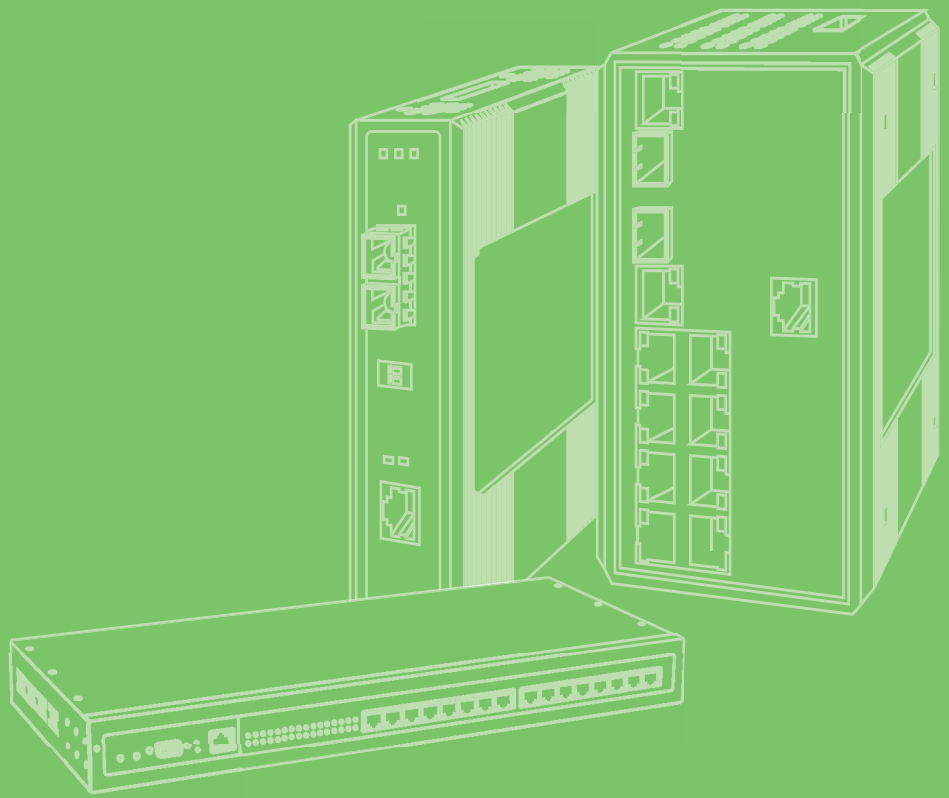


User Manual



EKI-9502G Series

EN50155 Train-To-Ground Wi-Fi/
Cellular Router

ADVANTECH

Enabling an Intelligent Planet

Copyright

The documentation and the software included with this product are copyrighted 2021 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	Specifications	2
1.4	Dimensions	4
Chapter 2	Getting Started	5
2.1	Hardware	6
2.1.1	Front View	6
2.1.2	LED Indicators	7
2.2	Connecting Hardware	8
2.2.1	SIM Cards	8
2.2.2	Wall Mounting	12
2.2.3	Wireless Connection	13
2.2.4	Network Connection	14
2.2.5	USB Connection	15
2.2.6	Console Connection	15
2.2.7	Power Connection	15
Chapter 3	Web Interface	20
3.1	Log In	21
3.1.1	Changing Default Password	22
3.2	Overview	23
3.3	Interface	25
3.3.1	LAN	25
3.3.2	ETHWAN	26
3.3.3	1 (WLAN)	27
3.3.4	2 (WLAN)	40
3.3.5	5 (Cellular)	40
3.4	Networking	44
3.4.1	Static Route	44
3.4.2	Forwarding	44
3.4.3	Scurity	46
3.4.4	OpenVPN	47
3.4.5	GRE	50
3.4.6	QoS Settings	51
3.4.7	WAN Load Balancing	53
3.4.8	WAN Handover	54
3.5	Management	56
3.5.1	Password Manager	56
3.5.2	Syslog	56
3.5.3	Alert	57
3.5.4	NTP / Time	57
3.5.5	Captive Portal	58
3.5.6	Applications	60
3.5.7	Configuration Manager	61
3.5.8	Firmware Upgrade	62
3.5.9	Reset System	62
3.5.10	Reboot Device	62
3.5.11	Apply Configuration	63
3.6	Tools	63

3.6.1	Diagnostics	63
3.6.2	GPS	64

List of Figures

Figure 1.1	Dimensions.....	4
Figure 2.1	Front View	6
Figure 2.2	System LED Panel	7
Figure 2.3	SIM Population Matrix	8
Figure 2.4	LTE Module Installation Order.....	8
Figure 2.5	LTE Module Installation Order.....	9
Figure 2.6	Releasing a Front Panel.....	10
Figure 2.7	Opening a Front Panel	10
Figure 2.8	Unlocking a Slot Cover.....	11
Figure 2.9	Installing a SIM Card	11
Figure 2.10	Installing a Front Panel.....	11
Figure 2.11	Securing a Front Panel.....	12
Figure 2.12	Wall Mount Installation	13
Figure 2.13	Installing an Antenna.....	13
Figure 2.14	Positioning the Antenna	14
Figure 2.15	M12 X-Coded Connector Pin Assignment.....	14
Figure 2.16	M12 A-Coded Connector Pin Assignment.....	15
Figure 2.17	Power Wiring for EKI-9502G Series.....	16
Figure 2.18	Grounding Connection	17
Figure 2.19	Removing a Protection Cap	18
Figure 2.20	Installing the Power Cable.....	18
Figure 2.21	Removing the Power Cable.....	19
Figure 2.22	Standard M12 4 Poles Male DC Power Input Connector.....	19
Figure 3.1	Login Screen	21
Figure 3.2	Management > Password Manager	22
Figure 3.3	Overview	23
Figure 3.4	Overview Continued.....	23
Figure 3.5	Interface > LAN	25
Figure 3.6	Interface > ETHWAN.....	26
Figure 3.7	1 (WLAN) > Basic.....	27
Figure 3.8	1 (WLAN) > Operation Mode > Wireless WAN	29
Figure 3.9	1 WLAN > Advanced.....	31
Figure 3.10	WLAN > Advanced.....	32
Figure 3.11	Interface > 1 (WLAN) > Security > Security Mode	33
Figure 3.12	Interface > 1 (WLAN) > Security > Security Mode > WEP	34
Figure 3.13	Interface > 1 (WLAN) > Security > Security Mode > WPA-Personal.....	35
Figure 3.14	Interface > 1 (WLAN) > Security > Security Mode > WPA/WPA2-Enterprise	36
Figure 3.15	Interface > 1 (WLAN) > Statistics	37
Figure 3.16	Interface > 1 (WLAN) > Site Survey	38
Figure 3.17	Interface > 1 (WLAN) > Traffic Control.....	38
Figure 3.18	Interface > 1 (WLAN) > Traffic Control.....	39
Figure 3.19	Interface > 1 (WLAN) > Log	40
Figure 3.20	Interface > 5 (Cellular) > Basic.....	41
Figure 3.21	Interface > 5 (Cellular) > SIM 1	42
Figure 3.22	Interface > 5 (Cellular) > SIM 1	43
Figure 3.23	Networking > Static Route.....	44
Figure 3.24	Networking > Forwarding > Port Forwarding.....	45
Figure 3.25	Networking > Forwarding > DMZ	45
Figure 3.26	Networking > Security > Filter	46
Figure 3.27	Networking > Security > VPN Passthrough.....	47
Figure 3.28	Networking > OpenVPN > Tunnel 1	48
Figure 3.29	Networking > GRE> Tunnel 1	50
Figure 3.30	Networking > QoS Settings> QoS Settings.....	51
Figure 3.31	Networking > QoS Settings> QoS IP Base Rules	52
Figure 3.32	Networking > QoS Settings> QoS Protocol Base Rules	52
Figure 3.33	Networking > WAN Load Balancing	53

Figure 3.34	Networking > WAN Handover.....	54
Figure 3.35	Networking > WAN Handover.....	55
Figure 3.36	Management > Password Manager.....	56
Figure 3.37	Management > Syslog.....	56
Figure 3.38	Management > Alert	57
Figure 3.39	Management > NTP / Time	57
Figure 3.40	Management > Captive Portal > Basic	58
Figure 3.41	Management > Captive Portal > Custom Pages	59
Figure 3.42	Management > Captive Portal > Log.....	60
Figure 3.43	Management > Applications	60
Figure 3.44	Management > Configuration Manager	61
Figure 3.45	Management > Firmware Upgrade.....	62
Figure 3.46	Management > Reset System	62
Figure 3.47	Management > Reboot Device	62
Figure 3.48	Management > Apply Configuration	63
Figure 3.49	Tools > Diagnostics	63
Figure 3.50	Tools > GPS > Basic	64
Figure 3.51	Tools > GPS > GPS Report.....	65

Chapter 1

Introduction

1.1 Overview

The EKI-9502G Series train-to-ground Wi-Fi/cellular router is designed for rolling stock applications. It provides secure Internet connectivity while offering superior application flexibility. EKI-9502G Series provides automatic wireless failover between WLAN and WAN connectivity and supports up to four WWAN(LTE) modules with dual SIM cards installation and up to two WIFI modules for 802.11a/b/g/n/ac with 2.4 Ghz/ 5 Ghz selective. With load balance, VPN tunneling, and configuration backup, it provides stable and reliable wireless connectivity that is ideal for transportation applications.

1.2 Device Features

- Cellular connectivity with dual SIM cards designed for each cellular module
- Supports up to 4 WWAN connectivity
- Supports wide temperature range: -40 ~ 70°C
- Designed with 24Vdc to 110Vdc isolated power input
- Flexible design with serial interface for Modbus RTU and serial communication protocol
- Supports GRE, OpenVPN secured tunnel
- Complies with EN50155
- Supports multi-WAN load balance
- Supports up to 1.3Gbps with 3x3 MIMO Wi-Fi

1.3 Specifications

Specifications	Description
Interface	
Power Connector	M12 A-Code Male
I/O Port	2 x 10/100/1000 Base-T M12 X-coded Female
Console Port	RS-232 (Terminal Block Male)
Serial Port	2 x RS-232/422/485 Selectable (Terminal Block Male)
USB Port	USB 2.0 Type-A female
GPS	1 x U-Blox NEO-8 with SMA Female connector
Cellular Interface	
LTE Bit rate	300 Mbps (DL), 50 Mbps (UL)
LTE Bands	B20 (800 MHz), B8 (900 MHz), B3 (1800 MHz), B1 (2100 MHz), B7 (2600 MHz)
3G Bit Rate	42.0 Mbps (DL), 5.76 Mbps (UL)
3G Bands	B1, B2, B3, B4, B5, B8
No. of SIM Slots	8
SIM Card Type	Mini Sim (2FF) 1.8V and 3V
ANT Connector	6 x SMA Female Connector
Physical	
Enclosure	Metal shell with solid mounting kits
Mounting	Wall
Dimensions (W x H x D)	280 x 160 x 85mm (11" x 6.3" x 3.5") without wall mount ears
Weight	1.2 Kg (2.65 lbs)

Specifications	Description	
LED Display	System LED	Power, Status
	Port LED	■ WLAN/LTE: Quality ■ LAN: Link/Active
Environment	Operating Temperature	-40 ~ 70°C (-40 ~ 158°F)
	Storage Temperature	-40 ~ 80°C (-40 ~ 176°F)
	Operating Humidity	10 ~ 95% RH
WLAN Modulation Techniques	IEEE 802.11a/g	OFDM (BPSK, QPSK, 16-QAM, 64-QAM)
	IEEE 802.11b	DSSS (DBPSK, DQPSK, CCK)
	IEEE 802.11n	OFDM (BPSK, QPSK, 16-QAM, 64-QAM)
	IEEE 802.11ac	OFDM (BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM)
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	802.11g 15 dBm 802.11a 15 dBm 802.11n/2.4GHz HT20: 18 dBm@MCS7 HT40: 18 dBm@MCS7 802.11n/5GHz HT20: 18 dBm@MCS7 HT40: 17 dBm@MCS7 802.11ac VHT80 15 dBm@MCS9
Receiver Sensitivity	802.11a Sensitivity	-73 dBm @ 54 Mbps
	802.11g Sensitivity	-75 dBm @ 54 Mbps
	802.11n/2.4GHz	HT20 -72 dBm @ MCS7 HT40 -68 dBm @ MCS7
	802.11n/5GHz	HT20 -70 dBm @ MCS7 HT40 -68 dBm @ MCS7
	802.11ac	VHT80 -57 dBm @ MCS9
Power	Power Input	24-110 VDC (±30%)
	Power Connector	M12 A-coded with 4 Poles
	Power Consumption	21W

Specifications	Description	
Software	Management	Web UI
	Wireless	Radio on/off, WMM, Output Power Control, Fragmentation Length, Beacon Interval, RTS/CTS threshold, DTIM Interval
Regulatory Approvals	EMC	CE, FCC Part 15 Subpart B (Class B)

1.4 Dimensions

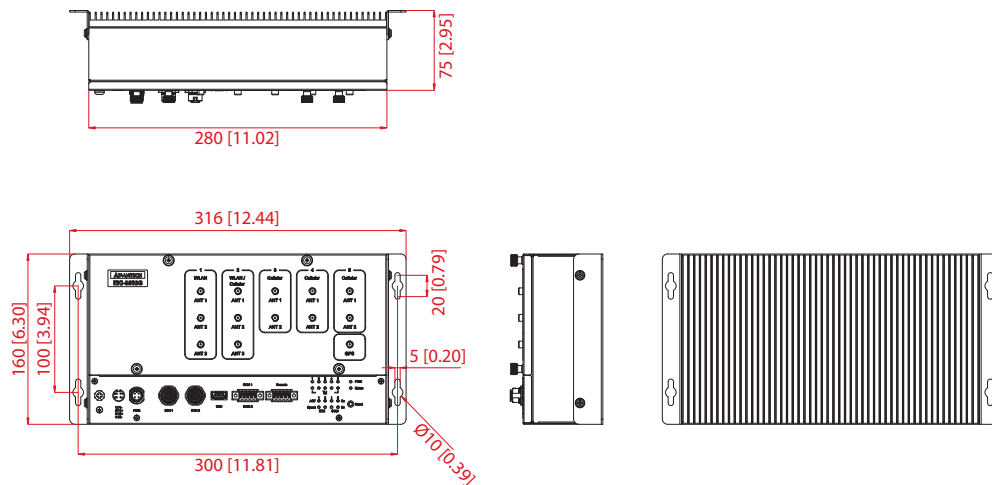


Figure 1.1 Dimensions

Chapter 2

Getting Started

2.1 Hardware

2.1.1 Front View

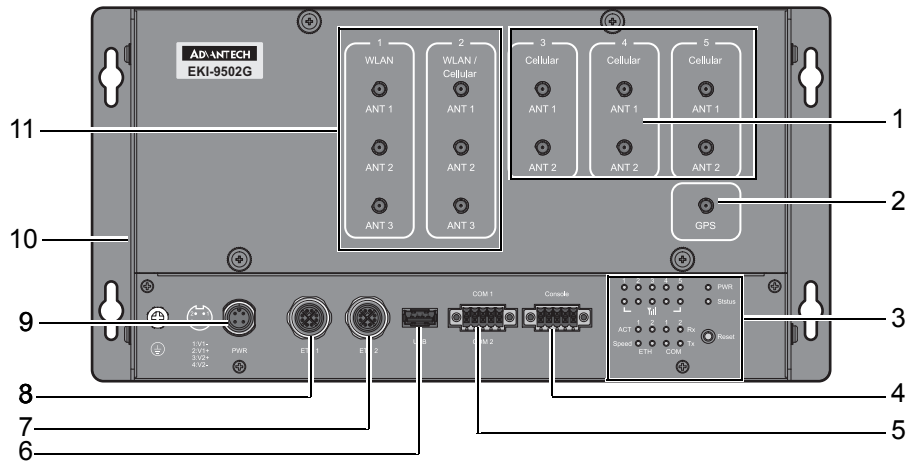


Figure 2.1 Front View

No.	Item	Description
1.	Antenna connector	Connector for LTE antenna.
2.	Antenna connector	Connector for GPS antenna, U-Blox NEO-8 (SMA Female connector)
3.	System LED panel	See “LED Indicators” on page 7 for further details.
4.	Console port	RS-232 (Terminal Block Male)
5.	Serial Port	2 x RS-232/422/485 Selectable (Terminal Block Male)
6.	USB port	USB 2.0 Front IO (Type A)
7.	ETH port 2	ETH ports x 2.
8.	ETH port 1	
9.	Power input port	M12 4-pin (male) DC power connector port.
10.	Wall mounting brackets	Dual brackets for wall mounting.
11.	Antenna connector	Connector for WLAN antenna.

2.1.2 LED Indicators

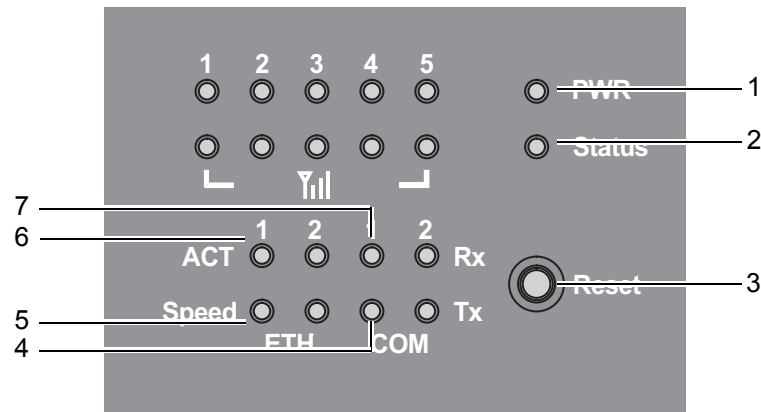


Figure 2.2 System LED Panel

No.	LED Name	LED Color	Description
1.	PWR1	Green	Power is on.
		Off	Power is off or power error condition exists.
2.	Status	Green, solid	System is ready.
		Off	System is not functioning.
3.	Reset Button	System reboot: Press and hold the Reset button for 2 seconds. Reset configuration to factory default: Press and hold the Reset button for 5 seconds.	
4.	COM	Tx	Blinking – There is activity on this port. Off – No link is established.
5.	Ethernet	Speed	Green on – Operating as a 1000 Gigabit connection. Amber on – Operating as a 100 Mbps connection. Off – Operating as a 10 Mbps connection.
6.	Ethernet	Activity	Blinking – There is activity on this port. Off – No link is established.
7.	COM	Rx	Blinking – There is activity on this port. Off – No link is established.

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.

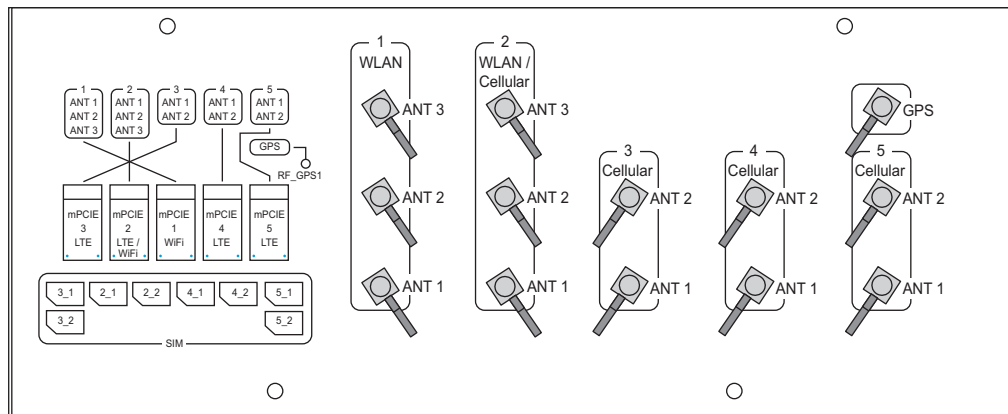


Figure 2.3 SIM Population Matrix

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

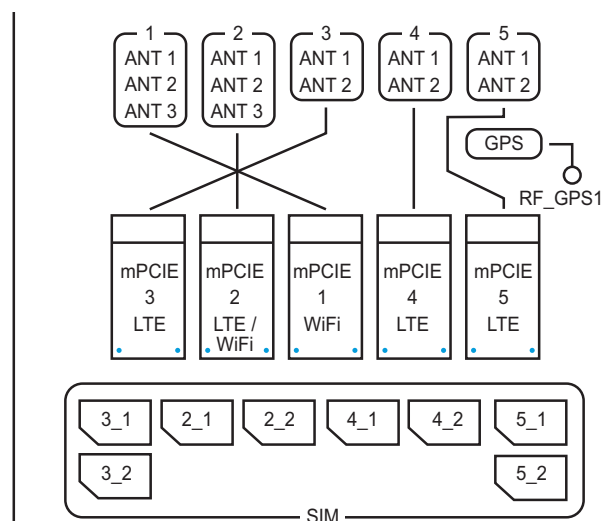


Figure 2.4 LTE Module Installation Order

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

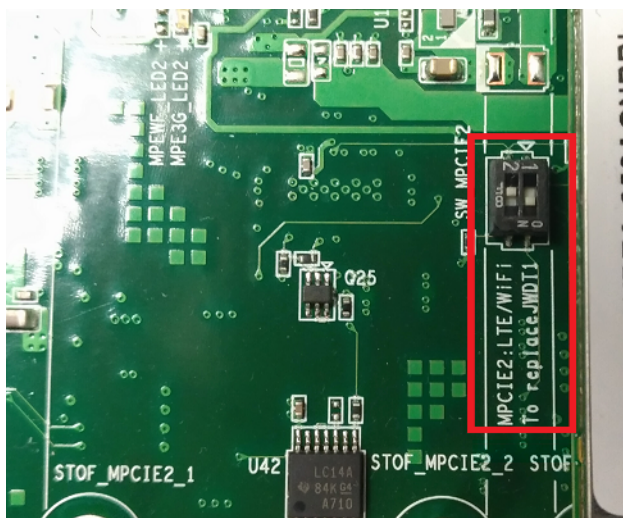


Figure 2.5 LTE Module Installation Order

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.

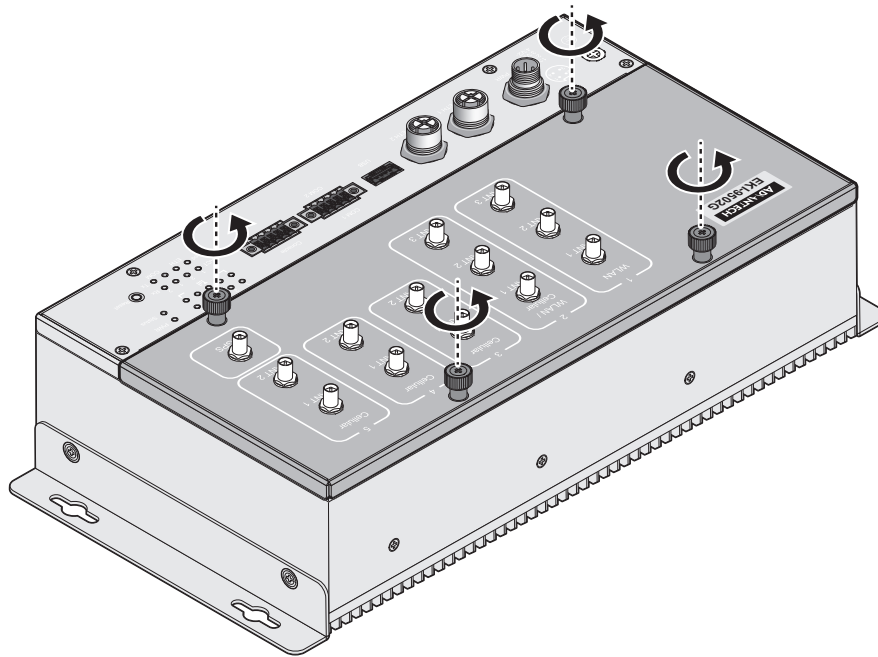


Figure 2.6 Releasing a Front Panel

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.

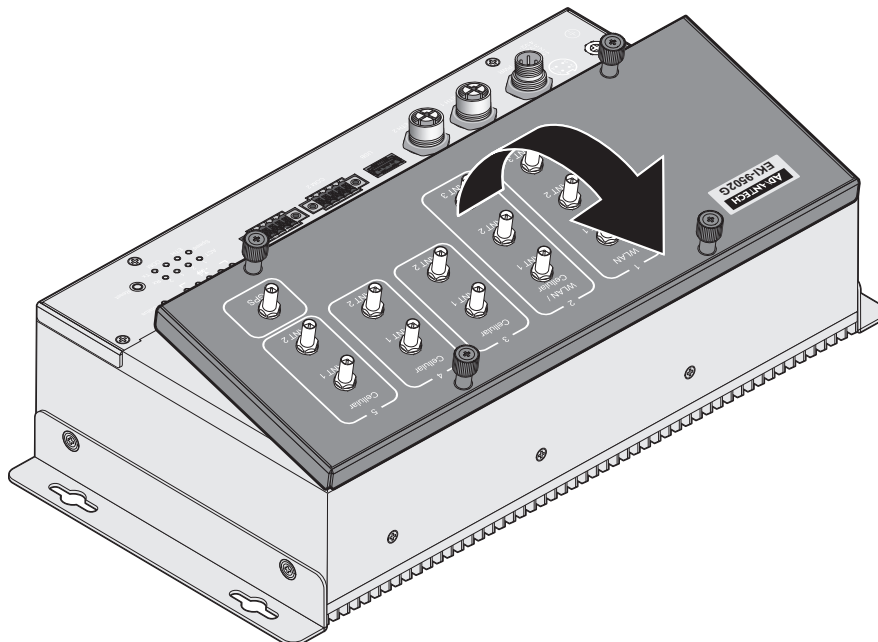


Figure 2.7 Opening a Front Panel

4. Locate the SIM slot for installation, see “SIM Population Matrix” on page 8 for further information.

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

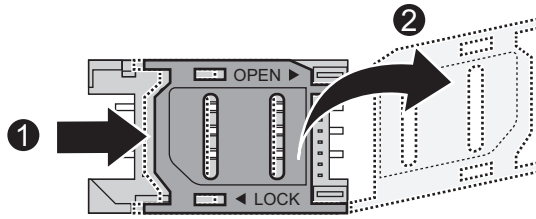


Figure 2.8 Unlocking a Slot Cover

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.

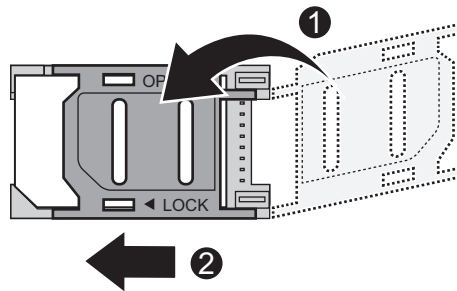


Figure 2.9 Installing a SIM Card

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.

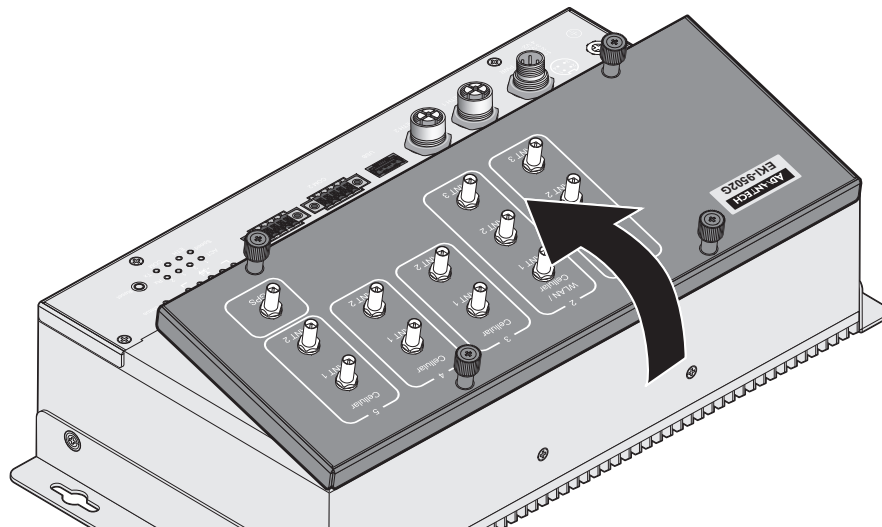


Figure 2.10 Installing a Front Panel

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

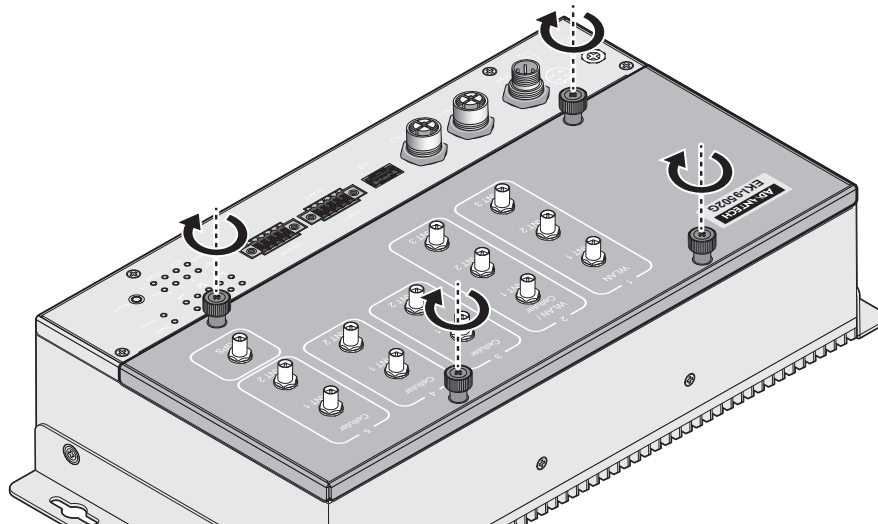


Figure 2.11 Securing a Front Panel

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. Insert the mounting screws on the drilled locations and tighten halfway. Do not tighten complete or the bracket cannot be installed properly.

7. Once the brackets are properly inserted through the screws, lower the device to lock the screws in the keyholes.

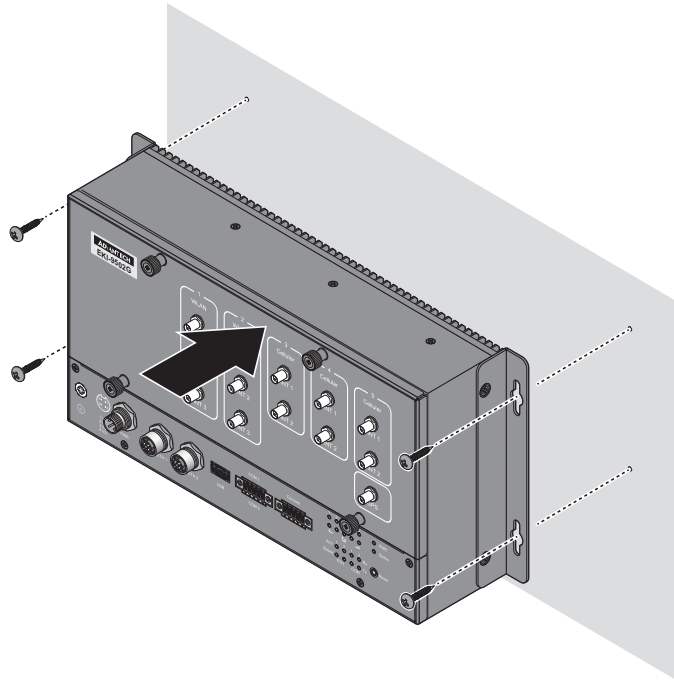


Figure 2.12 Wall Mount Installation

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

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.

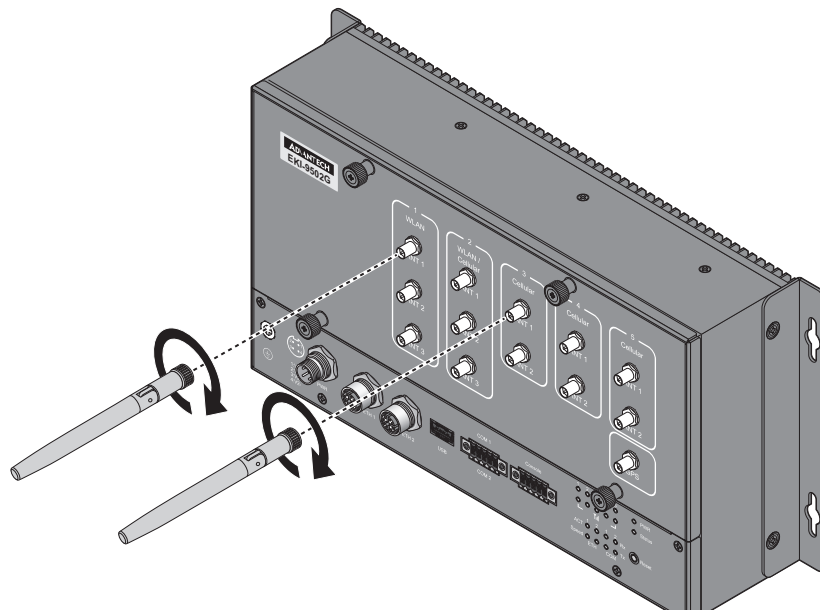


Figure 2.13 Installing an Antenna

2. Position the antenna for optimal signal strength.

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

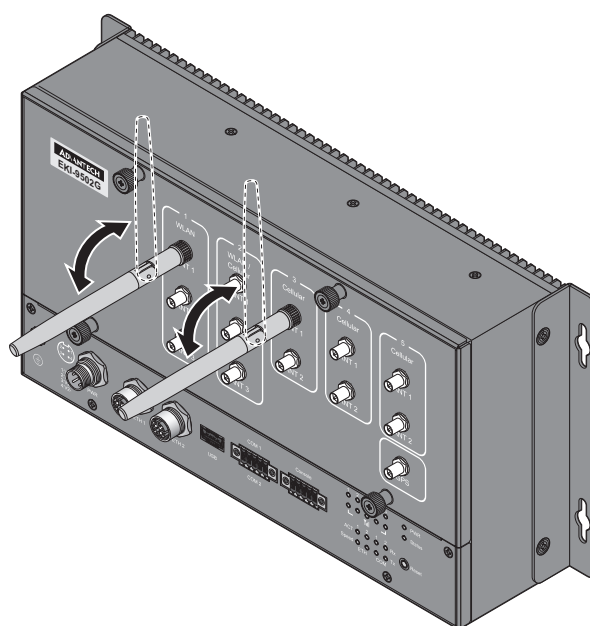


Figure 2.14 Positioning the Antenna

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

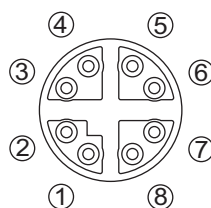


Figure 2.15 M12 X-Coded Connector Pin Assignment

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

2.2.5 USB Connection

The EKI-9502G Series includes a USB 2.0 Type-A port located on the front panel for firmware management.

Regarding the use of USB drives, if a USB drive with a configuration file is plugged into the device with default settings, the device reads the configuration file at boot up and applies the configuration automatically. This is dependent of the Automatic Backup function and does not require the function to be enabled.

2.2.6 Console Connection

The console port, used to access the managed switch's software, is an RS-232 terminal block (male) port.

2.2.6.1 RS-232 Terminal Block Pin Assignment

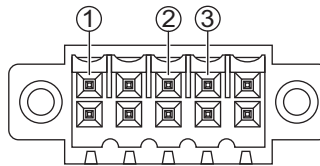


Figure 2.16 M12 A-Coded Connector Pin Assignment

Pin	Description
1	Ground
2	TX
3	RX

2.2.7 Power Connection

2.2.7.1 Overview

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



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



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

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



The devices can be powered by using the same DC source used to power other devices. A DC voltage range of 24 to 110 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.

EKI-9502G Series support 24 to 110 V_{DC}. Dual power inputs are supported and allow you to connect a backup power source.

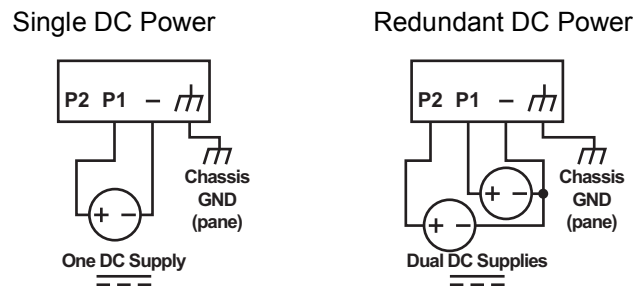



Figure 2.17 Power Wiring for EKI-9502G Series

2.2.7.2 Considerations

Take into consideration the following guidelines before wiring the device:

- The Terminal Block (CN1) is suitable for 12-24 AWG (3.31 - 0.205 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.

2.2.7.3 Grounding the Device

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



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

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



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



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



Caution! Do not block air ventilation 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.

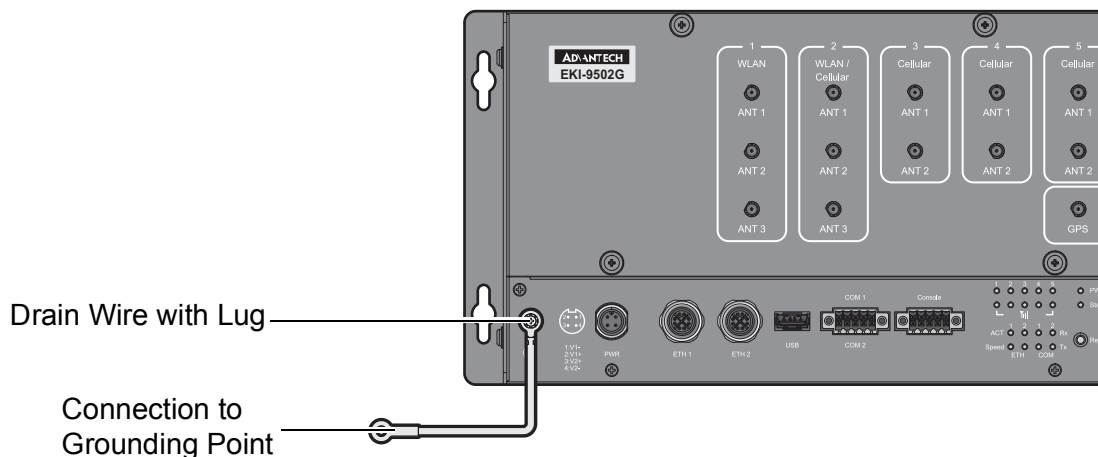


Figure 2.18 Grounding Connection

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.



2.2.7.4 Wiring the Power Inputs

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



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

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



To wire 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.

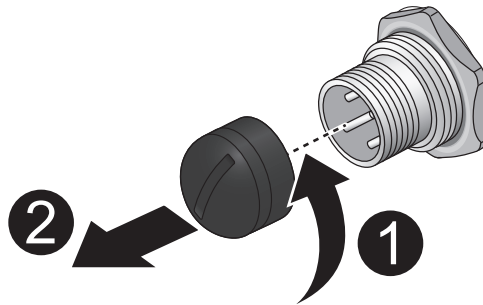


Figure 2.19 Removing a Protection Cap

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.

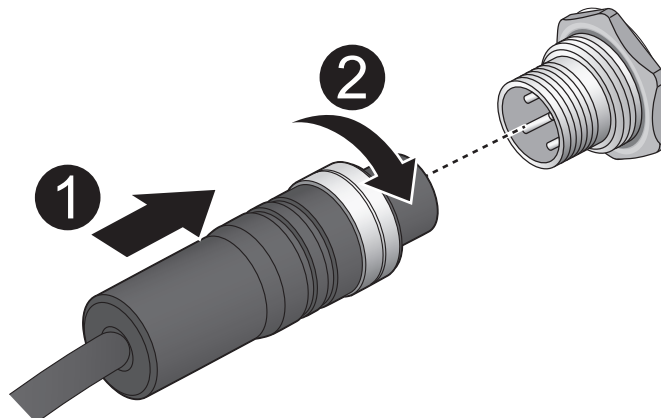


Figure 2.20 Installing the Power Cable

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.

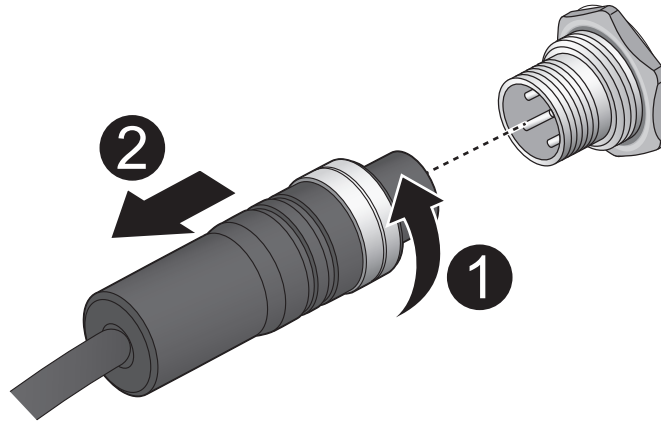


Figure 2.21 Removing the Power Cable

2.2.7.5 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.

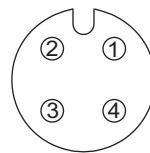


Figure 2.22 Standard M12 4 Poles Male DC Power Input Connector

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

Chapter 3

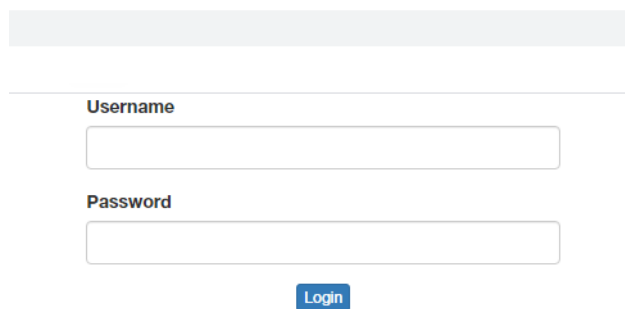
Web Interface

3.1 Log In

To access the login window, connect the device to the network, see “Network Connection” on page 14. 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 light gray header bar. Below it, the word "Username" is followed by a text input field. Below that, the word "Password" is followed by a 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 27.
2. Navigate to **Management > Password Manager**. The HTTP configuration page displays.
3. Enter the username 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.

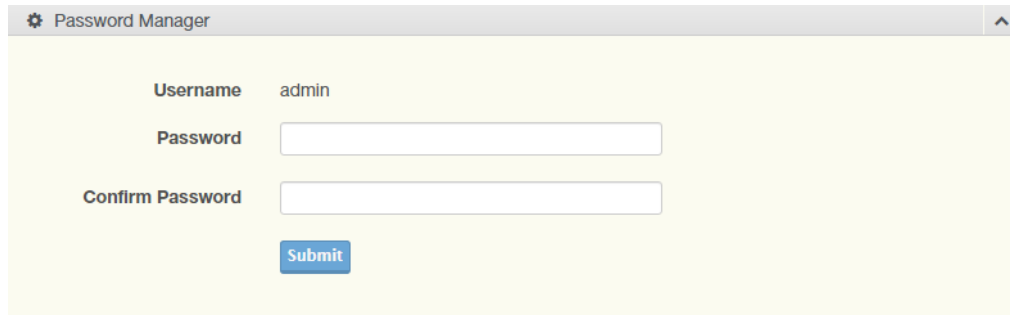
The screenshot shows a web browser window with the title "Password Manager". The page has a light yellow background. At the top, there is a header bar with a gear icon and the text "Password Manager". Below the header, the "Username" field is pre-filled with "admin". The "Password" and "Confirm Password" fields are empty text boxes. A blue "Submit" button is located at the bottom of the form.

Figure 3.2 Management > Password Manager

3.2 Overview

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

System Info	
Information Name	Information Value
Firmware Version	1.1.16
Local Hostname	Advantech
System Time	Thu May 14 02:15:52 1970
System Up Time	0 day 5 hr 7 min 46 sec
Model Name	EKI-9502G





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: 11.67 MB (85324 Pkts.) TX: 15.46 MB (80436 Pkts.) MAC-Address: 00:D0:C9:FF:68:D5
1 (WLAN) Status	 Mode: Access Point SSID: EKI-9502G BSSID: 00:D0:C9:FF:68:D6 Encryption: None Channel: 1 (2.412 GHz) Tx-Power: 30 dBm Country: US
2 (WLAN) Status	 Mode: Access Point SSID: EKI-9502G BSSID: 00:D0:C9:FF:68:D7 Encryption: None Channel: 149 (5.745 GHz) Tx-Power: 30 dBm Country: US

Figure 3.3 Overview

WAN Interface	
Information Name	Information Value
5 (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.			

Working WAN Interface	
Information Name	Information Value
Working WAN Interface	Cellular

System Status	
Information Name	Information Value
Memory Utilization	<div><div></div></div> 13%
CPU Utilization	<div><div></div></div> 10%

Figure 3.4 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"> Local IP Address: Displays the assigned IP address of the LAN interface. Local 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 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.
1 (WLAN) Status	Mode: Displays the WLAN mode type.
2 (WLAN) Status	<ul style="list-style-type: none"> 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	
5 (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**.

LAN Interface Setup

Local Hostname: Advantech

Domain Name: lan

Protocol: Static

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP Server

DHCP Server: ☒ Enabled ☐ Disabled

Start IP Address: 192.168.1.100

Pool Counter: 150

Leasetime: Day: 0 (0 - 365), Hour: 12 (0 - 23), Minute: 0 (0 - 59), Second: 0 (0 - 59)

Static DNS 1:

Static DNS 2:

Submit

Figure 3.5 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.
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.
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.

Item	Description
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.
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

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

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

- Ethernet WAN:** A dropdown menu with 'ETH 2' selected.
- Protocol:** A dropdown menu with 'Static' selected.
- IP Address:** A text input field containing '192.168.1.1'.
- Subnet Mask:** A text input field containing '255.255.0.0'.
- Default Gateway:** A text input field containing '192.168.1.1'.
- DNS Server 1:** A text input field containing '8.8.8.8'.
- DNS Server 2:** An empty text input field.
- Submit:** A blue button at the bottom.

Figure 3.6 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.
Protocol	Click the drop-down menu to assign the type of protocol to the ETHWAN: DHCP Client or Static.
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	Static Protocol Only: Enter a value to specify the primary DNS server for the interface.

Item	Description
DNS Server 2	Static Protocol Only: Enter a value to specify the secondary DNS server for the interface.
Submit	Click Submit to save the values and update the screen.

3.3.3 1 (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 **1 (WLAN) > Basic**.

Figure 3.7 1 (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.

Item	Description
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.
Maximum Clients	Enter the value (1 to 128) designating the maximum number of clients per wireless device.
BSSID	Display the MAC address of the device.
Using LAN Interface IP Settings	Click to select the LAN interface's IP settings for the WLAN network.
WLAN & LAN packet forwarding	Click to select the enable the packet forward function for the WLAN and LAN interface. IP address: Enter the IP address of the device to receive the forwarded packets. Subnet mask: Enter the subnet mask of the designated forwarding entry.
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.
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.

Item	Description
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 **1 (WLAN) > Basic > Operation Mode > Wireless WAN**.

Figure 3.8 1 (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.

Item	Description
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.
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	Static Protocol Only: Enter a value to specify the primary DNS server for the interface.
DNS Server 2	Static Protocol Only: Enter a value to specify the secondary DNS server for the interface.
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.
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

Access Point Settings

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 **1 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 Disable

HT LDPC Enable

Advanced WLAN Setting

RTS Threshold 2347 (1 - 2347)

Transmission Power Full

WMM Enable

Short Guard Interval Enable

Submit

Figure 3.9 1 WLAN > Advanced

The following table describes the items in the previous figure.

Item	Description
Client 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.
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.

Client Settings

The Client Settings are available under the Wireless WAN Operation Mode. The operation mode must be configured for Wireless WAN.

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

Advanced WLAN Settings

Client Settings

Roam: Enable

RSSI threshold: 65

RSSI hysteresis: 3

Scan interval(high): 120

Scan interval(low): 15

Watchdog: Disassociate

Watchdog Action: Restart WLAN

Disassociate Timer:

Advanced WLAN Setting

Transmission Power: Full

Short Guard Interval: Enable

Submit

Figure 3.10 WLAN > Advanced

The following table describes the items in the previous figure.

Item	Description
Client Settings	
Roam	Click to enable or disable (default) the Roam function allowing clients to move faster between SSIDs. When fast Roam is enabled, the client entry is not cleared and the delay is not enforced. With Roam disabled, a delay is enforced before clients are allowed to move between SSID.
RSSI threshold	Enter the value to designate the transmit power setting (range 1 - 75, default 65). A higher value causes the access points to operate at higher transmit power rates. A lower value results in lowered transmit power rates.
RSSI hysteresis (hysteresis)	Enter the value to indicate how much greater the signal strength of an access point must be to roam to it. Range: 3 to 20 dB (default: 3 dB).
Scan interval(high)	The interval time during an active RSSI > RSSI threshold scan, background scan. The default is 120 seconds.
Scan interval(low)	The interval time during a local RSSI <RSSI Threshold scan. The default is 15 seconds

Item	Description
Watchdog	<p>Click to set the Watchdog policy to Disable (default), Disassociate, Ping.</p> <ul style="list-style-type: none"> ■ Disable: Select to disable the Watchdog function (Default). ■ Disassociate: This disassociates the client after a period of time if the client is not re-associated to another AP. ■ Ping: Continuously ping a specific remote host for connection status using a user-defined IP address. <ul style="list-style-type: none"> – Watchdog Action: If the target IP address cannot be pinged the designated action (Restart WLAN, Reboot, Force re-association) will be taken. – Ping Target: Enter the specific remote host for connection. – Ping Waittime: Enter the time delay (in seconds) between two continuous ping packets in a Ping interval. – Ping Loss Counter: Enter the variable to define the number of failed ping count(s) that the device can send continuously. If the value is exceeded, the Action is initiated.
Advanced WLAN Setting	
Transmission Power	Click the drop-down menu to set the transmission power. Settings: Full, Half, Quarter.
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 > 1 (WLAN) > Security > Security Mode**.

Figure 3.11 Interface > 1 (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 > 1 (WLAN) > Security > Security Mode > WEP**.

The screenshot shows the 'WLAN Security/Encryption Settings' window. Under the 'Security Policy' section, the 'Security Mode' is set to 'WEP'. Below this, the 'Wire Equivalence Protection (WEP)' section contains a 'Default Key Index' dropdown set to 'Key 1'. There are four 'WEP Key' fields (Key 1 to Key 4), each with a text input and an 'ASCII' dropdown. Each key field also has an 'Unmask' checkbox. A 'Submit' button is at the bottom.

Figure 3.12 Interface > 1 (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
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	
Apply	Click Apply to save the values and update the screen.

Security Mode WPA-Personal

To access this page, click **Interface > 1 (WLAN) > Security > Security Mode > WPA-Personal**.

The screenshot shows a web interface titled "WLAN Security/Encryption Settings". Under the "Security Policy" section, the "Security Mode" is set to "WPA-Personal". Below this, under the "WPA-Personal" section, the "WPA Version" is set to "WPA1+WPA2", the "WPA Cipher" is set to "TKIP+AES", and there is a text input field for the "Pass Phrase". An "Unmask" checkbox is located below the pass phrase field, and a "Submit" button is at the bottom.

Figure 3.13 Interface > 1 (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 Pre-shared Key	
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 > 1 (WLAN) > Security > Security Mode > WPA/WPA2-Enterprise**.

WLAN Security/Encryption Settings

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 3.14 Interface > 1 (WLAN) > Security > Security Mode > WPA/WPA2-Enterprise

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 > 1 (WLAN) > Statistics**.

Overview

Information Name

Information Value

Mode

Access Point

SSID

EKI-9502G

Channel / Frequency

channel 1 (2412 MHz)

BSSID

00:D0:C9:FF:68:D6

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

156349

TX Bytes

24990773

RX Packets

0

RX Bytes

0

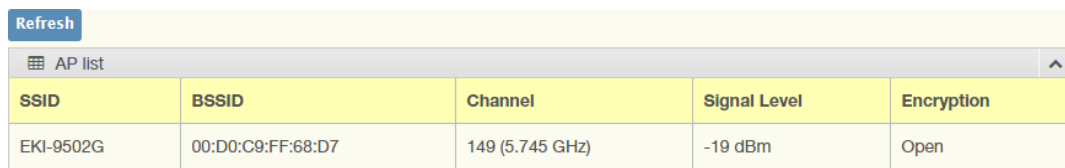
Figure 3.15 Interface > 1 (WLAN) > Statistics

The following table describes the items in the previous figure.

Item	Description
Overview	
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 List	
Station BSSID	Displays the basic service set identifier (BSSID), 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 (Tx) to receive (Rx) 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.
Wlan status	
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 Site Survey

To access this page, click **Interface > 1 (WLAN) > Site Survey**.



SSID	BSSID	Channel	Signal Level	Encryption
EKI-9502G	00:D0:C9:FF:68:D7	149 (5.745 GHz)	-19 dBm	Open

Figure 3.16 Interface > 1 (WLAN) > Site Survey

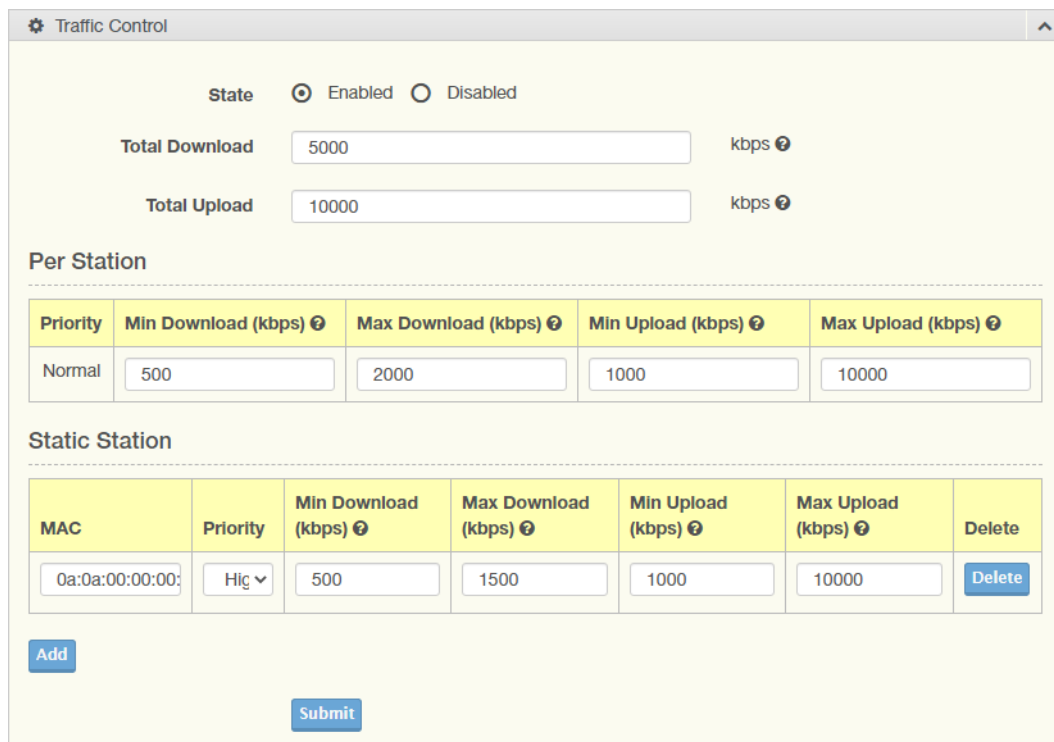
The following table describes the items in the previous figure.

Item	Description
Refresh	Click Refresh to initiate a AP list scan.
SSID	Displays the SSID string of the AP list.
BSSID	Displays the BSSID string of the AP list.
Channel	Displays the channel of the AP list.
Signal Level	Displays the signal level of the AP list.
Encryption	Displays the encryption of the AP list.

3.3.3.6 Traffic 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 > 1 (WLAN) > Traffic Control**.



Priority	Min Download (kbps)	Max Download (kbps)	Min Upload (kbps)	Max Upload (kbps)
Normal	500	2000	1000	10000

MAC	Priority	Min Download (kbps)	Max Download (kbps)	Min Upload (kbps)	Max Upload (kbps)	Delete
0a:0a:00:00:00:00	High	500	1500	1000	10000	Delete

Figure 3.17 Interface > 1 (WLAN) > Traffic Control

The following table describes the items in the previous figure.

Item	Description
Traffic Control	
State	Click the radio button to enable or disable the traffic control.
Total Download	Enter the value to configure the download bandwidth.

Item	Description
Total Upload	Enter the value to configure the upload bandwidth.
Per Station	
Priority	The priority of each station is normal, except for the static station.
Min Download	Enter the value to configure the minimum download bandwidth used to allocate each station, except for the static station.
Max Download	Enter the value to configure the maximum download bandwidth used to allocate each station, except for the static station.
Min Upload	Enter the value to configure the minimum upload bandwidth used to allocate each station, except for the static station.
Max Upload	Enter the value to configure the maximum upload bandwidth used to allocate each station, except for the static station.
Static Station	
MAC	Enter the MAC for the station.
Priority	Click the drop-down menu to select the priority for the station.
Min Download	Enter the value to configure the minimum download bandwidth used to allocate the station.
Max Download	Enter the value to configure the maximum download bandwidth used to allocate the station.
Min Upload	Enter the value to configure the minimum upload bandwidth used to allocate the station.
Max upload	Enter the value to configure the maximum upload bandwidth used to allocate the station.
Delete	Click Delete to remove the station from the available list.
Add	Click Add to include the station in the static station.
Submit	Click Submit to save the values and update the screen.

3.3.3.7 Interface > 1 (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 > 1 (WLAN) > Traffic Control**.

Access Control Method

Access Control Method: Deny

MAC 1

MAC 2

MAC 3

MAC 4

MAC 29

MAC 30

MAC 31

MAC 32

Submit

Figure 3.18 Interface > 1 (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.



3.3.3.8 Log

To access this page, click **Interface > 1 (WLAN) > Log**.

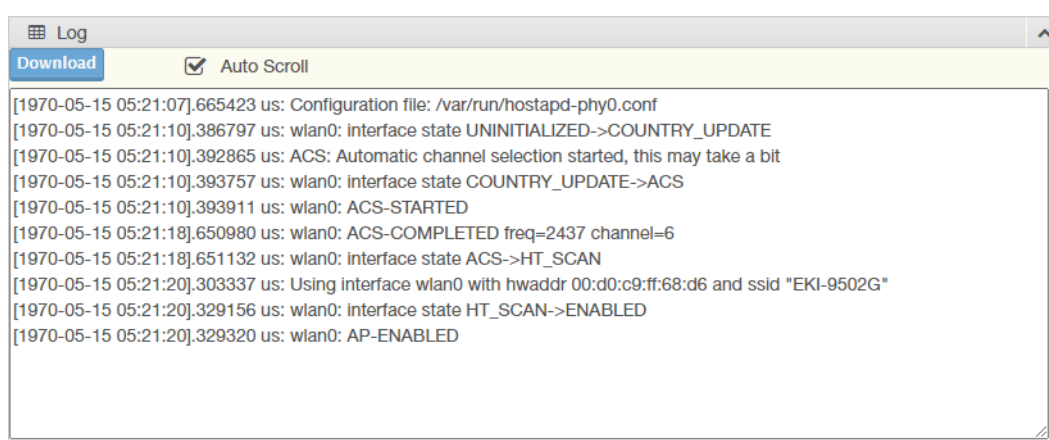


Figure 3.19 Interface > 1 (WLAN) > Log

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 2 (WLAN)

For further information regarding the 2 (WLAN) configuration settings, see "1 (WLAN)" on page 27.

3.3.5 5 (Cellular)

3.3.5.1 Basic

To access this page, click **Interface > 5 (Cellular) > Basic**.

The screenshot shows a 'Basic Settings' window with the following elements:

- Initial State:** A dropdown menu set to 'online'.
- Default SIM:** A dropdown menu set to 'SIM 1'.
- Switch to other SIM card when connection fails:** An unchecked checkbox.
- Ping IP Address:** A text input field containing '8.8.8.8'.
- Ping Interval:** A text input field containing '30', with a range '(3 - 3600)' indicated to the right.
- Submit:** A blue button at the bottom center.

Figure 3.20 Interface > 5 (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.
Switch to other	Click to enable or disable the switch function. The function selects the secondary SIM option in the event of a failed primary card.
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.

3.3.5.2 SIM 1

APN Configuration

To access this page, click **Interface > 5 (Cellular) > SIM 1**

The screenshot shows a configuration window titled 'SIM 1'. It is divided into two main sections: 'APN Configuration' and 'Data Limit Setting'.
APN Configuration:
 - **APN:** A text field containing 'Internet'.
 - **PIN:** A text field, currently empty, with a range '(0000 - 9999)' and a 'Verify' button to its right.
 - **PIN State:** A label with no input field.
 - **PAP/ CHAP Username:** A text field, currently empty.
 - **PAP/ CHAP Password:** A text field, currently empty.
Data Limit Setting:
 - **Data Limit:** Two radio buttons: 'Enabled' (unselected) and 'Disabled' (selected).
 - **My Internet package data limit is:** A text field containing '1024', with a range 'MB (1 - 999999)' to its right.
 - **Remind me when data usage is more then:** A text field containing '80', with a range '% (1 - 100)' to its right.
 - **Usage cycle reset date:** A text field containing '1', with a range 'Date of each month (1 - 31)' to its right.
 - A 'Submit' button is located at the bottom center.

Figure 3.21 Interface > 5 (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.
Data Limit Setting	
Data Limit	Click to enable or disable the data limit function.
My Internet Package Data Limit Is	Enter the variable to define the data limit in MB. Variable: 1 to 999999.
Remind Me When Data Usage Is More Than	Enter the percentage value to define the threshold required to initiate a notification of the used data limit. Variable: 1 to 100%.
Usage Cycle Reset Date	Enter the variable to define the day of the month to initiate the reset cycle. Variable: 1 to 31.
Submit	Click Submit to save the values and update the screen.

SIM Card Utilities

To access this page, click **Interface > 5 (Cellular) > SIM 1**

The screenshot shows a web interface titled "SIM1 Card Utilities". It contains three main sections:

- Unblock SIM Card:** Includes a "SIM PUK" input field (range: 00000000 - 99999999), a "New SIM PIN" input field (range: 0000 - 9999), and a "Submit" button.
- PIN Protection:** Includes a radio button group for "Enable PIN Protection" (On/Off), a "Current PIN" input field (range: 0000 - 9999), and a "Submit" button.
- Change PIN Code:** Includes three input fields: "Current PIN" (range: 0000 - 9999), "New PIN" (range: 0000 - 9999), and "Confirm New PIN" (range: 0000 - 9999), followed by a "Submit" button.

Figure 3.22 Interface > 5 (Cellular) > SIM 1

The following table describes the items in the previous figure.

Item	Description
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.
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.

3.3.5.3 SIM 2

For further information regarding configuration of SIM 2 see "SIM 1" on page 41.

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**.

Target IP Address	Netmask	Gateway	Interface	Metric	MTU	Delete
192.168.1.10	255.255.0.0	192.168.1.1	LAN	3	1500	Delete
			LAN			Delete

Add Submit

Figure 3.23 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**.

Enabled	Name	Start Port	End Port	Local IP	Local Port	Protocol	Delete
<input checked="" type="checkbox"/>	http_server	80	82	192.168.1.10	80	TCP	Delet
<input checked="" type="checkbox"/>	ftp_server	21	21	192.168.1.20	21	Both	Delet
<input checked="" type="checkbox"/>	ssh	22	22	192.168.1.30	22	Both	Delet
<input type="checkbox"/>						TCP	Delet

Add Apply

Figure 3.24 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**.

DMZ ☐ Enabled ☒ Disabled (Only for wireless wan mode)

IP

Apply

Figure 3.25 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 Scurity

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**.

Enabled	Direction	Source IP	Destination IP	Protocol	Source Port	Destination Port	Delete
<input checked="" type="checkbox"/>	LAN -> WAN	192.168.1.56	192.168.1.210	TCP	5000	8080	Delete
<input type="checkbox"/>	LAN -> WAN			TCP			Delete

Add Apply

Figure 3.26 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 taffic 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.

3.4.3.2 VPN Passthrough

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 > Security > VPN Passthrough**.

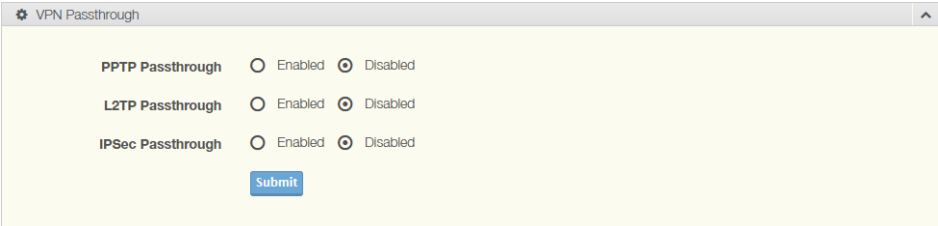


Figure 3.27 Networking > Security > VPN Passthrough

Item	Description
PPTP Passthrough	Click the radio button to enable or disable PPTP packets to pass through.
L2TP Passthrough	Click the radio button to enable or disable L2TP packets to pass through.
IPSec Passthrough	Click the radio button to enable or disable IPSEC packets to pass through.
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**.

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 47

3.4.4.3 Tunnel 3

For further information regarding the configuration of the OpenVPN Tunnel function see “Tunnel 1” on page 47

3.4.4.4 Tunnel 4

For further information regarding the configuration of the OpenVPN Tunnel function see “Tunnel 1” on page 47

3.4.5 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.

3.4.5.1 Tunnel 1

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

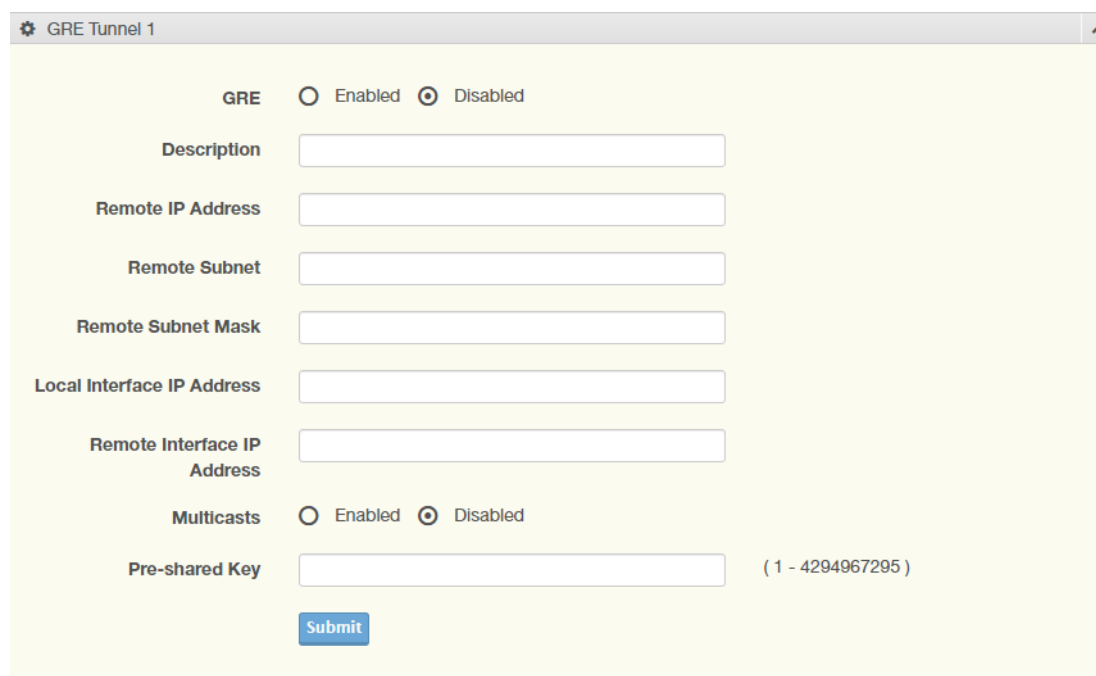


Figure 3.29 Networking > GRE> Tunnel 1

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.

Item	Description
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.

3.4.5.2 Tunnel 2

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

3.4.5.3 Tunnel 3

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

3.4.5.4 Tunnel 4

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

3.4.6 QoS Settings

3.4.6.1 QoS Settings

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

Figure 3.30 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.

3.4.6.2 QoS IP Base Rules

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

QoS Protocol Base Rules

Protocol	Source Port	Destination Port	Priority	Delete
UDP	80	5000	Medium	Delete
TCP			High	Delete

Add

Submit

Figure 3.31 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.

3.4.6.3 QoS Protocol Base Rules

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

QoS Protocol Base Rules

Protocol	Source Port	Destination Port	Priority	Delete
UDP	80	5000	Medium	Delete
TCP			High	Delete

Add

Submit

Figure 3.32 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.

3.4.7 WAN Load Balancing

To access this page, click **Networking > WAN Load Balancing**.

Cellular Interface

Enabled	Interface	Weight	Tracking IP	Interface Up	Interface Down	Tracking Interval
<input checked="" type="checkbox"/>	5 (Cellular)	3	8.8.8.8	3	3	5

WLAN Interface

Enabled	Interface	Weight	Tracking IP	Interface Up	Interface Down	Tracking Interval
<input checked="" type="checkbox"/>	1 (WLAN)	3	8.8.8.8	3	3	5
<input type="checkbox"/>	2 (WLAN)	3	8.8.8.8	3	3	5

WAN Load Balancing Settings

☒ Use the same WAN interface to route the traffic with the same source IP address with the prior traffic within the sticky timeout.

Sticky Timeout: 600 (1 - 1000000)

Submit

Figure 3.33 Networking > WAN Load Balancing

The following table describes the items in the previous figure.

Item	Description
Cellular Interface	
Enabled	Click the radio button to enable or disable the interface.
Interface	Displays the Interface bound to the interface entry.
Weight	Enter a value to setup a load balancing strategy based on weight. If based on weight, the device takes the ratio to take the line speed settings of the cellular interfaces as default ratio for data transfer. The ratio determines the number of sessions to transfer via each cellular interface for the following period.
Tracking IP	Enter the IP address used to generate traffic to be used to check delay/latency.
Interface Up	Number of successful tests to considered link as alive.
Interface Down	Number of failed tests to considered link as dead.
Tracking Interval	Number of seconds between each test.
WLAN Interface	
Enabled	Click the radio button to enable or disable the interface. The option is available if Operation Mode in WLAN is set to Wireless WAN. See "Basic" on page 27.
Interface	Displays the name of the interface.
Weight	Enter a value to setup a load balancing strategy based on weight. If based on weight, the device takes the ratio to take the line speed settings of the WAN interfaces as default ratio for data transfer. The ratio determines the number of sessions to transfer via each WAN interface for the following period.
Tracking IP	Enter the IP address used to generate traffic to be used to check delay/latency.

Item	Description
Interface Up	Number of successful tests to considered link as alive.
Interface Down	Number of failed tests to considered link as dead.
Tracking Interval	Number of seconds between each test.
WLAN Load Balancing Settings	
Use the same WAN ...	Click the radio button to enable the session persistence function. When activated, an affinity is created between a source IP from the same WAN interface to a specific IP address for the duration specified in the Sticky Timeout field.
Sticky Timeout	Enter a variable to define the affinity period between the same source WAN interface client and a same source IP address.
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**.

The following image was modified to facilitate easier instruction. The section is divided into two sections, however, the actual UI screen is a single interface.

Figure 3.34 Networking > WAN Handover

The following table describes the items in the previous figure.

Item	Description
WAN Handover	
WAN Handover	Click to enable or disable the WAN handover function.
WAN Interface	Click the drop-down menu to select the interface to bind to the WAN handover function.
Signal Strength Detection	
Detection Interval	Enter the value in seconds to define the interval to activate the signal strength detection function.

Item	Description
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.
Handover Condition	Select the radio button to specify the handover condition: <ul style="list-style-type: none"> Any WLAN adapter signal is worse than RSSI threshold All WLAN adapter signal are worse than RSSI threshold
Submit	Click Submit to save the values and update the screen.

3.4.8.2 Cellular Handover

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

4G RSSI Threshold: dBm (-65 ~ -95)

Handover Condition: ☐ Any Cellular adapter signal is worse than RSSI threshold
☒ All Cellular adapter signal are worse than RSSI threshold

3G

Excellent	Good	Fair	Poor	No Signal
-70dBm	-85dBm	-100dBm	-110dBm	

4G

Excellent	Good	Fair	Poor	No Signal
-65dBm	-75dBm	-85dBm	-95dBm	

Figure 3.35 Networking > WAN Handover

The following table describes the items in the previous figure.

Item	Description
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 RSSI 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.
Handover Condition	Select the radio button to specify the handover condition: <ul style="list-style-type: none"> Any Cellular adapter signal is worse than RSSI threshold All Cellular adapter signal are worse than RSSI threshold
Submit	Click Submit to save the values and update the screen.

3.5 Management

3.5.1 Password Manager

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



Figure 3.36 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.

3.5.2 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**.

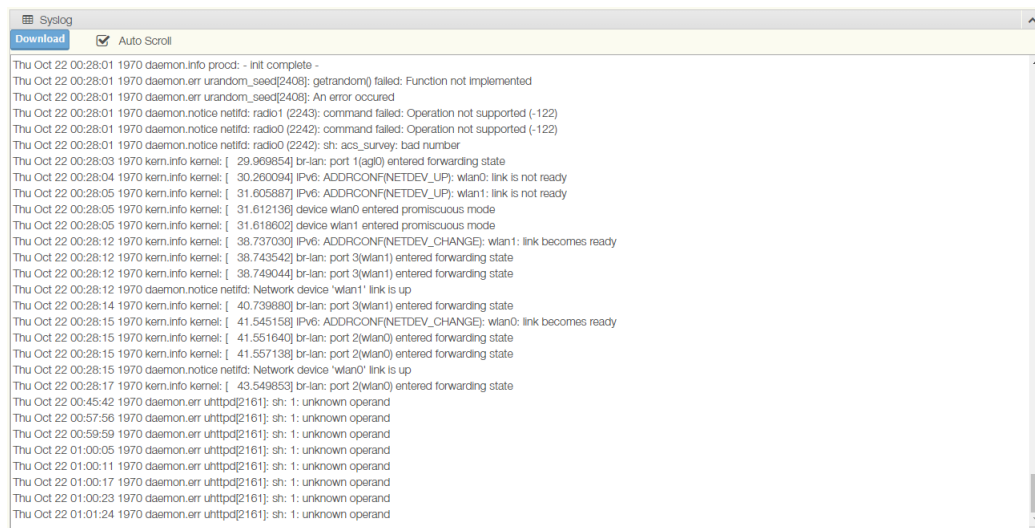


Figure 3.37 Management > Syslog

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.

3.5.3 Alert

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



Figure 3.38 Management > Alert

The following table describes the items in the previous figure.

Item	Description
Send SMS When Datalimit Exceeded	Enter the phone number to receive the SMS message.
Submit	Click Submit to save the values and update the screen.

3.5.4 NTP / Time

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

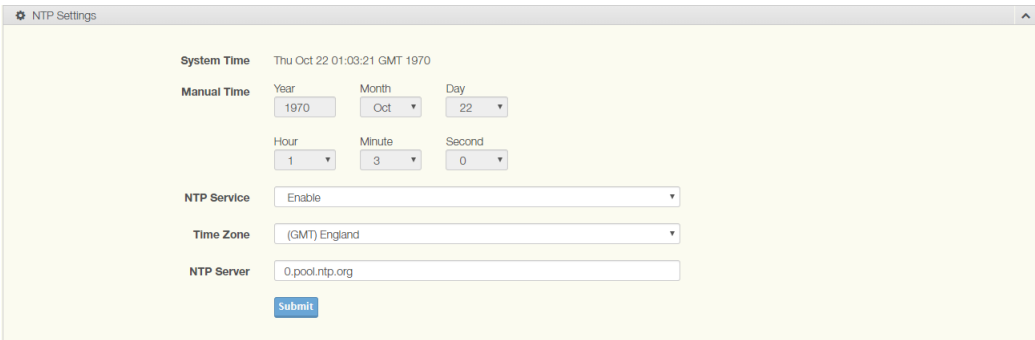


Figure 3.39 Management > NTP / Time

The following table describes the items in the previous figure.

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

3.5.5 Captive Portal

3.5.5.1 Basic

To access this page, click **Management > Captive Portal > Basic**.

Basic

Captive Portal ☐ Enabled ☒ Disabled

Interface 2 (WLAN)

Redirect URL http://www.advantech.com

Session Timeout 1200 Minutes (0 - 1440)

Gateway Name Advantech EKI-9502G

Submit

Figure 3.40 Management > Captive Portal > Basic

The following table describes the items in the previous figure.

Item	Description
Captive Portal	Click to enable or disable the captive portal function.
Interface	Select the interface to bind to the function. Settings: 1 (WLAN) or 2 (WLAN).
Redirect URL	After authentication, a user is redirected to their initial requested page unless Redirect URL is set. The user is redirected to the defined URL instead.
Session Timeout	In minutes, enter the value to designate the end of the interval after which clients are forced out. Values: 0 - 1440.
Gateway Name	Enter the string to designate as the name of the enabled gateway.
Submit	Click Submit to save the values and update the screen.

3.5.5.2 Custom Page

To access this page, click **Management > Captive Portal > Custom Page**.

Field Label	Input Type	Maxlength	Delete
Username	Text	32	Delete
E-Mail	E-Mail	32	Delete

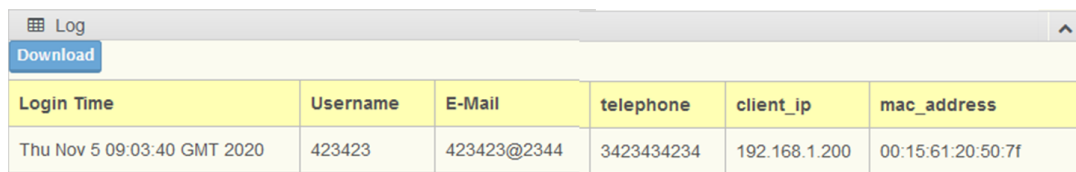
Figure 3.41 Management > Captive Portal > Custom Pages

The following table describes the items in the previous figure.

Item	Description
Title	Enter a string for use as the title of the customized captive portal page.
Welcome	Enter a string to define the welcome message of the captive portal page after user authentication.
User-defined Regulation Title	Enter a string for use as the Regulation title section.
User-defined Regulation	Enter a string for use as the regulation policy criteria.
Field Label	Enter the string to define the label entry.
Input Type	Click the drop-down menu to select the input type. Variables: Text, E-Mail, Number.
Maxlength	Enter the variable defining the maximum length of the field label.
Delete	Click Delete to remove the label entry.
Add	Click Add to add a label entry.
Submit	Click Submit to save the values and update the screen.
Logo	Click Choose File to select a file to upload.
Upload	Click Upload to select and upload a file onto the device for use as a logo. Max. size 1 MB. Accepted formats: .jpg, .png, .bmp

3.5.5.3 Log

To access this page, click **Management > Captive Portal > Log**.



Log					
Download					
Login Time	Username	E-Mail	telephone	client_ip	mac_address
Thu Nov 5 09:03:40 GMT 2020	423423	423423@2344	3423434234	192.168.1.200	00:15:61:20:50:7f

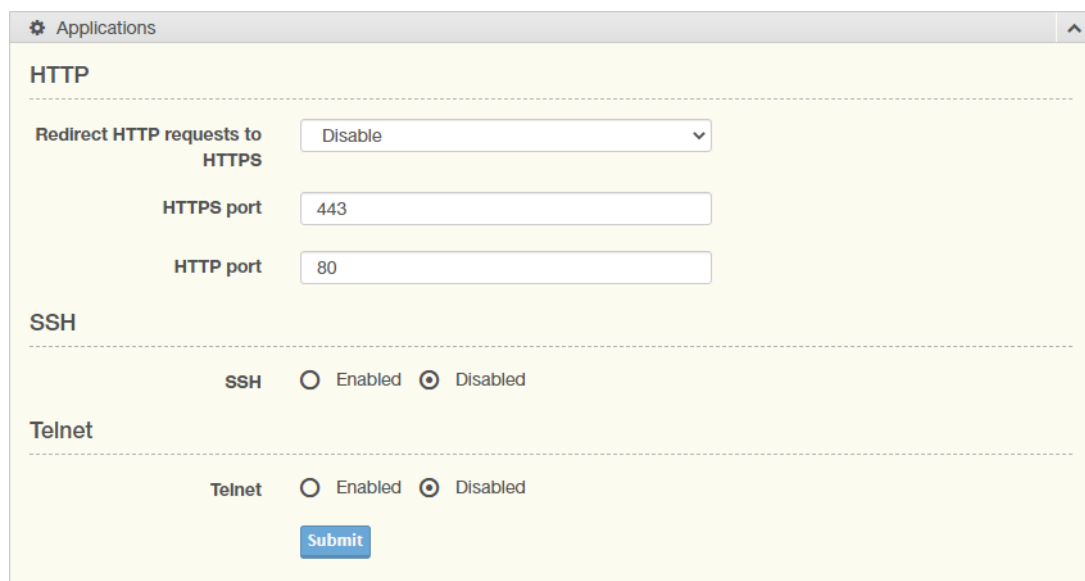
Figure 3.42 Management > Captive Portal > Log

The following table describes the items in the previous figure.

Item	Description
Download	Click Download to download the log report.
Log Time	Displays the time of the log entry.
Username	Displays the listed user name of the log entry.
E-Mail	Displays the listed Email of the log entry.
Telephone	Displays the listed telephone number of the log entry.
Client_Ip	Displays the listed client IP address of the log entry.
MAC_Address	Displays the listed MAC address of the log entry.

3.5.6 Applications

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



Applications

HTTP

Redirect HTTP requests to HTTPS:

HTTPS port:

HTTP port:

SSH

SSH: ☐ Enabled ☒ Disabled

Telnet

Telnet: ☐ Enabled ☒ Disabled

[Submit](#)

Figure 3.43 Management > Applications

The following table describes the items in the previous figure.

Item	Description
HTTP	
Redirect HTTP Requests to HTTPS	Click to enable 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.
SSH	
SSH	Click to enable or disable the SSH function.

Item	Description
Telnet	
Telnet	Click to enable or disable the Telnet function.
Submit	Click Submit to save the values and update the screen.

3.5.7 Configuration Manager

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

Figure 3.44 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.
USB Drive Backup	
Automatically Backup	Select Enabled or Disabled to enable the function.
Submit	Click Submit to save the values and update the screen.

3.5.8 Firmware Upgrade

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



Figure 3.45 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.

3.5.9 Reset System

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



Figure 3.46 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.

3.5.10 Reboot Device

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



Figure 3.47 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.

3.5.11 Apply Configuration

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

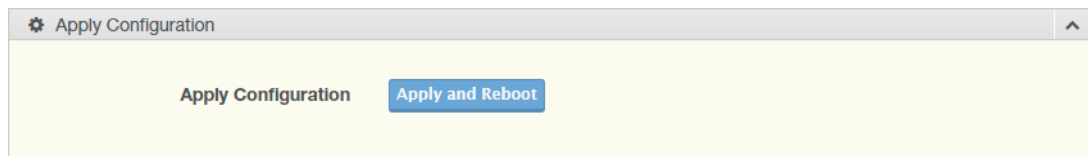


Figure 3.48 Management > Apply Configuration

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.

3.6 Tools

3.6.1 Diagnostics

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

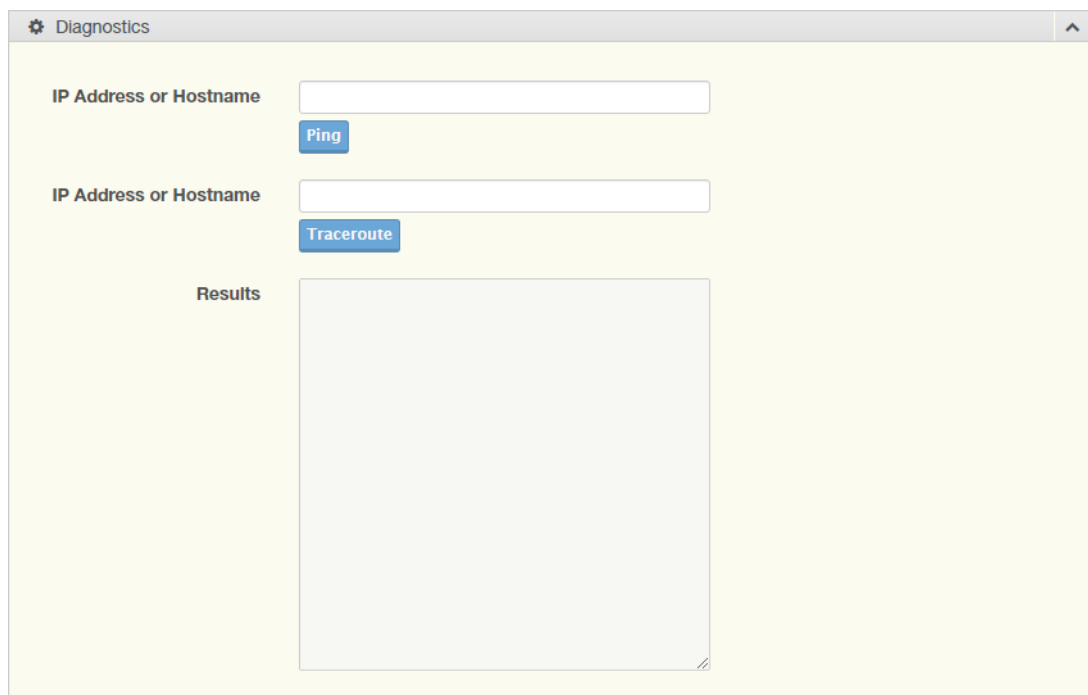


Figure 3.49 Tools > Diagnostics

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.

3.6.2 GPS

3.6.2.1 Basic

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

GPS Settings

GPS ☒ Enabled ☐ Disabled

Submit

GPS Data

Information Name	Information Value
Time	
Latitude	
Longitude	
Speed	

Satellite List

PRN	Elevation	Azimuth	SNR	Used
-----	-----------	---------	-----	------

Skyview

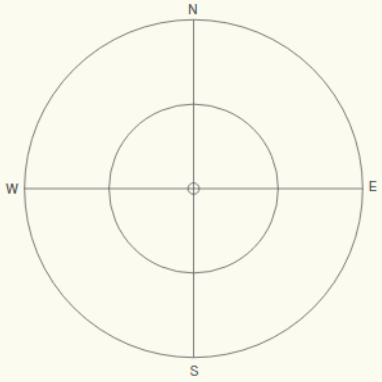


Figure 3.50 Tools > GPS > Basic

The following table describes the items in the previous figure.

Item	Description
GPS Settings	
GPS	Click to enable or disable the GPS function.
Submit	Click Submit to save the values and update the screen.
GPS Data	
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.
Satellite List	
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.

Item	Description
Used	Displays the usage status of the listing.
Skyview	Displays the aerial visibility diagram of the Satellite List.

3.6.2.2 GPS Report

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

Figure 3.51 Tools > GPS > GPS Report

The following table describes the items in the previous figure.

Item	Description
Remote Log	Click to enable or disable the Remote Log function.
Data Format	Click to select the format type for the log reporting: NMEA, JSON, or Both.
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.
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. 2021