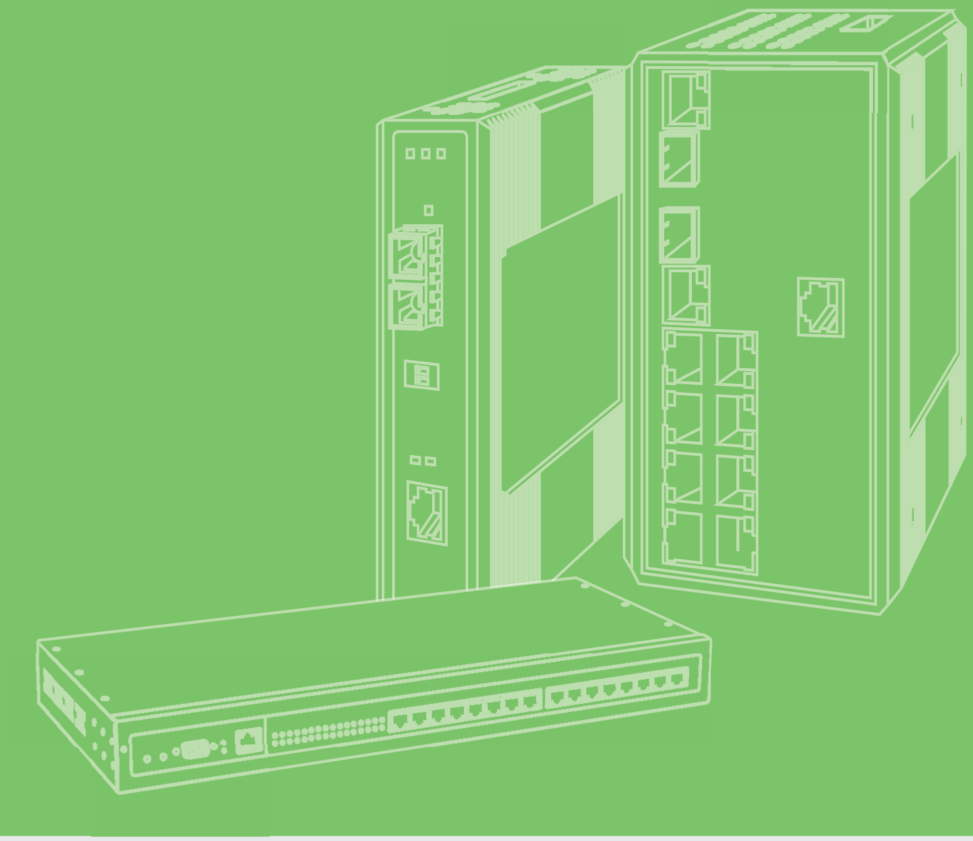


User Manual

EKI-6333AC-4GP

Idustrial IEEE 802.11 a/b/g/n/ac Wi-Fi AP with PoE

ADVANTECH

Enabling an Intelligent Planet

Copyright

Acknowledgments

Intel and Pentium are trademarks of Intel Corporation.

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.

All other product names or trademarks are properties of their respective owners.

Product Warranty (2 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for two years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For out of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any on-screen messages you get when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. If your product is diagnosed as defective, obtain an RMA (return merchandise authorization) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Part No. Edition 1
Printed in Taiwan January 2021

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC RF Radiation Exposure Statement:

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (7.87 inches) between the radiator and your body.

Technical Support and Assistance

1. Visit the Advantech web site at www.advantech.com/support where you can find the latest information about the product.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
   - Product name and serial number
   - Description of your peripheral attachments
   - Description of your software (operating system, version, application software, etc.)
   - A complete description of the problem
   - The exact wording of any error messages

Warnings, Cautions and Notes

Warning! *Warnings indicate conditions, which if not observed, can cause personal injury!*

Caution! *Cautions are included to help you avoid damaging hardware or losing data. e.g.*

There is a danger of a new battery exploding if it is incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Note! *Notes provide optional additional information.*

Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to: support@advantech.com

Packing List

Before setting up the system, check that the items listed below are included and in good condition. If any item does not accord with the table, please contact your dealer immediately.

- 1 x WiFi AP
- 1 x DIN Rail Bracket and Screws
- 1 x Wall-mounting Bracket
- 1 x 8-pin terminal block
- 1 x 4-pin terminal block

Safety Instructions

- Read these safety instructions carefully.
- Keep this User Manual for later reference.
- This device is for indoor use only.
- Disconnect this equipment from any DC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
- For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
- Keep this equipment away from humidity.
- Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
- The openings on the enclosure are for air convection. Protect the equipment from overheating. DO NOT COVER THE OPENINGS.
- Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
- Position the power cord so that people cannot step on it. Do not place anything over the power cord.
- All cautions and warnings on the equipment should be noted.
- If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.
- Never pour any liquid into an opening. This may cause fire or electrical shock.
- Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
- If one of the following situations arises, get the equipment checked by service personnel:
  - The power cord or plug is damaged.
  - Liquid has penetrated into the equipment.
  - The equipment has been exposed to moisture.
  - The equipment does not work well, or you cannot get it to work according to the user's manual.
  - The equipment has been dropped and damaged.
  - The equipment has obvious signs of breakage.

- DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO -40°C (-40°F) ~ 80°C (176°F). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.
- The sound pressure level at the operator's position according to IEC 704-1:1982 is no more than 70 dB (A).

  DISCLAIMER: This set of instructions is given according to IEC 704-1. Advantech disclaims all responsibility for the accuracy of any statements contained herein.

Safety Precaution - Static Electricity

Static electricity can cause bodily harm or damage electronic devices. To avoid damage, keep static-sensitive devices in the static-protective packaging until the installation period. The following guidelines are also recommended:

- Wear a grounded wrist or ankle strap and use gloves to prevent direct contact to the device before servicing the device. Avoid nylon gloves or work clothes, which tend to build up a charge.
- Always disconnect the power from the device before servicing it.
- Before plugging a cable into any port, discharge the voltage stored on the cable by touching the electrical contacts to the ground surface.

About the Device

This device is for indoor use only.

Contents

List of Figures

Chapter 1

Introduction

1.1 Overview

The EKI-6333AC-4GP is a feature rich wireless AP with din-rail type design which provides a reliable wireless connectivity for industrial environments. As an 802.11ac/n compliant device, EKI-6333AC-4GP provides higher data rates than legacy 802.11g devices.

With the support of WMM, EKI-6333AC-4GP effectively improves the reliability of wireless connectivity, especially in applications that need high reliability and high throughput data transmission. To secure wireless connections, EKI-6333AC-4GP implements the latest encryption technologies including WPA2/WPA/802.1x for powerful security authentication.

1.2 Device Features

- Equip 802.11 a/b/g/n/ac concurrent dual band WiFi module
- WLAN transmission rate up to 867 Mbps
- Supports secure access with WEP, 802.1x, WPA/WPA2-Personal, WPA/WPA2-Enterprise
- Provides Web-based configuration
- Support Dual band 2.4G, 5G concurrently
- 4 x Gigabit Ethernet Port with PoE 802.3at PSE support

1.3 Specifications

Specifications	Description	
Interface	I/O Port	4 x RJ45 + 1 x RJ45 (for WAN)
	Power Connector	Terminal block
Physical	Enclosure	Metal shell with solid mounting kits
	Mounting	DIN rail and wall
	Dimensions (W x H x D)	62 x 160 x 125 mm (2.44” x 6.3” x 4.92”)
	Weight	1.3 Kg (2.87 lbs)
LED Display	System LED	Power 1, Power 2, System Status
	Port LED	■ WLAN: Quality, Link/Active ■ LAN: Link/Active
Environment	Operating Temperature	-30°C ~ 70°C (-22°F ~ 158°F)
	Storage Temperature	-40°C ~ 80°C (-40°F ~ 176°F)
	Ambient Relative Humidity	10 ~ 95% RH
Wireless LAN Communications	Compatibility	IEEE 802.11a/b/g/n/ac
	Speed	Up to 867 Mbps for 11ac
	Antenna	4 x Reverse SMA (supports 2T2R for each radio)
	Free Space Range	Open space 100 m
	Wireless Security	WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise
Ethernet Communications	Compatibility	IEEE 802.11a/b/g/n/ac
	Speed	10/100/1000 Mbps
	Port Connector	8-pin RJ45

Specifications	Description	
Power	Power Consumption	max. 20 W + 120 W (for 4x PoE PD)
	Power Input	24 ~ 56 V_{DC}, redundant dual inputs
Software	Management	Web, Telnet CLI, command script, SNMPv3 Standard
	Security	■ VPN: IPSec, OpenVPN, PPTP, L2TP, GRE ■ Firewall: SPI firewall with stealth mode, IPS ■ Access Control: Packet filter, URL blocking, MAC filter
	Event Handling	Management/Notifying Events, Syslog, Email Alart
	Diagnostic	Packet Analyzer, Diagnostic Tools
Regulatory Approvals	EMC	CE, FCC Part 15 Subpart B (Class B)

1.4 Dimensions

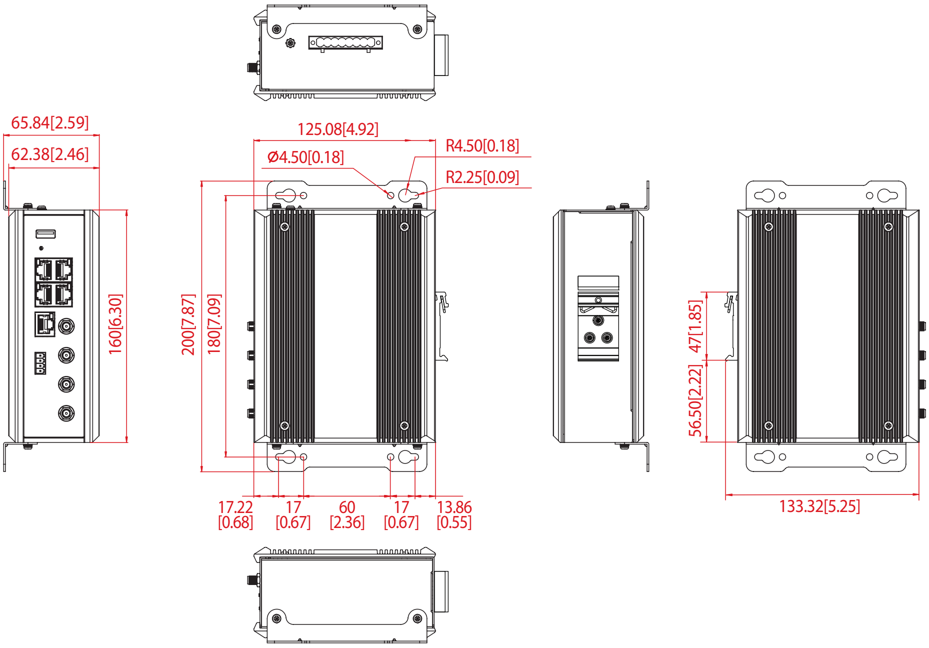


Figure 1.1 Dimensions

Chapter 2

Getting Started

2.1 Hardware

2.1.1 Front View

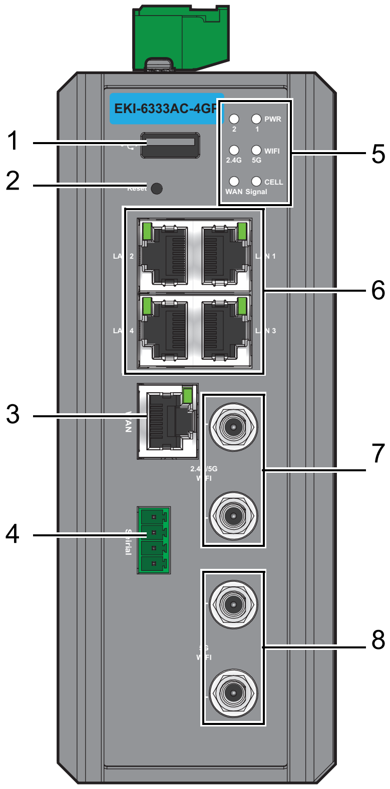


Figure 2.1 Front View

No.	Item	Description
1	USB port	
2	Reset button	Button allows for system soft reset or factory default reset.
3	Serial port	
4	ETH port	RJ45 ports x 1 to configure WAN.
5	System LED panel	See “LED Indicators” on page 7 for further details.
6	ETH port	RJ45 ports x 4.
7	Antenna connector	Connector for 2.4G/5G antenna.
8	Antenna connector	Connector for 5G antenna.

2.1.2 Rear View

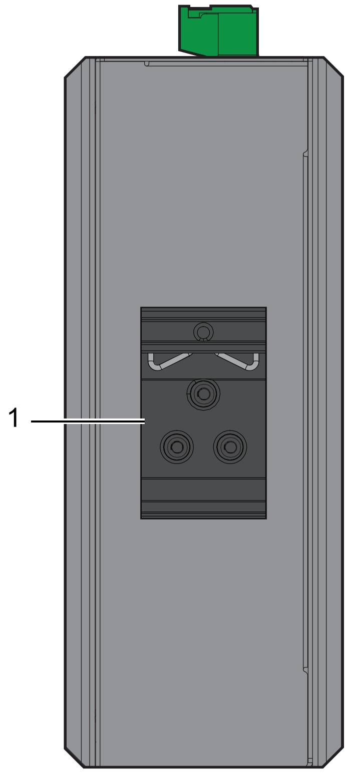


Figure 2.2 Rear View

No.	Item	Description
1	DIN rail mounting plate	Mounting plate used for the installation to a standard DIN rail

2.1.3 Top View

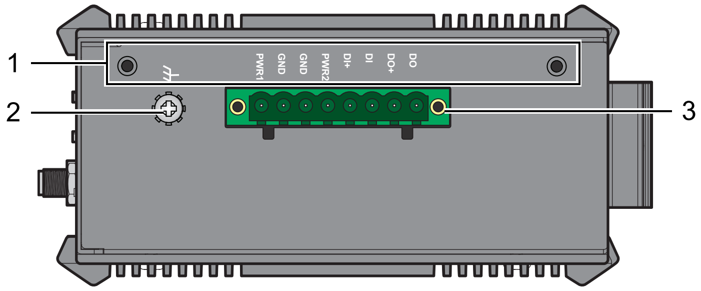


Figure 2.3 Top View

No.	Item	Description
1	Wall mounting holes	Screw holes (x4) used in the installation of a wall mounting plate
2	Ground terminal	Screw terminal used to ground chassis
3	Terminal block	Connect cabling for power and alarm wiring

2.1.4 LED Indicators

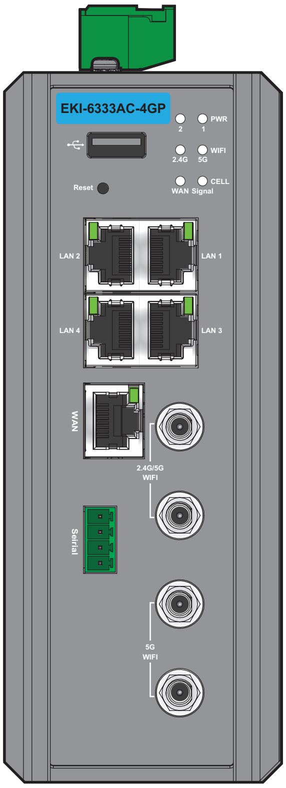


Figure 2.4 System LED Panel

LED Name	LED Color	Description
Power 1	Solid blue	Device is powered by power source 1.
	Off	Device is not powered by power source 1.
Power 2	Solid blue	Device is powered by power source 2.
	Off	Device is not powered by power source 3.
P1 ~ P4	Solid blue	Supply PoE Power through Ethernet Port. ***Note!*** *If the LED blinking slowly, there is power issue. Please check the power supply voltage or the connected device.*
	Off	No PoE power is supplied through the Ethernet Port.
LAN1 ~ LAN4	Solid green	Ethernet connection of LAN or WAN is established.
	Blinking	Data packets are transferring.
	Off	No Ethernet cable attached or the device is not linked.
Serial	Solid blue	Connect to a serial device.
	Off	Not connect to a serial device.
Status	Solid blue	Device is powered on.
	Off	Device is powered off.
2.4G/5G	Solid blue	2.4GHz/5GHz WiFi is enabled.
	Off	2.4GHz/5GHz WiFi is disabled.
5G	Solid blue	5GHz WiFi is enabled.
	Off	5GHz WiFi is disabled.

2.2 Connecting Hardware

2.2.1 DIN Rail Mounting

The DIN rail mount option is the quickest installation option. Additionally, it optimizes the use of rail space.

The metal DIN rail kit is secured to the rear of the device. The device can be mounted onto a standard 35 mm (1.37”) x 7.5 mm (0.3”) height DIN rail. The devices can be mounted vertically or horizontally. Refer to the following guidelines for further information.

Note! *A corrosion-free mounting rail is advisable.*

When installing, make sure to allow for enough space to properly install the cabling.

2.2.1.1 Installing the DIN Rail Kit

1. Position the rear panel of the device directly in front of the DIN rail, making sure that the top of the DIN rail clip hooks over the top of the DIN rail, as shown in the following illustration.

Warning! *Do not install the DIN rail under or in front of the spring mechanism on the DIN rail clip to prevent damage to the DIN rail clip or the DIN rail.*

Make sure the DIN rail is inserted behind the spring mechanism.

2. Once the DIN rail is seated correctly in the DIN rail clip, press the front of the device to rotate the device down and into the release tab on the DIN rail clip.

   If seated correctly, the bottom of the DIN rail should be fully inserted in the release tab.

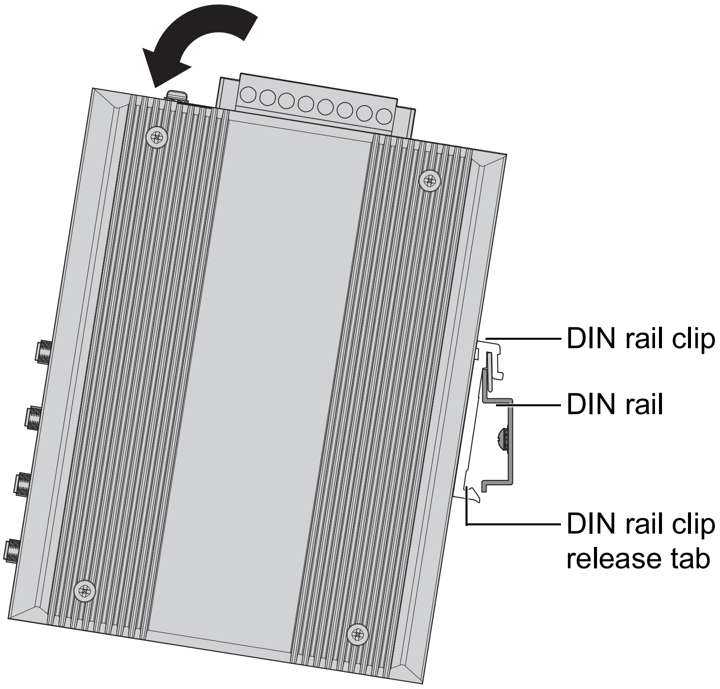


Figure 2.5 Installing the DIN Rail Kit

See the following figure for an illustration of a completed DIN installation procedure.

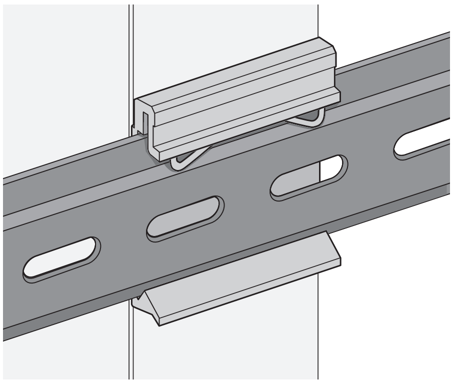


Figure 2.6 Correctly Installed DIN Rail Kit

3. Grasp the bottom of the device and slightly rotate it upwards. If there is resistance, the device is correctly installed. Otherwise, re-attempt the installation process from the beginning.

2.2.1.2 Removing the DIN Rail Kit

1. Ensure that power is removed from the device, and disconnect all cables and connectors from the front panel of the device.
2. Push down on the top of the DIN rail clip release tab with your finger. As the clip releases, lift the bottom of the device, as shown in the following illustration.

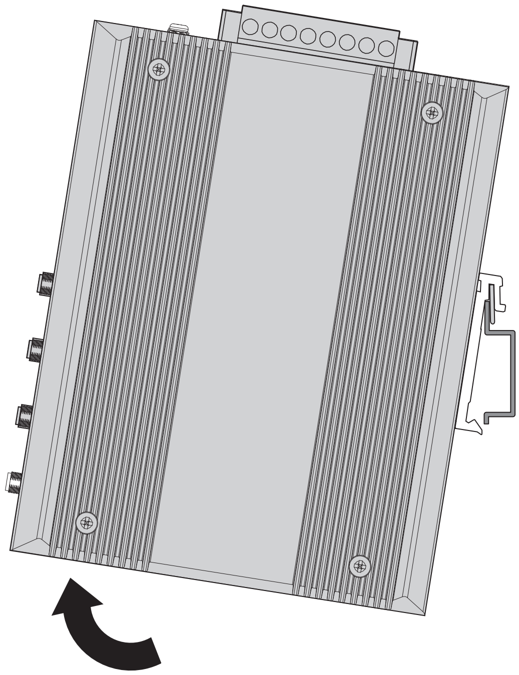


Figure 2.7 Removing the DIN Rail

2.2.2 Wall Mounting

The wall mounting option provides better shock and vibration resistance than the DIN rail vertical mount.

Note! *When installing, make sure to allow for enough space to properly install the cabling.*

Before the device can be mounted on a wall, you will need to remove the DIN rail plate.

1. Rotate the device to view the rear side and locate the DIN rail mounting plate.
2. Remove the screws securing the DIN rail mounting plate to the rear side.
3. Remove the DIN rail mounting plate. Store the DIN rail mounting plate and provided screws for later use.
4. Align the wall mounting brackets with the designated location as illustrated in the following figure. The screw holes on the device and the brackets align if seated correctly.
5. Secure the wall brackets to the device with M3 screws, see the following figure.

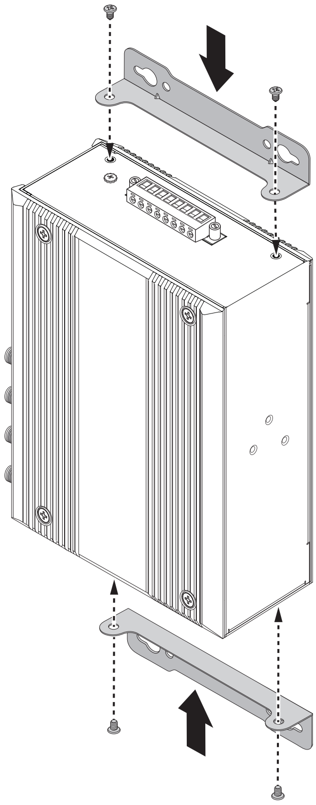


Figure 2.8 Installing Wall Mount Plates

Once the wall mounting brackets are secured on the device, mark the screw hole location on the wall area.

6. On the installation site, place the device firmly against the wall. Make sure the device is vertically and horizontally level.
7. Insert a pencil or pen through the screw holes on the mounting bracket to mark the location of the screw holes on the wall.
8. Remove the device from the wall and drill holes over each marked location (4) on the wall, keeping in mind that the holes must accommodate wall sinks in addition to the screws.

9. Insert the wall sinks into the walls.
10. Align the mounting bracket over the screw holes on the wall.
11. Starting with the upper bracket, insert a screw through the bracket and rotate it to secure. Do not tighten at this point. Repeat for the remaining locations, see the following figure.

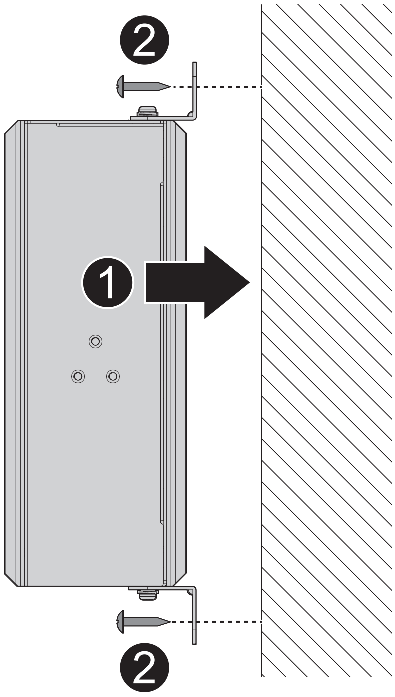


Figure 2.9 Wall Mount Installation

12. Once the device is installed on the wall, tighten the screws to secure the device.

2.2.3 Wireless Connection

1. Connect the antenna by screwing the antenna connectors in a clockwise direction.

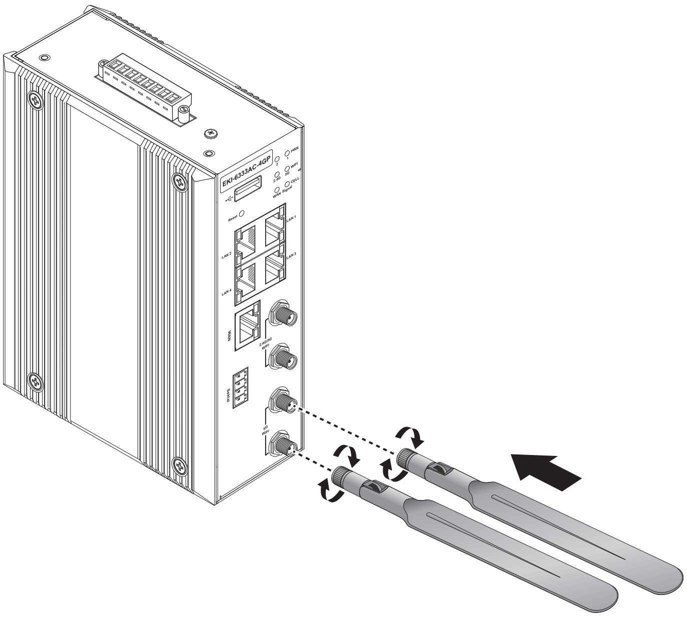


Figure 2.10 Installing the Antenna

2. Position the antenna for optimal signal strength.

Note! *The location and position of the antenna is crucial for effective wireless connectivity*

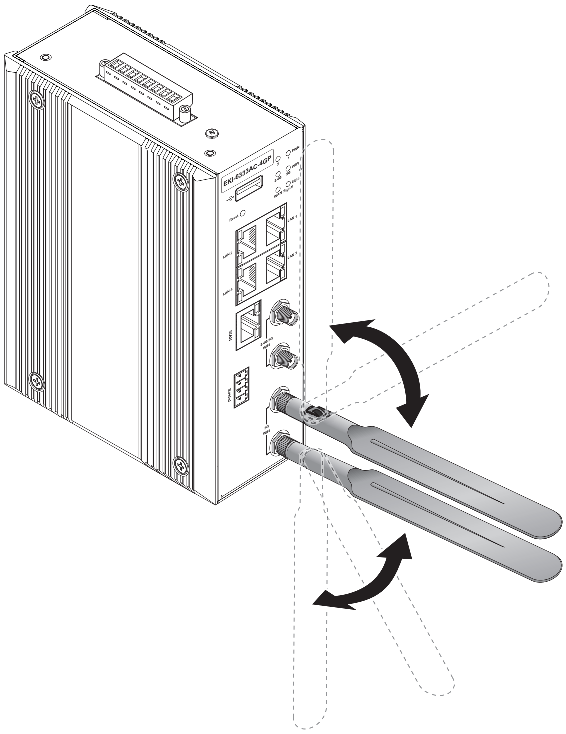


Figure 2.11 Positioning the Antenna

2.2.4 Network Connection

For RJ45 connectors, data-quality, twisted pair cabling (rated CAT5 or better) is recommended. The connector bodies on the RJ45 Ethernet ports are metallic and connected to the GND terminal. For best performance, use shielded cabling. Shielded cabling may be used to provide further protection.

Straight-thru Cable Wiring		Cross-over Cable Wiring	
Pin 1	Pin 1	Pin 1	Pin 3
Pin 2	Pin 2	Pin 2	Pin 6
Pin 3	Pin 3	Pin 3	Pin 1
Pin 6	Pin 6	Pin 6	Pin 2

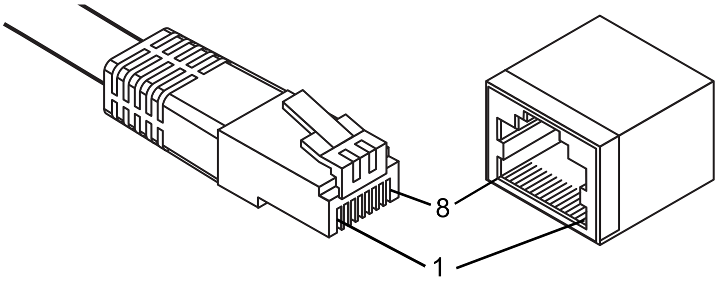


Figure 2.12 Ethernet Plug & Connector Pin Position

Maximum cable length: 100 meters (328 ft.) for 10/100BaseT.

2.2.5 Serial Connection

The devices provide 4-pin terminal block serial port for connecting to your serial device. Connect the serial device to the terminal block with the right pin assignments of RS-232/485 are shown as below.

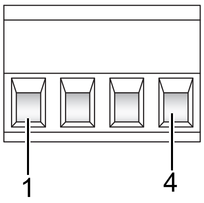


Figure 2.13 Serial Pin Position

	Pin1	Pin2	Pin3	Pin4
RS-232	GND	RXD	TXD	GND
RS-485	GND	DATA-	DATA+	GND

2.2.6 DI/DO Connection

There are one DI and one DO ports together with power terminal block. Please refer to the following specification to connect DI and DO devices.

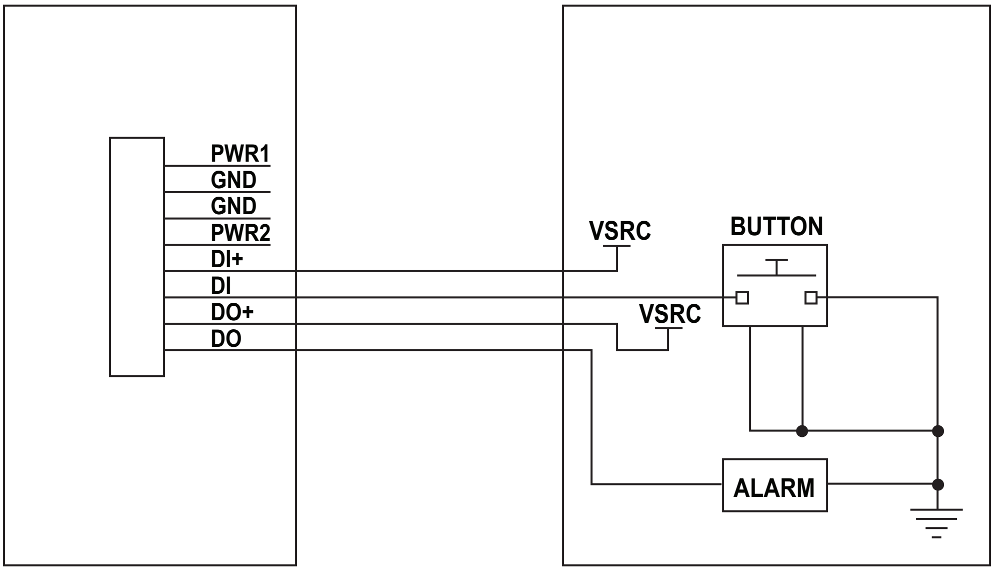


Figure 2.14 Example of Connection Diagram

Mode	Specification	
Digital Input	Trigger Voltage (high)	Logic level 1: 5V ~ 30V
	Normal Voltage (low)	Logic level 0: 0V ~ 2V
Digital Output	Voltage (Relay Mode)	Depends on external device maximum voltage is 30V
	Maximum Current	1A

2.2.7 Power Connection

2.2.7.1 Overview

Warning! *Power down and disconnect the power cord before servicing or wiring the device.*

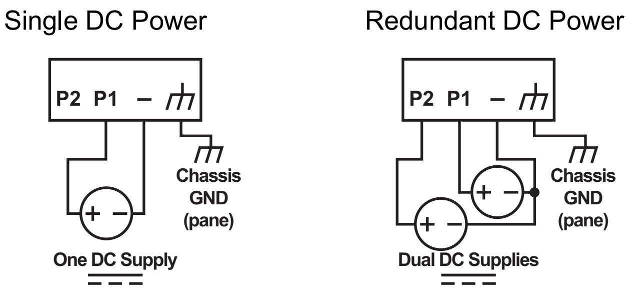
Caution! *Do not disconnect modules or cabling unless the power is first switched off.*

The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the device.

Caution! *Disconnect the power cord before installation or cable wiring.*

The devices can be powered by using the same DC source used to power other devices. A DC voltage range of 24 to 56 V_{DC} must be applied between the V1+ terminal and the V1- terminal (PW1), see the following illustrations. The chassis ground screw terminal should be tied to the panel or chassis ground. A redundant power configuration is supported through a secondary power supply unit to reduce network down time as a result of power loss.

EKI-6333AC-4GP support 24 to 56 V_{DC}. Dual power inputs are supported and allow you to connect a backup power source.



Single DC Power

Redundant DC Power

Figure 2.15 Power Wiring for EKI-6333AC-4GP

2.2.7.2 Considerations

Take into consideration the following guidelines before wiring the device:

- The Terminal Block (CN1) is suitable for 12-24 AWG (3.31 - 0.205 mm^2). Torque value 7 lb-in.
- The cross sectional area of the earthing conductors shall be at least 3.31 mm^2.
- Calculate the maximum possible current for each power and common wire. Make sure the power draw is within limits of local electrical code regulations.
- For best practices, route wiring for power and devices on separate paths.
- Do not bundle together wiring with similar electrical characteristics.
- Make sure to separate input and output wiring.
- Label all wiring and cabling to the various devices for more effective management and servicing.

Note! *Routing communications and power wiring through the same conduit may cause signal interference. To avoid interference and signal degradation, route power and communications wires through separate conduits.*

2.2.7.3 Grounding the Device

Caution! *Do not disconnect modules or cabling unless the power is first switched off.*

The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the device.

Caution! *Before connecting the device properly ground the device. Lack of a proper grounding setup may result in a safety risk and could be hazardous.*

Caution! *Do not service equipment or cables during periods of lightning activity.*

Caution! *Do not service any components unless qualified and authorized to do so.*

Caution! *Do not block air ventilation holes.*

Electromagnetic Interference (EMI) affects the transmission performance of a device. By properly grounding the device to earth ground through a drain wire, you can setup the best possible noise immunity and emissions.

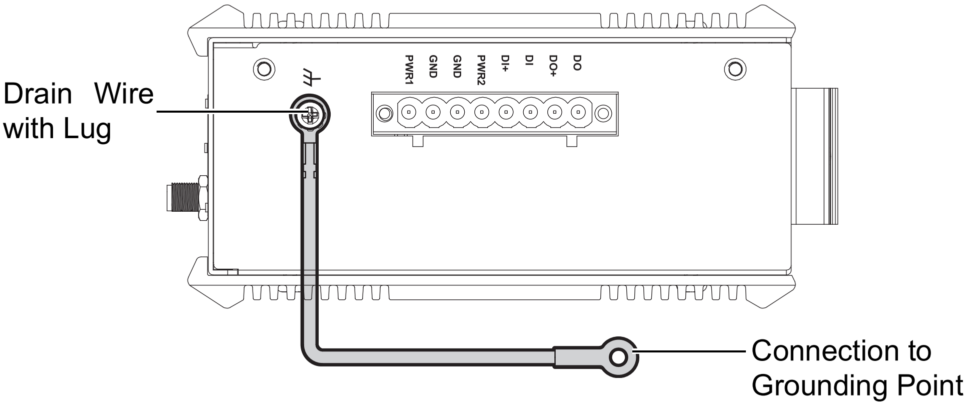


Figure 2.16 Grounding Connection

By connecting the ground terminal by drain wire to earth ground the device and chassis can be ground.

Note! *Before applying power to the grounded device, it is advisable to use a volt meter to ensure there is no voltage difference between the power supply's negative output terminal and the grounding point on the device.*

2.2.7.4 Wiring a Relay Contact

The following section details the wiring of the relay output. The terminal block on the EKI-6333AC-4GP is wired and then installed onto the terminal receptor located on the EKI-6333AC-4GP.

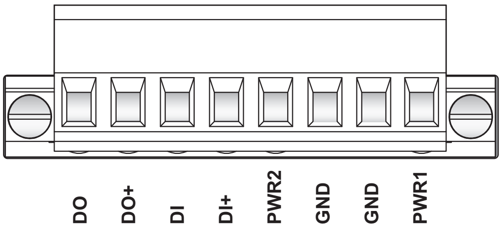


Figure 2.17 Terminal Receptor: Relay Contact

The terminal receptor includes a total of six pins: two for PWR1, two for PWR2 and two for a fault circuit.

2.2.7.5 Wiring the Power Inputs

Caution! ⚠ *Do not disconnect modules or cabling unless the power is first switched off.*

The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the device.

Warning! ⚠ *Power down and disconnect the power cord before servicing or wiring the device.*

There are two power inputs for normal and redundant power configurations. The power input 2 is used for wiring a redundant power configuration. See the following for terminal block connector views.

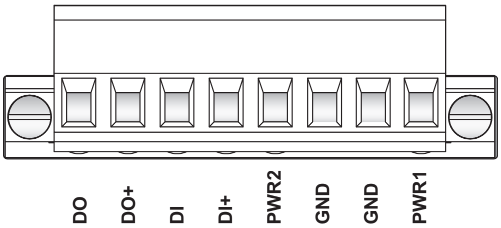


Figure 2.18 Terminal Receptor: Power Input Contacts

To wire the power inputs:

Make sure the power is not connected to the device or the power converter before proceeding.

1. Loosen the screws securing terminal block to the terminal block receptor.
2. Remove the terminal block from the device.

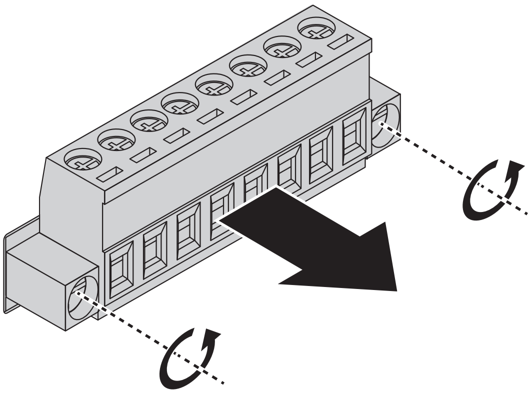


Figure 2.19 Removing a Terminal Block

3. Insert a small flat-bladed screwdriver in the V1+/V1- wire-clamp screws, and loosen the screws.
4. Insert the negative/positive DC wires into the V+/V- terminals of PW1. If setting up power redundancy, connect PW2 in the same manner.

5. Tighten the wire-clamp screws to secure the DC wires in place.

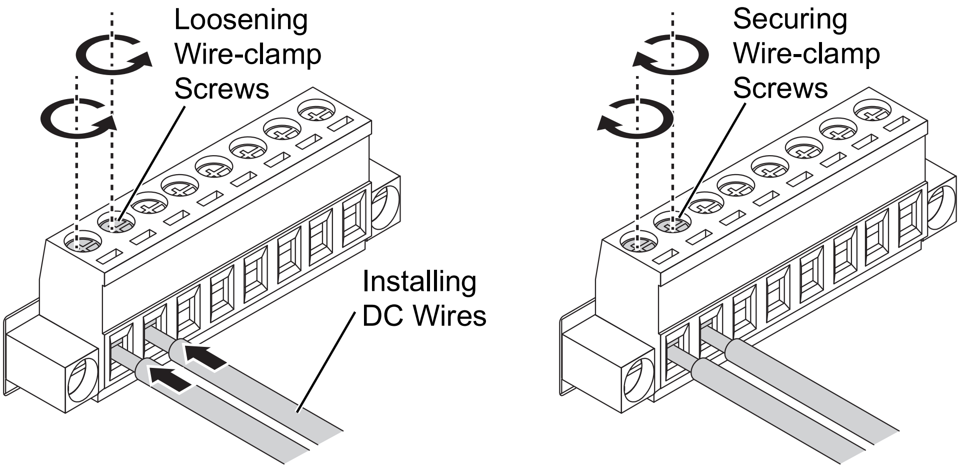


Figure 2.20 Installing DC Wires in a Terminal Block

6. Align the terminal block over the terminal block receptor on the device.
7. Insert the terminal block and press it in until it is flush with the terminal block receptor.
8. Tighten the screws on the terminal block to secure it to the terminal block receptor.

   If there is no gap between the terminal block and the terminal receptor, the terminal block is seated correctly.

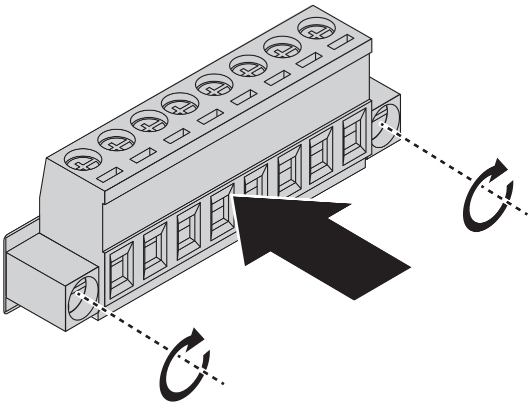


Figure 2.21 Securing a Terminal Block to a Receptor

2.3 Reset Button

Reset configuration to factory default:

Press and hold Reset button for 6 seconds.

System reboot:

Press and hold Reset button for 2 seconds.

Note! *Do NOT power off the WiFi AP when loading default settings.*

Chapter 3

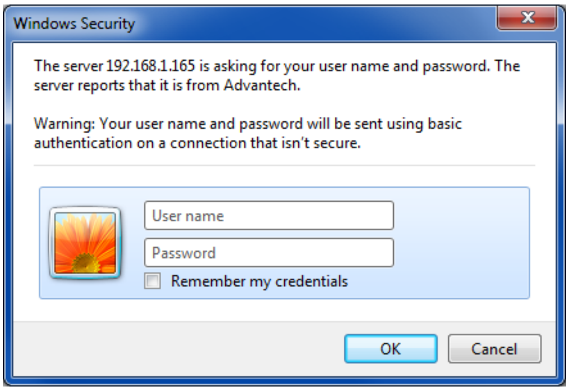
Web Interface

3.1 Log In

To access the login window, connect the device to the network, see “Network Connection” on page 12. Once the device is installed and connected, power on the device see the following procedures to log into your device.

When the device is first installed, the default IP is 192.168.1.1. You will need to make sure your network environment supports the device setup before connecting it to the network.

1. Launch your web browser on a computer.
2. In the browser’s address bar type in the device’s default IP address (192.168.1.1). The login screen displays.
3. Enter the default user name and password (admin/admin) to log into the management interface. You can change the default password after you have successfully logged in.
4. Click **Login** to enter the management interface.



Windows Security

The server 192.168.1.165 is asking for your user name and password. The server reports that it is from Advantech.

Warning: Your user name and password will be sent using basic authentication on a connection that isn’t secure.

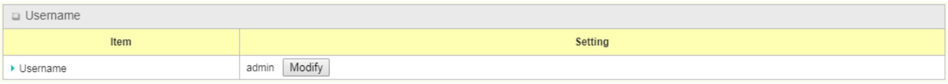
Figure 3.1 Login Screen

Note! *Screen may differ depending on Web browsers.*

3.1.1 Password

The HTTP page allows you to configure the WiFi AP login details.

1. Log in to the user interface menu, see “Log In” on page 20.
2. Navigate to **Administration** > **System Operation** > **Password & MMI**. The Password & MMI page displays.
3. In Username section, click **Modify**.
4. Enter the username of the profile to change, then enter the new password under the **Password** field.
5. Click **Save** to change the current account settings.



Username

Item	Setting
Username	admin Modify

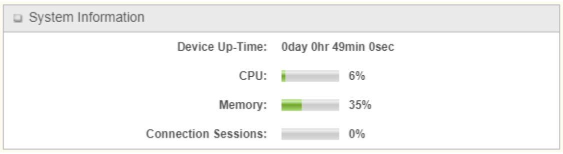
Figure 3.2 Administration > System Operation > Password & MMI

3.2 Status

3.2.1 Dashboard

To access this page, click **Status** > **Dashboard**.

The **System Information** screen shows the device Up-time and the resource utilization for the CPU, Memory, and Connection Sessions.



System Information

Device Up-Time:	0day 0hr 49min 0sec
CPU:	6%
Memory:	35%
Connection Sessions:	0%

Figure 3.3 Status > Dashboard > System Information

The **System Information History** screen shows the statistic graphs for the CPU and memory.

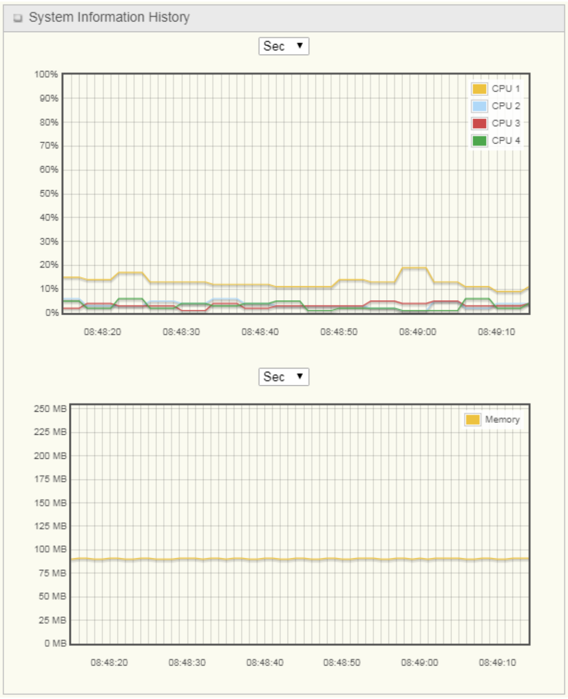
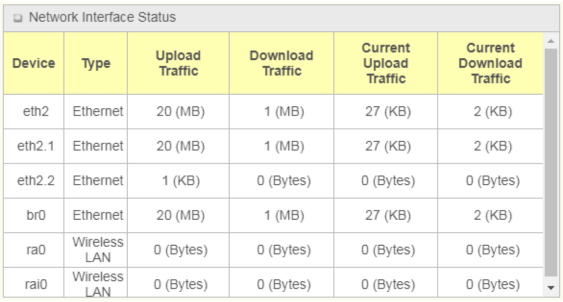


Figure 3.4 Status > Dashboard > System Information History

The **Network Interface Status** screen shows the statistic information for each network interface of the gateway. The statistic information includes the Interface Type, Upload Traffic, Download Traffic, and Current Upload / Download Traffic.

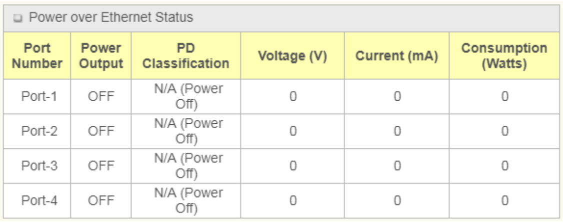


Network Interface Status

Device	Type	Upload Traffic	Download Traffic	Current Upload Traffic	Current Download Traffic
eth2	Ethernet	20 (MB)	1 (MB)	27 (KB)	2 (KB)
eth2.1	Ethernet	20 (MB)	1 (MB)	27 (KB)	2 (KB)
eth2.2	Ethernet	1 (KB)	0 (Bytes)	0 (Bytes)	0 (Bytes)
br0	Ethernet	20 (MB)	1 (MB)	27 (KB)	2 (KB)
ra0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
rai0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)

Figure 3.5 Status > Dashboard > Network Interface Status

The **Power over Ethernet Status** screen shows the PoE information for each port. The information includes the Power Output, PD Classification, Voltage, Current, and Consumption.



Power over Ethernet Status

Port Number	Power Output	PD Classification	Voltage (V)	Current (mA)	Consumption (Watts)
Port-1	OFF	N/A (Power Off)	0	0	0
Port-2	OFF	N/A (Power Off)	0	0	0
Port-3	OFF	N/A (Power Off)	0	0	0
Port-4	OFF	N/A (Power Off)	0	0	0

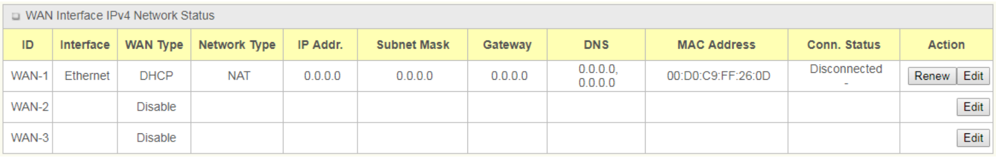
Figure 3.6 Status > Dashboard > Power over Ethernet Status

3.2.2 Basic Network

3.2.2.1 WAN & Uplink

To access this page, click **Status** > **Basic Network** > **WAN & Uplink**.

The **WAN & Uplink** screen shows the current status for different network type, including network configuration, connecting information, modem status and traffic statistics. The display will be refreshed on every five seconds.



WAN Interface IPv4 Network Status

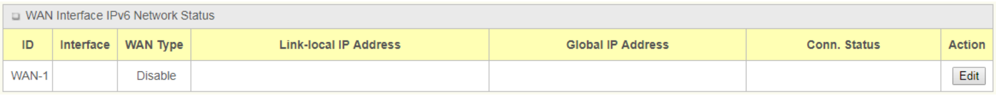
ID	Interface	WAN Type	Network Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	Ethernet	DHCP	NAT	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	00:D0:C9:FF:26:0D	Disconnected -	Renew Edit
WAN-2		Disable								Edit
WAN-3		Disable								Edit

Figure 3.7 Status > Basic Network > WAN & Uplink > WAN Interface IPv4 Network Status

The following table describes the items in the previous figure.

Item	Description
ID	It displays corresponding WAN interface WAN IDs.
Interface	It displays the type of WAN physical interface. Depending on the model purchased, it can be **WiFi Module** or **Ethernet**.
WAN Type	It displays the method which public IP address is obtained from your ISP. Depending on the model purchased, it can be **Static IP**, **Dynamic IP**, **PPPoE**, **PPTP**, or **L2TP**.
Network Type	It displays the network type for the WAN interface(s). Depending on the model purchased, it can be **NAT**, **Routing**, **Bridge**, or **IP Pass-through**.

Item	Description
IP Addr.	It displays the public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
Subnet Mask	It displays the subnet mask for public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
Gateway	It displays the gateway IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
DNS	It displays the IP address of DNS server obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
MAC Address	It displays the MAC address for your ISP to allow you for Internet access. ***Note:*** *Not all ISP may require this field.*
Conn. Status	It displays the connection status of the device to your ISP. Status are connected or disconnected.
Action	■ **Renew** button allows user to force the device to request an IP address from the DHCP server. ***Note:*** ***Renew** button is available when DHCP WAN Type is used and WAN connection is disconnected.* ■ **Release** button allows user to force the device to clear its IP address setting to disconnect from DHCP server. ***Note:*** ***Release** button is available when DHCP WAN Type is used and WAN connection is connected.* ■ **Connect** button allows user to manually connect the device to the Internet. ***Note:*** ***Connect** button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network** > **WAN & Uplink** > **Internet Setup**) and WAN connection status is disconnected.* ■ **Disconnect** button allows user to manually disconnect the device from the Internet. ***Note:*** ***Connect** button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network** > **WAN & Uplink** > **Internet Setup**) and WAN connection status is connected.*



WAN Interface IPv6 Network Status

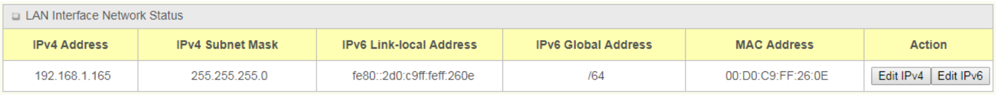
ID	Interface	WAN Type	Link-local IP Address	Global IP Address	Conn. Status	Action
WAN-1		Disable				Edit

Figure 3.8 Status > Basic Network > WAN & Uplink > WAN Interface IPv6 Network Status

The following table describes the items in the previous figure.

Item	Description
ID	It displays corresponding WAN interface WAN IDs.
Interface	It displays the type of WAN physical interface. Depending on the model purchased, it can be **WiFi Module** or **Ethernet**.

Item	Description
WAN Type	It displays the method which public IP address is obtained from your ISP. WAN type setting can be changed from **Basic Network** > **IPv6** > **Configuration**.
Link-local IP Address	It displays the LAN IPv6 Link-Local address.
Global IP Address	It displays the IPv6 global IP address assigned by your ISP for your Internet connection.
Conn. Status	It displays the connection status. The status can be connected, disconnected and connecting.
Action	**Edit** button when pressed, web-based utility will take you to the **IPv6** configuration page. (**Basic Network** > **IPv6** > **Configuration**)



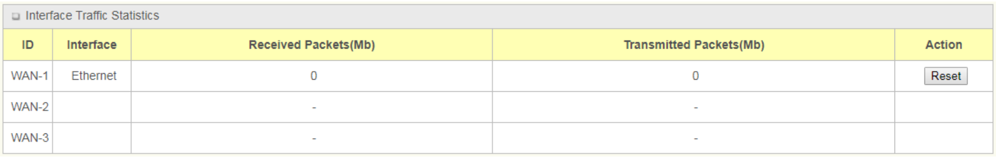
LAN Interface Network Status

IPv4 Address	IPv4 Subnet Mask	IPv6 Link-local Address	IPv6 Global Address	MAC Address	Action
192.168.1.165	255.255.255.0	fe80::2d0:c9ff:feff:260e	/64	00:D0:C9:FF:26:0E	Edit IPv4 Edit IPv6

Figure 3.9 Status > Basic Network > WAN & Uplink > LAN Interface Network Status

The following table describes the items in the previous figure.

Item	Description
IPv4 Address	It displays the current IPv4 IP address of the gateway. This is also the IP address user use to access Router’s Web-based Utility.
IPv4 Subnet Mask	It displays the current mask of the subnet.
IPv6 Link-local Address	It displays the current LAN IPv6 Link-Local address. This is also the IPv6 IP address user use to access router’s Web-based utility.
IPv6 Global Address	It displays the current IPv6 global IP address assigned by your ISP for your Internet connection.
MAC Address	It displays the LAN MAC address of the gateway
Action	■ **Edit IPv4** button when press, web-based utility will take you to the **Ethernet LAN** configuration page. (**Basic Network** > **LAN & VLAN** > **Ethernet LAN**). ■ **Edit IPv6** button when press, web-based utility will take you to the **IPv6** configuration page. (**Basic Network** > **IPv6** > **Configuration**)



Interface Traffic Statistics

ID	Interface	Received Packets(Mb)	Transmitted Packets(Mb)	Action
WAN-1	Ethernet	0	0	Reset
WAN-2		-	-	
WAN-3		-	-	

Figure 3.10 Status > Basic Network > WAN & Uplink > Interface Traffic Statistics

The following table describes the items in the previous figure.

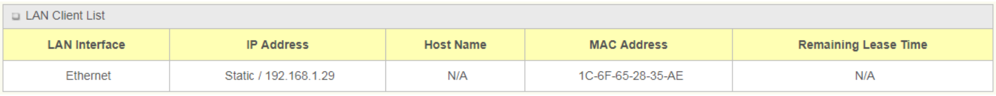
Item	Description
ID	It displays corresponding WAN interface WAN IDs.
Interface	It displays the type of WAN physical interface. Depending on the model purchased, it can be **Ethernet**, **3G/4G**, etc...
Received Packets (Mb)	It displays the statistics of downstream packets (Mb). It is reset when the device is rebooted.

Item	Description
Transmitted Packets (Mb)	It displays the statistics of upstream packets (Mb). It is reset when the device is rebooted.
Action	**Reset** button when pressed, allows user to reset the downstream/ upstream packets.

3.2.2.2 LAN & VLAN

To access this page, click **Status** > **Basic Network** > **LAN & VLAN**.

The **LAN Client List** shows you the LAN Interface, IP address, Host Name, MAC Address, and Remaining Lease Time of each device that is connected to this gateway.



❑ LAN Client List

LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Static / 192.168.1.29	N/A	1C-6F-65-28-35-AE	N/A

Figure 3.11 Status > Basic Network > LAN & VLAN

The following table describes the items in the previous figure.

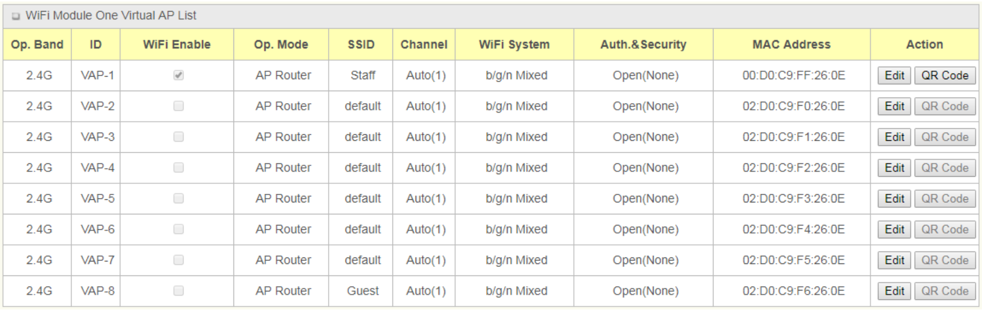
Item	Description
LAN Interface	Client record of LAN interface. String format.
IP Address	Client record of IP address type and the IP address. Type is string format and the IP address is IPv4 format.
Host Name	Client record of host name. String format.
MAC Address	Client record of MAC address. MAC Address format.
Remaining Lease Time	Client record of remaining lease time. Time format.

3.2.2.3 WiFi

To access this page, click **Status** > **Basic Network** > **WiFi**.

The **WiFi** screen shows the overall statistics of WiFi VAP entries.

The **WiFi Module Virtual AP List** shows all of the virtual AP information. The **Edit** button allows for quick configuration changes.



❑ WiFi Module One Virtual AP List

Op. Band	ID	WiFi Enable	Op. Mode	SSID	Channel	WiFi System	Auth.&Security	MAC Address	Action
2.4G	VAP-1	☑	AP Router	Staff	Auto(1)	b/g/n Mixed	Open(None)	00:D0:C9:FF:26:0E	Edit QR Code
2.4G	VAP-2	☐	AP Router	default	Auto(1)	b/g/n Mixed	Open(None)	02:D0:C9:F0:26:0E	Edit QR Code
2.4G	VAP-3	☐	AP Router	default	Auto(1)	b/g/n Mixed	Open(None)	02:D0:C9:F1:26:0E	Edit QR Code
2.4G	VAP-4	☐	AP Router	default	Auto(1)	b/g/n Mixed	Open(None)	02:D0:C9:F2:26:0E	Edit QR Code
2.4G	VAP-5	☐	AP Router	default	Auto(1)	b/g/n Mixed	Open(None)	02:D0:C9:F3:26:0E	Edit QR Code
2.4G	VAP-6	☐	AP Router	default	Auto(1)	b/g/n Mixed	Open(None)	02:D0:C9:F4:26:0E	Edit QR Code
2.4G	VAP-7	☐	AP Router	default	Auto(1)	b/g/n Mixed	Open(None)	02:D0:C9:F5:26:0E	Edit QR Code
2.4G	VAP-8	☐	AP Router	Guest	Auto(1)	b/g/n Mixed	Open(None)	02:D0:C9:F6:26:0E	Edit QR Code

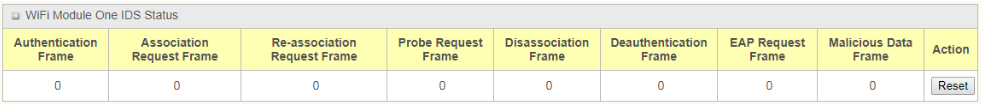
Figure 3.12 Status > Basic Network > WiFi > WiFi Module Virtual AP List

The following table describes the items in the previous figure.

Item	Description
Op. Band	It displays the WiFi operation band (2.4G or 5G) of VAP.
ID	It displays the ID of VAP.
WiFi Enable	It displays whether the VAP wireless signal is enabled or disabled.
Op. Mode	The WiFi operation mode of VAP. Depends of device model, modes are **AP Router**, **WDS Only** and **WDS Hybrid** and **Client**.
SSID	It displays the network ID of VAP.

Item	Description
Channel	It displays the wireless channel used.
WiFi System	The WiFi system of VAP.
Auth.&Security	It displays the authentication and encryption type used.
Auth.&Security	It displays MAC Address of VAP.
Action	Click **Edit** to make a quick access to the **WiFi** configuration page. (**Basic Network** > **WiFi** > **WiFi Module**) The **QR Code** button allow you to generate QR code for quick connect to the VAP by scanning the QR code.

The **WiFi Module IDS Status** shows all the received and transmitted packets on WiFi network.



WiFi Module One IDS Status

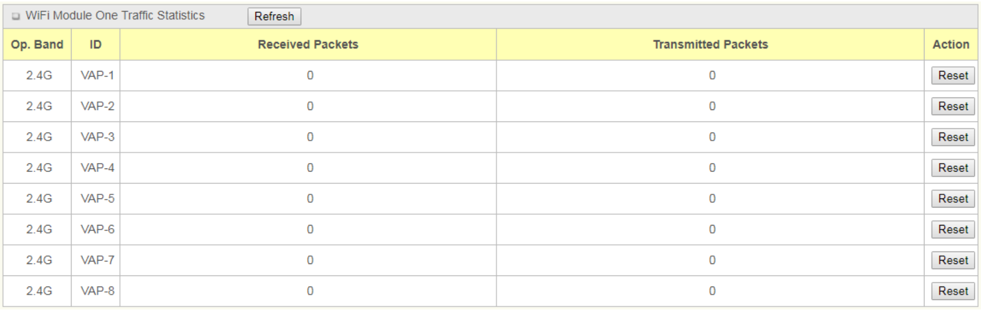
Authentication Frame	Association Request Frame	Re-association Request Frame	Probe Request Frame	Disassociation Frame	Deauthentication Frame	EAP Request Frame	Malicious Data Frame	Action
0	0	0	0	0	0	0	0	Reset

Figure 3.13 Status > Basic Network > WiFi > WiFi Module IDS Status

The following table describes the items in the previous figure.

Item	Description
Authentication Frame	It displays the receiving authentication frame count.
Association Request Frame	It displays the receiving association request frame count.
Re-association Request Frame	It displays the receiving re-association request frame count.
Probe Request Frame	It displays the receiving probe request frame count.
Disassociation Frame	It displays the receiving disassociation frame count.
Deauthentication Frame	It displays the receiving deauthentication frame count.
EAP Request Frame	It displays the receiving EAP request frame count.
Malicious Data Frame	It displays the number of receiving unauthorized wireless packets.
Action	Click **Reset** to clear the entire statistic and reset counter to 0.

The **WiFi Module Traffic Statistics** shows all the received and transmitted packets on WiFi network.



WiFi Module One Traffic Statistics Refresh

Op. Band	ID	Received Packets	Transmitted Packets	Action
2.4G	VAP-1	0	0	Reset
2.4G	VAP-2	0	0	Reset
2.4G	VAP-3	0	0	Reset
2.4G	VAP-4	0	0	Reset
2.4G	VAP-5	0	0	Reset
2.4G	VAP-6	0	0	Reset
2.4G	VAP-7	0	0	Reset
2.4G	VAP-8	0	0	Reset

Figure 3.14 Status > Basic Network > WiFi > WiFi Module Traffic Statistics

The following table describes the items in the previous figure.

Item	Description
Op. Band	It displays the WiFi operation band (2.4G or 5G) of VAP.
ID	It displays the VAP ID.
Received Packets	It displays the number of received packets.
Transmitted Packets	It displays the number of transmitted packets.

Item	Description
Action	Click **Reset** to clear individual VAP statistics.
Refresh	Click **Refresh** to update the entire VAP traffic statistic instantly.

3.2.3 Security

See “Security” on page 101 for further information.

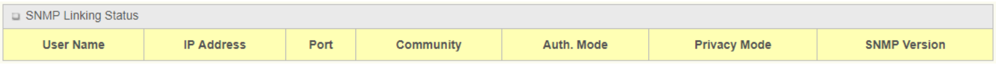
3.2.4 Administration

3.2.4.1 Configure & Manage

To access this page, click **Status** > **Administration** > **Configure & Manage**.

The **Configure & Manage** screen shows the status for managing remote network devices. The type of management available in your device is depended on the device model purchased. The commonly used ones are the SNMP, TR-069, and UPnP. The display will be refreshed on every five seconds.

The **SNMP Linking Status** shows the status of current active SNMP connections.



SNMP Linking Status

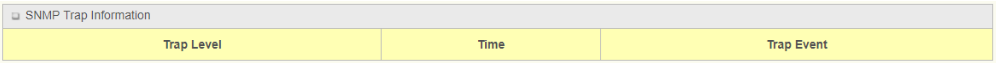
User Name	IP Address	Port	Community	Auth. Mode	Privacy Mode	SNMP Version

Figure 3.15 Status > Administration > Configure & Manage > SNMP Linking Status

The following table describes the items in the previous figure.

Item	Description
User Name	It displays the user name for authentication. This is only available for SNMP version 3.
IP Address	It displays the IP address of SNMP manager.
Port	It displays the port number used to maintain connection with the SNMP manager.
Community	It displays the community for SNMP version 1 or version 2c only.
Auth. Mode	It displays the authentication method for SNMP version 3 only.
Privacy Mode	It displays the privacy mode for version 3 only.
SNMP Version	It displays the SNMP Version employed.

The **SNMP Trap Information** shows the status of current received SNMP traps.



SNMP Trap Information

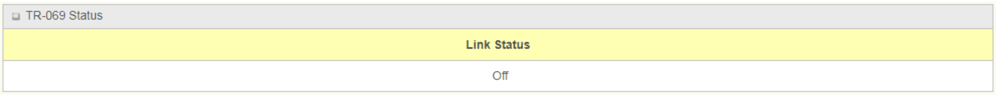
Trap Level	Time	Trap Event

Figure 3.16 Status > Administration > Configure & Manage > SNMP Trap Information

The following table describes the items in the previous figure.

Item	Description
Trap Level	It displays the trap level.
Time	It displays the time stamp of trap event.
Trap Event	It displays the IP address of the trap sender and event type.

The **TR-069 Status** shows the current connection status with the TR-068 server.



TR-069 Status

Link Status
Off

Figure 3.17 Status > Administration > Configure & Manage > TR-069 Status

The following table describes the items in the previous figure.

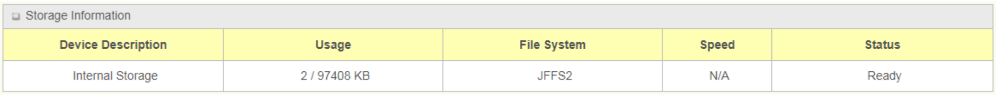
Item	Description
Link Status	It displays the current connection status with the TR-068 server. The connection status is either **On** when the device is connected with the TR-068 server or **Off** when disconnected.

3.2.4.2 Log Storage

To access this page, click **Status** > **Administration** > **Log Storage**.

The **Log Storage Status** screen shows the status for selected device storage.

The **Storage Information** shows the status of current the selected device storage. The status includes Device Select, Device Description, Usage, File System, Speed, and status



Storage Information

Device Description	Usage	File System	Speed	Status
Internal Storage	2 / 97408 KB	JFFS2	N/A	Ready

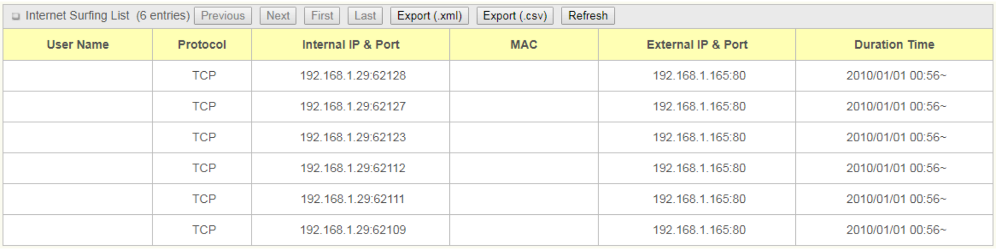
Figure 3.18 Status > Administration > Log Storage

3.2.5 Statistics & Reports

3.2.5.1 Connection Session

To access this page, click **Status** > **Statistics & Reports** > **Connection Session**.

The **Internet Surfing List** shows the connection tracks on this router.



User Name	Protocol	Internal IP & Port	MAC	External IP & Port	Duration Time
	TCP	192.168.1.29:62128		192.168.1.165:80	2010/01/01 00:56~
	TCP	192.168.1.29:62127		192.168.1.165:80	2010/01/01 00:56~
	TCP	192.168.1.29:62123		192.168.1.165:80	2010/01/01 00:56~
	TCP	192.168.1.29:62112		192.168.1.165:80	2010/01/01 00:56~
	TCP	192.168.1.29:62111		192.168.1.165:80	2010/01/01 00:56~
	TCP	192.168.1.29:62109		192.168.1.165:80	2010/01/01 00:56~

Figure 3.19 Status > Statistics & Reports > Connection Session

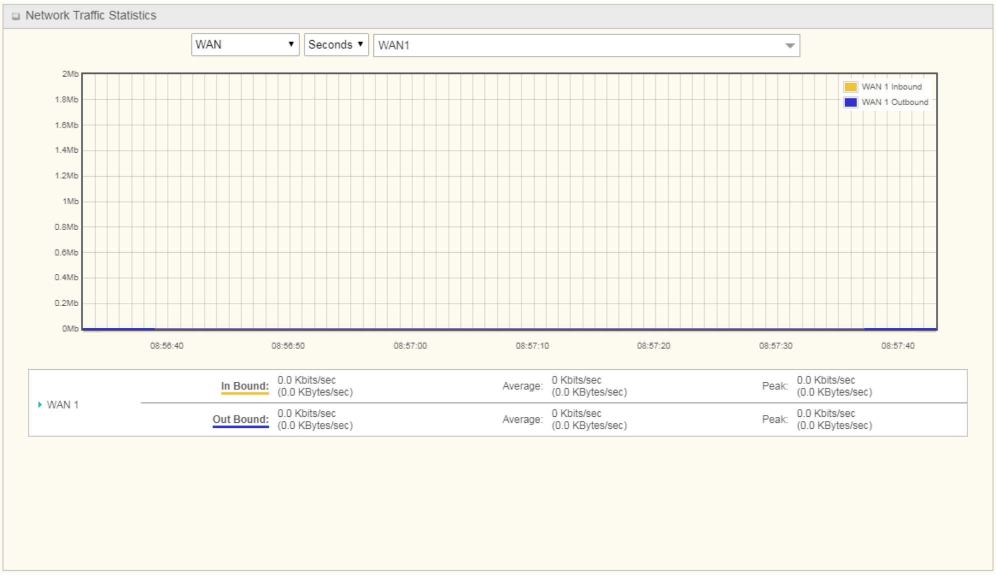
The following table describes the items in the previous figure.

Item	Description
Previous	Click the **Previous** button to see the previous page of track list.
Next	Click the **Next** button to see the next page of track list.
First	Click the **First** button to see the first page of track list.
Last	Click the **Last** button to see the last page of track list.
Export (.xml)	Click the **Export (.xml)** button to export the list to .xml file.
Export (.csv)	Click the **Export (.csv)** button to export the list to .csv file.
Refresh	Click the **Refresh** button to refresh the list.

3.2.5.2 Network Traffic

To access this page, click **Status** > **Statistics & Reports** > **Network Traffic**.

The **Network Traffic** screen shows the historical graph for the selected network interface. You can change the interface drop list and select the interface you want to monitor.



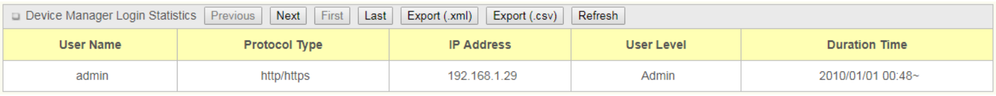
‣ WAN 1	In Bound:	0.0 Kbits/sec (0.0 KBytes/sec)	Average:	0 Kbits/sec (0.0 KBytes/sec)	Peak:	0.0 Kbits/sec (0.0 KBytes/sec)
	Out Bound:	0.0 Kbits/sec (0.0 KBytes/sec)	Average:	0 Kbits/sec (0.0 KBytes/sec)	Peak:	0.0 Kbits/sec (0.0 KBytes/sec)

Figure 3.20 Status > Statistics & Reports > Network Traffic

3.2.5.3 Login Statistics

To access this page, click **Status** > **Statistics & Reports** > **Login Statistics**.

The **Login Statistics** screen shows the login information.



User Name	Protocol Type	IP Address	User Level	Duration Time
admin	http/https	192.168.1.29	Admin	2010/01/01 00:48~

Figure 3.21 Status > Statistics & Reports > Login Statistics

The following table describes the items in the previous figure.

Item	Description
Previous	Click **Previous** to see the previous page of login statistics.
Next	Click **Next** to see the next page of login statistics.
First	Click **First** to see the first page of login statistics.
Last	Click **Last** to see the last page of login statistics.
Export (.xml)	Click **Export (.xml)** to export the login statistics to .xml file.
Export (.csv)	Click **Export (.csv)** to export the login statistics to .csv file.
Refresh	Click **Refresh** to refresh the login statistics.

3.3 Basic Network

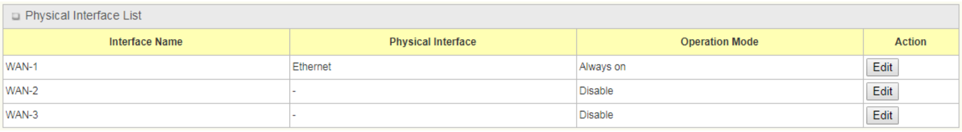
3.3.1 WAN & Uplink

3.3.1.1 Physical Interface

To access this page, click **Basic Network** > **WAN & Uplink** > **Physical Interface**.

The **Physical Interface** screen allows user to setup the physical WAN interface and to adjust WAN’s behavior.

> ***Note!*** *Numbers of available WAN Interfaces can be different for the purchased gateway.*

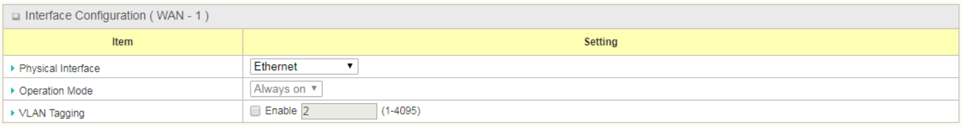


Physical Interface List

Interface Name	Physical Interface	Operation Mode	Action
WAN-1	Ethernet	Always on	Edit
WAN-2	-	Disable	Edit
WAN-3	-	Disable	Edit

Figure 3.22 Basic Network > WAN & Uplink > Physical Interface

When **Edit** button is applied, an **Interface Configuration** screen appears. WAN-1 interface is used in this example.



Interface Configuration (WAN - 1)

Item	Setting
Physical Interface	Ethernet ▾
Operation Mode	Always on ▾
VLAN Tagging	□ Enable 2 (1-4095)

Figure 3.23 Basic Network > WAN & Uplink > Physical Interface > Interface Configuration

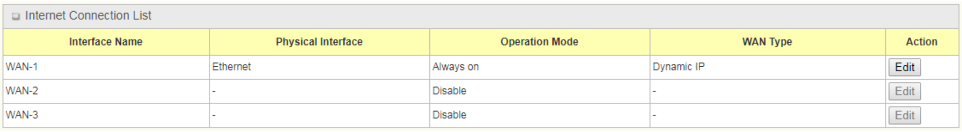
The following table describes the items in the previous figure.

Item	Description
Physical Interface	Select one expected interface from the available interface drop-down menu. It can be **Ethernet** or **WiFi Module**. Depending on the gateway model, Disable and failover options will be available only to multiple WAN gateways.
Operation Band	If WiFi module is specified as the physical interface, the Operation Band item will be displayed for radio band selection. Specify the radio band for WiFi uplink connection. If the WiFi module in use is a 2.4G/5GHz selectable module, please select one band for uplink connection. ***Note:*** *This is only available for 2.4G/5GHz selectable module.*

Item	Description
Operation Mode	Define the operation mode of the interface. ■ Select **Always** on to make this WAN always active. ■ Select **Disable** to disable this WAN interface. ■ Select **Failover** to make this WAN a failover WAN when the primary or the secondary WAN link failed. Then select the primary or the existed secondary WAN interface to switch failover from. ***Note:*** *For WAN-1, only Always on option is available.*
VLAN Tagging	Check **Enable** checkbox to enter tag value provided by your ISP. Otherwise uncheck the box. Value Range: 1 ~ 4096. ***Note:*** *This feature is NOT available for 3G/4G WAN connection.*

3.3.1.2 Connection Setup

To access this page, click **Basic Network** > **WAN & Uplink** > **Connection Setup**.

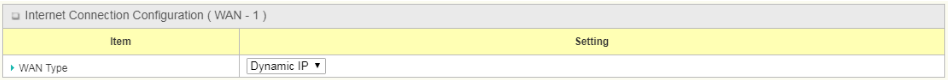


Internet Connection List

Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Dynamic IP	Edit
WAN-2	-	Disable	-	Edit
WAN-3	-	Disable	-	Edit

Figure 3.24 Basic Network > WAN & Uplink > Connection Setup

When **Edit** button is applied, the **Internet Connection Configuration** screen appears. WAN-1 interface is used in this example.



Internet Connection Configuration (WAN - 1)

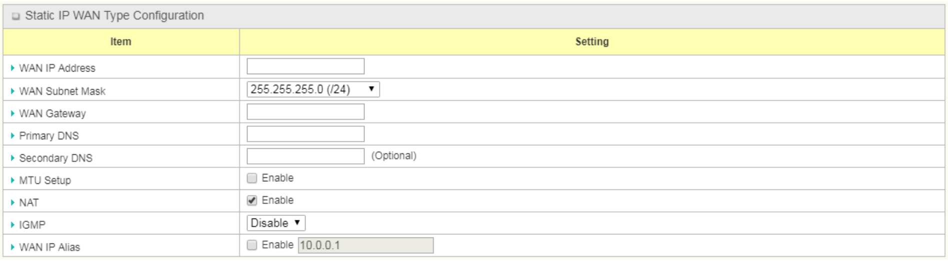
Item	Setting
WAN Type	Dynamic IP ▾

Figure 3.25 Basic Network > WAN & Uplink > Connection Setup > Internet Connection Configuration

The following table describes the items in the previous figure.

Item	Description
WAN Type	Click the drop-down menu to select WAN type, options: **Static IP**, **Dynamic IP** (Default), **PPPoE**, **PPTP**, or **L2TP**.

When **WAN Type** is **Static IP**, the **Static IP WAN Type Configuration** appears.



Static IP WAN Type Configuration

Item	Setting
WAN IP Address	
WAN Subnet Mask	255.255.255.0 (/24) ▾
WAN Gateway	
Primary DNS	
Secondary DNS	(Optional)
MTU Setup	□ Enable
NAT	☑ Enable
IGMP	Disable ▾
WAN IP Alias	□ Enable 10.0.0.1

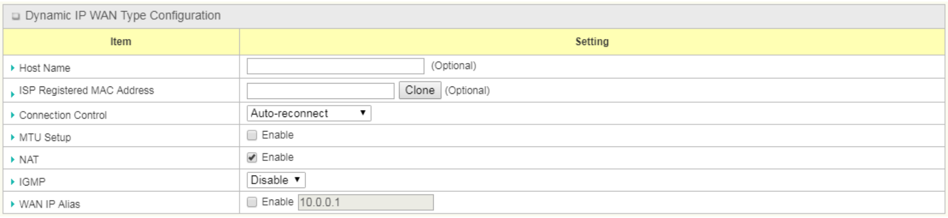
Figure 3.26 Basic Network > WAN & Uplink > Connection Setup > Static IP WAN Type Configuration

The following table describes the items in the previous figure.

Item	Description
WAN IP Address	Enter the WAN IP address given by your service provider.

Item	Description
WAN Subnet Mask	Enter the WAN subnet mask given by your service provider.
WAN Gateway	Enter the WAN gateway IP address given by your service provider.
Primary DNS	Enter the primary WAN DNS IP address given by your service provider.
Secondary DNS	Enter the secondary WAN DNS IP address given by your service provider.
MTU Setup	Check **Enable** checkbox to enable the MTU (Maximum Transmission Unit) limit, and specify the MTU for the 3G/4G connection. MTU (Maximum Transmission Unit) specifies the largest packet size permitted for Internet transmission. Value Range: 1200 ~ 1500.
NAT	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
IGMP	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	Enable WAN IP Alias then enter the IP address provided by your service provider. WAN IP Alias is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

When **WAN Type** is **Dynamic IP**, the **Dynamic IP WAN Type Configuration** appears.



Dynamic IP WAN Type Configuration

Item	Setting
Host Name	(Optional)
ISP Registered MAC Address	Clone (Optional)
Connection Control	Auto-reconnect ▾
MTU Setup	☐ Enable
NAT	☑ Enable
IGMP	Disable ▾
WAN IP Alias	☐ Enable 10.0.0.1

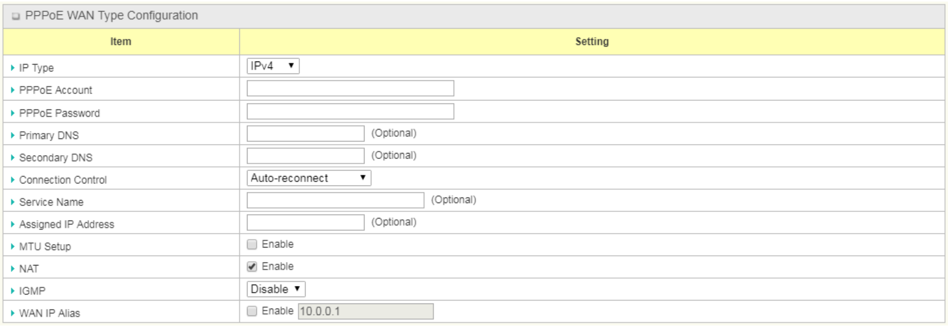
Figure 3.27 Basic Network > WAN & Uplink > Connection Setup > Dynamic IP WAN Type Configuration

The following table describes the items in the previous figure.

Item	Description
Host Name	Enter the host name provided by your service provider.
ISP Registered MAC Address	Enter the MAC address that you have registered with your service provider. Or click **Clone** to clone your PC’s MAC to this field. Usually this is the PC’s MAC address assigned to allow you to connect to Internet.

Item	Description
Connection Control	There are three connection modes. ■ **Auto-reconnect** enables the router to always keep the Internet connection on. ■ **Connect-on-demand** enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time. ■ **Connect Manually** allows user to connect to Internet manually. Internet connection will be inactive after it has been inactive for specified idle time.
MTU Setup	Check **Enable** checkbox to enable the MTU (Maximum Transmission Unit) limit, and specify the MTU for the 3G/4G connection. MTU (Maximum Transmission Unit) specifies the largest packet size permitted for Internet transmission. Value Range: 1200 ~ 1500.
NAT	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
IGMP	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	Enable WAN IP Alias then enter the IP address provided by your service provider. WAN IP Alias is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

When **WAN Type** is **PPPoE**, the **PPPoE WAN Type Configuration** appears.



PPPoE WAN Type Configuration

Item	Setting
IP Type	IPv4 ▾
PPPoE Account	
PPPoE Password	
Primary DNS	(Optional)
Secondary DNS	(Optional)
Connection Control	Auto-reconnect ▾
Service Name	(Optional)
Assigned IP Address	(Optional)
MTU Setup	□ Enable
NAT	☑ Enable
IGMP	Disable ▾
WAN IP Alias	□ Enable 10.0.0.1

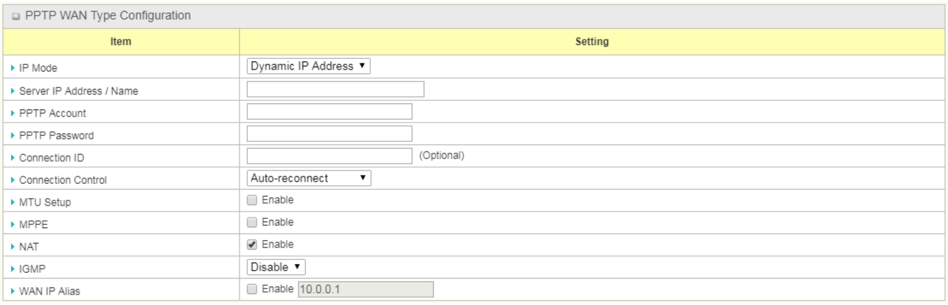
Figure 3.28 Basic Network > WAN & Uplink > Connection Setup > PPPoE WAN Type Configuration

The following table describes the items in the previous figure.

Item	Description
IP Type	Click the drop-down menu to select the IP type, options: **IPv4**, **IPv6**, or **IPv4/6**.
PPPoE Account	Enter the PPPoE user name provided by your service provider.
PPPoE Password	Enter the PPPoE password provided by your service provider.
Primary DNS	Enter the IP address of primary DNS server.
Secondary DNS	Enter the IP address of secondary DNS server.

Item	Description
Connection Control	There are three connection modes. ■ **Auto-reconnect** enables the router to always keep the Internet connection on. ■ **Connect-on-demand** enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time. ■ **Connect Manually** allows user to connect to Internet manually. Internet connection will be inactive after it has been inactive for specified idle time.
Service Name	Enter the service name if your ISP requires it.
Assigned IP Address	Enter the IP address assigned by your service provider.
MTU Setup	Check **Enable** checkbox to enable the MTU (Maximum Transmission Unit) limit, and specify the MTU for the 3G/4G connection. MTU refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Value Range: 1200 ~ 1500.
NAT	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
IGMP	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	Enable WAN IP Alias then enter the IP address provided by your service provider. WAN IP Alias is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

When **WAN Type** is **PPTP**, the **PPTP WAN Type Configuration** appears.



PPTP WAN Type Configuration

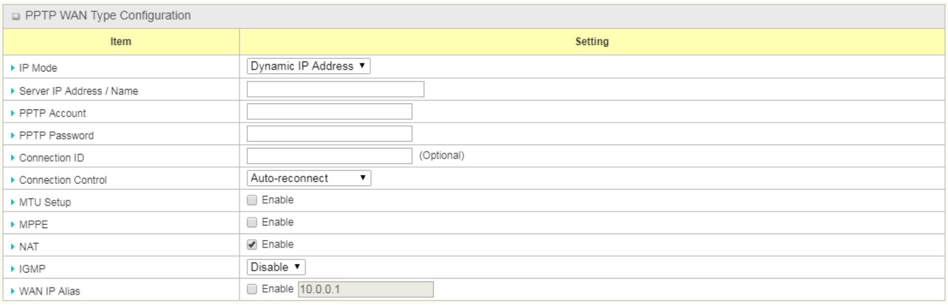
Item	Setting
IP Mode	Dynamic IP Address ▾
Server IP Address / Name	
PPTP Account	
PPTP Password	
Connection ID	(Optional)
Connection Control	Auto-reconnect ▾
MTU Setup	□ Enable
MPPE	□ Enable
NAT	☑ Enable
IGMP	Disable ▾
WAN IP Alias	□ Enable 10.0.0.1

Figure 3.29 Basic Network > WAN & Uplink > Connection Setup > PPTP WAN Type Configuration

The following table describes the items in the previous figure.

Item	Description
IP Mode	Select either Static or Dynamic IP address for PPTP Internet connection. ■ When **Static IP Address** is selected, you will need to enter the WAN IP Address, WAN Subnet Mask, and WAN Gateway. – **WAN IP Address:** Enter the WAN IP address given by your service provider. – **WAN Subnet Mask:** Enter the WAN subnet mask given by your service provider. – **WAN Gateway:** Enter the WAN gateway IP address given by your service provider. ■ When **Dynamic IP Address** is selected, there are no above settings required.
Server IP Address / Name	Enter the PPTP server name or IP Address.
PPTP Account	Enter the PPTP username provided by your service provider.
PPTP Password	Enter the PPTP connection password provided by your service provider.
Connection ID	Enter a name to identify the PPTP connection.
Connection Control	There are three connection modes. ■ **Auto-reconnect** enables the router to always keep the Internet connection on. ■ **Connect-on-demand** enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time. ■ **Connect Manually** allows user to connect to Internet manually. Internet connection will be inactive after it has been inactive for specified idle time.
MTU Setup	Check **Enable** checkbox to enable the MTU (Maximum Transmission Unit) limit, and specify the MTU for the 3G/4G connection. MTU refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Value Range: 1200 ~ 1500.
MPPE	Check **Enable** checkbox to enable MPPE (Microsoft Point-to-Point Encryption) security for PPTP connection.
NAT	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
IGMP	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	Enable WAN IP Alias then enter the IP address provided by your service provider. WAN IP Alias is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

When **WAN Type** is **L2TP**, the **L2TP WAN Type Configuration** appears.



PPTP WAN Type Configuration

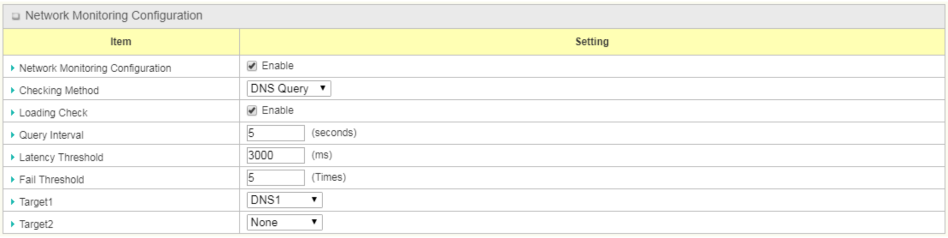
Item	Setting
IP Mode	Dynamic IP Address ▾
Server IP Address / Name	
PPTP Account	
PPTP Password	
Connection ID	(Optional)
Connection Control	Auto-reconnect ▾
MTU Setup	□ Enable
MPPE	□ Enable
NAT	☑ Enable
IGMP	Disable ▾
WAN IP Alias	□ Enable 10.0.0.1

Figure 3.30 Basic Network > WAN & Uplink > Connection Setup > L2TP WAN Type Configuration

The following table describes the items in the previous figure.

Item	Description
IP Mode	Select either Static or Dynamic IP address for L2TP Internet connection. ■ When **Static IP Address** is selected, you will need to enter the WAN IP Address, WAN Subnet Mask, and WAN Gateway. – **WAN IP Address:** Enter the WAN IP address given by your service provider. – **WAN Subnet Mask:** Enter the WAN subnet mask given by your service provider. – **WAN Gateway:** Enter the WAN gateway IP address given by your service provider. ■ When **Dynamic IP Address** is selected, there are no above settings required.
Server IP Address / Name	Enter the L2TP server name or IP Address.
L2TP Account	Enter the L2TP username provided by your service provider.
L2TP Password	Enter the L2TP connection password provided by your service provider.
Connection Control	There are three connection modes. ■ **Auto-reconnect** enables the router to always keep the Internet connection on. ■ **Connect-on-demand** enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time. ■ **Connect Manually** allows user to connect to Internet manually. Internet connection will be inactive after it has been inactive for specified idle time.
MTU Setup	Check **Enable** checkbox to enable the MTU (Maximum Transmission Unit) limit, and specify the MTU for the 3G/4G connection. MTU refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Value Range: 1200 ~ 1500.

Item	Description
Service Port	Enter the service port that the Internet service. There are three options can be selected: ■ **Auto:** Port will be automatically assigned. ■ **1701 (For Cisco):** Set service port to port 1701 to connect to CISCO server. ■ **User-defined:** enter a service port provided by your service provider.
MPPE	Check **Enable** checkbox enable MPPE (Microsoft Point-to-Point Encryption) security for PPTP connection.
NAT	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
IGMP	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	Enable WAN IP Alias then enter the IP address provided by your service provider. WAN IP Alias is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



Network Monitoring Configuration

Item	Setting
Network Monitoring Configuration	☑ Enable
Checking Method	DNS Query ▾
Loading Check	☑ Enable
Query Interval	5 (seconds)
Latency Threshold	3000 (ms)
Fail Threshold	5 (Times)
Target1	DNS1 ▾
Target2	None ▾

Figure 3.31 Basic Network > WAN & Uplink > Connection Setup > Network Monitoring Configuration

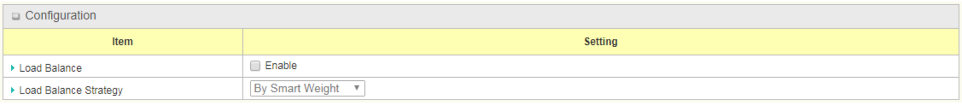
The following table describes the items in the previous figure.

Item	Description
Network Monitoring Configuration	When the Network Monitoring feature is enabled, the gateway will use DNS Query or ICMP to periodically check Internet connection – connected or disconnected.
Checking Method	Select either **DNS Query** or **ICMP Checking** to detect WAN link. ■ With **DNS Query**, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. ■ With **ICMP Checking**, the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2.
Loading Check	Enable Loading Check allows the router to ignore unreturned DNS Queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status.
Query Interval	Defines the transmitting interval between two DNS Query or ICMP checking packets.

Item	Description
Latency Threshold	Defines the tolerance threshold of responding time.
Fail Threshold	Specifies the detected disconnection before the router recognize the WAN link down status. Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged.
Target1	Specifies the first target of sending DNS query/ICMP request. ■ **DNS1:** set the primary DNS to be the target. ■ **DNS2:** set the secondary DNS to be the target. ■ **Gateway:** set the Current gateway to be the target. ■ **Other Host:** enter an IP address to be the target.
Target2	Specifies the second target of sending DNS query/ICMP request. ■ **None:** to disable Target2. ■ **DNS1:** set the primary DNS to be the target. ■ **DNS2:** set the secondary DNS to be the target. ■ **Gateway:** set the Current gateway to be the target. ■ **Other Host:** enter an IP address to be the target.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.3.1.3 Load Balance

To access this page, click **Basic Network** > **WAN & Uplink** > **Load Balance**.



Configuration

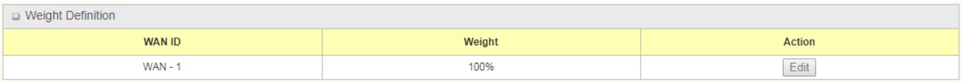
Item	Setting
Load Balance	□ Enable
Load Balance Strategy	By Smart Weight ▾

Figure 3.32 Basic Network > WAN & Uplink > Load Balance

The following table describes the items in the previous figure.

Item	Description
Load Balance	Check **Enable** checkbox to activate Load Balance function.
Load Balance Strategy	There are up to three load balance strategies. Select the preferred one. - **By Smart Weight:** System will operate load balance function automatically based on the embedded Smart Weight algorithm. - **By Specific Weight:** System will adjust the ratio of transferred sessions among all WANs based on the specified weights for each WAN. - **By User Policy:** System will route traffics through available WAN interface based on user defined rules. ***Note:*** *The number of available strategies depends on the model you purchased.*
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

When **By Specific Weight** is selected, user needs to adjust the percentage of WAN loading. System will give a value according to the bandwidth ratio of each WAN at first time and keep the value after clicking **Save**.



Weight Definition

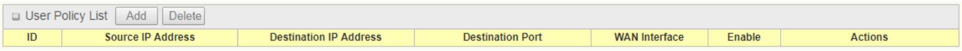
WAN ID	Weight	Action
WAN - 1	100%	Edit

Figure 3.33 Basic Network > WAN & Uplink > Load Balance

The following table describes the items in the previous figure.

Item	Description
WAN ID	The Identifier for each available WAN interface.
Weight	Enter the weight ratio for each WAN interface. Initially, the bandwidth ratio of each WAN is set by default. Value Range: 1 ~ 99. ***Note:*** *The sum of all weights can't be greater than 100%.*
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

When **By User Policy** is selected, a **User Policy List** screen appears. With properly configured your policy rules, system will route traffics through available WAN interface based on user defined rules.



User Policy List Add Delete

ID	Source IP Address	Destination IP Address	Destination Port	WAN Interface	Enable	Actions

Figure 3.34 Basic Network > WAN & Uplink > Load Balance

When **Add** button is applied, the **User Policy Configuration** appears.

Figure 3.35 Basic Network > WAN & Uplink > Load Balance > User Policy Configuration

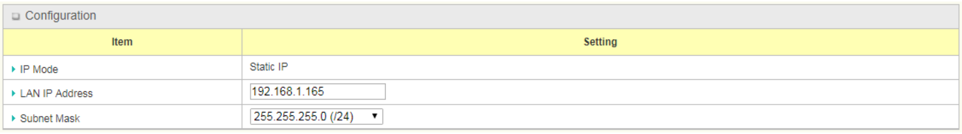
The following table describes the items in the previous figure.

Item	Description
Source IP Address	There are four options can be selected: ■ **Any:** No specific Source IP is provided. The traffic may come from any source. ■ **Subnet:** Specify the Subnet for the traffics come from the subnet. Input format is: xxx.xxx.xxx.xxx/xx e.g. 192.168.123.0/24. ■ **IP Range:** Specify the IP Range for the traffics come from the IPs. ■ **Single IP:** Specify a unique IP Address for the traffics come from the IP. Input format is: xxx.xxx.xxx.xxx e.g. 192.168.123.101.
Destination IP Address	There are five options can be selected: ■ **Any:** No specific destination IP is provided. The traffic may come to any destination. ■ **Subnet:** Specify the Subnet for the traffics come to the subnet. Input format is: xxx.xxx.xxx.xxx/xx e.g. 192.168.123.0/24. ■ **IP Range:** Specify the IP Range for the traffics come to the IPs. ■ **Single IP:** Specify a unique IP Address for the traffics come to the IP. Input format is: xxx.xxx.xxx.xxx e.g. 192.168.123.101. ■ **Domain Name:** Specify the domain name for the traffics come to the domain.
Destination Port	There are four options can be selected: ■ **All:** No specific destination port is provided. ■ **Port Range:** Specify the Destination Port Range for the traffics. ■ **Single Port:** Specify a unique destination Port for the traffics. ■ **Well-known Applications:** Select the service port of well-known application defined in drop-down menu.
Protocol	There are three options can be selected. They are **Both**, **TCP**, and **UDP**.
WAN Interface	User can select the interface that traffic should go. Note that the WAN interface drop-down menu will only show the available WAN interfaces.
Policy	Check **Enable** checkbox to activate the policy rule.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.3.2 LAN & VLAN

3.3.2.1 Ethernet LAN

To access this page, click **Basic Network** > **LAN & VLAN** > **Ethernet LAN**.



Configuration

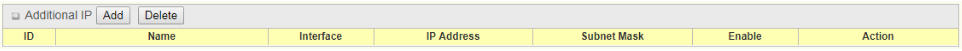
Item	Setting
IP Mode	Static IP
LAN IP Address	192.168.1.165
Subnet Mask	255.255.255.0 (/24) ▾

Figure 3.36 Basic Network > LAN & VLAN > Ethernet LAN

The following table describes the items in the previous figure.

Item	Description
IP Mode	It shows the LAN IP mode for the gateway according the related configuration. ■ **Static IP:** If there is at least one WAN interface activated, the LAN IP mode is fixed in Static IP mode. ■ **Dynamic IP:** If all the available WAN interfaces are disabled, the LAN IP mode can be Dynamic IP mode.
LAN IP Address	Enter the local IP address of this device. The network device(s) on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary. ***Note:*** *It's also the IP address of web UI. If you change it, you need to type new IP address in the browser to see web UI.*
Subnet Mask	Select the subnet mask for this gateway from the drop-down menu. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. Value Range: 255.0.0.0 (/8) ~ 255.255.255.252 (/30).
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

This gateway provides the LAN IP alias function for some special management consideration. You can add additional LAN IP for this gateway, and access to this gateway with the additional IP.

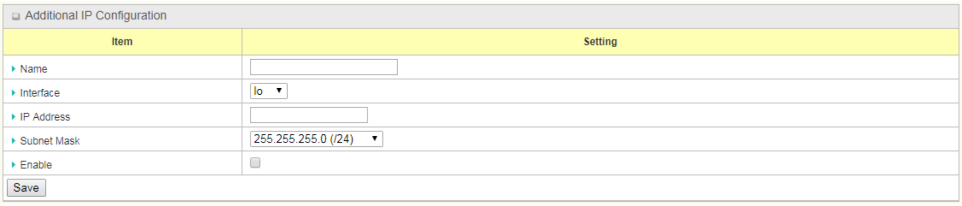


Additional IP [Add] [Delete]

ID	Name	Interface	IP Address	Subnet Mask	Enable	Action

Figure 3.37 Basic Network > LAN & VLAN > Ethernet LAN

When **Add** button is applied, the **Additional IP Configuration** screen appears.



Additional IP Configuration

Item	Setting
Name	
Interface	lo ▾
IP Address	
Subnet Mask	255.255.255.0 (/24) ▾
Enable	□

[Save]

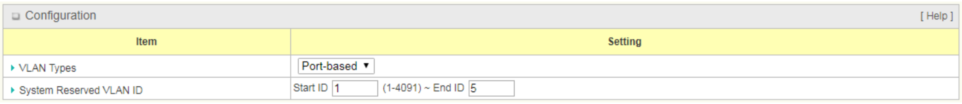
Figure 3.38 Basic Network > LAN & VLAN > Ethernet LAN > Additional IP Configuration

The following table describes the items in the previous figure.

Item	Description
Name	Enter the name for the alias IP address.
Interface	Specify the Interface type. It can be **lo** or **br0**.
IP Address	Enter the addition IP address for this device.
Subnet Mask	Select the subnet mask for this gateway from the drop-down menu. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/ 24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. Value Range: 255.0.0.0 (/8) ~ 255.255.255.255 (/32).
Enable	Click **Enable** checkbox to activate Additional IP function.
Save	Click **Save** to save the settings.

3.3.2.2 VLAN

To access this page, click **Basic Network** > **LAN & VLAN** > **VLAN**.



Configuration [Help]

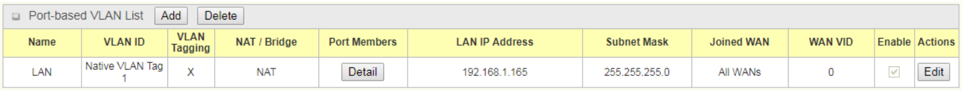
Item	Setting
VLAN Types	Port-based ▾
System Reserved VLAN ID	Start ID 1 (1-4091) ~ End ID 5

Figure 3.39 Basic Network > LAN & VLAN > VLAN

The following table describes the items in the previous figure.

Item	Description
VLAN Types	Select the VLAN type that you want to adopt for organizing you local subnets. ■ **Port-based:** Port-based VLAN allows you to add rule for each LAN port, and you can do advanced control with its VLAN ID. ■ **Tag-based:** Tag-based VLAN allows you to add VLAN ID, and select member and DHCP Server for this VLAN ID. Go to Tag-based VLAN List table.
System Reserved VLAN ID	Specify the start ID (1 - 4091) and end ID for the reserved VLAN.
Apply	Click **Apply** to save the settings.

The **Port-based VLAN List** allows you to custom each LAN port. There is a default rule shows the configuration of all LAN ports. Also, if your device has a DMZ port, you will see DMZ configuration, too. The maxima rule numbers is based on LAN port numbers.

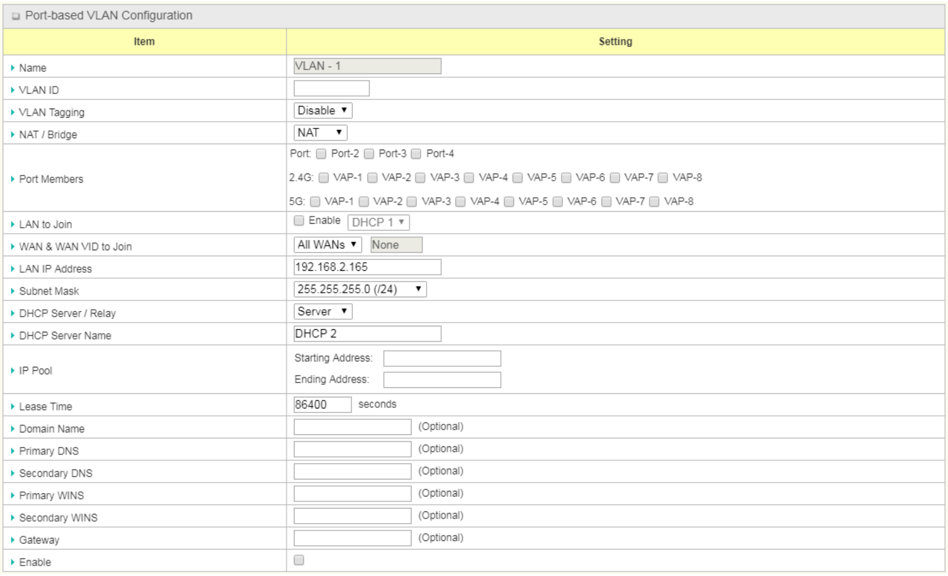


Port-based VLAN List Add Delete

Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
LAN	Native VLAN Tag 1	X	NAT	Detail	192.168.1.165	255.255.255.0	All WANs	0	☑	Edit

Figure 3.40 Basic Network > LAN & VLAN > VLAN > Port-based VLAN List

When **Add** button is applied, the **Port-based VLAN Configuration** screen will appear, which is including 3 sections: Port-based VLAN Configuration, IP Fixed Mapping Rule List, and **Inter VLAN Group Routing** (enter through a button).



Port-based VLAN Configuration

Item	Setting
Name	VLAN - 1
VLAN ID	
VLAN Tagging	Disable ▼
NAT / Bridge	NAT ▼
Port Members	Port: □ Port-2 □ Port-3 □ Port-4 2.4G: □ VAP-1 □ VAP-2 □ VAP-3 □ VAP-4 □ VAP-5 □ VAP-6 □ VAP-7 □ VAP-8 5G: □ VAP-1 □ VAP-2 □ VAP-3 □ VAP-4 □ VAP-5 □ VAP-6 □ VAP-7 □ VAP-8
LAN to Join	□ Enable DHCP 1 ▼
WAN & WAN VID to Join	All WANs ▼ None
LAN IP Address	192.168.2.165
Subnet Mask	255.255.255.0 (/24) ▼
DHCP Server / Relay	Server ▼
DHCP Server Name	DHCP 2
IP Pool	Starting Address: Ending Address:
Lease Time	86400 seconds
Domain Name	(Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)
Enable	□

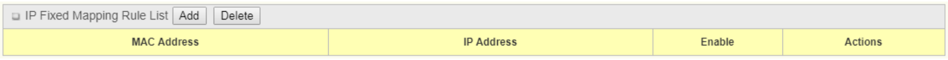
Figure 3.41 Basic Network > LAN & VLAN > VLAN > Port-based VLAN Configuration

The following table describes the items in the previous figure.

Item	Description
Name	Define the Name of this rule. It has a default text and cannot be modified.
VLAN ID	Define the VLAN ID number, range is 1 ~ 4094.
VLAN Tagging	The rule is activated according to **VLAN ID** and **Port Members** configuration when **Enable** is selected. The rule is activated according **Port Members** configuration when **Disable** is selected.
NAT / Bridge	Select **NAT** mode or **Bridge** mode for the rule.
Port Members	Select which LAN port(s) and VAP(s) that you want to add to the rule. ***Note:*** *The available member list can be different for the purchased product.*
LAN to Join	Check **Enable** checkbox to activate the function. Click the drop-down menu to select name of the emulated LAN to join. The emulated LAN name must already be configured on the switch. If the name is not configured on the switch, the device joins the default emulated LAN.
WAN & WAN VID to Join	Select which WAN or All WANs that allow accessing Internet. ***Note:*** *If Bridge mode is selected, you need to select a WAN and enter a VID.*
LAN IP Address	Assign an IP address for the DHCP server that the rule used, this IP address is a gateway IP.
Subnet Mask	Select a subnet mask for the DHCP server.

Item	Description
DHCP Server / Relay	Define the DHCP server type. There are three types you can select: **Server**, **Relay**, and **Disable**. ■ **Relay:** Select **Relay** to enable DHCP Relay function for the VLAN group, and you only need to fill the DHCP server IP Address field. ■ **Server:** Select **Server** to enable DHCP server function for the VLAN group, and you need to specify the DHCP server settings. ■ **Disable:** Select **Disable** to disable the DHCP server function for the VLAN group.
DHCP Server IP Address	If you select **Relay** type of **DHCP server**, assign a DHCP server IP address that the gateway will relay the DHCP requests to the assigned DHCP server.
DHCP Server Name	Define name of the DHCP Server for the specified VLAN group.
IP Pool	Define the IP Pool range. There are **Starting Address** and **Ending Address** fields. If a client requests an IP address from this DHCP server, it will assign an IP address in the range of IP pool.
Lease Time	Define a period of time for an IP Address that the DHCP server leases to a new device. By default, the lease time is 86400 seconds.
Domain Name	The domain name of this DHCP server. Value Range: 0 ~ 31 characters.
Primary DNS	The primary DNS of this DHCP Server.
Secondary DNS	The secondary DNS of this DHCP Server.
Primary WINS	The primary WINS of this DHCP Server.
Secondary WINS	The secondary WINS of this DHCP Server.
Gateway	The Gateway of this DHCP Server.
Enable	Click **Enable** checkbox to activate this rule.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

Besides, you can add some IP rules in the **IP Fixed Mapping Rule List** if DHCP Server for the VLAN groups is required.

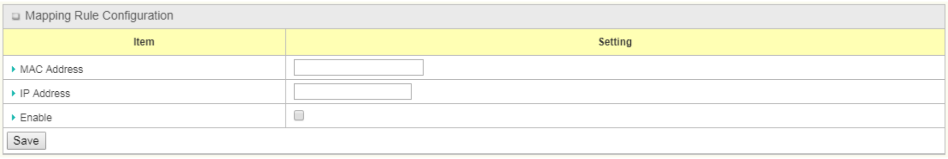


IP Fixed Mapping Rule List

MAC Address	IP Address	Enable	Actions

Figure 3.42 Basic Network > LAN & VLAN > VLAN > IP Fixed Mapping Rule List

When **Add** button is applied, the **Mapping Rule Configuration** screen appears.



Mapping Rule Configuration

Item	Setting
MAC Address	
IP Address	
Enable	□

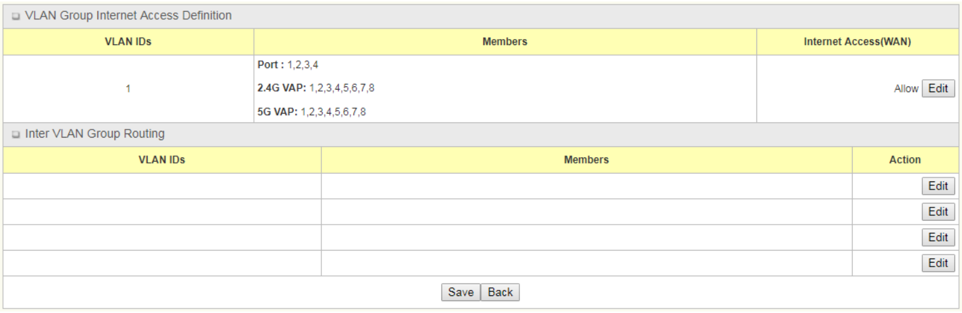
Figure 3.43 Basic Network > LAN & VLAN > VLAN > Mapping Rule Configuration

The following table describes the items in the previous figure.

Item	Description
MAC Address	Define the MAC address target that the DHCP server wants to match.
IP Address	Define the IP address that the DHCP server will assign. If there is a request from the MAC Address filled in the above field, the DHCP server will assign this IP Address to the client whose MAC address matched the rule.
Enable	Click **Enable** checkbox to activate this rule.
Save	Click **Save** to save the settings.

Note! *Ensure to always click on **Apply** button to apply the changes after the web browser refreshed taken you back to the VLAN page.*

Click **Inter VLAN Group Routing** button, the **VLAN Group Internet Access Definition** and **Inter VLAN Group Routing** screens appears.



VLAN Group Internet Access Definition

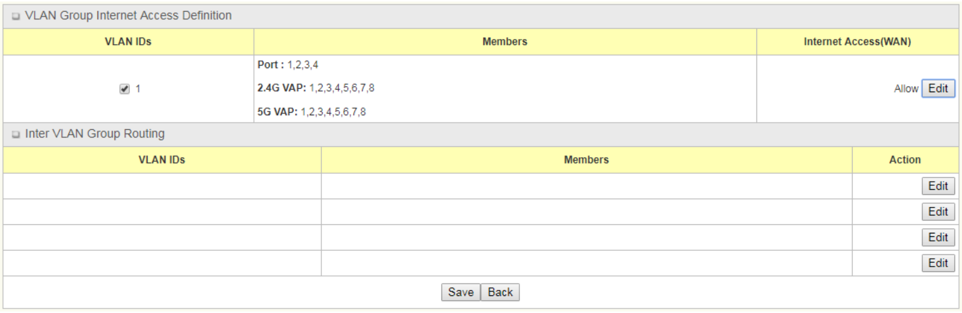
VLAN IDs	Members	Internet Access(WAN)
1	**Port :** 1,2,3,4 **2.4G VAP:** 1,2,3,4,5,6,7,8 **5G VAP:** 1,2,3,4,5,6,7,8	Allow Edit

Inter VLAN Group Routing

VLAN IDs	Members	Action
		Edit
		Edit
		Edit
		Edit

Figure 3.44 Basic Network > LAN & VLAN > VLAN

When **Edit** button is applied, a screen similar to this appears.



VLAN Group Internet Access Definition

VLAN IDs	Members	Internet Access(WAN)
☑ 1	**Port :** 1,2,3,4 **2.4G VAP:** 1,2,3,4,5,6,7,8 **5G VAP:** 1,2,3,4,5,6,7,8	Allow Edit

Inter VLAN Group Routing

VLAN IDs	Members	Action
		Edit
		Edit
		Edit
		Edit

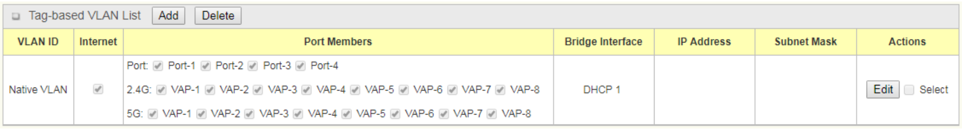
Figure 3.45 Basic Network > LAN & VLAN > VLAN

The following table describes the items in the previous figure.

Item	Description
VLAN Group Internet Access Definition	By default, all boxes are checked means all VLAN ID members are allow to access WAN interface. If uncheck a certain VLAN ID box, it means the VLAN ID member can't access Internet anymore. ***Note:*** *VLAN ID 1 is available always; it is the default VLAN ID of LAN rule. The other VLAN IDs are available only when they are enabled.*

Item	Description
Inter VLAN Group Routing	Click the expected VLAN IDs box to enable the Inter VLAN access function. By default, members in different VLAN IDs can't access each other. The gateway supports up to 4 rules for Inter VLAN Group Routing. For example, if ID_1 and ID_2 are checked, it means members in VLAN ID_1 can access members of VLAN ID_2, and vice versa.
Save	Click **Save** to save the settings.
Back	Click **Back** to return the previous screen.

The **Tag-based VLAN** allows you to customize each LAN port according to VLAN ID. There is a default rule shows the configuration of all LAN ports and all VAPs. Also, if your device has a DMZ port, you will see DMZ configuration, too. The router supports up to a maximum of 128 tag-based VLAN rule sets.

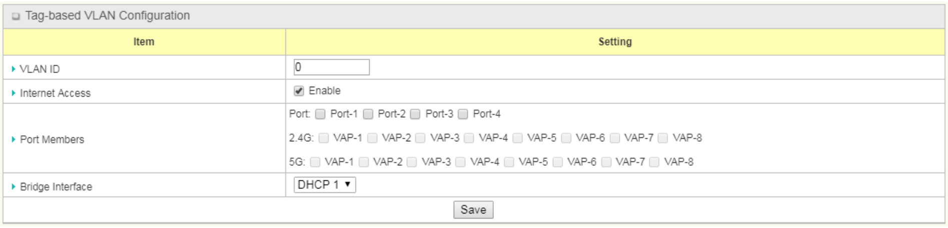


Tag-based VLAN List [Add] [Delete]

VLAN ID	Internet	Port Members	Bridge Interface	IP Address	Subnet Mask	Actions
Native VLAN	☑	Port: ☑ Port-1 ☑ Port-2 ☑ Port-3 ☑ Port-4 2.4G: ☑ VAP-1 ☑ VAP-2 ☑ VAP-3 ☑ VAP-4 ☑ VAP-5 ☑ VAP-6 ☑ VAP-7 ☑ VAP-8 5G: ☑ VAP-1 ☑ VAP-2 ☑ VAP-3 ☑ VAP-4 ☑ VAP-5 ☑ VAP-6 ☑ VAP-7 ☑ VAP-8	DHCP 1			[Edit] □ Select

Figure 3.46 Basic Network > LAN & VLAN > VLAN

When **Add** button is applied, the **Tag-based VLAN Configuration** screen appears.



Tag-based VLAN Configuration

Item	Setting
VLAN ID	0
Internet Access	☑ Enable
Port Members	Port: □ Port-1 □ Port-2 □ Port-3 □ Port-4 2.4G: □ VAP-1 □ VAP-2 □ VAP-3 □ VAP-4 □ VAP-5 □ VAP-6 □ VAP-7 □ VAP-8 5G: □ VAP-1 □ VAP-2 □ VAP-3 □ VAP-4 □ VAP-5 □ VAP-6 □ VAP-7 □ VAP-8
Bridge Interface	DHCP 1 ▾

[Save]

Figure 3.47 Basic Network > LAN & VLAN > VLAN

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Define the VLAN ID number, range is 6 ~ 4094.
Internet Access	Click **Enable** checkbox to allow the members in the VLAN group access to Internet.
Port Members	Check the box(es) to join the VLAN group. ***Note:*** *Only the wireless gateway has the VAP list.*
Bridge Interface	Select a bridge interface to these members of this VLAN group. To create or edit DHCP server for VLAN, refer to **Basic Network** > **LAN & VLAN** > **DHCP Server**.
Save	Click **Save** to save the settings. ***Note:*** *After clicking **Save** button, always click **Apply** button to apply the settings.*

3.3.2.3 PoE

Power over Ethernet (PoE) describes any of several standardized or ad-hoc systems which pass electric power along with data on twisted pair Ethernet cabling. This allows a single cable to provide both data connection and electric power to devices such as wireless access points, IP cameras, and VoIP phones.

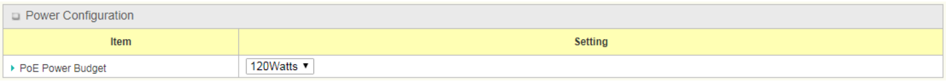
This PoE cellular gateway integrated four-port PoE switch function, and plays as Power Sourcing Equipment (PSE) role that provides power on the Ethernet cable. The PoE design is compliant to IEEE802.3af/at standard, The PSE can auto-detect the type of connected PD (Powered Device) and provide adequate power to it. The maximum allowed continuous output power per cable is 15.4W for IEEE 802.3af PD device, and 30W for IEEE802.3at PD device.

However, to make the PoE cellular gateway provide required power through the Ethernet cables, you have to prepare required PoE power supply and connect it to the PoE cellular gateway properly, as stated in “Connecting Hardware” on page 8. The PSE power sourcing capability is up to 120W. If you intend to connect four 802.3at PD devices to the PoE cellular gateway, you have to make sure your PoE power supply can provide enough power, more than 120W (e.g., power supply with rated capability 180W) to the gateway.

In addition to provide required power to connected PDs, this PoE cellular gateway also provides simple management function to control the power budgets and connected PDs. The PoE port management function includes PoE port control, PD failure check and Power Off/On by schedule.

To access this page, click **Basic Network** > **LAN & VLAN** > **PoE**.

The Power over Ethernet setting allows administrator to control PoE related function, such as Power Budget, Port Power Limit, etc…



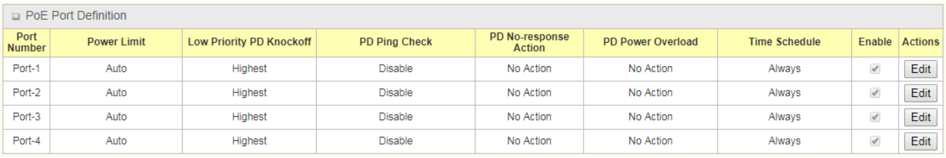
Power Configuration

Item	Setting
PoE Power Budget	120Watts ▼

Figure 3.48 Basic Network > LAN & VLAN > PoE

The following table describes the items in the previous figure.

Item	Description
PoE Power Budget	Specify the PoE power budget. It can be **120Watts**, **60Watts**, or **Manual**. If you select **Manual**, you have to enter the power budget. With specified power budget, the PoE gateway can monitor whether the connected PD devices caused power overflow, and force the connected PD with lowest priority to be off line to prevent power overflow situation. Value Range: 4 ~ 120 Watts.
Save	Click **Save** to save the settings.

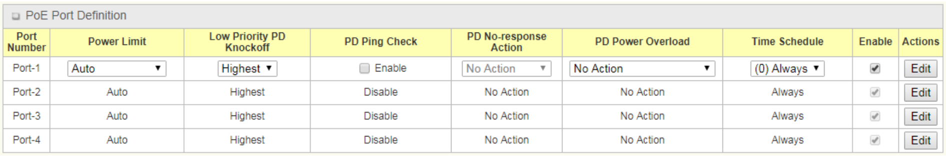


PoE Port Definition

Port Number	Power Limit	Low Priority PD Knockoff	PD Ping Check	PD No-response Action	PD Power Overload	Time Schedule	Enable	Actions
Port-1	Auto	Highest	Disable	No Action	No Action	Always	☑	Edit
Port-2	Auto	Highest	Disable	No Action	No Action	Always	☑	Edit
Port-3	Auto	Highest	Disable	No Action	No Action	Always	☑	Edit
Port-4	Auto	Highest	Disable	No Action	No Action	Always	☑	Edit

Figure 3.49 Basic Network > LAN & VLAN > PoE

Click the **Edit** button to edit the settings for each PoE port.



PoE Port Definition

Port Number	Power Limit	Low Priority PD Knockoff	PD Ping Check	PD No-response Action	PD Power Overload	Time Schedule	Enable	Actions
Port-1	Auto ▼	Highest ▼	□ Enable	No Action ▼	No Action ▼	(0) Always ▼	☑	Edit
Port-2	Auto	Highest	Disable	No Action	No Action	Always	☑	Edit
Port-3	Auto	Highest	Disable	No Action	No Action	Always	☑	Edit
Port-4	Auto	Highest	Disable	No Action	No Action	Always	☑	Edit

Figure 3.50 Basic Network > LAN & VLAN > PoE

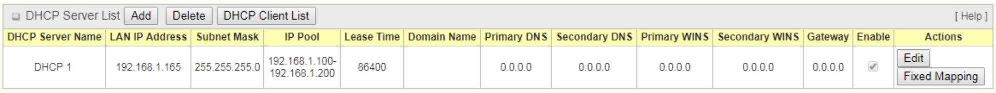
The following table describes the items in the previous figure.

Item	Description
Power Limit	Specify the Power Limit for the PoE port. It can be **Auto**, **802.3af (4W)**, **802.3af (7W)**, **802.3af(15.4W)**, **802.3at(30W)**, or **Manual**. If you select **Manual**, you have to enter the power limit. Value Range: 1 ~ 30 Watts.
Low Priority PD Knockoff	Specify the Port Priority. It can be **Highest**, **High**, or **Low**. Whenever there is a shortage of total power budget, the port with lowest priority will be disabled automatically to provide required power to the ports with higher priority. If there are more than one ports with the same lowest priority, the port number decide it, Port 1 > Port 2 > Port 3 > Port 4, it means Port 4 has the lowest priority on such case.
PD Ping Check	Check **Enable** checkbox to activate PD Ping Check function. In addition to enable the function, you have to specify a timeout value for timeout check. Value Range: 10 ~ 300 seconds.
PD No-response Action	Specify the action to take when the PD doesn't reply the Ping check activity. (PD No-response). It could be **No Action** or **Power off/on**. Select Power off/on to restart the PD device, if required.
PD Power Overload	Specify the action to take when the PD Power overflow occurs for a certain port. It can be **No Action** or **Power Long Time Off/On**. If the Power overload occurs (PD consumes more power than the value specified in the Power Limit setting), the PSE function for the PoE port will be disabled for 30 minutes. That is, PD device will be powered OFF for a long time, and then after 30minutes, it will be powered ON again. If you encountered such situation, please check if the Power Limit setting is properly, or the PD device always consumes too much power.
Time Schedule	Apply Time Schedule to control the power ON/OFF schedule of the connected PD, otherwise leave it as **(0) Always**. If the drop-down menu is empty, ensure **Time Schedule** is preconfigured. Refer to **Object Definition** > **Scheduling** > **Configuration**.
Enable	Check **Enable** checkbox to enable the PoE port.
Save	Click **Save** to save the settings.

3.3.2.4 DHCP Server

To access this page, click **Basic Network** > **LAN & VLAN** > **DHCP Server**.

The **DHCP Server** setting allows user to create and customize DHCP Server policies to assign IP Addresses to the devices on the local area network (LAN).

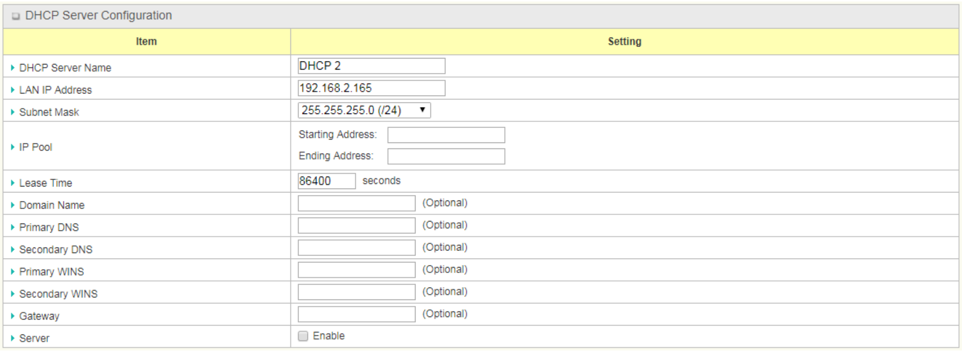


DHCP Server List | Add | Delete | DHCP Client List | [Help]

DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Enable	Actions
DHCP 1	192.168.1.165	255.255.255.0	192.168.1.100- 192.168.1.200	86400		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	☑	Edit Fixed Mapping

Figure 3.51 Basic Network > LAN & VLAN > DHCP Server

When **Add** button is applied, the **DHCP Server Configuration** screen appears.



DHCP Server Configuration

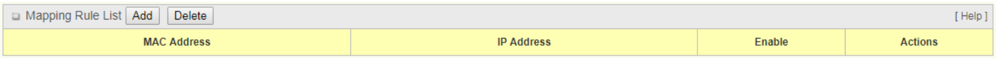
Item	Setting
DHCP Server Name	DHCP 2
LAN IP Address	192.168.2.165
Subnet Mask	255.255.255.0 (/24) ▼
IP Pool	Starting Address: Ending Address:
Lease Time	86400 seconds
Domain Name	(Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)
Server	□ Enable

Figure 3.52 Basic Network > LAN & VLAN > DHCP Server > DHCP Server Configuration

The following table describes the items in the previous figure.

Item	Description
DHCP Server Name	Enter a DHCP server name. Enter a name that is easy for you to understand.
LAN IP Address	The LAN IP Address of this DHCP server.
Subnet Mask	The Subnet Mask of this DHCP server.
IP Pool	The IP Pool of this DHCP server. It composed of **Starting Address** entered in this field and **Ending Address** entered in this field.
Lease Time	The lease time of this DHCP server. Value Range: 300 ~ 604800 seconds.
Domain Name	The domain name of this DHCP server.
Primary DNS	The primary DNS of this DHCP server.
Secondary DNS	The secondary DNS of this DHCP server.
Primary WINS	The primary WINS of this DHCP server.
Secondary WINS	The secondary WINS of this DHCP server.
Gateway	The gateway of this DHCP server.
Server	Click **Enable** checkbox to activate this DHCP server.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.
Back	Click **Back** to return the previous screen.

The gateway allows you to custom your Mapping Rule List on DHCP server. It supports up to a maximum of 64 rule sets. When **Fix Mapping** button is applied, the **Mapping Rule List** screen appears.

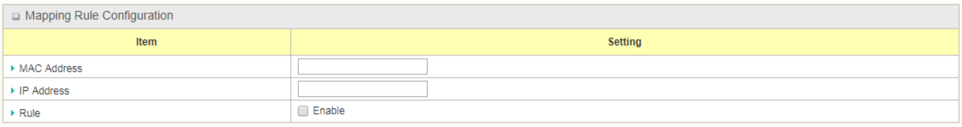


Mapping Rule List | Add | Delete | [Help]

MAC Address	IP Address	Enable	Actions

Figure 3.53 Basic Network > LAN & VLAN > DHCP Server > Mapping Rule List

When **Add** button is applied, the **Mapping Rule Configuration** screen appears.



Mapping Rule Configuration

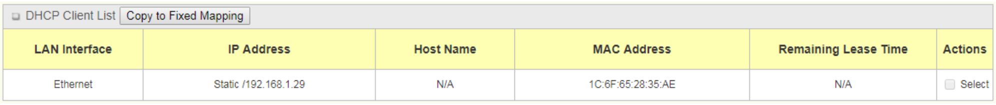
Item	Setting
MAC Address	
IP Address	
Rule	□ Enable

Figure 3.54 Basic Network > LAN & VLAN > DHCP Server > Mapping Rule Configuration

The following table describes the items in the previous figure.

Item	Description
MAC Address	The MAC address of this mapping rule.
IP Address	The IP address of this mapping rule.
Rule	Click **Enable** checkbox to activate this rule.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.
Back	Click **Back** to return the previous screen.

When **DHCP Client List** button is applied, the **DHCP Client List** screen appears.



DHCP Client List Copy to Fixed Mapping

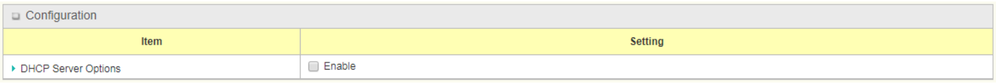
LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time	Actions
Ethernet	Static /192.168.1.29	N/A	1C:6F:65:28:35:AE	N/A	□ Select

Figure 3.55 Basic Network > LAN & VLAN > DHCP Server > DHCP Client List

The following table describes the items in the previous figure.

Item	Description
Copy to Fixed Mapping	Click **Copy to Fixed Mapping**, the IP and MAC address of DHCP Client will apply to the Mapping Rule List on specific DHCP Server automatically.

The DHCP Server Options setting allows user to set DHCP OPTIONS 66, 72, or 114.



Configuration

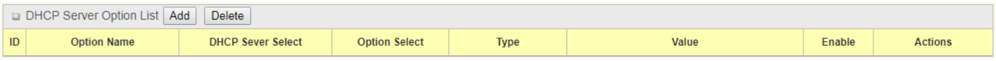
Item	Setting
DHCP Server Options	□ Enable

Figure 3.56 Basic Network > LAN & VLAN > DHCP Server

The following table describes the items in the previous figure.

Item	Description
Enable	Click **Enable** checkbox to activate the DHCP option function, and the DHCP Server will add the expected options in its sending out DHCPOFFER DHCPACK packages.

The gateway supports up to a maximum of 99 option settings.

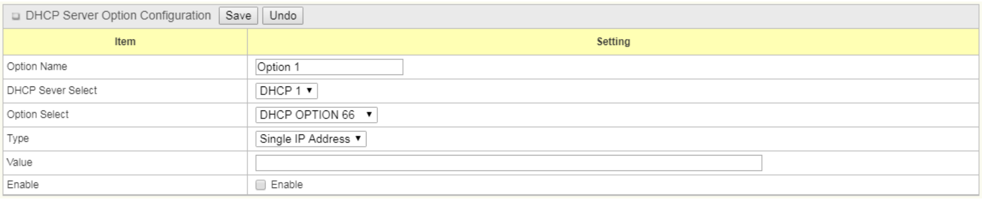


DHCP Server Option List Add Delete

ID	Option Name	DHCP Sever Select	Option Select	Type	Value	Enable	Actions

Figure 3.57 Basic Network > LAN & VLAN > DHCP Server > DHCP Server Option List

When **Add/Edit** button is applied, the **DHCP Server Option Configuration** screen appears.



DHCP Server Option Configuration [Save] [Undo]

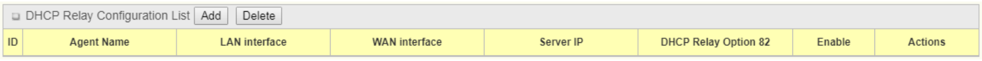
Item	Setting
Option Name	Option 1
DHCP Sever Select	DHCP 1 ▾
Option Select	DHCP OPTION 66 ▾
Type	Single IP Address ▾
Value	
Enable	□ Enable

Figure 3.58 Basic Network > LAN & VLAN > DHCP Server > DHCP Server Option Configuration

The following table describes the items in the previous figure.

Item	Description
Option Name	Enter a DHCP Server Option name. Enter a name that is easy for you to understand.
DHCP Sever Select	Select the DHCP server this option should apply to.
Option Select	Select the specific option from the drop-down menu. It can be **Option 66**, **Option 72**, **Option 144**, **Option 42**, **Option 150**, or **Option 160**. ■ **Option 42** for ntp server. ■ **Option 66** for tftp. ■ **Option 72** for www. ■ **Option 144** for url.
Type	Each different options has different value types. ■ **Option 66:** Single IP Address and Single FQDN ■ **Option 72:** IP Addresses List, separated by “,” ■ **Option 144:** Single URL ■ **Option 42:** IP Addresses List, separated by “,” ■ **Option 150:** IP Addresses List, separated by “,” ■ **Option 160:** Single IP Address and Single FQDN
Value	Should conform to **Type**: ■ **Option 66:** – Single IP Address: IPv4 format – Single FQDN: FQDN format ■ **Option 72:** – IP Addresses List, separated by “,”: IPv4 format, separated by “,” ■ **Option 144:** – Single URL: URL format
Enable	Click **Enable** checkbox to activate this setting.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

The gateway supports up to a maximum of 6 DHCP Relay configurations.

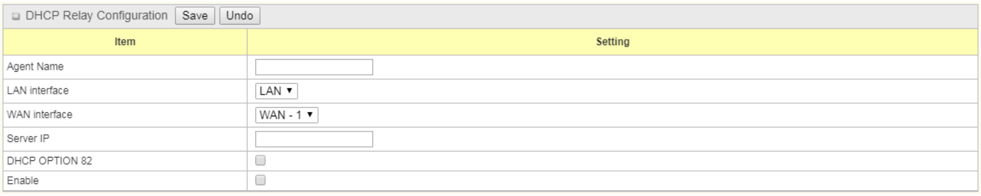


DHCP Relay Configuration List [Add] [Delete]

ID	Agent Name	LAN interface	WAN interface	Server IP	DHCP Relay Option 82	Enable	Actions

Figure 3.59 Basic Network > LAN & VLAN > DHCP Server > DHCP Server Option List

When **Add/Edit** button is applied, the **DHCP Relay Configuration** screen appears.



DHCP Relay Configuration Save Undo

Item	Setting
Agent Name	
LAN interface	LAN ▾
WAN interface	WAN - 1 ▾
Server IP	
DHCP OPTION 82	□
Enable	□

Figure 3.60 Basic Network > LAN & VLAN > DHCP Server > DHCP Relay Configuration List

The following table describes the items in the previous figure.

Item	Description
Agent Name	Enter a DHCP Relay name. Enter a name that is easy for you to understand. Value Range: 1 ~ 64 characters.
LAN interface	Select a LAN Interface for the drop-down menu to apply with the DHCP Relay function.
WAN interface	Select a WAN Interface for the drop-down menu to apply with the DHCP Relay function. It can be the available WAN interface(s), and L2TP connection.
Server IP	Assign a DHCP server IP address that the gateway will relay the DHCP requests to the assigned DHCP server via specified WAN interface.
DHCP OPTION 82	Check to enable the defined DHCP Option 82 function.
Enable	Click **Enable** checkbox to activate this setting.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

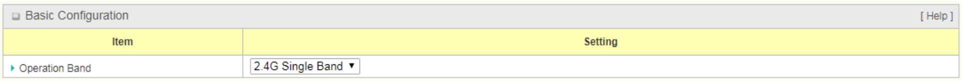
3.3.3 WiFi

3.3.3.1 WiFi Module One/Two

The WiFi configuration allows user to configure 2.4GHz or 5GHz WiFi settings.

Go to **Basic Network** > **WiFi** > **WiFi Module One**. If the gateway is equipped with two WiFi modules, there will be another **WiFi Module Two**. You can do the similar configurations on both WiFi modules.

To access this page, click **Basic Network** > **WiFi** > **WiFi Module One/Two**.



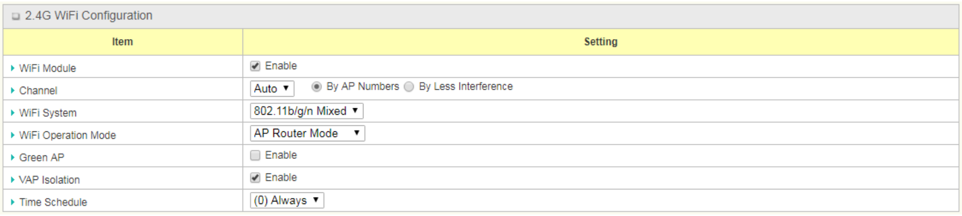
Basic Configuration [Help]

Item	Setting
Operation Band	2.4G Single Band ▾

Figure 3.61 Basic Network > WiFi > WiFi Module One/Two

The following table describes the items in the previous figure.

Item	Description
Operation Band	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the product. However, there is some module with selectable band for user to select according to his network environment. Under such situation, you can specify which operation band is suitable for the application.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



2.4G WiFi Configuration

Item	Setting
WiFi Module	☑ Enable
Channel	Auto ▾ ● By AP Numbers ○ By Less Interference
WiFi System	802.11b/g/n Mixed ▾
WiFi Operation Mode	AP Router Mode ▾
Green AP	□ Enable
VAP Isolation	☑ Enable
Time Schedule	(0) Always ▾

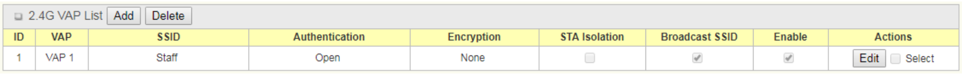
Figure 3.62 Basic Network > WiFi > WiFi Module One/Two > 2.4G WiFi Configuration

The following table describes the items in the previous figure.

Item	Description
WiFi Module	Check **Enable** checkbox to activate WiFi function.
Channel	Select a radio channel for the VAP. Each channel is corresponding to different radio band. The permissible channels depend on the Regulatory Domain. There are two available options when Auto is selected: ■ **By AP Numbers:** The channel will be selected according to AP numbers (The less, the better). ■ **By Less Interference:** The channel will be selected according to interference. (The lower, the better).
WiFi System	Specify the preferred WiFi system. The drop-down menu of WiFi system is based on IEEE 802.11 standard. ■ 2.4G WiFi can select b, g and n only or mixed with each other. ■ 5G WiFi can select a, n and ac only or mixed with each other.

Item	Description
WiFi Operation Mode	Specify the WiFi operation mode according to your application. ***Note:*** *The available operation modes depend on the product specification.*
Lazy Mode	The function is only available when **WiFi Operation Mode** is **WDS Hybird Mode**. Check the **Enable** checkbox to activate this function. With the function been enabled, the device can auto-learn WDS peers without manually entering other AP's MAC address. But at least one of the APs has to fill remote AP MAC addresses.
Green AP	Check **Enable** checkbox to activate Green AP function.
VAP Isolation	Check **Enable** checkbox to activate this function. By default, the box is checked; it means that stations which associated to different VAPs cannot communicate with each other.
Time Schedule	Apply a specific time schedule to this rule; otherwise leave it as **(0) Always**. If the drop-down menu is empty ensure **Time Schedule** is preconfigured. Refer to **Object Definition** > **Scheduling** > **Configuration**.
Scan Remote AP's MAC List	The function is only available when **WiFi Operation Mode** is **WDS Only Mode** or **WDS Hybird Mode**. Click **Scan** to scan the spatial AP information, and then select one from the AP list, the MAC of selected AP will be auto filled in the following remote AP MAC table.
Remote AP MAC 1~4	The function is only available when **WiFi Operation Mode** is **WDS Only Mode** or **WDS Hybird Mode**. Enter the remote AP's MAC manually, or via auto-scan approach, The device will bridge the traffic to the remote AP when associated successfully.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

By default, VAP 1 is enabled and security key is required to connect to the gateway wirelessly to enhance the security level and prevent unexpected access of unauthorized devices.

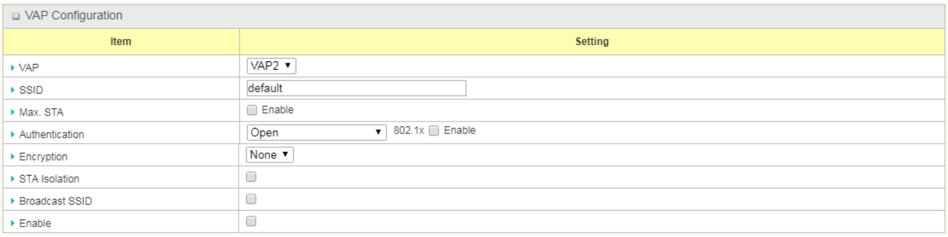


□ 2.4G VAP List Add Delete

ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	Staff	Open	None	□	☑	☑	Edit □ Select

Figure 3.63 Basic Network > WiFi > WiFi Module One/Two > 2.4G VAP List

Click **Add/Edit** button to create or edit the settings for a VAP. The **VAP Configuration** screen appears.



□ VAP Configuration

Item	Setting
VAP	VAP2 ▾
SSID	default
Max. STA	□ Enable
Authentication	Open ▾ 802.1x □ Enable
Encryption	None ▾
STA Isolation	□
Broadcast SSID	□
Enable	□

Figure 3.64 Basic Network > WiFi > WiFi Module One/Two > VAP Configuration

The following table describes the items in the previous figure.

Item	Description
VAP	Click the drop-down menu to select a VAP.

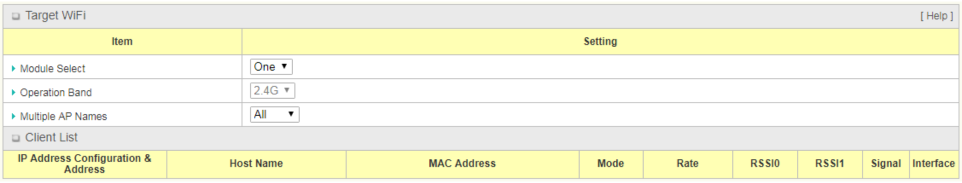
Item	Description
SSID	Enter the SSID for the VAP, and decide whether to broadcast the SSID or not. The SSID is used for identifying from another AP, and client stations will associate with AP according to SSID.
Max. STA	Check this box and enter a limitation to limit the maximum number of client station. The box is unchecked by default. It means no special limitation on the number of connected STAs.
Authentication	For security, there are several authentication methods supported. Client stations should provide the key when associate with this device. ■ When **Open** is selected The check box named 802.1x shows up next to the drop-down menu. – **802.1x** (The box is unchecked by default) When 802.1x is enabled, it means the client stations will be authenticated by RADIUS server. – **RADIUS Server IP** (The default IP is 0.0.0.0) – **RADIUS Server Port** (The default value is 1812) – **RADIUS Shared Key** ■ When **Shared** is selected The pre-shared WEP key should be set for authenticating. ■ When **Auto** is selected The device will select Open or Shared by requesting of client automatically. The check box named 802.1x shows up next to the drop-down menu. – **802.1x** (The box is unchecked by default) When 802.1x is enabled, it means the client stations will be authenticated by RADIUS server. – **RADIUS Server IP** (The default IP is 0.0.0.0) – **RADIUS Server Port** (The default value is 1812) – **RADIUS Shared Key** ■ When **WPA** or **WPA2** is selected They are implementation of IEEE 802.11i. **WPA** only had implemented part of IEEE 802.11i, but owns the better compatibility. **WPA2** had fully implemented 802.11i standard, and owns the highest security. – **RADIUS Server** The client stations will be authenticated by RADIUS server. – **RADIUS Server IP** (The default IP is 0.0.0.0) – **RADIUS Server Port** (The default value is 1812) – **RADIUS Shared Key** ■ When **WPA** / **WPA2** is selected It owns the same setting as **WPA** or **WPA2**. The client stations can associate with this device via **WPA** or **WPA2**. ■ When **WPA-PSK** or **WPA2-PSK** is selected It owns the same encryption system as WPA or WPA2. The authentication uses pre-shared key instead of RADIUS server. ■ When **WPA-PSK** / **WPA2-PSK** is selected It owns the same setting as **WPA-PSK** or **WPA2-PSK**. The client stations can associate with this device via **WPA-PSK** or **WPA2-PSK**.

Item	Description
Encryption	Select a suitable encryption method and enter the required key(s). The available method in the drop-down menu depends on the Authentication you selected. ■ **None:** It means that the device is open system without encrypting. ■ **WEP:** Up to 4 WEP keys can be set, and you have to select one as current key. The key type can set to **HEX** or **ASCII**. If **HEX** is selected, the key should consist of (0 to 9) and (A to F). If **ASCII** is selected, the key should consist of ASCII table. ■ **TKIP:** TKIP was proposed instead of WEP without upgrading hardware. Enter a pre-shared key for it. The length of key is from 8 to 63 characters. ■ **AES:** The newest encryption system in WiFi, it also designed for the fast 802.11n high bitrates schemes. Enter a pre-shared key for it. The length of key is from 8 to 63 characters. You are recommended to use **AES** encryption instead of any others for security. ■ **TKIP / AES:** TKIP / AES mixed mode. It means that the client stations can associate with this device via **TKIP** or **AES**. Enter a pre-shared key for it. The length of key is from 8 to 63 characters.
STA Isolation	Check **Enable** checkbox to activate this function. By default, the box is checked; it means that stations which associated to the same VAP cannot communicate with each other.
Broadcast SSID	Check **Enable** checkbox to activate this function. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with this device by scanning SSID.
Enable	Check **Enable** checkbox to activate this VAP.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.3.3.2 Wireless Client List

To access this page, click **Basic Network** > **WiFi** > **Wireless Client List**.

The **Wireless Client List** screen shows the information of wireless clients which are associated with this device.



Target WiFi

Item	Setting
Module Select	One
Operation Band	2.4G
Multiple AP Names	All

Client List

IP Address Configuration & Address	Host Name	MAC Address	Mode	Rate	RSSI0	RSSI1	Signal	Interface

Figure 3.65 Basic Network > WiFi > Wireless Client List

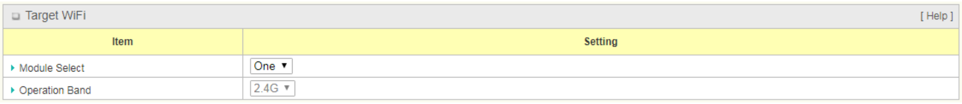
The following table describes the items in the previous figure.

Item	Description
Module Select	Select the WiFi module to check the information of connected clients. For those single WiFi module products, this option is hidden.

Item	Description
Operation Band	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the product. However, there is some module with selectable band for user to select according to his network environment. Under such situation, you can specify which operation band is suitable for the application.
Multiple AP Names	Specify the VAP to show the associated clients information in the following Client List. By default, All VAP is selected.
IP Address Configuration & Address	It shows the Client's IP address and the deriving method. ■ **Dynamic** means the IP address is derived from a DHCP server. ■ **Static** means the IP address is a fixed one that is self-filled by client.
Host Name	It shows the host name of client.
MAC Address	It shows the MAC address of client.
Mode	It shows what kind of WiFi system the client used to associate with this device.
Rate	It shows the data rate between client and this device.
RSSI0	It shows the RX sensitivity (RSSI) value for each radio path.
RSSI1	It shows the RX sensitivity (RSSI) value for each radio path.
Signal	The signal strength between client and this device.
Interface	It shows the VAP ID that the client associated with.
Refresh	Click **Refresh** to shows the information for wireless clients that is associated with the selected VAP(s).

3.3.3.3 Advanced Configuration

To access this page, click **Basic Network** > **WiFi** > **Advanced Configuration**.



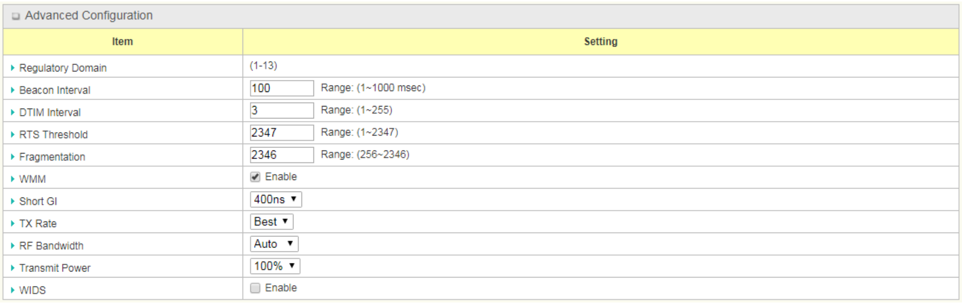
Target WiFi [Help]

Item	Setting
Module Select	One ▾
Operation Band	2.4G ▾

Figure 3.66 Basic Network > WiFi > Advanced Configuration

The following table describes the items in the previous figure.

Item	Description
Module Select	Select the WiFi module to check the information of connected clients. For those single WiFi module products, this option is hidden.
Operation Band	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the product. However, there is some module with selectable band for user to select according to his network environment.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



Advanced Configuration

Item	Setting
Regulatory Domain	(1-13)
Beacon Interval	100 Range: (1~1000 msec)
DTIM Interval	3 Range: (1~255)
RTS Threshold	2347 Range: (1~2347)
Fragmentation	2346 Range: (256~2346)
WMM	☑ Enable
Short GI	400ns ▾
TX Rate	Best ▾
RF Bandwidth	Auto ▾
Transmit Power	100% ▾
WIDS	□ Enable

Figure 3.67 Basic Network > WiFi > Advanced Configuration > Advanced Configuration

The following table describes the items in the previous figure.

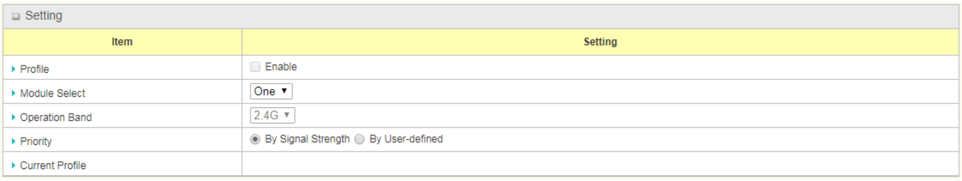
Item	Description
Regulatory Domain	It limits the available radio channel of this device. The permissible channels depend on the **Regulatory Domain**.
Beacon Interval	It shows the time interval between each beacon packet broadcasted. The beacon packet contains **SSID**, **Channel ID** and **Security setting**.
DTIM Interval	A Delivery Traffic Indication Message (DTIM) is a countdown informing clients of the next window for listening to broadcast message. When the device has buffered broadcast message for associated client, it sends the next DTIM with a DTIM value.
RTS Threshold	Request to Send (RTS) Threshold means when the packet size is over the setting value, then active RTS technique. RTS/CTS is a collision avoidance technique. It means RTS never activated when the threshold is set to 2347.
Fragmentation	Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference at the limits of RF coverage.
WMM	WiFi Multimedia (WMM) can help control latency and jitter when transmitting multimedia content over a wireless connection.
Short GI	Short Guard Interval (GI) is defined to set the sending interval between each packet. Note that lower Short GI could increase not only the transition rate but also error rate.
TX Rate	It means the data transition rate. When Best is selected, the device will select a proper data rate according to signal strength.
RF Bandwidth	The setting of RF bandwidth limits the maximum data rate.
Transmit Power	Normally the wireless transmitter operates at 100% power. By setting the transmit power to control the WiFi coverage.
5G Band Steering	When the client station associate with 2.4G WiFi, the device will send the client to 5G WiFi automatically if the client is available on accessing this 5G WiFi band. This option is only available on the module that supports 5GHz band.
WIDS	The WIDS (Wireless Intrusion Detection System) will analyze all packets and make a statistic table in WiFi status. Go to **Status** > **Basic Network** > **WiFi** for detailed WIDS status.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.3.3.4 Uplink Profile

This device provides WiFi Uplink function for connecting to a wireless access point just like connected to a wired WAN or cellular WAN connection. It can operate as a NAT gateway and link the devices wirelessly to the uplink network or hosts.

To connect to the wireless access point, user has to enable the wireless Uplink function for a certain WiFi module (refer to **Basic Network** > **WAN & Uplink** > **Physical Interface**, **Internet Setup**) first, and then configure the Uplink profile(s) for the access point to be connected to in the Uplink Profile page.

To access this page, click **Basic Network** > **WiFi** > **Uplink Profile**.



Setting

Item	Setting
Profile	□ Enable
Module Select	One ▾
Operation Band	2.4G ▾
Priority	● By Signal Strength ○ By User-defined
Current Profile	

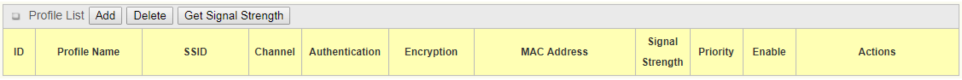
Figure 3.68 Basic Network > WiFi > Uplink Profile

The following table describes the items in the previous figure.

Item	Description
Profile	Check **Enable** checkbox to activate the profile function. It is available only when the selected WiFi module is configured at WiFi Uplink mode.
Module Select	Select the WiFi module to check or configure the expected uplink profile(s). For those single WiFi module products, this option is hidden.
Operation Band	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the gateway product. However, there are some module with selectable band for user to select according to his network environment. Under such situation, you can specify which operation band is suitable for the application.
Priority	Specify the network selection methodology for connection to an available wireless uplink network. It can be **By Signal Strength** or **By User-defined** priority. ■ When **By Signal Strength** is selected, the gateway will try to connect to the available uplink network whose wireless signal strength is the strongest. ■ When **By User-defined** is selected, the gateway will try to connect to the available uplink network whose priority is the highest (1 is the highest priority, and 16 is the lowest priority).
Current Profile	Displays the current profile.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

Note! *To apply the defined uplink profile(s) for the gateway to find a best fit profile for connecting to a certain uplink network, user has to enable the profile auto-connect function (Refer to **Basic Network** > **WiFi** > **(Module 1/ Module 2) WiFi Configuration**.*

The **Profile List** shows the settings for the created uplink profiles. The information includes Profile Name, SSID, Channel, Authentication, Encryption, MAC Address, Signal Strength, Priority, and Enable.

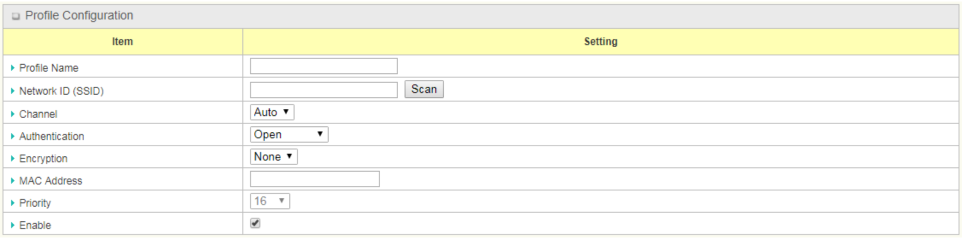


Profile List [Add] [Delete] [Get Signal Strength]

ID	Profile Name	SSID	Channel	Authentication	Encryption	MAC Address	Signal Strength	Priority	Enable	Actions

Figure 3.69 Basic Network > WiFi > Uplink Profile > Profile List

When **Add** button is applied, the **Profile Configuration** screen appears.



Profile Configuration

Item	Setting
Profile Name	
Network ID (SSID)	[Scan]
Channel	Auto ▾
Authentication	Open ▾
Encryption	None ▾
MAC Address	
Priority	16 ▾
Enable	☑

Figure 3.70 Basic Network > WiFi > Uplink Profile > Profile Configuration

The following table describes the items in the previous figure.

Item	Description
Profile Name	Enter a profile name for the uplink network specified below. It is a name that is easy for you to understand. Value Range: 1 ~ 64 characters.
Network ID (SSID)	Enter the SSID for the VAP, and decide whether to broadcast the SSID or not. The SSID is used for identifying from another AP, and client stations will associate with AP according to SSID. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with this device by scanning SSID.
Channel	Select a radio channel for the VAP. Each channel is corresponding to different radio band. The permissible channels depend on the Regulatory Domain. There are two available options when **Auto** is selected: ■ **By AP Numbers:** The channel will be selected according to AP numbers (The less, the better). ■ **By Less Interference:** The channel will be selected according to interference. (The lower, the better).
Authentication	Specify the authentication method for connecting with the uplink network. It can be **Open**, **Shared**, **WPA-SPK**, or **WPA2-PSK**. ■ When **Open** is selected, the pre-shared WEP key could be set for authentication; ■ When **Shared** is selected, the pre-shared WEP key should be set for authentication; ■ When **WPA-PSK** or **WPA2-PSK** is selected, The the TKIP or AES pre-shared key should be set for authentication.

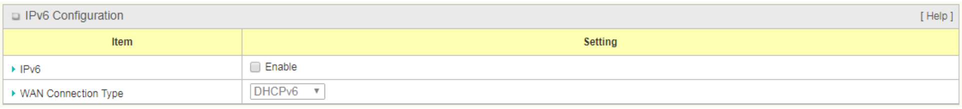
Item	Description
Encryption	Select a suitable encryption method and enter the required key(s). The available method in the drop-down menu depends on the Authentication you selected. ■ **None:** It means that the device is open system without encrypting. ■ **WEP:** Up to 4 WEP keys can be set, and you have to select one as current key. The key type can set to **HEX** or **ASCII**. If **HEX** is selected, the key should consist of (0 to 9) and (A to F). If **ASCII** is selected, the key should consist of ASCII table. ■ **TKIP:** TKIP was proposed instead of WEP without upgrading hardware. Enter a pre-shared key for it. The length of key is from 8 to 63 characters. ■ **AES:** The newest encryption system in WiFi, it also designed for the fast 802.11n high bitrates schemes. Enter a pre-shared key for it. The length of key is from 8 to 63 characters. You are recommended to use AES encryption instead of any others for security.
MAC Address	Specify the MAC address of the access point (with the network ID) to be connected to.
Priority	Specify a priority setting for the uplink profile when the **By User-defined** methodology is selected. The priority value can be 1 ~ 16. 1 is the highest priority, and 16 is the lowest priority).
Enable	Click the **Enable** checkbox to activate this profile.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.
Back	Click **Back** to return the previous screen.

3.3.4 IPv6

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP). It is designed to succeed the Internet Protocol version 4 (IPv4). The Internet operates by transferring data between hosts in small packets that are independently routed across networks as specified by an international communications protocol known as the Internet Protocol.

3.3.4.1 Configuration

To access this page, click **Basic Network** > **IPv6** > **Configuration**.



IPv6 Configuration [Help]

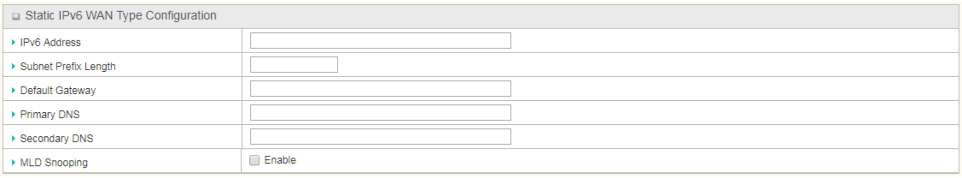
Item	Setting
IPv6	□ Enable
WAN Connection Type	DHCPv6 ▼

Figure 3.71 Basic Network > IPv6 > Configuration

The following table describes the items in the previous figure.

Item	Description
IPv6	Check **Enable** checkbox to activate the IPv6 function.

Item	Description
WAN Connection Type	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity. ■ Select **Static IPv6** when your ISP provides you with a set IPv6 addresses. Then go to Static IPv6 WAN Type Configuration. ■ Select **DHCPv6** when your ISP provides you with DHCPv6 services. ■ Select **PPPoEv6** when your ISP provides you with PPPoEv6 account settings. ■ Select **IPv6** when you want to use IPv6 connection. ***Note:*** *For the products just having 3G/4G WAN interface, only* ***IPv6*** *is supported.*
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



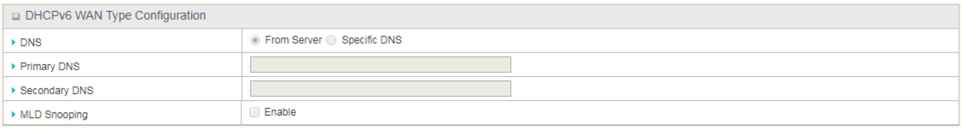
Static IPv6 WAN Type Configuration

IPv6 Address	
Subnet Prefix Length	
Default Gateway	
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

Figure 3.72 Basic Network > IPv6 > Configuration > Static IPv6 WAN Type Configuration

The following table describes the items in the previous figure.

Item	Description
IPv6 Address	Enter the WAN IPv6 address for the router.
Subnet Prefix Length	Enter the WAN subnet prefix Length for the router.
Default Gateway	Enter the WAN default gateway IPv6 address.
Primary DNS	Enter the WAN primary DNS server.
Secondary DNS	Enter the WAN secondary DNS server.
MLD Snooping	Enable/disable the MLD snooping function.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



DHCPv6 WAN Type Configuration

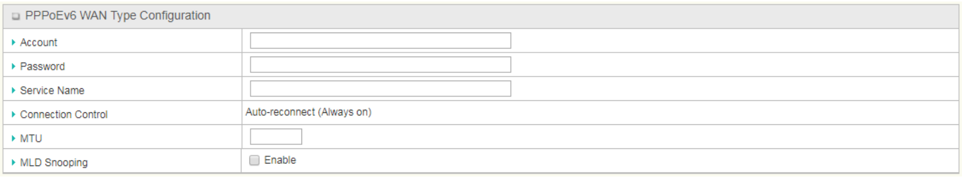
DNS	● From Server ○ Specific DNS
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

Figure 3.73 Basic Network > IPv6 > Configuration > DHCPv6 WAN Type Configuration

The following table describes the items in the previous figure.

Item	Description
DNS	Select **Specific DNS** to active primary DNS and secondary DNS. Then fill the DNS information.
Primary DNS	Enter the WAN primary DNS server.
Secondary DNS	Enter the WAN secondary DNS server.

Item	Description
MLD Snooping	Enable/disable the MLD snooping function.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



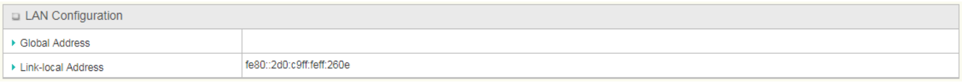
PPPoEv6 WAN Type Configuration

Account	
Password	
Service Name	
Connection Control	Auto-reconnect (Always on)
MTU	
MLD Snooping	□ Enable

Figure 3.74 Basic Network > IPv6 > Configuration > PPPoEv6 WAN Type Configuration

The following table describes the items in the previous figure.

Item	Description
Account	Enter the account for setting up PPPoEv6 connection. If you want more information, please contact your ISP. Value Range: 0 ~ 45 characters.
Password	Enter the password for setting up PPPoEv6 connection. If you want more information, please contact your ISP.
Service Name	Enter the service name for setting up PPPoEv6 connection. If you want more information, please contact your ISP. Value Range: 0 ~ 45 characters.
Connection Control	The value is Auto-reconnect (Always on).
MTU	Enter the MTU for setting up PPPoEv6 connection. If you want more information, please contact your ISP. Value Range: 1280 ~ 1492.
MLD Snooping	Enable/disable the MLD snooping function.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



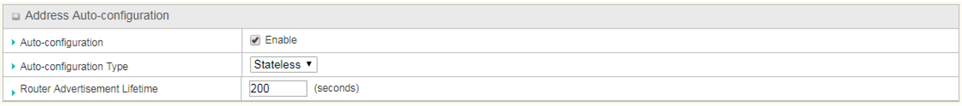
LAN Configuration

Global Address	
Link-local Address	fe80::2d0:c9ff:feff:260e

Figure 3.75 Basic Network > IPv6 > Configuration > LAN Configuration

The following table describes the items in the previous figure.

Item	Description
Global Address	Enter the LAN IPv6 address for the router.
Link-local Address	Show the link-local address for LAN interface of router.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



Address Auto-configuration

Auto-configuration	☑ Enable
Auto-configuration Type	Stateless ▾
Router Advertisement Lifetime	200 (seconds)

Figure 3.76 Basic Network > IPv6 > Configuration > Address Auto-configuration

The following table describes the items in the previous figure.

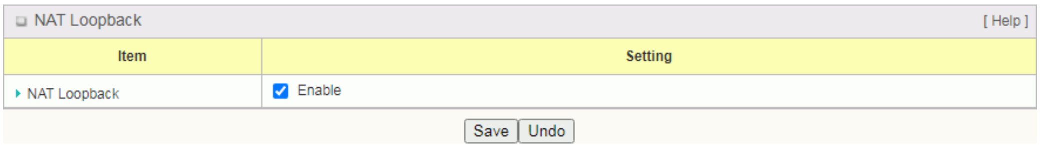
Item	Description
Auto-configuration	Check to enable the auto configuration feature.
Auto-configuration Type	Define the selected IPv6 WAN connection type to establish the IPv6 connectivity. ■ Select **Stateless** to manage the Local Area Network to be SLAAC + RDNSS. ■ Select **Stateful** to manage the Local Area Network to be Stateful (DHCPv6).
Router Advertisement Lifetime	The function is available when **Auto-configuration Type** is **Stateless**. Enter the Router Advertisement Lifetime (in seconds). 200 is set by default. Value Range: 0 ~ 65535.
IPv6 Address Range(Start)	The function is available when **Auto-configuration Type** is **Stateful**. Enter the start IPv6 address for the DHCPv6 range for your local computers. 0100 is set by default. Value Range: 0001 ~ FFFF.
IPv6 Address Range(End)	The function is available when **Auto-configuration Type** is **Stateful**. Enter the end IPv6 address for the DHCPv6 range for your local computers. 0200 is set by default. Value Range: 0001 ~ FFFF.
IPv6 Address Lifetime	The function is available when **Auto-configuration Type** is **Stateful**. Enter the DHCPv6 lifetime for your local computers. 36000 is set by default. Value Range: 0 ~ 65535.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.3.5 Port Forwarding

3.3.5.1 Configuration

Allow you to access the external IP address from inside your home or office network. This is useful when you run a server inside your network.

To access this page, click **Basic Network** > **IPv6** > **Configuration**.



Item	Setting
NAT Loopback	☑ Enable

Figure 3.77 Basic Network > Port Forwarding > Configuration

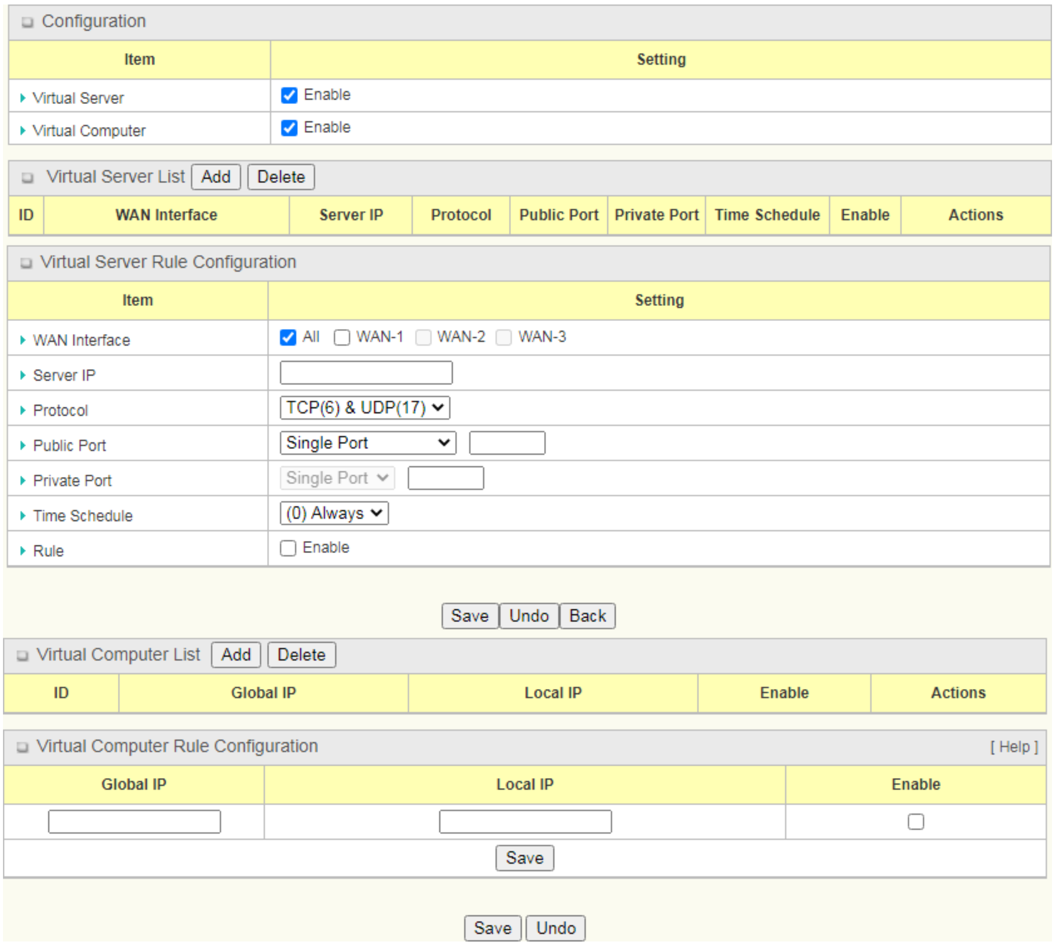
The following table describes the items in the previous figure.

Item	Description
NAT Loopback	Click the radio-button to enable or disable the NAT Loopback function.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.3.5.2 Virtual Server & Virtual Computer

To access this page, click **Basic Network** > **Port Forwarding** > **Virtual Server & Virtual Computer**.

Note! *The following figure was modified to incorporate all menu aspects for easier instruction.*



Configuration

Item	Setting
Virtual Server	☑ Enable
Virtual Computer	☑ Enable

Virtual Server List [Add] [Delete]

ID	WAN Interface	Server IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions

Virtual Server Rule Configuration

Item	Setting
WAN Interface	☑ All ☐ WAN-1 ☐ WAN-2 ☐ WAN-3
Server IP	
Protocol	TCP(6) & UDP(17)
Public Port	Single Port
Private Port	Single Port
Time Schedule	(0) Always
Rule	☐ Enable

[Save] [Undo] [Back]

Virtual Computer List [Add] [Delete]

ID	Global IP	Local IP	Enable	Actions

Virtual Computer Rule Configuration [Help]

Global IP	Local IP	Enable
		☐

[Save]

[Save] [Undo]

Figure 3.78 Basic Network > Port Forwarding > Virtual Server & Virtual computer

The following table describes the items in the previous figure.

Item	Description
Configuration	
Virtual Server	Click the radio button to enable or disable the Virtual Server option.
Virtual Computer	Click the radio button to enable or disable the Virtual Computer option.
Virtual Server List	
Add	Click **Add** to add a Virtual Server listing.
Delete	Click **Delete** to remove a defined Virtual Server listing.
Virtual Server Rule Configuration	
WAN Interface	Click to select and enable the WAN interface to allow traffic to the port forwarding designation. Settings: ■ All ■ WAN-1 ■ WAN-2 ■ WAN-3

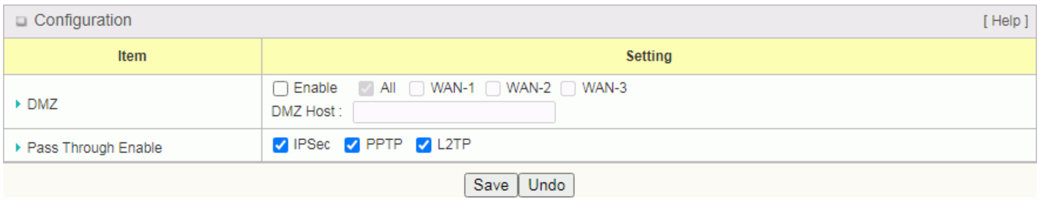
Item	Description
Server IP	Enter the IP address of the virtual server or computer designated as the port forwarding server.
Protocol	Click the drop-down menu to select the protocol for the defined WAN interface. Settings: ■ ICMPv4(1) ■ TCP(6) ■ UDP(17) ■ TCP(6) & UDP(17) (default) ■ GRE(47) ■ ESP(50) ■ SCTP(132) ■ User-defined
Public Port	Click the drop-down menu to select a pre-defined port setting, a specific single port, or a port range. Settings: ■ Well-known Service: FTP (21), SSH (TCP:22), Telnet (23), DNS (53), TFTP (UDP:69), HTTP (TCP:80), POP3 (110), Auth (113), SFTP (TCP:115), SNMP & Traps (UDP:161-162), LDAP (TCP:389), HTTPS (TCP:443), SMTPs (TCP:465), ISAKMP (500), RTSP (TCP:554), POP3s (TCP:995), NetMeeting (1720), L2TP (UDP:1701), PPTP (TCP:1723) ■ Single Port ■ Port Range
Private Port	If Single Port or Port Range is selected in Public Port, a single Port or a Range of Ports can be selected. Enter the Port(s) to define the Private Port. When Well-known Services is selected, the Private Port is already defined.
Time Schedule	Click the drop-down menu to select a specific Time Schedule (0 - Always: Default).
Rule	Click the radio button to enable or disable (default) the Port Forwarding rule.
Save	Click **Save** to save the Rule Configuration settings.
Undo	Click **Undo** to cancel the settings.
Back	Click **Back** to return to the previous menu.
Virtual Computer List	
Add	Click **Add** to add a Virtual Computer listing.
Delete	Click **Delete** to remove a defined Virtual Computer listing.
Global IP	Enter the IP address of the host virtual computer that traffic is addressed to use.
Local IP	Enter the IP address of the NAT-enabled virtual computer to direct the traffic.
Enable	Click to enable or disable the rule configuration.
Save	Click **Save** to save the Rule Configuration settings.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.3.5.3 DMZ & Pass Through

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the

Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries. You can indicate a IP address of certain LAN computer to be a DMZ host.

To access this page, click **Basic Network** > **Port Forwarding** > **DMZ & Pass Through**.



Configuration [Help]

Item	Setting
DMZ	☐ Enable ☑ All ☐ WAN-1 ☐ WAN-2 ☐ WAN-3 DMZ Host :
Pass Through Enable	☑ IPSec ☑ PPTP ☑ L2TP

Figure 3.79 Basic Network > Port Forwarding > DMZ & Pass Through

The following table describes the items in the previous figure.

Item	Description
Configuration	
DMZ	Click Enable to enable or disable the DMZ function. Click the interface to select to set as the DMZ area. Settings: ■ All ■ WAN-1 ■ WAN-2 ■ WAN-3 Enter a string to use as the DMZ host variable for easier identification.
Pass Through Enable	Select the VPN protocol to enable DMZ function to run though to it.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.3.6 Routing

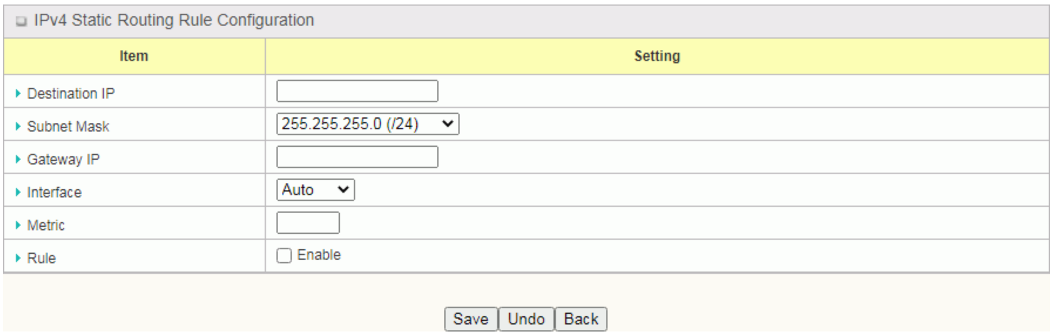
If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other. The routing table allows you to determine which physical interface address to use for outgoing IP data grams.

3.3.6.1 Static Routing

If you have another router with a LAN-to-LAN connection, you may create a static routing on the router that is the gateway to Internet.

Static Routing: For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, Router, and hop for each routing rule, and then enable or disable the rule by checking or un-checking the Enable check box.

To access this page, click **Basic Network** > **Port Forwarding** > **DMZ & Pass Through**.



IPv4 Static Routing Rule Configuration

Item	Setting
Destination IP	
Subnet Mask	255.255.255.0 (/24)
Gateway IP	
Interface	Auto
Metric	
Rule	□ Enable

Figure 3.80 Basic Network > Routing > Static Routing

The following table describes the items in the previous figure.

Item	Description
IPv4 Static Routing Rule Configuration	
Destination IP	Enter the route destination for the destination IP address. For example, you can enter either 10.0.0.0/24 or 10.0.0.0.
Subnet Mask	Enter the destination network mask length for the subnet mask. For example, you can enter either 255.255.255.0.
Gateway IP	Enter the destination IP address length for the gateway address.
Interface	Click the drop-down menu to specify the static interface that a routing host can access to the device. Settings: Auto (default), WAN-1, LAN.
Metric	Enter an integer value to associate with the route. The integer is used to compare static routes to routes from other sources to the same destination.
Rule	Click the radio button to enable or disable the **Rule**.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.
Back	Click **Back** to return the previous screen.

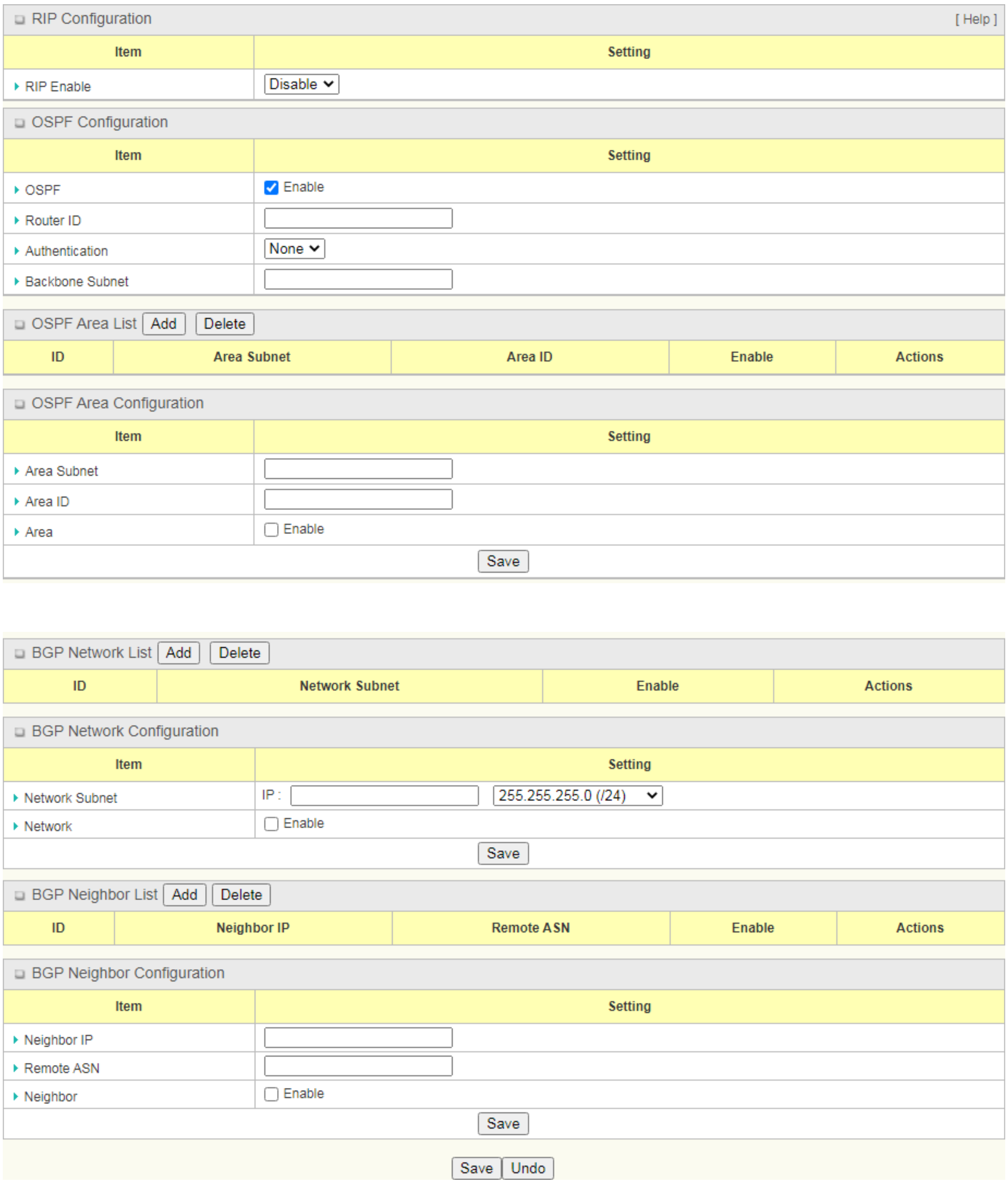
3.3.6.2 Dynamic Routing

Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network.

Select this option to specify the RIP version, including RIP-1, RIP-2. Select RIP2 only if you have different subnets in your network. Otherwise, please select RIPv1.

To access this page, click **Basic Network** > **Routing** > **Dynamic Routing**.

Note! *Due to the length of the Dynamic Routing menu, the following screen has been divided in two parts for easier reading.*



RIP Configuration [Help]

Item	Setting
RIP Enable	Disable

OSPF Configuration

Item	Setting
OSPF	☑ Enable
Router ID	
Authentication	None
Backbone Subnet	

OSPF Area List Add Delete

ID	Area Subnet	Area ID	Enable	Actions

OSPF Area Configuration

Item	Setting
Area Subnet	
Area ID	
Area	□ Enable

Save

BGP Network List Add Delete

ID	Network Subnet	Enable	Actions

BGP Network Configuration

Item	Setting
Network Subnet	IP : 255.255.255.0 (/24)
Network	□ Enable

Save

BGP Neighbor List Add Delete

ID	Neighbor IP	Remote ASN	Enable	Actions

BGP Neighbor Configuration

Item	Setting
Neighbor IP	
Remote ASN	
Neighbor	□ Enable

Save

Save Undo

Figure 3.81 Basic Network > Routing > Dynamic Routing

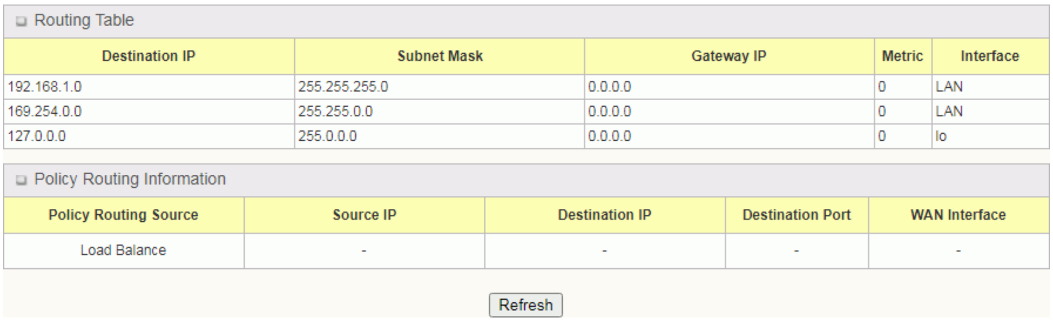
The following table describes the items in the previous figure.

Item	Description
RIP Configuration	
RIP Enable	Click the drop-down menu to select the RIP version. Settings: ■ Disabled ■ RIP-v1: class-based routing version, which does not include subnet information. ■ RIP-v2: broadcasts data throughout the subnet.

Item	Description
OSPF Configuration	
OSPF	Click to enable or disable the OSPF function to advertise interfaces.
Router ID	Enter the router ID to assign.
Authentication	Click to select the RIP v2 authentication parameter. Settings: ■ None ■ Text: input the authentication key to be sent along with the RIPv2 message. ■ MD5: input a unique key ID to create the Authentication Data for this RIP v2 message.
Backbone Subnet	Enter the backbone area (0 or 0.0.0.0) to configure more than one area assignment.
OSPF Area List	
Add	Click **Add** to add an Area List.
Delete	Click **Delete** to delete an Area List.
OSPF Area Configuration	
Area Subnet	Enter the subnet to define an entry.
Area ID	Enter the string to define the area to which the routing will be attached.
Area	Click to enable or disable the Area.
Save	Click **Save** to save the Area Configuration settings.
BGP Configuration	
BGP	Click to enable or disable the BGP routing.
ASN	Enter the autonomous system numbers to assign to the BGP process.
Router ID	Enter the router identifier as AS number.
BGP Network List	
Add	Click **Add** to add a BGP Network listing.
Delete	Click **Delete** to delete a BGP Network listing.
BGP Network Configuration	
Network Subnet	Enter the network subnet to assign as a BGP listing. Click the drop-down menu to assign a subnet.
Network	Click to enable to disable the network configuration.
Save	Click **Save** to save the BGP Configuration settings.
BGP Neighbor List	
Add	Click **Add** to add a BGP Neighbor listing.
Delete	Click **Delete** to delete a BGP Neighbor listing.
Neighbor IP	Enter the IP address of the BGP neighbor listing.
Remote ASN	Enter the autonomous system number of the BGP Neighbor listing.
Neighbor	Click to enable to disable the BGP Neighbor configuration.
Save	Click **Save** to save the BGP Neighbor settings.
Save	Click **Save** to save the Dynamic Routing settings.
Undo	Click **Undo** to cancel the settings.

3.3.6.3 Routing Information

To access this page, click **Basic Network** > **Routing** > **Routing Information**.



Routing Table

Destination IP	Subnet Mask	Gateway IP	Metric	Interface
192.168.1.0	255.255.255.0	0.0.0.0	0	LAN
169.254.0.0	255.255.0.0	0.0.0.0	0	LAN
127.0.0.0	255.0.0.0	0.0.0.0	0	lo

Policy Routing Information

Policy Routing Source	Source IP	Destination IP	Destination Port	WAN Interface
Load Balance	-	-	-	-

Figure 3.82 Basic Network > Routing > Routing Information

The following table describes the items in the previous figure.

Item	Description
Routing Table	
Destination IP	
Subnet Mask	
Gateway IP	Displays the gateway IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
Metric	
Interface	
Policy Routing Information	
Policy Routing Source	
Source IP	
Destination IP	
WAN Interface	Specify the static interface that a routing host can access to the device. Settings: Auto (default), WAN-1, LAN.
Refresh	Click **Refresh** to update the entire VAP traffic statistic instantly.

3.3.7 QoS

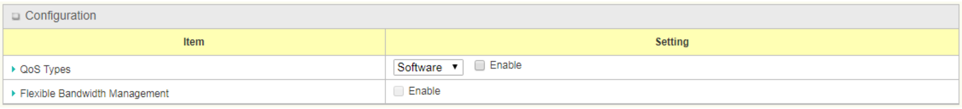
The total amount of data traffic increases nowadays as the higher demand of mobile applications, like Game / Chat / VoIP / P2P / Video / Web access. In order to pose new requirements for data transport, e.g. low latency, low data loss, the entire network must ensure them via a connection service guarantee.

The main goal of QoS (Quality of Service) is prioritizing incoming data, and preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn’t interfere with other data flows. So, QoS helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice packets given higher priority than Web data packets.

To utilize your network throughput completely, administrator must define bandwidth control rules carefully to balance the utilization of network bandwidth for all users to access. It is indeed required that an access gateway satisfies the requirements of latency-critical applications, minimum access right guarantee, fair bandwidth usage for same subscribed condition and flexible bandwidth management. AMIT Security Gateway provides a Rule-based QoS to carry out the requirements.

3.3.7.1 Configuration

To access this page, click **Basic Network** > **QoS** > **Configuration**.



Configuration

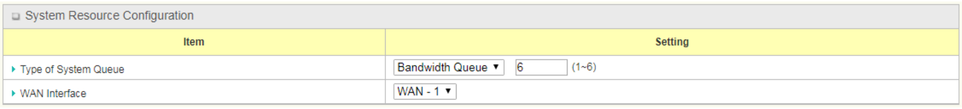
Item	Setting
QoS Types	Software ▾ □ Enable
Flexible Bandwidth Management	□ Enable

Figure 3.83 Basic Network > QoS > Configuration

The following table describes the items in the previous figure.

Item	Description
QoS Types	Select the QoS type from the drop-down menu, and then click **Enable** checkbox to activate the QoS function. The default QoS type is set to **Software** QoS. For some models, there is another option for **Hardware** QoS.
Flexible Bandwidth Management	Click **Enable** checkbox to activate the Flexible Bandwidth Management function.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

Check **Enable** checkbox to activate the **Rule-based QoS** function. Also enable the Flexible Bandwidth Management (FBM) feature when needed. When FBM is enabled, system adjusts the bandwidth distribution dynamically based on current bandwidth usage situation to reach maximum system network performance while transparent to all users. Certainly, the bandwidth subscription profiles of all current users are considered in system's automatic adjusting algorithm.



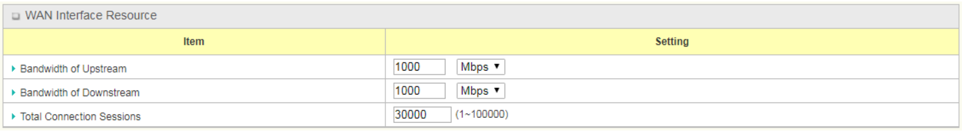
System Resource Configuration

Item	Setting
Type of System Queue	Bandwidth Queue ▾ 6 (1~6)
WAN Interface	WAN - 1 ▾

Figure 3.84 Basic Network > QoS > Configuration > System Resource Configuration

The following table describes the items in the previous figure.

Item	Description
Type of System Queue	Define the system queues that are available for the QoS settings. The supported type of system queues are **Bandwidth Queue** and **Priority Queues**. Value Range: 1 ~ 6.
WAN Interface	Select the WAN interface and then the following WAN Interface Resource screen will show the related resources for configuration.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



WAN Interface Resource

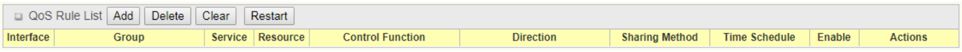
Item	Setting
Bandwidth of Upstream	1000 Mbps ▾
Bandwidth of Downstream	1000 Mbps ▾
Total Connection Sessions	30000 (1~100000)

Figure 3.85 Basic Network > QoS > Configuration > WAN Interface Resource

The following table describes the items in the previous figure.

Item	Description
Bandwidth of Upstream	Specify total upload bandwidth of the selected WAN. Value Range: For Gigabit Ethernet:1 ~ 1024000 Kbps, or 1 ~ 1000 Mbps; For Fast Ethernet: 1 ~ 102400 Kbps, or 1 ~ 100 Mbps; For 3G/4G: 1 ~ 153600 Kbps, or 1 ~ 150 Mbps.
Bandwidth of Downstream	Specify total download bandwidth of the selected WAN. Value Range: For Gigabit Ethernet:1 ~ 1024000 Kbps, or 1 ~ 1000 Mbps; For Fast Ethernet: 1 ~ 102400 Kbps, or 1 ~ 100 Mbps; For 3G/4G: 1 ~ 153600 Kbps, or 1 ~ 150 Mbps.
Total Connection Sessions	Specify total connection sessions of the selected WAN. Value Range: 1 ~ 10000.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

After enabled the QoS function and configured the system resources, you have to further specify some QoS rules for provide better service on the interested traffics. The gateway supports up to a maximum of 128 rule-based QoS rule sets.

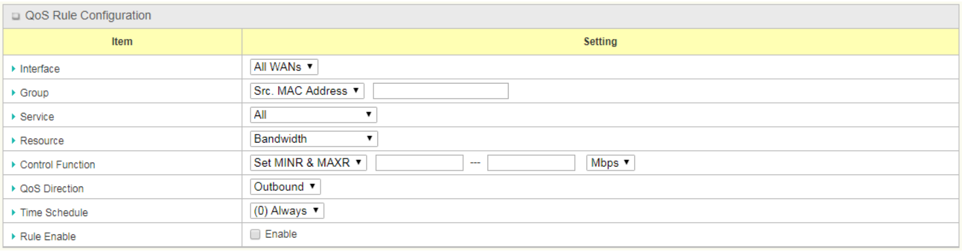


QoS Rule List [Add] [Delete] [Clear] [Restart]

Interface	Group	Service	Resource	Control Function	Direction	Sharing Method	Time Schedule	Enable	Actions

Figure 3.86 Basic Network > QoS > Configuration > QoS Rule List

When **Add** button is applied, the **QoS Rule Configuration** screen appears.



QoS Rule Configuration

Item	Setting
Interface	All WANs ▾
Group	Src. MAC Address ▾ [ ]
Service	All ▾
Resource	Bandwidth ▾
Control Function	Set MINR & MAXR ▾ [ ] ~ [ ] Mbps ▾
QoS Direction	Outbound ▾
Time Schedule	(0) Always ▾
Rule Enable	□ Enable

Figure 3.87 Basic Network > QoS > Configuration > QoS Rule Configuration

The following table describes the items in the previous figure.

Item	Description
Interface	Specify the WAN interface to apply the QoS rule. Select **All WANs** or a certain **WAN-n** to filter the packets entering to or leaving from the interface(s).

Item	Description
Group	Specify the Group category for the QoS rule. It can be **Src. MAC Address**, **IP**, or **Host Name**. ■ Select **Src. MAC Address** to prioritize packets based on MAC. ■ Select **IP** to prioritize packets based on IP address and subnet mask. ■ Select **Host Name** to prioritize packets based on a group of a preconfigured group of host from the drop-down menu. If the drop-down menu is empty, ensure if any group is preconfigured. ***Note:*** *The required host groups must be created in advance and corresponding QoS checkbox in the Multiple Bound Services field is checked before the Host Group option become available. Refer to **Object Definition** > **Grouping** > **Host Grouping**.*
Service	Specify the service type of traffics that have to be applied with the QoS rule. It can be **All**, **DSCP**, **TOS**, **User-defined Service**, or **Well-known Service**. ■ Select **All** for all packets. ■ Select **DSCP** for DSCP type packets only. ■ Select **TOS** for TOS type packets only. You have to select a service type (Minimize-Cost, Maximize-Reliability, Maximize-Throughput, or Minimize-Delay) from the drop-down menu as well. ■ Select **User-defined Service** for user-defined packets only. You have to define the port range and protocol as well. ■ Select **Well-known Service** for specific application packets only. You have to select the required service from the drop-down menu as well.
Resource and Control Function	Specify the Resource Type and corresponding Control function for the QoS rule. The available Resource options are **Bandwidth**, **Connection Sessions**, **Priority Queues**, and **DiffServ Code Points**. ■ **Bandwidth:** Select **Bandwidth** as the resource type for the QoS rule, and you have to assign the min rate, max rate and rate unit as the bandwidth settings in the Control Function / Set MINR & MAXR field. ■ **Connection Sessions:** Select **Connection Sessions** as the resource type for the QoS rule, and you have to assign supported session number in the Control Function / Set Session Limitation field. ■ **Priority Queues:** Select **Priority Queues** as the resource type for the QoS rule, and you have to specify a priority queue in the Control Function / Set Priority field. ■ **DiffServ Code Points:** Select **DiffServ Code Points** as the resource type for the QoS rule, and you have to select a DSCP marking from the Control Function / DSCP Marking drop-down menu.

Item	Description
QoS Direction	Specify the traffic flow direction for the packets to apply the QoS rule. It can be **Outbound**, **Inbound**, or **Both**. ■ **Outbound:** Select **Outbound** to prioritize the traffics going to the Internet via the specified interface. Under such situation, the hosts specified in the Group field is a source group. ■ **Inbound:** Select **Inbound** to prioritize the traffics coming from the Internet via the specified interface. Under such situation, the hosts specified in the Group field is a destination group. ■ **Both:** Select **Both** to prioritize the traffics passing through the specified interface, both Inbound and Outbound are considered. Under such situation, the hosts specified in the Group field can be a source or destination group.
Time Schedule	Apply time schedule to this rule; otherwise leave it as **(0) Always**. (refer to **Object Definition** > **Scheduling** > **Configuration** settings)
Rule Enable	Click **Enable** checkbox to activate this QoS rule.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.
Back	Click **Back** to return the previous screen.

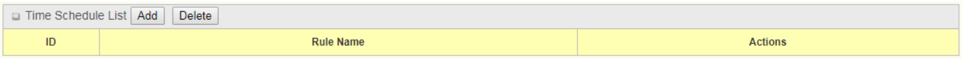
3.4 Object Definition

3.4.1 Scheduling

3.4.1.1 Configuration

To access this page, click **Object Definition** > **Scheduling** > **Configuration**.

The **Scheduling** screen provides ability of adding/deleting time schedule rules, which can be applied to other functionality.



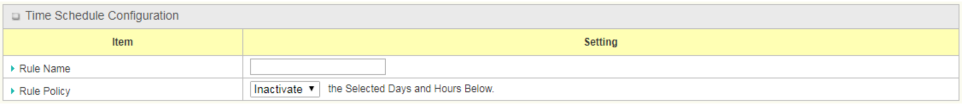
ID	Rule Name	Actions

Figure 3.88 Object Definition > Scheduling > Configuration

The following table describes the items in the previous figure.

Item	Description
Add	Click **Add** to configure time schedule rule.
Delete	Click **Delete** to delete selected rule(s).
Save	Click **Save** to save the settings.
Refresh	Click **Refresh** to refresh the time schedule list.

When **Add** button is applied, the **Time Schedule Configuration** and **Time Period Definition** screens appears.



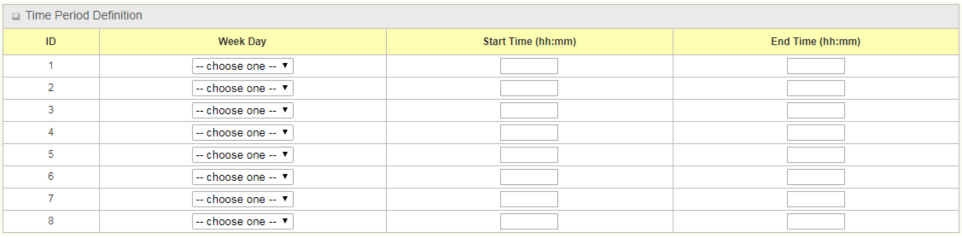
Time Schedule Configuration

Item	Setting
Rule Name	
Rule Policy	Inactivate ▾ the Selected Days and Hours Below.

Figure 3.89 Object Definition > Scheduling > Configuration > Time Schedule Configuration

The following table describes the items in the previous figure.

Item	Description
Rule Name	Set rule name.
Rule Policy	Inactivate/activate the function been applied to in the time period below.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



Time Period Definition

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one --		
2	-- choose one --		
3	-- choose one --		
4	-- choose one --		
5	-- choose one --		
6	-- choose one --		
7	-- choose one --		
8	-- choose one --		

Figure 3.90 Object Definition > Scheduling > Configuration > Time Period Definition

The following table describes the items in the previous figure.

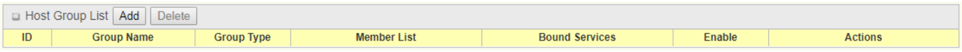
Item	Description
Week Day	Select everyday or one of weekday.
Start Time (hh:mm)	Start time in selected weekday.
End Time (hh:mm)	End time in selected weekday.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.4.2 Grouping

3.4.2.1 Host Grouping

To access this page, click **Object Definition** > **Grouping** > **Host Grouping**.

The **Host Grouping** screen allows user to make host group for some services, such as QoS, Firewall, and Communication Bus. The supported service types could be different for the purchased product.



Host Group List Add Delete

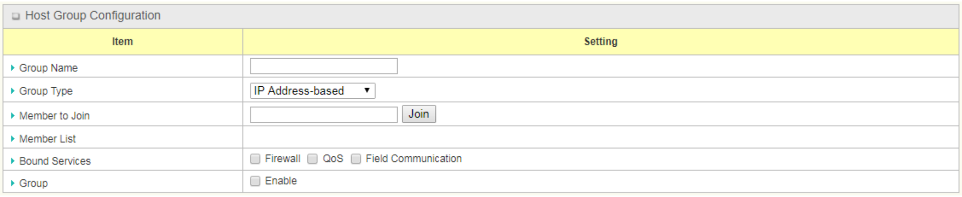
ID	Group Name	Group Type	Member List	Bound Services	Enable	Actions

Figure 3.91 Object Definition > Grouping > Host Grouping

The following table describes the items in the previous figure.

Item	Description
Add	Click **Add** to configure time schedule rule.
Delete	Click **Delete** to delete selected rule(s).
Refresh	Click **Refresh** to refresh the host group list.

When **Add** button is applied, the **Host Group Configuration** screen appears.



Host Group Configuration

Item	Setting
Group Name	
Group Type	IP Address-based ▾
Member to Join	Join
Member List	
Bound Services	□ Firewall □ QoS □ Field Communication
Group	□ Enable

Figure 3.92 Object Definition > Grouping > Host Grouping

The following table describes the items in the previous figure.

Item	Description
Group Name	Enter a group name for the rule. It is a name that is easy for you to understand.
Group Type	Select the group type for the host group. It can be **IP Address-based**, **MAC Address-based**, or **Host Name-based**. ■ When **IP Address-based** is selected, only IP address can be added in **Member to Join**. ■ When **MAC Address-based** is selected, only MAC address can be added in **Member to Join**. ■ When **Host Name-based** is selected, only host name can be added in **Member to Join**. ***Note:*** *The available group type can be different for the purchased model.*
Member to Join	Add the members to the group in this field. You can enter the member information as specified in the **Member Type** above, and click **Join** to add. Only one member can be add at a time, so you have to add the members to the group one by one.
Member List	This field will indicate the hosts (members) contained in the group.

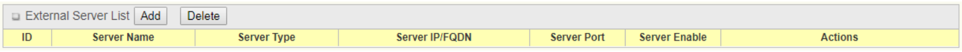
Item	Description
Bound Services	Binding the services that the host group can be applied. If you enable the firewall, the produced group can be used in firewall service. Same as by enable QoS and communication bus. ***Note:*** *The supported service type can be different for the purchased product.*
Group	Check **Enable** checkbox to activate the host group rule. So that the group can be bound to selected service(s) for further configuration.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.4.3 External Server

3.4.3.1 External Server

To access this page, click **Object Definition** > **External Server** > **External Server**.

The **External Server** setting allows user to add external server.



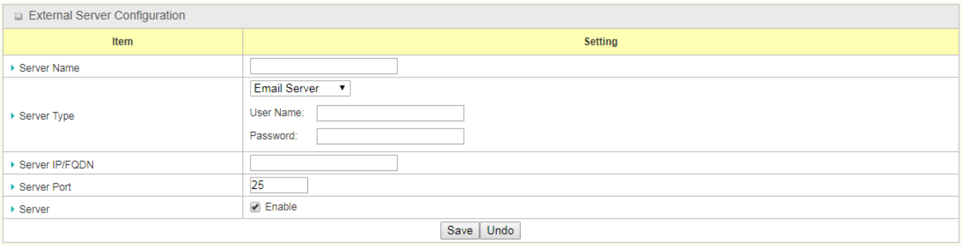
ID	Server Name	Server Type	Server IP/FQDN	Server Port	Server Enable	Actions

Figure 3.93 Object Definition > External Server > External Server

The following table describes the items in the previous figure.

Item	Description
Add	Click **Add** to configure external server rule.
Delete	Click **Delete** to delete selected rule(s).
Refresh	Click **Refresh** to refresh the external server list.

When **Add** button is applied, the **External Server Configuration** screen appears.



Item	Setting
Server Name	
Server Type	Email Server ▾ User Name: Password:
Server IP/FQDN	
Server Port	25
Server	☑ Enable

Figure 3.94 Object Definition > External Server > External Server > External Server Configuration

The following table describes the items in the previous figure.

Item	Description
Server Name	Enter a server name. Enter a name that is easy for you to understand.
Server Type	Specify the server type of the external server, and enter the required settings for the accessing the server. ■ **Email Server:** When **Email Server** is selected, User Name, and Password are also required. – **User Name** (String format: any text) – **Password** (String format: any text)

Item	Description
Server Type (Continued)	■ **RADIUS Server:** When **RADIUS Server** is selected, the following settings are also required. – Primary: **Shared Key** (String format: any text) **Authentication Protocol** (By default CHAP is selected) **Session Timeout** (By default 1): The values must be between 1 and 60. **Idle Timeout** (By default 1): The values must be between 1 and 15. – Secondary: **Shared Key** (String format: any text) **Authentication Protocol** (By default CHAP is selected) **Session Timeout** (By default 1): The values must be between 1 and 60. **Idle Timeout** (By default 1): The values must be between 1 and 15. ■ **FTP(SFTP) Server:** When **FTP(SFTP) Server** is selected, the following settings are also required. – **User Name** (String format: any text) – **Password** (String format: any text) – **Protocol** (Select FTP or SFTP) – **Encryption** (Select Plain, Explicit FTPS or Implicit FTPS) **Transfer mode** (Select Passive or Active)
Server IP/FQDN	Specify the IP address or FQDN used for the external server.
Server Port	Specify the port used for the external server. If you selected a certain server type, the default server port number will be set. ■ For **Email Server** 25 will be set by default. ■ For **Syslog Server**, port 514 will be set by default. ■ For **RADIUS Server**, port 1812 will be set by default. ■ For **FTP(SFTP) Server**, port 21 will be set by default. Value Range: 1 ~ 65535.
Authentication Port	The function is only available when **RADIUS Server** is selected as the **Server Type**. Enter the server port for authentication requests (default is 1812).
Accounting Port	The function is only available when **Server Type** is **RADIUS Server**. Specify the accounting port used if you selected external RADIUS server. Value Range: 1 ~ 65535.
Server	Click **Enable** checkbox to activate this external server.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.4.4 Certificate

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are genuine. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner (http://en.wikipedia.org/wiki/Public_key_certificate).

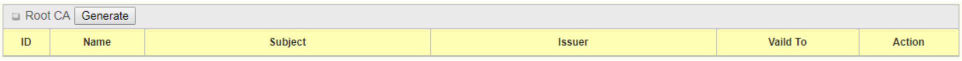
In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company such as VeriSign which charges customers to issue certificates for them. In a web of trust scheme, the signer is either the key's owner (a self-signed certificate) or other users (“endorsements”) whom the person examining the certificate might know and trust. The device also plays as a CA role.

Certificates are an important component of Transport Layer Security (TLS, sometimes called by its older name SSL), where they prevent an attacker from impersonating a secure website or other server. They are also used in other important applications, such as email encryption and code signing. Here, it can be used in IPSec tunneling for user authentication.

3.4.4.1 Configuration

To access this page, click **Object Definition** > **Certificate** > **Configuration**.

The **Configuration** screen allows user to create Root Certificate Authority (CA) certificate and configure to set enable of SCEP. Root CA is the top-most certificate of the tree, the private key of which is used to “sign” other certificates.

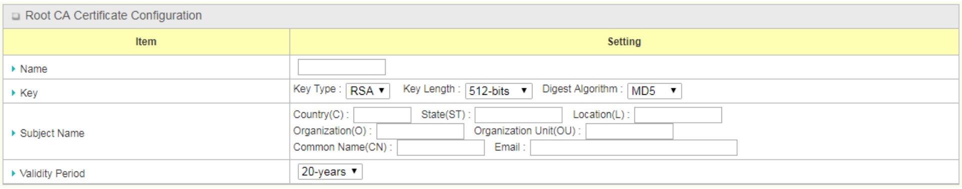


Root CA Generate

ID	Name	Subject	Issuer	Vaild To	Action

Figure 3.95 Object Definition > Certificate > Configuration

When **Generate** button is applied, the **Root CA Certificate Configuration** screen appears. The required information to be filled for the root CA includes the name, key, subject name and validity.



Root CA Certificate Configuration

Item	Setting
Name	
Key	Key Type : RSA ▾ Key Length : 512-bits ▾ Digest Algorithm : MD5 ▾

Subject Name	Country(C) : State(ST) : Location(L) :
	Organization(O) : Organization Unit(OU) :
	Common Name(CN) : Email :

Validity Period	20-years ▾

Figure 3.96 Object Definition > Certificate > Configuration > Root CA Certificate Configuration

The following table describes the items in the previous figure.

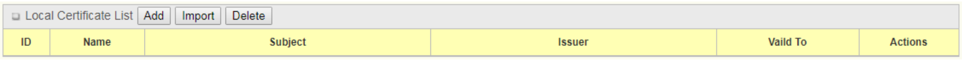
Item	Description
Name	Enter a Root CA certificate name. It will be a certificate file name.
Key	This field is to specify the key attribute of certificate. ■ **Key Type** to set public-key cryptosystems. It only supports RSA now. ■ **Key Length** to set s the size measured in bits of the key used in a cryptographic algorithm. ■ **Digest Algorithm** to set identifier in the signature algorithm identifier of certificates.
Subject Name	This field is to specify the information of certificate. ■ **Country(C)** is the two-letter ISO code for the country where your organization is located. ■ **State(ST)** is the state where your organization is located. ■ **Location(L)** is the location where your organization is located. ■ **Organization(O)** is the name of your organization. ■ **Organization Unit(OU)** is the name of your organization unit. ■ **Common Name(CN)** is the name of your organization. ■ **Email** is the email of your organization. It has to be email address style.
Validity Period	This field is to specify the validity period of certificate.

Item	Description
Save	Click **Save** to save the settings.
Back	Click **Back** to return the previous screen.

3.4.4.2 My Certificate

To access this page, click **Object Definition** > **Certificate** > **My Certificate**.

The **My Certificate** screen allows user to create local certificates. In “My Certificate” page, there are two configuration windows for the “My Certificate” function. The “Local Certificate List” window shows the stored certificates or CSRs for representing the gateway. The “Local Certificate Configuration” window can let you fill required information necessary for corresponding certificate to be generated by itself, or corresponding CSR to be signed by other CAs.

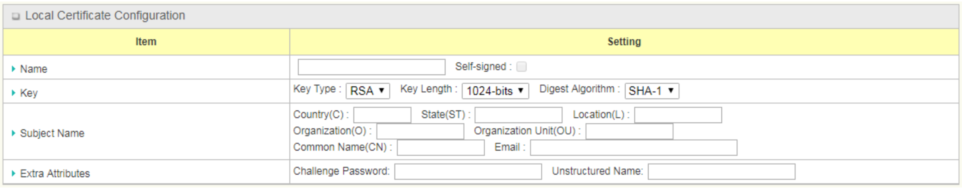


Local Certificate List [Add] [Import] [Delete]

ID	Name	Subject	Issuer	Vaild To	Actions

Figure 3.97 Object Definition > Certificate > My Certificate > Local Certificate Configuration

When **Add** button is applied, the **Local Certificate Configuration** screen appears. The required information to be filled for the certificate or CSR includes the name, key and subject name. It is a certificate if the “Self-signed” box is checked; otherwise, it is a CSR.



Local Certificate Configuration

Item	Setting
Name	Self-signed : □
Key	Key Type : RSA Key Length : 1024-bits Digest Algorithm : SHA-1

Subject Name	Country(C) :
	State(ST) :
	Location(L) :
	Organization(O) :
	Organization Unit(OU) :
	Common Name(CN) :
	Email :

Extra Attributes	Challenge Password: Unstructured Name:

Figure 3.98 Object Definition > Certificate > My Certificate

The following table describes the items in the previous figure.

Item	Description
Name	Enter a certificate name. It will be a certificate file name If **Self-signed** is checked, it will be signed by root CA. If **Self-signed** is not checked, it will generate a certificate signing request (CSR).
Key	This field is to specify the key attributes of certificate. ■ **Key Type** to set public-key cryptosystems. Currently, only RSA is supported. ■ **Key Length** to set the length in bits of the key used in a cryptographic algorithm. It can be 512/768/1024/1536/2048. ■ **Digest Algorithm** to set identifier in the signature algorithm identifier of certificates. It can be MD5/SHA-1.
Subject Name	This field is to specify the information of certificate. ■ **Country(C)** is the two-letter ISO code for the country where your organization is located. ■ **State(ST)** is the state where your organization is located. ■ **Location(L)** is the location where your organization is located. ■ **Organization(O)** is the name of your organization. ■ **Organization Unit(OU)** is the name of your organization unit. ■ **Common Name(CN)** is the name of your organization. ■ **Email** is the email of your organization. It has to be email address setting only.

Item	Description
Extra Attributes	This field is to specify the extra information for generating a certificate. ■ **Challenge Password** for the password you can use to request certificate revocation in the future. ■ **Unstructured Name** for additional information.
Save	Click **Save** to save the settings.
Back	Click **Back** to return the previous screen.

When **Import** button is applied, an Import screen appears. You can import a certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.

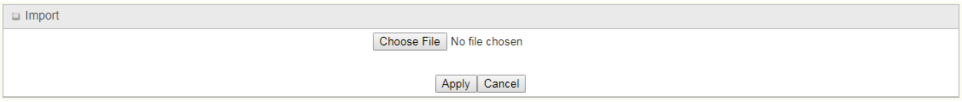


Figure 3.99 Object Definition > Certificate > My Certificate > Import

The following table describes the items in the previous figure.

Item	Description
Choose File	Click **Choose File** to select a certificate file from user's computer.
Apply	Click **Apply** to import the specified certificate file to the gateway.
Cancel	Click **Cancel** to discard the import operation and the screen will return to the My Certificates page.

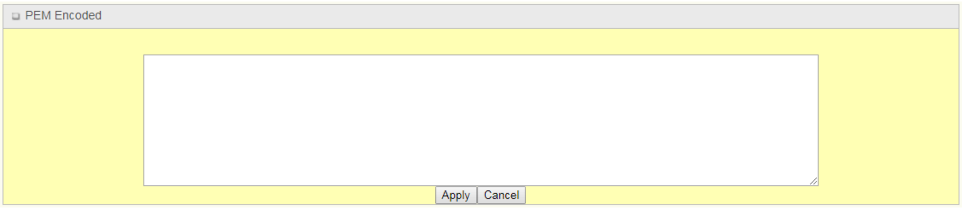


Figure 3.100 Object Definition > Certificate > My Certificate > PEM Encoded

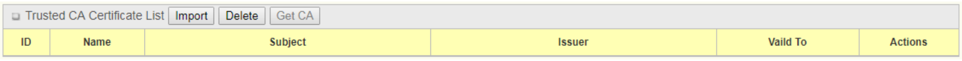
The following table describes the items in the previous figure.

Item	Description
Text filed	This is an alternative approach to import a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string.
Apply	Click **Apply** to import the specified certificate file to the gateway.
Cancel	Click **Cancel** to discard the import operation and the screen will return to the My Certificates page.

3.4.4.3 Trusted Certificate

To access this page, click **Object Definition** > **Certificate** > **Trusted Certificate**.

The **Trusted Certificate** screen allows user to import trusted certificates and keys.



ID	Name	Subject	Issuer	Vaild To	Actions

Figure 3.101 Object Definition > Certificate > Trusted Certificate > Trusted CA Certificate List

When **Import** button is applied, the **Trusted CA Import** screen appears. You can import a Trusted CA certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.

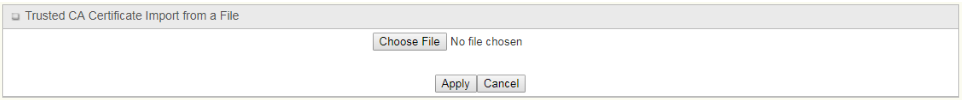


Figure 3.102 Object Definition > Certificate > Trusted Certificate > Trusted CA Certificate Import from a File

The following table describes the items in the previous figure.

Item	Description
Choose File	Click **Choose File** to select a CA certificate file from user's computer.
Apply	Click **Apply** to import the specified CA certificate to the gateway.
Cancel	Click **Cancel** to discard the import operation and the screen will return to the **Trusted Certificates** page.

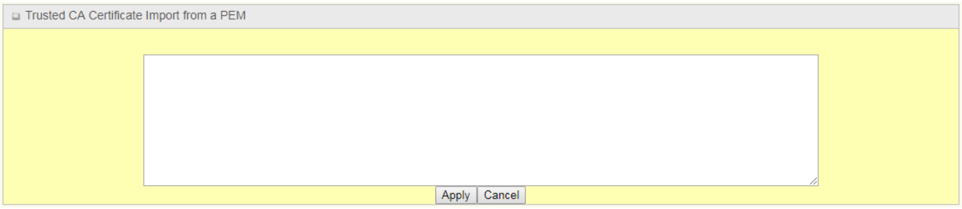
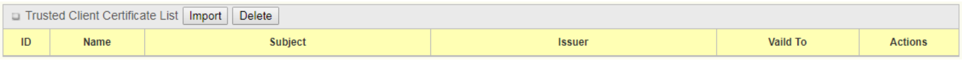


Figure 3.103 Object Definition > Certificate > Trusted Certificate > Trusted CA Certificate Import from a PEM

The following table describes the items in the previous figure.

Item	Description
Text filed	This is an alternative approach to import a CA certificate. You can directly fill in (Copy and Paste) the PEM encoded CA certificate string.
Apply	Click **Apply** to import the specified CA certificate to the gateway.
Cancel	Click **Cancel** to discard the import operation and the screen will return to the **Trusted Certificates** page.



ID	Name	Subject	Issuer	Vaild To	Actions

Figure 3.104 Object Definition > Certificate > Trusted Certificate > Trusted Client Certificate List

When **Import** button is applied, the **Trusted Client Certificate Import** screen appears. You can import a Trusted Client Certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.

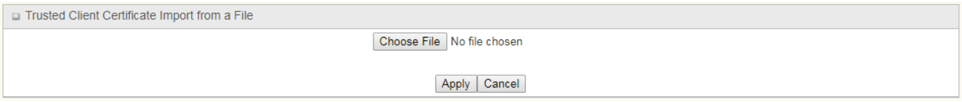


Figure 3.105 Object Definition > Certificate > Trusted Certificate > Trusted Client Certificate Import from a File

The following table describes the items in the previous figure.

Item	Description
Choose File	Click **Choose File** to select a certificate file from user's computer.
Apply	Click **Apply** to import the specified certificate to the gateway.
Cancel	Click **Cancel** to discard the import operation and the screen will return to the **Trusted Certificates** page.

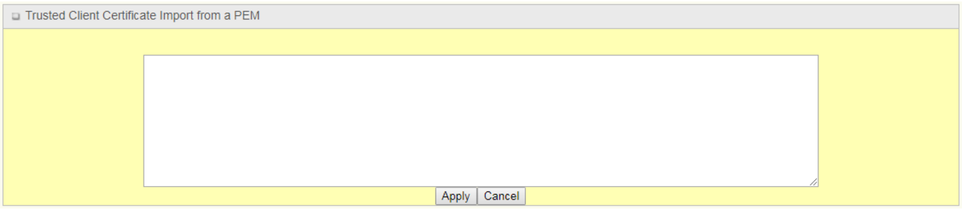


Figure 3.106 Object Definition > Certificate > Trusted Certificate > Trusted Client Certificate Import from a PEM

The following table describes the items in the previous figure.

Item	Description
Text filed	This is an alternative approach to import a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string.
Apply	Click **Apply** to import the specified certificate to the gateway.
Cancel	Click **Cancel** to discard the import operation and the screen will return to the **Trusted Certificates** page.

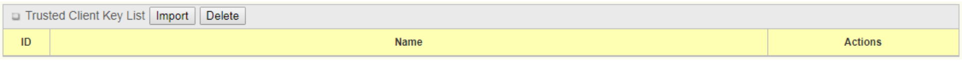


Figure 3.107 Object Definition > Certificate > Trusted Certificate > Trusted Client Key List

When **Import** button is applied, the **Trusted Client Key Import** screen appears. You can import a Trusted Client Key from an existed file, or directly paste a PEM encoded string as the key.

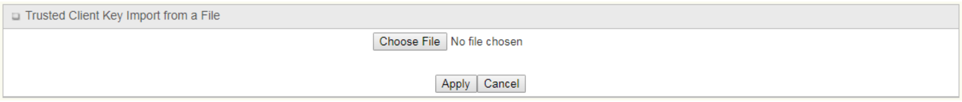


Figure 3.108 Object Definition > Certificate > Trusted Certificate > Trusted Client Key Import from a File

The following table describes the items in the previous figure.

Item	Description
Choose File	Click **Choose File** to select a certificate key file from user's computer.
Apply	Click **Apply** to import the specified certificate key to the gateway.
Cancel	Click **Cancel** to discard the import operation and the screen will return to the **Trusted Certificates** page.

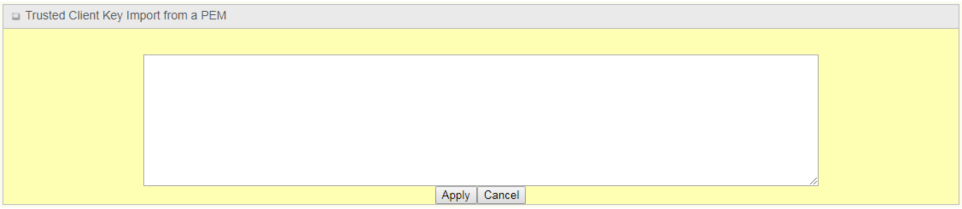


Figure 3.109 Object Definition > Certificate > Trusted Certificate > Trusted Client Key Import from a PEM

The following table describes the items in the previous figure.

Item	Description
Text filed	This is an alternative approach to import a certificate key. You can directly fill in (Copy and Paste) the PEM encoded certificate key string.
Apply	Click **Apply** to import the specified certificate key to the gateway.
Cancel	Click **Cancel** to discard the import operation and the screen will return to the **Trusted Certificates** page.

3.4.4.4 Issued Certificate

To access this page, click **Object Definition** > **Certificate** > **Issued Certificate**.

The **Issue Certificate** screen allows user to import Certificate Signing Request (CSR) to be signed by root CA.

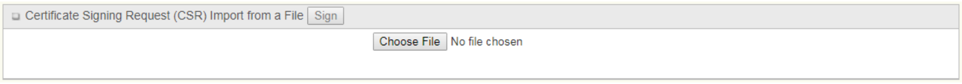


Figure 3.110 Object Definition > Certificate > Issued Certificate > Certificate Signing Request (CSR) Import from a File

The following table describes the items in the previous figure.

Item	Description
Sign	When root CA is exist, click **Sign** sign and issue the imported certificate by root CA.
Choose File	Click **Choose File** to select a certificate signing request file you're your computer for importing to the gateway.

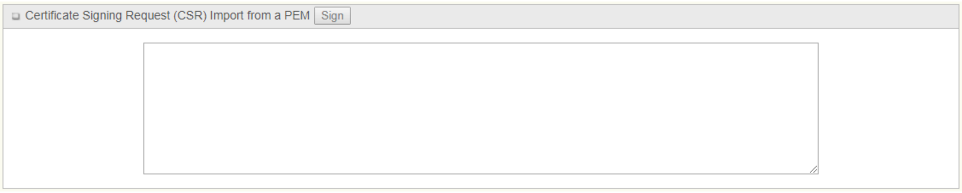


Figure 3.111 Object Definition > Certificate > Issued Certificate > Certificate Signing Request (CSR) Import from a PEM

The following table describes the items in the previous figure.

Item	Description
Sign	When root CA is exist, click **Sign** sign and issue the imported certificate by root CA.
Text filed	Enter (copy-paste) the certificate signing request PEM encoded certificate to the gateway.

3.5 Field Communication

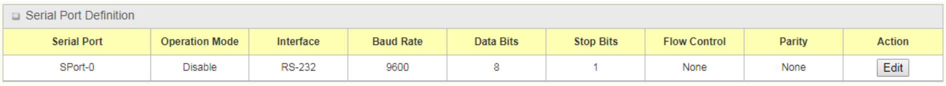
3.5.1 Bus & Protocol

The gateway may equip a serial port for various serial communication use through connecting the RS-232 or RS-485 serial device to an IP-based Ethernet LAN. These communication protocols make user access serial devices anywhere over a local LAN or the Internet easily. They can be “Virtual COM” and “Modbus”.

3.5.1.1 Port Configuration

To access this page, click **Field Communication** > **Bus & Protocol** > **Port Configuration**.

In **Port Configuration** page, there is only one configuration window for the serial port settings. The **Configuration** window can let you specify serial port parameters including the operation mode being “Virtual COM”, “Modbus” or disabled, the interface being “RS-232” or “RS-485”, the baud rate, the data bit length, the stop bit length, the flow control being “RTS/CTS”, “DTS/DSR” or “None”, and the parity.

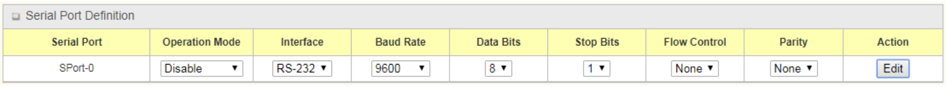


Serial Port Definition

Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Disable	RS-232	9600	8	1	None	None	Edit

Figure 3.112 Field Communication > Bus & Protocol > Port Configuration

When **Edit** button is applied, a screen similar to this appears.



Serial Port Definition

Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Disable ▼	RS-232 ▼	9600 ▼	8 ▼	1 ▼	None ▼	None ▼	Edit

Figure 3.113 Field Communication > Bus & Protocol > Port Configuration

The following table describes the items in the previous figure.

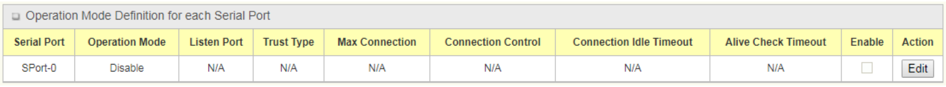
Item	Description
Serial Port	It displays the serial port ID of the serial port. The number of serial ports varies from the purchased model.
Operation Mode	It displays the current selected operation mode for the serial interface. Depending on the purchase model, the available modes can be **Disable**, **Virtual COM** and **Modbus**.
Interface	Select **RS-232** or **RS-485** physical interface for connecting to the access device(s) with the same interface specification.
Baud Rate	Select the appropriate baud rate for serial device communication. ■ **RS-232:** 1200 / 2400 / 4800 / 9600 / 19200 / 38400 / 57600 / 115200 ■ **RS-485** can use higher baud rate for 230400 and 460800. It depends on the cable length and the installed environment. The longer cable, the lower baud rate for it.
Data Bits	Select 8 or 7 for data bits.
Stop Bits	Select 1 or 2 for stop bits.
Flow Control	Select None / RTS, CTS / DTS, DSR for flow control in RS-232 mode. The supporting of flow control depends on the purchased model.
Parity	Select None / Even / Odd for Parity bit.
Action	Click **Edit** to change the operation mode, or modify the parameters mentioned above for the serial interface communication.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.5.1.2 Virtual COM

To use the **Virtual COM** function, you have to specify the operation mode for the multi-function serial port first. Go to **Field Communication** > **Bus & Protocol** > **Port Configuration**, select the Virtual COM as expected operation mode, and finish the related port configuration as well.

To access this page, click **Field Communication** > **Bus & Protocol** > **Virtual COM**.

Configure the gateway as the TCP (Transmission Control Protocol) Client. In TCP Client mode, device initiates a TCP connection with a TCP server when there is data to transmit. Device disconnects from the server when the connection is Idle for a specified period. You may also enable full time connection with the TCP server.

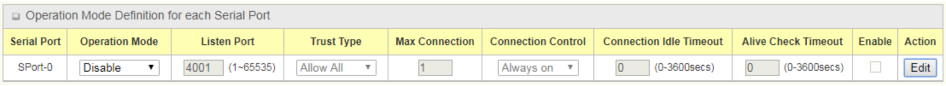


Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	Disable	N/A	N/A	N/A	N/A	N/A	N/A	□	Edit

Figure 3.114 Field Communication > Bus & Protocol > Virtual COM

When **Edit** button is applied, a screen similar to this appears.



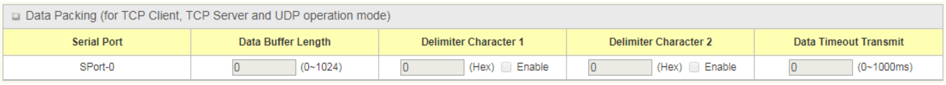
Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	Disable ▾	4001 (1~65535)	Allow All ▾	1	Always on ▾	0 (0-3600secs)	0 (0-3600secs)	□	Edit

Figure 3.115 Field Communication > Bus & Protocol > Virtual COM

The following table describes the items in the previous figure.

Item	Description
Serial Port	It displays the serial port ID of the serial port. The number of serial ports varies from the purchased model.
Operation Mode	Select **TCP Client** mode.
Connection Control	Select **Always on** for a TCP full time connection. Otherwise, select **On-Demand** to initiate TCP connection only when required to transmit and disconnect at idle timeout.
Connection Idle Timeout	Enter the idle timeout in minutes. The idle timeout is used to disconnect the TCP connection when idle time elapsed. Idle timeout is only available when **On-Demand** is selected in the **Connection Control** field. Value Range: 0 ~ 3600 seconds.
Alive Check Timeout	Enter the time period of alive check timeout. The TCP connection will be terminated if it doesn’t receive response of alive-check longer than this timeout setting. Alive check timeout is only available when **On-Demand** is selected in the **Connection Control** field. Value Range: 0 ~ 3600 seconds.
Enable	Check **Enable** checkbox to activate the corresponding serial port in specified operation mode.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



Data Packing (for TCP Client, TCP Server and UDP operation mode)

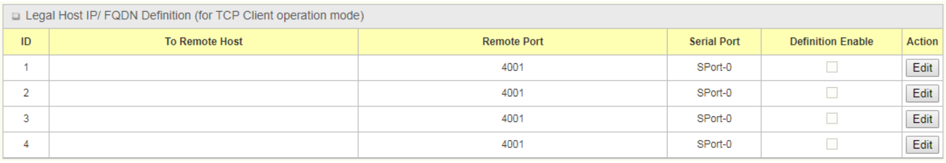
Serial Port	Data Buffer Length	Delimiter Character 1	Delimiter Character 2	Data Timeout Transmit
SPort-0	0 (0~1024)	0 (Hex) □ Enable	0 (Hex) □ Enable	0 (0~1000ms)

Figure 3.116 Field Communication > Bus & Protocol > Virtual COM > Data Packing (for TCP Client, TCP Server and UDP operation mode)

Figure 3.117

The following table describes the items in the previous figure.

Item	Description
Data Buffer Length	Enter the data buffer length for the serial port. Value Range: 0 ~ 1024.
Delimiter Character 1	Check **Enable** checkbox to activate the delimiter character 1, and enter the Hex code for it. Value Range: 0x00 ~ 0xFF.
Delimiter Character 2	Check **Enable** checkbox to activate the delimiter character 2, and enter the Hex code for it. Value Range: 0x00 ~ 0xFF.
Data Timeout Transmit	Enter the data timeout interval for transmitting serial data through the port. By default, it is set to 0 and the timeout function is disabled. Value Range: 0 ~ 1000ms.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

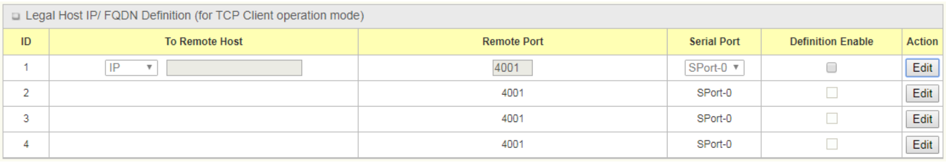


Legal Host IP/ FQDN Definition (for TCP Client operation mode)

ID	To Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	□	Edit
2		4001	SPort-0	□	Edit
3		4001	SPort-0	□	Edit
4		4001	SPort-0	□	Edit

Figure 3.118 Field Communication > Bus & Protocol > Virtual COM > Legal Host IP/FQDN Definition (for TCP Client operation mode)

When **Edit** button is applied, a screen similar to this appears.



Legal Host IP/ FQDN Definition (for TCP Client operation mode)

ID	To Remote Host	Remote Port	Serial Port	Definition Enable	Action
1	IP ▾	4001	SPort-0 ▾	□	Edit
2		4001	SPort-0	□	Edit
3		4001	SPort-0	□	Edit
4		4001	SPort-0	□	Edit

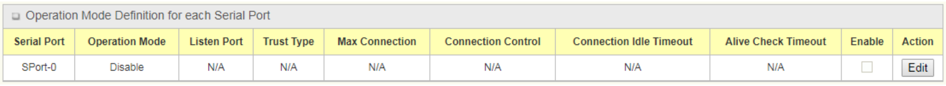
Figure 3.119 Field Communication > Bus & Protocol > Virtual COM > Legal Host IP/FQDN Definition (for TCP Client operation mode)

The following table describes the items in the previous figure.

Item	Description
To Remote Host	Click **Edit** to enter IP address or FQDN of the remote TCP server to transmit serial data.
Remote Port	Enter the TCP port number. This is the listen port of the remote TCP server. Value Range: 1 ~ 65535.
Serial Port	Apply the TCP server connection for a selected serial port. Up to 4 TCP servers can be configured at the same time for each serial port.
Definition Enable	Check **Enable** checkbox to enable the TCP server configuration.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

Configure the gateway as the TCP (Transmission Control Protocol) Server. The TCP Server waits for connections to be initiated by a remote TCP client device to receive serial data. The setting allows user to specify specific TCP clients or allow any to send serial data for serial data transmission bandwidth control and access control.

The TCP Server supports up to 128 simultaneous connections to receive serial data from multiple TCP clients.

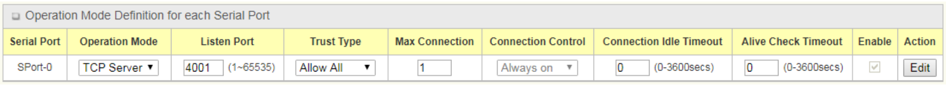


Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	Disable	N/A	N/A	N/A	N/A	N/A	N/A	□	Edit

Figure 3.120 Field Communication > Bus & Protocol > Virtual COM

When **Edit** button is applied, a screen similar to this appears.



Operation Mode Definition for each Serial Port

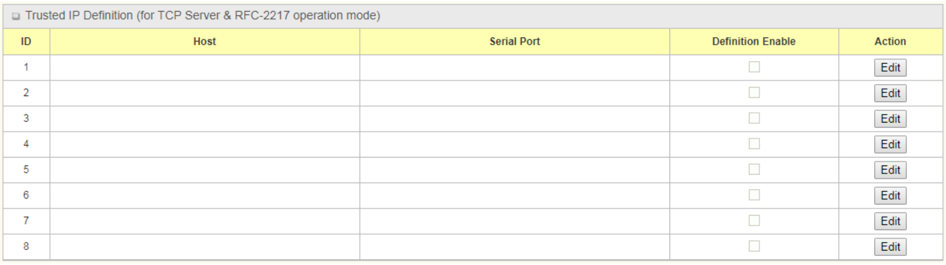
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	TCP Server ▼	4001 (1~65535)	Allow All ▼	1	Always on ▼	0 (0-3600secs)	0 (0-3600secs)	☑	Edit

Figure 3.121 Field Communication > Bus & Protocol > Virtual COM

The following table describes the items in the previous figure.

Item	Description
Serial Port	It displays the serial port ID of the serial port. The number of serial ports varies from the purchased model.
Operation Mode	Select **TCP Server** mode.
Listen Port	Indicate the listening port of TCP connection. Value Range: 1 ~ 65535.
Trust Type	Select **Allow All** to allow any TCP clients to connect. Otherwise select **Specific IPs** to limit certain TCP clients.
Max Connection	Set the maximum number of concurrent TCP connections. Up to 128 simultaneous TCP connections can be established. Value Range: 1 ~ 128.
Connection Idle Timeout	Enter the idle timeout in minutes. The idle timeout is used to disconnect the TCP connection when idle time elapsed. Idle timeout is only available when **On-Demand** is selected in the **Connection Control** field. Value Range: 0 ~ 3600 seconds.
Alive Check Timeout	Enter the time period of alive check timeout. The TCP connection will be terminated if it doesn't receive response of alive-check longer than this timeout setting. Alive check timeout is only available when **On-Demand** is selected in the **Connection Control** field. Value Range: 0 ~ 3600 seconds.
Enable	Check **Enable** checkbox to activate the corresponding serial port in specified operation mode.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

If you selected **Specific IPs** as the **Trust Type**, the **Trusted IP Definition** window appears. The settings are valid for both TCP Server and RFC-2217 modes.

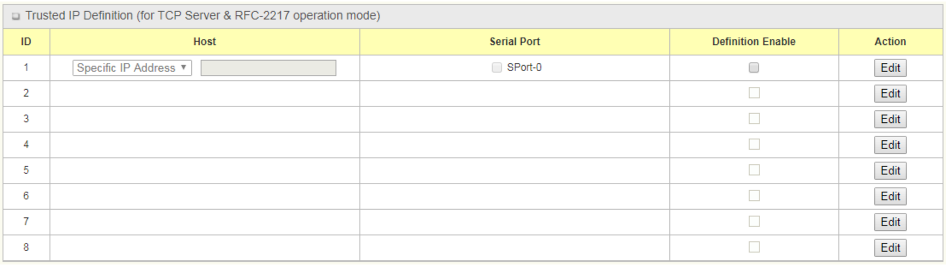


Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

ID	Host	Serial Port	Definition Enable	Action
1			□	Edit
2			□	Edit
3			□	Edit
4			□	Edit
5			□	Edit
6			□	Edit
7			□	Edit
8			□	Edit

Figure 3.122 Field Communication > Bus & Protocol > Virtual COM > Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

When **Edit** button is applied, a screen similar to this appears.



Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

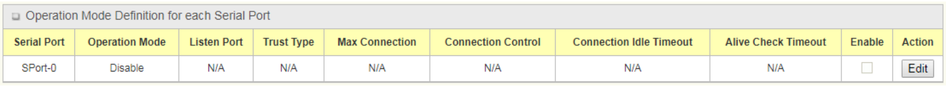
ID	Host	Serial Port	Definition Enable	Action
1	Specific IP Address ▾	☐ SPort-0	☐	Edit
2			☐	Edit
3			☐	Edit
4			☐	Edit
5			☐	Edit
6			☐	Edit
7			☐	Edit
8			☐	Edit

Figure 3.123 Field Communication > Bus & Protocol > Virtual COM > Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

The following table describes the items in the previous figure.

Item	Description
Host	Enter the IP address range of allowed TCP clients.
Serial Port	Check the box to specify the rule for selected serial port.
Definition Enable	Check **Enable** checkbox to enable the rule.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

UDP (User Datagram Protocol) enables applications using UDP socket programs to communicate with the serial ports on the serial server. The UDP mode provides connectionless communications, which enable you to multicast data from the serial device to multiple host computers, and vice versa, making this mode ideal for message display applications.

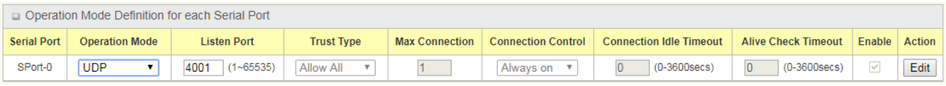


Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	Disable	N/A	N/A	N/A	N/A	N/A	N/A	☐	Edit

Figure 3.124 Field Communication > Bus & Protocol > Virtual COM

When **Edit** button is applied, a screen similar to this appears.



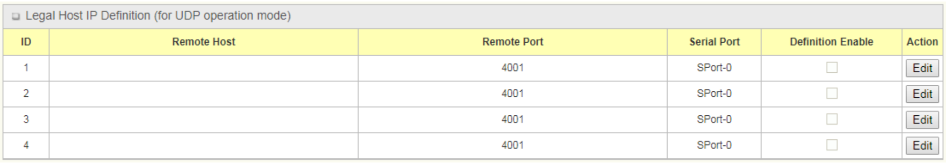
Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	UDP ▾	4001 (1~65535)	Allow All ▾	1	Always on ▾	0 (0-3600secs)	0 (0-3600secs)	☑	Edit

Figure 3.125 Field Communication > Bus & Protocol > Virtual COM

The following table describes the items in the previous figure.

Item	Description
Serial Port	It displays the serial port ID of the serial port. The number of serial ports varies from the purchased model.
Operation Mode	Select **UDP** mode.
Listen Port	Indicate the listening port of UDP connection. Value Range: 1 ~ 65535
Enable	Check **Enable** checkbox to activate the corresponding serial port in specified operation mode.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

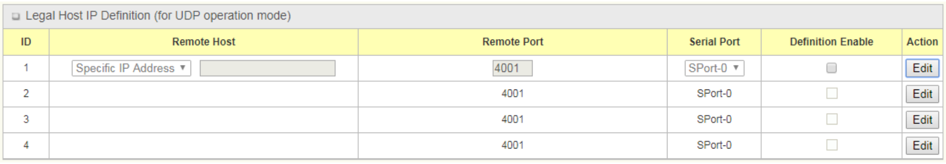


Legal Host IP Definition (for UDP operation mode)

ID	Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	□	Edit
2		4001	SPort-0	□	Edit
3		4001	SPort-0	□	Edit
4		4001	SPort-0	□	Edit

Figure 3.126 Field Communication > Bus & Protocol > Virtual COM > Legal Host IP Definition (for UDP operation mode)

When **Edit** button is applied, a screen similar to this appears.



Legal Host IP Definition (for UDP operation mode)

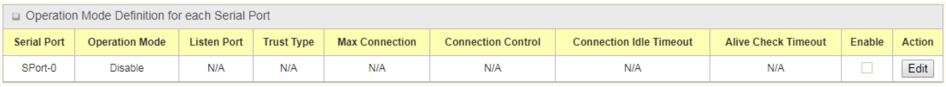
ID	Remote Host	Remote Port	Serial Port	Definition Enable	Action
1	Specific IP Address ▾	4001	SPort-0 ▾	□	Edit
2		4001	SPort-0	□	Edit
3		4001	SPort-0	□	Edit
4		4001	SPort-0	□	Edit

Figure 3.127 Field Communication > Bus & Protocol > Virtual COM

The following table describes the items in the previous figure.

Item	Description
Remote Host	Press **Edit** button to enter IP address range of remote UDP hosts.
Remote Port	Indicate the UDP port of peer UDP hosts. Value Range: 1 ~ 65535
Serial Port	Apply the UDP hosts for a selected serial port. Up to 4 UDP servers can be configured at the same time for each serial port.
Definition Enable	Check **Enable** checkbox to enable the rule.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

RFC-2217 defines general COM port control options based on telnet protocol. With the RFC-2217 mode, remote host can monitor and manage remote serially attached devices, as though they were connected to the local serial port. When a virtual serial port on the local serial device is being created, it is required to specify the IP address of the remote hosts to establish connection with.

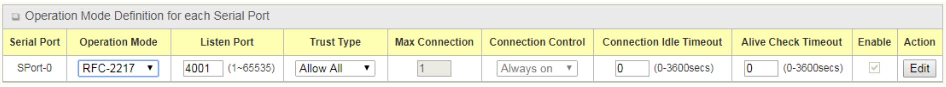


Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	Disable	N/A	N/A	N/A	N/A	N/A	N/A	□	Edit

Figure 3.128 Field Communication > Bus & Protocol > Virtual COM

When **Edit** button is applied, a screen similar to this appears.



Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	RFC-2217 ▾	4001 (1~65535)	Allow All ▾	1	Always on ▾	0 (0-3600secs)	0 (0-3600secs)	☑	Edit

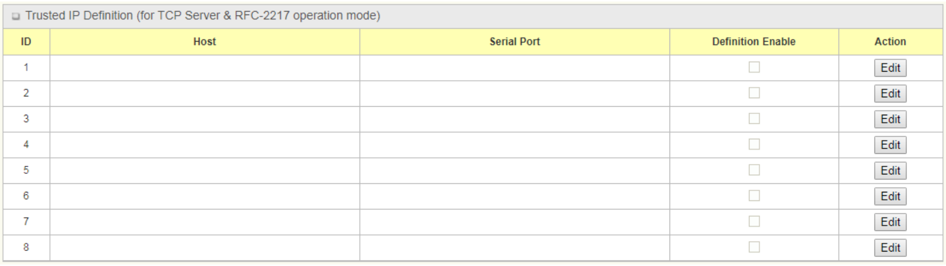
Figure 3.129 Field Communication > Bus & Protocol > Virtual COM

The following table describes the items in the previous figure.

Item	Description
Serial Port	It displays the serial port ID of the serial port. The number of serial ports varies from the purchased model.
Operation Mode	Select **RFC-2217** mode.
Listen Port	Indicate the listening port of RFC-2217 connection. Value Range: 1 ~ 65535

Item	Description
Trust Type	Select **Allow All** to allow any clients to connect. Otherwise select **Specific IPs** to limit certain clients.
Connection Idle Timeout	Enter the idle timeout in minutes. The idle timeout is used to disconnect the TCP connection when idle time elapsed. Idle timeout is only available when **On-Demand** is selected in the **Connection Control** field. Value Range: 0 ~ 3600 seconds.
Alive Check Timeout	Enter the time period of alive check timeout. The TCP connection will be terminated if it doesn't receive response of alive-check longer than this timeout setting. Alive check timeout is only available when **On-Demand** is selected in the **Connection Control** field. Value Range: 0 ~ 3600 seconds.
Enable	Check **Enable** checkbox to activate the corresponding serial port in specified operation mode.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

If you selected **Specific IPs** as the **Trust Type**, the **Trusted IP Definition** window appears. The settings are valid for both TCP Server and RFC-2217 modes.

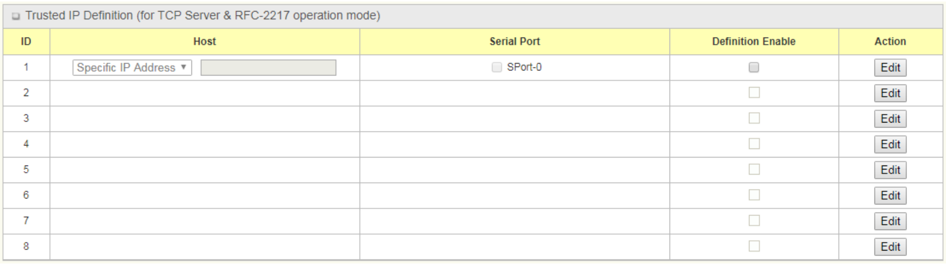


Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

ID	Host	Serial Port	Definition Enable	Action
1			□	Edit
2			□	Edit
3			□	Edit
4			□	Edit
5			□	Edit
6			□	Edit
7			□	Edit
8			□	Edit

Figure 3.130 Field Communication > Bus & Protocol > Virtual COM > Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

When **Edit** button is applied, a screen similar to this appears.



Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

ID	Host	Serial Port	Definition Enable	Action
1	Specific IP Address ▾	□ SPort-0	□	Edit
2			□	Edit
3			□	Edit
4			□	Edit
5			□	Edit
6			□	Edit
7			□	Edit
8			□	Edit

Figure 3.131 Field Communication > Bus & Protocol > Virtual COM > Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

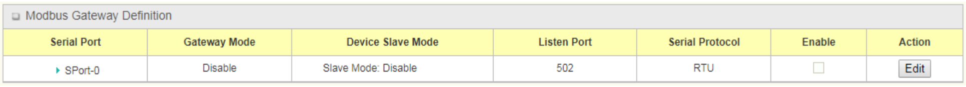
The following table describes the items in the previous figure.

Item	Description
Host	Enter the IP address range of allowed TCP clients.
Serial Port	Check the box to specify the rule for selected serial port.
Definition Enable	Check **Enable** checkbox to enable the rule.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.5.1.3 Modbus

To access this page, click **Field Communication** > **Bus & Protocol** > **Modbus**.

The **Modbus** screen enables user to configure the gateway to operate as a Modbus gateway, and allow access among Modbus TCP devices (which are connected to Ethernet network) and Modbus RTU/ASCII devices (which are connected to the Serial Port of the gateway). Once completed the Modbus settings in this section, ensure to select Modbus Operation Mode in Port Configuration screen to enable Modbus communication on the serial port.



Modbus Gateway Definition

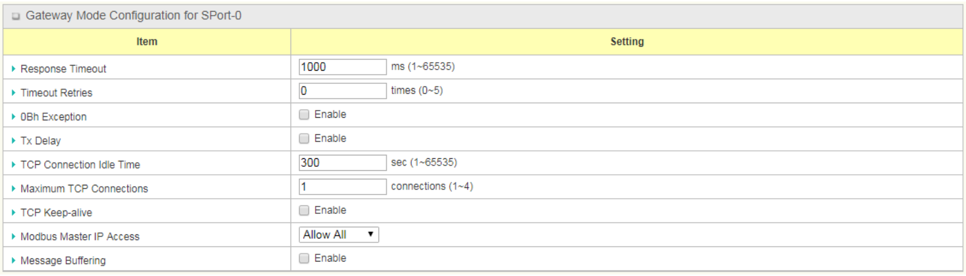
Serial Port	Gateway Mode	Device Slave Mode	Listen Port	Serial Protocol	Enable	Action
▸ SPort-0	Disable	Slave Mode: Disable	502	RTU	□	Edit

Figure 3.132 Field Communication > Bus & Protocol > Modbus

The following table describes the items in the previous figure.

Item	Description
Serial Port	It displays the name of the serial port used. E.g. SPort-0. The number of serial ports varies from the purchased model.
Gateway Mode	Specify the Modbus gateway mode for the selected serial port. It can be **Disable**, **Serial as Slave** or **Serial as Master**. A serial port can be attached with one Modbus Master, or daisy-chained a group of Modbus Salve devices. ■ **Disable:** Select this to disable the respective Modbus gateway function for the selected serial port. ■ **Serial as Slave:** Select this when the attached serial device(s) are all Modbus Slave devices. ■ **Serial as Master:** Select this when the attached serial device is a Modbus Master device.
Device Slave Mode	Check **Enable** checkbox to activate the integrated Modbus Salve function, and enter the preferred ID for the integrated Modbus slave. So that, it can function as a Modbus Slave device, and can be accessed with legacy Modbus Function Code from a SCADA management system. Supported Modbus commands are listed in the following table. Value Range: 1 ~ 247.
Listen Port	Specify the listen port number if Slave device(s) is attached to the selected serial port. It is a don't care setting if a Master device is attached. Value Range: 1 ~ 65535. ***Note:*** *Use different port number among the serial ports for the product with multiple serial ports.*
Serial Protocol	Select the serial protocol that is adopted by the attached Modbus device(s). It can be **RTU** or **ASCII**.
Enable	It displays whether the specific Modbus serial port is enabled or disabled. To enable or disable Modbus serial port, go to **Field Communication** > **Bus & Protocol** > **Port Configuration**, and set the operation mode as Modbus.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

When **Edit** button is applied, the **Gateway Mode Configuration** screen appears.



Gateway Mode Configuration for SPort-0

Item	Setting
Response Timeout	1000 ms (1~65535)
Timeout Retries	0 times (0~5)
0Bh Exception	□ Enable
Tx Delay	□ Enable
TCP Connection Idle Time	300 sec (1~65535)
Maximum TCP Connections	1 connections (1~4)
TCP Keep-alive	□ Enable
Modbus Master IP Access	Allow All ▾
Message Buffering	□ Enable

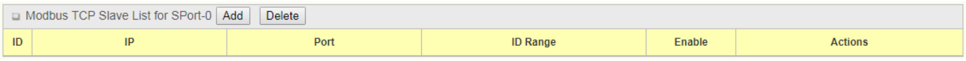
Figure 3.133 Field Communication > Bus & Protocol > Modbus

The following table describes the items in the previous figure.

Item	Description
Response Timeout	This sets the response timeout of the slave after master request sent. If the slave does not response within the specified time, data would be discarded. This applies to the serially attached Master sent request over to the remote Slave or requests send from the remote Master sent to the serially attached Slave. Value Range: 1 ~ 65535.
Timeout Retries	If the slave does not respond to the Master's request, the gateway will resend the request stored in the buffer. If timeout retries is set to null (value zero), the gateway would not buffer Master requests. If a value other than zero is specified, the gateway would store the Master request in the buffer and retries to send the request in a number of specified times. Once the retries are exhausted, the gateway will send a Modbus error message to the Master. However, if the **0Bh Exception** box is checked (see below), a 0Bh hex code based-error message will be send instead. Value Range: 0 ~ 5.
0Bh Exception	Check **Enable** checkbox to enable gateway to send a 0Bh exception code message to Modbus Master to indicate that the slave device does not respond within the timeout interval.
Tx Delay	Check **Enable** checkbox to activate to the minimum amount of time after receiving a response before the next message can be sent out. When Tx Delay is enabled the gateway would insert a Tx delay between Master requests. The delay gives sufficient time for the slave devices to turn their transmitters off and their receivers back on.
TCP Connection Idle Time	Enter the idle timeout in seconds. If the gateway does not receive another TCP request before the idle timeout elapsed, the TCP session will be terminated automatically. Value Range: 1 ~ 65535.
Maximum TCP Connections	Enter the allowed maximum simultaneous TCP connections. Value Range: 1 ~ 4.
TCP Keep-alive	Check **Enable** checkbox to ensure to keep the TCP session connected.
Modbus Master IP Access	Specify authorized masters on the TCP network. Select **Allow All** to allow any Modbus Master to reach the attached Slave(s). Otherwise, limit only specific Master to reach the Slave(s) by selecting **Specific IPs**. When **Specific IPs** is selected, the **Trusted IP Definition** function appears.

Item	Description
Trusted IP Definition	The function is only available when **Modbus Master IP Access** is **Specific IPs**. Click **Edit** to fill in the IP definition settings. ■ **Source IP:** – Select **Specific IP Address** to only allow an IP address of the allowed Master to access the attached Slave(s). – Select **IP Range** to only allow a set range of IP addresses of the allowed Master to access the attached Slave(s). – Select **IP Address-based Group** to only allow pre-defined group of IP address of the allowed Master to access the attached Slave(s). ■ **Enable:** Check **Enable** checkbox to enable this rule. ***Note:*** *Group must be pre-defined before this selection become available. Refer to **Object Definition** > **Grouping** > **Host Grouping**. You may also access to create a group by the Add Rule shortcut button. Setting done through the **Add** button will also appear in the **Host Grouping** screen. Then check **Enable** checkbox to enable this rule.*
Message Buffering	Check **Enable** checkbox to buffer up to 32 requests from Modbus Master. If the **Enable** checkbox is checked, a Modbus Priority Definition dialog will appear consequently. So that, the buffered Master requests can further be configured to prioritize request queue to transmit to Slave based on Master's IP address if requests are coming from remote Master, or based on remote Slave ID if requests are coming from serially attached Master, or based on Function Code.
Modbus Priority Definition	The function is only available when **Message Buffering** is **Enable**. Click **Edit** to fill in the priority settings. ■ **Modbus Priority:** A Priority List for setting the priority of specified Modbus identity. Modbus Priority 1 ~ Modbus Priority 4. ■ **Priority Base:** User can specify a Modbus identity with **IP Address**, **Slave ID**, or **Function Code**. The buffered Modbus message that matched the specified identity will be handled with given priority. The Modbus Master requests can be buffered to a certain priority queue according to the Master's IP address if requests are coming from remote Master, or the remote Slave's device ID if requests are coming from serially attached Master, or the specific function code that issued by Master. ■ **Enable:** Check **Enable** checkbox to enable the priority settings.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

If there is a Modbus Master device is attached to a certain serial port of the Modbus Gateway, user has to further specify the Modbus TCP Slave device(s) to send requests to from the attached Modbus RTU/ASCII Master device.

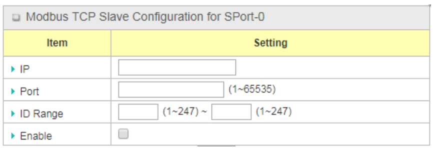


Modbus TCP Slave List for SPort-0

ID	IP	Port	ID Range	Enable	Actions

Figure 3.134 Field Communication > Bus & Protocol > Modbus > Modbus TCP Slave List

When **Add** button is applied, the **Modbus TCP Slave Configuration** screen appears.



Modbus TCP Slave Configuration for SPort-0

Item	Setting
IP	
Port	(1~65535)
ID Range	(1~247) ~ (1~247)
Enable	□

Figure 3.135 Field Communication > Bus & Protocol > Modbus > Modbus TCP Slave Configuration

The following table describes the items in the previous figure.

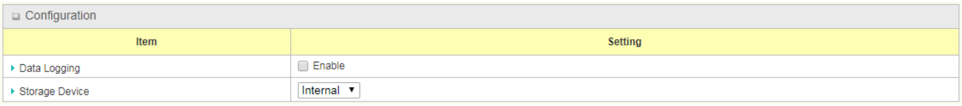
Item	Description
IP	Enter the IP address of the remote Modbus TCP Slave device.
Port	Enter the TCP port on which the remote Modbus TCP Slave device listens (to the TCP client session request). Value Range: 1 ~ 65535.
ID Range	Enter the Modbus ID range for the Modbus TCP Slave(s) that will respond to the Master's request. In addition to specify the Slave IP and Port, for accessing those Remote Modbus RTU Salve(s) located behind another Modbus gateway, user has to specify the Modus ID range of the Modbus RTU Slave(s). Value Range: 1 ~ 247.
Enable	Check **Enable** checkbox to enable this rule.
Save	Click **Save** to save the settings.

3.5.2 Data Logging

Data Logging is commonly used in monitoring systems to collect and analyze the field data. With proper configuration, the Gateway will record Modbus messages according to the specified rule list.

3.5.2.1 Configuration

To access this page, click **Field Communication** > **Data Logging** > **Configuration**.



Configuration

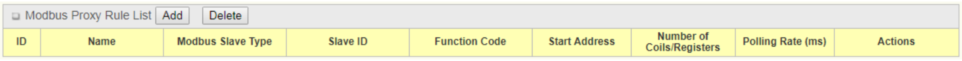
Item	Setting
Data Logging	□ Enable
Storage Device	Internal ▾

Figure 3.136 Field Communication > Data Logging > Configuration

The following table describes the items in the previous figure.

Item	Description
Data Logging	Check **Enable** checkbox to activate to data logging function.
Storage Device	Select the storage device to store the log files. It can be **External** or **Internal**, depends on the product specification.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

The Gateway allows you to customize your proxy mode rule list. It supports up to a maximum of 20 rules.

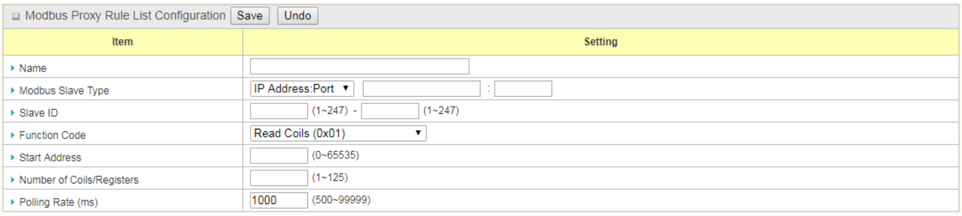


Modbus Proxy Rule List Add Delete

ID	Name	Modbus Slave Type	Slave ID	Function Code	Start Address	Number of Coils/Registers	Polling Rate (ms)	Actions

Figure 3.137 Field Communication > Data Logging > Configuration

When **Add** button is applied, the **Modbus Proxy Rule List Configuration** screen appears.



Modbus Proxy Rule List Configuration [Save] [Undo]

Item	Setting
Name	
Modbus Slave Type	IP Address:Port ▾ :
Slave ID	(1~247) - (1~247)
Function Code	Read Coils (0x01) ▾
Start Address	(0~65535)
Number of Coils/Registers	(1~125)
Polling Rate (ms)	1000 (500~99999)

Figure 3.138 Field Communication > Data Logging > Configuration

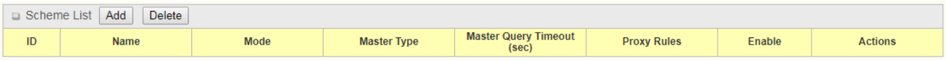
The following table describes the items in the previous figure.

Item	Description
Name	Specify a name as the identifier of the Modbus proxy rule. Value Range: 1 ~ 32 characters.
Modbus Slave Type	Specify the Modbus Slave devices to apply with the Modbus proxy rule. It can be **IP Address:Port** for Modbus TCP Slaves or **Local Serial Port** for local attached Modbus RTU/ASCII Slaves. Value Range: 1 ~ 65535 for port number.
Slave ID	Specify the ID range for the Slave device(s) to apply with the Modbus proxy rule. Value Range: 1 ~ 247.
Function Code	Specify a certain read function for the data logging proxy to issue and record the responses from device(s).
Start Address	Specify the start address of registers to apply with the specified function code. Value Range: 0 ~ 65535.
Number of Coils/ Registers	Specify the number of coils/registers to apply with the specified function code. Value Range: 1 ~ 125. ***Note:*** *Start Address plus Number must be smaller than 65536.*
Polling Rate (ms)	Enter the poll time in milliseconds to apply the proxy mode rule. Once the proxy mode is activated, the Modbus gateway will issue predefined Modbus message on each Poll Time interval accordingly. Value Range: 500 ~ 99999.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.5.2.2 Scheme Setup

To access this page, click **Field Communication** > **Data Logging** > **Scheme Setup**.

There are five data logging schemes to meet different management requirements. They are the **Sniffer Mode**, **Offline Proxy Mode**, **Full-Time Proxy Mode**, and the mixed modes for sniffer and proxy combinations. User has to configure the required data logging rules with selected scheme in the **Scheme Setup** page.

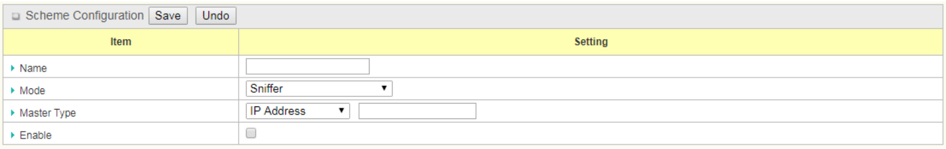


Scheme List [Add] [Delete]

ID	Name	Mode	Master Type	Master Query Timeout (sec)	Proxy Rules	Enable	Actions

Figure 3.139 Field Communication > Data Logging > Scheme Setup

When the Add button is applied, the **Scheme Configuration** screen appears.



Scheme Configuration Save Undo

Item	Setting
Name	
Mode	Sniffer ▾
Master Type	IP Address ▾
Enable	□

Figure 3.140 Field Communication > Data Logging > Scheme Setup > Scheme Configuration

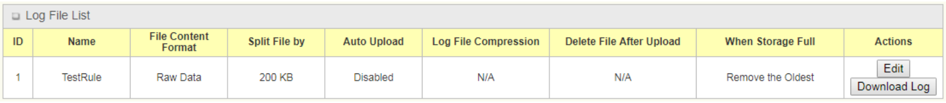
The following table describes the items in the previous figure.

Item	Description
Name	Specify a name as the identifier of the data logging rule. Value Range: 1 ~ 16 characters.
Mode	Select an expected data logging scheme for the data logging rule. There are five available schemes: ■ **Sniffer:** The Modbus gateway will record all the Modbus transactions between the Master and Slave devices. ■ **Off-Line Proxy:** When the connection between the Modbus gateway and Master is lost, the predefined proxy rule will be triggered and the Modbus gateway will issue specified function code to collect and record the data / status from the Slave devices ■ **Full-Time Proxy:** The predefined proxy rule will be triggered all the time and the Modbus gateway will issue specified function code to collect and record the data / status from the slave devices ■ **Sniffer & Off-Line Proxy:** This is a mixed mode for both Sniffer and Off-Line Proxy modes. ■ **Sniffer & Full-Time Proxy:** This is a mixed mode for both Sniffer and Full-Time Proxy modes.
Master Type	Specify the Modbus Master device to apply with the data logging rule. It can be IP address for Modbus TCP Master, or local serial port for local attached Modbus RTU/ASCII Master.
Master Query Timeout (sec)	Specify the timeout value for querying Modbus Master. If no response from the master for the specified timeout setting, selected proxy rule will be triggered and applied with the data logging rule. ***Note:*** *If **Off-Line Proxy** scheme is selected, the timeout setting will be used to check. Otherwise, it is a don't care value.*
Proxy Rules	Select the proxy rule to be applied with the data logging rule. ***Note:*** *If any proxy scheme is selected, please create the required Proxy rules in advance, and select from the list.*
Enable	Check **Enable** checkbox to activate the data logging rule.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.5.2.3 Log File Management

To access this page, click **Field Communication** > **Data Logging** > **Log File Management**.

If user had created data log rules in the **Field Communication** > **Data Logging** > **Scheme Setup**, there will be a log file list shown in the following **Log File** list screen. The default log file management settings will be applied if user didn't change it via the **Edit** button.

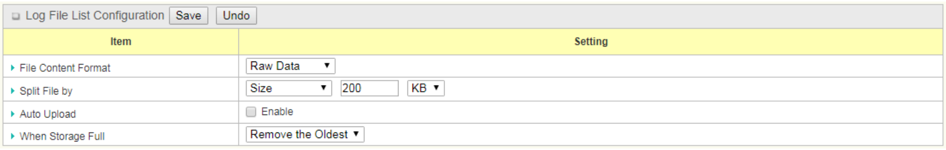


Log File List

ID	Name	File Content Format	Split File by	Auto Upload	Log File Compression	Delete File After Upload	When Storage Full	Actions
1	TestRule	Raw Data	200 KB	Disabled	N/A	N/A	Remove the Oldest	Edit Download Log

Figure 3.141 Field Communication > Data Logging > Log File Management

When **Edit** button is applied, the **Log File List Configuration** screen appears.



Log File List Configuration Save Undo

Item	Setting
File Content Format	Raw Data ▾
Split File by	Size ▾ 200 KB ▾
Auto Upload	□ Enable
When Storage Full	Remove the Oldest ▾

Figure 3.142 Field Communication > Data Logging > Log File Management > Log File List Configuration

The following table describes the items in the previous figure.

Item	Description
File Content Format	Select the data format for the log files. It can be **Raw Data**, or **Modbus Type**.
Split File by	Specify the split file methodology. It can be by **Size**, or by **Time Interval**. User has to specify a certain file size or time interval for splitting the data logs into a series of files. Value Range: 1 ~ 99999.
Auto Upload	Check **Enable** checkbox to activate the auto upload function for logged files. Once been enabled, user has to specify an external FTP server from the drop-down menu for auto uploading the log files to the server. Refer to **Object Definition** > **External Server** > **External Server**, or create the FTP server with the Add Object button.
Log File Compression	The function is only available when **Auto Upload** is **Enable**. User can further specify whether to compress the log file prior it is uploaded or not. Check **Enable** checkbox to activate the Log File Compression function.
Delete File After Upload	The function is only available when **Auto Upload** is **Enable**. User can further specify whether to delete the transferred log from the gateway storage or not. Check **Enable** checkbox to activate the function.
When Storage Full	Specify the operation to take when the storage is full. It can be **Remove the Oldest** log file, or **Stop Recording**. ■ When **Remove the Oldest** is selected, the gateway will delete the oldest file once the storage is full, and keep on the data logging activity; ■ When **Stop Recording** is selected, the gateway will stop the data logging activity once the storage is full.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

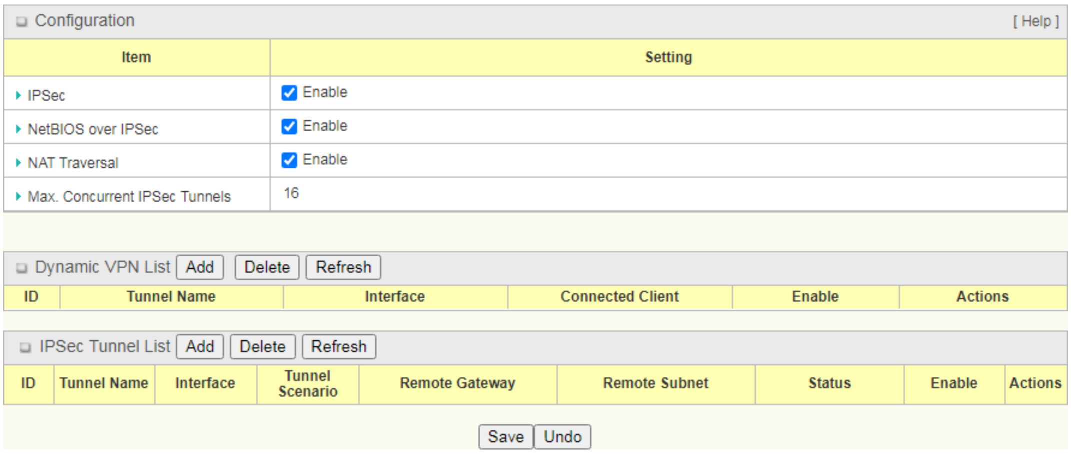
When **Download Log** button is applied, the web browser will download a file named as 'log.tar' to the managing host computer.

3.6 Security

3.6.1 VPN

3.6.1.1 IPSec

To access this page, click **Security** > **VPN** > **IP Sec**



Item	Setting
IPSec	☑ Enable
NetBIOS over IPSec	☑ Enable
NAT Traversal	☑ Enable
Max. Concurrent IPSec Tunnels	16

ID	Tunnel Name	Interface	Connected Client	Enable	Actions

ID	Tunnel Name	Interface	Tunnel Scenario	Remote Gateway	Remote Subnet	Status	Enable	Actions

Figure 3.143 Security > VPN > IPSec

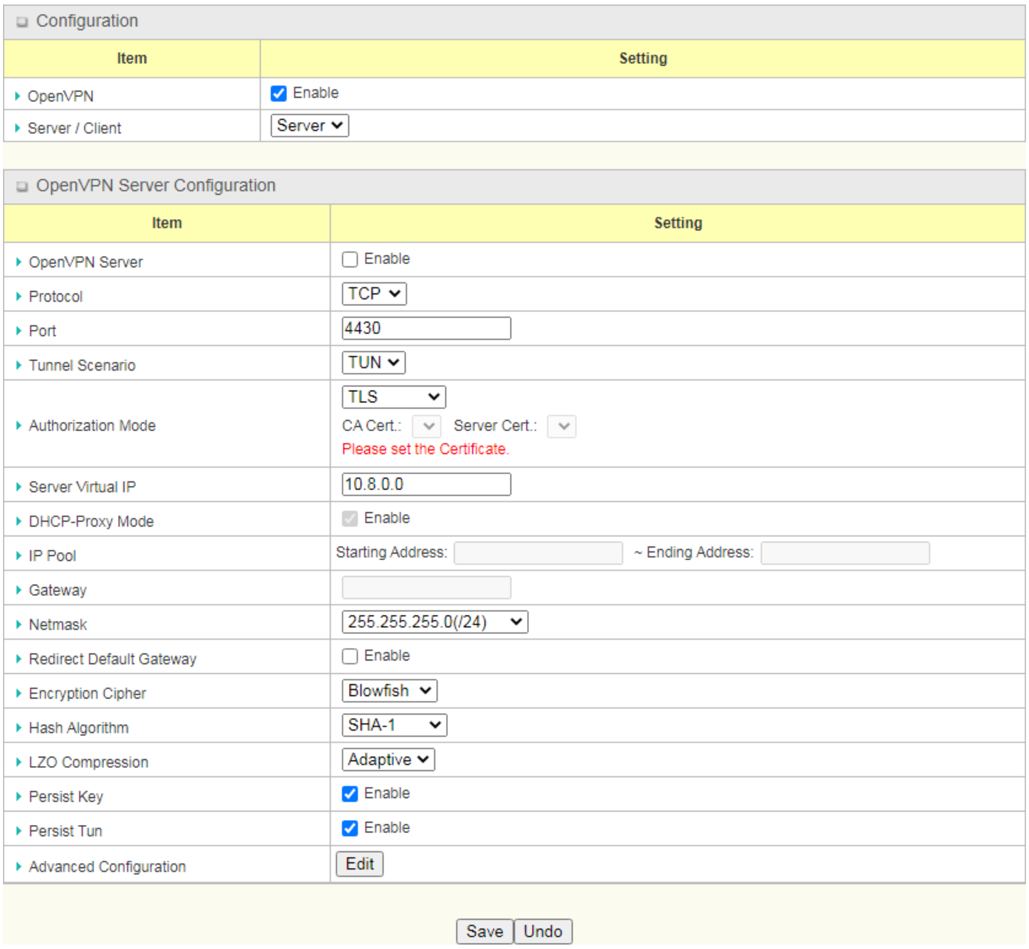
The following table describes the items in the previous figure.

Item	Description
Configuration	
IPSec	Click to enable or disable IPSec for VPN.
NetBIOS over IPSec	Click to enable or disable NetBIOS over IPSec for VPN.
NAT Traversal	Click to enable or disable NAT Traversal for VPN.
Max. Concurrent IPSec Tunnels	Displays the maximum number of concurrent IPSec tunnel routes.
Dynamic VPN List	
Add	Click to **Add** a Dynamic VPN listing.
Delete	Click to **Delete** a Dynamic VPN listing.
Refresh	Click to synchronize the displayed information.
ID	Displays the defined number assigned as the ID of the listing.
Tunnel Name	Displays the defined tunnel name of the listing.
Interface	Displays the assigned interface for the listing.
Connected Client	Displays the connection status of the listing.
Enable	Click on the radio button to enable or disable the listing.
Actions	Click **Edit** to modify the settings of the selected VPN listing. Click the radio button to select the listing when adding or deleting entries.
IPSec Tunnel List	
Add	Click to **Add** an IPSec Tunnel listing.
Delete	Click to **Delete** a IPSec Tunnel listing.
Refresh	Click to synchronize the displayed information.
ID	Displays the defined number assigned as the ID of the listing.
Tunnel Name	Displays the defined tunnel name of the listing.
Interface	Displays the assigned interface for the listing.

Item	Description
Tunnel Scenario	Displays the tunneling scenario for the listing. Settings: ■ Site to Site ■ Site to Host ■ Host to Site ■ Host to Host
Remote Gateway	Displays the remote gateway configuration assigned to the configuration.
Remote Subnet	Displays the remote subnet configuration assigned to the configuration.
Status	Displays the current status of the configuration listing.
Enable	Click on the radio button to enable or disable the listing.
Actions	Click **Edit** to modify the settings of the selected VPN listing. Click the radio button to select the listing when adding or deleting entries.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.6.1.2 OpenVPN

To access this page, click **Security** > **VPN** > **OpenVPN**.



Configuration

Item	Setting
OpenVPN	☑ Enable
Server / Client	Server

OpenVPN Server Configuration

Item	Setting
OpenVPN Server	□ Enable
Protocol	TCP
Port	4430
Tunnel Scenario	TUN
Authorization Mode	TLS CA Cert.: Server Cert.: Please set the Certificate.
Server Virtual IP	10.8.0.0
DHCP-Proxy Mode	☑ Enable
IP Pool	Starting Address: ~ Ending Address:
Gateway	
Netmask	255.255.255.0(/24)
Redirect Default Gateway	□ Enable
Encryption Cipher	Blowfish
Hash Algorithm	SHA-1
LZO Compression	Adaptive
Persist Key	☑ Enable
Persist Tun	☑ Enable
Advanced Configuration	Edit

Figure 3.144 Security > VPN > OpenVPN

The following table describes the items in the previous figure.

Item	Description
Configuration	
OpenVPN	Click to enable or disable the OpenVPN configuration.
Server/Client	Click the drop-down menu to select the designation of the server: Server or Client.
OpenVPN Server Configuration	
OpenVPN Server	Click to enable or disable the OpenVPN Server configuration.
Protocol	Click the drop-down menu to select the protocol: TCP or UCDP.
Port	Enter the port number for the OpenVPN Server
Tunnel Scenario	Click the drop-down menu to select the scenario: TAP or TUN.
Authorization Mode	Click to select the authorization: TLS or Static Key Settings: ■ TLS: Once the certificate is set, select CA or Server side certificates. ■ Static Key: Enter the local endpoint IP and remote endpoint IP addresses along with the static key for this mode.
Server Virtual IP	Enter the IP address to route traffic to the virtual IP.
DHCP-Proxy Mode	Available if Tunnel Scenario is TAP. Click to enable or disable the DHCP-proxy mode.TCP
IP Pool	If DHCP-proxy mode is not selected, enter the starting and ending addresses of the IP pool to assign to clients.
Gateway	Enter the gateway address for the setting.
Netmask	Click the drop-down menu to select a predefined netmask.
Redirect Default Gateway	Click to enable to disable the redirect default.
Encryption Cipher	Click the drop-down menu to select the cipher type: Blowfish, AES-256, AES-192, AES-128, None.
Hash Algorithm	Click the drop-down menu to select the hash algorithm: Settings: ■ SHA-1 ■ MD5 ■ MD4 ■ SHA-256 ■ SHA-512 ■ None ■ Disable
LZO Compression	Click the drop-down menu to select the LZO compression type: Settings: ■ Adaptive ■ Yes ■ No ■ Default
Persist Key	Click to enable to disable Persist key function.
Persist Tun	Click to enable to disable Persist tun function.

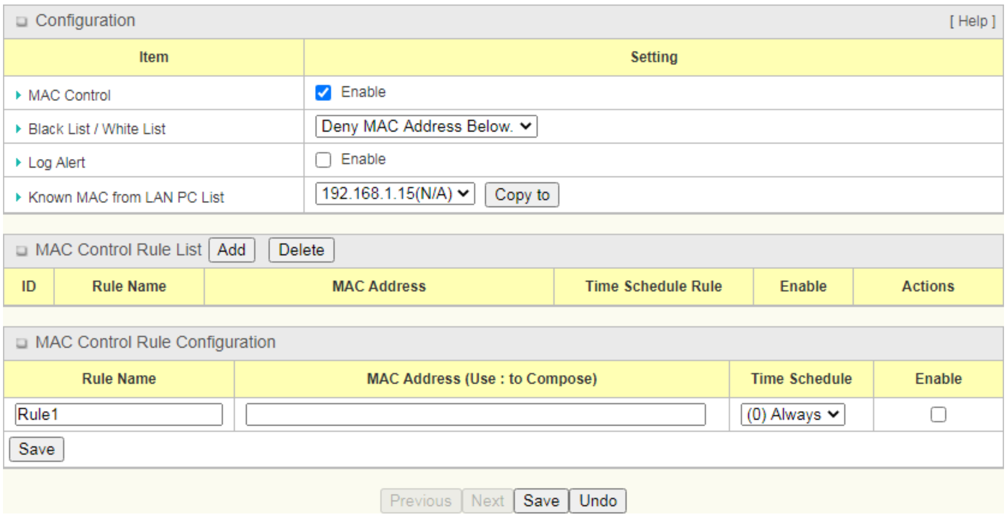
Item	Description
Advanced Configuration	Click to open the OpenVPN Server Advanced Configuration settings. Settings: ■ TLS Cipher ■ TLS Auth. Key ■ Client to Client ■ Duplicate CN ■ Tunnel MTU ■ Tunnel UDP Fragment ■ Tunnel UDP MSS-Fix ■ CCD-Dir Default File ■ Client Connection Script ■ Additional Configuration
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.6.2 Firewall

3.6.2.1 MAC Control

MAC Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

To access this page, click **Security** > **Firewall** > **MAC Control**.



Configuration [Help]

Item	Setting
MAC Control	☑ Enable
Black List / White List	Deny MAC Address Below.
Log Alert	□ Enable
Known MAC from LAN PC List	192.168.1.15(N/A) Copy to

MAC Control Rule List Add Delete

ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions

MAC Control Rule Configuration

Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
Rule1		(0) Always	□

Save

Previous Next Save Undo

Figure 3.145 Security > Firewall > MAC Control

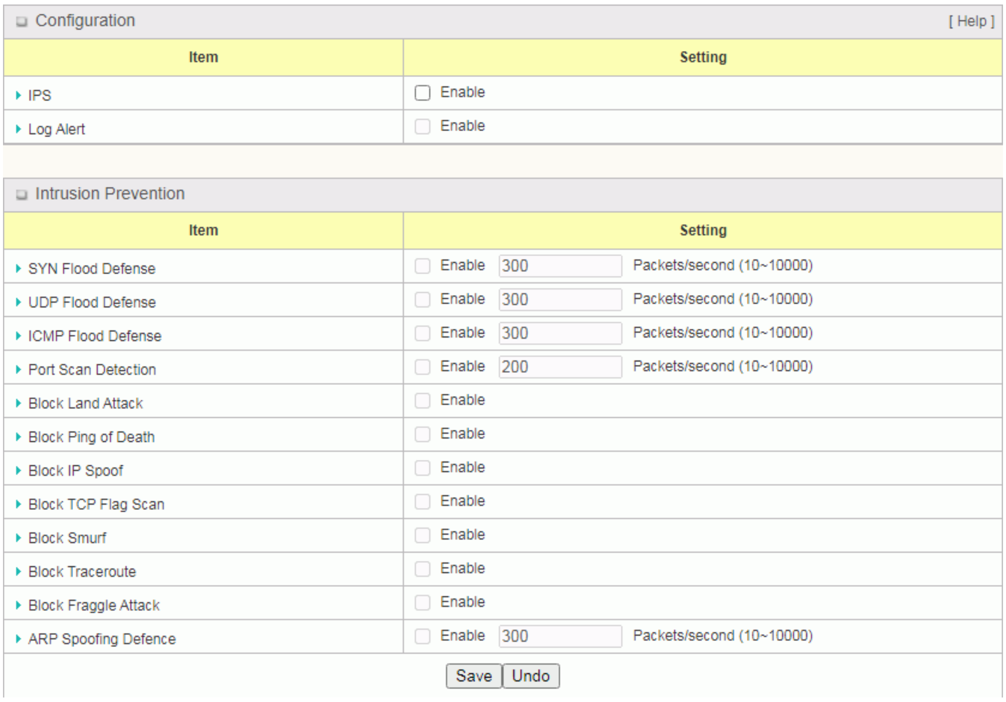
The following table describes the items in the previous figure.

Item	Description
Configuration	
MAC Control	Check **Enable** to enable the MAC Address Control. All of the settings in this page will take effect only when **Enable** is checked.
Black List / White List	Click the drop-down menu to allow or deny the define address access.
Log Alert	Click to enable or disable log notification.
Known MAC from LAN PC List	Click the drop-down menu to select the protocol: TCP or UCDP.

Item	Description
MAC Control Rule List	
Add	Click to add a Rule entry.
Delete	Click to delete a Rule entry.
Previous	Click to display the previous page listings.
Save	Click to display the following page listings.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.6.2.2 IPS

To access this page, click **Security** > **Firewall** > **IPS**.



Configuration [Help]

Item	Setting
IPS	□ Enable
Log Alert	□ Enable

Intrusion Prevention

Item	Setting
SYN Flood Defense	□ Enable 300 Packets/second (10~10000)
UDP Flood Defense	□ Enable 300 Packets/second (10~10000)
ICMP Flood Defense	□ Enable 300 Packets/second (10~10000)
Port Scan Detection	□ Enable 200 Packets/second (10~10000)
Block Land Attack	□ Enable
Block Ping of Death	□ Enable
Block IP Spoof	□ Enable
Block TCP Flag Scan	□ Enable
Block Smurf	□ Enable
Block Traceroute	□ Enable
Block Fraggle Attack	□ Enable
ARP Spoofing Defence	□ Enable 300 Packets/second (10~10000)

Figure 3.146 Security > Firewall > IPS

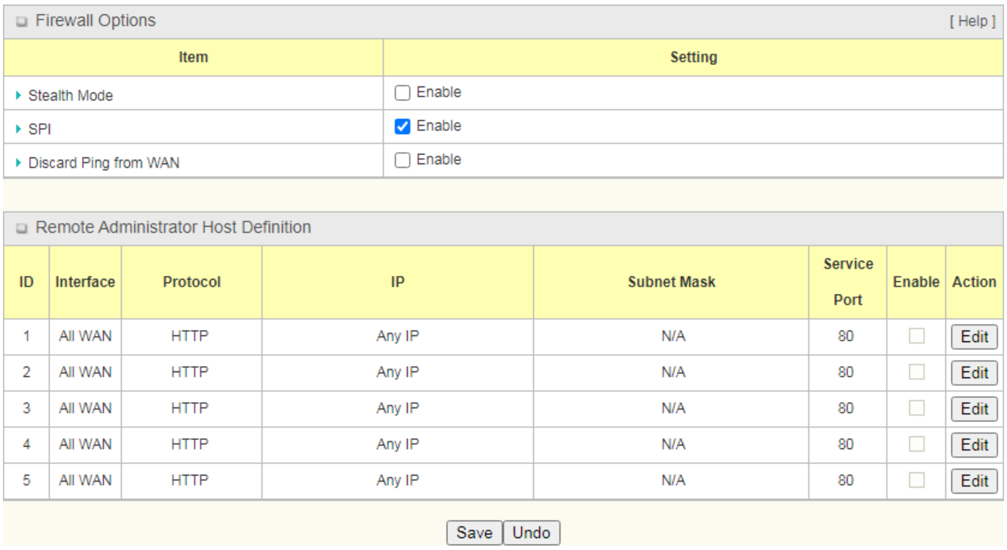
The following table describes the items in the previous figure.

Item	Description
Configuration	
IPS	Click to enable or disable the IPS function. IPS (Intrusion Prevention Systems) are network security appliances that monitor network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. You can enable the DoS flood, scan, fragment Defense functions and check the listed intrusion activities if necessary.
Log Alert	Available if IPS is enabled. Click to enable or disable the Log Alert function.
Intrusion Prevention	
SYN Flood Defense	Available if IPS is enabled. Click to enable and enter a variable to define the number of allowed packets per seconds (10 to 10000).

Item	Description
UDP Flood Defense	Available if IPS is enabled. Click to enable and enter a variable to define the number of allowed packets per seconds (10 to 10000).
ICMP Flood Defense	Available if IPS is enabled. Click to enable and enter a variable to define the number of allowed packets per seconds (10 to 10000).
Port Scan Detection	Available if IPS is enabled. Click to enable and enter a variable to define the number of allowed packets per seconds (10 to 10000).
Block Land Attack	Available if IPS is enabled. Click to enable or disable the setting.
Block Ping of Death	Available if IPS is enabled. Click to enable or disable the setting.
Block IP Spoof	Available if IPS is enabled. Click to enable or disable the setting.
Block TCP Flag Scan	Available if IPS is enabled. Click to enable or disable the setting.
Block Smurf	Available if IPS is enabled. Click to enable or disable the setting.
Block Traceroute	Available if IPS is enabled. Click to enable or disable the setting.
Block Fraggle Attack	Available if IPS is enabled. Click to enable or disable the setting.
ARP Spoofing Defense	Available if IPS is enabled. Click to enable and enter a variable to define the number of allowed packets per seconds (10 to 10000).
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.6.2.3 Options

To access this page, click **Security** > **Firewall** > **Options**.



Firewall Options [Help]

Item	Setting
Stealth Mode	□ Enable
SPI	☑ Enable
Discard Ping from WAN	□ Enable

Remote Administrator Host Definition

ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTP	Any IP	N/A	80	□	Edit
2	All WAN	HTTP	Any IP	N/A	80	□	Edit
3	All WAN	HTTP	Any IP	N/A	80	□	Edit
4	All WAN	HTTP	Any IP	N/A	80	□	Edit
5	All WAN	HTTP	Any IP	N/A	80	□	Edit

Figure 3.147 Security > Firewall > Options

Remote Administrator Host and Ports

In general, only LAN users can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits '/nn' notation to specified a group of trusted IP addresses for example, '10.1.2.0/24'.

The following table describes the items in the previous figure.

Item	Description
Firewall Options	
Stealth Mode	Enable this Feature, the Device will not respond to port scans from the WAN so that make it less susceptible to discovery and attacks on the Internet.
SPI	When this feature is enabled, the router will record the packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.
Discard Ping from WAN	When this feature is enabled, any host on the WAN side can`t ping this product. It means this device won`t reply any ICMP packet from Internet.
Remote Administrator Host Definition	
ID	Displays the host ID.
Interface	Displays the host configured interface.
Protocol	Displays the host protocol for the interface.
IP	Displays the host interface IP setting.
Subnet Mask	Displays the host interface subnet mask.
Service Port	Displays the host the interface defined port number.
Enable	Click to enable or disable the selected host.
Action	Click to edit the selected host entry.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

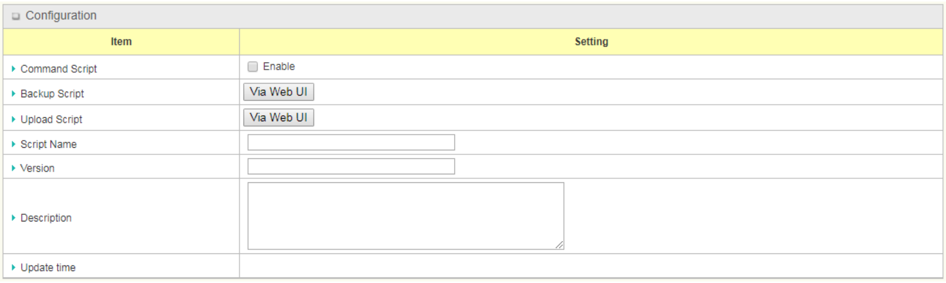
3.7 Administration

3.7.1 Configure & Manage

3.7.1.1 Command Script

To access this page, click **Administration** > **Configure & Manage** > **Command Script**.

Command script configuration is the application that allows administrator to setup the pre-defined configuration in plain text style and apply configuration on startup.



Configuration

Item	Setting
Command Script	□ Enable
Backup Script	Via Web UI
Upload Script	Via Web UI
Script Name	
Version	
Description	
Update time	

Figure 3.148 Administration > Configure & Manage > Command Script

The following table describes the items in the previous figure.

Item	Description
Command Script	Check **Enable** checkbox to activate the command script function.
Backup Script	Click **Via Web UI** or **Via Storage** to backup the existed command script in a .txt file. You can specify the script file name in **Script Name** below.
Upload Script	Click **Via Web UI** or **Via Storage** to Upload the existed command script from a specified .txt file.
Script Name	Specify a script file name for script backup, or display the selected upload script file name. Value Range: 0 ~ 32 characters.
Version	Specify the version number for the applied command script. Value Range: 0 ~ 32 characters.
Description	Enter a short description for the applied command script.
Update time	It records the upload time for last command script upload.
Save	Click **Save** to save the settings.

You can edit the plain text configuration settings in the configuration screen.

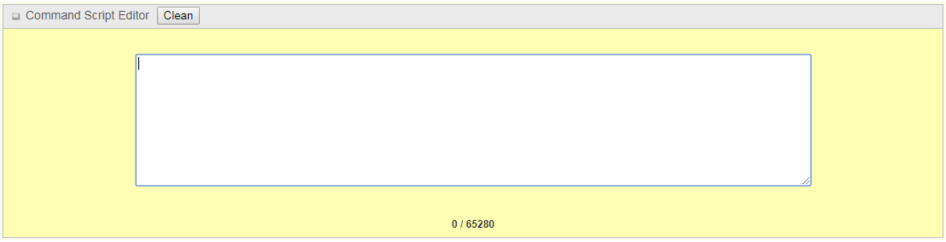


Figure 3.149 Administration > Configure & Manage > Command Script > Command Script Editor

The following table describes the items in the previous figure.

Item	Description
Clean	Click **Clean** to clean text area. (You should click **Save** to further clean the configuration already saved in the system.)
Backup	Click **Backup** to backup and download configuration.
Save	Click **Save** to save the settings.

The supported plain text configuration items are shown in the following list. For the settings that can be executed with standard Linux commands, you can put them in a script file, and apply to the system configure with STARTUP command. For those configurations without corresponding Linux command set to configure, you can configure them with proprietary command set.

Configuration Content Key	Value Setting	Description
OPENVPN_ENABLED	1: enable 0: disable	Enable or disable OpenVPN client function.
OPENVPN_DESCRIPTION	A must filled setting	Specify the tunnel name for the OpenVPN client connection.

Configuration Content Key	Value Setting	Description
OPENVPN_PROTO	udp tcp	Define the protocol for the OpenVPN client. ■ Select **TCP** or **TCP /UDP** The OpenVPN will use TCP protocol, and port will be set as 443 automatically. ■ Select **UDP** The OpenVPN will use UDP protocol, and port will be set as 1194 automatically.
OPENVPN_PORT	A must filled setting	Specify the port for the OpenVPN client to use.
OPENVPN_REMOTE_IPADDR	IP or FQDN	Specify the **Remote IP/FQDN** of the peer OpenVPN server for this OpenVPN client tunnel. Fill in the IP address or FQDN.
OPENVPN_PING_INTVL	seconds	Specify the time interval for OpenVPN keep-alive checking.
OPENVPN_PING_TOUT	seconds	Specify the timeout value for OpenVPN client keep-alive checking.
OPENVPN_COMP	Adaptive	Specify the **LZO Compression** algorithm for OpenVPN client.
OPENVPN_AUTH	Static Key/TLS	Specify the authorization mode for the OpenVPN tunnel. ■ TLS The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Client Cert.** and **Client Key** need to specify as well.
OPENVPN_CA_CERT	A must filled setting	Specify the trusted CA certificate for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_CERT	A must filled setting	Specify the local certificate for OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_KEY	A must filled setting	Specify the local key for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_EXTRA_OPTS	Options	Specify the extra options setting for the OpenVPN client.
IP_ADDR1	IP	Ethernet LAN IP.
IP_NETM1	Net mask	Ethernet LAN mask.
PPP_MONITORING	1: enable 0: disable	When the network monitoring feature is enabled, the router will use DNS query or ICMP to periodically check Internet connection – connected or disconnected.

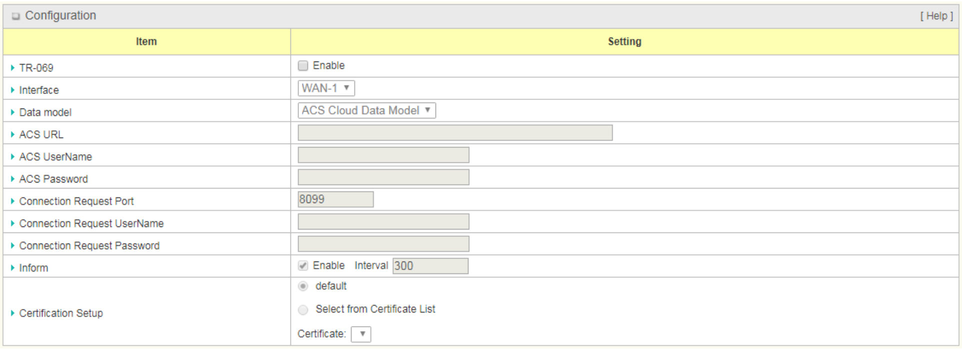
Configuration Content Key	Value Setting	Description
PPP_PING	0: DNS Query 1: ICMP Query	With **DNS Query**, the system checks the connection by sending DNS query packets to the destination specified in PPP_PING_IPADDR. With **ICMP Query**, the system will check connection by sending ICMP request packets to the destination specified in PPP_PING_IPADDR.
PPP_PING_IPADDR	IP	Specify an IP address as the target for sending DNS query/ICMP request.
PPP_PING_INTVL	seconds	Specify the time interval for between two DNS query or ICMP checking packets.

STARTUP	Script file	For the configurations that can be configured with standard Linux commands, you can put them in a script file, and apply the script file with STARTUP command.
		For example,
		STARTUP=#!/bin/sh
		STARTUP=echo “startup done” > /tmp/demo

3.7.1.2 TR-069

To access this page, click **Administration** > **Configure & Manage** > **TR-069**.

In **TR-069** screen, there is only one configuration window for TR-069 function. In the window, you must specify the related information for your security gateway to connect to the ACS. Drive the function to work by specifying the URL of the ACS server, the account information to login the ACS server, the service port and the account information for connection requesting from the ACS server, and the time interval for job inquiry. Except the inquiry time, there are no activities between the ACS server and the gateways until the next inquiry cycle. But if the ACS server has new jobs that are expected to do by the gateways urgently, it will ask these gateways by using connection request related information for immediate connection for inquiring jobs and executing.



Configuration [Help]

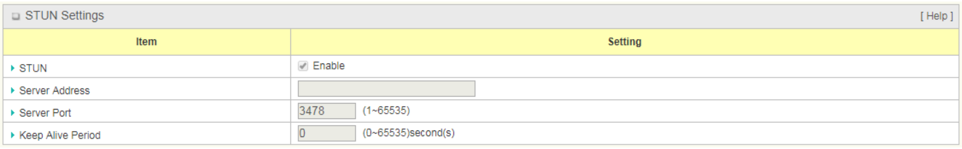
Item	Setting
TR-069	□ Enable
Interface	WAN-1 ▾
Data model	ACS Cloud Data Model ▾
ACS URL	
ACS UserName	
ACS Password	
Connection Request Port	8099
Connection Request UserName	
Connection Request Password	
Inform	☑ Enable Interval 300
Certification Setup	● default ○ Select from Certificate List Certificate: ▾

Figure 3.150 Administration > Configure & Manage > TR-069

The following table describes the items in the previous figure.

Item	Description
TR-069	Check **Enable** checkbox to activate TR-069 function.
Interface	When you finish set basic network WAN-1 ~ WAN-n, you can select WAN-1 ~ WAN-n. When you finish set **Security** > **VPN** > **IPSec/OpenVPN/PPTP/L2TP/GRE**, you can select **IPSec/OpenVPN/PPTP/L2TP/GRE** tunnel, the interface just like “IPSec #1”.
Data model	Select the TR-069 dat model for the remote management. ■ **Standard:** The ACS server is a standard one, which is fully comply with TR-069. ■ **ACS Cloud Data Model:** Select this data model if you intend to use cloud ACS server to managing the deployed gateways.
ACS URL	You can ask ACS manager provide ACS URL and manually set.
ACS UserName	You can ask ACS manager provide ACS username and manually set.
ACS Password	You can ask ACS manager provide ACS password and manually set.
Connection Request Port	You can ask ACS manager provide ACS ConnectionRequest Port and manually set. Value Range: 0 ~ 65535.
Connection Request UserName	You can ask ACS manager provide ACS ConnectionRequest Username and manually set.
Connection Request Password	You can ask ACS manager provide ACS ConnectionRequest Password and manually set

Item	Description
Inform	When the **Enable** checkbox is checked, the gateway (CPE) will periodically send inform message to ACS server according to the Interval setting. Value Range: 0 ~ 86400 for Inform Interval.
Certification Setup	You can leave it as **default** or select an expected certificate and key from the drop-down menu. Refer to **Object Definition** > **Certificate** for the **Certificate** configuration.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



STUN Settings [Help]

Item	Setting
STUN	☑ Enable
Server Address	
Server Port	3478 (1~65535)
Keep Alive Period	0 (0~65535)second(s)

Figure 3.151 Administration > Configure & Manage > TR-069 > STUN Settings

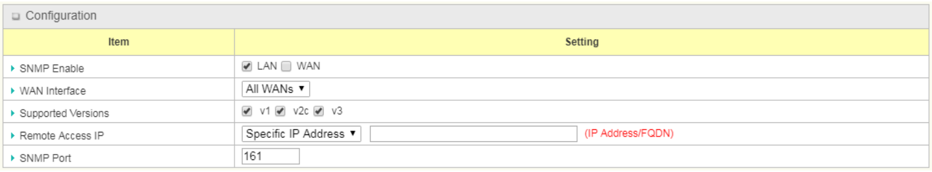
The following table describes the items in the previous figure.

Item	Description
STUN	Check **Enable** checkbox to activate STUN function.
Server Address	Specify the IP address for the expected STUN server.
Server Port	Specify the port number for the expected STUN server. Value Range: 1 ~ 65535.
Keep Alive Period	Specify the keep alive time period for the connection with STUN server. Value Range: 0 ~ 65535.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.7.1.3 SNMP

To access this page, click **Administration** > **Configure & Manage** > **SNMP**.

The SNMP allows user to configure SNMP relevant setting which includes interface, version, access control and trap receiver.



Configuration

Item	Setting
SNMP Enable	☑ LAN ☐ WAN
WAN Interface	All WANs ▾
Supported Versions	☑ v1 ☑ v2c ☑ v3
Remote Access IP	Specific IP Address ▾ (IP Address/FQDN)
SNMP Port	161

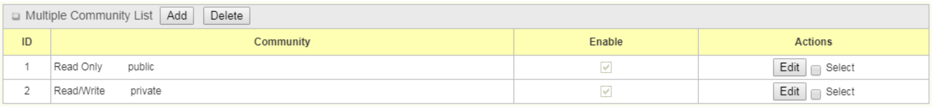
Figure 3.152 Administration > Configure & Manage > SNMP

The following table describes the items in the previous figure.

Item	Description
SNMP Enable	Select the interface for the SNMP and enable SNMP functions. ■ When check the **LAN** box, it will activate SNMP functions and you can access SNMP from LAN side; ■ When check the **WAN** box, it will activate SNMP functions and you can access SNMP from WAN side.

Item	Description
WAN Interface	Specify the WAN interface that a remote SNMP host can access to the device. By default, **All WANs** is selected, and there is no limitation for the WAN interface.
Supported Versions	Select the version for the SNMP ■ When check the **v1** box: It means you can access SNMP by version 1. ■ When check the **v2c** box: It means you can access SNMP by version 2c. ■ When check the **v3** box: It means you can access SNMP by version 3.
Remote Access IP	Specify the remote access IP for WAN. ■ Select **Specific IP Address**, and fill in a certain IP address. It means only this IP address can access SNMP from LAN/ WAN side. ■ Select **IP Range**, and fill in a range of IP addresses. It means the IP address within specified range can access SNMP from LAN/WAN side. If you left it as blank, it means any IP address can access SNMP from WAN side.
SNMP Port	Specify the SNMP port. You can fill in any port number. But you must ensure the port number is not to be used. Value Range: 1 ~ 65535.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

The SNMP allows you to custom your access control for version 1 and version 2 user. The router supports up to a maximum of 10 community sets.

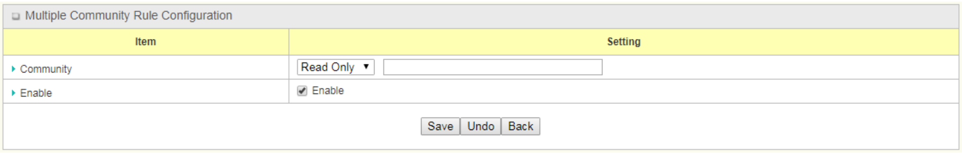


Multiple Community List

ID	Community	Enable	Actions
1	Read Only public	☑	Edit □ Select
2	Read/Write private	☑	Edit □ Select

Figure 3.153 Administration > Configure & Manage > SNMP

When **Add** button is applied, the **Multiple Community Rule Configuration** screen appears.



Multiple Community Rule Configuration

Item	Setting
Community	Read Only ▾
Enable	☑ Enable

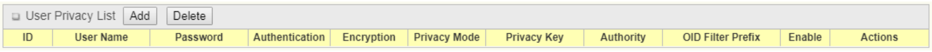
Figure 3.154 Administration > Configure & Manage > SNMP > Multiple Community Rule Configuration

The following table describes the items in the previous figure.

Item	Description
Community	Specify this version 1 or version v2c user's community that will be allowed Read Only (GET and GETNEXT) or Read-Write (GET, GETNEXT and SET) access respectively. The maximum length of the community is 32.
Enable	Click **Enable** checkbox to enable this version 1 or version v2c user.

Item	Description
Save	Click **Save** to save the settings. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show “Click on save button to apply your changes” remind user to click main page **Save** button.
Undo	Click **Undo** to cancel the settings.
Back	Click **Back** to return the previous screen.

The SNMP allows you to custom your access control for version 3 user. The router supports up to a maximum of 128 User Privacy sets.

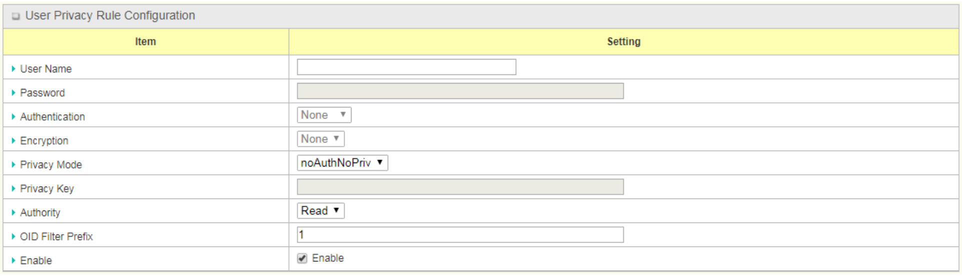


User Privacy List Add Delete

ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	OID Filter Prefix	Enable	Actions

Figure 3.155 Administration > Configure & Manage > SNMP > User Privacy List

When **Add** button is applied, the **User Privacy Rule Configuration** screen appears.



User Privacy Rule Configuration

Item	Setting
User Name	
Password	
Authentication	None
Encryption	None
Privacy Mode	noAuthNoPriv
Privacy Key	
Authority	Read
OID Filter Prefix	1
Enable	☑ Enable

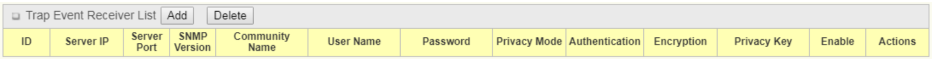
Figure 3.156 Administration > Configure & Manage > SNMP > User Privacy Rule Configuration

The following table describes the items in the previous figure.

Item	Description
User Name	Specify the user name for this version 3 user. Value Range: 1 ~ 32 characters.
Password	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the password for this version 3 user. Value Range: 8 ~ 64 characters.
Authentication	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the authentication types for this version 3 user. Selected the authentication types **MD5**/**SHA-1** to use.
Encryption	When your **Privacy Mode** is **authPriv**, you must specify the encryption protocols for this version 3 user. Selected the encryption protocols **DES**/**AES** to use.
Privacy Mode	Specify the **Privacy Mode** for this version 3 user. ■ **noAuthNoPriv:** You do not use any authentication types and encryption protocols. ■ **authNoPriv:** You must specify the Authentication and Password. ■ **authPriv:** You must specify the Authentication, Password, Encryption and Privacy Key.
Privacy Key	When your **Privacy Mode** is **authPriv**, you must specify the privacy key (8 ~ 64 characters) for this version 3 user.
Authority	Specify this version 3 user’s authority that will be allowed **Read Only** (GET and GETNEXT) or **Read-Write** (GET, GETNEXT and SET) access respectively.
OID Filter Prefix	The **OID Filter Prefix** restricts access for this version 3 user to the sub-tree rooted at the given OID. Value Range: 1 ~2080768.

Item	Description
Enable	Click **Enable** checkbox to enable this version 3 user.
Save	Click **Save** to save the settings. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show “Click on save button to apply your changes” remind user to click main page **Save** button.
Undo	Click **Undo** to cancel the settings.
Back	Click **Back** to return the previous screen.

The SNMP allows you to custom your trap event receiver. The router supports up to a maximum of 4 Trap Event Receiver sets.

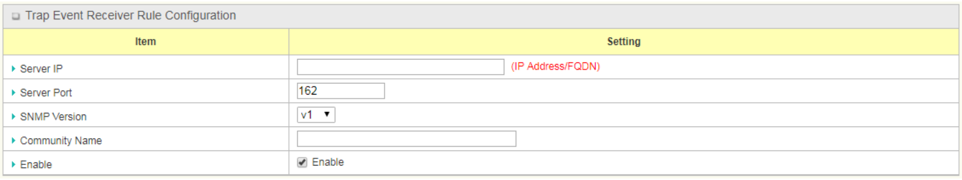


□ Trap Event Receiver List Add Delete

ID	Server IP	Server Port	SNMP Version	Community Name	User Name	Password	Privacy Mode	Authentication	Encryption	Privacy Key	Enable	Actions

Figure 3.157 Administration > Configure & Manage > SNMP

When **Add** button is applied, the **Trap Event Receiver Rule Configuration** screen appears. The default SNMP Version is v1. The configuration screen will provide the version 1 must filled items.



□ Trap Event Receiver Rule Configuration

Item	Setting
Server IP	(IP Address/FQDN)
Server Port	162
SNMP Version	v1 ▾
Community Name	
Enable	☑ Enable

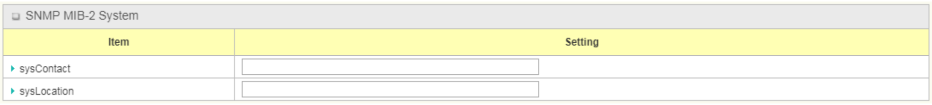
Figure 3.158 Administration > Configure & Manage > SNMP > Trap Event Receiver Rule Configuration

The following table describes the items in the previous figure.

Item	Description
Server IP	Specify the trap **Server IP** or **FQDN**. The DUT will send trap to the server IP/FQDN.
Server Port	Specify the trap server port. You can fill in any port number. But you must ensure the port number is not to be used. Value Range: 1 ~ 65535.
SNMP Version	Select the version for the trap ■ Selected the **v1**: The configuration screen will provide the version 1 must filled items. ■ Selected the **v2c**: The configuration screen will provide the version 2c must filled items. ■ Selected the **v3**: The configuration screen will provide the version 3 must filled items.
Community Name	Specify the community name for this version 1 or version v2c trap. Value Range: 1 ~ 32 characters.
User Name	The function is only available when **SNMP Version** is **v3**. Specify the user name for this version 3 trap. Value Range: 1 ~ 32 characters.
Password	The function is only available when **SNMP Version** is **v3**. When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the password for this version 3 trap. Value Range: 8 ~ 64 characters.

Item	Description
Privacy Mode	The function is only available when **SNMP Version** is **v3**. Specify the Privacy Mode for this version 3 trap. ■ **noAuthNoPriv:** You do not use any authentication types and encryption protocols. ■ **authNoPriv:** You must specify the Authentication and Password. ■ **authPriv:** You must specify the Authentication, Password, Encryption and Privacy Key.
Authentication	The function is only available when **SNMP Version** is **v3**. When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the authentication types for this version 3 trap. Selected the authentication types **MD5/SHA-1** to use.
Encryption	The function is only available when **SNMP Version** is **v3**. When your **Privacy Mode** is **authPriv**, you must specify the encryption protocols for this version 3 trap. Selected the encryption protocols **DES/AES** to use.
Privacy Key	The function is only available when **SNMP Version** is **v3**. When your **Privacy Mode** is **authPriv**, you must specify the privacy key (8 ~ 64 characters) for this version 3 trap.
Enable	Click **Enable** checkbox to enable this trap receiver.
Save	Click **Save** to save the settings. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" remind user to click main page **Save** button.
Undo	Click **Undo** to cancel the settings.
Back	Click **Back** to return the previous screen.

If required, you can also specify the required information of the MIB-2 System.



SNMP MIB-2 System

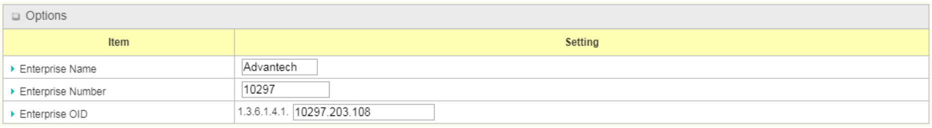
Item	Setting
sysContact	
sysLocation	

Figure 3.159 Administration > Configure & Manage > SNMP > SNMP MIB-2 System

The following table describes the items in the previous figure.

Item	Description
sysContact	Specify the contact information for MIB-2 system. Value Range: 0 ~ 64 characters.
sysLocation	Specify the location information for MIB-2 system. Value Range: 0 ~ 64 characters.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

If you use some particular private MIB, you must fill the enterprise name, number and OID.



Options

Item	Setting
Enterprise Name	Advantech
Enterprise Number	10297
Enterprise OID	1.3.6.1.4.1. 10297.203.108

Figure 3.160 Administration > Configure & Manage > SNMP > Options

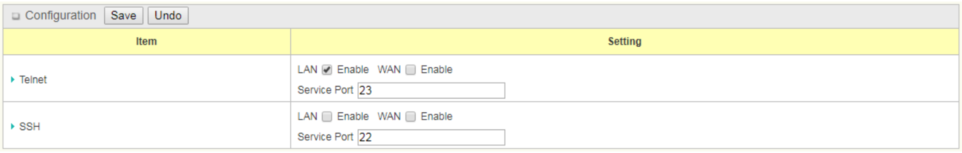
The following table describes the items in the previous figure.

Item	Description
Enterprise Name	Specify the enterprise name for the particular private MIB. Value Range: 1 ~ 10 characters, and only string with A ~ Z, a ~ z, 0 ~ 9, '–', '_'.
Enterprise Number	Specify the enterprise number for the particular private MIB. Value Range: 1 ~2080768.
Enterprise OID	Specify the Enterprise OID for the particular private MIB. The range of the each OID number is 1 ~ 2080768. The maximum length of the enterprise OID is 31. The seventh number must be identical with the enterprise number.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.7.1.4 Telnet & SSH

To access this page, click **Administration** > **Configure & Manage** > **Telnet & SSH**.

The **Telnet & SSH** screen allows administrator to access this device through the traditional Telnet or SSH Telnet program. Before you can telnet (login) to the device, please configure the related settings and password with care. The password management part allows you to set root password for logging telnet and SSH.

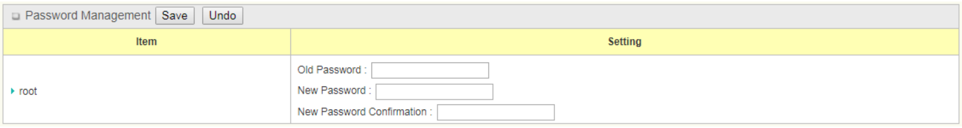


Item	Setting
Telnet	LAN ☑ Enable WAN □ Enable Service Port 23
SSH	LAN □ Enable WAN □ Enable Service Port 22

Figure 3.161 Administration > Configure & Manage > Telnet & SSH

The following table describes the items in the previous figure.

Item	Description
Telnet	Check **Enable** checkbox to activate the Telnet function for connecting from LAN or WAN interfaces. You can set which number of service port you want to provide for the corresponding service. Value Range: 1 ~ 65535.
SSH	Check **Enable** checkbox to activate the SSH Telnet function for connecting from LAN or WAN interfaces. You can set which number of service port you want to provide for the corresponding service. Value Range: 1 ~ 65535.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.



Item	Setting
root	Old Password : New Password : New Password Confirmation :

Figure 3.162 Administration > Configure & Manage > Telnet & SSH > Password Management

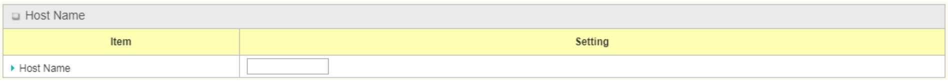
The following table describes the items in the previous figure.

Item	Description
root	Type old password and specify new password to change root password. ***Note:*** *You are highly recommended to change the default telnet password with yours before the device is deployed.* ***Note:*** *If you have trouble for the default password for previous FW version, please check the corresponding User Manual to get the correct one.*
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.7.2 System Operation

3.7.2.1 Password & MMI

To access this page, click **Administration** > **System Operation** > **Password & MMI**.



Host Name

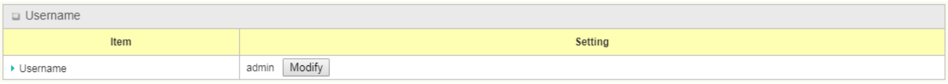
Item	Setting
Host Name	

Figure 3.163 Administration > System Operation > Password & MMI > Host Name

The following table describes the items in the previous figure.

Item	Description
Host Name	Enter new host name to replace the current setting.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

Change Username screen allows network administrator to change the web-based MMI login account to access gateway.

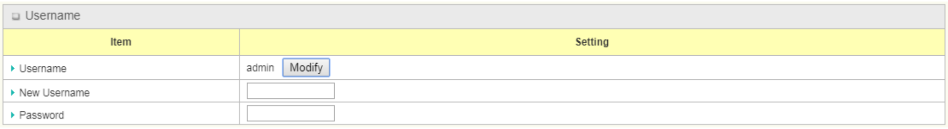


Username

Item	Setting
Username	admin Modify

Figure 3.164 Administration > System Operation > Password & MMI > Username

Click **Modify** button and provide the new username setting.



Username

Item	Setting
Username	admin Modify
New Username	
Password	

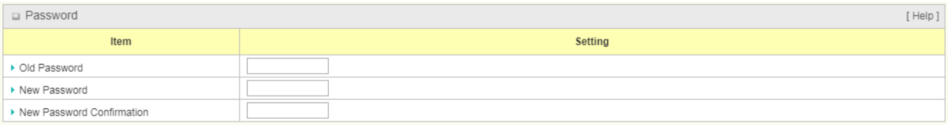
Figure 3.165 Administration > System Operation > Password & MMI > Username

The following table describes the items in the previous figure.

Item	Description
Username	Display the current MMI login account (username).
New Username	Enter new username to replace the current setting.

Item	Description
Password	Enter current password to verify if you have the permission to change the username setting.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

Change password screen allows network administrator to change the web-based MMI login password to access gateway.



Password [Help]

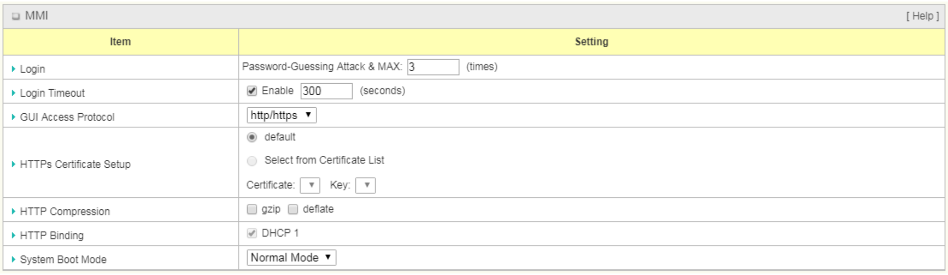
Item	Setting
Old Password	
New Password	
New Password Confirmation	

Figure 3.166 Administration > System Operation > Password & MMI > Password

The following table describes the items in the previous figure.

Item	Description
Old Password	Enter the current password to enable you unlock to change password.
New Password	Enter new password.
New Password Confirmation	Enter new password again to confirm.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

This is the gateway's web-based MMI access which allows administrator to access the gateway for management. The gateway's web-based MMI will automatically logout when the idle time has elapsed. The setting allows administrator to enable automatic logout and set the logout idle time. When the login timeout is disabled, the system won't logout the administrator automatically.



MMI [Help]

Item	Setting
Login	Password-Guessing Attack & MAX: 3 (times)
Login Timeout	☑ Enable 300 (seconds)
GUI Access Protocol	http/https ▼
HTTPs Certificate Setup	● default ○ Select from Certificate List Certificate: ▼ Key: ▼
HTTP Compression	□ gzip □ deflate
HTTP Binding	☑ DHCP 1
System Boot Mode	Normal Mode ▼

Figure 3.167 Administration > System Operation > Password & MMI > MMI

The following table describes the items in the previous figure.

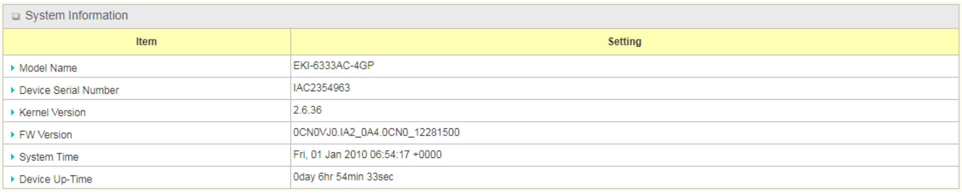
Item	Description
Login	Enter the login trial counting value. If someone tried to login the web GUI with incorrect password for more than the counting value, an warning message "Already reaching maximum Password-Guessing times, please wait a few seconds!" will be displayed and ignore the following login trials. Value Range: 3 ~ 10.
Login Timeout	Check **Enable** checkbox to activate the auto logout function, and specify the maximum idle time as well. Value Range: 30 ~ 65535.

Item	Description
GUI Access Protocol	Select the protocol that will be used for GUI access. It can be **http/https**, **http only**, or **https only**.
HTTPs Certificate Setup	If the **https** access protocol is selected, the **HTTPs Certificate Setup** option will be available for further configuration. You can leave it as default or select a expected certificate and key from the drop-down menu. Refer to **Object Definition** > **Certificate** for the **Certificate** configuration.
HTTP Compression	Click the checkbox (**gzip**, or **deflate**) if any compression method is preferred.
HTTP Binding	Click the checkbox to enable the function. The HTTP Binding function provides connectivity for SOAP over HTTP in a JBI 1.0 compliant environment.
System Boot Mode	Select the system boot mode that will be adopted to boot up the device. ■ **Normal Mode:** It takes longer boot up time, about 200 seconds, with complete firmware image check during the device booting. ■ **Fast Mode:** It takes shorter boot up time, about 120 seconds, without checking the firmware image during the device booting. ■ **Quick Mode:** It takes shorter boot up time, about 90 seconds, without checking the firmware image and create the internal database for User/Group/Captive Portal functions. ***Note:*** *Use **Quick Mode** with care, once selected, the User/Group/Captive Portal function will become non-functional.*
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.7.2.2 System Information

To access this page, click **Administration** > **System Operation** > **System Information**.

System Information screen gives network administrator a quick look up on the device information for the purchases gateway.



System Information

Item	Setting
Model Name	EKI-6333AC-4GP
Device Serial Number	IAC2354963
Kernel Version	2.6.36
FW Version	0CN0VJ0.IA2_0A4.0CN0_12281500
System Time	Fri, 01 Jan 2010 06:54:17 +0000
Device Up-Time	0day 6hr 54min 33sec

Figure 3.168 Administration > System Operation > System Information

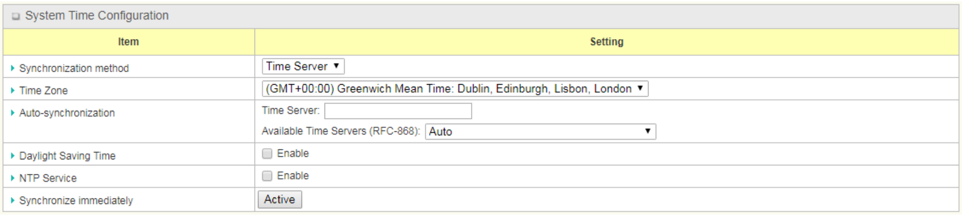
The following table describes the items in the previous figure.

Item	Description
Model Name	It displays the model name of this product.
Device Serial Number	It displays the serial number of this product.
Kernel Version	It displays the Linux kernel version of the product.
FW Version	It displays the firmware version of the product.
System Time	It displays the current system time that you browsed this web page.

Item	Description
Device Up-Time	It displays the statistics for the device up-time since last boot up.
Refresh	Click **Refresh** to update the system Information immediately.

3.7.2.3 System Time

To access this page, click **Administration** > **System Operation** > **System Time**.



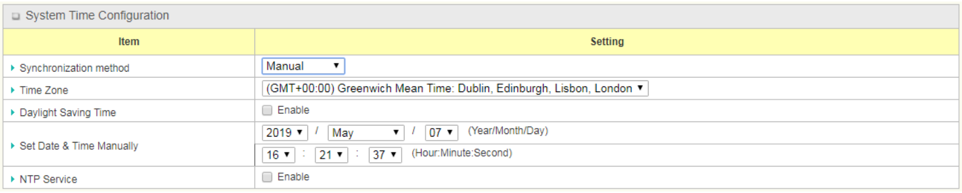
System Time Configuration

Item	Setting
Synchronization method	Time Server ▾
Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾
Auto-synchronization	Time Server: Available Time Servers (RFC-868): Auto ▾
Daylight Saving Time	□ Enable
NTP Service	□ Enable
Synchronize immediately	Active

Figure 3.169 Administration > System Operation > System Time

The following table describes the items in the previous figure.

Item	Description
Synchronization method	Select **Time Server** as the synchronization method for the system time.
Time Zone	Select a time zone where this device locates.
Auto-synchronization	Enter the IP or FQDN for the NTP time server you expected, or leave it as auto mode so that the available server will be used for time synchronization one by one.
Daylight Saving Time	Check **Enable** checkbox to activate the daylight saving function. When you enabled this function, you have to specify the start date and end date for the daylight saving time duration.
NTP Service	Check **Enable** checkbox to activate the NTP service function. When you enabled this function, the gateway can provide NTP server service for its local connected devices.
Synchronize immediately	Click **Active** to synchronize the system time with specified time server immediately.
Save	Click **Save** to save the settings.
Refresh	Click **Refresh** to update the system Information immediately.



System Time Configuration

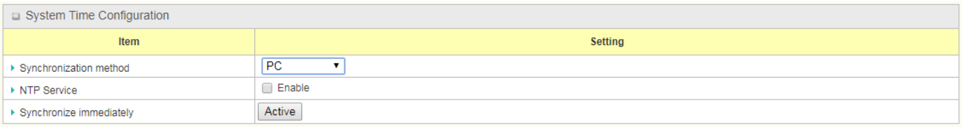
Item	Setting
Synchronization method	Manual ▾
Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾
Daylight Saving Time	□ Enable
Set Date & Time Manually	2019 ▾ / May ▾ / 07 ▾ (Year/Month/Day) 16 ▾ : 21 ▾ : 37 ▾ (Hour:Minute:Second)
NTP Service	□ Enable

Figure 3.170 Administration > System Operation > System Time

The following table describes the items in the previous figure.

Item	Description
Synchronization method	Select **Manual** as the synchronization method for the system time. It means administrator has to set the date & time manually.
Time Zone	Select a time zone where this device locates.
Daylight Saving Time	Check **Enable** checkbox to activate the daylight saving function. When you enabled this function, you have to specify the start date and end date for the daylight saving time duration.

Item	Description
Set Date & Time Manually	Manually set the date (Year/Month/Day) and time (Hour:Minute:Second) as the system time.
NTP Service	Check **Enable** checkbox to activate the NTP Service function. When you enabled this function, the gateway can provide NTP server service for its local connected devices.
Save	Click **Save** to save the settings.
Refresh	Click **Refresh** to update the system Information immediately.



System Time Configuration

Item	Setting
Synchronization method	PC ▾
NTP Service	□ Enable
Synchronize immediately	Active

Figure 3.171 Administration > System Operation > System Time

The following table describes the items in the previous figure.

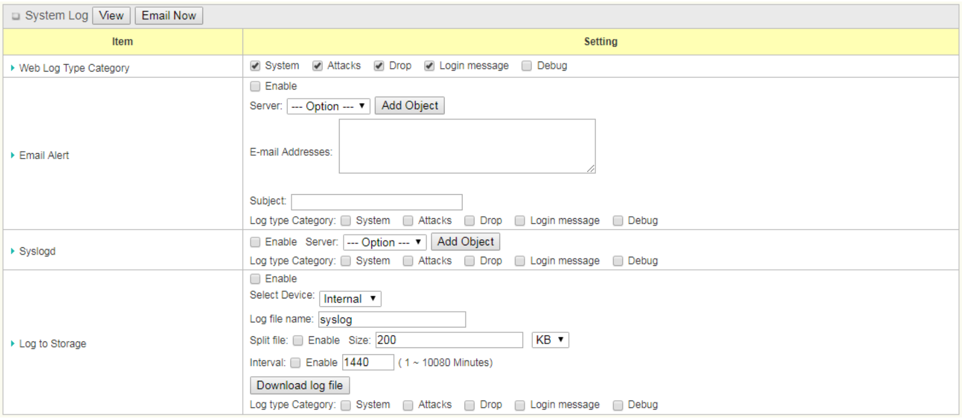
Item	Description
Synchronization method	Select **PC** as the synchronization method for the system time to let system synchronize its date and time to the time of the administration PC.
NTP Service	Check **Enable** checkbox to activate the NTP service function. When you enabled this function, the gateway can provide NTP server service for its local connected devices.
Synchronize immediately	Click **Active** to synchronize the system time with specified time server immediately.
Save	Click **Save** to save the settings.
Refresh	Click **Refresh** to update the system Information immediately.

3.7.2.4 System Log

To access this page, click **Administration** > **System Operation** > **System Log**.

System Log screen contains various event log tools facilitating network administrator to perform local event logging and remote reporting.

Web Log Type Category screen allows network administrator to select the type of events to log and be displayed in the Web Log List Window as described in the previous section.



System Log | View | Email Now

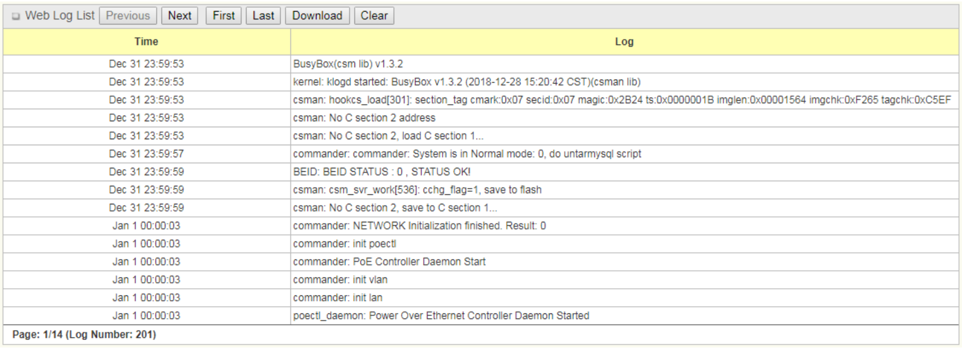
Item	Setting
Web Log Type Category	☑ System ☑ Attacks ☑ Drop ☑ Login message □ Debug
Email Alert	□ Enable Server: --- Option --- ▾ Add Object E-mail Addresses: Subject: Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug
Syslogd	□ Enable Server: --- Option --- ▾ Add Object Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug
Log to Storage	□ Enable Select Device: Internal ▾ Log file name: syslog Split file: □ Enable Size: 200 KB ▾ Interval: □ Enable 1440 (1 ~ 10080 Minutes) Download log file Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

Figure 3.172 Administration > System Operation > System Log

The following table describes the items in the previous figure.

Item	Description
Web Log Type Category	■ **System:** Check to log system events and to display in the Web Log List window. ■ **Attacks:** Check to log attack events and to display in the Web Log List window. ■ **Drop:** Check to log packet drop events and to display in the Web Log List window. ■ **Login message:** Check to log system login events and to display in the Web Log List window. ■ **Debug:** Check to log debug events and to display in the Web Log List window.
Email Alert	■ **Enable:** Check **Enable** checkbox to enable sending event log messages to destined Email account defined in the E-mail Addresses blank space. ■ **Server:** Select one email server from the Server drop-down menu to send Email. If none has been available, click the **Add Object** button to create an outgoing Email server. You may also add an outgoing Email server from **Object Definition** > **External Server** > **External Server**. ■ **E-mail address:** Enter the recipient's Email address. Separate Email addresses with comma ',' or semicolon ';'. Enter the Email address in the format of 'myemail@domain.com'
Email Alert (Continued)	■ **Subject:** Enter an Email subject that is easy for you to identify on the Email client. ■ **Log type category:** Select the type of events to log and be sent to the designated Email account. Available events are **System**, **Attacks**, **Drop**, **Login message**, and **Debug**.
Syslogd	■ **Enable:** Check **Enable** checkbox to activate the Syslogd function, and send event logs to a syslog server ■ **Server:** Select one syslog server from the Server drop-down menu to sent event log to. If none has been available, click the **Add Object** button to create a system log server. You may also add an system log server from the **Object Definition** > **External Server** > **External Server**. ■ **Log type category:** Select the type of event to log and be sent to the destined syslog server. Available events are **System**, **Attacks**, **Drop**, **Login message**, and **Debug**.
Log to Storage	■ **Enable:** Check **Enable** checkbox to enable sending log to storage. ■ **Select Device:** Select internal or external storage. ■ **Log file name:** Enter log file name to save logs in designated storage. ■ **Split file Enable:** Check **Enable** checkbox to split file whenever log file reaching the specified limit. ■ **Split file Size:** Enter the file size limit for each split log file. Value Range: 10 ~1000. ■ **Log type category:** Check which type of logs to send: **System**, **Attacks**, **Drop**, **Login message**, **Debug**
View	Click **View** to view Log History in Web Log List Window.
Email Now	Click **Email Now** to send Log History via Email instantly.
Save	Click **Save** to save the settings.
Refresh	Click **Refresh** to update the system Information immediately.

When **View** button is applied, the **Web Log List** screen appears.



Time	Log
Dec 31 23:59:53	BusyBox(csm lib) v1.3.2
Dec 31 23:59:53	kernel: klogd started: BusyBox v1.3.2 (2018-12-28 15:20:42 CST)(csman lib)
Dec 31 23:59:53	csman: hookcs_load[301]: section_tag cmark:0x07 secid:0x07 magic:0x2B24 ts:0x0000001B imglen:0x00001564 imgchk:0xF265 tagchk:0xC5EF
Dec 31 23:59:53	csman: No C section 2 address
Dec 31 23:59:53	csman: No C section 2, load C section 1...
Dec 31 23:59:57	commander: commander: System is in Normal mode: 0, do untarmysql script
Dec 31 23:59:59	BEID: BEID STATUS : 0 , STATUS OK!
Dec 31 23:59:59	csman: csm_svr_work[536]: cchg_flag=1, save to flash
Dec 31 23:59:59	csman: No C section 2, save to C section 1...
Jan 1 00:00:03	commander: NETWORK Initialization finished. Result: 0
Jan 1 00:00:03	commander: init poectl
Jan 1 00:00:03	commander: PoE Controller Daemon Start
Jan 1 00:00:03	commander: init vlan
Jan 1 00:00:03	commander: init lan
Jan 1 00:00:03	poectl_daemon: Power Over Ethernet Controller Daemon Started

Page: 1/14 (Log Number: 201)

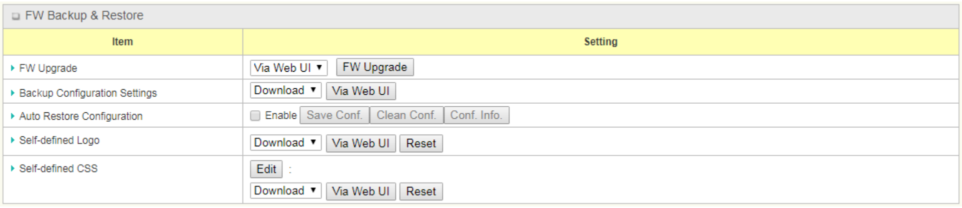
Figure 3.173 Administration > System Operation > System Log > Web Log List

The following table describes the items in the previous figure.

Item	**Description**
Time column	It displays event time stamps.
Log column	It displays log messages.
Previous	Click **Previous** to move to the previous page.
Next	Click **Next** to move to the next page.
First	Click **First** to jump to the first page.
Last	Click **Last** to jump to the last page.
Download	Click **Download** to download log to your PC in .tar file format.
Clear	Click **Clear** to clear all log.
Back	Click **Back** to return to the previous page.

3.7.2.5 Backup & Restore

To access this page, click **Administration** > **System Operation** > **Backup & Restore**.



Item	Setting
FW Upgrade	Via Web UI ▾ FW Upgrade
Backup Configuration Settings	Download ▾ Via Web UI
Auto Restore Configuration	□ Enable Save Conf. Clean Conf. Conf. Info.
Self-defined Logo	Download ▾ Via Web UI Reset
Self-defined CSS	Edit : Download ▾ Via Web UI Reset

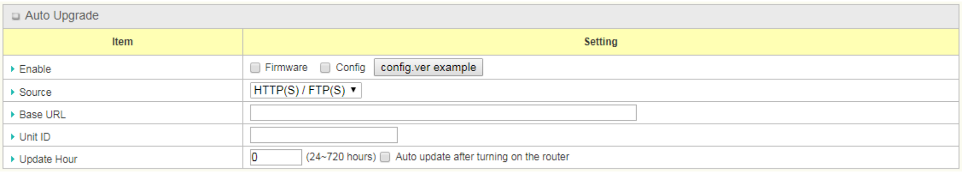
Figure 3.174 Administration > System Operation > Backup & Restore > FW Backup & Restore

The following table describes the items in the previous figure.

Item	**Description**
FW Upgrade	If new firmware is available, click the FW Upgrade button to upgrade the device firmware via Web UI, or Via Storage. After clicking **FW Upgrade** button, you need to specify the file name of new firmware by clicking **Browse**, and then click **Upgrade** to start the FW upgrading process on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”.

Item	Description
Backup Configuration Settings	You can backup or restore the device configuration settings by clicking the **Via Web UI** button. ■ **Download:** for backup the device configuration to a config.bin file. ■ **Upload:** for restore a designated configuration file to the device. ■ **Via Web UI:** to retrieve the configuration file via Web GUI.
Auto Restore Configuration	Check **Enable** checkbox to activate the customized default setting function. Once the function is activated, you can save the expected setting as a customized default setting by clicking **Save Conf.**, or clicking **Clean Conf.** to erase the stored customized configuration.
Self-defined Logo	The logo for the web UI can be downloaded or uploaded from or to the router. ***Note:*** *The file name must be "logo.gif".*
Self-defined CSS	The CSS style guide used by the interface can be edited by clicking **Edit**. The style guide can also be uploaded or downloaded as a CSS file. ***Note:*** *The file name must be "wmqa01.css".*
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

Auto Upgrade via HTTP(S)/FTP(S) source can be configured in the bottom part. If the Firmware or Configuration found on the server is newer than the current one, it will be updated.



Auto Upgrade

Item	Setting
Enable	□ Firmware □ Config [config.ver example]
Source	HTTP(S) / FTP(S) ▾
Base URL	
Unit ID	
Update Hour	0 (24~720 hours) □ Auto update after turning on the router

Figure 3.175 Administration > System Operation > Backup & Restore > Auto Upgrade

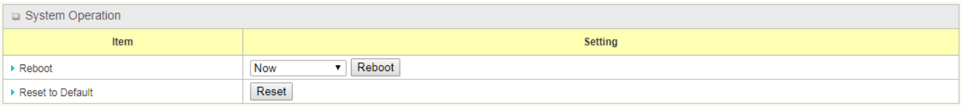
The following table describes the items in the previous figure.

Item	Description
Enable	Enable **Firmware** or **Configuration** upgrade or both: ■ **Firmware:** The router will look for a newer firmware file and update when found. ■ **Config:** The device check for a configuration update by comparing the file dates and installs it using this setting. **config .ver example** button will prompt the download of .ver file example needed on server for Config update.
Source	Select the location of the upgrade files: ■ **HTTP(S) / FTP(S):** Updates are downloaded from the Base URL address below. Used protocol is specified by the address: HTTP, HTTPS, FTP or FTPS.
Base URL	IP address from which the configuration file will be downloaded. This option also specifies the communication protocol, example: http://example.com

Item	Description
Unit ID	Name of configuration file (name of the file without extension). If not filled, the MAC address of the router is used as the filename (the dots are used as delimiter instead of colons.)
Update Hour	Set the time (range 24 to 720 hours) to regularly check for updates. If the **Auto update after turning on the router** checkbox is enabled, the check is performed five minutes after the device is powered up or rebooted. If the detected firmware or configuration file is newer than the running one, it is downloaded and the router is rebooted automatically.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.7.2.6 Reboot & Reset

To access this page, click **Administration** > **System Operation** > **Reboot & Reset**.



System Operation

Item	Setting
Reboot	Now ▾ Reboot
Reset to Default	Reset

Figure 3.176 Administration > System Operation > Reboot & Reset

The following table describes the items in the previous figure.

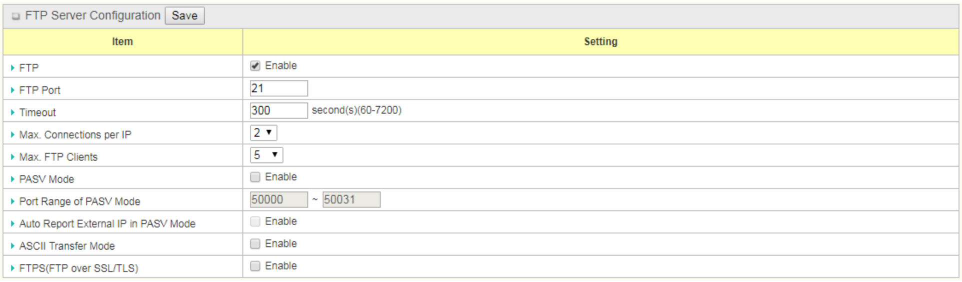
Item	Description
Reboot	Chick **Reboot** to reboot the gateway immediately or on a pre-defined time schedule. ■ **Now:** Reboot immediately. ■ **Time Schedule:** Select a pre-defined auto-reboot time schedule rule to reboot the auto device on a designated time. To define a time schedule rule, go to **Object Definition** > **Scheduling** > **Configuration**.
Reset to Default	Click **Reset** to reset the device configuration to its default value.
Save	Click **Save** to save the settings.

3.7.3 FTP

3.7.3.1 Server Configuration

To access this page, click **Administration** > **FTP** > **Server Configuration**.

Sever Configuration allows user to setup the embedded FTP and SFTP server for retrieving the interested fog files.



FTP Server Configuration Save

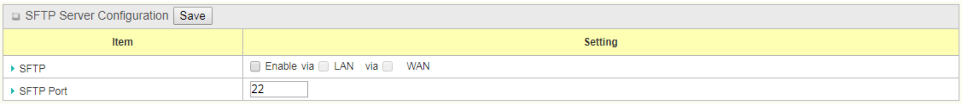
Item	Setting
FTP	☑ Enable
FTP Port	21
Timeout	300 second(s)(60-7200)
Max. Connections per IP	2 ▾
Max. FTP Clients	5 ▾
PASV Mode	□ Enable
Port Range of PASV Mode	50000 ~ 50031
Auto Report External IP in PASV Mode	□ Enable
ASCII Transfer Mode	□ Enable
FTPS(FTP over SSL/TLS)	□ Enable

Figure 3.177 Administration > FTP > Server Configuration > FTP Server Configuration

The following table describes the items in the previous figure.

Item	Description
FTP	Check **Enable** checkbox to activate the embedded FTP server function. With the FTP server enabled, you can retrieve or delete the stored log files via FTP connection. ***Note:*** *The embedded FTP Server is only for log downloading, so no any write permission is implemented for user file upload to the storage.*
FTP Port	Specify a port number for FTP connection. The gateway will listen for incoming FTP connections on the specified port. Value Range: 1 ~ 65535.
Timeout	Specify the maximum timeout interval for the FTP connection. Supported range is 60 to 7200 seconds.

Item	Description
Max. Connections per IP	Specify the maximum number of clients from the same IP address for the FTP connection. Up to 5 clients from the same IP address is supported.
Max. FTP Clients	Specify the maximum number of clients for the FTP connection. Up to 32 clients is supported.
PASV Mode	Check **Enable** checkbox to activate the support of PASV mode for a FTP connection from FTP clients.
Port Range of PASV Mode	Specify the port range to allocate for PASV style data connection. Value Range: 1024 ~ 65535.
Auto Report External IP in PASV Mode	Check **Enable** checkbox to activate the support of overriding the IP address advertising in response to the PASV command.
ASCII Transfer Mode	Check **Enable** checkbox to activate the support of ASCII mode data transfers. Binary mode is supported by default.
FTPS(FTP over SSL/TLS)	Check **Enable** checkbox to activate the support of secure connections via SSL/TLS.
Save	Click **Save** to save the settings.



SFTP Server Configuration [Save]

Item	Setting
SFTP	□ Enable via □ LAN via □ WAN
SFTP Port	22

Figure 3.178 Administration > FTP > Server Configuration > SFTP Server Configuration

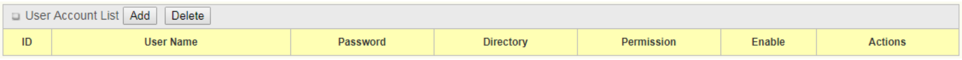
The following table describes the items in the previous figure.

Item	Description
SFTP	Check **Enable** checkbox to activate the embedded SFTP server function. With the SFTP server enabled, you can retrieve or delete the stored log files via secure SFTP connection.
SFTP Port	Specify a port number for SFTP connection. The gateway will listen for incoming SFTP connections on the specified port. Value Range: 1 ~ 65535.
Save	Click **Save** to save the settings.

3.7.3.2 User Account

To access this page, click **Administration** > **FTP** > **User Account**.

User Account allows user to setup user accounts for logging to the embedded FTP and SFTP server to retrieve the interested fog files.

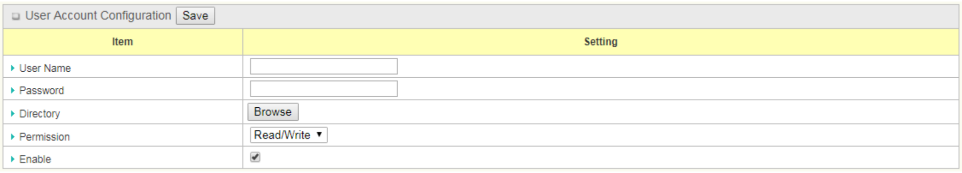


User Account List Add Delete

ID	User Name	Password	Directory	Permission	Enable	Actions

Figure 3.179 Administration > FTP > User Account

When **Add** button is applied, the **User Account Configuration** screen appears.



User Account Configuration Save

Item	Setting
User Name	
Password	
Directory	Browse
Permission	Read/Write ▾
Enable	☑

Figure 3.180 Administration > FTP > User Account

The following table describes the items in the previous figure.

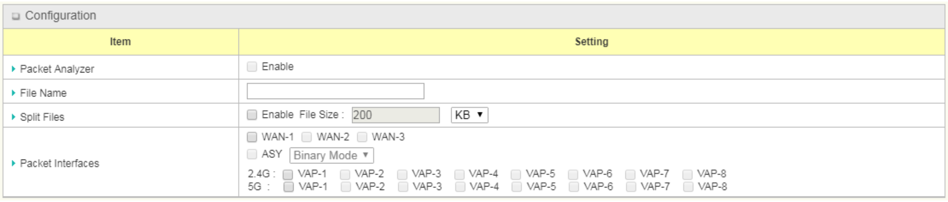
Item	Description
User Name	Enter the user account for login to the FTP server. Value Range: 1 ~ 15 characters.
Password	Enter the user password for login to the FTP server.
Directory	Select a root directory after user login.
Permission	Select the read/write permission. ***Note:*** *The embedded FTP server is only for log downloading, so no any write permission is implemented for user file upload to the storage, even Read/Write option is selected.*
Enable	Check **Enable** checkbox to activate the FTP user account.
Save	Click **Save** to save the settings.

3.7.4 Diagnostic

3.7.4.1 Packet Analyzer

To access this page, click **Administration** > **Diagnostic** > **Packet Analyzer**.

The Packet Analyzer can capture packets depend on user settings. User can specify interfaces to capture packets and filter by setting rule. Ensure the log storage is available (either embedded SD-Card or external USB Storage), otherwise Packet Analyzer cannot be enabled.



Configuration

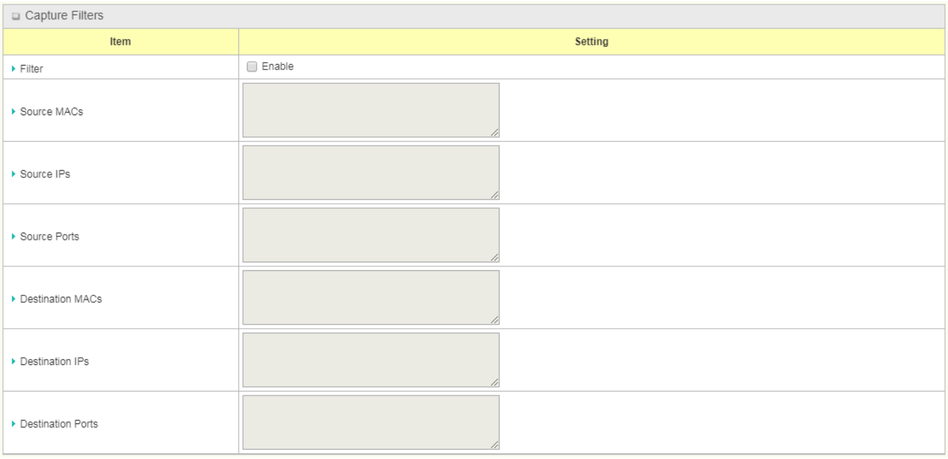
Item	Setting
Packet Analyzer	□ Enable
File Name	
Split Files	□ Enable File Size : 200 KB ▾
Packet Interfaces	□ WAN-1 □ WAN-2 □ WAN-3 □ ASY Binary Mode ▾ 2.4G : □ VAP-1 □ VAP-2 □ VAP-3 □ VAP-4 □ VAP-5 □ VAP-6 □ VAP-7 □ VAP-8 5G : □ VAP-1 □ VAP-2 □ VAP-3 □ VAP-4 □ VAP-5 □ VAP-6 □ VAP-7 □ VAP-8

Figure 3.181 Administration > Diagnostic > Packet Analyzer > Configuration

The following table describes the items in the previous figure.

Item	Description
Packet Analyzer	Check **Enable** checkbox to activate the Packet Analyzer function. If you cannot enable the checkbox, please check if the storage is available or not. Plug in the USB storage and then enable the Package Analyzer function.
File Name	Enter the file name to save the captured packets in log storage. If Split Files option is also enabled, the file name will be appended with an index code "_<index>". The extension file name is .pcap.
Split Files	Check **Enable** checkbox to split file whenever log file reaching the specified limit. If the **Split Files** option is enabled, you can further specify the File Size and Unit for the split files. Value Range: 10 ~ 99999. ***Note:*** *File Size cannot be less than 10 KB*
Packet Interfaces	Define the interface(s) that Packet Analyzer should work on. At least, one interface is required, but multiple selections are also accepted. The supported interfaces can be: ■ **WAN:** When the WAN is enabled at Physical Interface, it can be selected here. ■ **ASY:** This means the serial communication interface. It is used to capture packets appearing in the Field Communication. Therefore, it can only be selected when specific field communication protocol, like Modbus, is enabled. Select **Binary mode** or **String mode** for the serial interface. ■ **VAP:** This means the virtual AP. When WiFi and VAP are enabled, it can be selected here.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

Once you enabled the Packet Analyzer function on specific Interface(s), you can further specify some filter rules to capture the packets which matched the rules.



Capture Filters

Item	Setting
Filter	□ Enable
Source MACs	
Source IPs	
Source Ports	
Destination MACs	
Destination IPs	
Destination Ports	

Figure 3.182 Administration > Diagnostic > Packet Analyzer > Capture Filters

The following table describes the items in the previous figure.

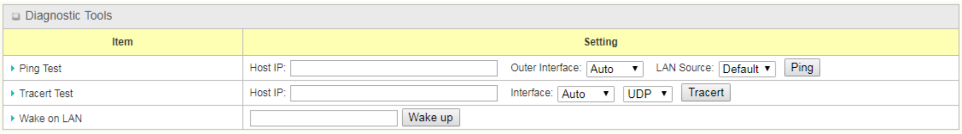
Item	Description
Filter	Check **Enable** checkbox to activate the capture filter function.
Source MACs	Define the filter rule with source MACs, which means the source MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with “;”. e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.
Source IPs	Define the filter rule with source IPs, which means the source IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with “;”. e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.
Source Ports	Define the filter rule with source ports, which means the source port of packets. The packets will be captured when match any port in the rule. Up to 10 ports are supported, but they must be separated with “;”. e.g. 80; 53 Value Range: 1 ~ 65535.
Destination MACs	Define the filter rule with destination MACs, which means the destination MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with “;”. e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.
Destination IPs	Define the filter rule with destination IPs, which means the destination IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with “;”. e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.
Destination Ports	Define the filter rule with destination Ports, which means the destination port of packets. The packets will be captured when match any port in the rule. Up to 10 ports are supported, but they must be separated with “;”. e.g. 80; 53 Value Range: 1 ~ 65535.

Item	Description
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.7.4.2 Diagnostic Tools

To access this page, click **Administration** > **Diagnostic** > **Diagnostic Tools**.

The **Diagnostic Tools** provide some frequently used network connectivity diagnostic tools (approaches) for the network administrator to check the device connectivity.



Diagnostic Tools

Item	Setting
Ping Test	Host IP: Outer Interface: Auto LAN Source: Default Ping
Tracert Test	Host IP: Interface: Auto UDP Tracert
Wake on LAN	Wake up

Figure 3.183 Administration > Diagnostic > Diagnostic Tools

The following table describes the items in the previous figure.

Item	Description
Ping Test	This allows you to specify an IP/FQDN and the test interface (LAN, WAN, or Auto), so system will try to ping the specified device to test whether it is alive after clicking **Ping** button. A test result window will appear beneath it.
Tracert Test	Trace route (tracert) command is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Trace route proceeds until all (three) sent packets are lost for more than twice, then the connection is lost and the route cannot be evaluated. First, you need to specify an IP/FQDN, the test interface (LAN, WAN, or Auto) and the protocol (UDP or ICMP), and by default, it is **UDP**. Then, system will try to trace the specified host to test whether it is alive after clicking **Tracert**. A test result window will appear beneath it.
Wake on LAN	Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can specify the MAC address of the computer, in your LAN network, to be remotely turned on by clicking **Wake up**.
Save	Click **Save** to save the settings.

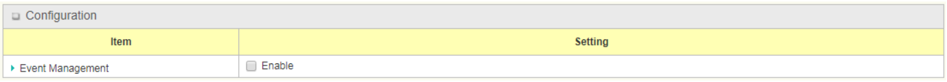
3.8 Service

3.8.1 Event Handling

Event handling is the service that allows administrator to setup the predefined events, handlers, or response behavior with individual profiles.

3.8.1.1 Configuration

To access this page, click **Service** > **Event Handling** > **Configuration**.



Configuration

Item	Setting
Event Management	□ Enable

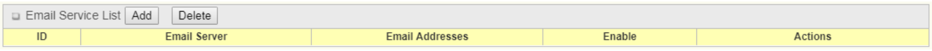
Figure 3.184 Service > Event Handling > Configuration > Configuration

Figure 3.185 Item

The following table describes the items in the previous figure.

Item	Description
Event Management	Check **Enable** checkbox to activate the event management function.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

Setup the Email Service Account for event notification. It supports up to a maximum of 5 accounts.

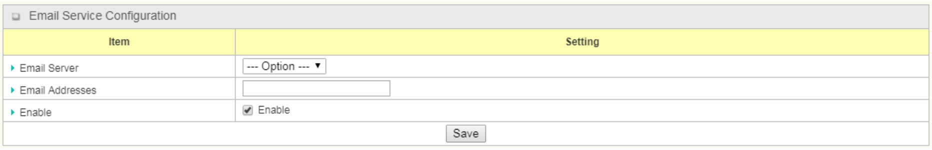


Email Service List Add Delete

ID	Email Server	Email Addresses	Enable	Actions

Figure 3.186 Service > Event Handling > Configuration > Email Service List

When **Add** button is applied, the **Email Service Configuration** screen appears.



Email Service Configuration

Item	Setting
Email Server	--- Option --- ▾
Email Addresses	
Enable	☑ Enable

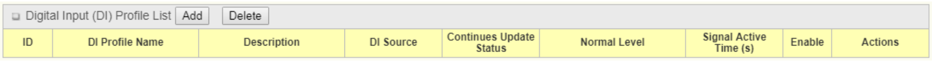
Save

Figure 3.187 Service > Event Handling > Configuration > Email Service Configuration

The following table describes the items in the previous figure.

Item	Description
Email Server	Select an Email server profile from external server setting for the email account setting.
Email Addresses	Specify the destination Email addresses.
Enable	Click **Enable** checkbox to activate this account.
Save	Click **Save** to save the settings.

Setup the Digital Input (DI) Profile rules. It supports up to a maximum of 10 profiles.

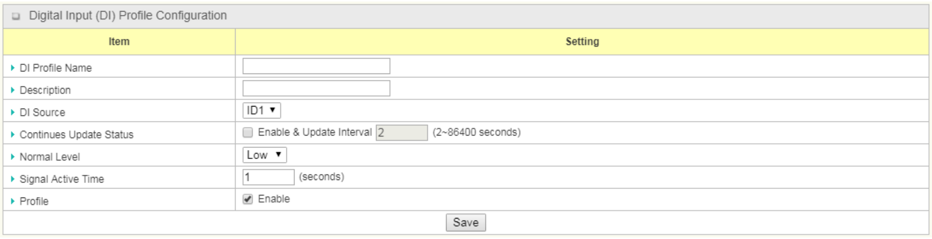


Digital Input (DI) Profile List Add Delete

ID	DI Profile Name	Description	DI Source	Continues Update Status	Normal Level	Signal Active Time (s)	Enable	Actions

Figure 3.188 Service > Event Handling > Configuration > Digital Input (DI) Profile List

When **Add** button is applied, the **Digital Input (DI) Profile Configuration** screen appears.



Digital Input (DI) Profile Configuration

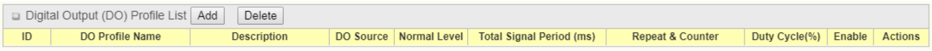
Item	Setting
DI Profile Name	
Description	
DI Source	ID1 ▾
Continues Update Status	□ Enable & Update Interval 2 (2~86400 seconds)
Normal Level	Low ▾
Signal Active Time	1 (seconds)
Profile	☑ Enable

Figure 3.189 Service > Event Handling > Configuration > Digital Input (DI) Profile Configuration

The following table describes the items in the previous figure.

Item	Description
DI Profile Name	Specify the DI profile name. Value Range: 1 ~ 32 characters.
Description	Specify a brief description for the profile.
DI Source	Specify the DI source. It could be **ID1** or **ID2**. The number of available DI source could be different for the purchased product.
Continues Update Status	Click **Enable** checkbox to enable the function. Specify the interval for the DI event. If the event condition is active for an extended period of time, the gateway sends repeated notification events for each interval. Value Range: 0 ~ 86400 seconds. ***Note:*** *To modify the number of notifications for the same situation, adjust the interval period for the application.*
Normal Level	Specify the normal level. It could be **Low** or **High**.
Signal Active Time	Specify the signal active time. Value Range: 1 ~ 10 seconds.
Profile	Click **Enable** checkbox to activate this profile setting.
Save	Click **Save** to save the settings.

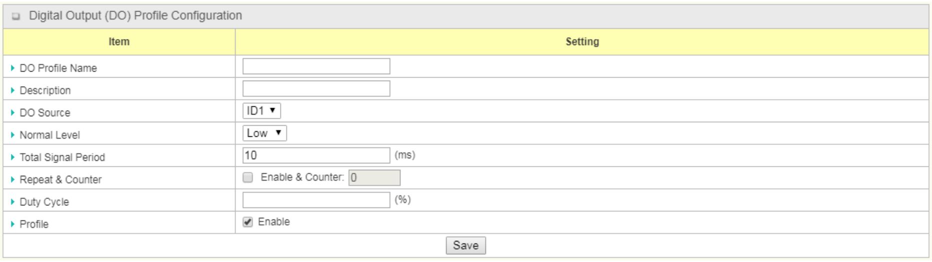
Setup the Digital Output (DO) Profile rules. It supports up to a maximum of 10 profiles.



ID	DO Profile Name	Description	DO Source	Normal Level	Total Signal Period (ms)	Repeat & Counter	Duty Cycle(%)	Enable	Actions

Figure 3.190 Service > Event Handling > Configuration > Digital Output (DO) Profile List

When **Add** button is applied, the **Digital Output (DO) Profile Configuration** screen appears.



Digital Output (DO) Profile Configuration

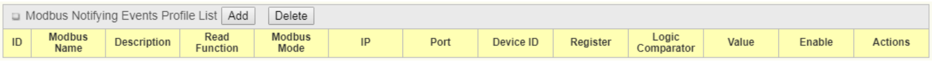
Item	Setting
DO Profile Name	
Description	
DO Source	ID1 ▾
Normal Level	Low ▾
Total Signal Period	10 (ms)
Repeat & Counter	□ Enable & Counter: 0
Duty Cycle	(%)
Profile	☑ Enable

Figure 3.191 Service > Event Handling > Configuration >Digital Output (DO) Profile Configuration

The following table describes the items in the previous figure.

Item	Description
DO Profile Name	Specify the DO profile name. Value Range: 1 ~ 32 characters.
Description	Specify a brief description for the profile.
DO Source	Specify the DO Source. It could be **ID1**.
Normal Level	Specify the normal level. It could be **Low** or **High**.
Total Signal Period	Specify the total signal period. Value Range: 10 ~ 10000 ms.
Repeat & Counter	Check **Enable** checkbox to activate the repeated Digital Output, and specify the repeat times. Value Range: 0 ~ 65535.
Duty Cycle	Specify the duty cycle for the Digital Output. Value Range: 1 ~100 %.
Profile	Click **Enable** checkbox to activate this profile setting.
Save	Click **Save** to save the settings.

Setup the Modbus Notifying Events Profile. It supports up to a maximum of 10 profiles.

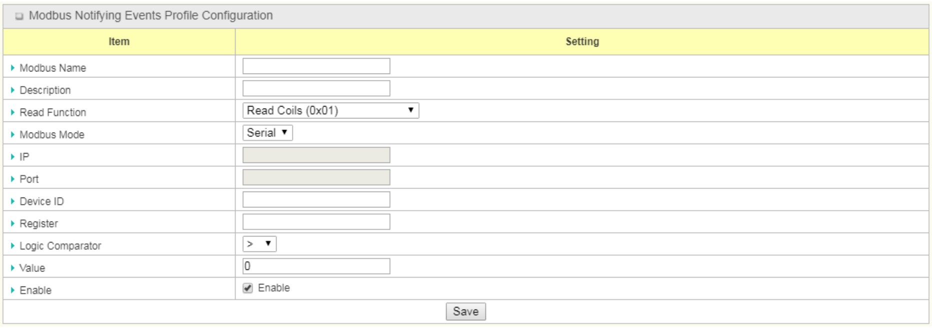


Modbus Notifying Events Profile List [Add] [Delete]

ID	Modbus Name	Description	Read Function	Modbus Mode	IP	Port	Device ID	Register	Logic Comparator	Value	Enable	Actions

Figure 3.192 Service > Event Handling > Configuration > Modbus Notifying Events Profile List

When **Add** button is applied, the **Modbus Notifying Events Profile Configuration** screen appears.



Modbus Notifying Events Profile Configuration

Item	Setting
Modbus Name	
Description	
Read Function	Read Coils (0x01) ▾
Modbus Mode	Serial ▾
IP	
Port	
Device ID	
Register	
Logic Comparator	> ▾
Value	0
Enable	☑ Enable

[Save]

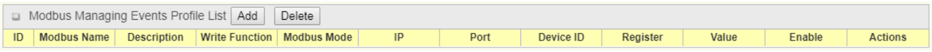
Figure 3.193 Service > Event Handling > Configuration > Modbus Notifying Events Profile Configuration

The following table describes the items in the previous figure.

Item	Description
Modbus Name	Specify the Modbus profile name. Value Range: 1 ~ 32 characters.
Description	Specify a brief description for the profile.
Read Function	Specify the read function for Notifying Events.
Modbus Mode	Specify the Modbus mode. It could be **Serial** or **TCP**.
IP	Specify the IP for TCP on Modbus mode. IPv4 format.
Port	Specify the port for TCP on Modbus mode. Value Range: 1 ~ 65535.
Device ID	Specify the device ID of the Modbus device. Value Range: 1 ~ 247.

Item	Description
Register	Specify the register number of the Modbus device. Value Range: 0 ~ 65535.
Logic Comparator	Specify the logic comparator for Notifying Events. It could be ‘>’, ‘<’, ‘=’, ‘>=’, or ‘<=’.
Value	Specify the value. Value Range: 0 ~ 65535.
Enable	Click **Enable** checkbox to activate this profile setting.
Save	Click **Save** to save the settings.

Setup the Modbus Managing Events Profile. It supports up to a maximum of 10 profiles.

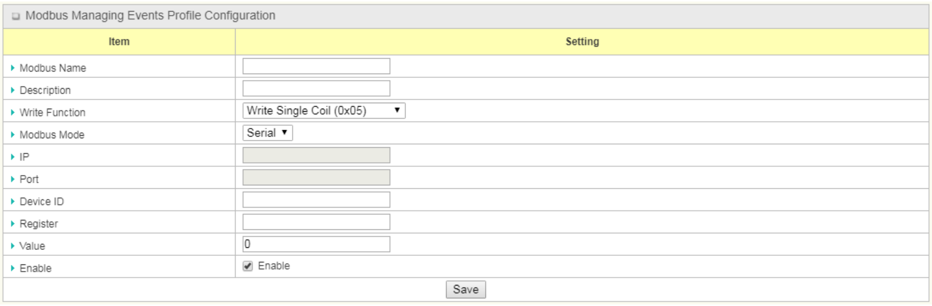


Modbus Managing Events Profile List Add Delete

ID	Modbus Name	Description	Write Function	Modbus Mode	IP	Port	Device ID	Register	Value	Enable	Actions

Figure 3.194 Service > Event Handling > Configuration > Modbus Managing Events Profile List

When **Add** button is applied, the **Modbus Managing Events Profile Configuration** screen appears.



Modbus Managing Events Profile Configuration

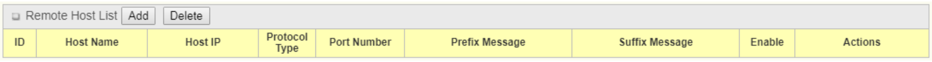
Item	Setting
Modbus Name	
Description	
Write Function	Write Single Coil (0x05) ▾
Modbus Mode	Serial ▾
IP	
Port	
Device ID	
Register	
Value	0
Enable	☑ Enable

Save

Figure 3.195 Service > Event Handling > Configuration > Modbus Managing Events Profile Configuration

The following table describes the items in the previous figure.

Item	Description
Modbus Name	Specify the Modbus profile name. Value Range: 1 ~ 32 characters.
Description	Specify a brief description for the profile.
Write Function	Specify the write function for Managing Events.
Modbus Mode	Specify the Modbus mode. It could be **Serial** or **TCP**.
IP	Specify the IP for TCP on Modbus mode. IPv4 format.
Port	Specify the port for TCP on Modbus mode. Value Range: 1 ~ 65535.
Device ID	Specify the device ID of the Modbus device. Value Range: 1 ~ 247.
Register	Specify the register number of the Modbus device. Value Range: 0 ~ 65535.
Value	Specify the value. Value Range: 0 ~ 65535.
Enable	Click **Enable** checkbox to activate this profile setting.
Save	Click **Save** to save the settings.

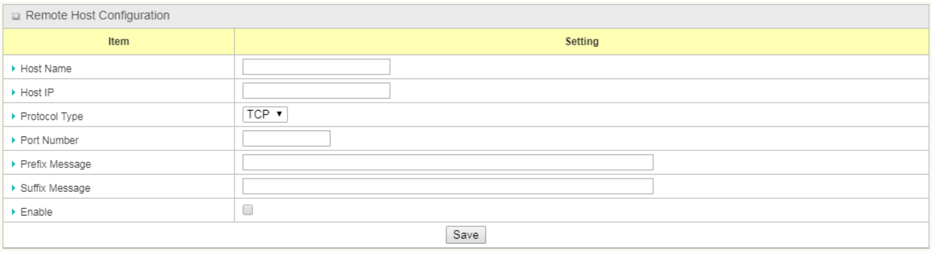


Remote Host List Add Delete

ID	Host Name	Host IP	Protocol Type	Port Number	Prefix Message	Suffix Message	Enable	Actions

Figure 3.196 Service > Event Handling > Configuration > Remote Host List

When **Add** button is applied, the **Remote Host Configuration** screen appears.



Remote Host Configuration

Item	Setting
Host Name	
Host IP	
Protocol Type	TCP ▾
Port Number	
Prefix Message	
Suffix Message	
Enable	□

Save

Figure 3.197 Service > Event Handling > Configuration > Remote Host Configuration

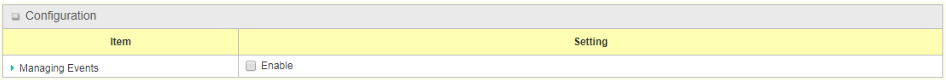
The following table describes the items in the previous figure.

Item	Description
Host Name	Specify the name of the host.
Host IP	Specify the host IP address.
Protocol Type	Select type of protocol, TCP or UDP
Port Number	Specify TCP/UDP port number.
Prefix Message	Enter message prefix.
Suffix Message	Enter message suffix.
Enable	Click **Enable** checkbox to activate this profile setting.
Save	Click **Save** to save the settings.

3.8.1.2 Managing Events

To access this page, click **Service** > **Event Handling** > **Managing Events**.

Managing Events allow administrator to define the relationship (rule) among event trigger, handlers and response.



Configuration

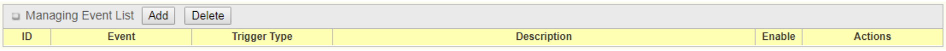
Item	Setting
Managing Events	□ Enable

Figure 3.198 Service > Event Handling > Managing Events > Configuration

The following table describes the items in the previous figure.

Item	Description
Managing Events	Check **Enable** checkbox to activate the managing events function.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

Setup the Managing Event rules. It supports up to a maximum of 128 rules.

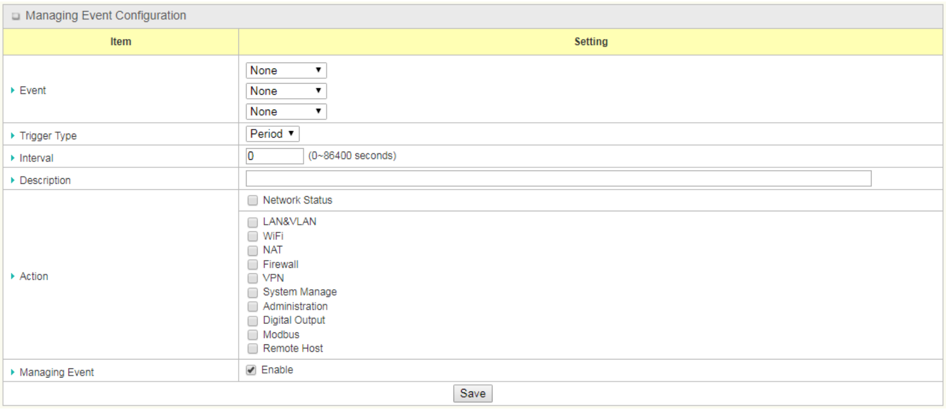


Managing Event List Add Delete

ID	Event	Trigger Type	Description	Enable	Actions

Figure 3.199 Service > Event Handling > Managing Events > Managing Event List

When **Add** button is applied, the **Managing Event Configuration** screen appears.



Managing Event Configuration

Item	Setting
Event	None ▾ None ▾ None ▾
Trigger Type	Period ▾
Interval	0 (0~86400 seconds)
Description	
Action	□ Network Status □ LAN&VLAN □ WiFi □ NAT □ Firewall □ VPN □ System Manage □ Administration □ Digital Output □ Modbus □ Remote Host
Managing Event	☑ Enable

Figure 3.200 Service > Event Handling > Managing Events > Managing Event Configuration

The following table describes the items in the previous figure.

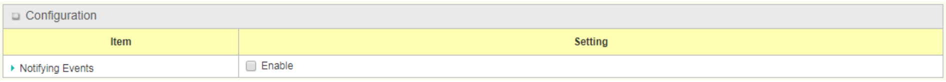
Item	Description
Event	Specify the event type (**SNMP Trap**, **Digital Input**, or **None**) and an event identifier / profile. ■ **SNMP:** Select **SNMP Trap** and fill the message in the textbox to specify SNMP Trap Event. ■ **Digital Input:** Select **Digital Input** and a DI profile you defined to specify a certain Digital Input Event. ***Note:*** *The available event type could be different for the purchased product.*
Trigger Type	Specify the trigger type (Period or Once). ■ **Period:** Event will be executed in a period set by Interval below. ■ **Once:** Event will be executed just once.
Interval	The function is only available when **Trigger Type** is **Period**. Time interval for event execution in period. Value Range: 0 ~ 86400 seconds.
Description	Enter a brief description for the Managing Event.
Action	Specify network status, or at least one rest action to take when the expected event is triggered. ■ **Network Status:** Select **Network Status** checkbox to get the network status as the action for the event. ■ **LAN&VLAN:** Select **LAN&VLAN** checkbox and the interested sub-items (Port link On/Off), the gateway will change the settings as the action for the event. ■ **WiFi:** Select **WiFi** checkbox and the interested sub-items (WiFi radio On/Off), the gateway will change the settings as the action for the event. ■ **NAT:** Select **NAT** checkbox and the interested sub-items (Virtual Server Rule On/Off, DMZ On/Off), the gateway will change the settings as the action for the even.

Item	Description
Action (Continued)	■ **Firewall:** Select **Firewall** checkbox and the interested sub-items (Remote Administrator Host ID On/Off), the gateway will change the settings as the action for the event. ■ **VPN:** Select **VPN** checkbox and the interested sub-items (IPSec Tunnel ON/Off, PPTP Client On/Off, L2TP Client On/Off, OpenVPN Client On/Off), the gateway will change the settings as the action for the event. ■ **System Manage:** Select **System Manage** checkbox and the interested sub-items (WAN SSH Service On/Off, TR-069 On/Off), the gateway will change the settings as the action for the event. ■ **Administration:** Select **Administration** checkbox and the interested sub-items (Backup Config, Restore Config, Reboot, Save Current Setting as Default), the gateway will change the settings as the action for the event. ■ **Digital Output:** Select **Digital Output** checkbox and a DO profile you defined as the action for the event. ■ Modbus: Select **Modbus** checkbox and a Modbus Managing Event profile you defined as the action for the event. ■ **Remote Host:** Select **Remote Host** checkbox and a remote host profile you defined as the action for the event. ***Note:*** *The available event type could be different for the purchased product.*
Managing Event	Click **Enable** checkbox to activate this Managing Event setting.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

3.8.1.3 Notifying Events

To access this page, click **Service** > **Event Handling** > **Notifying Events**.

Notifying Events Setting allows administrator to define the relationship (rule) between event trigger and handlers.



Configuration

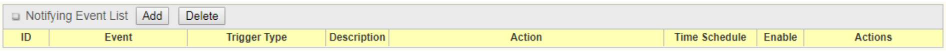
Item	Setting
Notifying Events	□ Enable

Figure 3.201 Service > Event Handling > Notifying Events > Configuration

The following table describes the items in the previous figure.

Item	Description
Notifying Events	Check **Enable** checkbox to activate the Notifying Events function.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

Setup your Notifying Event rules. It supports up to a maximum of 128 rules.

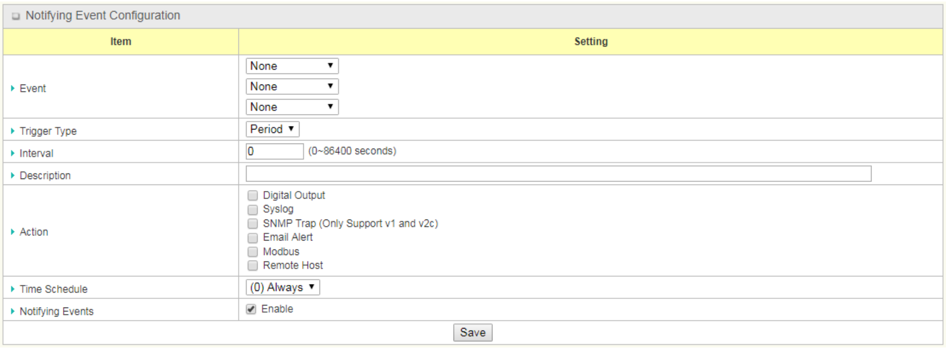


Notifying Event List Add Delete

ID	Event	Trigger Type	Description	Action	Time Schedule	Enable	Actions

Figure 3.202 Service > Event Handling > Notifying Events > Notifying Event List

When **Add** button is applied, the **Notifying Event Configuration** screen appears.



Notifying Event Configuration

Item	Setting
Event	None ▾ None ▾ None ▾
Trigger Type	Period ▾
Interval	0 (0~86400 seconds)
Description	
Action	□ Digital Output □ Syslog □ SNMP Trap (Only Support v1 and v2c) □ Email Alert □ Modbus □ Remote Host
Time Schedule	(0) Always ▾
Notifying Events	☑ Enable

Figure 3.203 Service > Event Handling > Notifying Events > Notifying Event Configuration

The following table describes the items in the previous figure.

Item	Description
Event	Specify the event type and corresponding event configuration. The supported event type could be: ■ **Digital Input:** Select **Digital Input** and a DI profile you defined to specify a certain Digital Input Event. ■ **WAN:** Select **WAN** and a trigger condition to specify a certain WAN Event. ■ **LAN&VLAN:** Select **LAN&VLAN** and a trigger condition to specify a certain LAN&VLAN Event. ■ **WiFi:** Select **WiFi** and a trigger condition to specify a certain WiFi Event. ■ **DDNS:** Select **DDNS** and a trigger condition to specify a certain DDNS Event. ■ **Administration:** Select **Administration** and a trigger condition to specify a certain Administration Event. ■ **Modbus:** Select **Modbus** and a Modbus Notifying Event profile you defined to specify a certain Modbus Event. ***Note:*** *The available event type could be different for the purchased product.*
Trigger Type	Specify the trigger type (**Period** or **Once**). ■ **Period:** Event will be executed in a period set by Interval below. ■ **Once:** Event will be executed just once.
Interval	The function is only available when **Trigger Type** is **Period**. Time interval for event execution in period. Value Range: 0 ~ 86400 seconds.
Description	Enter a brief description for the Notifying Event.

Item	Description
Action	Specify at least one action to take when the expected event is triggered. ■ **Digital Output:** Select **Digital Output** and a DO profile you defined as the action for the event. ■ **Syslog:** Select **Syslog** and select/unselect the **Enable** checkbox to as the action for the event. ■ **SNMP Trap:** Select **SNMP Trap**, and the gateway will send out SNMP trap to the defined SNMP Event Receivers as the action for the event. ■ **Email Alert:** Select **Email Alert**, and the gateway will send out an Email to the defined Email accounts as the action for the event. ■ **Modbus:** Select **Modbus** and a Modbus Notifying Event profile you defined as the action for the event. ■ **Remote Host:** Select **Remote Host** and a Remote Host profile you defined as the action for the event. ***Note:*** *The available event type could be different for the purchased product.*
Time Schedule	Select a time scheduling rule for the Notifying Event.
Notifying Events	Click **Enable** checkbox to activate this Notifying Event setting.
Save	Click **Save** to save the settings.
Undo	Click **Undo** to cancel the settings.

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com