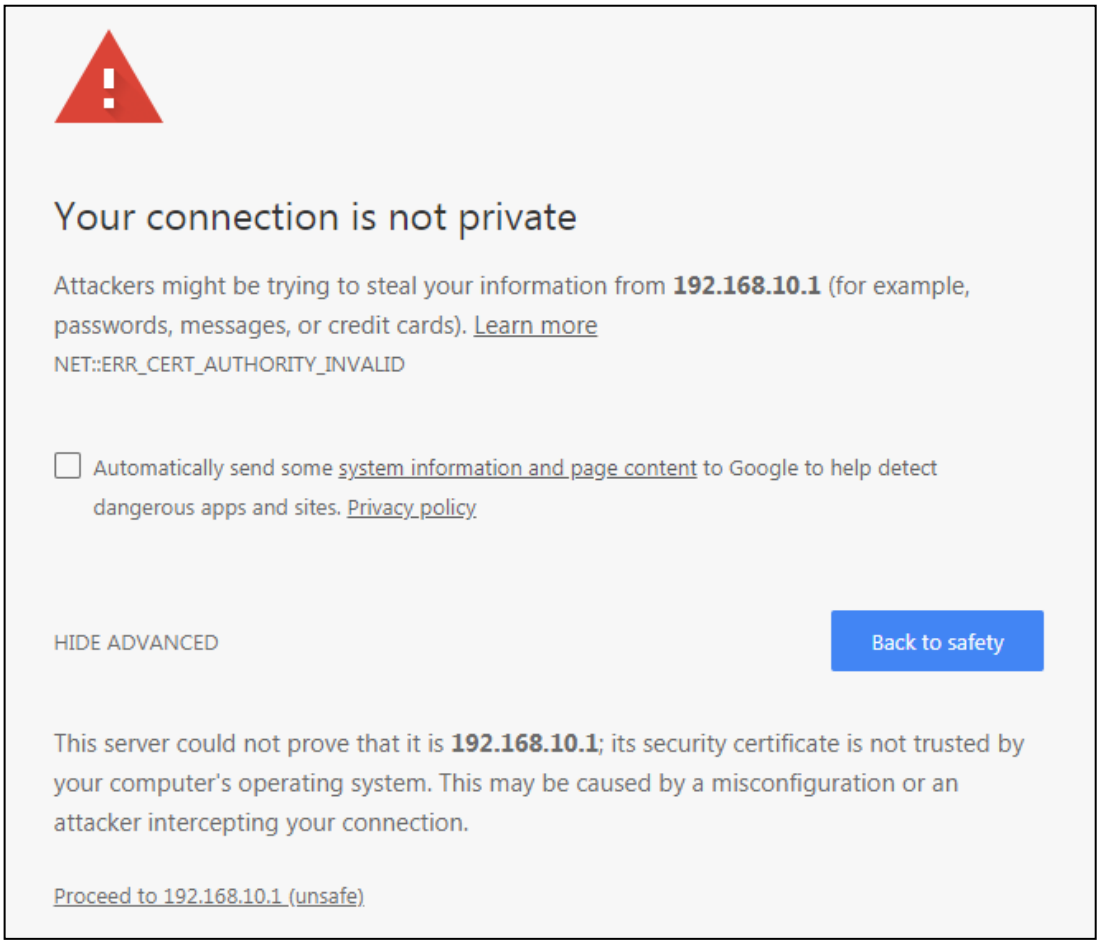
The description of the columns is as below:

TERMS	DESCRIPTION
Telnet	Allows the user to remotely login and manage the device by Telnet. When user doesn't enable it, the connection through telnet will not allow.
SNMP	Allows the user to remotely login and manage the device by SNMP. When user doesn't enable it, the connection through SNMP will not allow.
SSH	Allows the user to remotely login and manage the device by SSH/ When user doesn't enable it, the connection through SSH will not allow.
HTTPS Only	Allows the user to remotely login and manage the device by HTTPS access for secure connection, and it would disable the HTTP access.

Once User finishes configuring the settings, click on **Submit** to apply configuration.

HTTPS Only

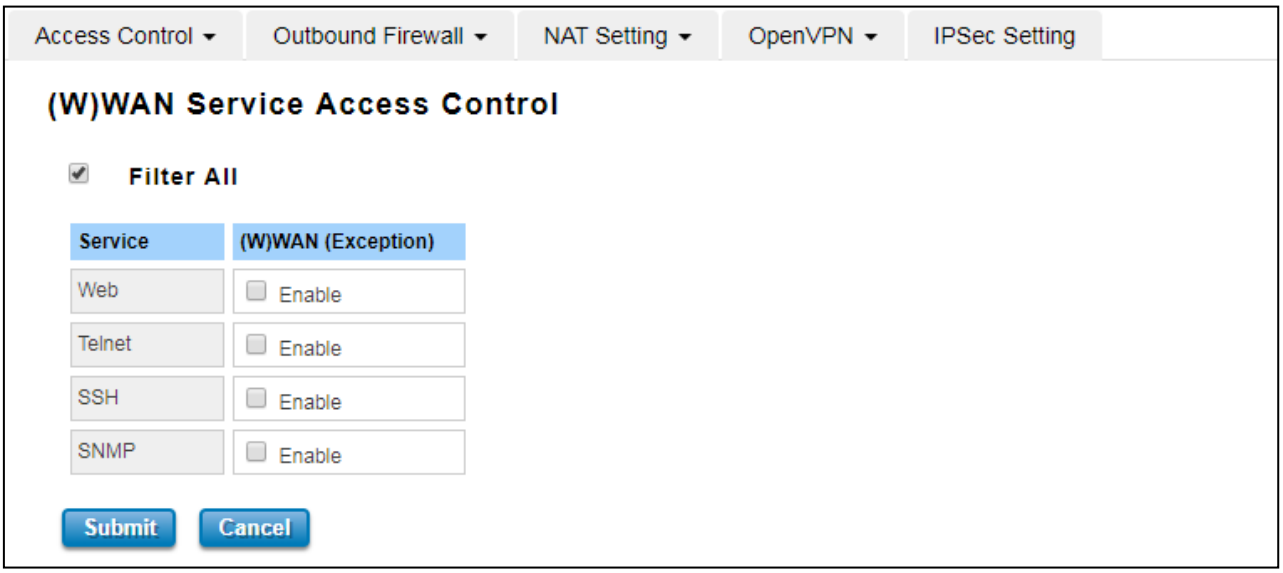
HTTP Secure is the use of the HTTP protocol over an SSL/TLS protocol. It is used primarily to protect against eavesdropping of communication between a web browser and the web site to which it is connected. This is especially important when you wish to have a secure connection over a public network such as the internet. HTTPS connections are secured through the use of certificates issued by trusted certificate authorities. When a web browser makes a connection attempt to a secured web site, a digital certificate is sent to the browser so that it can verify the authenticity of the site using a built-in list of trusted certificate authorities.



If user uses the HTTPS Only, a warning page would appear when user access the device in order to provide a secure access. The picture above is the warning message about the digital certificate and user just need to accept this warning by click **"Proceed to 192.168.10.1 (unsafe)"**.

WAN Access

When user changes the device mode to **router mode (Port 1 – WAN interface)** the WAN Access feature can be activated. This feature is about the exception to access the device through the WAN interface for security concern. So that the access or the traffic that coming through the WAN interface can be limited as required. The user may choose the **Filter All** functions to block all access from the WAN interface or enable the exception options, then the router allows user to remotely access to the router from WAN interface.



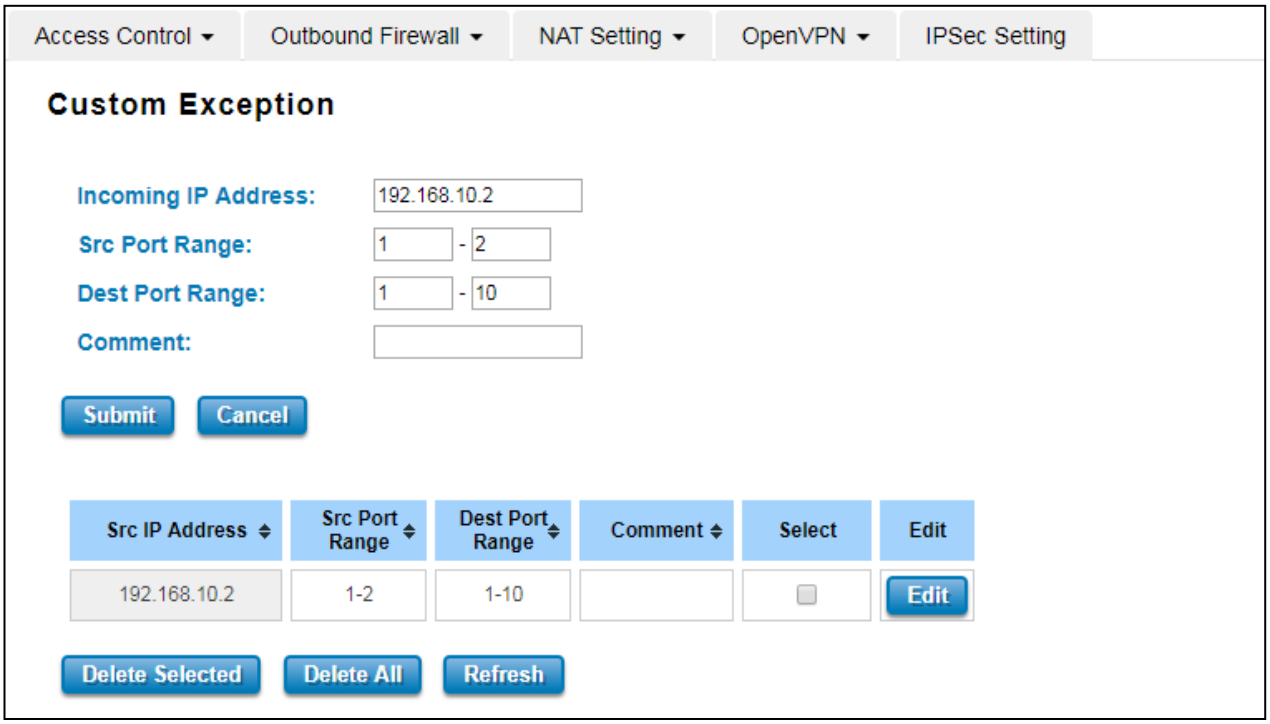
The description of the columns is as below:

TERMS	DESCRIPTION
Filter All	By select Filter All, it will block all external access from WAN interface to the device (such as SSH, SNMP, Web and Telnet) and unblock the exception options.
Web	Select this option to allow access to the router using Web (HTTP or HTTPS) from the WAN Interface
Telnet	Select this option to allow access to the router using Telnet from the WAN Interface
SSH	Select this option to allow access to the router using SSH from the WAN Interface
SNMP	Select this option to allow access to the router using SNMP from the WAN Interface

Once User finishes configuring the settings, click on **Submit** to apply configuration.

Custom Exception

Another choice for the access control is also provided by WoMaster, it is called custom exception feature. Through this feature, it can help to allow the incoming access through the firewall to local devices. If the condition does not meet the requirement from the table, then the access would be denied.



The description of the columns is as below:

TERMS	DESCRIPTION
Src IP Address	Set up the source IP Address that may access the device.
Src Port Range	Set up the source port range where the access came from.
Dest Port Range	Set up the destination port range where the access is going to.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete,
Edit	Click edit to modify the parameters

Once User finishes configuring the settings, click on **Submit** to apply configuration and a new line will directly appear on the table.

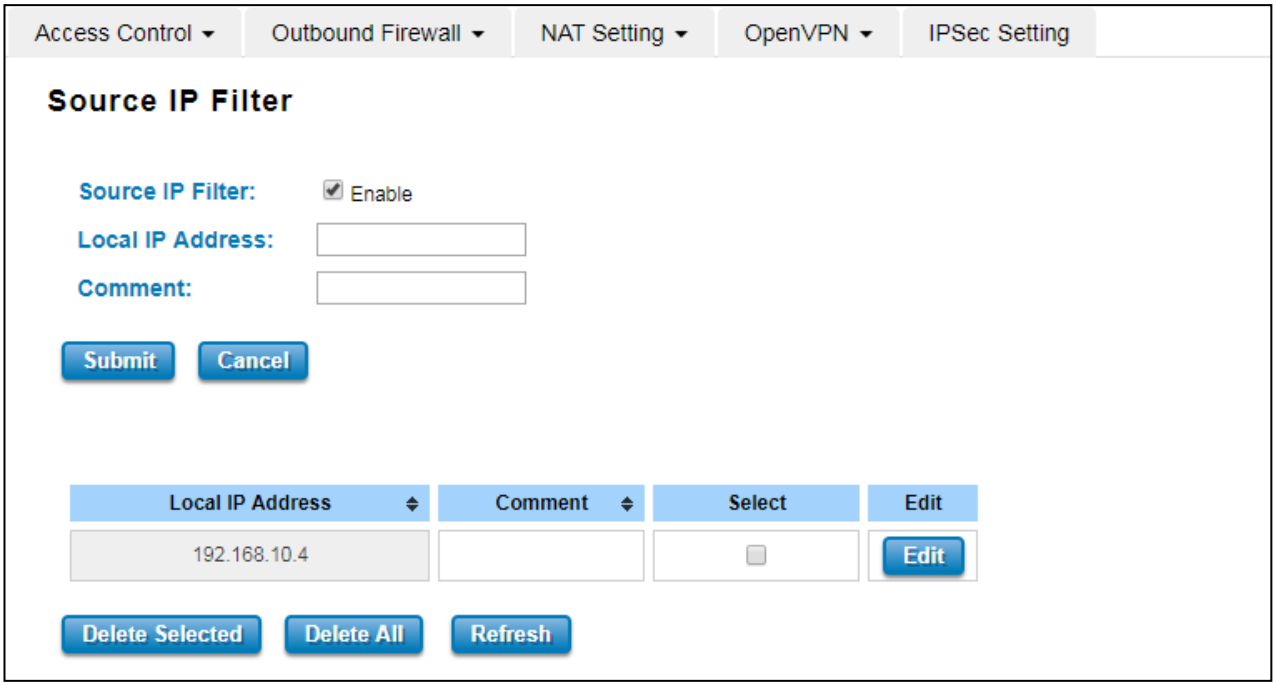
3.5.2 Outbound Firewall

WoMaster' router has different types firewall settings, user can enable the setting, configure the rules. The following section is Outbound Firewall Settings pages where user can configure the Outbound Firewall setting.

TERMS	DESCRIPTION
Source IP Filter	Source IP addresses Filtering from LAN to Internet through the router.
Destination IP Filter	Destination IP addresses Filtering from the LAN to Internet through the router.
Source Port Filtering	Source Ports Filtering from the LAN to Internet through the router.
Destination Port Filtering	Destination Ports Filtering from the LAN to Internet through the router

Src IP Filter

By entries parameter in this table, it can restrict certain types of data packets from the local network to the internet through the Router. The Source IP Filter will help to filter all of the packets that coming into the router. If the source IP is on the list, then the packets would be dropped. But if the source IP is not on the list, then the packets can be received. Select **Enable** to activate **Source IP Filtering**, type the **Local IP Address** and **Comment** to write notes for the entry. Click Submit to activate the settings. After applied, then user can see the new entry shown in the below table.



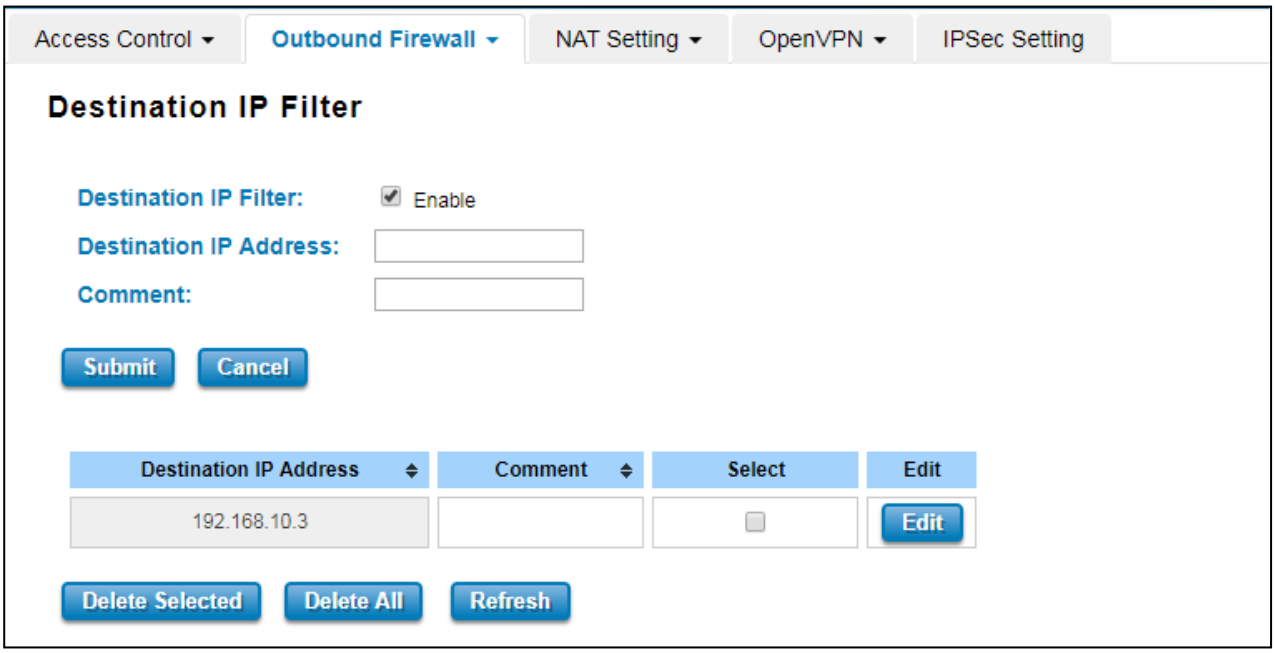
The description of the columns is as below:

TERMS	DESCRIPTION
Local IP Address	Display the Source IP address.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete,
Edit	Click edit to modify the parameters

Click **Refresh** to refresh the table

Dest IP Filter

By entries parameters in this table are used to restrict the computers in LAN from accessing certain websites in WAN according to IP address. The concept is the same as the source IP Filter. The packet would not send to the specific IP Address that showed on the list. Only the IP Address that shows on the list that cannot receive the packets. Select **Enable** to activate **Destination IP Filtering**, type the **Destination IP Address** and **Comment** to write a note for the entry and then click Submit to apply the settings. After applied, then user can see the new entry shown in the below table.



The description of the columns is as below:

TERMS	DESCRIPTION
Destination IP Address	Display the Destination IP address.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete,
Edit	Click edit to modify the parameters

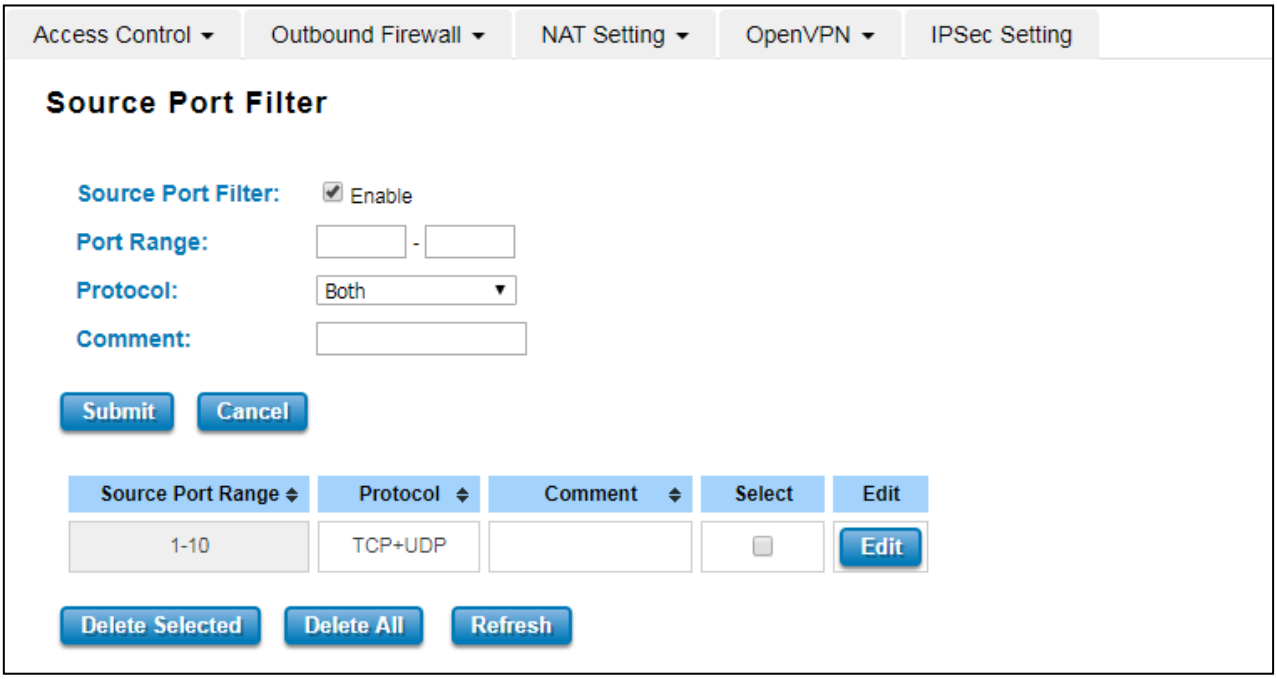
Click **Refresh** to refresh the table

Src Port Filter

Entries in this table are used to restrict certain ports of data packets from user's local network to the Internet through the Router. Use of such filters can be helpful in securing or restricting local network. The device just cannot receive any packets from the source port that showed on the list, the other packet that sent from any source port that not on the list would be received.

Select **Enable Source Port filtering**, type the **Port Range** of below **Protocol** type, the protocol type can be **UDP, TCP or Both**. Type the **Comment** to write a note for the entry and then click **Submit** to activate the settings.

After applied, user can see the new entry shown in the below table.



The description of the columns is as below:

TERMS	DESCRIPTION
Source Port Range	Display the Source Port Range (Range is from 1 to 65535)
Protocol	Display the protocol that has been chosen by the user.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete,
Edit	Click edit to modify the parameters

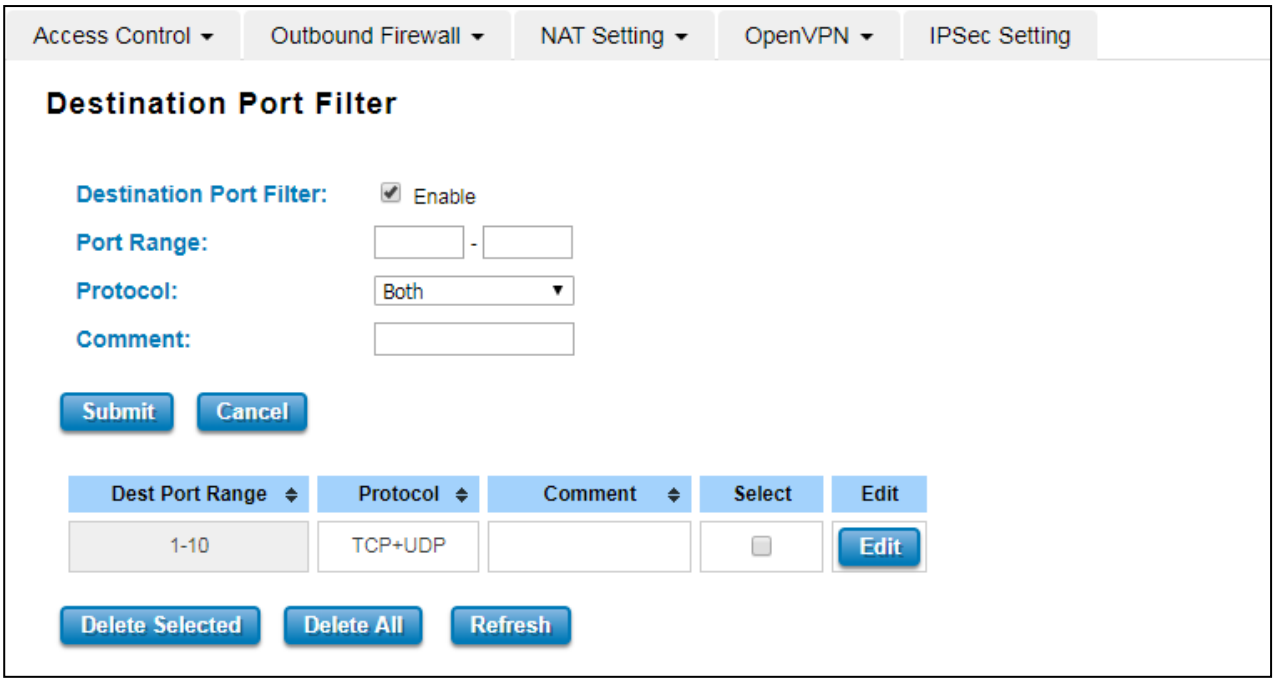
Click **Refresh** to refresh the table

Dest Port Filter

Entries in this table are used to restrict certain ports of data packets from user's local network to Internet through the router. Use of such filters can be helpful in securing or restricting local network. And the device cannot send any packets to the destination port that showed on the list.

Select **Enable Destination Port Filtering**, type the **Port Range** of below **Protocol** type, the protocol type can be **UDP, TCP or Both**. Type the **Comment** to write note for the entry and then press **Submit** to apply the settings.

After applied, then user can see the new entry shown in the below table.



The description of the columns is as below:

TERMS	DESCRIPTION
Dest Port Range	Display the Destination Port Range (Range is from 1 to 65535)
Protocol	Display the protocol that has been chosen by the user.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete,
Edit	Click edit to modify the parameters

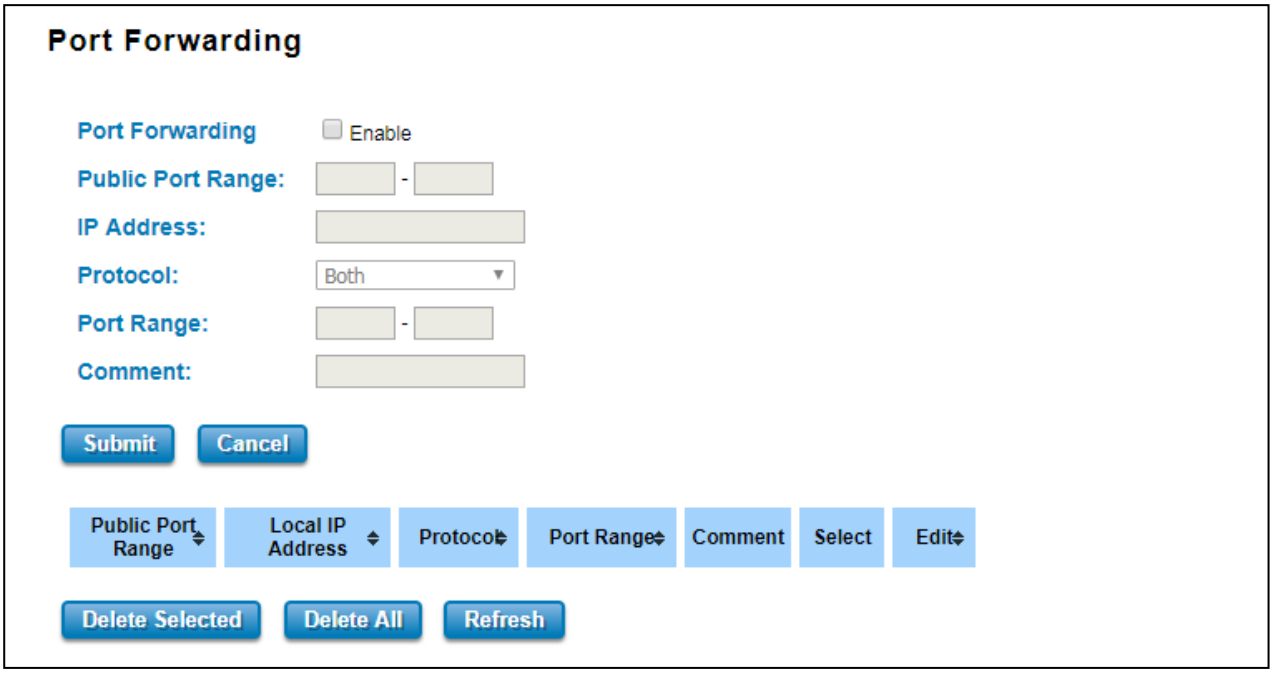
Click **Refresh** to refresh the table

3.5.3 NAT Setting

Network Address Translation is the process where a network device, usually a firewall, assigns a public address to a device or group of devices inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economic and security purposes. The simple type of NAT provides one to one translation of IP address. It can be used to interconnect two IP networks, normally one network is for Local Area Network and the other network is for Wide Area Network/Internet. To support this function, there are two ways to do it, by using Source Network Address Translation (SNAT), Destination Network Address Translation (DNAT). Basically, Network Address Translation (NAT) occurs when one of the IP addresses in an IP packet header is changed. In a SNAT, the destination IP address is maintained and the source IP address is changed. Most commonly, a SNAT allows a host on the "inside" of the NAT, in an RFC 1918 IP address space, to initiate a connection to a host on the "outside" of the NAT. It supports the Port Forwarding, DMZ and 1 to 1 NAT configuration. A DNAT, by way of contrast, occurs when the destination address is changed and the source IP address is maintained. A DNAT allows a host on the "outside" to connect to a host on the "inside". In both cases, the NAT has to maintain a connection table which tells the NAT where to route returning packets. An important difference between a SNAT and a DNAT is that a SNAT allows multiple hosts on the "inside" to get to any host on the "outside". By way of contrast, a DNAT allows any host on the "outside" to get to a single host on the "inside". It is supported in NAPT and 1 to 1 NAT features.

To configure the NAT Setting, the **Port Forwarding, DMZ, Port Mapping Policy and 1 to 1 NAT** configuration page are provided in this section.

Port Forwarding



By configuring this table, it allows user to automatically redirect common network services to a specific machine behind the NAT firewall. Select **Enable** to activate **Port Forwarding** function and then input all of the parameters to configure the port forwarding.

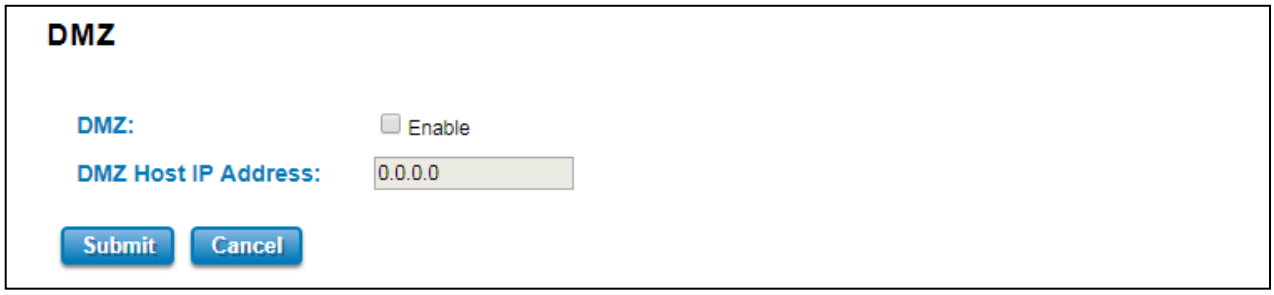
The description of the columns is as below:

TERMS	DESCRIPTION
Port Forwarding	Select Enable to activate Port Forwarding function.
Public Port Range	Configure the port range, which will be public to a WAN / Internet. User can configure one or a range of TCP/UDP port number.
IP Address	Configure the IP Address of the LAN PC. The traffic from the public port range will be redirected to this IP address.
Protocol	Configure TCP, UDP or Both (TCP + UDP) protocol type.
Port Range	Configure the port range of the LAN; the traffic from the public port will be redirected to these ports.
Comment	Add information to the entry.

Once User finishes configuring the settings, click on **Submit** to apply User configuration.

DMZ

A **Demilitarized Zone** is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains device accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.



Click **Enable** to activate the function and assign the IP address of **DMZ Host IP Address**. This is the DMZ computer's IP address. Click Submit to activate the function.

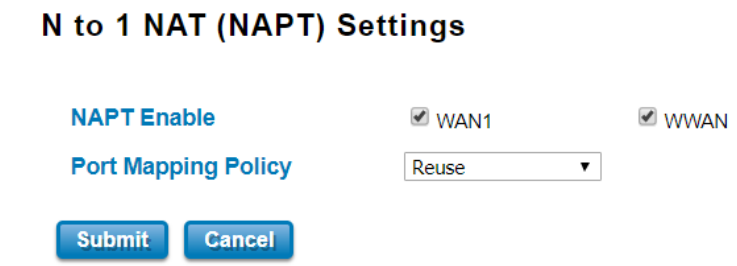
The description of the columns is as below:

TERMS	DESCRIPTION
DMZ	Select Enable to activate DMZ function.
DMZ Host IP Address	Configure the port range, which will be public to a WAN / Internet. User can configure one or a range of TCP/UDP port number.

Click **Submit** to apply the configuration.

N to 1 NAT (NAPT) /Port Mapping Policy

This page allows user to Enable NAPT interface and configure the Port Mapping policy from NAT Setting.



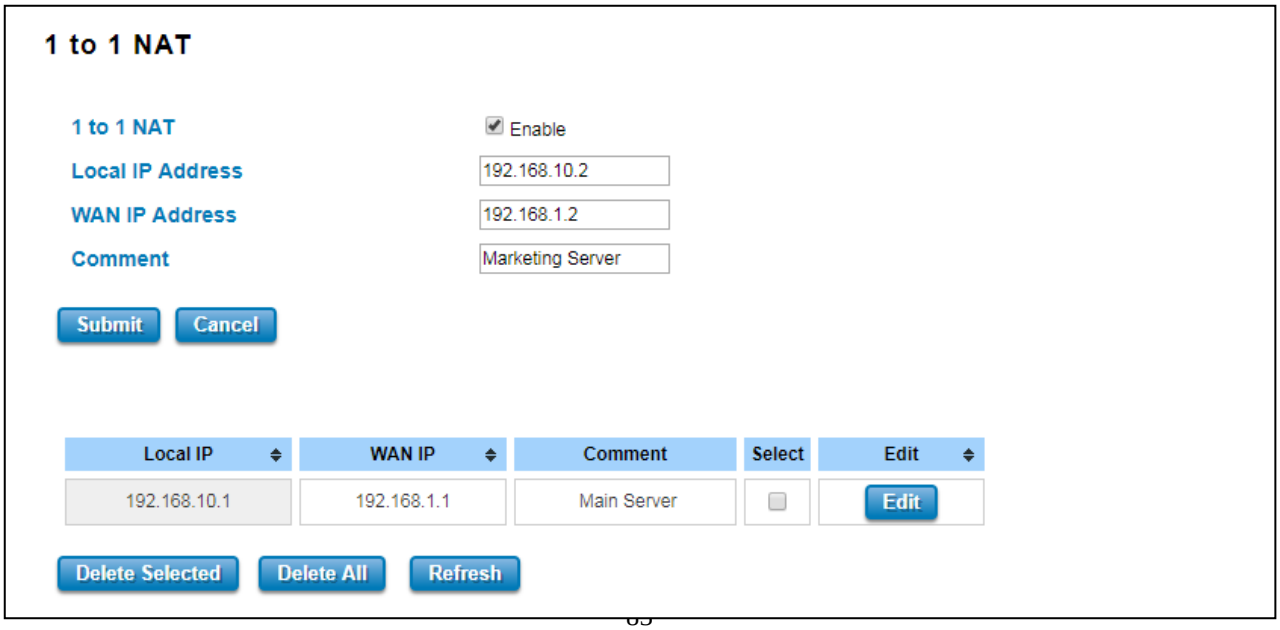
The description of the columns is as below:

TERMS	DESCRIPTION
NAPT Enable	Select the Interface while the router supports multiple WAN ports. There is only one activate WAN interfaces in this AP, select either Ethernet WAN or Wireless WAN. While you select Router/Client Router mode for both Ethernet and Wireless LAN interfaces, Client Router of Wireless WAN has higher priority and only it works.
Port Mapping Policy	**Default: Reuse** Reuse: Use the same port number that has been used to access the same remote device. Randomize: Change the port number every time access the remote device.

Click **Submit** to apply the configuration.

1 to 1 NAT

One-to-one NAT is a way to make systems behind a firewall and configured with private IP addresses (those reserved for private use in RFC 1918) appear to have public IP addresses. With one-to-one NAT, you assign local systems RFC 1918 addresses then establish a one-to-one mapping between those addresses and public IP addresses. For outgoing connections SNAT (Source Network Address Translation) occurs and on incoming connections DNAT (Destination Network Address Translation) occurs. Below is the 1 to 1 NAT section interface.



The description of the columns is as below:

TERMS	DESCRIPTION
1 to 1 NAT	Check the box to enable the function
Local IP Address	The target local IP Address
WAN IP Address	The incoming IP Address that coming through the WAN
Comment	Enter a comment

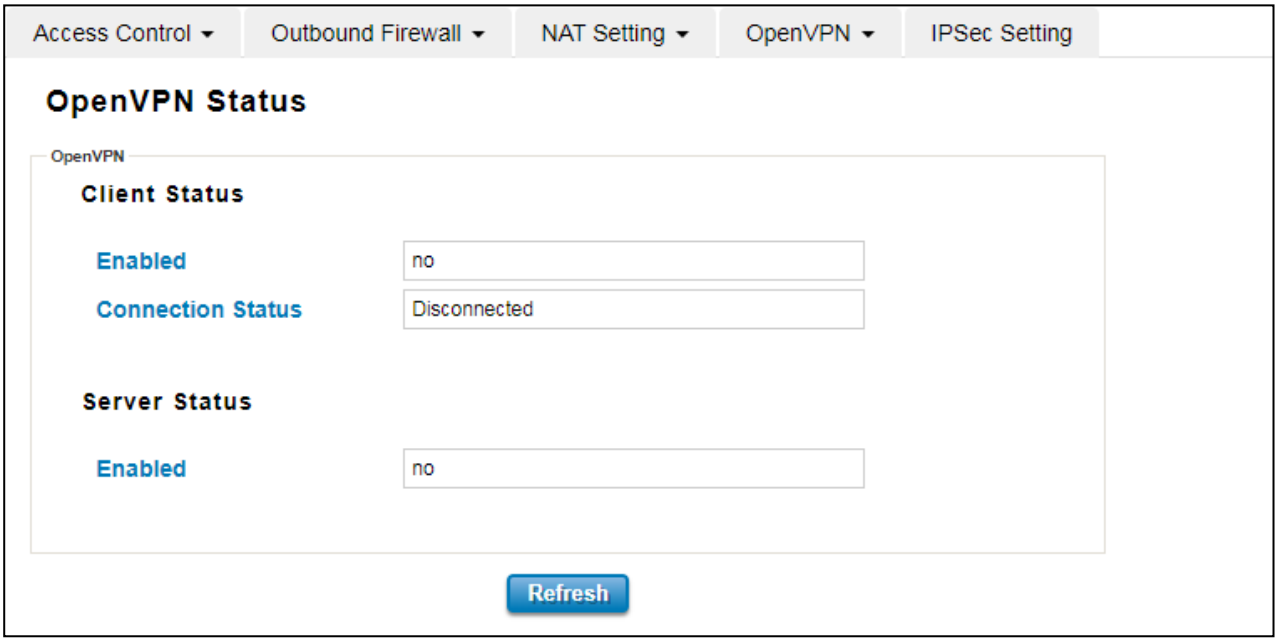
Click **Submit** to apply the configuration.

3.5.4 OpenVPN

WoMaster router supports OpenVPN. It implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections. It is possible to create one-to-many tunnel for the VPN Server. OpenVPN implementation offers a cost-effective, simply configurable alternative to other VPN technologies. OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. The server and client have almost the same configuration. The difference in the client configuration is the remote endpoint IP or hostname field. Also, the client can set up the keepalive settings.

OpenVPN Status

This section shows the VPN Client and Server current status.



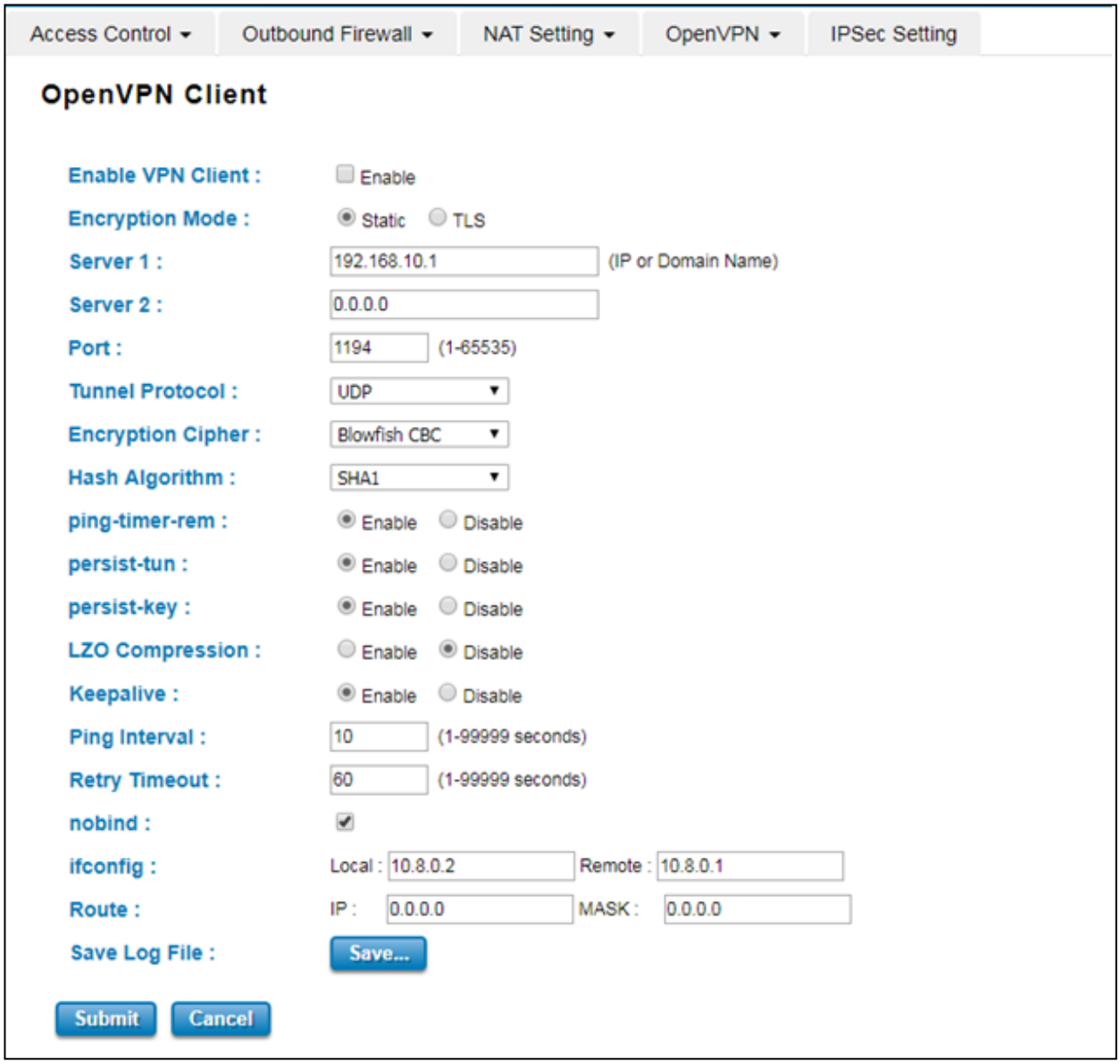
The description of the columns is as below:

TERMS	DESCRIPTION
Enabled	**Default: no** **yes:** The VPN function is enabled. **no:** The VPN function is not enabled
Connection Status	**Default: Disconnected** **Connected:** The VPN connection is established **Disconnected:** The VPN connection is not established

Click **Refresh** to update the information.

OpenVPN Client

This page is about the OpenVPN Client configuration page. While the device set as the VPN client, the parameters must follow the VPN Server settings. User should adjust the parameters with the administrator of the VPN server to entry the correct parameters. Two VPN servers IP are also provided in order to have the backup connection for VPN Server.



The description of the columns is as below:

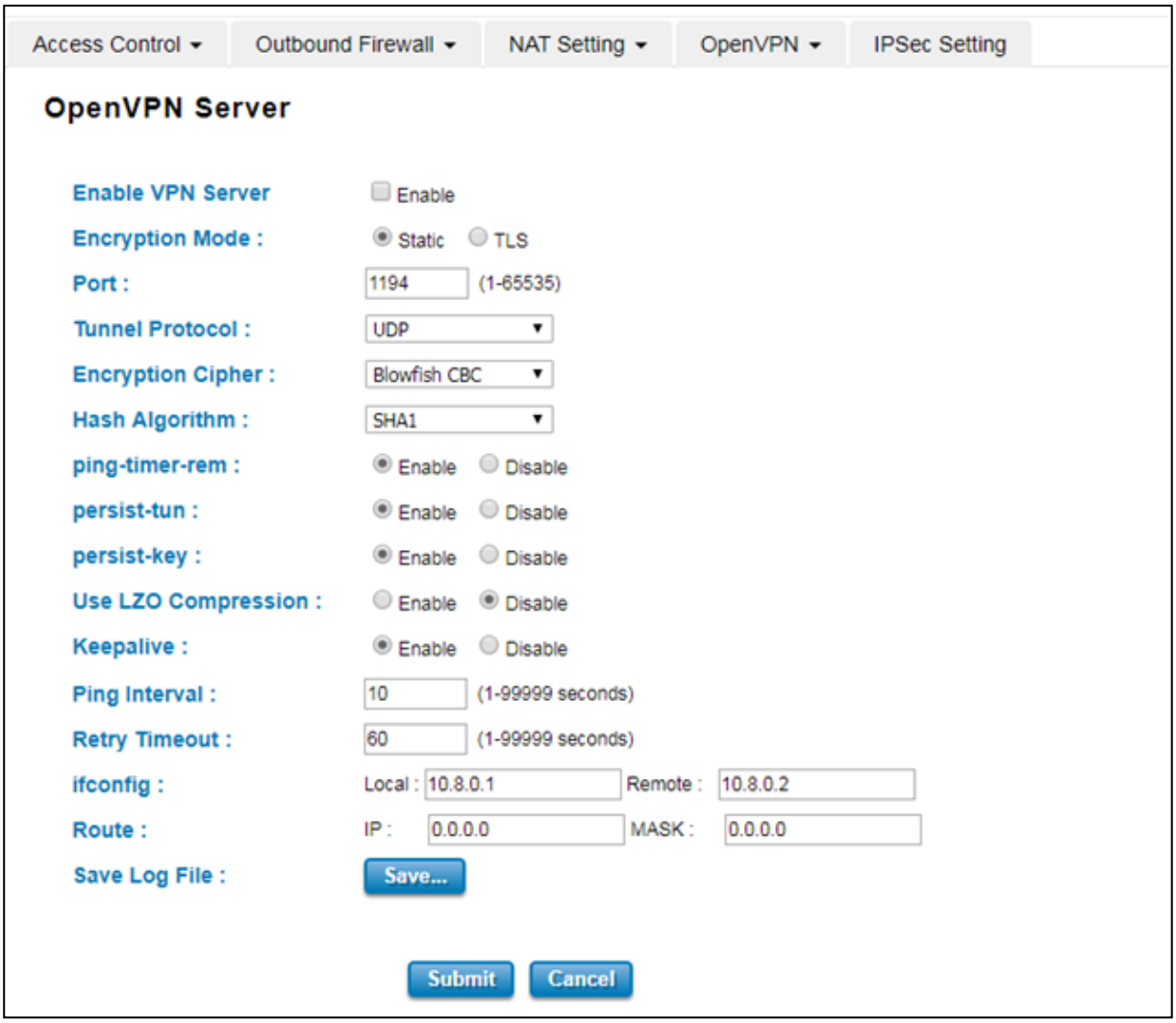
TERMS	DESCRIPTION
Enable VPN Client	Select Enable to activate the VPN Client function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the second IP Address of the VPN Server if needed.

Port	**Default: 1194** Input the port number that VPN service used. Please check the VPN Server port setting. The range from 1-65535.
Tunnel Protocol	Choose use TCP or UDP to establish the VPN connection.
Encryption Cipher	Select the encryption cipher from Blowfish to AES in Pull-down menus.
Hash Algorithm	Hash algorithm provides a method of quick access to data, including SHA1，SHA256，SHA512，MD5
ping-timer-rem	**Default: Enable** Select enable or disable the ping-timer-rem, this function prevent unnecessary restart at server/client when network fail.
persist-tun	**Default: Enable** Select enable or disable the persist-tun, enable this function will keep tun(layer 3) device linkup after Keepalive timeout.
persist-key	**Default: Enable** Select enable or disable the persist-key, enable this function will keep the key first use if VPN restart after Keepalive timeout.
LZO Compression	**Default: Disable** Select use LZO Compression or not, this function compresses data to decrease the traffic but also need more CPU effort.
Keepalive	**Default: Enable** Select enable or disable Keepalive function, this function is use to detect the status of connection.
Ping Interval	**Default: 10** Input the ping interval, the range can from 1~99999 seconds.
Retry Timeout	**Default: 60** Input the retry timeout, the range can from 1~99999 seconds.
nobind	Check the box to activate nobind function. With nobind function, the source ports are random.
ifconfig	Input the tunnel IP addresses that VPN use.
Route	Input the route IP and MASK. This is the target IP domain that user can access through the VPN tunnel.
Save Log File	Click Save to keep the VPN Client Log.

Click **Submit** to apply the configuration.

OpenVPN Server

To help user create the One to One Secure connection for the remote devices, WoMaster device supports both OpenVPN Server and OpenVPN Client. This Server setting allows user to configure the Secure M2M connection for one remote Client. But WoMaster router also supports one to multiple for VPN Client.



The description of the columns is as below:

TERMS	DESCRIPTION
Enable VPN Server	Select Enable to activate the VPN Server function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the second IP Address of the VPN Server if needed.
Port	**Default: 1194** Input the port number that VPN service used. Please check the VPN Server port setting. The range from 1-65535.
Tunnel Protocol	Choose use TCP or UDP to establish the VPN connection.

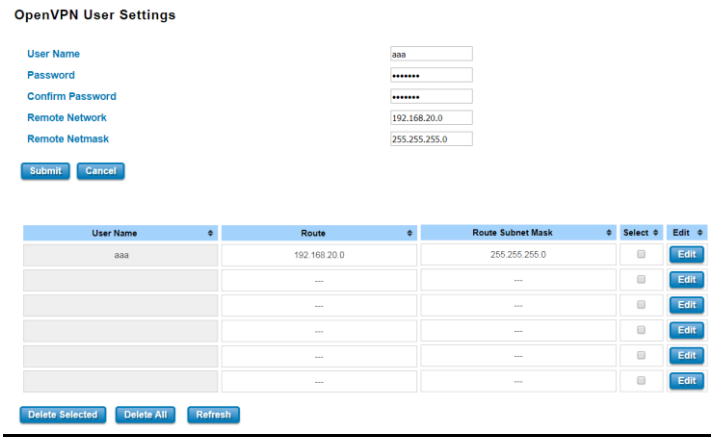
Encryption Cipher	Select the encryption cipher from Blowfish to AES in Pull-down menus.
Hash Algorithm	Hash algorithm provides a method of quick access to data, including SHA1, SHA256, SHA512, and MD5
ping-timer-rem	**Default: Enable** Select enable or disable the ping-timer-rem, this function is to prevent unnecessary restart at server/client when the network fails.
persist-tun	**Default: Enable** Select enable or disable the persist-tun, enable this function will keep tun(layer 3) device linkup after Keepalive timeout.
persist-key	**Default: Enable** Select enable or disable the persist-key, enable this function will keep the key first use if VPN restart after Keepalive timeout.
LZO Compression	**Default: Disable** Select use LZO Compression or not, this function compresses data to decrease the traffic, but also need more CPU effort.
Keepalive	**Default: Enable** Select enable or disable Keepalive function, this function is used to detect the status of the connection.
Ping Interval	Input the ping interval, the range can from 1~99999 seconds.
Retry Timeout	Input the retry timeout, the range can from 1~99999 seconds.
ifconfig	Input the tunnel IP addresses that VPN use.
Route	Input the route IP and MASK. This is the target IP domain that user can access through the VPN tunnel.
Save Log File	Click Save to keep the VPN Server Log.

Click **Submit** to apply the configuration.

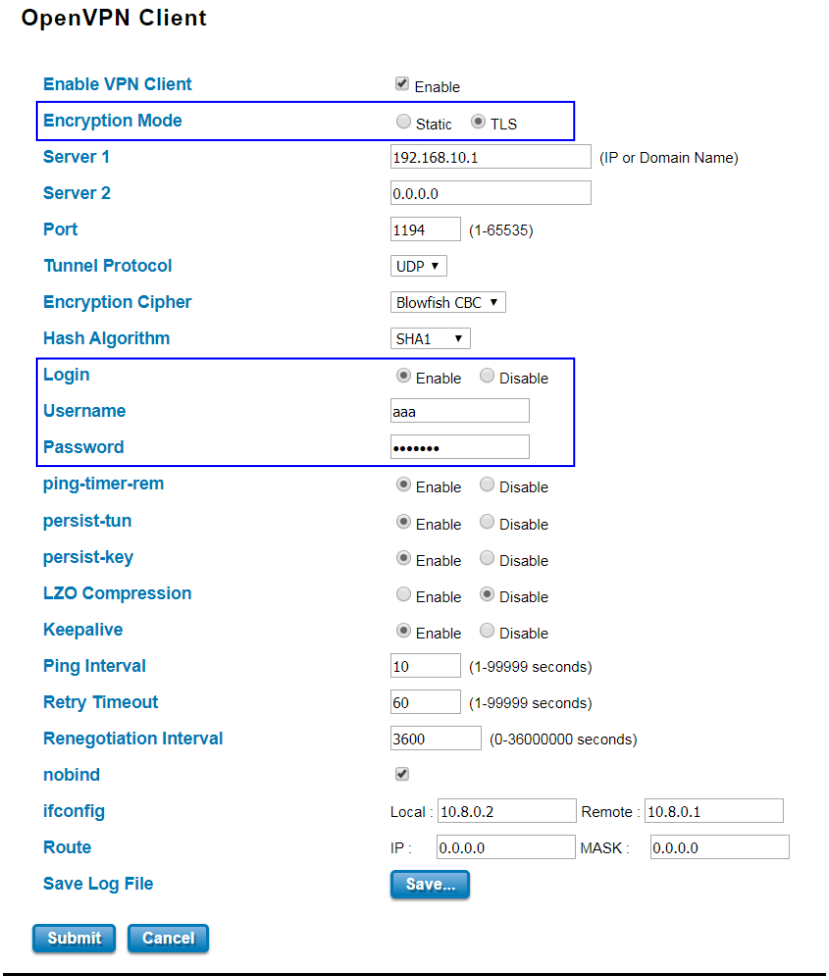
OpenVPN User Settings

This is extended setting of OpenVPN Server and applied in 1 Server to N Clients OpenVPN connectivity.

You can add User Name settings in this page. Add User Name, Password and Confirm Password, Remote Network and Netmask and click “Submit”. Then you can see the User Name database in below column.

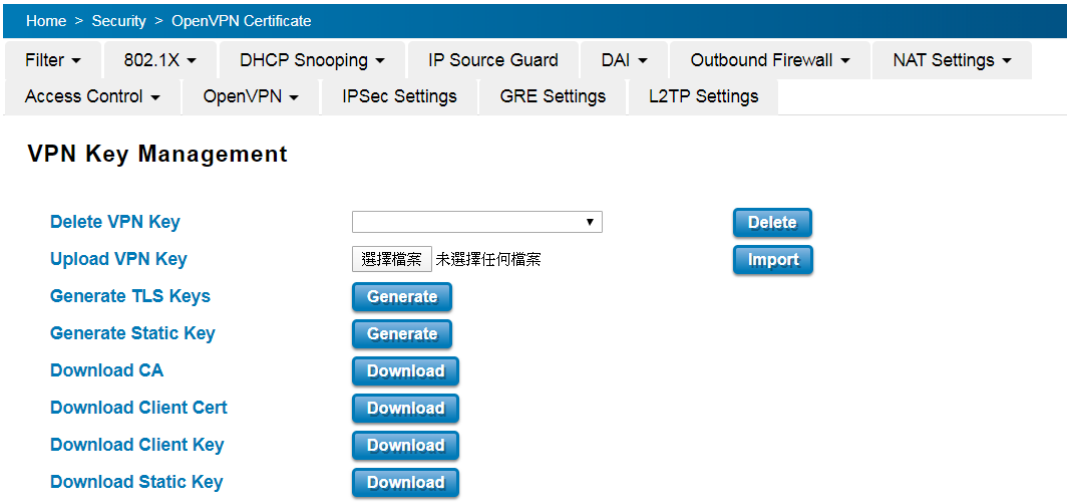


In OpenVPN client, you must type correct user name and password for authentication. Below is our OpenVPN client setting page, select the "**TLS**" Encryption Mode and Enable "**Login**" checkbox, then the Username/Password columns are displayed. Type correct Username and password added in OpenVPN User Settings.



OpenVPN Certificate

Using digital certificates for authentication instead of preshared keys in VPNs is considered more secure. In WoMaster' devices, digital certificates are one way of authenticating two peer devices to establish a VPN tunnel.



Key Generation in the device

For OpenVPN connectivity, the OpenVPN Client must have the client Key/CA file generated by the OpenVPN Server. Normally, you can generate the key in your VPN server and upload to the router switch which is Open VPN client. However, while you just want to establish site to site VPN connectivity, install another Open VPN server may consume lots of cost and engineer effort.

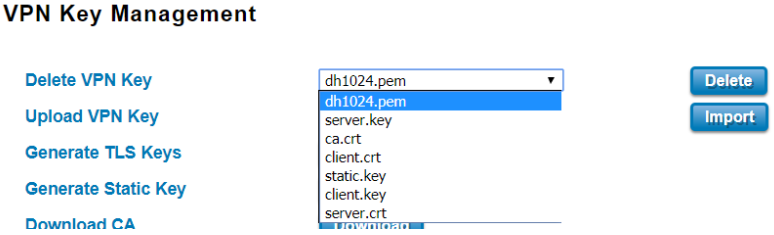
In the latest firmware, the WoMaster Secure Router Switch supports Key generation feature. Click **"Generate"** in **"Generate TLS Keys"** and **"Generate Static Key" in the Open VPN Router**, the system prompts you to wait 30 seconds to generate the key. Click "Yes" to start and wait 30 seconds. After generated, there are some VPN key/CA files generated and stored within the system. The files include both OpenVPN Server and Client key/ca files.

The two key/ca files, **dh1024.pem and server.crt** are applied to Open VPN Server only. The two files must be stored within the Open VPN server. **For security concern, the files are not allowed to download. You just need to generate the keys while configured the Router as an Open VPN Server.**

The rest of key/ca files include **CA, Client Cert and Client Key**. The three files must be stored within both the Open VPN server and client. You can download the keys to your PC and upload the files to OpenVPN client. Then the client has the same key. This is usefully tool for you to build you OpenVPN connectivity.

If you prefer to use Static Key, you can generate the **static.key** in OpenVPN Server and put the key in both OpenVPN Server and Clients.

You can see the files' name by select the drop-down menu of "Delete VPN Key", download/import OpenVPN client key/ca files in below columns.

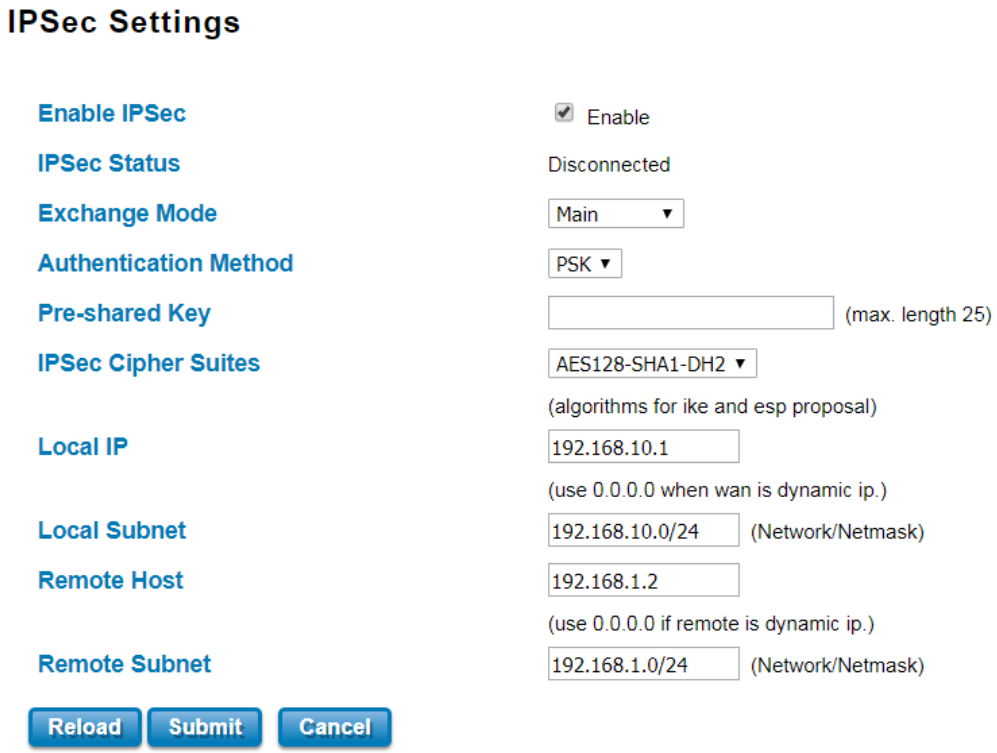


The description of the columns is as below:

TERMS	DESCRIPTION
Delete VPN Key	Display the ca/key files after generated TLS/Static Key. You can select and Delete the ca/key file here.
Upload VPN Key	Upload a certificate file from a specified file location.
Generate TLS Keys	The setting allows you to generate TLS key/ca files by the router switch. After click Generate, the system prompts you to wait 30 seconds to generate the key. Click Yes to start…then you will have multiple key/ca files.
Generate Static Key	The setting allows you to generate Static key by the router switch. After click Generate, the system prompts you to wait 30 seconds to generate the key. Click Yes to start… then you will have static.key file in the system.
Download CA	Download the generated ca.crt file here. Copy and Upload the key to the OpenVPN client Router.
Download Client Cert	Download the generated client.crt file here. Copy and Upload the key to the OpenVPN client Router.
Download Client Key	Download the generated client.key file here. Copy and Upload the key to the OpenVPN client Router.
Download Static Key	Download the generated static.key file here. Copy and Upload the key to the OpenVPN client Router while you prefer to establish OpenVPN connectivity by using Static Key.

3.5.5 IPSEC Settings

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. By configure this configuration page, user allows IPsec tunnels to pass through the router.



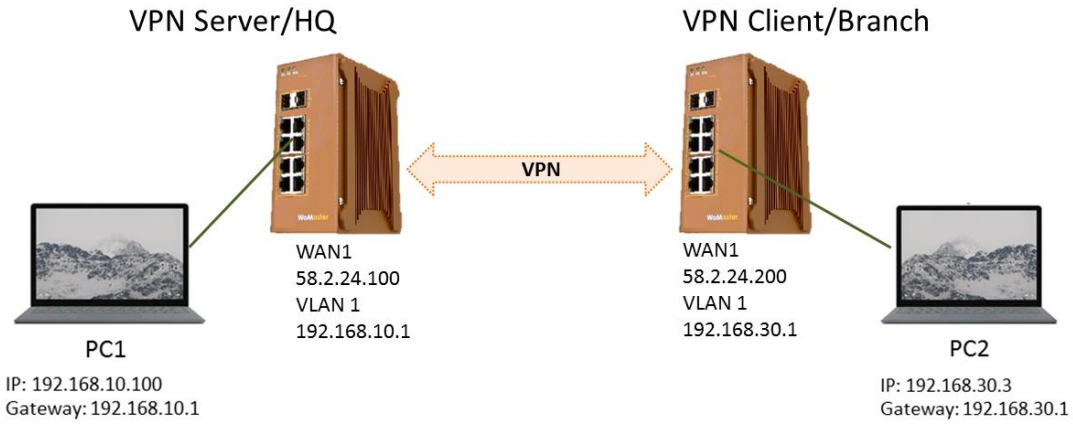
The description of the columns is as below:

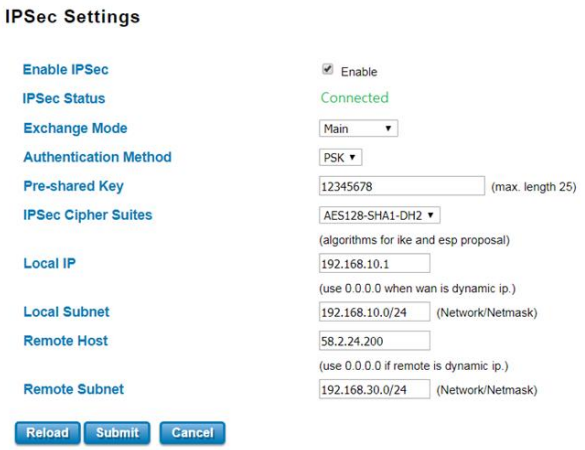
TERMS	DESCRIPTION
Enable IPsec	Select Enable to activate the IPsec function
IPsec Status	Display the IPsec status, whether it is connected or disconnected When the VPN is connected, the IPsec status will display “Connected”. IPsec Status Connected
Exchange Mode	Main or Aggressive mode selection
Authentication Method	Default: PSK Optional: Pre Shared Key or Certificate
Pre-shared key	**Default: none** Type the Pre-shared key. The Pre-share key must be the same in both ends.
IPsec Cipher Suites	**Default: AES128-SHA1-DH2** Set algorithms for IKE and ESP proposal, choose AES128-SHA1-DH2, DES-SHA1-DH2, 3DES-SHA1-DH2 and AES256-SHA1-DH2. The cipher must be the same in both ends.
Local IP	IP Address of the local side of the tunnel. (Use 0.0.0.0 when WAN is dynamic IP.)
Local Subnet	Set IPSec local protected subnet and subnet mask, i.e. 192.168.1.0/24
Remote Host	**Default: 0.0.0.0** Set IPsec Remote Host, use the default setting if remote is dynamic IP

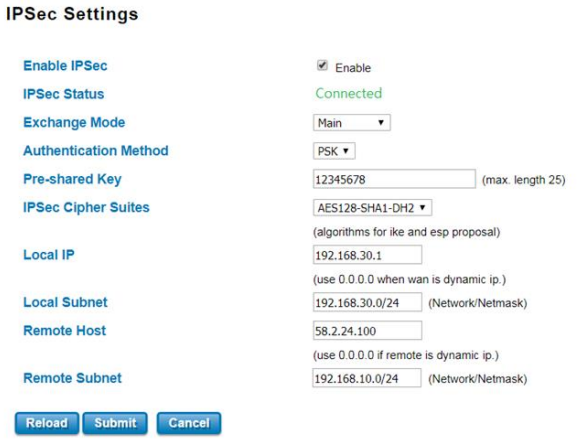
Remote Subnet	Set IPsec Remote Protected Subnet/Subnet Netmask

Click **Submit** to apply the configuration.

An Example of IPSec VPN:







The reference topology above is how the branch office can get the access to the headquarter. The two laptops are connected to the secure router switch through the Ethernet cable.

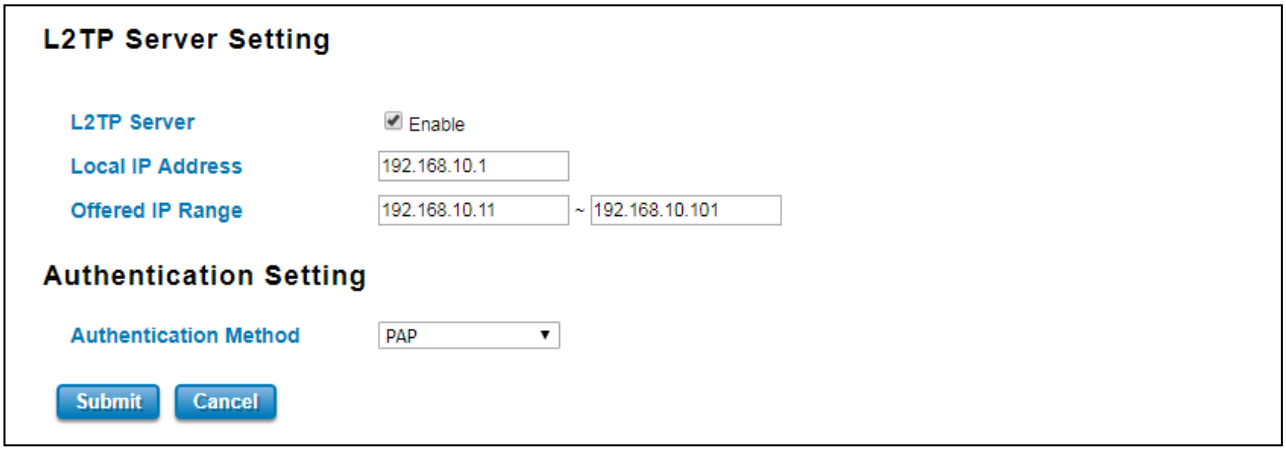
Enable the IPSec, type the same pre-share key and select the same cipher for both ends.

Configure the IP address for both ends. The Router at the branch office normally acts as the VPN Client role (not really client mode in IPSec), the Router at head quarter normally acts as the VPN Server role. The HQ normally has public IP, that's the Remote IP of the router in branch office. The local subnet in HQ is the remote subnet of the router in branch office. If you have public IP in branch, it's better to use public IP address for the WAN interface. If you just have dynamic IP address for branch office, then use 0.0.0.0 as local IP.

To check the connection status, you can use Ping tool in Router's Web GUI to check the WAN connection. You must ping remote WAN IP address successfully first. Then you can try ping from PC2 to its connected interface, WAN IP of two routers and then remote PC1. This is also the typical debugging rule to check WAN and VPN connectivity.

3.5.6 L2TP SETTING

L2TP is a popular choice for remote roaming users for VPN applications since an L2TP client is built in to the Microsoft Windows operating system. In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy. Below is the L2TP Server Setting interface.

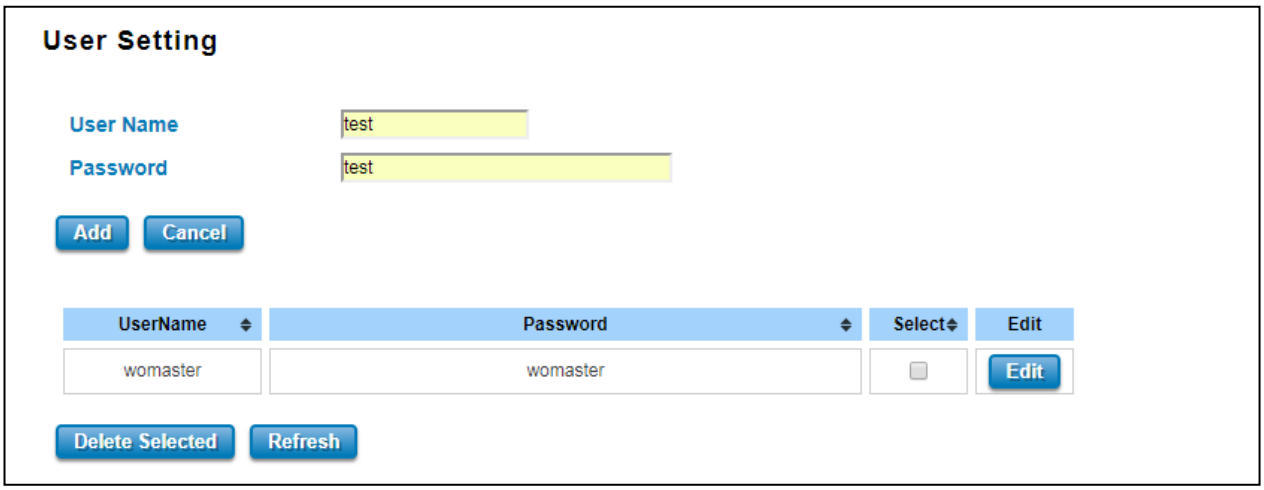


The description of the column is as below:

TERMS	DESCRIPTION
L2TP Server	Check the box to enable the function.
Local IP Address	The IP Address of the L2TP Server.
Offered IP Range	Offered IP Address range for the L2TP Clients (Maximum 10 clients)
Authentication Method	This section belongs to User Setting section. User can choose authentication using the password authentication protocol (PAP) and challenge handshake authentication protocol (CHAP).

Click the **Submit** button to apply the configuration.

Below is the User Setting for the L2TP Authentication connection.



The description of the column is as below:

TERMS	DESCRIPTION
User Name	Username for L2TP connection

Password	Password for L2TP connection
Select	Select the list on the table, so user can press **Edit** or **Delete Selected** to delete.

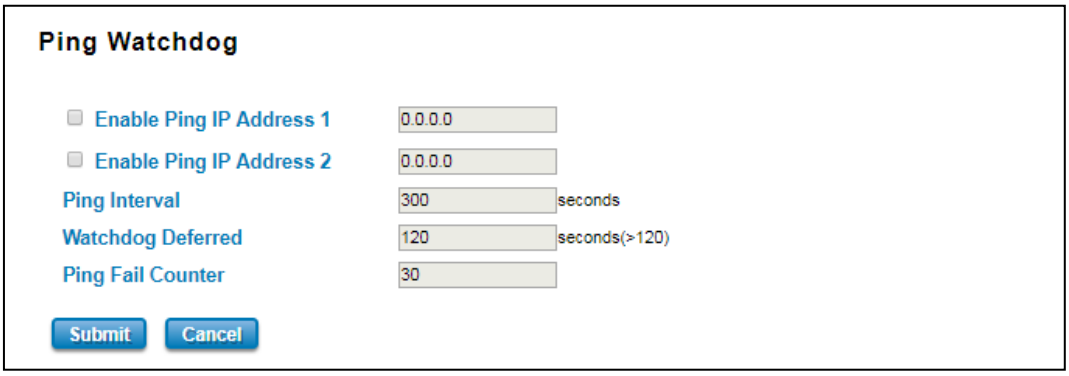
Click the **Refresh** button to refresh the list.

3.6 Warning

WoMaster' router provides several types of Warning feature for remote monitoring of end devices status or network changes.

3.6.1 Ping Watchdog

Ping Watchdog is a feature that helps WoMaster' router to allow user continuously ping a specific remote host for



connection status using a user-defined IP address (or an Internet gateway). In this section, WoMaster provides two target IP Addresses, in order if the other IP Address cannot be reached, so there is another backup IP address. There are two conditions in this Ping Watchdog section, the first one is when the device continuously ping the target IP and in the end, it can reach one of the target IPs the device would not reboot. But if both targets IPs cannot be reached, the device will start counting the Ping Fail Counter time till it can be reached. If it is unable to ping the target IP address, this device will automatically reboot. After User finishes configuring the settings, click on **Submit** to apply User configuration.

The description of the columns is as below:

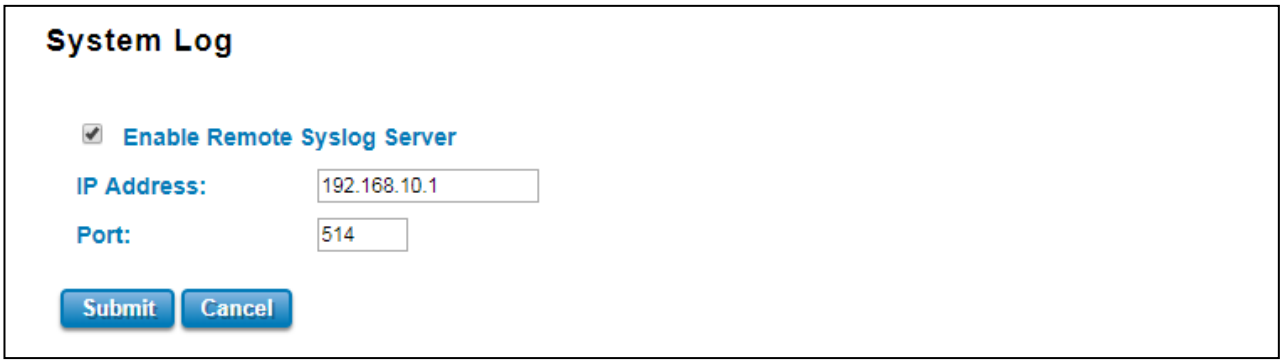
TERMS	DESCRIPTION
Enable Ping IP Address 1	Clicks enable to activate the feature. Set the first IP Address to check if the device is alive or not
Enable Ping IP Address 2	Clicks enable to activate the feature. Set the second IP Address to check if the device is alive or not
Ping Interval	**Default: 300 (seconds)** Set the interval timer to Ping the remote device. Every 300 seconds the device will try to ping the target IP.
Watchdog Deferred	**Default: 120 (seconds) >120** The device needs time to boot, the startup delay use to buffer to prevent the device continue to reboot itself.
Ping Fail Counter	**Default: 30** When the remaining Ping Fail Counter reach to 0 or reach the failure count, the device will reboot.

Click **Submit** to apply the configuration.

3.6.2 SYSLOG Settings

System Log is useful to provide system administrator locally or remotely monitor router events history.

Once User finishes configuring the settings, click on **Submit** to apply User configuration. User can monitor the system



logs in [Diagnostics] / [Event Log] page

The condition or term described as following table.

TERMS	DESCRIPTION
Enable Remote Syslog Server	Select Enable to enable system log
IP Address	Specify the IP address of the server.
Port	**Default: 514** Specify the port number of the server

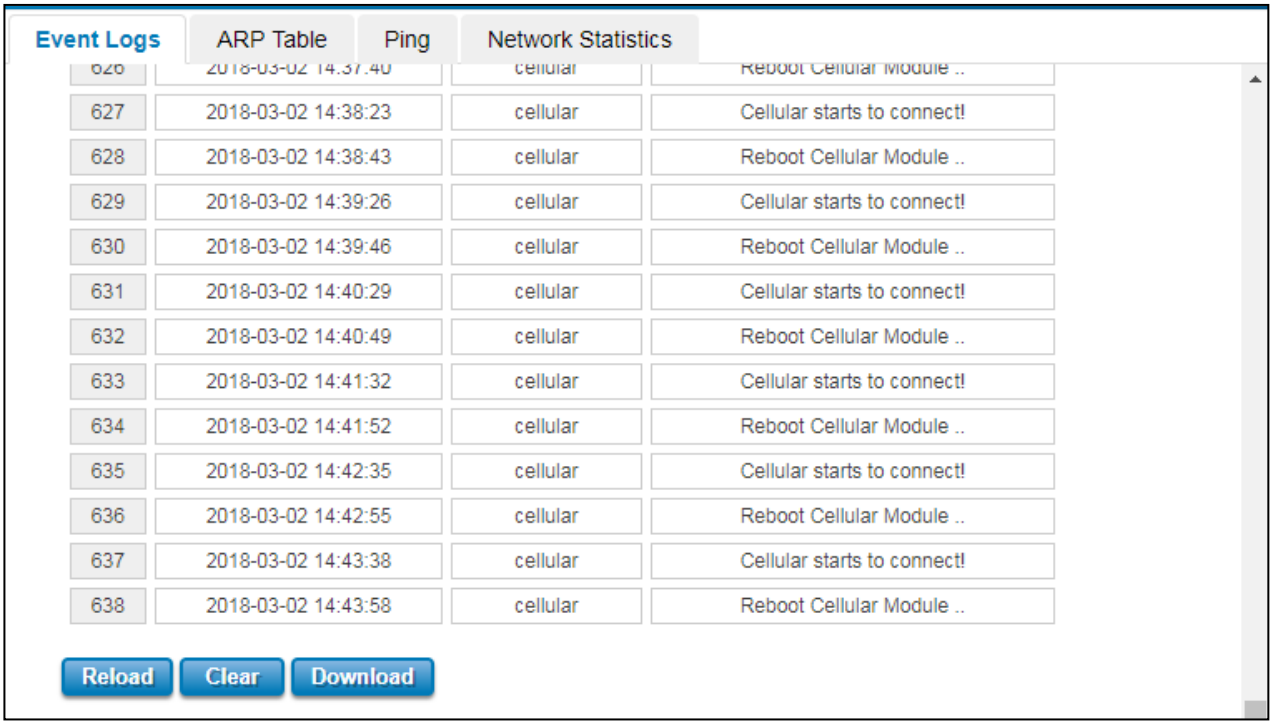
After finish with the configuration, clicks **Submit** to activate the function.

3.7 Diagnostics

WoMaster Router provides several types of features for User to monitor the status of the router or diagnostic for User to check the problem when encountering problems related to the router.

3.7.1 Event Logs

When remote System Log server mode is activated, the router will record occurred events in local log table. This page shows this log table. The entry includes the index, occurred data, time and content of the events.



TERMS	DESCRIPTION
#	Event index assigned to identify the event sequence.
Time	The time is updated based on how the current date and time is set in the Basic Setting page.
Source	Show the log's source.
Message	Show the record status.

Click **Reload** to refresh the table. Click **Clear** to remove the entire event logs list. User may download the event logs file by click **Download**.

3.7.2 ARP Table

Basically, WoMaster device is supported with two types of ARP which is the standard ARP and ARP with 802.2 LLC Type 2. Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. The other ARP feature is ARP with 802.2 LLC Type 2 is the new level of ARP where the device will response the request of 802.2 snap ARP on the Ethernet port and not support sending the request of 802.2 snap ARP. Below is the Data format.

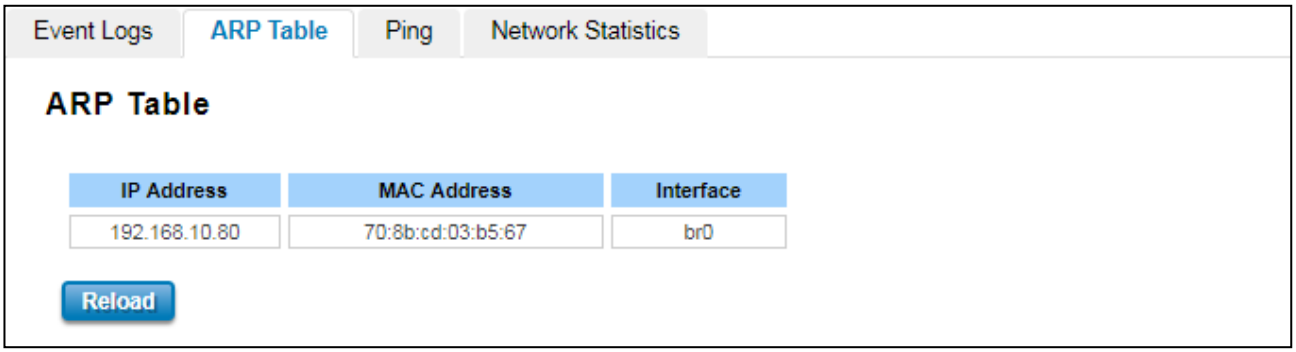
Data Format

Protocol Header:

802.3 + 802.2 LLC + 802.2 snap

|- (DS + SA + Len) -|- DSAP + SSAP + CTRL -|- Org + type

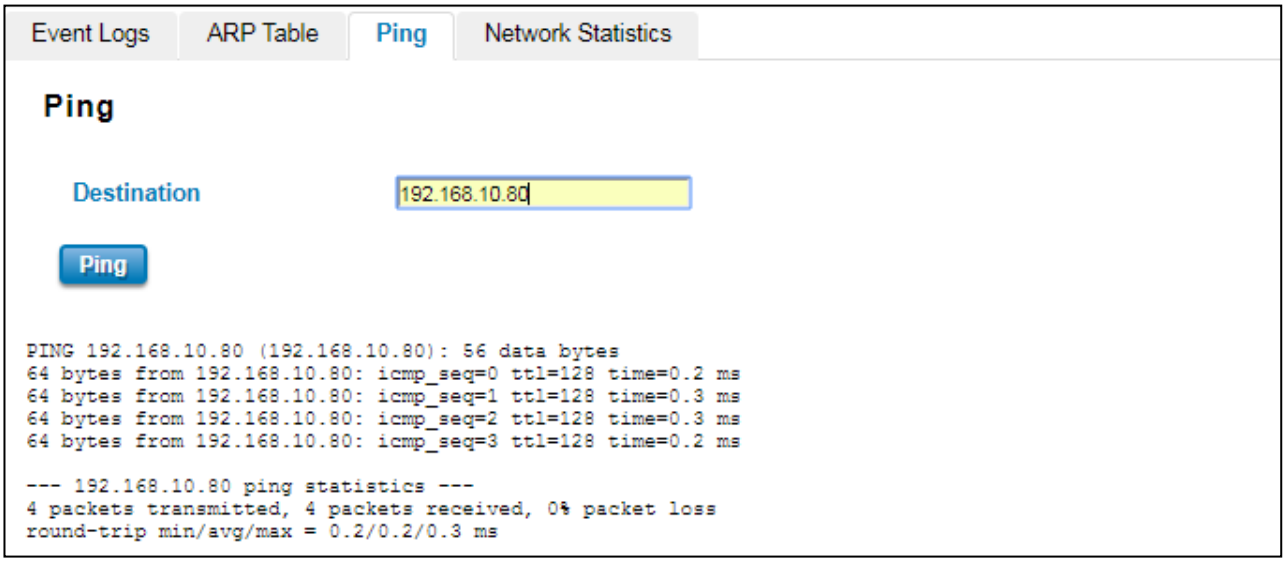
This page shows the routers active ARP table. An ARP table contains recently cached MAC addresses of every immediate device that was communicating with the router.



Click on **Reload** to change the value.

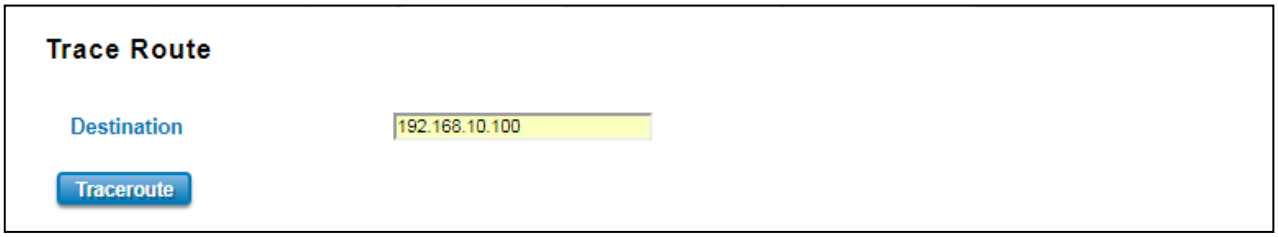
3.7.3 Ping

WoMaster' provides **Ping** utility in the management interface, the function is to give users a simple but powerful tool for troubleshooting network problems and check that the remote device is still alive or not. Type **Destination** IP address of the target device and click on **Ping** to start the ping.

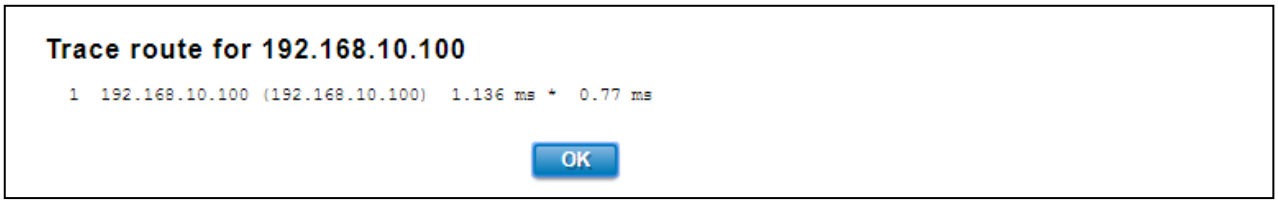


3.7.4 Traceroute

Traceroute is a diagnostics tool for displaying the route (path) and measuring transit delays of packets across an Internet IP network. Log containing route information will be shown after few seconds. Enter the destination IP Address then click traceroute to start the process.

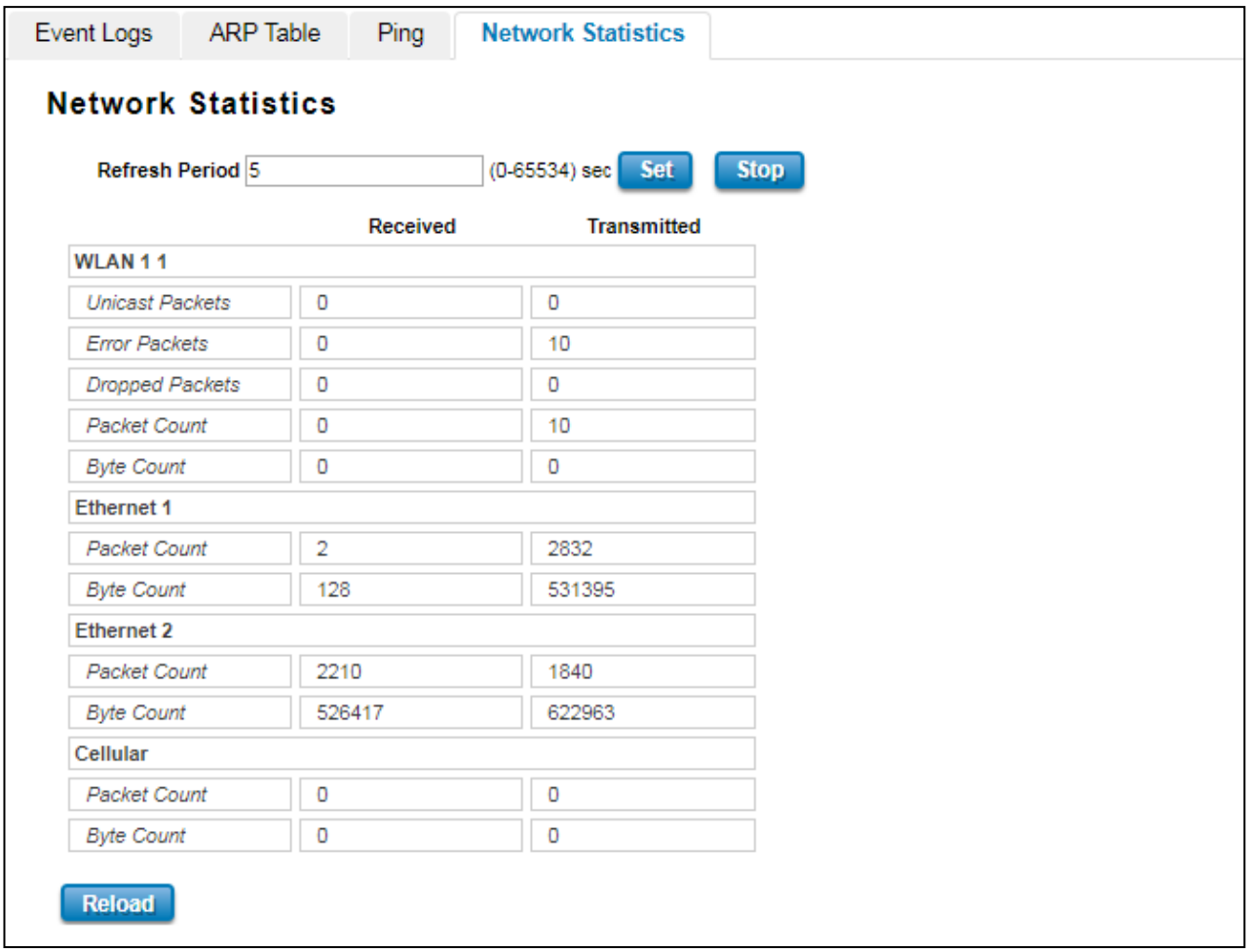


It will start search the route and measuring the transit delays of the packet.



3.7.5 Network Statistics

This section shows about the packet data that transmitted or received regarding the Ethernet and Cellular activity. The Cellular packets include Wi-Fi and 2G/3G/LTE transmission.



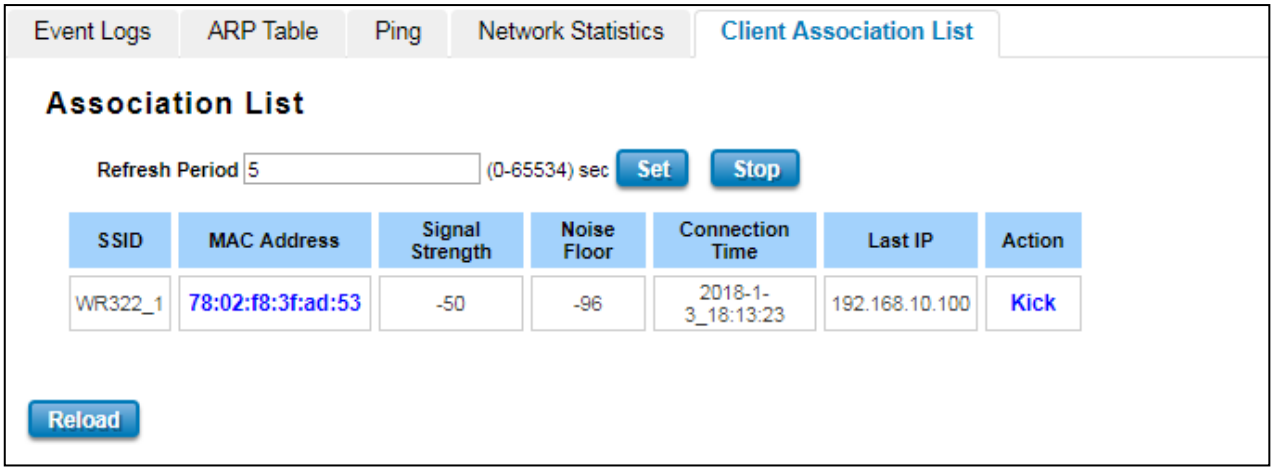
Click on **Reload** to refresh the table.

The description of the columns is as below:

TERMS	DESCRIPTION
Poll Interval	**Default: 5** To set the Poll Interval time setting with range from 0 to 65534. (second)
Set	To set new Interval time. Stop the old Poll Interval first before set the new interval.
Stop	To stop Polling Interval, this action can be executed when user wants to change the poll interval time.

3.7.6 Client Association List

This Client Association List displays the current wireless connection status when there is a client that connected to the AP. It shows the SSID, MAC Address, Signal Strength, Noise Floor, Connection Time, Last IP and Action. For the security concern, in this page user can do the security action, such as **Kick** the unexpected user from the wireless networks. This page also provides the refresh function to refresh the list automatically, where user may set the refresh period for refresh the list. Click **Set** to apply the setting, click **Stop** to stop the refresh function.



Click **Reload** to refresh the list.

The description of the columns is as below:

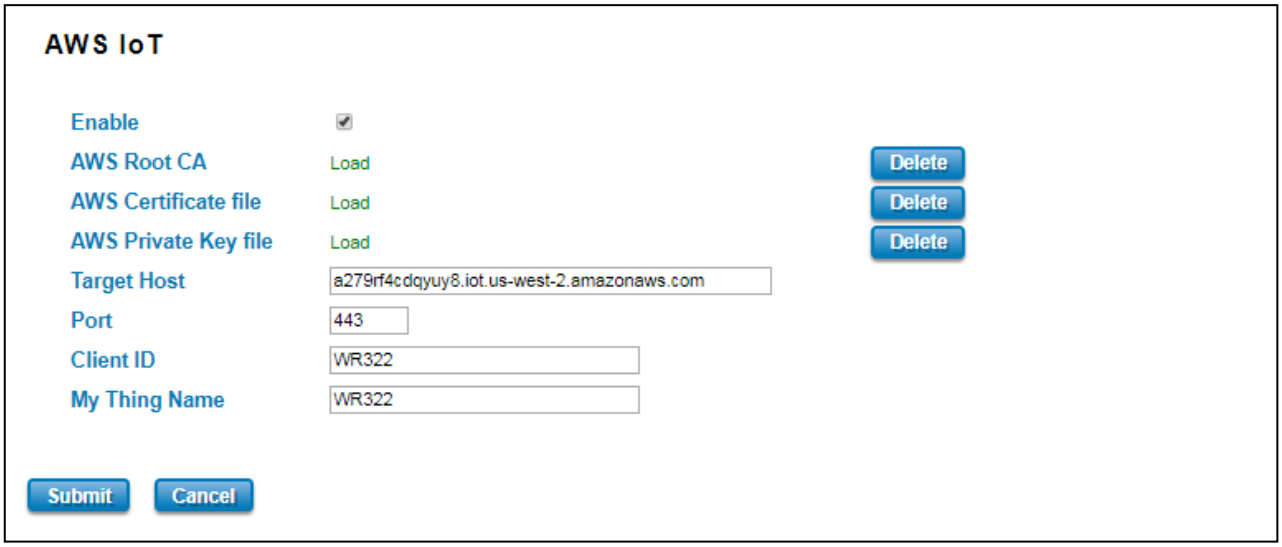
TERMS	DESCRIPTION
SSID	Display the primary name of the SSID that available on the network.
MAC Address	Display the MAC Address that connected to the AP.
Signal Strength	Display the connection signal strength.
Noise Floor	Display the background noise level.
Connection Time	Display the time when the client connected to the AP.
Last IP	Show the IP Address of the wireless client.
Action	In this section user may do an action by **kick** the unexpected wireless client.

3.8 IoT

Over the past decade or so, the word “cloud” has taken on a new meaning to many people. Rather than a visible mass of condensed water vapor floating in the sky, the cloud has taken to the IoT industry in the form of data. WoMaster Industrial Router is supported with private clouds, ThingsMaster and public clouds, AWS and Microsoft Azure. Clouds offer great promise in improving the agility and flexibility of IT to respond to the requirements of the business cost effectively. The security challenges raised by the loss of control and visibility in the journey to the cloud can be addressed in terms of securing infrastructure, information, identities, and devices.

3.8.1 AWS IoT

Amazon Web Services IoT enables secure, bi-directional communication between Internet-connected things (such as sensors, actuators, embedded devices, or smart appliances) and the AWS cloud over MQTT and HTTP. For more information please visit: http://aws.amazon.com/iot/.



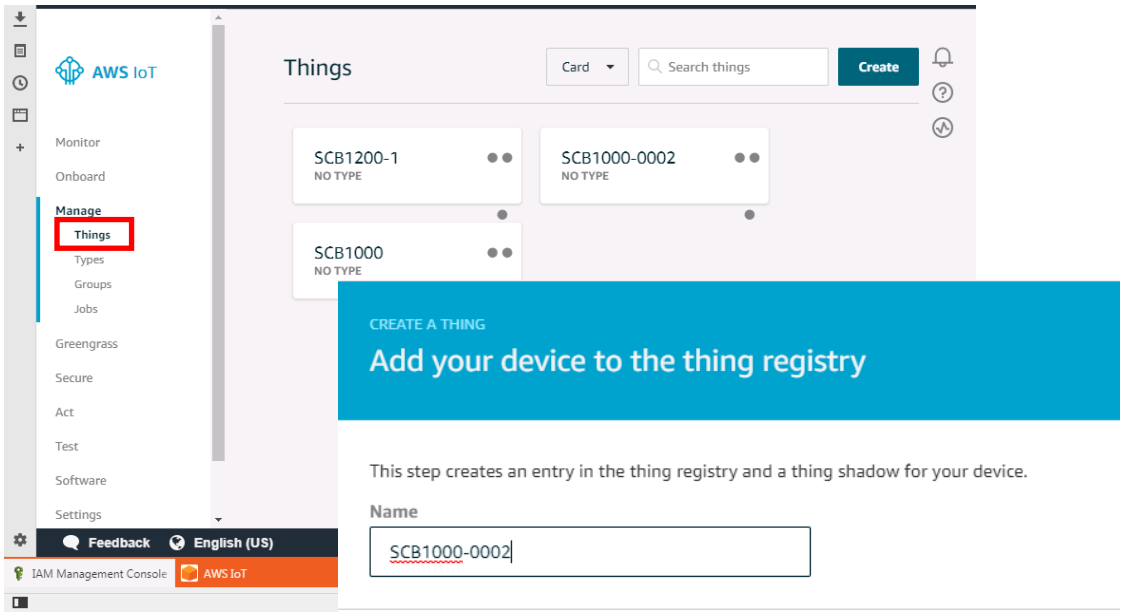
The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Enable the AWS IoT function
AWS Root CA	Root CA is necessary. User can download it from the AWS.
AWS Certificate file	Certificate is necessary. User can download it from the AWS.
AWS Private Key file	Private key is necessary. User can download it from the AWS.
Target Host	Enter the target host
Port	**Default: 433** Because AWS uses the HTTPS traffic, user need to add an inbound rule on port 443
Client ID	Enter the device client ID
My Thing Name	Enter the registered device name (Need to be the same)

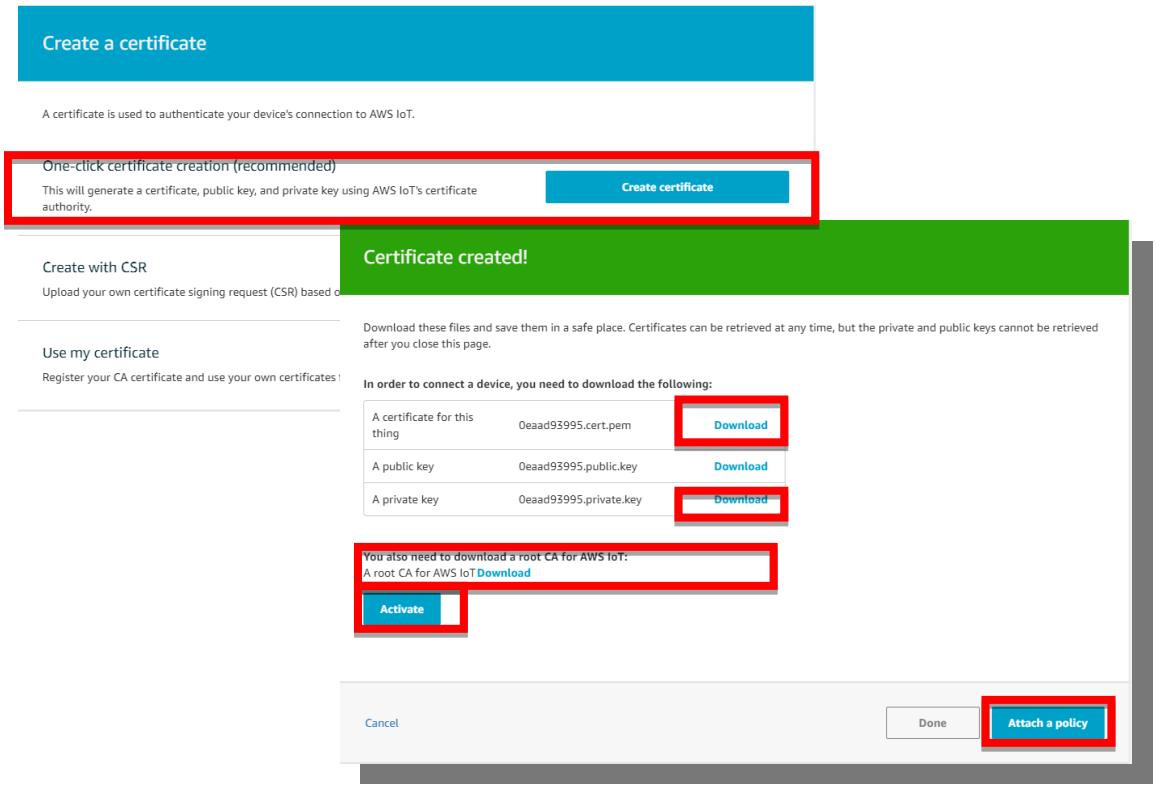
Click **Submit** to apply the configuration.

HOW TO CONNECT THE DEVICE TO AWS

- Create and login to AWS account.
- Select AWS IoT Services – click Thing.
- Add your device shadow.



- Create and download the key or certificate.

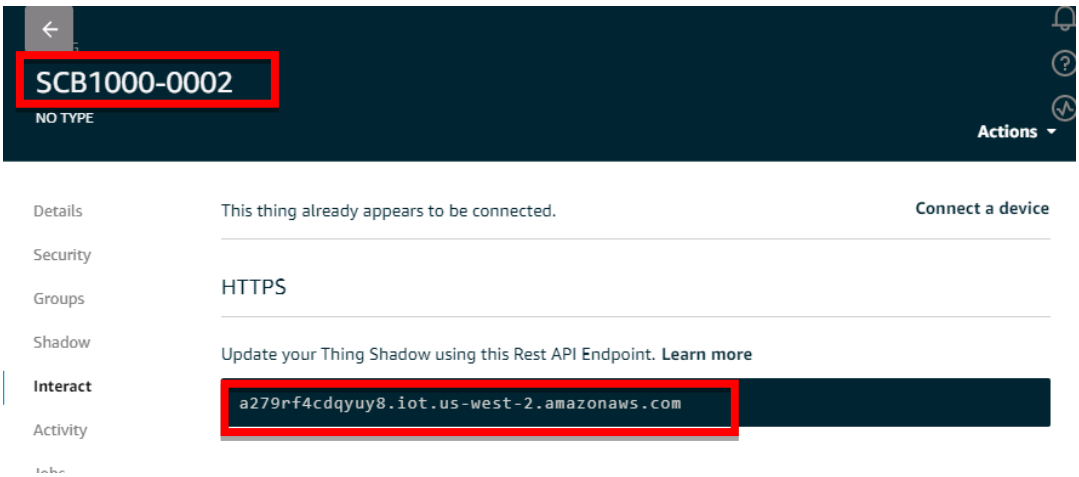


Certificate, private key, root CA is necessary. Public key is used by AWS server to authenticate with private key. The public key and private cannot be downloaded back after the user closes the page. Policy can be added later.

- Get the Target host to connect with the device.

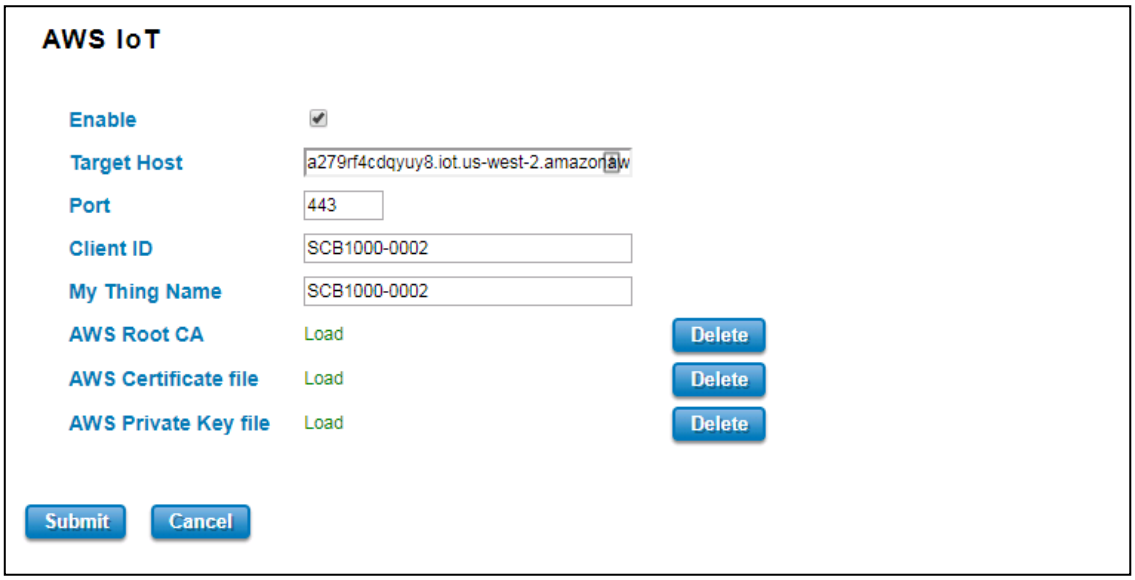
  Go to Manage -> Things -> click the device name -> Click Interact.

  Copy the HTTPS link to update user's Thing Shadow using this Rest API Endpoint.



- Connect the device to AWS.

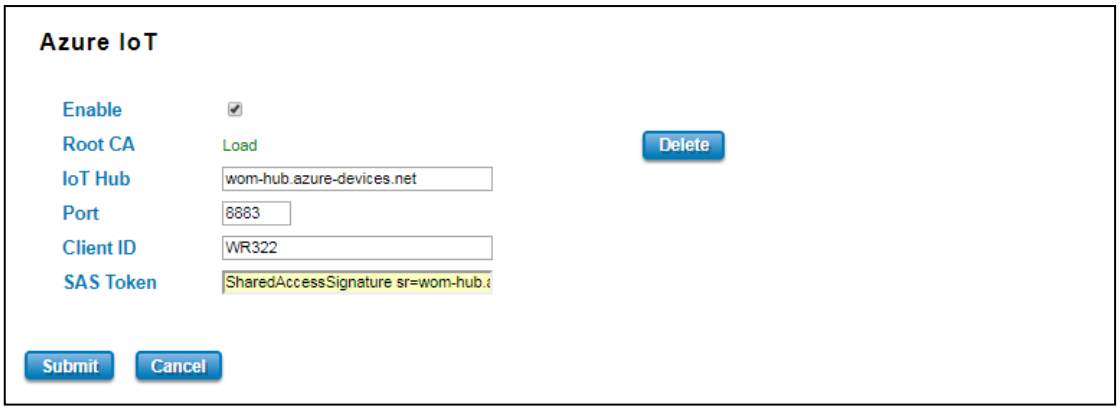
  Copy the link and paste on the Target Host field at the AWS IoT page.



3.8.2 AZURE IoT

Azure IoT Hub is a fully managed service that enables reliable and secure bi-directional communications between millions of Internet of Things (IoT) devices and a solution back end. One of the biggest challenges that IoT projects face is how to reliably and securely connect devices to the solution back end. To address this challenge, IoT Hub:

- Offers reliable device-to-cloud and cloud-to-device hyper-scale messaging.
- Enables secure communications using per-device security credentials and access control.
- Includes the most popular communication protocols.



The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Enable Azure IoT function
Root CA	Download and enter the root CA.
IoT Hub	Enter the IoT hub server, this information can be found at the azure platform
Port	**Default: 8883** Display the port number. Because Azure IoT uses the MQTT protocol, so user needs to enter 8883 port number that belongs to MQTT protocol.
Client ID	Enter the client ID
SAS Token	Enter the SAS Token that needs to be generated by software. (Azure Device Explorer)

Click **Submit** to apply the configuration.

HOW TO CONNECT THE DEVICE TO MICROSOFT AZURE

CREATE IOT HUB

To register the device in Azure Portal, user has to follow the guide “Get started with Azure IoT Hub for Java”: https://azure.microsoft.com/en-us/documentation/articles/iot-hub-java-java-getstarted/.

The guide explains how to create an IoT Hub and a device entity. It is important to annotate the connection string generated after creating the device entity. User will need this parameter later for the device configuration (WoM IoT Configuration).

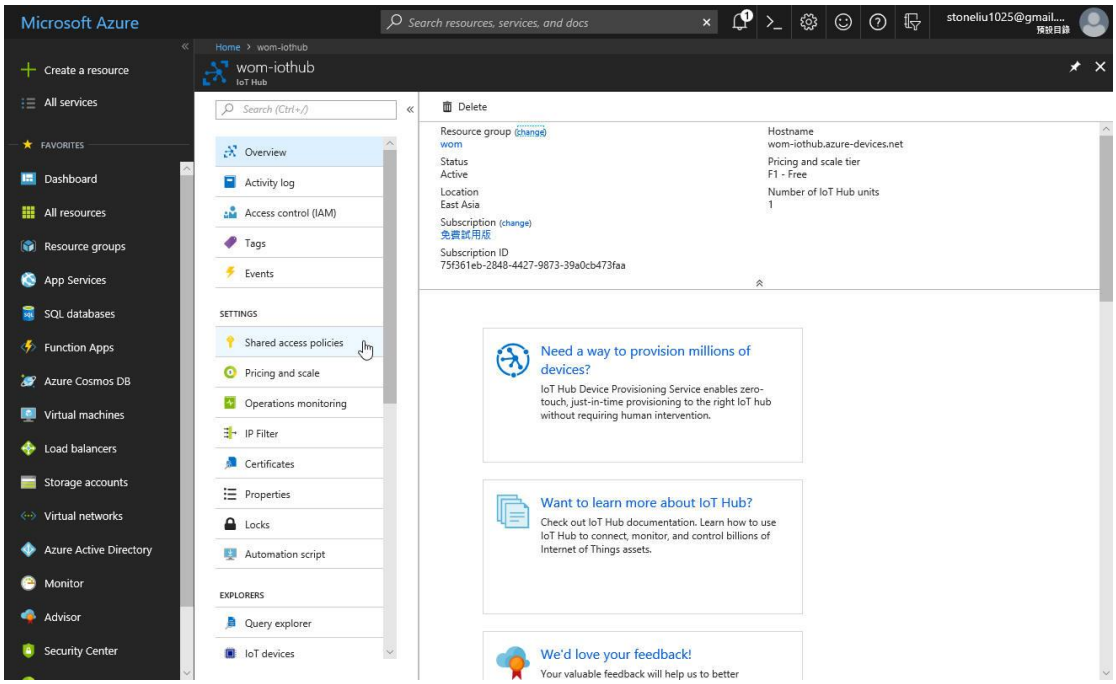
CONFIGURE THE DEVICE AS A MQTT CLIENT

In the Microsoft Azure Portal, go to IoT Hub menu and select:

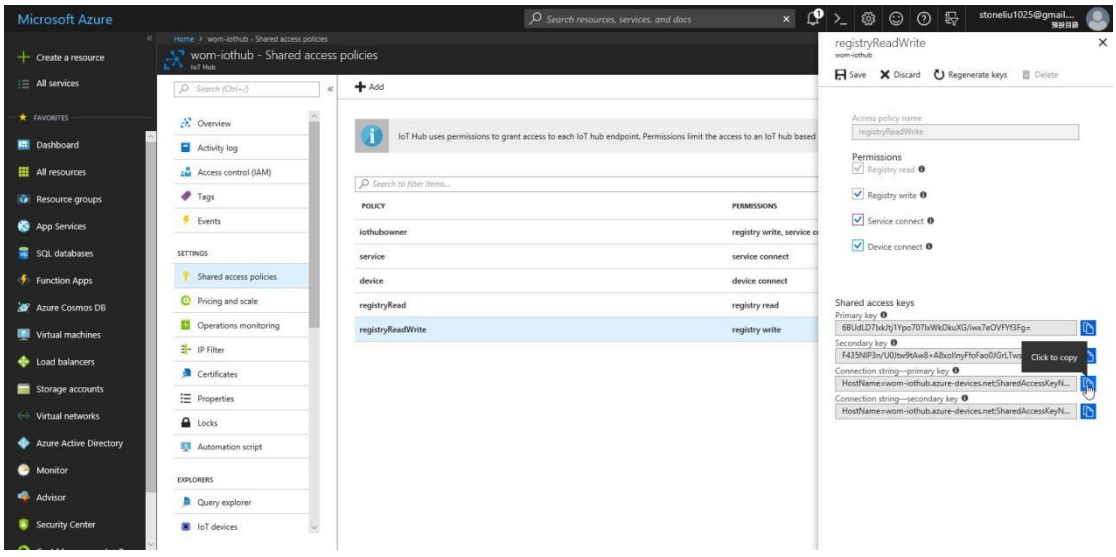
Devices > myCreatedDevice > Shared access policies > iothubowner > Connection string - primary key.

User has to annotate the value of this field.

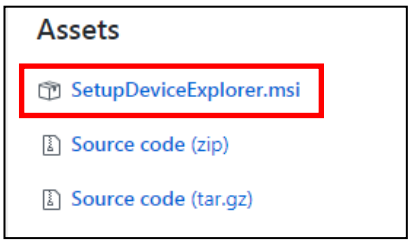
1. Get the connection string. Click the IoT Hub -> Shared access policies.



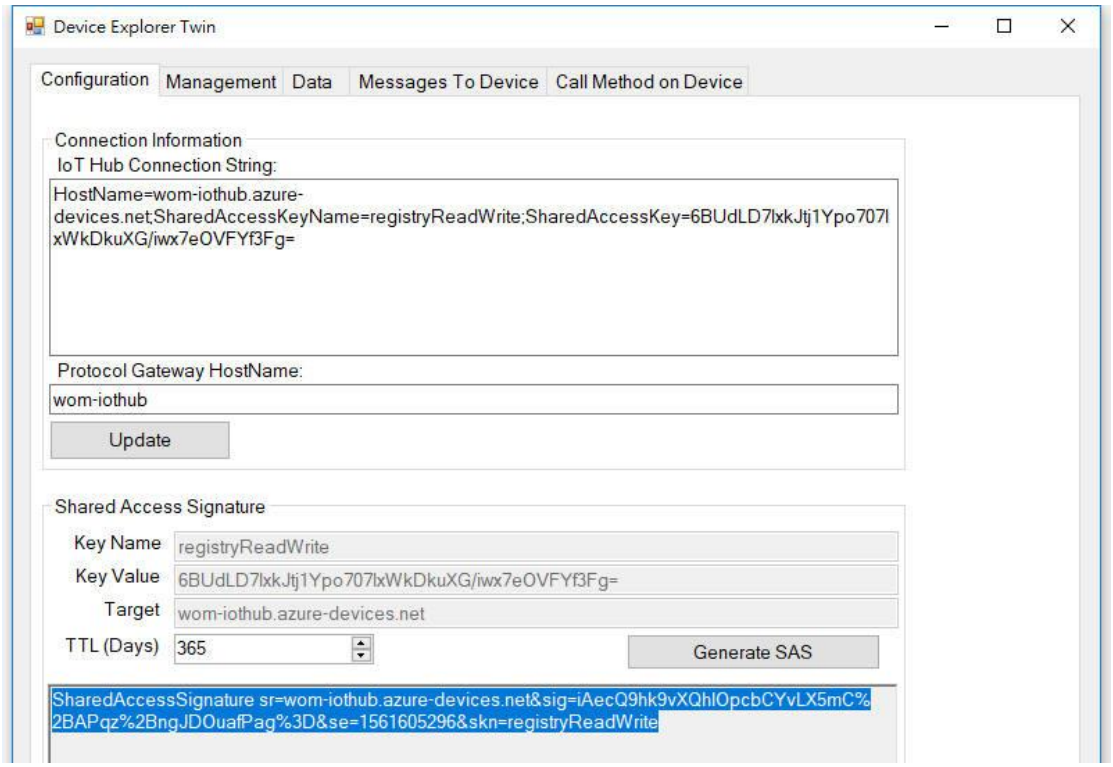
2. Click registryReadWrite -> copy the Connection string---Primary Key.



3. Download and install the Azure Device Explorer to generate the SAS Token. Go to this link to download the software: https://github.com/Azure/azure-iot-sdk-csharp/releases/download/2018-3-13/SetupDeviceExplorer.msi



4. Paste the Connection String --- Primary Key to the IoT Hub Connection String box. Then type the Protocol Gateway HostName and click Update. In the end, generate the SAS Token.



5. Configure the MQTT Client from the Web GUI. Enter the value based on the IoT Hub setting. And the device is connected to the cloud.

Please find the Root CA through this link: https://github.com/Azure/azure-iot-sdk-c/blob/master/certs/certs.c

3.8.3 Private IoT

WoMaster provides its own cloud service, ThingsMaster that could support the Industrial Plants Network. Under the cloud architecture, software, hardware, applications, and storage can all be provided as services. The cloud network service has the advantages of easy expansion, rapid adjustment, and minimal management, and can dynamically meet increasing demands. Users can access the data which stored on the cloud anywhere, anytime, and seamlessly share to any authorized users.

The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Enable the WoM IoT function
Connection Status	Show the status of the connection between the device and ThingsMaster
IoT Server	Enter the address of Private IoT Server.
Port	Enter the port of Private IoT Server.

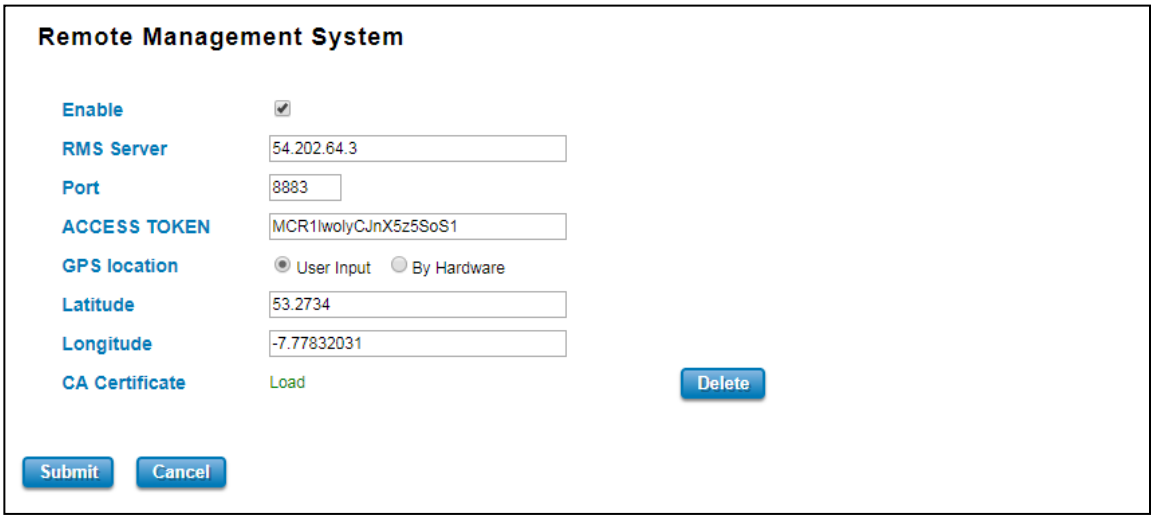
Client ID	Enter the client ID that has been registered.
MQTT Publish Topic	Specify the MQTT Topic
MQTT Publish Interval	The interval time to update the data
Update on change	**Default: Uncheck** Check the box to send update on when data changed.
CA Certificate	The function from this certificate file is to create an encrypted MQTT communication. User will get this file when download the ThingsMaster server file. **Note. This field only supports in ThingsMaster v1.1 and later version**
Debug Mode	Check to enable debug mode for CoAP connection.
Debug Log	Download log for problem analysis between device and CoAP server

Click **Submit** to apply the configuration.

3.8.4 RMS (Remote Management System)

WoMaster supports Over-the-Air Remote Monitoring System (RMS), **ThingMaster OTA**. This page allows the user to configure the RMS settings for the device, so that the device will be monitored through the ThingsMaster OTA RMS. The software is strong and easily to monitor your network over-the-air, you can apply the software with up to thousand nodes monitoring from our sales.

Not every version firmware supports this feature, while you have need to run over-the-air monitoring and doesn't find the configuration file, please contact our sales/technical window for further discuss.



The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Check the box to enable the RMS function.
RMS Server	Enter the RMS Server IP Address

Port	**Default: 8883**
ACCESS TOKEN	Generate the token from ThingsMaster RMS; this access token is used to access the device.
GPS Location	**User Input**: User input the device location information. **By Hardware**: if the device is supported with the GPS feature, then it will directly generate the location.
Latitude	Enter the Latitude coordinate of the device
Longitude	Enter the Longitude coordinate of the device
CA Certificate	The function from this certificate file is to create an encrypted MQTT communication. User will get this file when download the ThingsMaster server file. **Note. This field only supports in ThingsMaster v1.1**

Click Submit to apply the configuration. After succeed with the registration then the device will appear on the ThingsMaster OTA RMS dashboard.

HOW TO ESTABLISH AND CONNECT TO THE THINGSMASTER OTA RMS SERVER

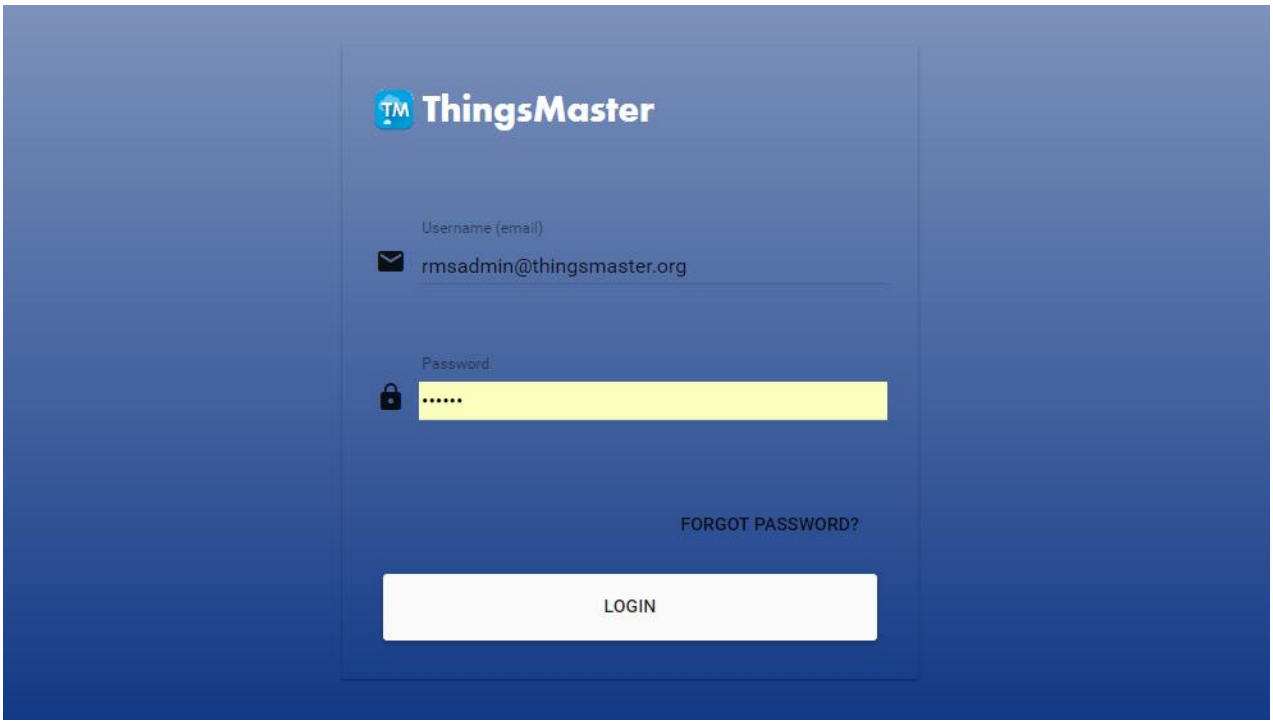
Note: The UI of the ThingMaster, ThingMaster OTA RMS and VMWare software and download link is often updated, following steps and figures may be updated.

1. Contact our Sales to get the access to the ThingsMaster RMS Account.

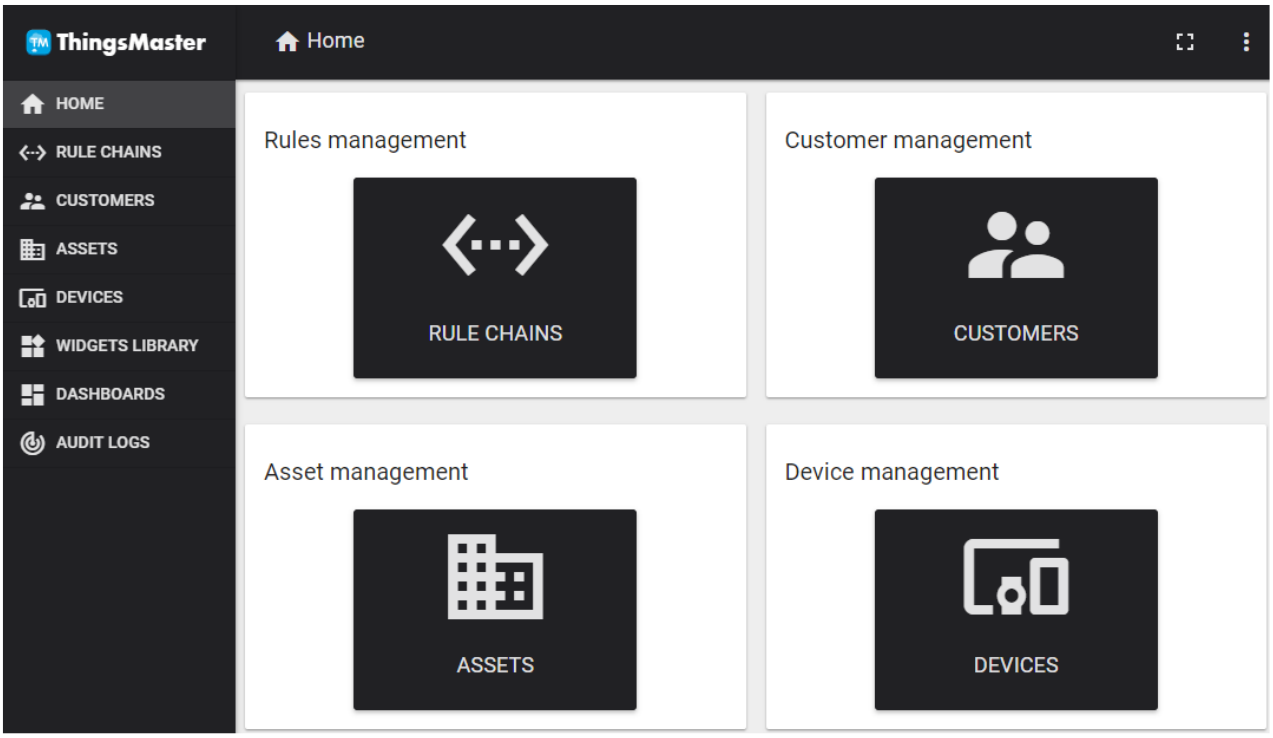
2. Login to ThingsMaster OTA RMS, using RMS Account.

Login: <User RMS Account>

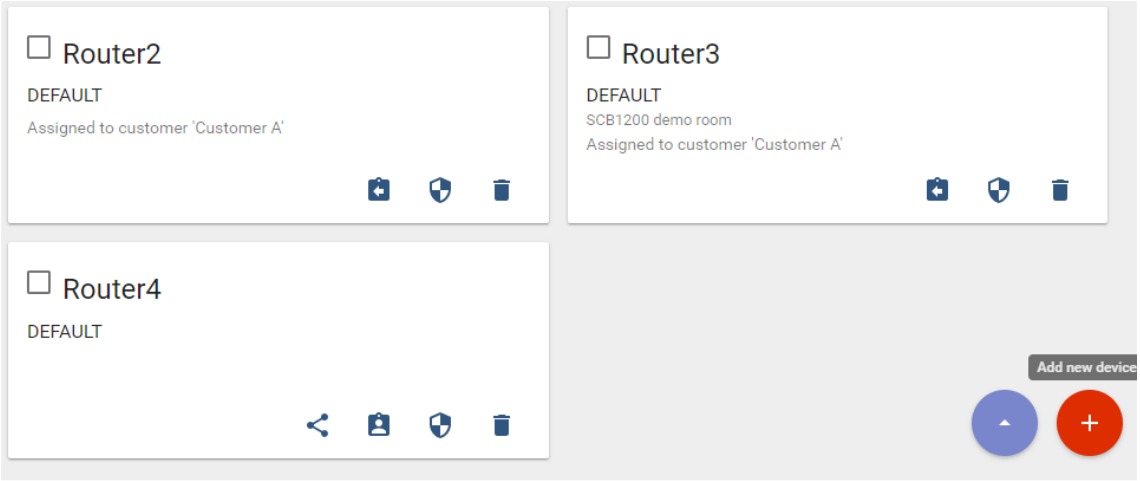
Password: <User RMS Password>



3. Go to Home -> Device Management to register the device.

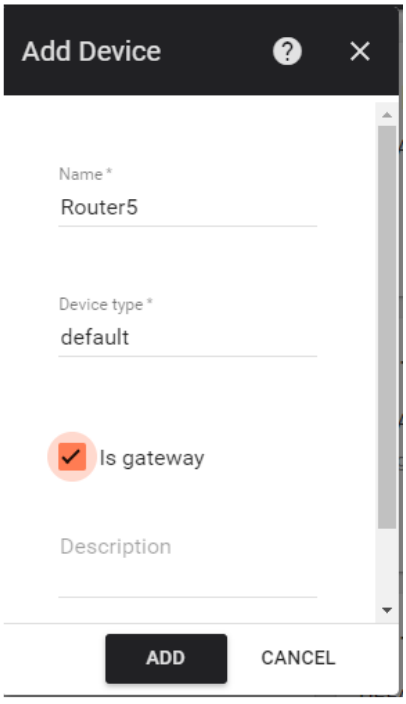


4. Add new device information, by clicking the “+” at the corner of the page.

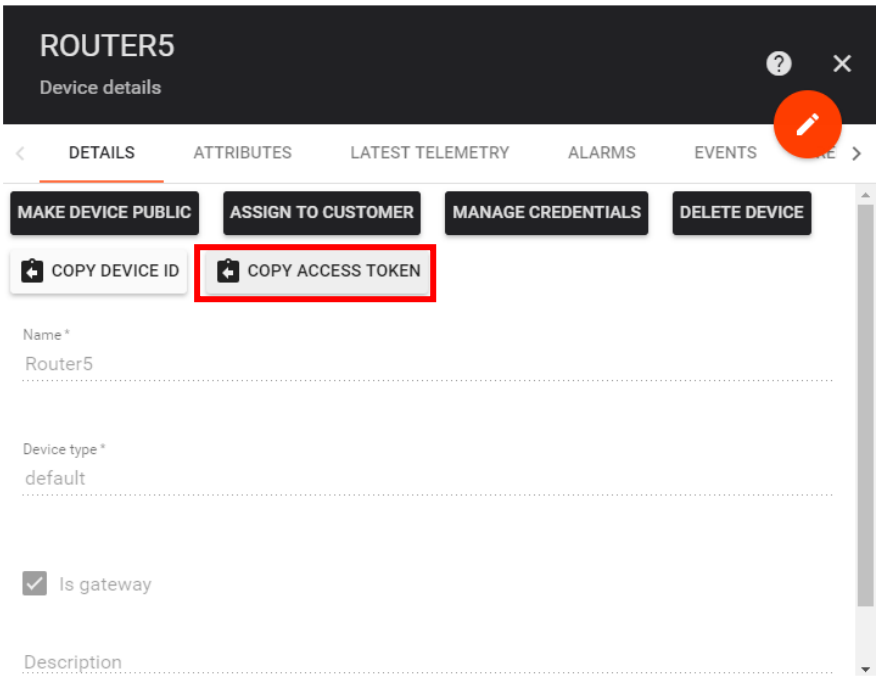


After click “+” menu then a page will pop up. Enter the device information.

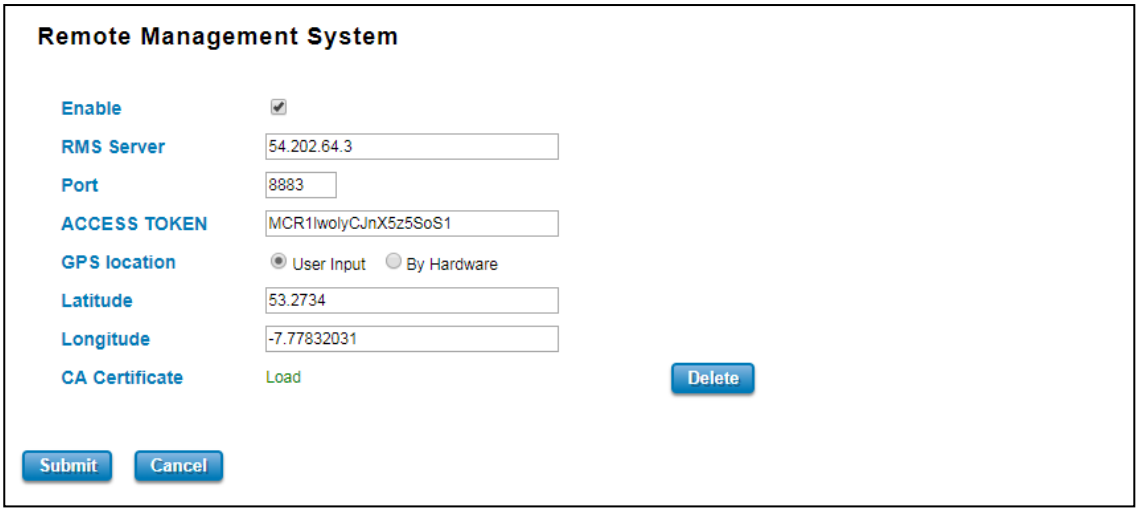
- Name: Please start the name with Router + Number.
- Device type: default
- Is gateway: check the box
- Click **Add**



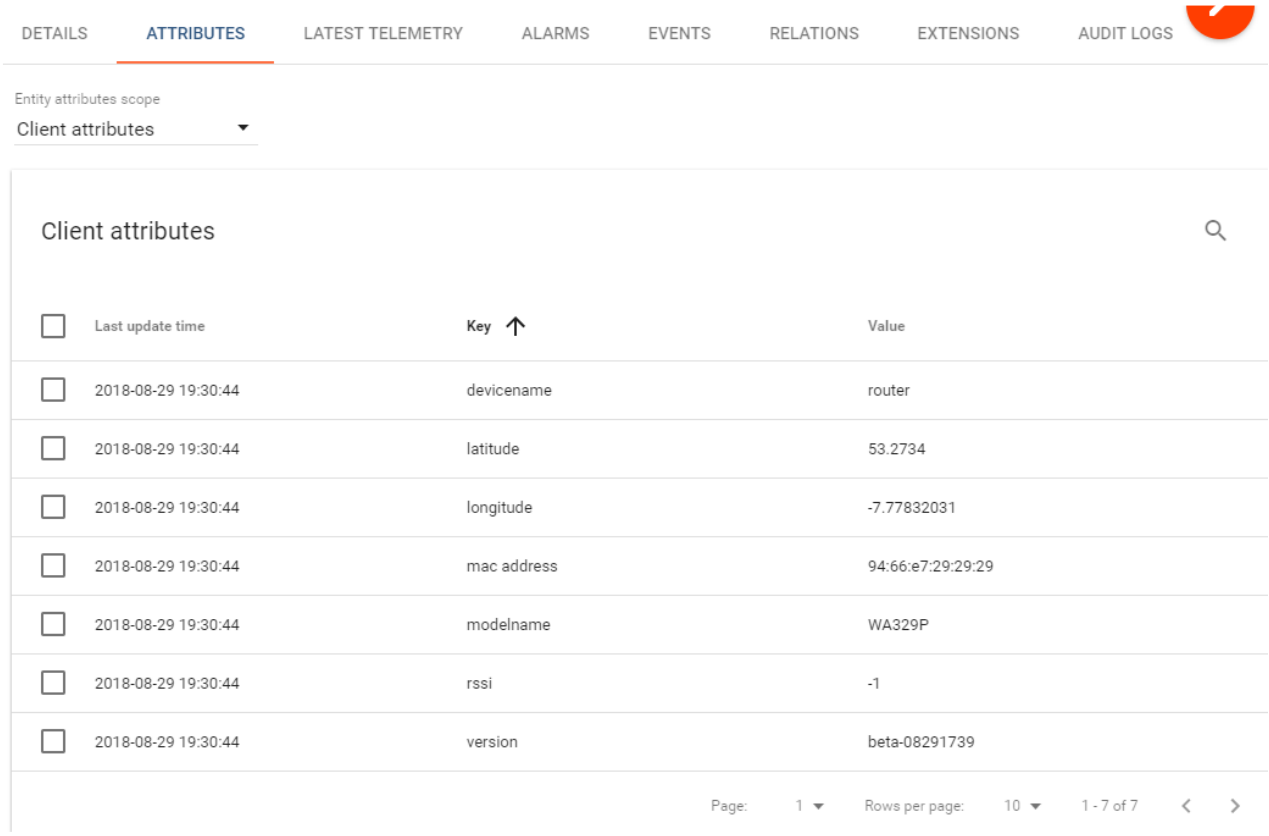
5. After the device is registered, then click on the device folder go to Details -> Click on Copy Access Token. This access token is code to link the device with the RMS Server.



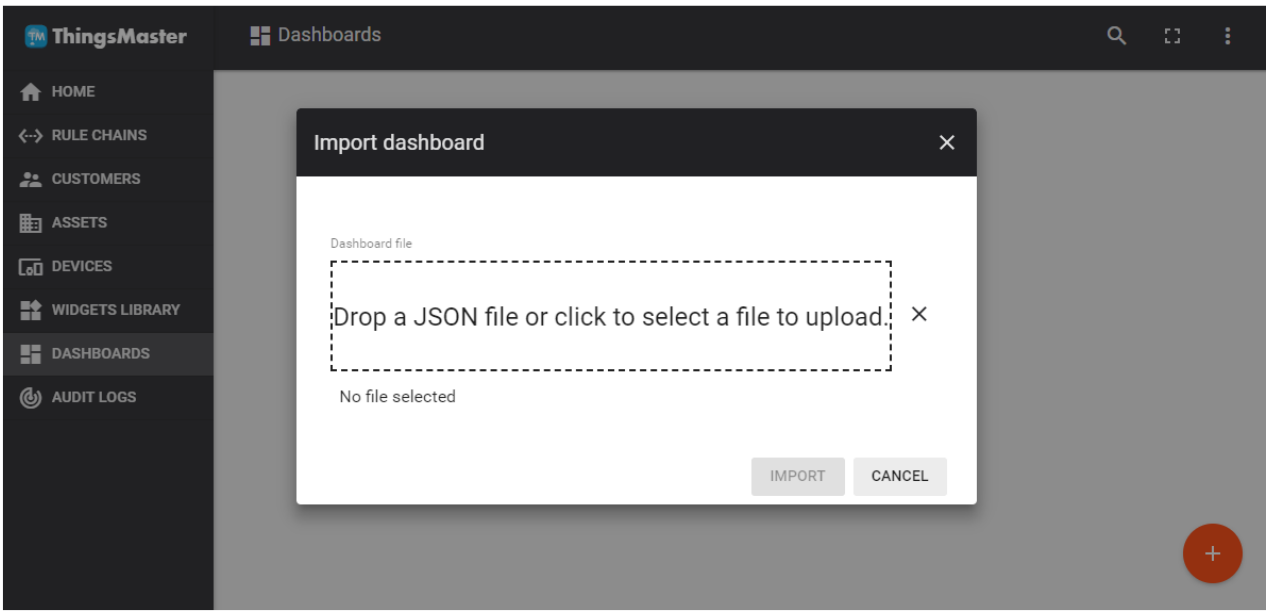
6. Go to the Web GUI -> IoT -> RMS. Paste the Access Token code to the Web GUI. And complete the configuration.



7. After the configuration is done then go back to ThingsMaster RMS Server. And then click on the newly added Router -> Attributes-> Client Attributes to see if the data has been uploaded.

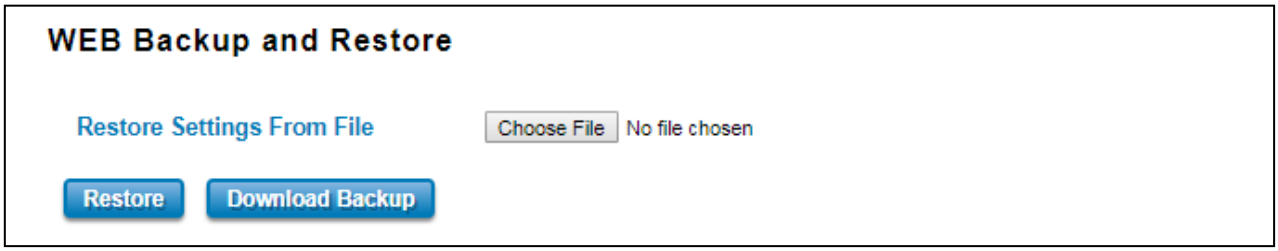


8. If all of the data has been uploaded, user can create a dashboard to visualize the data. Go to Dashboards menu. In this page, user can upload the JSON file that sent by the WoMaster Sales in the email. Click the “+” to import JSON File or Create a new Dashboard.



3.9 Backup and Restore

User can use WoMaster's Backup and Restore configuration to save and load configuration through the router.



Users can browse the target folder and then type the file name to back-up the configuration. Browse the target folder and select existed configuration file to restore the configuration back to the router. This mode is only provided by Web UI while CLI is not supported. Also, this feature provides the Download Backup button in order to download the backup configuration from the router.

3.10 Firmware Upgrade

WoMaster provides the latest firmware online at www.womaster.eu. The new firmware may include new features, bug fixes or other software changes. WoMaster also provides the release notes for the update as well. For technical viewpoint, WoMaster suggests user uses the latest firmware before installing the router to the customer site.

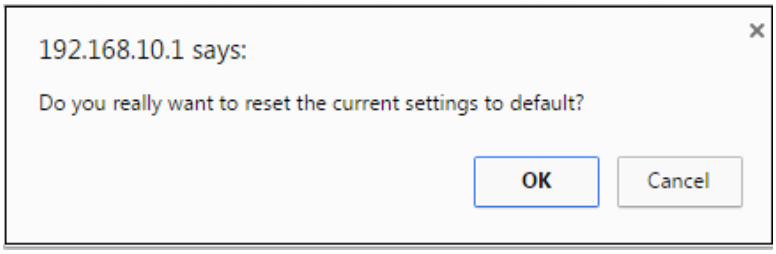
> Note that the system will be automatically rebooted after User finished upgrading the new firmware. Please remind the attached network users before User performs this function.

Users can browse the target folder and then type the file name to back-up the configuration. Users also can browse the target folder and select the existed upgrade file. This mode is only provided by Web UI while CLI is not supported.

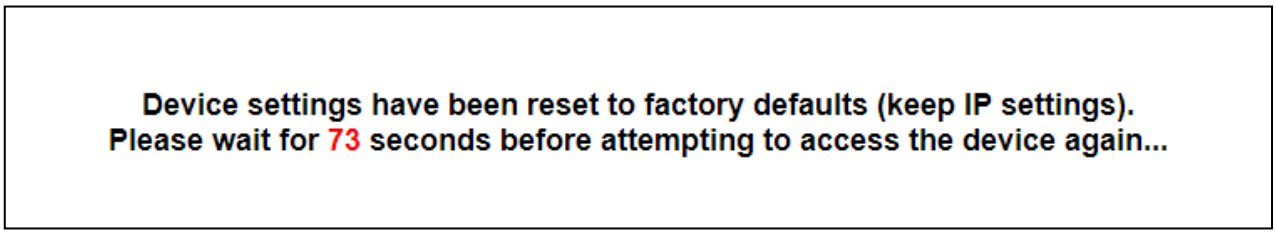
3.11 Reset to Defaults

This function provides users with a quick way of restoring the WoMaster router's configuration to factory defaults. By check the Restore Factory default IP setting, it means the IP of the device will directly change to the default IP (192.168.10.1).

Pop-up message screen to show User that have done the command. Click on **OK** to close the screen and reboot the device.

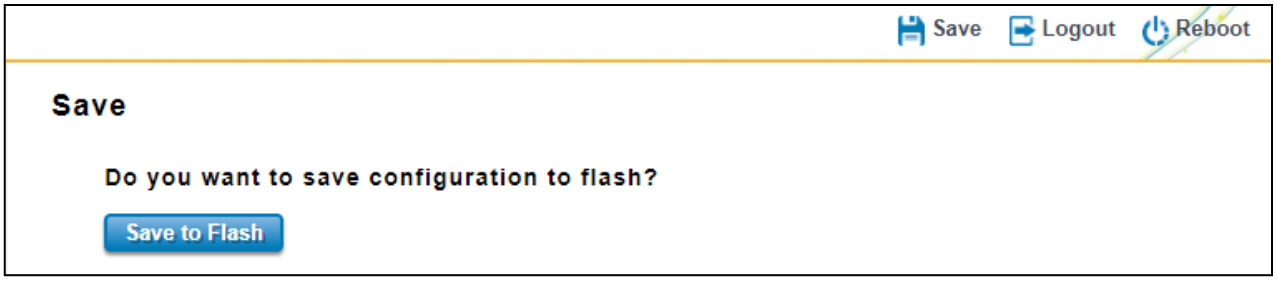


Below is the interface for resetting the device with keep the IP Settings.



3.12 Save

Save option allows user to save any configuration. Powering off the router without clicking on **Save** will cause loss of new settings. After selecting **Save**, click on **Yes** to save new configuration.



3.13 Logout

There are 2 logout methods. If user doesn't input any command within 30 seconds, the web connection will be logged out. The Logout command allows user to manually logout the web connection. Click on **Yes** to logout.

3.14 Reboot

System Reboot allows user to reboot the device. Some of the feature changes require user to reboot the system. Click on **Reboot** to reboot device.

> Remember to click on Save button to save configuration settings. Otherwise, the settings user made will be gone when the router is powered off.

Reboot main screen, to do confirmation request. Click **Yes**, then the router will reboot immediately.

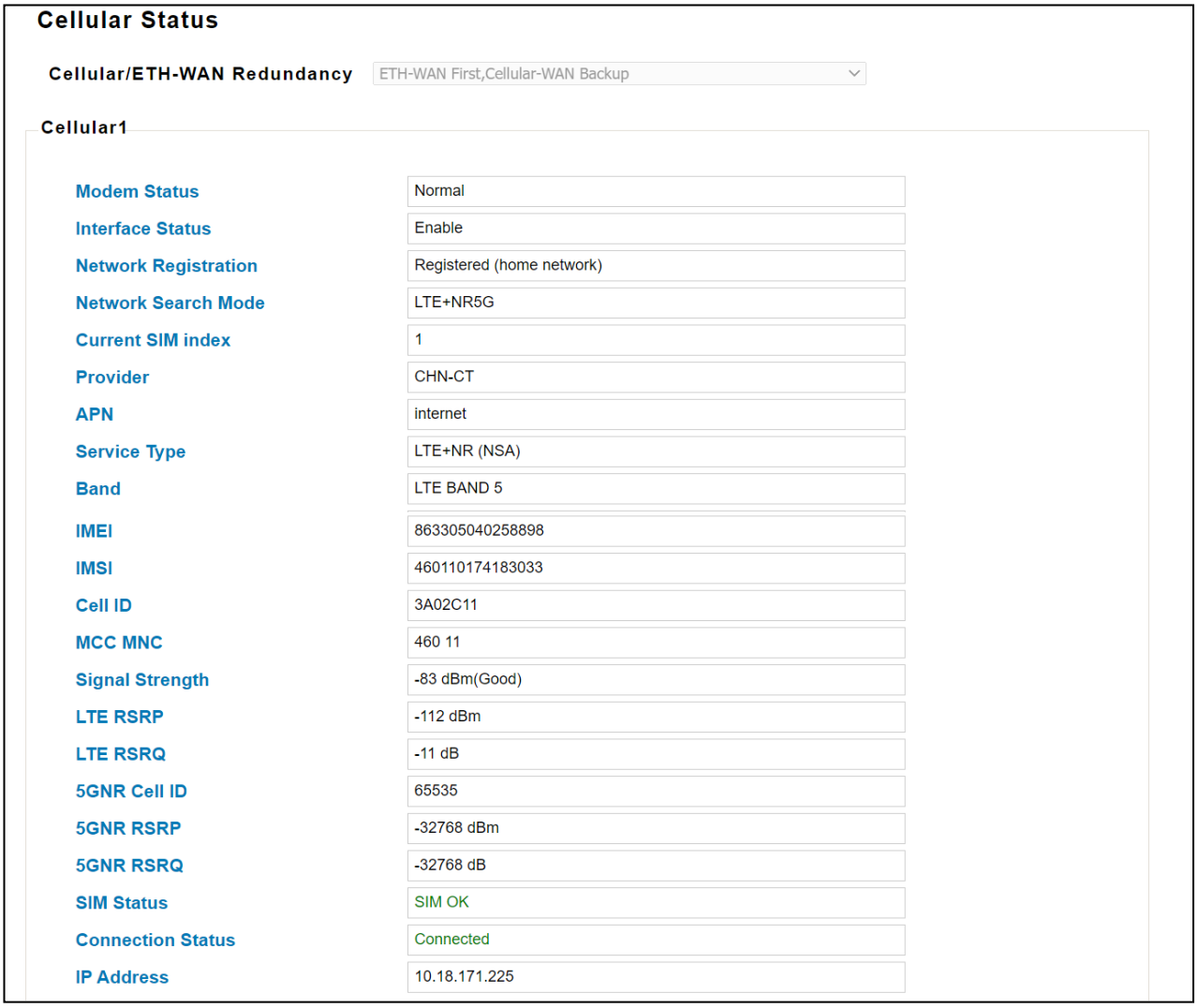
3.15 CELLULAR(WA512G-D-M2)

The Cellular page is available for the router while the Cellular Module is installed. This Cellular page provides the Cellular Status; configure Cellular Setting, and configure SIM Setting. This device is supported with redundant SIM and Dual SIM Card; user can choose SIM1 or SIM2 for the main SIM Card.

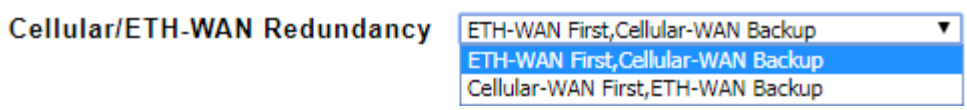
The Cellular Software feature can work with Wireless AP, Client and MESH AP modes, not include MESH RE mode.

3.15.1 CELLULAR STATUS

The figure below shows Cellular Status.



The description of the columns is as below:

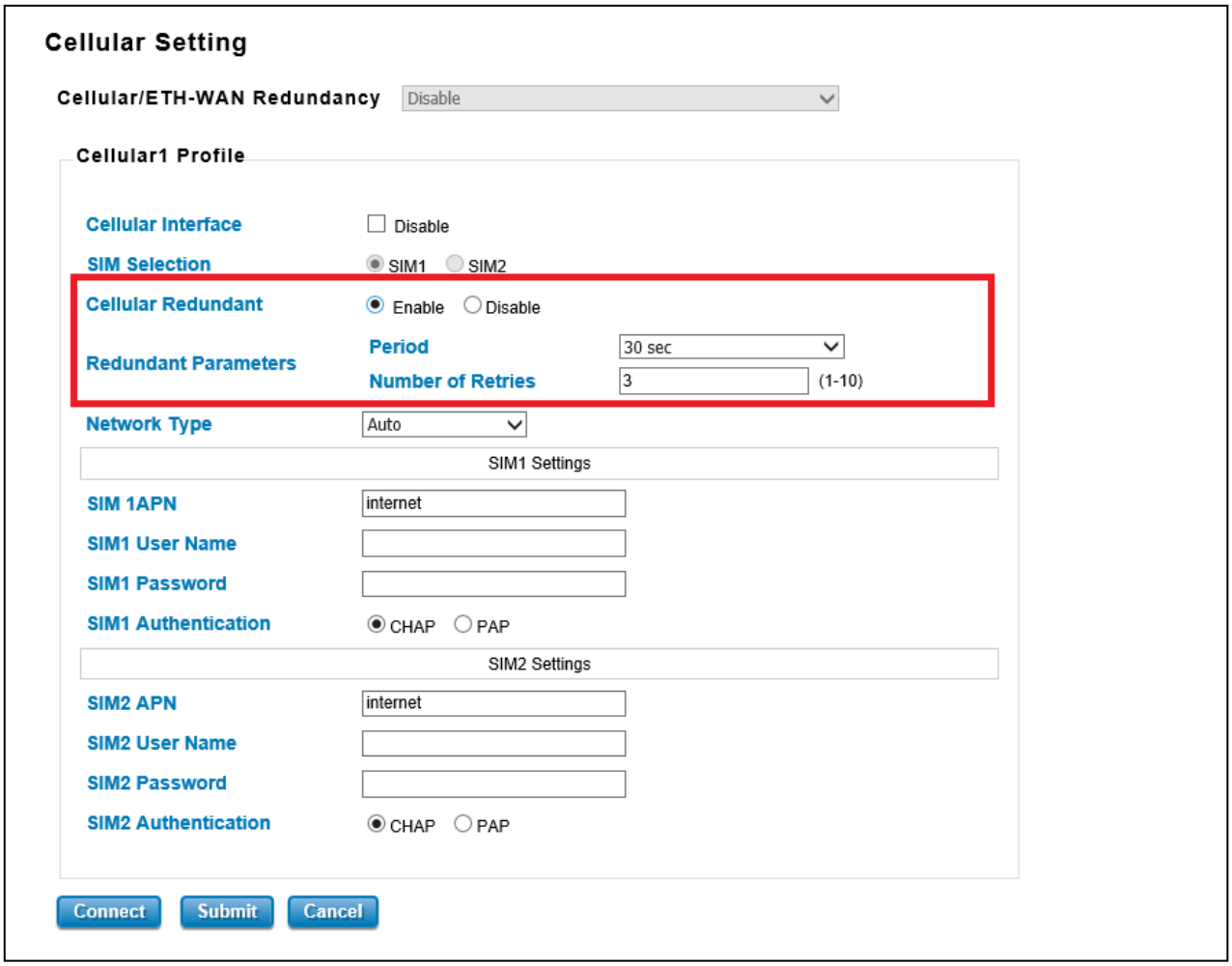
TERMS	DESCRIPTION
Cellular/ETH.WAN Redundancy	**Default: Disabled** User can choose the redundancy mode: 

	ETH-WAN First, Cellular-WAN Backup: by choosing this mode, the redundancy mode would be like prioritize the ETH-WAN connection; if the ETH-WAN connection has a problem then the Cellular-WAN would be the backup connection. **Cellular-WAN First, ETH-WAN Backup**: by choosing this mode, the redundancy mode would be like prioritize the Cellular-WAN connection; if the Cellular-WAN connection has a problem then the ETH-WAN would be the backup connection.
Modem Status	Display the modem status
Interface Status	Display the Cellular interface status Enabled or Disabled
Network Registration	Display the status of the network registration
Network Search Mode	Display the network search mode (Auto, 2G Only, 3G Only and LTE Only)
Current SIM index	Display the current SIM that user used.
Provider	Display the ISP that user used.
APN	Every ISP has a specific APN (Access Point Name) assigned to its cellular network. The system can read this name from the SIM card.
Service Type	The connected ISP will update the service type here. The possible types are GSM – 2G, UMTS – 3G, GSM W/EGPRS, UTRAN W/HSDPA (download), UTRAN W/HSUPA(upload), UTRAN W/HSDPA and HSUPA(download & upload), E-UTRAN - LTE , LTE+NR (NSA)，No Service(default value)
Band	Display the frequency band used by the current connection
IMEI	Display the International Mobile Equipment Identity (IMEI)
IMSI	Display the International Mobile Subscriber Identity (IMSI)
Cell ID	Display the Cell Identity (CID)
MCC MNC	Display the Mobile Country Code (MCC) and Mobile Network Code (MNC)
Signal Strength	The signal strength to the remote connected base station. If the signal strength shows low, please change the device location or mounting the antenna in better location. Below are the signal strength definitions in our system: 0 dBm (Default value while no connection) -113 dBm or less (Low) -111 dBm (Medium) -109…-53 dBm (Good) -51 dBm or greater (Excellent) -Not known or not detectable
LTE RSRP	Displays the LTE RSRP of the current connection.Value range: - 44 ~ - 140dBm, the larger the value, the better.
LTE RSRQ	Displays the LTE RSRQ of the current connection.Value range: - 3 ~ - 19.5dB, the larger the value, the better.
5GNR Cell ID	Display the 5GNR Cell Identity (CID)
5GNR RSRP	Displays the 5GNR RSRP of the current connection.

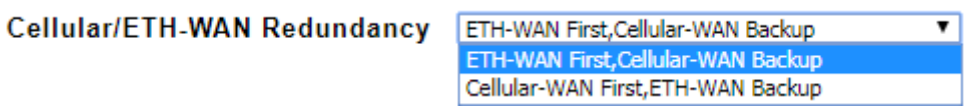
5GNR RSRQ	Displays the 5GNR RSRQ of the current connection.
SIM Status	Show the installed SIM Status. **SIM OK:** The SIM card is okay to use. **SIM not inserted:** The SIM card is not inserted. **SIM PIN Locked:** The SIM card is locked due to PIN error. It may be caused by error typing PIN password many times. **SIM PUK Locked:** The SIM Card PUK is locked due to PIN error after user three times input the wrong password. Contact the ISP to resolve the issue.
Connection Status	**Connection Status:** **Connected:** The cellular interface is connected. **Not Connected:** The cellular interface is not connected.
IP Address	The IP Address assigned by the ISP. While the cellular is connected, the IP address will display here.

3.15.2 CELLULAR SETTING

This section displays the Cellular Setting configuration page and also in this configuration page user may activate the redundant SIM function. In this section, user may configure the Cellular Interface, SIM Selection, Cellular Redundant, Network Type, SIM1/2 APN, User Name, Password and the Authentication mode.



The description of the columns is as below:

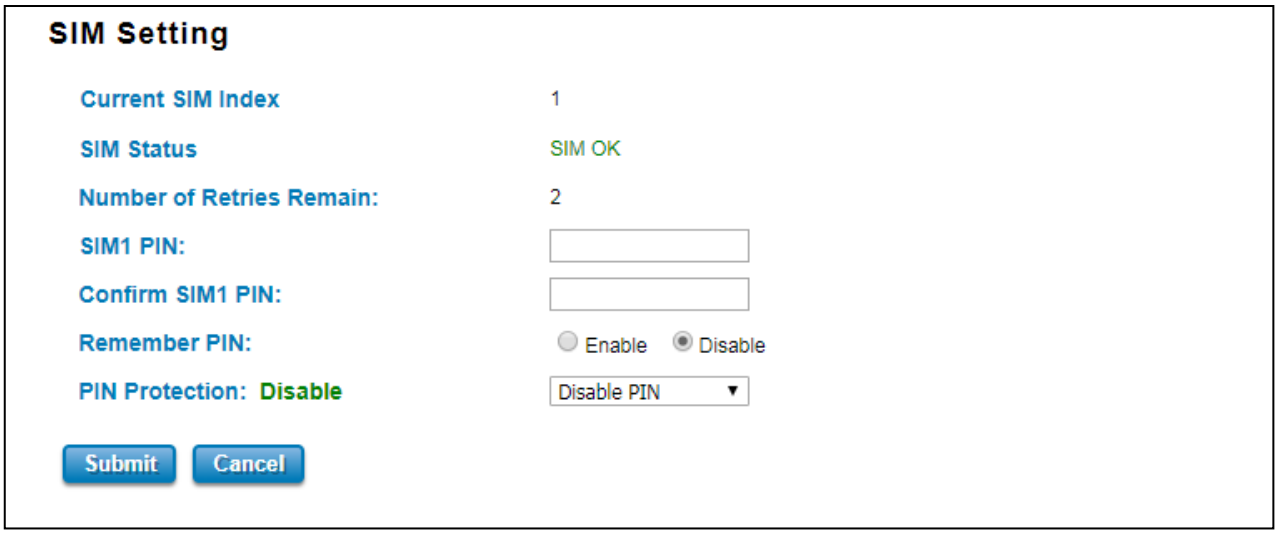
TERMS	DESCRIPTION
Cellular/ETH.WAN Redundancy	**Default: Disabled** After configured the Router mode in "System/Network Setting", the router will support Cellular and Ethernet-WAN redundant, user can choose the redundancy mode:  **ETH-WAN First, Cellular-WAN Backup**: by choosing this mode, the redundancy mode would be like prioritize the ETH-WAN connection; if the ETH-WAN connection has a problem then the Cellular-WAN would be the backup connection. **Cellular-WAN First, ETH-WAN Backup**: by choosing this mode, the redundancy mode would be like prioritize the Cellular-WAN connection; if the Cellular-WAN connection has a problem then the ETH-WAN would be the backup connection.

Cellular Interface	To enable or disable the cellular interface. Click check to disable the function.
SIM Selection	**Default: SIM1** User can select the SIM card 1 or 2 that want to be activated or used. Not every model supports dual SIM, it the hardware doesn't support dual SIM, the SIM2 setting is not available.
Cellular Redundant	**Default: Disable** By enable this function, the SIM redundant function will be activated. The main function of this feature is to have the backup SIM if the main SIM card is unable to use or have a problem connection. **Redundant Parameters** configuration appears after the user enables the function. If the SIM card cannot be read after the redundant parameters are expired then it will directly change to read the other SIM card. **Period:** Set the period time to read the SIM card. The default value is 30 Seconds. **Number of Entries:** Set the number of entries to give the remaining trial to read the SIM card. The default value is 3.
Network Type	Set the Network Type, the option would be: **Auto: Search the network automatically** **2G Only: only receive the 2G signal.** **3G Only: only receive the 3G signal.** **LTE Only: only receive LTE/4G signal.** **NR5G: only receive the 5GNR signal, or known as 5GNR SA mode.** **LTE+NR5G: available to receive the 5GNR signal, or known as 5GNR NSA mode.** The network type in different models is different. The GUI only shows the available type.
SIM1/2 APN	Set the APN of the ISP.
SIM1/2 User Name	Set the User Name
SIM1/2 Password	Set the password.
SIM1/2 Authentication	Choose CHAP or PAP mode for the authentication mode. **CHAP**: Challenge Handshake Authentication Protocol, With CHAP, the authenticator (i.e. the server) sends a randomly generated ``challenge'' string to the client, along with its hostname. **PAP**: Password Authentication Protocol, PAP works basically the same way as the normal login procedure. The authenticates itself by sending a user name and a password to the server

Click **Submit** to apply the configuration.

3.15.3 SIM SETTING

This section displays the SIM configuration such as SIM Status and SIM pin configuration. And in this section, user can enable or disable the SIM protection function. Apply the PIN number to the SIM cards; and make sure user enters the correct PIN number when activating the connection, after that the connection will start working. And also user can change the new PIN settings.

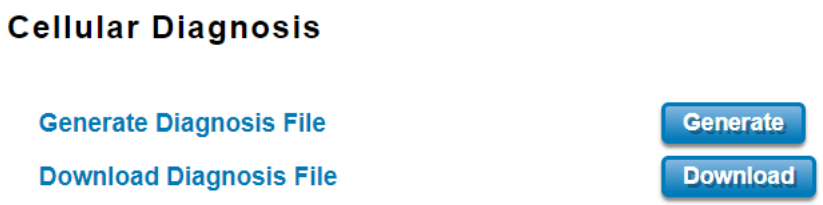


TERMS	DESCRIPTION
Current SIM Index	Display the current in used SIM Card slot (1 / 2)
SIM Status	Show the installed SIM Status. **SIM OK:** The SIM card is okay to use. **SIM not inserted:** The SIM card is not inserted. **SIM PIN Locked:** The SIM card is locked due to PIN error. It may be caused by error typing PIN password many times. **WARNING:** SIM PUK Locked status will appear when the SIM Card PUK is locked due to PIN error after user three times input the wrong password. Contact the ISP to resolve the issue.
Number of Retries Remain	Display the remaining chance to enter the PIN numbers.
SIM1/2 PIN	Enter new SIM1/2 PIN numbers
Confirm SIM1/2 PIN	Confirm the new SIM1/2 PIN numbers
Remember PIN	Click enable to save the PIN numbers
PIN Protection	Activate the PIN protection feature. Choose the mode from the drop list. **Disable PIN**: Disable the PIN Protection feature **Enable PIN**: Activate the PIN Protection feature **Change PIN**: Change the PIN number, make sure user type the new PIN Number first at the SIM1 PIN textbox.

Click **Submit** to apply the configuration.

3.15.4 CELLULAR DIAG

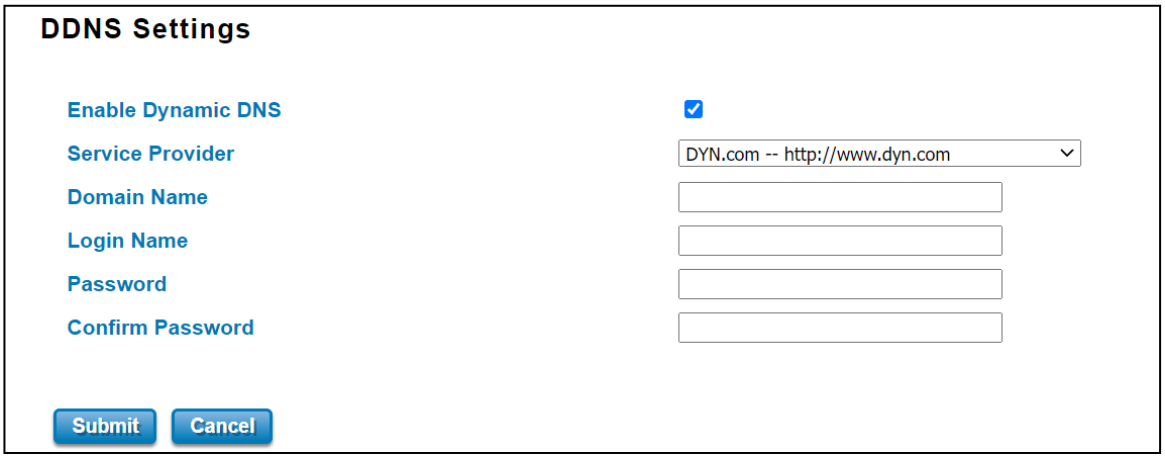
The Cellular Diag is used to get further information for the device of cellular records.

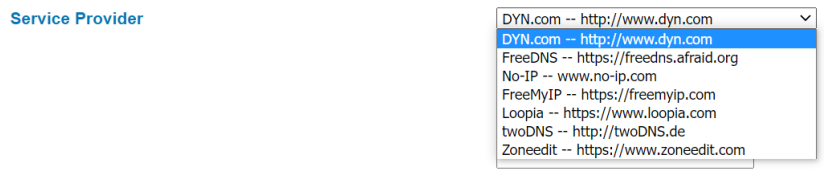


TERMS	DESCRIPTION
Generate Diagnosis File	Klick the button “Generate” and wait for 10S to generate the log file.
Download Diagnosis File	Klick the button “Download” for the log file.

3.15.5 DDNS SETTING

The DDNS (Dynamic Domain Name Service) is a method of keeping a domain name mapping to a dynamic public IP address. A dynamic public IP address is assigned for every connection request. After the user sets up the DDNS service, the DDNS service provider will automatically update the connection information if the public IP address has been changed. In this section, the user may configure the DDNS Setting.



TERMS	DESCRIPTION
Enable Dynamic DNS	Check the box to enable the function
Service Provider	Select the Domain service provider from the list. 
Domain Name	Enter the domain name
Login Name	Enter Login Name that used when applying the domain name
Password	Enter Password that used when applying the domain name
Confirm Password	Enter the Password once again to confirm.

Click **Submit** to apply the configuration.

4. REVISION HISTORY

Version	Description	Date	Editor
V1.0	1st released User Manual No N:1 NAT page No OpenVPN user page	20191212	Andrew
V1.1	Update WA512G-D with DC Terminal Block Input -Appearance, Wiring power input with DC terminal block Update description of MESH Status Add 3.4.2.6 Client Router (Wireless WAN NAT) mode for Wireless interface. Supported by V1.4 and later firmware. Add Fast Roaming chapter in Advanced WLAN Setting. Supported by V1.4 and latest firmware Update/Add description of Web Management: Update N to 1 NAT (one active WAN only) Update MESH Setting and MESH network Status Update OpenVPN Server/Client/User description Add OpenVPN Certificate Design and description Update IPSec Description Update RMS Description Update ThingMaster OTA description Note: The manual is user configuration guide, not includes RED declaration of conformity, RF specification and Safety precaution. We offer other declaration of conformity form. Please check our web site for the latest documents or contact our sales/support window.	20200506	Orwell
V1.2b	1. Add Product DOC and Safe Precaution. 2. Add WA512GM-IP67 Wiring Antenna and Wiring Waterproof Connector. 3. Update Pole/Wall-mount installation instruction. 4. Update WA512GM-D product appearance figures. 5. Add WA512GM-D Chassis ground installation instruction. 6. Update Fast Roaming description ready by firmware V1.4.5. Wait updating MESH, RF data…	20200821	Orwell
V1.2c	1. Add more description in Safety Precaution. 2. Update WA512GM-D product figure, dimension, Din Clip dimension with wall-mount installation, Add Default Antenna spec.	Sep.21,2020	Orwell
V1.2d	1. Updated by UL. Add wall-mount screwing, remove outdoor cabling,	Sep.24,2020	Orwell

	48V 0.5A rating for PoE.		
V1.3	Add FCC Statement	Oct.7,2020	Orwell
V1.4_2021 11	Add WA512GM-D-M2 series Add Chapter 2.3 WA512G-D-M2 hardware installation guide Add Web GUI introduction, highlight importance of “Save to Flash”. Add Web GUI-Cellular Features for WA512G-D-M2 series. Update description of the Safety Precaution. Remove Proprietary Fast Roaming.	Revised and updated at Oct.19,2021-> Nov.2,2021	Orwell