

EKI-1652WT Series

EN50155 Industrial M12 WiFi/LTE Router

ADVANTECH

Enabling an Intelligent Planet

Copyright

The documentation and the software included with this product are copyrighted 2024 by Advantech Co., Ltd. All rights are reserved. Advantech Co., Ltd. reserves the right to make improvements in the products described in this manual at any time without notice. No part of this manual may be reproduced, copied, translated or transmitted in any form or by any means without the prior written permission of Advantech Co., Ltd. Information provided in this manual is intended to be accurate and reliable. However, Advantech Co., Ltd. assumes no responsibility for its use, nor for any infringements of the rights of third parties, which may result from its use.

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 (5 years)

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

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 / Cellular Router
- 13 x Antennas

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

Chapter 1	Introduction.....	1
1.1	Overview	2
1.2	Device Features	2
1.3	Benefits	2
1.4	Specifications	2
1.5	Dimensions	4
Chapter 2	Getting Started.....	5
2.1	Hardware.....	6
2.1.1	Front View	6
2.1.2	Top View	6
2.1.3	Bottom View.....	7
2.1.4	LED Indicators	7
2.2	Connecting Hardware	9
2.2.1	SIM Cards	9
2.2.2	Wall Mounting	13
2.2.3	Wireless Connection	14
2.2.4	Network Connection.....	15
2.3	Alarm Contact for Monitoring Internal Power	16
2.3.1	Power Connection.....	16
Chapter 3	Web Interface	21
3.1	Log In	22
3.1.1	Changing Default Password	23
3.2	Overview	24
3.3	Interface	27
3.3.1	LAN	27
3.3.2	ETHWAN	28
3.3.3	WLAN.....	31
3.3.4	Cellular.....	39
3.4	Networking	41
3.4.1	Static Route	41
3.4.2	Forwarding	42
3.4.3	Security	43
3.4.4	OpenVPN.....	44
3.4.5	IPSEC VPN.....	47
3.4.6	GRE	50
3.4.7	QoS Settings.....	51
3.4.8	WAN Handover	52
3.5	L2 Switch.....	54
3.5.1	Port Mirror	54
3.5.2	Storm Control.....	54
3.5.3	LLDP	56
3.6	Management	58
3.6.1	Password Manager	58
3.6.2	Syslog	58
3.6.3	NTP / Time.....	59
3.6.4	Applications.....	60
3.6.5	Configuration Manager	61
3.6.6	Firmware Upgrade	61
3.6.7	Reset System.....	62

	3.6.8	Reboot Device	62
	3.6.9	Apply Configuration	62
3.7		Tools	63
	3.7.1	Diagnostics	63
	3.7.2	GPS	64

List of Figures

Figure 1.1	Dimensions.....	4
Figure 2.1	Front View	6
Figure 2.2	Top View.....	6
Figure 2.3	Bottom View	7
Figure 2.4	System LED Panel	7
Figure 2.5	SIM Population Matrix	9
Figure 2.6	LTE Module Installation Order.....	9
Figure 2.7	LTE Module Installation Order.....	10
Figure 2.8	Releasing a Front Panel.....	11
Figure 2.9	Opening a Front Panel	11
Figure 2.10	Unlocking a Slot Cover.....	12
Figure 2.11	Installing a SIM Card	12
Figure 2.12	Installing a Front Panel.....	12
Figure 2.13	Securing a Front Panel.....	13
Figure 2.14	Wall Mount Installation	14
Figure 2.15	Installing an Antenna	14
Figure 2.16	Positioning the Antenna.....	15
Figure 2.17	M12 X-Coded Connector Pin Assignment.....	15
Figure 2.18	Alarm Contact Pin Assignment.....	16
Figure 2.19	Power Wiring for EKI-1652WT Series	17
Figure 2.20	Grounding Connection.....	18
Figure 2.21	Removing a Protection Cap.....	19
Figure 2.22	Installing the Power Cable.....	19
Figure 2.23	Removing the Power Cable.....	20
Figure 2.24	Standard M12 4 Poles Male DC Power Input Connector	20
Figure 3.1	Login Screen	22
Figure 3.2	Management > Password Manager.....	23
Figure 3.3	Overview.....	24
Figure 3.4	Overview Continued	24
Figure 3.5	Overview Continued	25
Figure 3.6	Interface > LAN	27
Figure 3.7	Interface > ETHWAN > PPTP	28
Figure 3.8	Interface > ETHWAN > PPPoE	29
Figure 3.9	Interface > ETHWAN > Static.....	30
Figure 3.10	Interface > ETHWAN.....	30
Figure 3.11	Interface > ETHWAN.....	31
Figure 3.12	WLAN > Basic	31
Figure 3.13	WLAN > Operation Mode > Wireless WAN	33
Figure 3.14	1 WLAN > Advanced	34
Figure 3.15	Interface > WLAN > Security > Security Mode.....	35
Figure 3.16	Interface > WLAN > Security > Security Mode > WEP.....	35
Figure 3.17	Interface > WLAN > Security > Security Mode > WPA-Personal	36
Figure 3.18	Interface > WLAN > Security > Security Mode.....	37
Figure 3.19	Interface > WLAN > Statistics.....	37
Figure 3.20	Interface > WLAN > Traffic Control	38
Figure 3.21	Interface > WLAN > Log.....	39
Figure 3.22	Interface > Cellular > Basic	39
Figure 3.23	Interface > Cellular > SIM 1	40
Figure 3.24	Networking > Static Route.....	41
Figure 3.25	Networking > Forwarding > Port Forwarding.....	42
Figure 3.26	Networking > Forwarding > DMZ.....	42
Figure 3.27	Networking > Security > Filter	43
Figure 3.28	Networking > OpenVPN > Tunnel 1	44
Figure 3.29	Networking > IPSEC VPN	47
Figure 3.30	Networking > IPSEC VPN	47
Figure 3.31	Networking > IPSEC VPN	48

Figure 3.32	Networking > GRE> Tunnel 1	50
Figure 3.33	Networking > QoS Settings> QoS Settings	51
Figure 3.34	Networking > QoS Settings> QoS IP Base Rules	51
Figure 3.35	Networking > QoS Settings> QoS Protocol Base Rules	52
Figure 3.36	Networking > WAN Handover	52
Figure 3.37	L2 Switching > Port Mirror	54
Figure 3.38	Security > Storm Control > Global Settings	54
Figure 3.39	Security > Storm Control > Port Settings	55
Figure 3.40	Management > LLDP > LLDP System Settings	56
Figure 3.41	Management > LLDP > LLDP Remote Device Info	57
Figure 3.42	Management > Password Manager	58
Figure 3.43	Management > Syslog	58
Figure 3.44	Management > NTP / Time	59
Figure 3.45	Management > Applications	60
Figure 3.46	Management > Configuration Manager	61
Figure 3.47	Management > Firmware Upgrade	61
Figure 3.48	Management > Reset System	62
Figure 3.49	Management > Reboot Device	62
Figure 3.50	Management > Apply Configuration	62
Figure 3.51	Tools > Diagnostics	63
Figure 3.52	Tools > GPS > Basic	64
Figure 3.53	Tools > GPS > GPS Report	65

Chapter 1

Introduction

1.1 Overview

The EKI-1652WT is a ruggedized, high-performance router specifically designed for the harsh operating conditions of railway environments, particularly rolling stock applications. It offers versatile connectivity options, robust construction, and reliable performance even in remote locations.

1.2 Device Features

- Multi-mode Operation: Supports AP, Bridge, and Client modes for flexible network deployment.
- Built-in LTE Module: Provides reliable WAN connectivity even when Wi-Fi infrastructure is unavailable.
- High-Speed Wi-Fi: Delivers IEEE 802.11ac dual-band a/b/g/n/ac connectivity with MIMO technology for maximum speed and range.
- Industrial-grade M12 Connectors: Ensures secure and vibration-resistant connections for harsh environments.
- Wide Operating Temperature Range: Operates flawlessly in extreme temperatures (-40°C to 75°C).
- Wide range power input 24/48/72/96/110 V_{DC}

1.3 Benefits

The EKI-1652WT is the ideal choice for railway operators seeking a dependable and versatile networking solution for their rolling stock.

- Enhanced Connectivity: Ensures reliable data transmission even in challenging railway environments.
- Flexible Deployment: Adapts to diverse network configurations and applications.
- Rugged Performance: Withstands shock, vibration, and extreme temperatures.
- Simplified Installation: M12 connectors offer quick and secure connections.
- High-Capacity Data Transfer: Ideal for video surveillance, passenger Wi-Fi, and critical data communication.

1.4 Specifications

Specifications	Description
Interface	
Power Connector	M12 A-Code male (5-pin)
Console Port	M12 A-Code female
USB Port	M12 A-Code female
Cellular Interface	
LTE Bit rate	150 Mbps (DL), 50 Mbps (UL)
LTE FDD	B1/B3/B5/B7/B8/B20
LTE TDD	B38/B40/B41
WCDMA	B1/B5/B8
No. of SIM Slots	2
SIM Card Type	Mini SIM (2FF) 1.8V and 3V
ANT Connector	2 x SMA female connector

Specifications	Description
Physical	
	Enclosure Metal shell with solid mounting kits
	Mounting Wall
	Dimensions (W x H x D) 186 x 50.1 x 104.8 mm (7.32" x 1.97" x 4.13")
	Weight 1.5 kg (3.31 lbs)
LED Display	
	System LED SYS, PWR1, PWR2, ALM
	Port LED Data
Environment	
	Operating Temperature -20 ~ 60°C (-4 ~ 140°F)
	Storage Temperature -40 ~ 80°C (-40 ~ 176°F)
	Operating Humidity 10 ~ 95% RH
WLAN Channel Support	
	IEEE 802.11b/g/gn ■ HT20 ■ FCC: CH1 ~ CH11; ETSI: CH1 ~ CH13
	IEEE 802.11gn ■ HT40 ■ FCC: CH3 ~ CH9; ETSI: CH3 ~ CH11
	IEEE 802.11a/an/ac ■ FCC: 5.15~5.25GHz;5.725~5.85GHz ■ ETSI: 5.15~5.25GHz;5.47~5.725GHz
Wireless Transmission Rates	
	Transmitted Power ■ 802.11b 20dBm ■ 802.11a 18dBm @ 6 Mbps, 15dBm @ 54 Mbps ■ 802.11g 21dBm @ 6 Mbps, 18dBm @ 54 Mbps ■ 802.11n HT20 21dBm @ MCS0/8, 16dBm @ MCS7/15 ■ 802.11n HT40 20dBm @ MCS0/8, 16dBm @ MCS7/15 ■ 802.11ac VHT20 18dBm @ MCS0; 13dBm @ MCS8 ■ 802.11ac VHT40 18dBm @ MCS0; 13dBm @ MCS9 ■ 802.11ac VHT80 18dBm @ MCS0; 13dBm @ MCS9
Receiver Sensitivity	
	802.11b Sensitivity -95 dBm @ 1 Mbps; -80 dBm @ 11 Mbps
	802.11a/g Sensitivity -94 dBm @ 6 Mbps; -80 dBm @ 54 Mbps
	802.11n HT20 -93 dBm @ MCS0; -76 dBm @ MCS7
	802.11n HT40 -92 dBm @ MCS0; -73 dBm @ MCS7
	802.11ac VHT20 -93 dBm @ MCS0; -71 dBm @ MCS8
	802.11ac VHT40 -90 dBm @ MCS0; -66 dBm @ MCS9
	802.11ac VHT80 -88 dBm @ MCS0; -65 dBm @ MCS9

Specifications	Description	
Power	Power Input	24-48V _{DC} (LV model), 72/96/110V _{DC} (HV model)
	Power Type	Dual power
	Power Consumption	14W (LV model) / 21W (HV model)
Software	Operation Modes	Access Point/Bridge/Client mode
	Management	Web UI
	Wireless	Radio on/off, WMM/Regatta Mode, Output Power Control, Fragmentation Length, Beacon interval, RTS/CTS threshold, DTIM interval
	Protocol	ARP, ICMP, IPv4, IPv6, TCP, UDP, DHCP Client, DNS, HTTP, SNTP, DHCP Server, NAT, DNS proxy, QoS, Load balancing, OpenVPN, IPsec, GRE
Regulatory Approvals	EMC	CE, FCC Part 15 Subpart B (Class B)

1.5 Dimensions

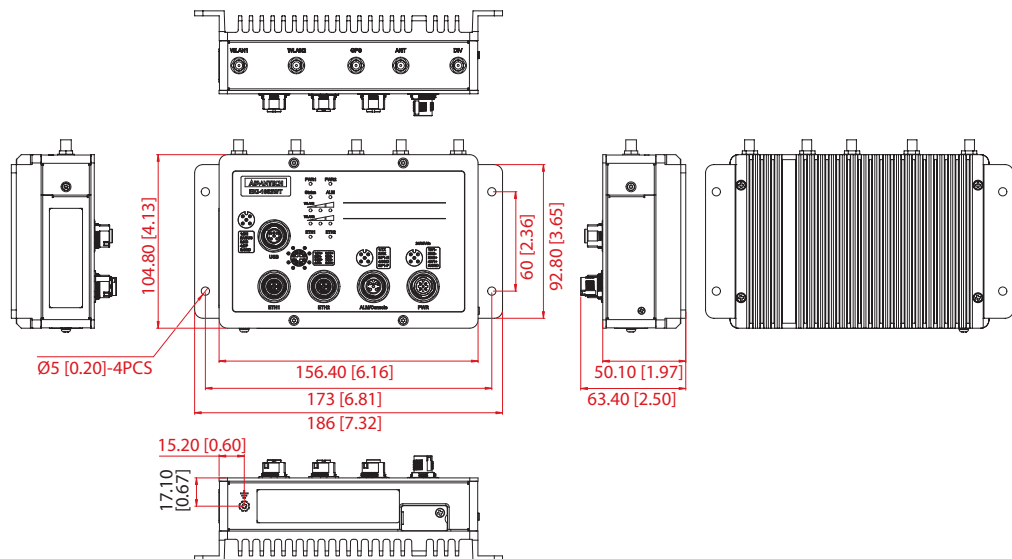


Figure 1.1 Dimensions

Chapter 2

Getting Started

2.1 Hardware

2.1.1 Front View

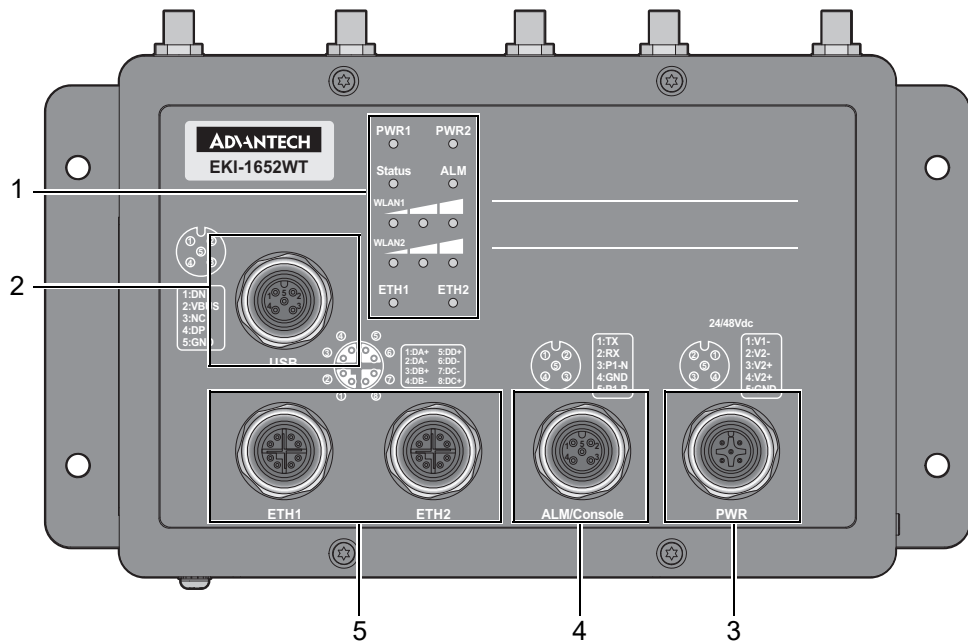


Figure 2.1 Front View

No.	Item	Description
1.	System LED panel	See “LED Indicators” on page 7 for further details.
2.	USB port	USB 2.0 Front IO (Type A)
3.	Power input port	M12 A-Code 5-pin (male) DC power connector port
4.	ALM / Console port	<div>■ M12 5-pin (female) port to attach monitoring wires</div> <div>■ M12 5-pin (female) port to access switch software</div>
5.	ETH port	M12 D-code (100Mbps) or X-Code (1000Mbps) female for Fast Ethernet

2.1.2 Top View

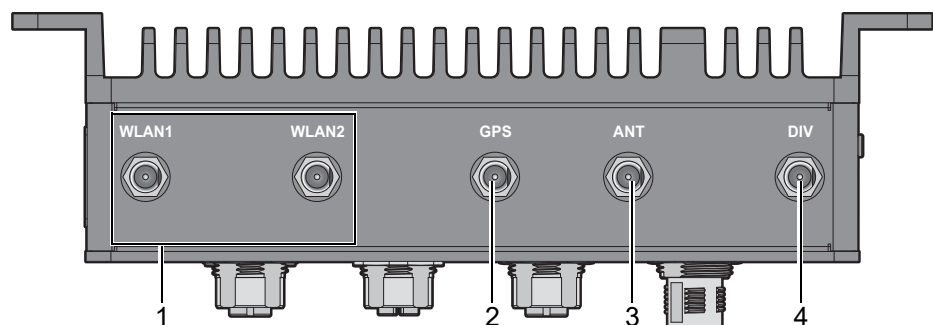


Figure 2.2 Top View

No.	Item	Description
1.	Antenna connector	Connectors for WLAN 1/2 antennas
2.	Antenna connector	Connectors for GPS antenna
3.	Antenna connector	Connector for LTE antenna port
4.	Antenna connector	Connector for Diversity antenna connector

2.1.3 Bottom View

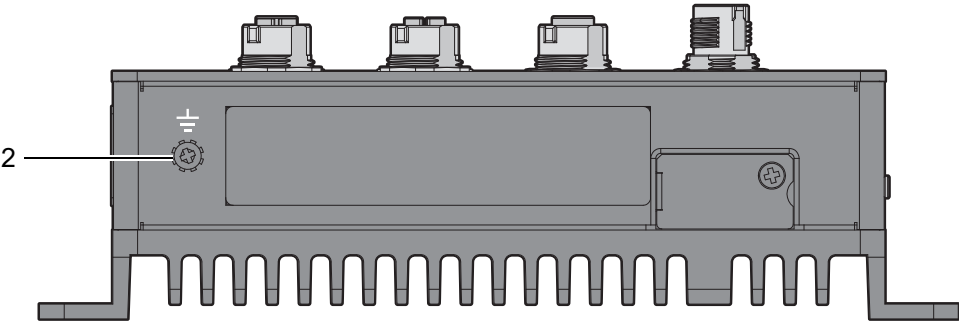


Figure 2.3 Bottom View

No.	Item	Description
1.	Ground terminal	Screw terminal used to ground chassis

2.1.4 LED Indicators

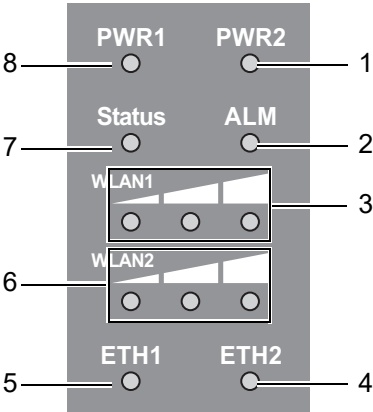


Figure 2.4 System LED Panel

No.	LED Name	LED Color	Description
1.	PWR2	Green	Power is on.
		Off	Power is off or power error condition exists.
2.	ALM	Red, solid	Defined major policies are detected,
		Off	Power off or system alarm is cleared or masked.
3.	Wireless Signal Strength	Green	AP mode
			■ Enable: LED1 on; LED2, LED3 off
			■ Disable: LED1, LED2, LED3 off
			Client mode
			LED1 On: AP connected successfully
			■ RSSI > -50dB: LED2, LED3 on
4.	ETH2	Speed	■ -50dB > RSSI > -60dB: LED2 on, LED3 blinking
			■ -60dB > RSSI > -80dB: LED2 on, LED3 off
			■ -80dB > RSSI: LED2 blinking, LED3 off
			Green on – Operating at 1000 Gigabits.
			Amber on – Operating as a 100 Mbps connection.
			Off – Operating at 10 Mbps.

No.	LED Name	LED Color	Description
5.	ETH1	Speed	Green on – Operating at 1000 Gigabits.
			Amber on – Operating at 100 Mbps.
			Off – Operating as a 10 Mbps connection.
6.	Wireless Signal Strength	Green	AP mode
			■ Enable: LED1 on; LED2, LED3 off
			■ Disable: LED1, LED2, LED3 off
			Client mode
			LED1 On: AP connected successfully
			■ RSSI > -50dB: LED2, LED3 on
7.	PWR1	Green	Power is on.
			Off
			Power is off or power error condition exists.
8.	Status	Green, solid	System is ready.
		Off	System is initiating.

2.2 Connecting Hardware

2.2.1 SIM Cards

2.2.1.1 SIM Population Matrix

Prerequisites

To configure the 4G LTE module, the following are required:

- You must have 4G LTE network coverage where your router is installed.
- You must have a service plan with a wireless service provider and a SIM card.
- You must have your access point name (APN).
- You must install the SIM card before you can configuring the 4G LTE module.

Guidelines and Limitations

The following guidelines and limitations apply to configuring the 4G LTE module:

- Throughput: the experienced throughput is dependent on the number of active users or congestion in a given network.
- Latency rates are dependent on the technology and carrier. Latency is affected by network congestion.
- Your carrier may have restrictions that are a part of the terms of service.

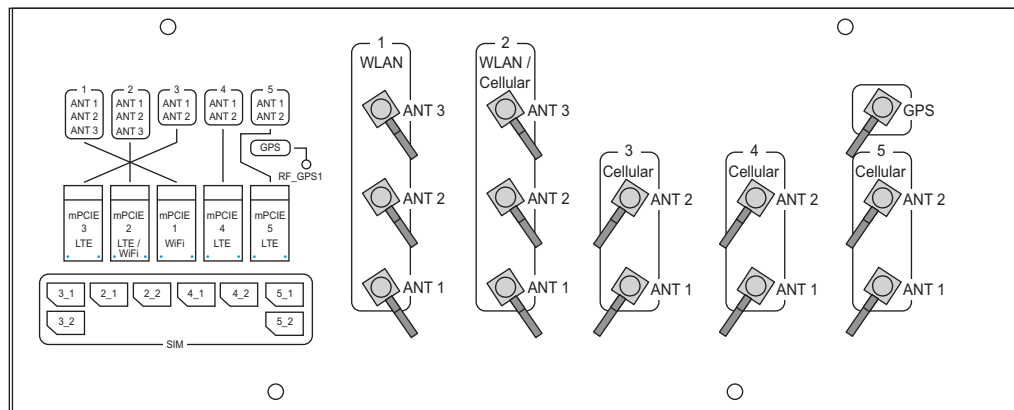


Figure 2.5 SIM Population Matrix

When installing an LTE module the specified order in which the device launches the LTE module is listed as follows: mPCIE 5 LTE -> mPCIE 4 LTE -> mPCIE 3 LTE

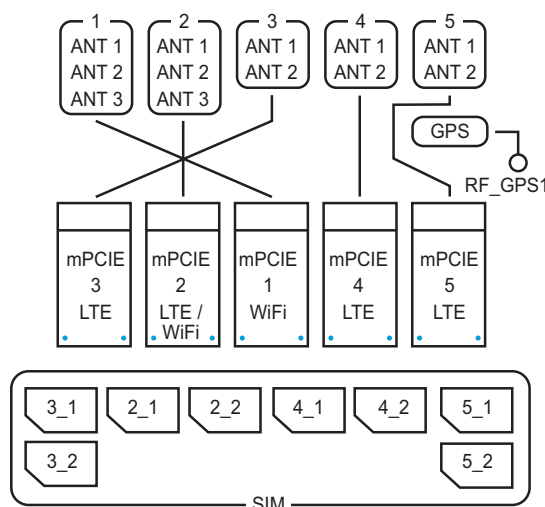


Figure 2.6 LTE Module Installation Order

The mPCIE 2 is a combo slot for WiFi/LTE as designated by the dip switch settings.

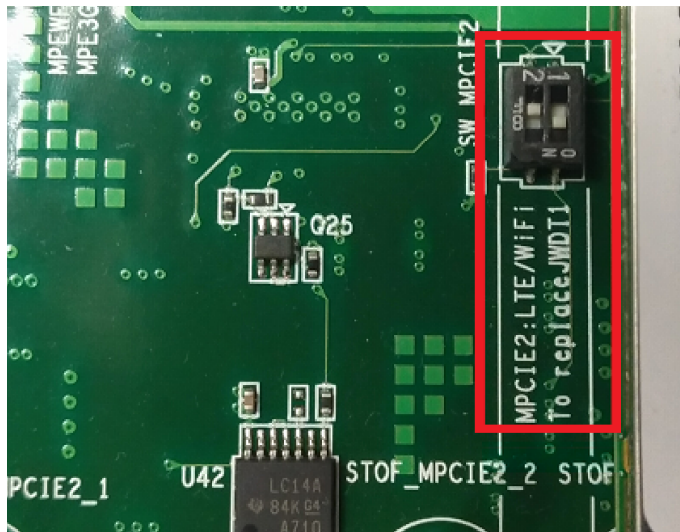


Figure 2.7 LTE Module Installation Order

In the previous figure, the DIP switch is shown. See the following for DIP switch settings:

- DIP switch 2 ON: LTE is enabled
- DIP switch 2 OFF: WiFi is enabled.

2.2.1.2 Installing a SIM Card

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.*



To install a SIM card:

1. Position the device on a clean work surface.

2. Turn the thumb screws to release the front panel.

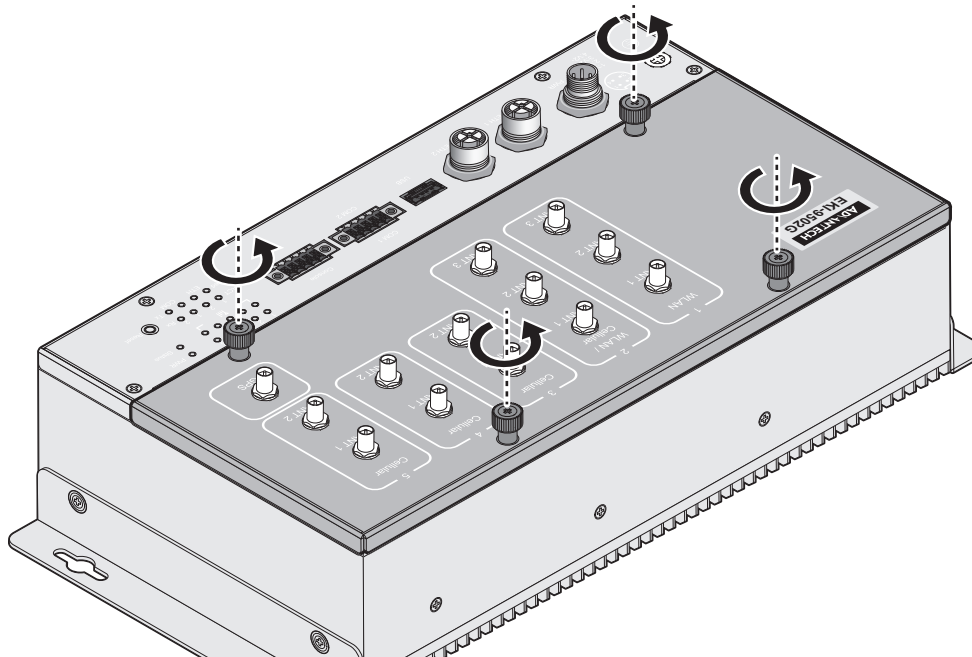


Figure 2.8 Releasing a Front Panel

3. Grasp the edge of the front panel and rotate it to open it. Do not completely pull off the front panel to prevent the connected cables from detaching or possible damage.

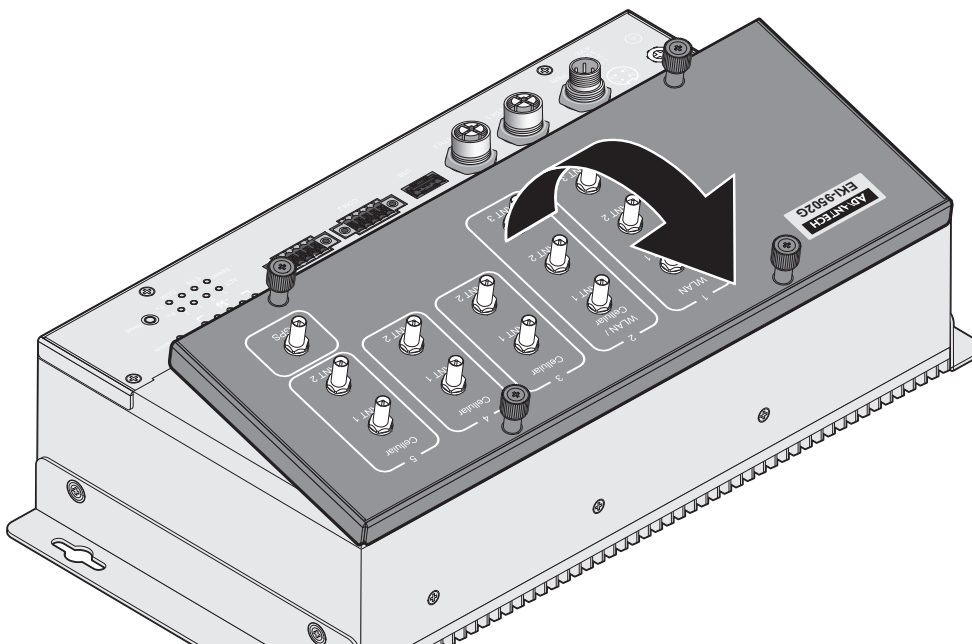


Figure 2.9 Opening a Front Panel

4. Locate the SIM slot for installation, see “SIM Population Matrix” on page 9 for further information.

5. Slide the slot cover to unlock it and rotate it open.

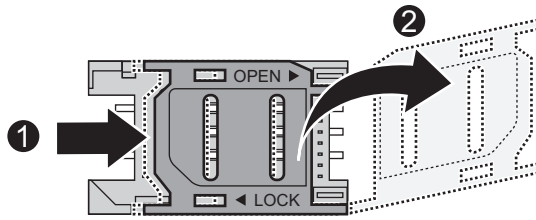


Figure 2.10 Unlocking a Slot Cover

6. Insert the SIM card into the slot with the gold contacts facing down, refer to the markings displayed next to the slot for correct placement.
7. Rotate the slot cover to the closed position and slide it to lock the SIM card in place.

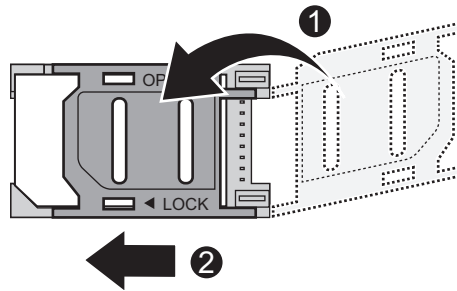


Figure 2.11 Installing a SIM Card

8. Rotate the front panel over the device and install it. Make sure the screw holes on the cover are aligned with those on the device.

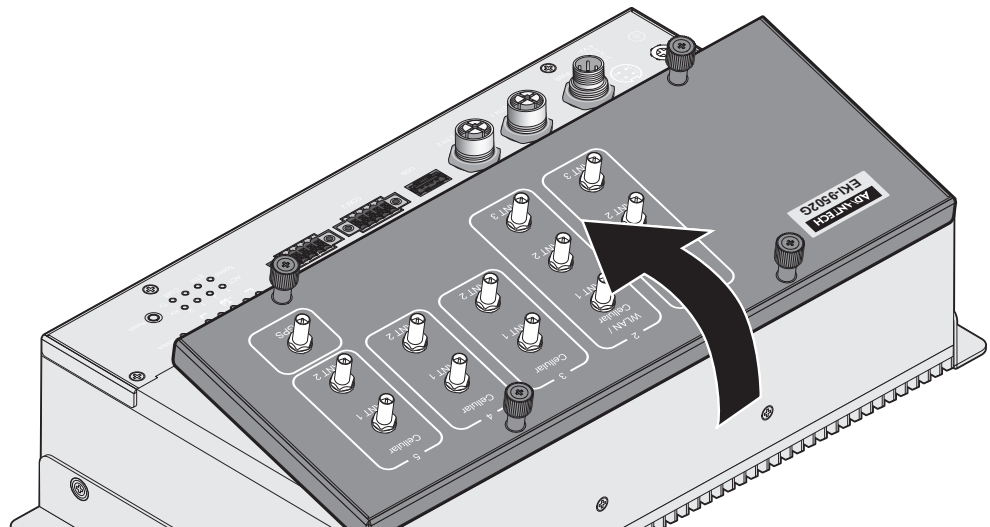


Figure 2.12 Installing a Front Panel

9. Lock the front panel in place by securing it with the screws.

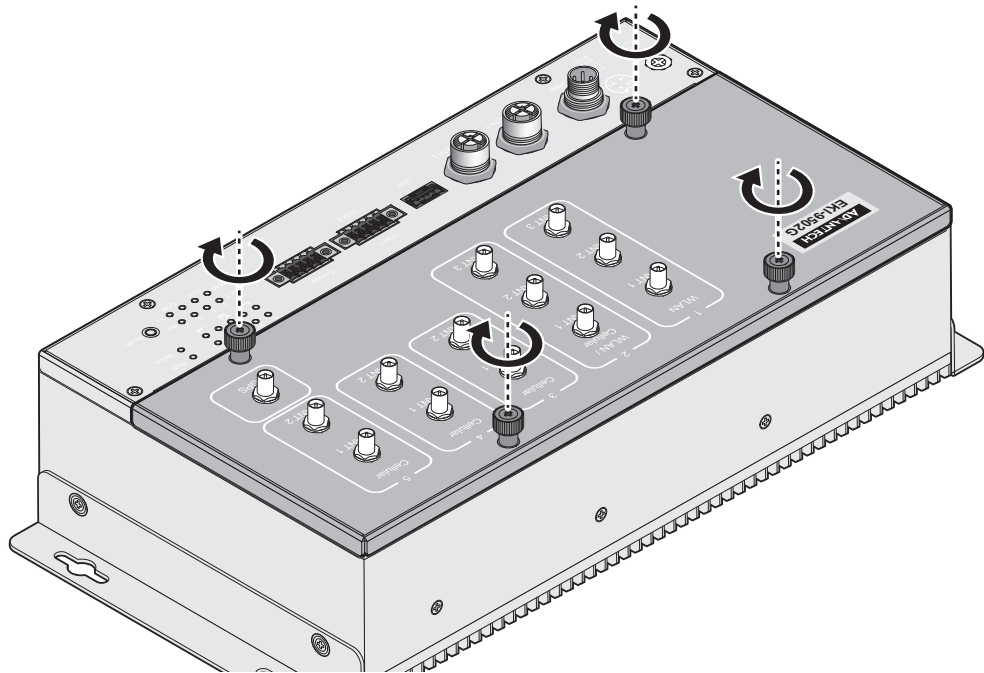


Figure 2.13 Securing a Front Panel

2.2.2 Wall Mounting

The wall mounting option provides protection from shock and vibration when in operation.

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



To wall mount the device

1. Locate the mounting brackets and position them on the sides of the device.
2. Secure the brackets to the device with the provided screws.
3. On the installation site, place the device firmly against the wall. Make sure the device is vertically and horizontally level.
4. Insert a pencil or pen through the screw holes on the mounting brackets to mark the location of the screw holes on the wall.
5. Remove the device from the wall and drill holes over each marked location (4) on the wall. If installing on a wooden surface, keeping in mind that the holes must accommodate wall sinks in addition to the screws. If necessary, insert the wall sinks into the drilled screw holes.
6. Reposition the device over the marked area and align the screw holes.
7. Starting from one corner insert a screw and half tighten them to install the device.

8. Starting from one corner and continuing diagonally, tighten each screw to secure the mounted device.

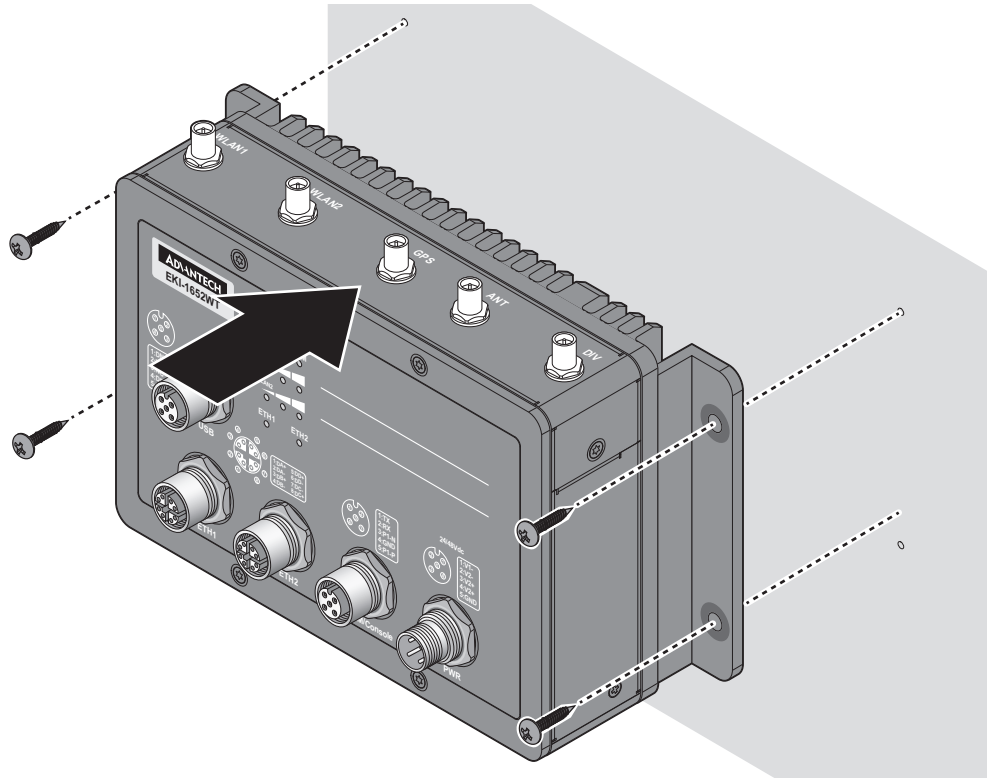


Figure 2.14 Wall Mount Installation

2.2.3 Wireless Connection

WLAN and LTE antennas are supported by the device. To install an antenna see the following information.

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

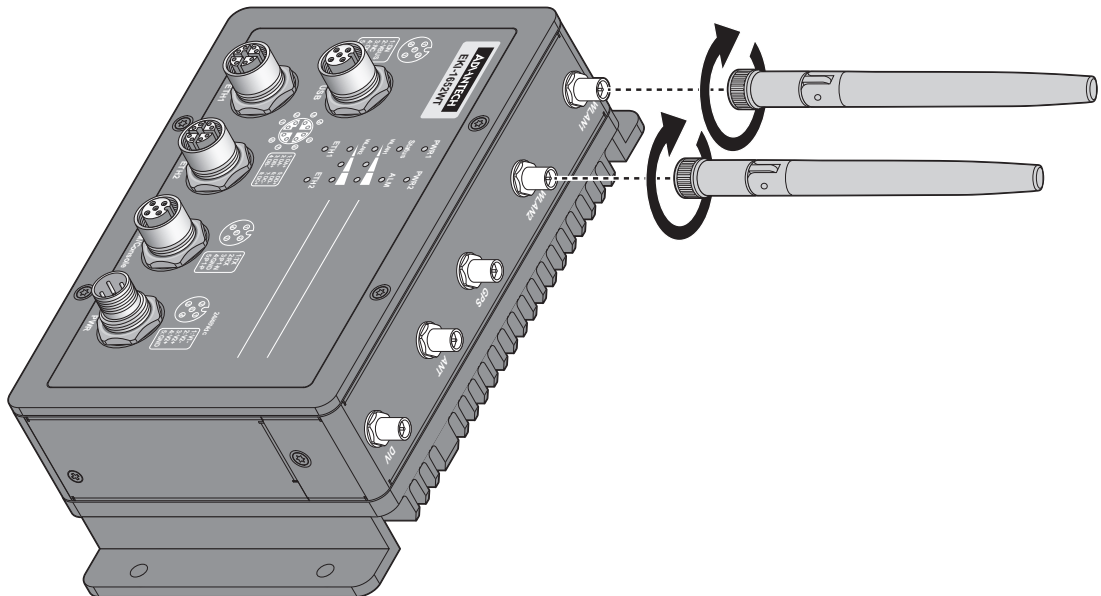


Figure 2.15 Installing an Antenna

2. Position the antenna for optimal signal strength.

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

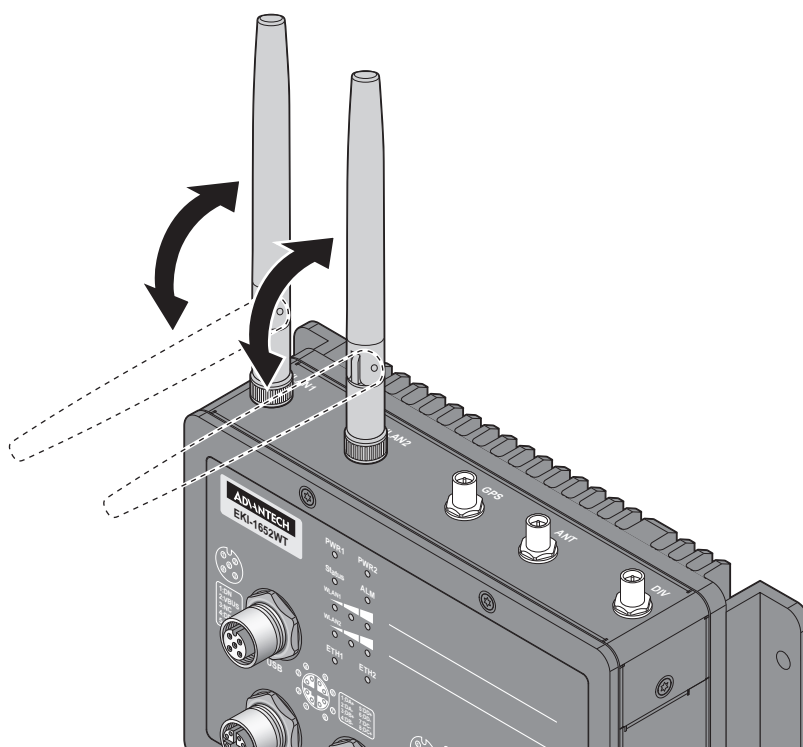


Figure 2.16 Positioning the Antenna

2.2.4 Network Connection

The managed Ethernet models have Gigabit Ethernet ports (8-pin shielded M12 connector with X coding) circular connectors. The 10/100/1000Mbps ports located on the switch's front side are used to connect to Ethernet-enabled devices.

2.2.4.1 M12 X-Coded Connector Pin Assignment

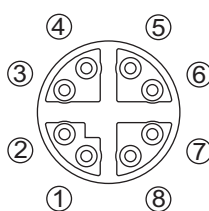


Figure 2.17 M12 X-Coded Connector Pin Assignment

Pin	Description
1	DA+
2	DA-
3	DB+
4	DB-
5	DD+
6	DD-
7	DC-
8	DC+

2.3 Alarm Contact for Monitoring Internal Power

The Alarm Contacts feature, standard on EKI-1652WT Series, provides one Form Normally Closed (NC) contact to which the user can attach one set of status monitoring wires at the green terminal block.

The NC Alarm Contact is held closed when there is power on the mainboard inside of the switch. This provides a “Hardware Alarm” (labeled H/W) because the NC contacts will open when internal power is lost, either from an external power down condition or by the failure of the power supply inside of the EKI-1652WT Series.

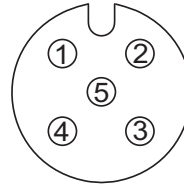


Figure 2.18 Alarm Contact Pin Assignment

Pin	Description
1	P1-N
2	P1-P
3	P1-N
4	P2-P
5	NA

2.3.1 Power Connection

2.3.1.1 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 device can be powered by using the same DC source used to power other devices. A DC voltage range of 24 to 48 V_{DC} must be applied, 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. Dual power inputs are supported and allow you to connect a backup power source.

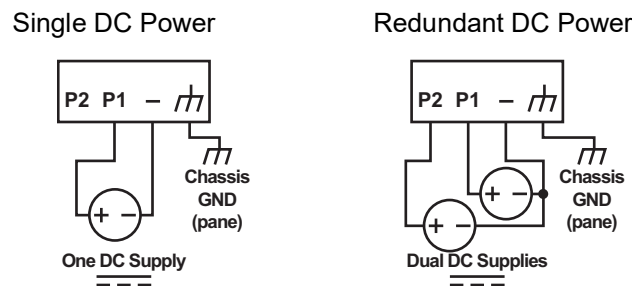


Figure 2.19 Power Wiring for EKI-1652WT Series

2.3.1.2 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 mm²). Torque value 7 lb-in.
- The cross sectional area of the earthing conductors shall be at least 3.31 mm².
- 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.*



2.3.1.3 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 grills.



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.

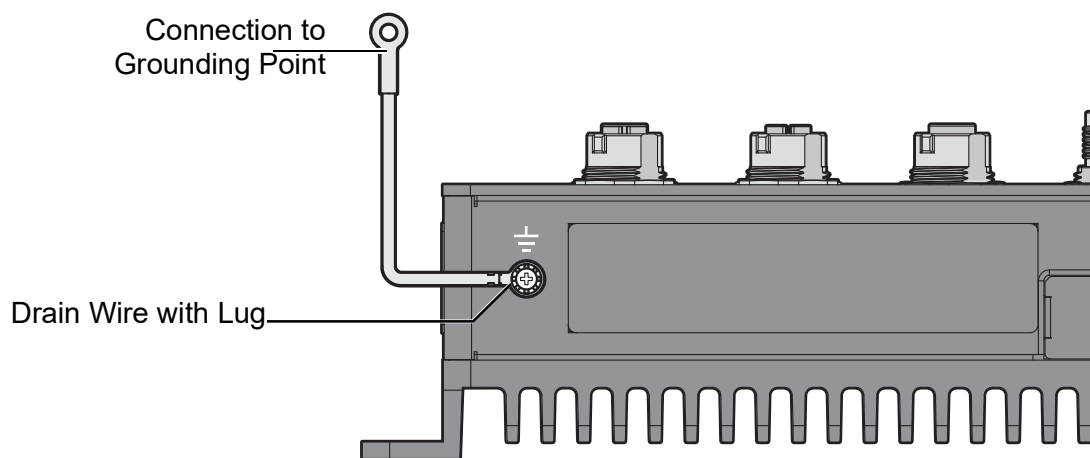


Figure 2.20 Grounding Connection

By connecting the ground terminal with a drain wire to earth ground, the device and chassis can be grounded.

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.



2.3.1.4 Connecting 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.



To connect the power inputs:

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

1. Remove the protection cap from the port.

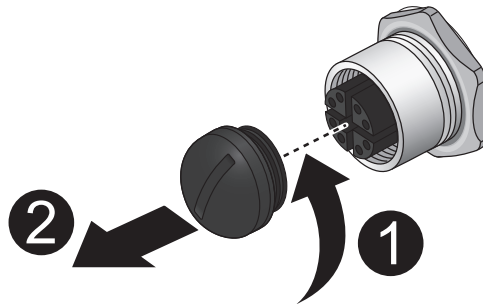


Figure 2.21 Removing a Protection Cap

2. Align the notch on the cable with the protrusion on the connector port. Before inserting the cable, the cable must be aligned to the connector to prevent damage to the pins in the port.
3. Insert the cable and gently push it in. If there is any resistance, remove the cable and re-align it with the connector.
4. Once the cable is fully seated in the port, turn the nut on the cable to secure it to the connector.

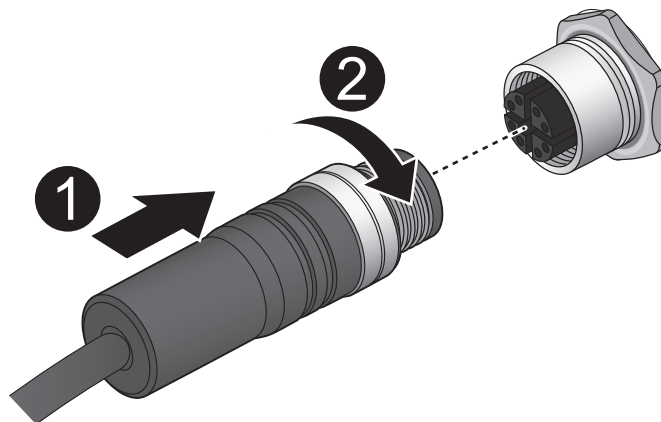


Figure 2.22 Installing the Power Cable

The power input is now connected to the switch. The switch can be powered on.

To remove the power inputs:

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

1. Loosen the screws securing the connector to the power cable receptor.
2. Remove the power cable from the device.

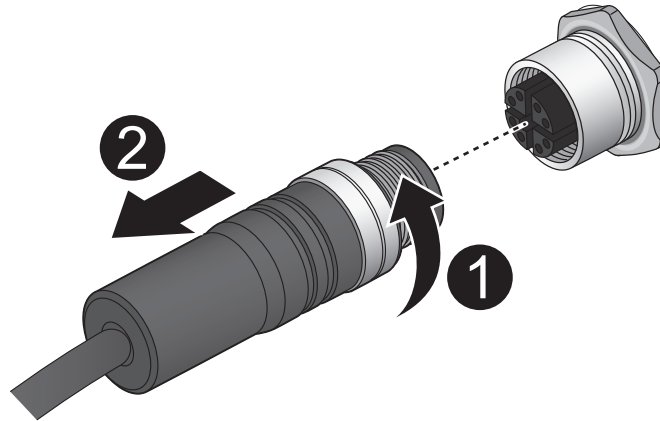


Figure 2.23 Removing the Power Cable

2.3.1.5 Standard M12 A-Coded 4 Poles Pin Assignment

This section describes the proper connection of the 24, 48, 72, 96 and 110 V_{DC} to the DC power connector on the switch. The DC input connector is located on the left side of the front panel. The power terminals are connected as shown in the following figure. Simply align the keyed female connector to the male connector and twist the threaded to secure.

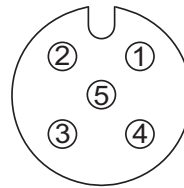


Figure 2.24 Standard M12 4 Poles Male DC Power Input Connector

Pin	Description
1	V1-
2	V1+
3	V2+
4	V2-
5	GND

Chapter 3

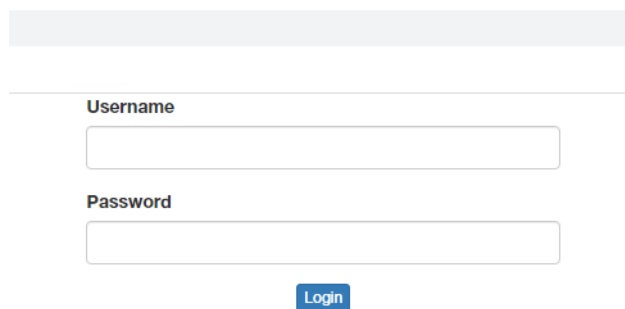
Web Interface

3.1 Log In

To access the login window, connect the device to the network, see “Network Connection” on page 15. 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.



The screenshot shows a web browser window with a login form. At the top is a grey header bar. Below it, the word "Username" is followed by a text input field. Below that, the word "Password" is followed by another text input field. At the bottom of the form is a blue button with the word "Login" in white text.

Figure 3.1 Login Screen

Note! Screen may differ depending on Web browsers.



3.1.1 Changing Default Password

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

1. Log in to the user interface menu, see “Basic” on page 31.
2. Navigate to **Management > Password Manager**. The HTTP configuration page displays.
3. Enter the user name of the profile to change (currently logged in user displays), then enter the new password under the **Password** field.
4. Re-type the same password in the **Confirm Password** field.
5. Click **Submit** to change the current account settings.

A screenshot of a web browser window titled "Password Manager". The interface has a light yellow background. It contains three input fields: "Username" with the value "admin", "Password" (empty), and "Confirm Password" (empty). Below the "Confirm Password" field is a blue "Submit" button.

Figure 3.2 Management > Password Manager

3.2 Overview

To access this page, click **Overview**.

System Info	
Information Name	Information Value
Firmware Version	1.2.3
Local Hostname	Advantech
System Time	Fri Dec 15 03:29:06 2023
System Up Time	0 day 20 hr 40 min 19 sec
Model Name	EKI-1652WT





LAN Interface	
Information Name	Information Value
LAN Status	 Address: 192.168.1.1 Netmask: 255.255.255.0 Gateway: 0.0.0.0 DNS Server: RX: 11.37 MB (101283 Pkts.) TX: 24.54 MB (103249 Pkts.) MAC-Address: 02:DB:1C:7D:76:AA
WLAN Status	 Mode: Access Point SSID: EKI-1652WT BSSID: 02:DB:1C:7D:76:AB Encryption: None Channel: 6 (2.437 GHz) Tx-Power: 30 dBm Country: US

Figure 3.3 Overview

WAN Interface	
Information Name	Information Value
ETHWAN	 Address: 192.168.20.102 Netmask: 255.255.255.0 Gateway: 192.168.20.1 DNS Server: RX: 0 B (0 Pkts.) TX: 240 B (2 Pkts.) MAC-Address: 02:DB:1C:7D:76:AC
Cellular Status	 Type: Current SIM: Network Provider: Signal Level: dBm Internet Status: Disconnected IP Address: Netmask: Default Gateway: Connection Time: 0 day 0 hr 0 min 0 sec

DHCP Leases			
Hostname	IPv4-Address	MAC-Address	Lease Time Remaining
There are no active leases.			

Figure 3.4 Overview Continued

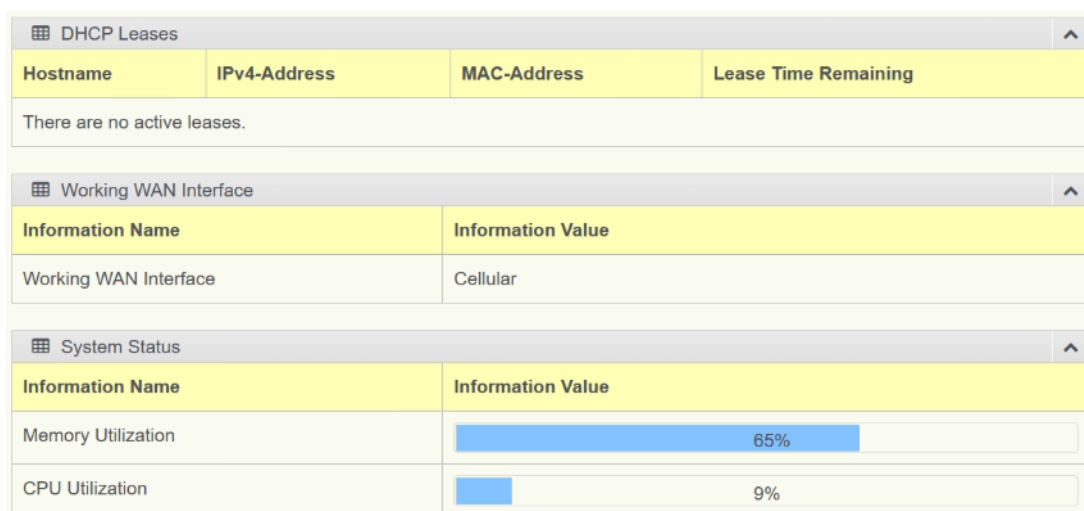


Figure 3.5 Overview Continued

The following table describes the items in the previous figure.

Item	Description
System Info	
Firmware Version	Displays the current firmware version of the device.
Local Hostname	Displays the current local hostname of the device.
System Time	Displays the current date of the device.
System Up Time	Displays the time since the last device reboot.
Model Name	Displays the model name of the device.
LAN Interface	
LAN Status	<ul style="list-style-type: none"> ■ Address: Displays the assigned IP address of the LAN interface. ■ Netmask: Displays the assigned netmask of the LAN interface. ■ Gateway: Displays the assigned gateway for the LAN interface. ■ DNS Server: Displays the IP address of the LAN interface. ■ RX: Displays the receiving volume of data in bytes. ■ TX: Displays the transmission volume of data in bytes. ■ MAC Address: Displays the MAC address of the device.
WLAN Status	<ul style="list-style-type: none"> ■ Mode: Displays the WLAN mode type. ■ SSID: Displays the assigned WLAN SSID. ■ BSSID: Displays the assigned the WLAN BSSD. ■ Encryption: Displays the assigned WLAN encryption. ■ Channel: Displays the assigned WLAN encryption. ■ Tx-Power: Displays the assigned WLAN transmission power. ■ Country: Displays the designated country code.
WAN Interface	

Item	Description
ETHWAN	<ul style="list-style-type: none"> ■ Address: Displays the assigned IP address of the ETHWAN interface. ■ Netmask: Displays the assigned netmask of the ETHWAN interface. ■ Gateway: Displays the assigned gateway for the ETHWAN interface. ■ DNS Server: Displays the IP address of the ETHWAN interface. ■ RX: Displays the receiving volume of data in bytes. ■ TX: Displays the transmission volume of data in bytes. ■ MAC Address: Displays the MAC address of the device.
Cellular Status	<ul style="list-style-type: none"> ■ Type: Displays the LTE type. ■ Current SIM: Displays the status of the SIM slot. ■ Network Provider: Displays the name of the provider of the LTE carrier. ■ Signal Level: Displays the signal level in dBm. ■ Internet Status: Displays the status of the Internet connection. ■ IP Address: Displays the IP address of the current connection. ■ Netmask: Displays the netmask of the current connection. ■ Default Gateway: Displays the gateway of the current connection. ■ Connection Time: Displays the uptime of the connection.
DHCP Leases	
Active Leases	Displays the active DHCP leases.
Working WAN Interface	
Working WAN Interface	Displays the active WAN interfaces (Cellular).
System Status	
Memory Utilization	Displays the total memory utilization in terms of percentage.
CPU Utilization	Displays the total CPU utilization in terms of percentage.

3.3 Interface

3.3.1 LAN

To access this page, click **Interface** > **LAN**.

The screenshot shows the 'LAN Interface Setup' window. It contains the following fields and sections:

- Local Hostname:** Text box with 'Advantech'.
- Domain Name:** Text box with 'lan'.
- Protocol:** Drop-down menu set to 'Static'.
- IP Address:** Text box with '192.168.1.1'.
- Subnet Mask:** Text box with '255.255.255.0'.
- DHCP Server:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Start IP Address:** Text box with '192.168.1.100'.
- Pool Counter:** Text box with '150'.
- Leasetime:** Four spin boxes for Day (0-365), Hour (0-23), Minute (0-59), and Second (0-59). Values are 0, 12, 0, and 0 respectively.
- Static DNS 1:** Text box.
- Static DNS 2:** Text box.
- Static Hosts:** A table with columns 'IP Address', 'Identified by', and 'Delete'. Below the table are 'Add' and 'Submit' buttons.

Figure 3.6 Interface > LAN

The following table describes the items in the previous figure.

Item	Description
LAN Interface Setup	
Local Hostname	Enter the device name: up to 31 alphanumeric characters.
Domain Name	Enter the name to be assigned for the interface domain.
Protocol	Click the drop-down menu to assign the type of protocol to the interface: DHCP Client or Static (default).
IP Address	Static Protocol Only: Enter a value to specify the IP address of the interface. The default is 192.168.1.1.
Subnet Mask	Static Protocol Only: Enter a value to specify the IP subnet mask for the interface. The default is 255.255.255.0.
DHCP Server	
DHCP Server	Click to enable or disable the DHCP server function.
Start IP Address	Enter the starting IP address of the DHCP pool.
Pool Counter	Enter the value to define the number of allowed DHCP leases.
Leasetime	Enter the lease time duration in Days (0-365), Hours, (0-23), Minutes (0-59), and Seconds (0-59).
Static DNS 1	Enter the IP address of the primary DNS.
Static DNS 2	Enter the IP address of the secondary DNS.
Static Hosts	
Submit	Click Submit to save the values and update the screen.

Note! All new configurations will take effect after rebooting. To reboot the device, click **Management > Reboot Device**.



3.3.2 ETHWAN

The ETHWAN function provides support for different Protocol settings, such as: PPTP, PPPoE, DHCP, and Disabled.

3.3.2.1 PPTP

To access this page, click **Interface > ETHWAN > Protocol**.

The screenshot shows the 'ETHWAN Interface Setup' window. It contains the following fields:

- Ethernet WAN:** A drop-down menu with 'ETH 2' selected.
- Protocol:** A drop-down menu with 'PPTP' selected.
- IP Address:** A text input field containing '192.168.20.102'.
- Subnet Mask:** A text input field containing '255.255.255.0'.
- Default Gateway:** A text input field containing '192.168.20.1'.
- Service IP Address:** An empty text input field.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Submit:** A blue button at the bottom.

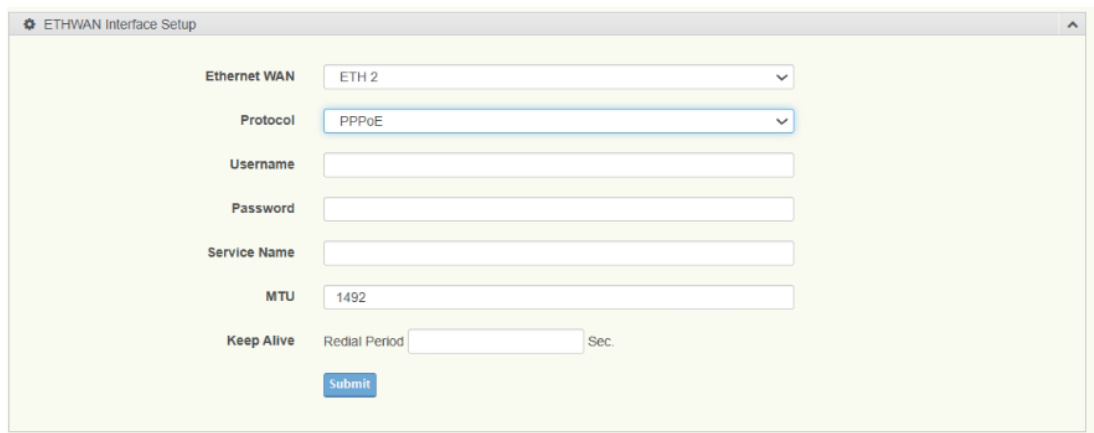
Figure 3.7 Interface > ETHWAN > PPTP

The following table describes the items in the previous figure.

Item	Description
Ethernet WAN	Click the drop-down menu to select the WAN interface: Disable or ETH 2.
Protocol	Click the drop-down menu to determines the specific communication protocol that the interface will use to transmit and receive data over the Wide Area Network (WAN). Options: PPTP - Point-to-Point Tunneling Protocol for a secure, encrypted tunnel over a public network.
IP Address	Static Protocol Only: Enter a value to specify the IP address of the interface. The default is 192.168.1.1.
Subnet Mask	Static Protocol Only: Enter a value to specify the IP subnet mask for the interface. The default is 255.255.255.0.
Default Gateway	Static Protocol Only: Enter a value to specify the default gateway for the interface.
Service IP Address	Enter the IP address that serves as the specific destination address to initiate and establish the PPTP VPN tunnel over the WAN connection.
Username	Enter the string to define a user name.
Password	Enter a string to bind to the defined user name.
Submit	Click Submit to save the values and update the screen.

3.3.2.2 PPPoE

To access this page, click **Interface > ETHWAN > Protocol**.



The screenshot shows the 'ETHWAN Interface Setup' window. It contains the following fields and controls:

- Ethernet WAN:** A dropdown menu currently showing 'ETH 2'.
- Protocol:** A dropdown menu currently showing 'PPPoE'.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Service Name:** An empty text input field.
- MTU:** A text input field containing the value '1492'.
- Keep Alive:** A section with a label 'Redial Period' followed by an empty text input field and the unit 'Sec'.
- Submit:** A blue button at the bottom.

Figure 3.8 Interface > ETHWAN > PPPoE

The following table describes the items in the previous figure.

Item	Description
Ethernet WAN	Click the drop-down menu to select the WAN interface: Disable or ETH 2.
Protocol	Click the drop-down menu to determines the specific communication protocol that the interface will use to transmit and receive data over the Wide Area Network (WAN). Options: PPPoE (Point-to-Point Protocol over Ethernet) - Used for broadband connections like DSL or cable.
Username	Enter the string to define a user name.
Password	Enter a string to bind to the defined user name.
Service Name	Enter the unique identifier string to specify the particular PPPoE service to establish a connection at the ISP (Internet Service Provider).
MTU	Enter the value to determine the largest size of a data packet, measured in bytes, that can be transmitted over the PPPoE connection.
Keep Alive	Enter the value in seconds to determine the frequency in which packets are sent out to the PPPoE server at the ISP to reaffirm the connection to the ISP, preventing termination due to inactivity.
Submit	Click Submit to save the values and update the screen.

3.3.2.3 Static

To access this page, click **Interface > ETHWAN > Protocol**.

The screenshot shows the 'ETHWAN Interface Setup' window. It contains several fields: 'Ethernet WAN' is a dropdown menu set to 'ETH 2'; 'Protocol' is a dropdown menu set to 'Static'; 'IP Address' is a text field with '192.168.20.102'; 'Subnet Mask' is a text field with '255.255.255.0'; 'Default Gateway' is a text field with '192.168.20.1'; 'DNS Server 1' and 'DNS Server 2' are empty text fields. A blue 'Submit' button is at the bottom.

Figure 3.9 Interface > ETHWAN > Static

The following table describes the items in the previous figure.

Item	Description
Ethernet WAN	Click the drop-down menu to select the WAN interface: Disable or ETH 2.
Protocol	Click the drop-down menu to determines the specific communication protocol that the interface will use to transmit and receive data over the Wide Area Network (WAN). Options: Static IP - Manually configuring a fixed IP address and other network settings.
IP Address	Static Protocol Only: Enter a value to specify the IP address of the interface. The default is 192.168.1.1.
Subnet Mask	Static Protocol Only: Enter a value to specify the IP subnet mask for the interface. The default is 255.255.255.0.
Default Gateway	Static Protocol Only: Enter a value to specify the default gateway for the interface.
DNS Server 1	Enter the primary server address to query for a DNS resolution.
DNS Server 2	Enter the secondary server address to query for a DNS resolution.
Submit	Click Submit to save the values and update the screen.

3.3.2.4 DHCP

To access this page, click **Interface > ETHWAN > Protocol**.

The screenshot shows the 'ETHWAN Interface Setup' window. It contains several fields: 'Ethernet WAN' is a dropdown menu set to 'ETH 2'; 'Protocol' is a dropdown menu set to 'DHCP Client'; a blue 'Submit' button is at the bottom.

Figure 3.10 Interface > ETHWAN

The following table describes the items in the previous figure.

Item	Description
Ethernet WAN	Click the drop-down menu to select the WAN interface: Disable or ETH 2.

Item	Description
Protocol	Click the drop-down menu to determines the specific communication protocol that the interface will use to transmit and receive data over the Wide Area Network (WAN). Options: DHCP - Request IP settings from the DHCP server.
Submit	Click Submit to save the values and update the screen.

3.3.2.5 Disable

To access this page, click **Interface > ETHWAN > Protocol**.

The screenshot shows a window titled 'ETHWAN Interface Setup'. Inside, there is a label 'Ethernet WAN' followed by a dropdown menu currently showing 'Disable'. Below the dropdown is a blue 'Submit' button.

Figure 3.11 Interface > ETHWAN

The following table describes the items in the previous figure.

Item	Description
Ethernet WAN	Click the drop-down menu to select the WAN interface: Disable or ETH 2.
Submit	Click Submit to save the values and update the screen.

3.3.3 WLAN

3.3.3.1 Basic

The WLAN settings function provides two operation mode types: Access Point and Wireless WAN.

Access Point Mode

The Access Point mode is available under the Basic WLAN Settings.

To access this page, click **WLAN > Basic**.

The screenshot shows a window titled 'Basic WLAN Settings'. Under the 'WLAN Network' section, there are several settings: 'Operation Mode' is a dropdown set to 'Access Point'; 'State' has radio buttons for 'Enabled' (selected) and 'Disabled'; 'SSID' is a text field with 'EKI-1652WT'; 'SSID Broadcast' is a dropdown set to 'Enable'; 'AP Isolation' is a dropdown set to 'Enable'; 'BSSID' is a text field showing '02:DB:1C:7D:76:AB'. Under the 'Operation Frequency' section, there are four dropdowns: 'Country Code' set to 'US (United States)', 'Band' set to '2.4G', 'Channel Bandwidth' set to '11b/g - Non-HT(Legacy)', and 'Channel / Frequency' set to 'AutoSelect'. A blue 'Submit' button is at the bottom.

Figure 3.12 WLAN > Basic

The following table describes the items in the previous figure.

Item	Description
Wireless Network	
Operation Mode	Click the drop-down menu to select an operation mode: Access Point or Wireless WAN.
State	Click the radio button to enable or disable the operation mode.
SSID	Enter the name to distinguish it from other networks in your neighborhood.
SSID Broadcast	Click the drop-down menu to enable or disable the SSID broadcast function. The function is only enabled when Operation Mode is set to Access Point.
AP Isolation	Click the drop-down menu to enable or disable the AP Isolation function. The function is only enabled when Operation Mode is set to Access Point.
BSSID	Display the MAC address of the device.
Operation frequency	
Country Code	Click the drop-down menu to select the country code to specify different selectable channels. Available options: US (United States), Germany, France, China and Japan. Some specific channels and/or operational frequency bands are country dependent.
Band	Click the drop-down menu to select the band channel.
Channel Bandwidth	Click the drop-down menu to select the band and channel bandwidth: 11b/g - Non-HT (Legacy), 11n - HT20, 11n - HT40, or 11ac - VHT 80.
Channel / Frequency	Click the drop-down menu to select a wireless channel/frequency: <ul style="list-style-type: none"> – AutoSelect – Channel 1: 2.412 GHz – Channel 2: 2.417 GHz – Channel 3: 2.422 GHz – Channel 4: 2.427 GHz – Channel 5: 2.432 GHz – Channel 6: 2.437 GHz – Channel 7: 2.442 GHz – Channel 8: 2.447 GHz – Channel 9: 2.452 GHz – Channel 10: 2.457 GHz – Channel 11: 2.462 GHz – Channel 12: 2.467 GHz – Channel 13: 2.472 GHz – Channel 14: 2.484 GHz (802.11b)
Submit	Click Submit to save the values and update the screen.

Wireless WAN Mode

The Wireless WAN mode is available under the Basic WLAN Settings.

To access this page, click **WLAN > Basic > Operation Mode > Wireless WAN**.

The screenshot shows the 'Basic WLAN Settings' window. The 'WLAN Network' section includes: 'Operation Mode' set to 'Wireless WAN'; 'State' with 'Enabled' selected; 'SSID' set to 'EKI-1652WT'; 'AP BSSID' as an empty field; 'Scan Hidden SSID' as an unchecked checkbox; 'MAC Address' as '02:DB:1C:7D:76:AB'; and 'Protocol' set to 'DHCP Client'. The 'Operation Frequency' section includes: 'Country Code' set to 'US (United States)' and 'Channel Selection' set to 'Auto'. Two 'Submit' buttons are located at the bottom of the form.

Figure 3.13 WLAN > Operation Mode > Wireless WAN

The following table describes the items in the previous figure.

Item	Description
WLAN Network	
Operation Mode	Click the drop-down menu to select an operation mode: Access Point or Wireless WAN.
State	Click the radio button to enable or disable the operation mode.
SSID	Enter the name to distinguish it from other networks in your neighborhood.
AP BSSID	Click the drop-down menu to enable or disable the SSID broadcast function. The function is only enabled when Operation Mode is set to Access Point.
Scan Hidden SSID	Click the drop-down menu to enable or disable the AP Isolation function. The function is only enabled when Operation Mode is set to Access Point.
MAC Address	Display the MAC address of the device.
Protocol	Click the drop-down menu to assign the type of protocol to the network: DHCP Client or Static.
Operation frequency	
Country Code	Click the drop-down menu to select the country code to specify different selectable channels. Available options: US (United States), Germany, France, China and Japan. Some specific channels and/or operational frequency bands are country dependent.
Channel Selection	Click the drop-down menu to select Auto (default) or Manual. The Auto selection allows the device to select a band. The Manual selection provides access to a selection of the option band (2.4GHz / 5GHz). The function is only enabled when Operation Mode is set to Client.
Submit	Click Submit to save the values and update the screen.

3.3.3.2 Advanced

The Access Point Settings are available under the Access Point Operation Mode. The operation mode must be configured for Access Point.

To access this page, click **WLAN > Advanced**.

Advanced WLAN Settings

Access Point Settings

Beacon Interval: 100 ms (20 - 999)

Data Beacon Rate (DTIM): 2 ms (1 - 255)

20/40 Coexistence: Enable

HT LDPC: Enable

Advanced WLAN Setting

RTS Threshold: 2347 (1 - 2347)

Transmission Power: Full

WMM: Enable

Short Guard Interval: Enable

Submit

Figure 3.14 1 WLAN > Advanced

The following table describes the items in the previous figure.

Item	Description
Access Point Settings	
Beacon interval	Enter the value to define the time lag between each of the beacons sent by the access point. Default: 100 ms (20 - 999).
Data beacon rate (DTIM)	Enter the value to define the rate at which beacons are sent. Default: 2 ms (1 - 255).
20/40 Coexistence	Click to disable or enable the coexistence, when enabled it functions to avoid interference between wireless networks.
HT LDPC	Click to disable or enable the HT Low Density Parity Check (LDPC) support, when enabled it supports receiving LDPC coded packets.
Advanced WLAN Setting	
RTS Threshold	Enter the value as the threshold for the request to send function. A lower threshold increases the WLAN stability, default: 2347 (1 -2347).
Transmission Power	Click the drop-down menu to set the transmission power. Settings: Full, Half, Quarter.
WMM	Wireless Multimedia (WMM) is enabled by default.
Short Guard Interval	Click the drop-down menu to enable/disable the short guard interval. In 802.11 operation, the guard interval is 800ns. The short guard interval time is 400ns to allow for an increased throughput.
Submit	Click Submit to save the values and update the screen.

3.3.3.3 Security

Security Mode None

To access this page, click **Interface > WLAN > Security > Security Mode**.

The screenshot shows a web interface titled "WLAN Security/Encryption Settings". Under the "Security Policy" section, there is a "Security Mode" dropdown menu currently set to "None". Below the dropdown is a blue "Submit" button.

Figure 3.15 Interface > WLAN > Security > Security Mode

The following table describes the items in the previous figure.

Item	Description
Security Policy	
Security Mode	Click the drop-down menu to select the encryption when communication. Available options: None, WEP, WPA-Personal and WPA/WPA2-Enterprise. If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.
Submit	Click Submit to save the values and update the screen.

Security Mode WEP

To access this page, click **Interface > WLAN > Security > Security Mode > WEP**.

The screenshot shows the "WLAN Security/Encryption Settings" page with "Security Mode" set to "WEP". Below this, the "Wire Equivalence Protection (WEP)" section is expanded, showing a "Default Key Index" dropdown set to "Key 1". There are four rows for "WEP Key 1" through "WEP Key 4". Each row has a text input field, an "ASCII" dropdown menu, and an "Unmask" checkbox. A blue "Submit" button is at the bottom.

Figure 3.16 Interface > WLAN > Security > Security Mode > WEP

The following table describes the items in the previous figure.

Item	Description
Security Policy	
Security Mode	Click the drop-down menu to select the encryption when communication. Available options: None, WEP, WPA-Personal and WPA/WPA2-Enterprise. If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.
Wire Equivalence Protection (WEP)	
Default Key Index	Click the drop-down menu to select one of the four defined key indexes as defined by the WEP Key # fields in the following

Item	Description
WEP Key 1	Enter up to four WEP keys. Enter a string of characters dependent on the key type: ASCII -- Upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #. Hex -- Digits 0 to 9 and the letters A to F. Click Unmask to view the password entry.
WEP Key 2	
WEP Key 3	
WEP Key 4	
Submit	Click Submit to save the values and update the screen.

Security Mode WPA-Personal

To access this page, click **Interface > WLAN > Security > Security Mode > WPA-Personal**.

The screenshot shows the 'WLAN Security/Encryption Settings' window. Under the 'Security Policy' section, the 'Security Mode' is set to 'WPA-Personal'. Below this, the 'WPA-Personal' section contains three settings: 'WPA Version' set to 'WPA1+WPA2', 'WPA Cipher' set to 'TKIP+AES', and a 'Pass Phrase' field. There is an 'Unmask' checkbox and a 'Submit' button at the bottom of the form.

Figure 3.17 Interface > WLAN > Security > Security Mode > WPA-Personal

The following table describes the items in the previous figure.

Item	Description
Security Policy	
Security Mode	Click the drop-down menu to select the encryption when communication. Available options: None, WEP, WPA-Personal and WPA/WPA2-Enterprise. If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.
WPA-Personal	
WPA Version	Click the drop-down menu to designate the specific authentication type. Settings: WPA1+WPA2, WPA1, WPA2.
WPA Cipher	Click the drop-down menu to apply the encryption. Settings: TKIP+AES, TKIP, AES.
Pass Phrase	Enter the a unique password to define the passphrase for authentication access. Click Unmask to view the password entry.
Submit	Click Submit to save the values and update the screen.

Security Mode WPA/WPA2-Enterprise

To access this page, click **Interface > WLAN > Security > Security Mode**.

Security Policy

Security Mode: WPA/WPA2-Enterprise

WPA-enterprise settings

Radius Server IP Address: 192.168.1.2

Port: 1812

Shared Secrets: *****

☐ Unmask

Submit

Figure 3.18 Interface > WLAN > Security > Security Mode

The following table describes the items in the previous figure.

Item	Description
Security Policy	
Security Mode	Click the drop-down menu to select the encryption when communication. Available options: None, WEP, WPA-Personal and WPA/WPA2-Enterprise. If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.
WPA-enterprise Settings	
Radius Server IP Address	Enter the IP address of the target radius server.
Port	Enter the port address of the listed radius server.
Shared Secrets	Enter the value to server as the shared secret key for the identified server. Click Unmask to view the password entry.
Submit	Click Submit to save the values and update the screen.

3.3.3.4 Statistics

To access this page, click **Interface > WLAN > Statistics**.

Overview

Information Name	Information Value
Mode	Access Point
SSID	EKI-1652WT
Channel / Frequency	channel 6 (2437 MHz)
BSSID	02:DB:1C:7D:76:AB

Station List

Station BSSID	Signal Level	Connected Time	Tx/Rx Rate	Tx Packets/Bytes	Rx Packets/Bytes
---------------	--------------	----------------	------------	------------------	------------------

Wlan status

Information Name	Information Value
TX Packets	46509
TX Bytes	7165577
RX Packets	0
RX Bytes	0

Figure 3.19 Interface > WLAN > Statistics

The following table describes the items in the previous figure.

Item	Description
Mode	Display the current operation mode of the device.
SSID	Display the SSID.
Channel / Frequency	Display the current channel / frequency of the device.
BSSID	Display the MAC address of the device.
Station BSSID	Displays the basic service set identifier, access point unique MAC address.
Signal Level	Displays the power level measure in decibel-milliwatts of the listed BSSID.
Connected Time	Displays the total uptime period.
Tx/Rx Rate	Displays the transmit to receive rate of the connected client.
Tx Packets/Bytes	Displays the total Tx packets and corresponding bytes.
Rx Packets/Bytes	Displays the total Rx packets and corresponding bytes.
TX Packets	Display the current Tx packets.
TX Bytes	Display the current Tx bytes.
RX Packets	Display the current Rx packets.
RX Bytes	Display the current Rx bytes.

3.3.3.5 Interface > WLAN > Access Control

Access Control allows for an administrator to allow or deny access by defining specific devices through their MAC address.

To access this page, click **Interface > WLAN > Traffic Control**.

Figure 3.20 Interface > WLAN > Traffic Control

Access Control Method	Click the drop-down menu to set the access control method: Disable (default), Deny or Allow. In the Deny or Allow menu, enter the MAC address of the target device - support for up to 32 target devices.
Submit	Click Submit to save the values and update the screen.

Note! The previous figure was altered for instructional purposes.



3.3.3.6 Log

To access this page, click **Interface > WLAN > Log**.

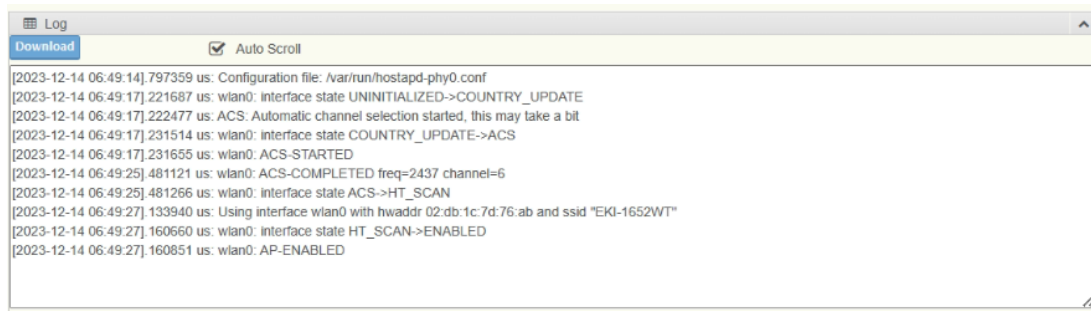


Figure 3.21 Interface > WLAN > Log

The following table describes the items in the previous figure.

Item	Description
Download	Click Download to download the log file.
Auto Scroll	Click to allow for auto scrolling in the event of a large log entry list.

3.3.4 Cellular

3.3.4.1 Basic

To access this page, click **Interface > Cellular > Basic**.

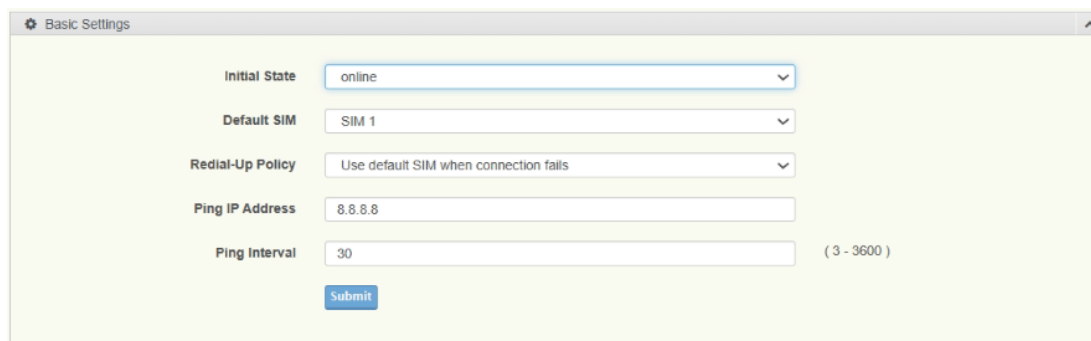


Figure 3.22 Interface > Cellular > Basic

The following table describes the items in the previous figure.

Item	Description
Initial State	Click to define the state of the service. Setting: Online or Offline.
Default SIM	Click the drop-down menu to select the default SIM slot. Setting: SIM 1 or SIM 2.
Redial-Up Policy	Click to select how the device reconnects to the cellular network if a connection is lost or fails to establish initially.
Ping IP Address	Enter the IP address to initiate a ping test to determine the SIM connectivity state.
Ping Interval	Enter a variable to determine the frequency between ping functions. Settings: 3 - 36000
Submit	Click Submit to save the values and update the screen.

3.3.4.2 SIM 1

APN Configuration

To access this page, click **Interface > Cellular > SIM 1**

The screenshot displays the 'SIM 1' configuration page. It is divided into three main sections: 'APN Configuration', 'SIM1 Card Utilities', and 'PIN Protection'. The 'APN Configuration' section includes fields for 'APN' (set to 'internet'), 'PIN' (with a '(0000 - 9999)' hint), 'PIN State', 'PAP/ CHAP Username', and 'PAP/ CHAP Password', each with a corresponding 'Submit' button. The 'SIM1 Card Utilities' section contains 'Unlock SIM Card' fields for 'SIM PUK' (with a '(00000000 - 99999999)' hint) and 'New SIM PIN' (with a '(0000 - 9999)' hint), followed by a 'Submit' button. The 'PIN Protection' section has a radio button for 'Enable PIN Protection' (set to 'Off'), a 'Current PIN' field (with a '(0000 - 9999)' hint), and a 'Submit' button. Below this is a 'Change PIN Code' section with fields for 'Current PIN', 'New PIN', and 'Confirm New PIN' (all with '(0000 - 9999)' hints), and a 'Submit' button.

Figure 3.23 Interface > Cellular > SIM 1

The following table describes the items in the previous figure.

Item	Description
APN Configuration	
APN	Enter the access point name setting to setup a connection between the carrier's cellular network and the public network.
PIN	Enter the variable of the current PIN code. Variable: 0000 to 9999.
PIN State	Displays the state of the current PIN.
PAP / CHAP Username	Enter the string of the authentication protocol.
PAP / CHAP Password	Enter the password bound to the define protocol username.
Submit	Click Submit to save the values and update the screen.
Unlock SIM Card	
SIM PUK	Enter the variable to define the personal unlock key. Variable: 00000000 to 99999999.
New SIM PIN	Enter the variable to create a PIN for the SIM after a successful unlock.
Submit	Click Submit to save the values and update the screen.
PIN Protection	
Enable PIN Protection	Click to enable or disable the PIN protection function.
Current PIN	Enter the current PIN of the SIM card.

Item	Description
Submit	Click Submit to save the values and update the screen.
Change PIN Code	
Current PIN	Enter the variable to define the current PIN code. Variable: 0000 to 9999.
New PIN	Enter the variable to define a new PIN code. Variable: 0000 to 9999.
Confirm New PIN	Enter the variable to confirm the New Pin entry. Variable: 0000 to 9999.
Submit	Click Submit to save the values and update the screen.

3.3.4.3 SIM 2

For further information regarding configuration of SIM 2 see “SIM 1” on page 40.

3.4 Networking

3.4.1 Static Route

A static route provide fixed routing path through the network. It is manually configured on the router and must be updated if the network topology was changed recently. Static routes are private routers unless they are redistributed by a routing protocol.

To access this page, click **Networking > Static Route**.

Figure 3.24 Networking > Static Route

The following table describes the items in the previous figure.

Item	Description
Target IP Address	Enter an IP address (static route) for this static route.
Netmask	Enter a netmask setting (static route) for this static route.
Gateway	Enter a gateway setting (static route) for this static route.
Interface	Enter an interface for this static route, options: LAN, WAN, Wireless 2.4GHz, or Wireless 5GHz.
Metric	Enter the administrative distance (default: 1) used by the ap to choose the best path for two or more routes to the same destination.
MTU	Enter the maximum transmission value for the data packets if applicable.
Delete	Click Delete to remove the route from the available list.
Add	Click Add to include the route in the static routing policy.
Submit	Click Submit to save the values and update the screen.

3.4.2 Forwarding

3.4.2.1 Port Forwarding

Port forwarding, also known as port mapping, allows for the application of network addresses (NAT) the redirection of a communication request from an address and port to a specified address while the packets traverse the firewall.

The function are designed for networks hosting a specific server, such as a web server or mail server, on the private local network and behind the NAT firewall.

To access this page, click **Networking > Forwarding > Port Forwarding**.

Figure 3.25 Networking > Forwarding > Port Forwarding

The following table describes the items in the previous figure.

Item	Description
Enabled	Click Download to download the log file.
Name	Enter a text string to identify the port forwarding entry.
Start Port	Enter the value of the starting port for this entry.
End Port	Enter the value of the ending port for this entry.
Local IP	Enter the IP address defining the static address of the local IP.
Local Port	Enter the value defining the local port.
Protocol	Click the drop-down menu to select the protocol setting, options: TCP, UDP, Both.
Delete	Click Delete to remove the selected entry from the port forwarding policy.
Add	Click Add to include the entry in the port forwarding policy.
Submit	Click Submit to save the values and update the screen.

3.4.2.2 DMZ

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

To access this page, click **Networking > Forwarding > DMZ**.

Figure 3.26 Networking > Forwarding > DMZ

The following table describes the items in the previous figure.

Item	Description
DMZ	Click the radio button to enable or disable the DMZ function.
IP	Enter the IP address to designate a static IP address as the DMZ target.
Submit	Click Submit to save the values and update the screen.

3.4.3 Security

3.4.3.1 Filter

The firewall is a system or group of systems that enforce an access control policy between two networks. It may also be defined as a mechanism used to protect a

trusted network from an un-trusted network. The device has capabilities of Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding as well as DMZ.

Source IP Filtering: The source IP filtering gives users the ability to restrict certain types of data packets from users local network to Internet through the device. Use of such filters can be helpful in securing or restricting users local network.

To access this page, click **Networking > Security > Filter**.

Figure 3.27 Networking > Security > Filter

Item	Description
Filter	Click the radio button to enable or disable the Filter policy.
Enabled	Select to enable the defined filter entry.
Direction	Click the drop-down menu to select the direction of the data packet traffic for the entry: LAN to WAN, WAN to LAN.
Source IP	Enter the IP address of the sender address.
Destination IP	Enter the IP address of the destination address.
Protocol	Click the drop-down menu to select the protocol type for the entry: TCP, UDP, ICMP.
Source port	Enter the port number of the sender IP address.
Destination port	Enter the port number of the destination IP address.
Delete	Click Delete to remove the entry from the Filter policy.
Add	Click Add to include the entry in the Filter policy.
Submit	Click Submit to save the values and update the policy.

3.4.4 OpenVPN

3.4.4.1 Tunnel 1

VPN pass-through is a function of the router, which provides outbound VPN function. VPN pass-through does not provide inbound VPN function. You can enable VPN passthrough without the need to open any ports, and it will run automatically.

To access this page, click **Networking > OpenVPN > Tunnel 1**.

OpenVPN 1

Status Stop

Tunnel 1 ☐ Enabled ☒ Disabled

Protocol UDP

Port (1 - 65535)

Remote IP Address

Remote Subnet

Remote Subnet Mask

Server Network

Server Netmask

Redirect Gateway ☐

Local Interface IP Address

Remote Interface IP Address

Ping Interval (1 - 86400)

Ping Timeout (1 - 86400)

Renegotiate Interval (0 - 86400)

Renegotiate Interval (0 - 86400)

Max Fragment Size (128 - 16384)

Compression None

NAT Rules Applied ☐

Authenticate Mode None

Pre-shared Secret 選擇檔案 沒有選擇檔案

CA Certificate 選擇檔案 沒有選擇檔案

DH Parameters 選擇檔案 沒有選擇檔案

Local Certificate 選擇檔案 沒有選擇檔案

Local Private Key 選擇檔案 沒有選擇檔案

Username

Password

Extra Options

Submit

Figure 3.28 Networking > OpenVPN > Tunnel 1

Item	Description
Status	Displays the current status of the OpenVPN
Tunnel 1	Click to enable or disable the tunnel.

Item	Description
Protocol	Click to define the protocol for the tunnel. Settings: UDP, TCP Server, or TCP Client.
Port	Enter the variable to define the tunnel port.
Remote IP Address	Enter the IP address of the remote endpoint.
Remote Subnet	Enter the subnet address of the remote endpoint.
Remote Subnet Mask	Enter the remote subnet mask of the remote endpoint.
Server Network	If Authenticate mode is selected under Server Mode, you need to assign a server IP address.
Server Netmask	If Authenticate mode is selected under Server Mode, you need to assign a server network mask.
Redirect Gateway	Adds (rewrites) the default gateway. All packets are then sent to this gateway via tunnel, if there is no other specified default gateway inside them.
Local Interface IP Address	Specifies the IPv4 address of a local interface.
Remote Interface IP Address	Specifies the IPv4 address of the interface of opposite side of the tunnel.
Ping Interval	Enter the variable to define the frequency of the ping activity. Variable: 1 to 86400.
Ping Timeout	Enter the variable to define the timeout period for a failed ping.
Renegotiate Interval	Enter the variable to define the period of time before initiating a renegotiation. Variable: 0 to 86400.
Max Fragment Size	Maximum size of a sent packet.
Compression	Click the drop-down menu to select the type of compression. Setting: None or LZO.
NAT Rules Applied	Activates/deactivates the NAT rules for the OpenVPN tunnel.
Authenticate Mode	Click the drop-down menu to select the authentication mode: Setting: None, Server Mode, Secret, Password, TLS MClient, TLS Server, TCL Client.
Pre-Shared Secret	Click Choose File to browse and select a file containing the pre-shared secret.
CA Certificate	Click Choose File to browse and select a certificate.
DH Parameters	Click Choose File to browse and select a file containing key exchange protocol.
Local Certificate	Click Choose File to browse and select a file containing the local certificate.
Local Private Key	Click Choose File to browse and select a file containing a designated private key.
Username	Enter the string to define a user name.
Password	Enter a string to bind to the defined user name.
Extra Options	Specifies additional parameters for the OpenVPN tunnel, such as DHCP options. The parameters are proceeded by two dashes.
Submit	Click Submit to save the values and update the policy.

3.4.4.2 Tunnel 2

For further information regarding the configuration of the OpenVPN Tunnel function see "Tunnel 1" on page 44

3.4.4.3 Tunnel 3

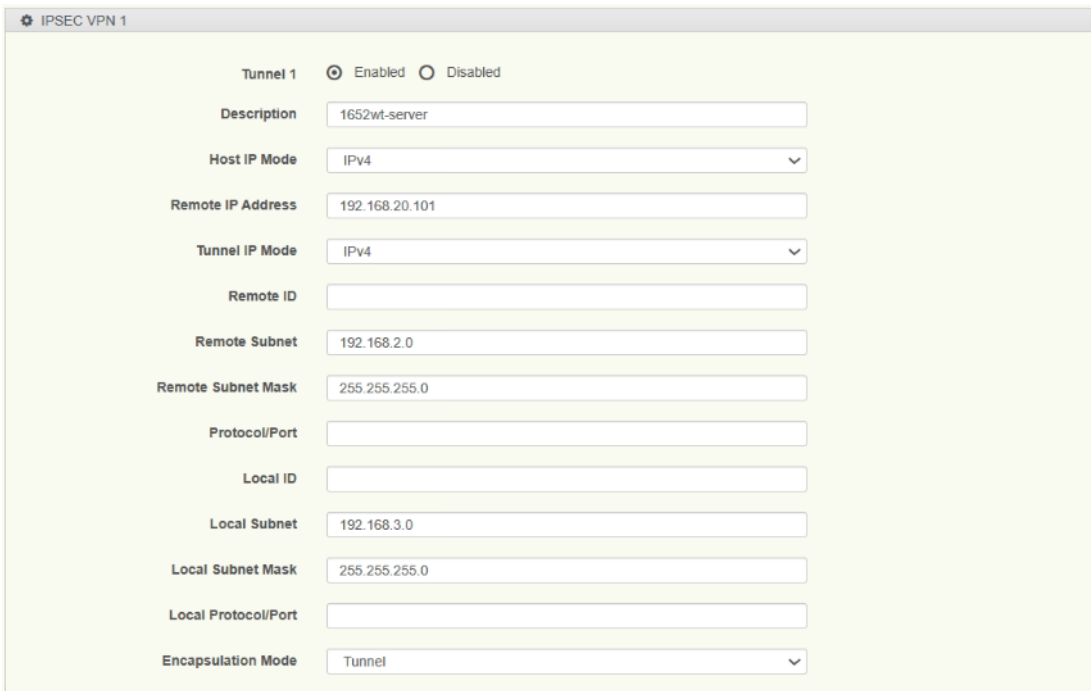
For further information regarding the configuration of the OpenVPN Tunnel function see “Tunnel 1” on page 44

3.4.4.4 Tunnel 4

For further information regarding the configuration of the OpenVPN Tunnel function see “Tunnel 1” on page 44

3.4.5 IPSEC VPN

To access this page, click **Networking > IPSEC VPN**



IPSEC VPN 1

Tunnel 1 ☒ Enabled ☐ Disabled

Description: 1652wt-server

Host IP Mode: IPv4

Remote IP Address: 192.168.20.101

Tunnel IP Mode: IPv4

Remote ID:

Remote Subnet: 192.168.2.0

Remote Subnet Mask: 255.255.255.0

Protocol/Port:

Local ID:

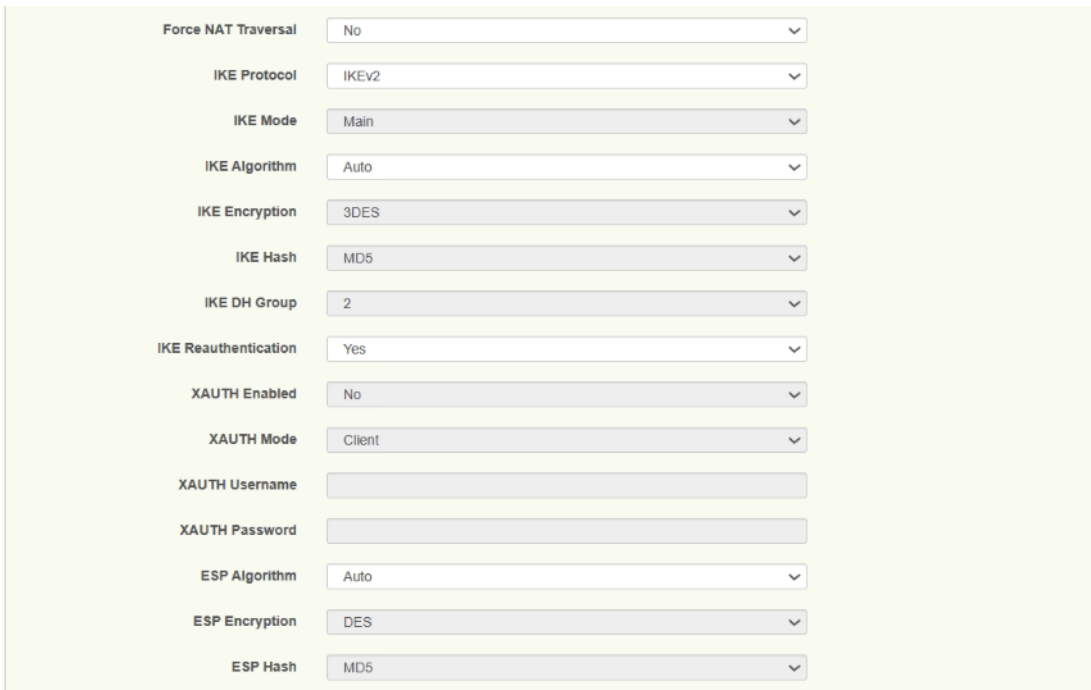
Local Subnet: 192.168.3.0

Local Subnet Mask: 255.255.255.0

Local Protocol/Port:

Encapsulation Mode: Tunnel

Figure 3.29 Networking > IPSEC VPN



Force NAT Traversal: No

IKE Protocol: IKEv2

IKE Mode: Main

IKE Algorithm: Auto

IKE Encryption: 3DES

IKE Hash: MD5

IKE DH Group: 2

IKE Reauthentication: Yes

XAUTH Enabled: No

XAUTH Mode: Client

XAUTH Username:

XAUTH Password:

ESP Algorithm: Auto

ESP Encryption: DES

ESP Hash: MD5

Figure 3.30 Networking > IPSEC VPN

The screenshot displays the IPSEC VPN configuration page. It includes input fields for Rekey Margin (540, range 1-86400), Rekey Fuzz (100, range 0-200), DPD Delay (20, range 1-3600), and DPD Timeout (60, range 1-3600). The Authenticate Mode is set to 'Pre-shared Key'. The Pre-shared Key field contains a masked value '*****'. Below these are sections for certificates and keys, each with a '選擇檔案' (Select File) button and a '沒有選擇檔案' (No file selected) status. The Local Passphrase field is empty. The Debug dropdown is set to 'Control'. A 'Submit' button is at the bottom.

Figure 3.31 Networking > IPSEC VPN

The following table describes the items in the previous figure.

Item	Description
Tunnel #	Click to Enable (default) or Disable the function.
Description	Enter a description to identify the VPN tunnel.
Host IP Mode	Click to select the setting to determine how IP addresses are handled. Options: IPv4, IPv6.
Remote IP Address	Enter the destination address to identify the endpoint of the VPN tunnel.
Tunnel IP Mode	Click to select the setting to determine how IP addresses are handled at the endpoint of the VPN tunnel. Options: IPv4, IPv6.
Remote ID	Enter a description to identify the endpoint of the VPN tunnel.
Remote Subnet	Displays the remote subnet configuration assigned to the configuration.
Remote Subnet Mask	Enter the destination subnet mask address to identify the endpoint of the VPN tunnel.
Protocol/Port	Enter the protocol/port for the setting.
Local ID	Enter the identifier string to define the starting point of the tunnel within the local network.
Local Subnet	Enter the identifier string to define the starting point of the tunnel within the local network.
Local Subnet mask	Enter the subnet mask to define the starting point of the tunnel within the local network.
Local Protocol/Port	Enter the protocol/port setting to define the starting point of the tunnel within the local network.
Encapsulation Mode	Click to select the encapsulation mode to determine the tunnel security.
Force NAT Traversal	Click to allow or disallow the function when the VPN endpoints are behind a firewall.
IKE Protocol	Click to select the Internet Key Exchange protocol for the channel.
IKE Mode	Click to select the Internet Key Exchange mode for the channel.
IKE Algorithm	Click to select the algorithm to define the security setting for the channel.
IKE Encryption	Click to select the encryption, shared key, to be used between the VPN peers.

Item	Description
IKE Hash	Click to select the specific hash algorithm to be used for authentication purposes.
IKE DH Group	Click to select the technique to allow both peers to securely establish a shared secret key.
IKE Reauthentication	Click to allow or disallow the encryption to periodically verify the identifies of the VPN peers and renegotiates encryption keys.
XAUTH Enabled	Click to allow or disallow user credentials or external authentication methods requirement for VPN access.
XAUTH Mode	Click to the type of mode for user authentication.
XAUTH Username	Enter the user name of the username for the unique identifier (username) that users must provide, along with their password or other credentials for VPN access.
XAUTH Password	Enter the password corresponding to the username for the unique identifier (username) that users must provide, along with their password or other credentials for VPN access.
ESP Algorithm	Click to select the method to encapsulate security payloads to add authentication for integrity.
ESP Encryption	Click to select the encryption type for the selected encapsulation type.
ESP Hash	Click to select the type of fingerprint for each data packet to ensure transmission integrity.
PFS	Click to enable or disable (default) the Perfect Forward Secrecy ensuring past communication sessions remain secure even if long-term encryption keys are compromised.
PFS DH Group	Click to select the key exchange (default: 2) for perfect forward secrecy, ensuring each session generates unique, temporary keys to protect past communication.
Key Lifetime	Enter the variable in seconds (default: 3600) to define the time in which PFS keys remain valid before refreshing.
IKE Lifetime	Enter the variable in seconds (default: 3600) to define the frequency in which the IKE exchange key is refreshed.
Rekey Margin	Enter the variable (default: 540) in seconds to automatically renew encryption keys before they expire.
Rekey Fuzz	Enter the variable (default: 100) in percentage to define how often the timing of the automatic key refresh is randomly generated.
DPD Delay	Enter the variable (default: 20) in seconds to define the grace period before triggering a connection drop after a timeout.
DPD Timeout	Enter the variable (default: 20) in seconds to define the period of time before dropping out an idle connection.
Authenticate Mode	Click to select the authentication mode to determine how VPN peers verify identifies before establishing a secure tunnel.
Pre-shared Key	Enter a pre-shared key, secret password, which is shared between devices to allow only authorized parties to establish a secure tunnel.
CA Certificate	Click to import a certificate file.
Remote Certificate / PubKey	Click to import a remote certificate key as a secure digital ID card.
Local Certificate / PubKey	Click to import a local certificate key as a secure digital ID card.
Local Private Key	Click to import the local device's private key.
Local Passphrase	Enter a string to be used as the password to grant access to the device's private key and enabling a secure tunnel.

Item	Description
Debug	Click to select the debug mode for the function.
Submit	Click Submit to save the values and update the screen.

3.4.6 GRE

The Generic Routing Encapsulation (GRE) protocol encapsulates data packets one routing protocol inside the packet of another protocol.

GRE enables the support of protocols not normally supported by a network.

3.4.6.1 Tunnel 1

To access this page, click **Networking > GRE> Tunnel 1**.

Figure 3.32 Networking > GRE> Tunnel 1

The following table describes the items in the previous figure.

Item	Description
GRE	Click to enable or disable the GRE function.
Description	Enter a string to describe the tunnel entry.
Remote IP Address	Enter the IP address of the remote network to establish the tunnel with the device.
Remote Subnet	Enter the subnet of the assigned remote IP address endpoint.
Remote Subnet Mask	Enter the subnet mask of the assigned remote IP address endpoint.
Local Interface IP Address	Enter the IP address of the local IP address to designate as the tunnel endpoint.
Remote Interface IP Address	Enter the IP address of the remote IP address to designate as the tunnel endpoint.
Multicasts	Click to enable or disable the multicast function.
Pre-Shared Key	Enter a value to define the security key. Value: 1 to 4294967295.
Submit	Click Submit to save the values and update the screen.

3.4.6.2 Tunnel 2

For further information regarding the configuration of the OpenVPN Tunnel function see “Tunnel 1” on page 50.

3.4.6.3 Tunnel 3

For further information regarding the configuration of the OpenVPN Tunnel function see “Tunnel 1” on page 50.

3.4.6.4 Tunnel 4

For further information regarding the configuration of the OpenVPN Tunnel function see “Tunnel 1” on page 50.

3.4.7 QoS Settings

3.4.7.1 QoS Settings

To access this page, click **Networking > QoS Settings> QoS Settings**.

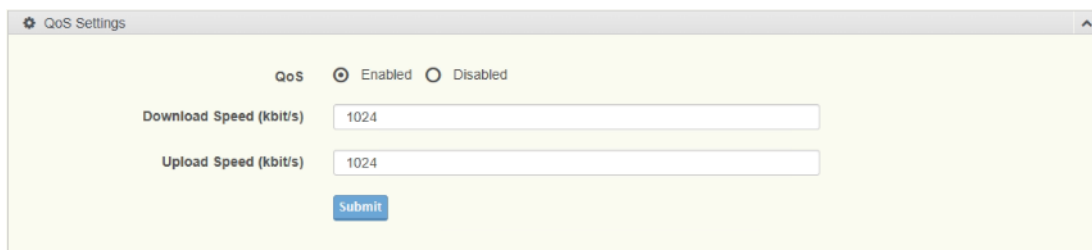


Figure 3.33 Networking > QoS Settings> QoS Settings

The following table describes the items in the previous figure.

Item	Description
QoS	Click the radio button to enable or disable the QoS policy on the selected interface.
Download Speed (kbit/s)	Enter the value (kbit/s) to define the download speed of the policy: 1024 to 102400, default: 85000)
Upload Speed (kbit/s)	Enter the value (kbit/s) to define the upload speed of the policy: 1024 to 102400, default: 10000)
Submit	Click Submit to save the values and update the screen.

3.4.7.2 QoS IP Base Rules

To access this page, click **Networking > QoS Settings> QoS IP Base Rules**.

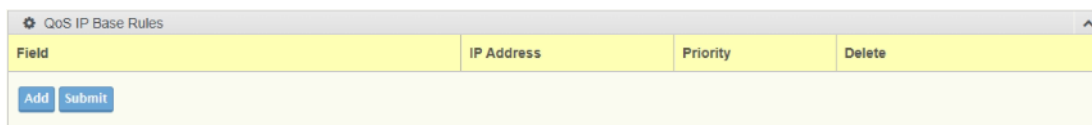


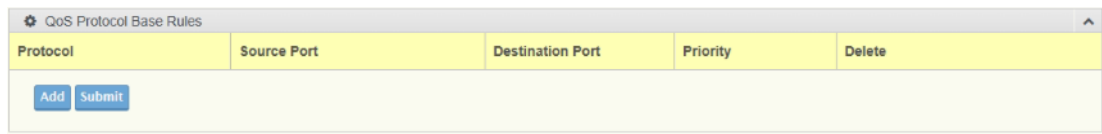
Figure 3.34 Networking > QoS Settings> QoS IP Base Rules

The following table describes the items in the previous figure.

Item	Description
Field	Click the drop-down menu to classify the traffic type for the rule.
IP Address	Enter the IP address to bind to the rule.
Priority	Click the drop-down menu to set the priority for the rule. Value: Low, Normal, Medium, or High.
Delete	Click Delete to remove the selected rule.
Add	Click Add to include the selected rule.
Submit	Click Submit to save the values and update the screen.

3.4.7.3 QoS Protocol Base Rules

To access this page, click **Networking > QoS Settings> QoS Protocol Base Rules**.



Protocol	Source Port	Destination Port	Priority	Delete
----------	-------------	------------------	----------	--------

Figure 3.35 Networking > QoS Settings> QoS Protocol Base Rules

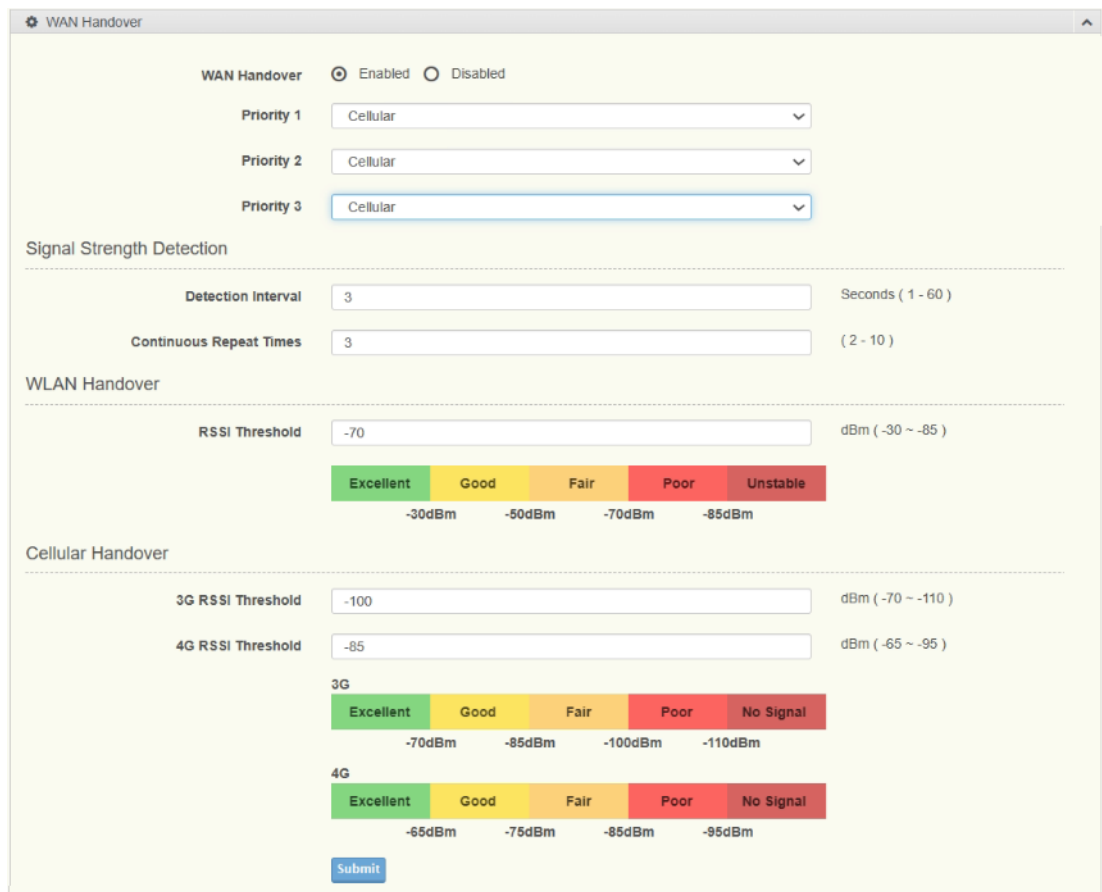
The following table describes the items in the previous figure.

Item	Description
Protocol	Click the drop-down menu to select the protocol type. Value: UDP, TCP.
Source Port	Enter the port value for the source endpoint.
Destination Port	Enter the port value for the destination endpoint.
Priority	Click the drop-down menu to set the priority for the rule. Value: Low, Normal, Medium, or High.
Delete	Click Delete to remove the selected rule.
Add	Click Add to include the selected rule.
Submit	Click Submit to save the values and update the screen.

3.4.8 WAN Handover

3.4.8.1 WAN Handover

To access this page, click **Networking > WAN Handover**.



WAN Handover ☒ Enabled ☐ Disabled

Priority 1: Cellular
Priority 2: Cellular
Priority 3: Cellular

Signal Strength Detection

Detection Interval: 3 Seconds (1 - 60)
Continuous Repeat Times: 3 (2 - 10)

WLAN Handover

RSSI Threshold: -70 dBm (-30 ~ -85)

Signal Quality Bar: Excellent (-30dBm), Good (-50dBm), Fair (-70dBm), Poor (-85dBm), Unstable

Cellular Handover

3G RSSI Threshold: -100 dBm (-70 ~ -110)
4G RSSI Threshold: -85 dBm (-65 ~ -95)

3G Signal Quality Bar: Excellent (-70dBm), Good (-85dBm), Fair (-100dBm), Poor (-110dBm), No Signal

4G Signal Quality Bar: Excellent (-65dBm), Good (-75dBm), Fair (-85dBm), Poor (-95dBm), No Signal

Figure 3.36 Networking > WAN Handover

The following table describes the items in the previous figure.

Item	Description
WAN Handover	Click to enable or disable the WAN handover function.
Priority 1	Click to select which active connection takes precedence when switching between available WAN links.
Priority 2	
Priority 3	
Signal Strength Detection	
Detection Interval	Enter the value in seconds to define the interval to activate the signal strength detection function.
Continuous Repeat Times	Enter the value to define the frequency of the signal detection function. Value: 2 to 10.
WLAN Handover	
RSSI Threshold	Enter the value in dBm to define the threshold for removing a client when it goes below the value. Value: -70 to -110.
Cellular Handover	
3G RSSI Threshold	Enter the value in dBm to define the 3G threshold for removing a client when it goes below the value. Value: -70 to -110.
4G RDDI Threshold	Enter the value in dBm to define the 4G threshold for removing a client when it goes below the value. Value: -65 to -95.
Submit	Click Submit to save the values and update the screen.

3.5 L2 Switch

3.5.1 Port Mirror

Port mirroring function allows the sending of a copy of network packets seen on one switch port to a network monitoring connection on another switch port. Port mirroring can be used to analyze and debug data or diagnose errors on a network or to mirror either inbound or outbound traffic (or both).

There are no preset values in the Port Mirror. The displayed values do not represent the actual setting values.

To access this page, click **L2 Switching > Port Mirror**.

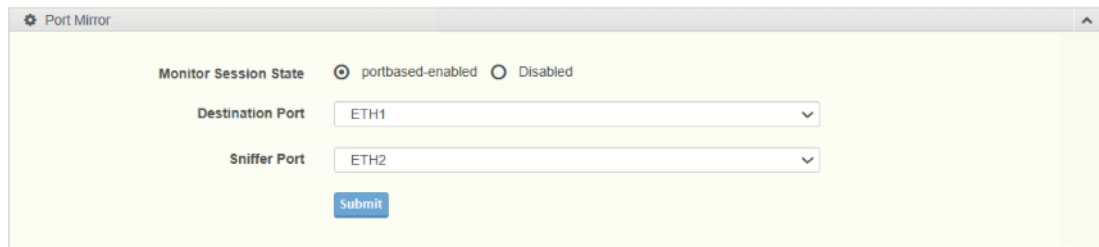


Figure 3.37 L2 Switching > Port Mirror

The following table describes the items in the previous figure.

Item	Description
Monitor session state	Click the drop-down menu to enable or disable the session mode for a selected session ID.
Destination Port	Click the drop-down menu to select the destination port and receive all the traffic from configured mirrored port(s).
Sniffer Ports	Click to select the port to function as the dedicated eavesdropper and receive copies of traffic from mirrored ports.
Submit	Click Submit to save the values and update the screen.

3.5.2 Storm Control

The Storm Control page allows you to setup the units and Preamble/IFG to manage the occurrence of packet flooding on the LAN and consequent traffic to prevent the degrading of network performance.

3.5.2.1 Global Settings

To access this page, click **Security > Storm Control > Global Settings**.

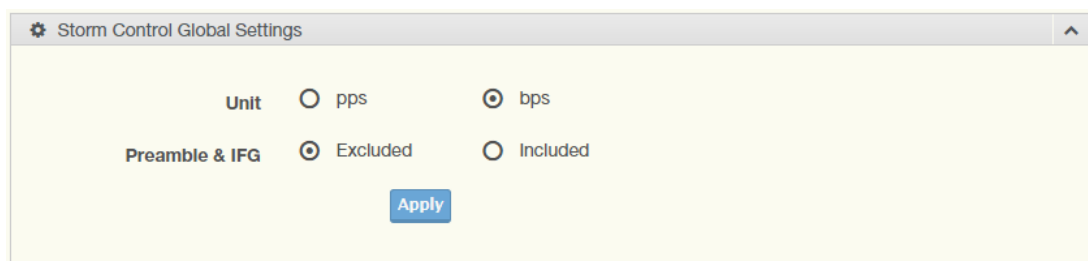


Figure 3.38 Security > Storm Control > Global Settings

The following table describes the items in the previous figure.

Item	Description
Unit	Select pps or bps control units for the Storm Control function.

Item	Description
Preamble & IFG	Select Excluded or Included to setup the Storm Control Global settings. <ul style="list-style-type: none"> ■ Excluded: exclude preamble & IFG (20 bytes) when count ingress storm control rate. ■ Included: include preamble & IFG (20 bytes) when count ingress storm control rate.
Apply	Click Apply to save the values and update the screen.

The ensuing table for **Storm Control Global Information** settings are informational only and display the following: Unit and Preamble & IFG.

3.5.2.2 Port Settings

The Port Settings page allows you to configure the port and the type of storm control association along with the value of the storm rate for the selected port.

To access this page, click **Security > Storm Control > Port Settings**.

Figure 3.39 Security > Storm Control > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to designate the local port for the Storm Control function.
Port State	Select Disabled or Enabled to define the port state
Action	Click the drop-down menu to select the type of action to designate for the selected port during a Storm Control incident. The options are Drop and Shutdown.
Type Enable	Click the radio button to enable Broadcast, Unknown Multicast, or Unknown Unicast. <ul style="list-style-type: none"> ■ Broadcast: Select the variable in Kbps to define the broadcast bandwidth. ■ Unknown Multicast: Select the variable in Kbps to define the multicast setting. ■ Broadcast: Select the variable in Kbps to define the unknown unicast setting.
Apply	Click Apply to save the values and update the screen.

The ensuing table for **Storm Control Port Information** settings are informational only and display the following: Port, Port State, Broadcast (Kbps), Unknown Multicast (Kbps), Unknown Unicast (Kbps) and Action.

3.5.3 LLDP

LLDP is a one-way protocol without request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function.

3.5.3.1 LLDP System Settings

The LLDP System Settings allows you to configure the status (enabled or disabled) for the protocol, set the interval for frame transmission, set the hold time multiplier and the re-initialization delay.

To access this page, click **Management > LLDP > LLDP System Settings**.

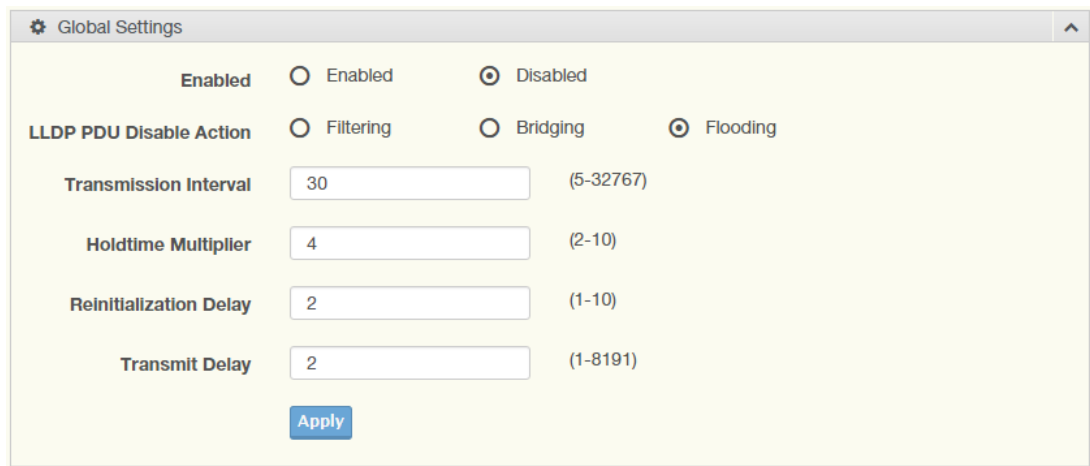


Figure 3.40 Management > LLDP > LLDP System Settings

The following table describes the items in the previous figure.

Item	Description
Enabled	Click Enabled or Disabled to set the Global Settings state.
LLDP PDU Disable Action	Click to select the LLDP PDU handling action when LLDP is globally disabled. Options include: Filtered, Bridged, or Flooded.
Transmission Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5 to 32768 seconds.
Holdtime Multiplier	Select the multiplier on the transmit interval to assign to TTL.
Reinitialization Delay	Select the delay length before re-initialization.
Transmit Delay	Select the delay after an LLDP frame is sent.
Apply	Click Apply to save the values and update the screen.

The ensuing table for **LLDP Global Config** settings are informational only and display the following: LLDP Enabled, LLDP PDU Disable Action, Transmission Interval, Holdtime Multiplier, Reinitialization Delay and Transmit Delay.

3.5.3.2 LLDP Local Device Info

The LLDP Local Device Info page allows you to view information regarding network devices, providing that the switch has already obtained LLDP information on the devices.

To access this page, click **Management > LLDP > LLDP Local Device Info**.

The ensuing table for **Local Device Summary** settings are informational only and display the following: Chassis ID Subtype, Chassis ID, System Name, System Description, Capabilities Supported, Capabilities Enabled and Port ID Subtype.

The ensuing table for **Port Status** settings are informational only and display the following: Port, Selected VLAN and **Detail** (click the radio box and click **Detail** to displays the details).

3.5.3.3 LLDP Remote Device Info

The LLDP Remote Device Info page allows you to view information about remote devices, LLDP information must be available on the switch.

To access this page, click **Management > LLDP > LLDP Remote Device Info**.

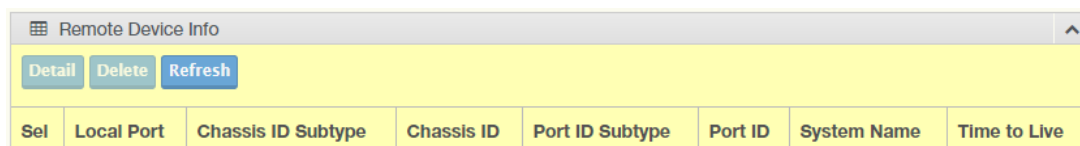


Figure 3.41 Management > LLDP > LLDP Remote Device Info

The following table describes the items in the previous figure.

Item	Description
Detail	Click to display the device details.
Delete	Click to delete the selected devices.
Refresh	Click to refresh the remote device information list.

3.6 Management

3.6.1 Password Manager

To access this page, click **Management > Password Manager**.

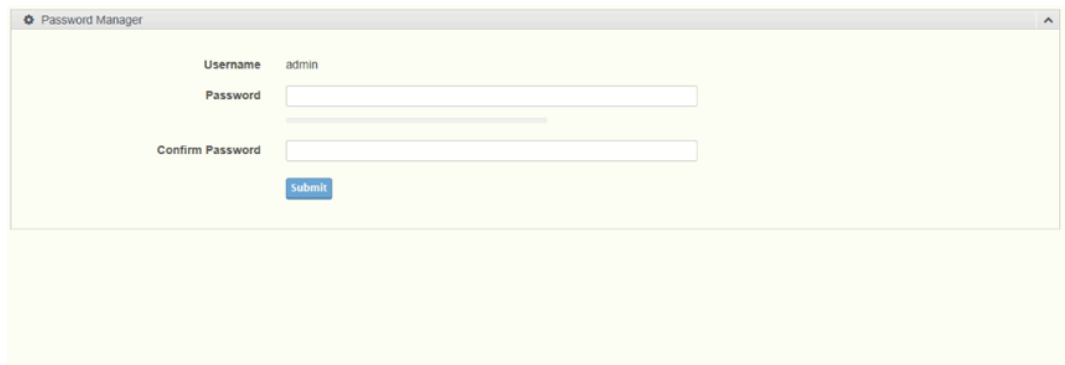


Figure 3.42 Management > Password Manager

The following table describes the items in the previous figure.

Item	Description
Password Manager	
Username	Displays the current user name.
Password	Enter the character set for the define password type.
Confirm Password	Retype the password entry to confirm the profile password.
Submit	Click Submit to save the values and update the screen.

3.6.2 Syslog

Users can enable the syslog function to record log events or messages locally or on a remote syslog server.

To access this page, click **Management > Syslog**.

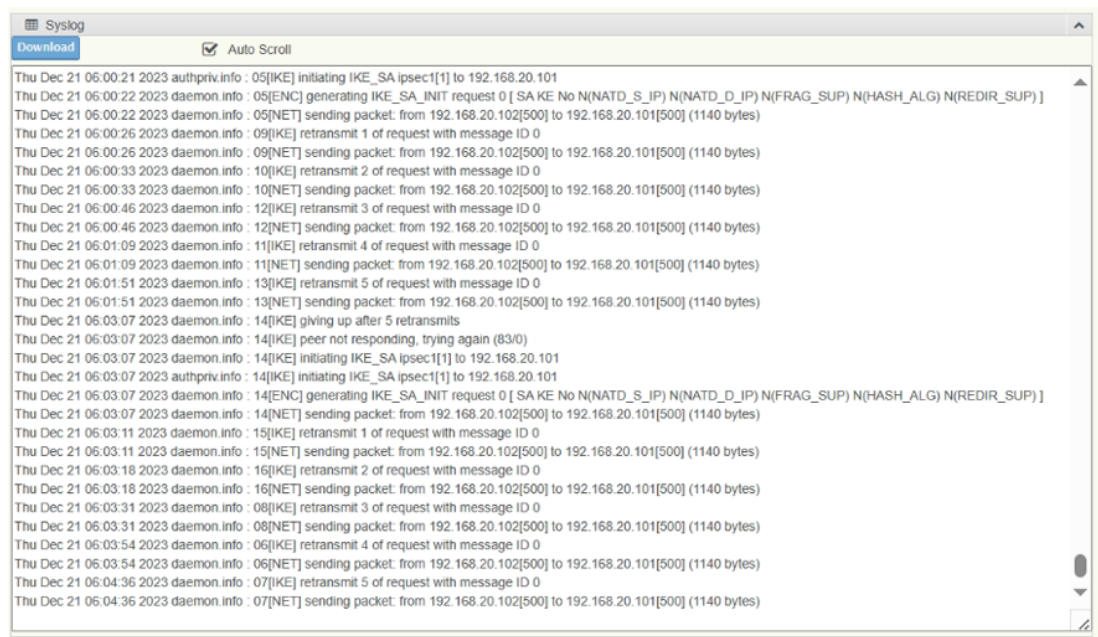


Figure 3.43 Management > Syslog

The following table describes the items in the previous figure.

Item	Description
Download	Click Download to download the log file.
Auto Scroll	Click the checkbox to enable the Auto Scroll function.

3.6.3 NTP / Time

To access this page, click **Management > NTP / Time**.

Figure 3.44 Management > NTP / Time

The following table describes the items in the previous figure.

Item	Description
System Time	Displays the system date and time.
NTP Client	
NTP Service	Click the drop-down menu to enable the NTP server.
Manual Time	Set the system date and time.
Time Zone	Click the drop-down menu to select a system time zone.
NTP Server	Enter the address of the NTP server.
NTP Server	
NTP Server	Enter the remote server ID of the NTP server.
Submit	Click Submit to save the values and update the screen.

3.6.4 Applications

To access this page, click **Management > Applications**.

The screenshot shows the 'Applications' configuration window. It has a title bar with a gear icon and an expand/collapse arrow. The main content area is divided into three sections: HTTP, SSH, and Telnet. The HTTP section contains four settings: 'Redirect HTTP requests to HTTPS' (a dropdown menu set to 'Enable'), 'HTTPS port' (a text input field with '443'), 'HTTP port' (a text input field with '80'), and 'HTTP remote management' (a dropdown menu set to 'Disable'). The SSH section contains one setting: 'SSH' (radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected). The Telnet section contains one setting: 'Telnet' (radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected). At the bottom of the Telnet section is a blue 'Submit' button.

Figure 3.45 Management > Applications

The following table describes the items in the previous figure.

Item	Description
HTTP	
Redirect HTTP Requests to HTTPS	Click to enable (default) or disable the redirect to HTTP function.
HTTPS Port	Enter the port number for the assigned remote HTTPS address.
HTTP Port	Enter the port number for the assigned remote HTTPS address.
HTTP remote management	Click to enable or disable (default) the remote management access.
SSH	
SSH	Click to enable or disable (default) the SSH function.
Telnet	
Telnet	Click to enable or disable (default) the Telnet function.
Submit	Click Submit to save the values and update the screen.

3.6.5 Configuration Manager

To access this page, click **Management > Configuration Manager**.

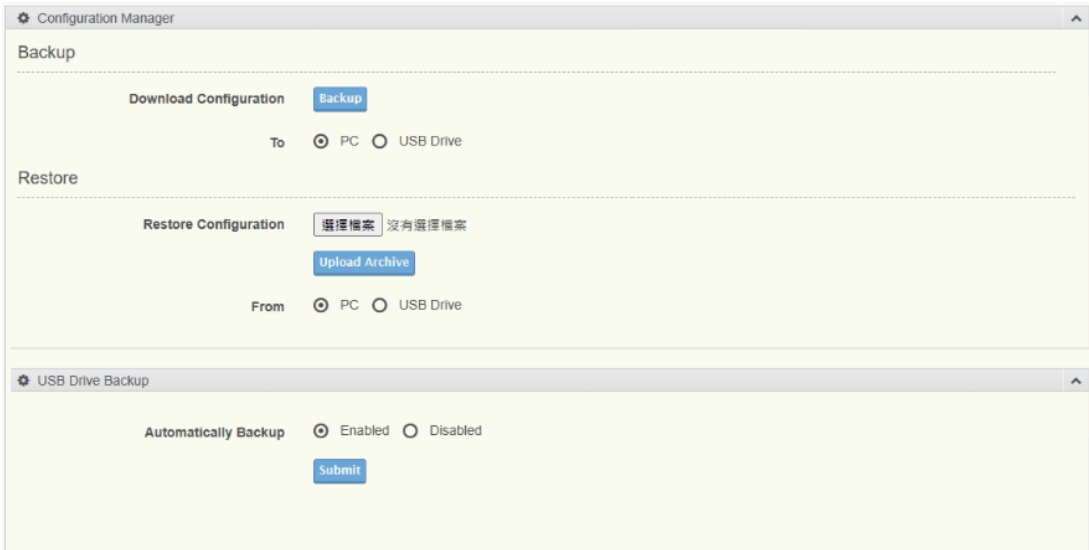


Figure 3.46 Management > Configuration Manager

The following table describes the items in the previous figure.

Item	Description
Backup	
Download Configuration	Click Backup to backup the device settings.
To	Click PC or USB Drive to select the correct file location.
Restore	
Choose File	Click Choose File to select the configuration file.
Upload Archive	Click Upload Archive to restore the configuration to the device.
From	Click PC or USB Drive to select the correct file location.
Automatically Backup	Select Enabled or Disabled to enable the function.
Submit	Click Submit to save the values and update the screen.

3.6.6 Firmware Upgrade

To access this page, click **Management > Firmware Upgrade**.



Figure 3.47 Management > Firmware Upgrade

The following table describes the items in the previous figure.

Item	Description
Upgrade Manager	Click Choose File to select the configuration file.
Upload	Click Upload to upload to the current version.

3.6.7 Reset System

To access this page, click **Management > Reset System**.



Figure 3.48 Management > Reset System

The following table describes the items in the previous figure.

Item	Description
Reset	Click Reset to have all configuration parameters reset to their factory default values. All changes that have been made will be lost, even if you have issued a save.

3.6.8 Reboot Device

To access this page, click **Management > Reboot Device**.



Figure 3.49 Management > Reboot Device

The following table describes the items in the previous figure.

Item	Description
Reset	Click Reset to have all configuration parameters reset to their factory default values. All changes that have been made will be lost, even if you have issued a save.

3.6.9 Apply Configuration

To access this page, click **Management > Apply Configuration**.

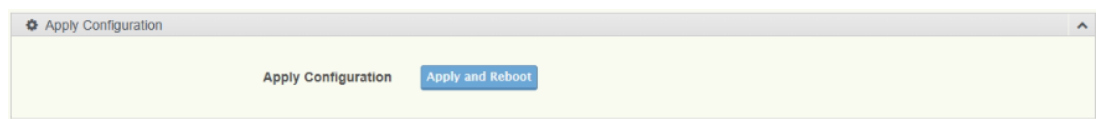


Figure 3.50 Management > Apply Configuration

The following table describes the items in the previous figure.

Item	Description
Apply Configuration	Click Apply and Reboot to have configuration changes you have made to be saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.

3.7 Tools

3.7.1 Diagnostics

To access this page, click **Tools > Diagnostics**.

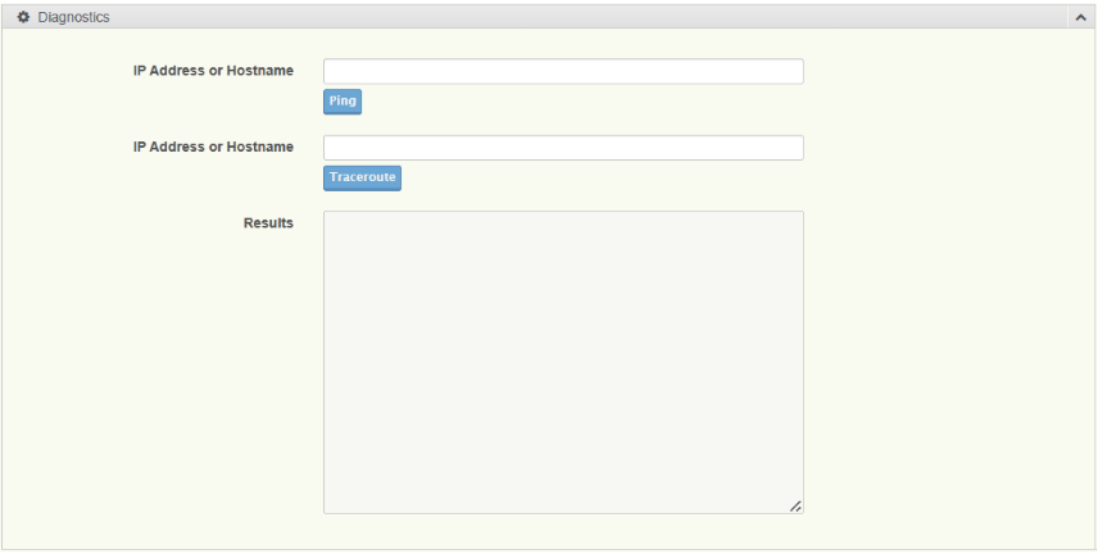


Figure 3.51 Tools > Diagnostics

The following table describes the items in the previous figure.

Item	Description
IP Address or Hostname	Enter the IP address or hostname of a device on the network to execute a ping test. Click Ping to initiate and display the ping result for the device.
IP Address or Hostname	Enter the IP address or hostname of the host to initiate a trace route from the switch to the defined host. Click Traceroute to initiate and display the trace results.
Results	Displays the results of the Ping or Traceroute test.

3.7.2 GPS

3.7.2.1 Basic

To access this page, click **Tools > GPS > Basic**.

The screenshot displays the 'GPS Settings' interface. At the top, there's a 'GPS' status section with 'Enabled' selected. Below this is the 'GNSS Server Configuration' section, which includes a 'Server Port' input field set to '2947' (with a range of 1-65535) and an 'Allow Clients From' dropdown menu set to 'LAN Only'. A 'Submit' button is located below these fields. The 'GPS Data' section is a table with two columns: 'Information Name' and 'Information Value'. It lists 'Time', 'Latitude', 'Longitude', and 'Speed'. The 'Satellite List' section is a table with columns: 'PRN', 'Elevation', 'Azimuth', 'SNR', and 'Used'. To the right of this table is a circular diagram representing a compass rose with 'N', 'S', 'E', and 'W' markers, used for visualizing satellite azimuth.

Figure 3.52 Tools > GPS > Basic

The following table describes the items in the previous figure.

Item	Description
GPS	Click to enable or disable the GPS function.
GNSS Server Configuration	
Server Port	Enter the port number which will be designated to allow authorized devices and applications to connect and exchange GNSS data.
Allow Clients From	Click to select which source channel is authorized to connect and exchange GNSS data.
Submit	Click Submit to save the values and update the screen.
Information Name	Displays the geolocation and time information from a GPS receiver. Values: Time, Latitude, Longitude, Speed
Information Value	Displays the values of the information listed in the previous field.
PRN	Displays the Pseudo-random Noise sequence of the satellite.
Elevation	Displays the elevation of the satellite.
Azimuth	Displays the azimuth of the satellite.
SNR	Displays the signal-to-noise ratio of the satellite.
Used	Displays the usage status of the listing.

3.7.2.2 GPS Report

To access this page, click **Tools > GPS > GPS Report**.



Figure 3.53 Tools > GPS > GPS Report

The following table describes the items in the previous figure.

Item	Description
GPS Report	Click to enable or disable the Remote Log function.
Remote IP	Enter the IP address of the remote server to receive the report.
UDP Port	Enter the Port of the designated remote server to receive the report.
Data Format	Click to select the format type for the log reporting: NMEA, JSON, or Both.
Delete	Click to delete the selected GPS report.
Submit	Click Submit to save the values and update the screen.



Enabling an Intelligent Planet

www.advantech.com

Please verify specifications before quoting. This guide is intended for reference purposes only.

All product specifications are subject to change without notice.

No part of this publication may be reproduced in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission of the publisher.

All brand and product names are trademarks or registered trademarks of their respective companies.

© Advantech Co., Ltd. 2024