User Manual



EKI-6333BE-4GD Series

IEEE 802.11 a/b/g/n/ac/ax/be WiFi AP

ADVANTECH

Enabling an Intelligent Planet

Copyright

The documentation and the software included with this product are copyrighted 2026 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 (2 years)

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

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

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

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

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

Edition 1

Printed in Taiwan September 2026

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 22 centimeters (7.87 inches) between the radiator and your body.

VCCI

この装置は、クラス A 機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

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 EKI-6333BE-4GD Wi-Fi AP
- 6 x Antennas
- 1 x Din-rail bracket and wall mount kit

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.

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 Rear View 6
2.1.3 Bottom View 7
2.1.4 Left View 7
2.1.5 LED Indicators 8
2.2 Connecting Hardware 9
2.2.1 DIN Rail Mounting 9
2.2.2 Wall-Mounting 11
2.2.3 Wireless Connection 13
2.2.4 Network Connection 14
2.2.5 Power Connection 15
2.3 Reset Button 19

Chapter 3 Web Interface 20

3.1 Log In 21
3.1.1 Password 22
3.2 Overview 22
3.3 Address Resolution Protocol 24
3.4 Interface Settings 25
3.4.1 LAN 25
3.4.2 WAN 26
3.4.3 Wireless 2.4GHz 28
3.4.4 Wireless 5GHz 42
3.4.5 Wireless 6GHz 43
3.4.6 Wireless MLO 45
3.4.7 EasyMesh 48
3.5 Network Settings 51
3.5.1 Static Route 51
3.5.2 NAT 52
3.5.3 Forwarding 52
3.5.4 Security 54
3.5.5 IP-QoS 55
3.6 Management 56
3.6.1 Account Manager 56
3.6.2 Syslog 57
3.6.3 NTP / Time 58
3.6.4 SNMP 58
3.6.5 Remote Services 61
3.6.6 Configuration Manager 61
3.6.7 Firmware Upgrade 62
3.6.8 Reset System 62
3.6.9 Apply Configuration 62
3.6.10 Reboot Device 63

3.7 Tools 63
3.7.1 Diagnostics 63

List of Figures

Figure 1.1 Dimensions 4
Figure 2.1 Front View 6
Figure 2.2 Rear View 6
Figure 2.3 Bottom View as Seen Without a Port Cover 7
Figure 2.4 Left View 7
Figure 2.5 System LED Panel 8
Figure 2.6 Installing the DIN-Rail Mounting Kit 9
Figure 2.7 Correctly Installed DIN Rail Kit 10
Figure 2.8 Removing the DIN-Rail 10
Figure 2.9 Installing Wall Mount Plates 11
Figure 2.10 Wall Mounting Screw Dimensions 12
Figure 2.11 Wall Mount Installation 12
Figure 2.12 Installing the Antenna 13
Figure 2.13 Positioning the Antenna 13
Figure 2.14 Ethernet Plug & Connector Pin Position 14
Figure 2.15 Power Wiring for EKI-6333BE-4GD Series 15
Figure 2.16 Grounding Connection 17
Figure 2.17 Terminal Receptor: Power Input Contacts 17
Figure 2.18 Removing a Terminal Block 18
Figure 2.19 Installing DC Wires in a Terminal Block 18
Figure 2.20 Securing a Terminal Block to a Receptor 18
Figure 3.1 Login Screen 21
Figure 3.2 Change Password (First Login) 21
Figure 3.3 Management > Account Manager 22
Figure 3.4 Status > Overview, System Info and LAN Interface 23
Figure 3.5 Status > Overview, WAN Interface, DHCP Leases, and System Status 23
Figure 3.6 Status > ARP 24
Figure 3.7 Interface > LAN 25
Figure 3.8 Interface > WAN > Network Mode (Disable) 26
Figure 3.9 Interface > WAN > Network Mode > Static 27
Figure 3.10 Interface > WAN > Network Mode > DHCP 27
Figure 3.11 Interface > WAN > Network Mode > PPPoE 28
Figure 3.12 Wireless WAN Topology 28
Figure 3.13 Wireless - 2.4GHz > Basic > Access Point 29
Figure 3.14 Wireless - 2.4GHz > Basic > Client 30
Figure 3.15 Wireless - 2.4GHz > Advanced 31
Figure 3.16 Wireless - 2.4GHz > Advanced (Client Mode) 32
Figure 3.17 Wireless - 2.4GHz > Security 33
Figure 3.18 Wireless Settings > Security 34
Figure 3.19 Security Mode > WPA-Personal 34
Figure 3.20 Security Mode > WPA-Enterprise 36
Figure 3.21 Wireless - 2.4GHz > Multiple SSID 37
Figure 3.22 Wireless - 2.4GHz > Statistics 39
Figure 3.23 Wireless - 2.4GHz > Access Control 40
Figure 3.24 Wireless - 2.4GHz > Traffic Control 41
Figure 3.25 Wireless - 2.4GHz > Site Survey 42
Figure 3.26 Wireless - 6GHz > Basic > Access Point 44
Figure 3.27 Wireless - 6GHz > Security (WPA3 forced) 44
Figure 3.28 Wireless - MLO > Basic 46
Figure 3.29 Wireless - MLO > Advanced 46
Figure 3.30 Wireless - MLO > Security 46
Figure 3.31 Wireless - MLO > Bandwidth Control 47
Figure 3.32 Wireless - MLO > Statistics 47
Figure 3.33 Wireless - MLO > Access Control 47
Figure 3.34 EasyMesh Network Topology 48
Figure 3.35 EasyMesh > Settings 49

Figure 3.36 EasyMesh > Topology 50
Figure 3.37 Networking > Static Route 51
Figure 3.38 NAT Diagram 52
Figure 3.39 Port Forwarding 52
Figure 3.40 Networking > Forwarding > Port Forwarding 53
Figure 3.41 Networking > Forwarding > DMZ 53
Figure 3.42 Networking > Security > Filter 54
Figure 3.43 Networking > Security > VPN Passthrough 54
Figure 3.44 Networking > IP-QoS > Basic 55
Figure 3.45 Networking > IP-QoS > Limit Rate (empty) 55
Figure 3.46 Networking > IP-QoS > Limit Rate (one entry) 56
Figure 3.47 Management > Account Manager 56
Figure 3.48 Management > Syslog 57
Figure 3.49 Management > NTP / Time 58
Figure 3.50 Management > SNMP 59
Figure 3.51 Management > Remote Services 61
Figure 3.52 Management > Configuration Manager 61
Figure 3.53 Management > Firmware Upgrade 62
Figure 3.54 Management > Reset System 62
Figure 3.55 Management > Apply Configuration 62
Figure 3.56 Management > Reboot Device 63
Figure 3.57 Tools > Diagnostics 63

Chapter 1

Introduction

1.1 Overview

The EKI-6333BE-4GD is an industrial-grade wireless access point featuring Wi-Fi 7 with 2x2x2 MU-MIMO for high-speed and reliable connectivity. It supports Multi-Link Operation (MLO), enabling data transmission across multiple frequency bands simultaneously, improving throughput and reducing latency, which is crucial for realtime applications.

With its DIN-rail mount and wide temperature range (-40°C to 75°C), the EKI-6333BE-4GD is designed for harsh industrial environments. The redundant dual power inputs provide continuous operation, ensuring reliable performance even during power failures.

The EKI-6333BE-4GD also supports protocols like STP, WMM, making it ideal for high-traffic environments. WPA3 encryption ensures advanced security, protecting sensitive data from breaches.

With its MLO capabilities, robust design, and high performance, the EKI-6333BE-4GD is the perfect choice for demanding industrial applications such as automation, monitoring,

and surveillance.

1.2 Device Features

- Supports 802.11be MU-MIMO 2x2x2 (Backward compatible with 802.11a/b/g/n/ac/ax)
- Enjoy smooth streaming and romaing with speeds of 5.8 Gbps on 6 GHz, 2.9Gbps on 5 GHz, and 700 Mbps on 2.4 GHz
- Supports secure access with 802.1x, WPA2/WPA3-Personal, WPA2-Enterprise
- ultra-fast 2.5GBASE-T RJ45 Ethernet ports, IEEE 802.3bz compliant
- -40 to 75 °C Wide temperature design

1.3 Specifications

Specifications	Description	
Interface	I/O Port	4 x RJ45
Physical	Enclosure	Metal shell with solid mounting kits
	Mounting	DIN-rail, Wall
	Dimensions (W x H x D)	140 x 107.3 x 42 mm(5.51" x 4.22" x 1.65")
	Weight	1.2kg
	IP Rating	IP30
LED Display	System LED	Status: Power 2.4G: Link/Active 5G: Link/Active 6G: Link/Active
	Reboot Trigger	Built-in WDT(watchdog timer)
Environment	Operating Temperature	-40 ~ 75 °C (-40~167°F)
	Storage Temperature	-40 ~ 85°C (-40 ~ 185°F)
	Ambient Relative Humidity	10 ~ 95% RH

Specifications	Description	
Wireless LAN Communications	Compatibility	■ 802.11b 11M, 5.5M, 2M, 1Mbps ■ 802.11a/g 54M, 48M, 36M,18M, 12M, 9M, 6Mbps ■ 802.11n HT20 MCS0~15 / HT40 MCS0~15 ■ 802.11ac VHT80 MCS0~9 ■ 802.11ax 2.4 GHz: 9 to 1,148 (MCS0 to MCS11, NSS = 1 to 4) 5 GHz: 18 to 2,400 (MCS0 to MSC11, NSS = 1 to 4) 6 GHZ: 18 to 4,800 (MCS0 to MSC13, NSS = 1 to 4) ■ 802.11be 2.4 GHz: Max 700 (MCS0 to MCS11, NSS = 1 to 4) 5 GHz: Max 2,900 (MCS0 to MSC11, NSS = 1 to 4) 6 GHZ: Max 5,800 (MCS0 to MSC13, NSS = 1 to 4)
	Speed	2.4GHz:700Mbps 5GHz: 2900Mbps 6GHz: 5800Mbps
	Network Mode	Infrastructure
	Free Space Range	Open space 100m
	Antenna	6 x reverse SMA connectors Default external 6 Omni antenna
	Wireless Security	WPA2/WPA3-Personal, WPA2-Enterprise
Ethernet Communications	Compatibility	IEEE 802.3
	Speed	10/100/1000/2500 Mbps
	Port Connector	4 x 8-pin RJ45
	Protection	Built-in 1.5 KV magnetic isolation
Power	Consumption	18W
	Input	12 ~ 48 V_{DC}
	Connector	Terminal block
Software	Management	Telnet, FTP, SNMP, WebUI, SSH
	Wireless	Radio on/off, WMM, Output Power Control, Beacon Interval, RTS/ CTS threshold, DTIM Interval
	Operation Modes	AP, Client
	Configuration	Web Browser
	Protocol	ARP, ICMP, IPv4, TCP, UDP, DHCP Client, DHCP Server, DNS, SNMP, HTTP, HTTPS, DMZ, PPPoE, VPN Passthrough, Telnet Server, SSH Server, QoS
Regulatory Approvals	EMC	CE, FCC Part 15 Subpart B (Class B)

1.4 Dimensions

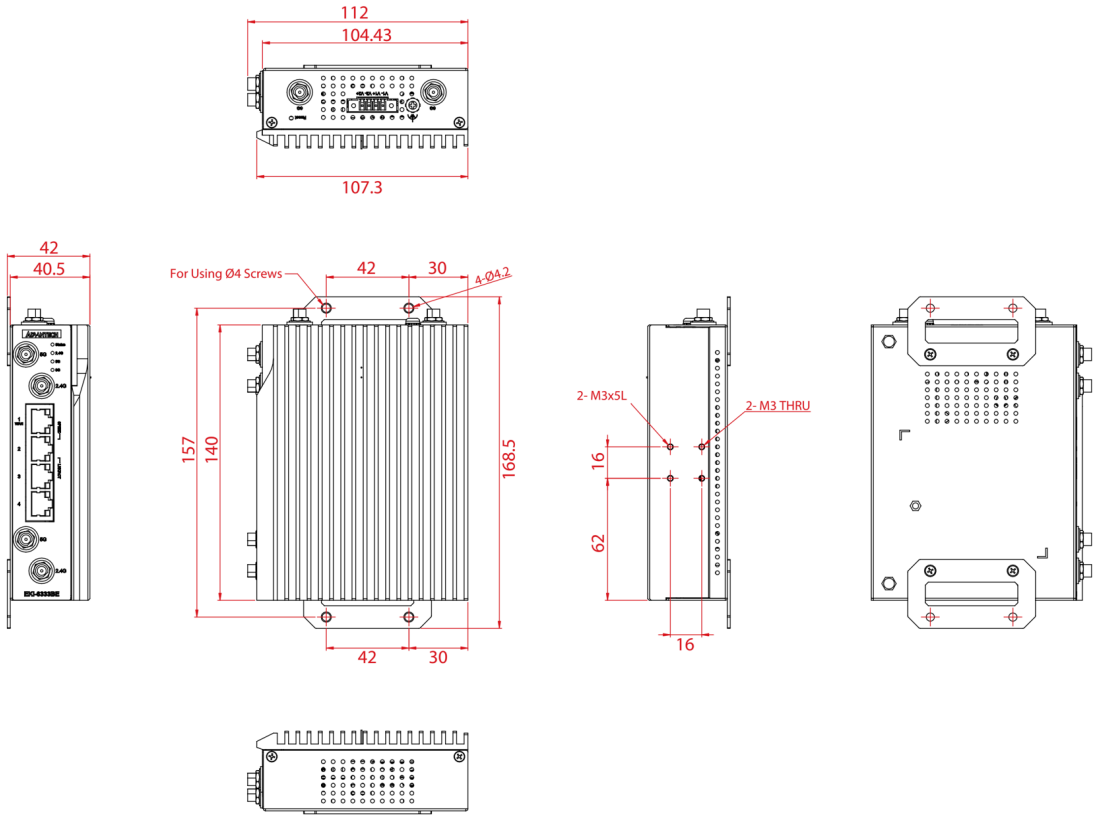


Figure 1.1 Dimensions

Chapter 2

Getting Started

2.1 Hardware

2.1.1 Front View

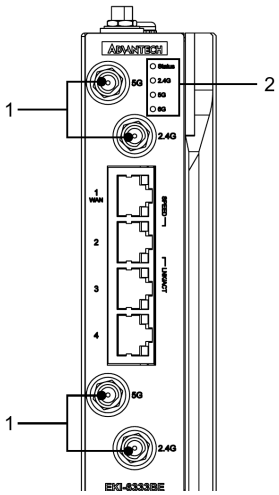


Figure 2.1 Front View

No.	Item	Description
1.	Antenna connector	Reverse SMA connector for 2.4/5 GHz WLAN antenna
2.	System LED panel	See 'LED Indicators' on page 8 for further details.

2.1.2 Rear View

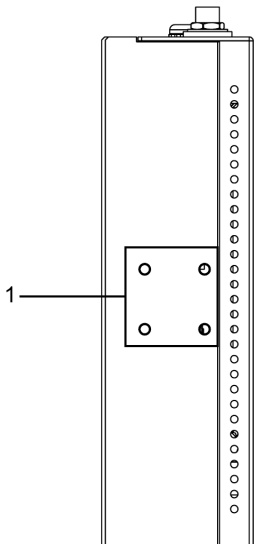


Figure 2.2 Rear View

No.	Item	Description
1.	DIN-Rail mounting holes	Screw holes (3) used in the in installation of a standard DIN rail.

2.1.3 Bottom View

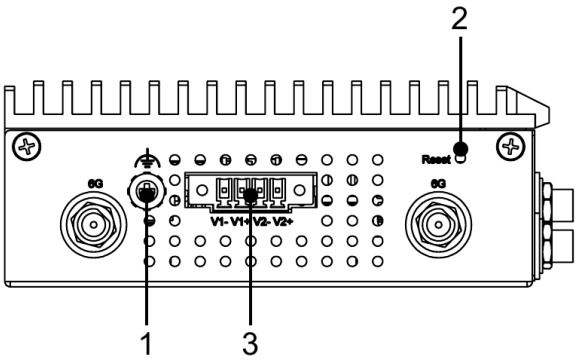


Figure 2.3 Bottom View as Seen Without a Port Cover

No.	Item	Description
1.	GND	Grounding connector
2.	Reset button	Button allows for system soft reset or factory default reset
3.	Terminal block	Connect cabling for power

2.1.4 Left View

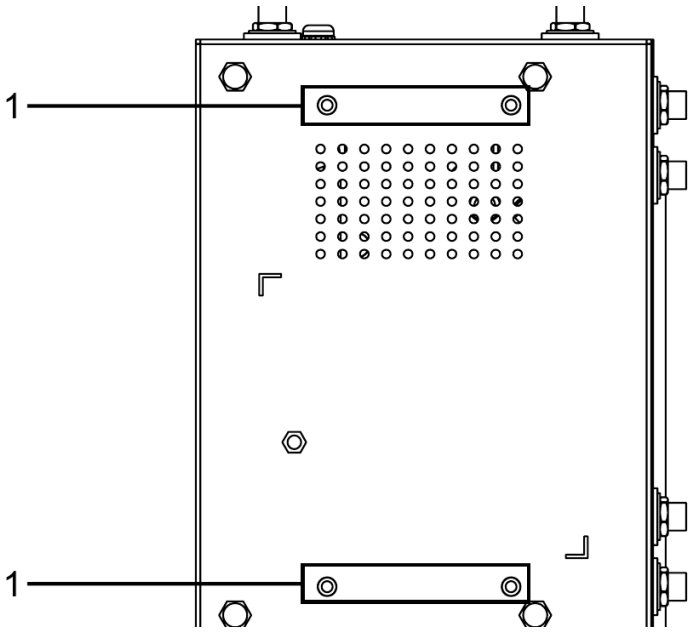


Figure 2.4 Left View

No.	Item	Description
1.	Wall mounting holes	Screw holes (4) used in the installation of a wall mounting kit

2.1.5 LED Indicators

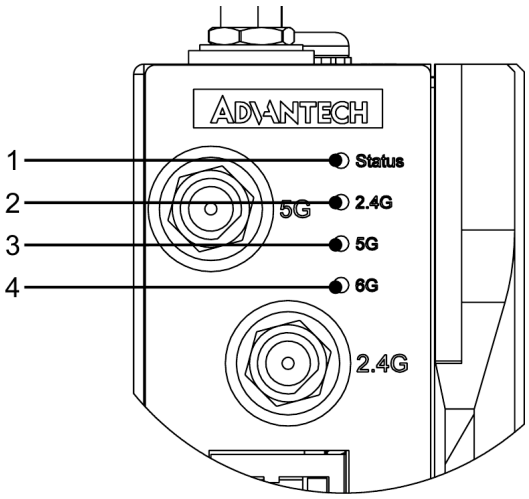


Figure 2.5 System LED Panel

No.	LED Name	LED Color	Description
1.	Status	Green on	Software function is active
		Green blinking	Boot state
2.	WLAN (2.4 GHz)	Green on	AP Mode: Wireless function is active Client Mode: Connection to AP
		Green blinking	Wireless port is transmitting or receiving data
3.	WLAN (5 GHz)	Green on	AP Mode: Wireless function is active Client Mode: Connection to AP
		Green blinking	Wireless port is transmitting or receiving data
4.	WLAN (6 GHz)	Green on	AP Mode: Wireless function is active Client Mode: Connection to AP
		Green blinking	Wireless port is transmitting or receiving data

2.2 Connecting Hardware

2.2.1 DIN Rail Mounting

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

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

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

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

2.2.1.1 Installing the DIN-Rail Mounting Kit

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

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

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

2. Once the DIN rail is seated correctly in the DIN rail clip, press the front of the gateway to rotate the gateway down and into the release tab on the DIN rail clip. If seated correctly, the bottom of the DIN rail should be fully inserted in the release tab.

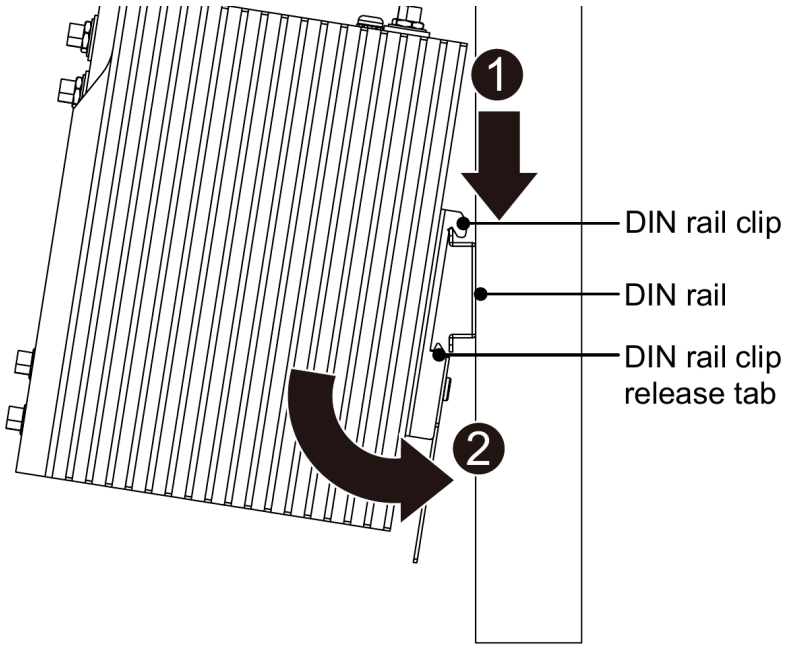


Figure 2.6 Installing the DIN-Rail Mounting Kit

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

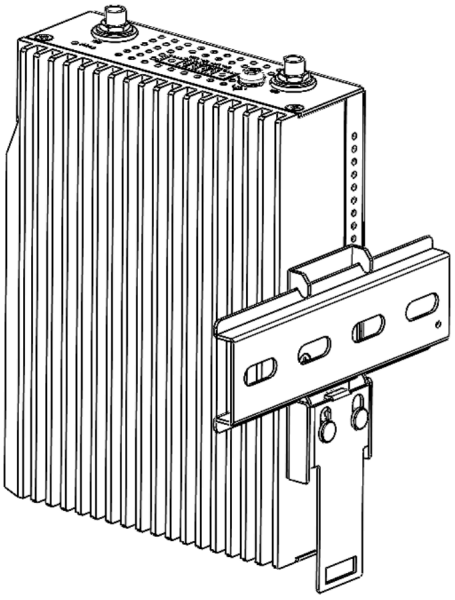


Figure 2.7 Correctly Installed DIN Rail Kit

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

2.2.1.2 Removing the DIN-Rail Mounting Kit

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

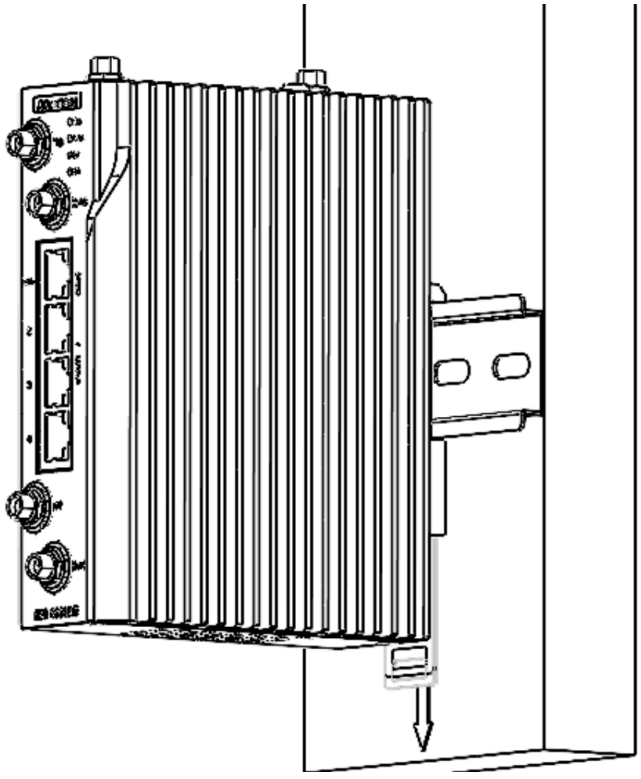


Figure 2.8 Removing the DIN-Rail

2.2.2 Wall-Mounting

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

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

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

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

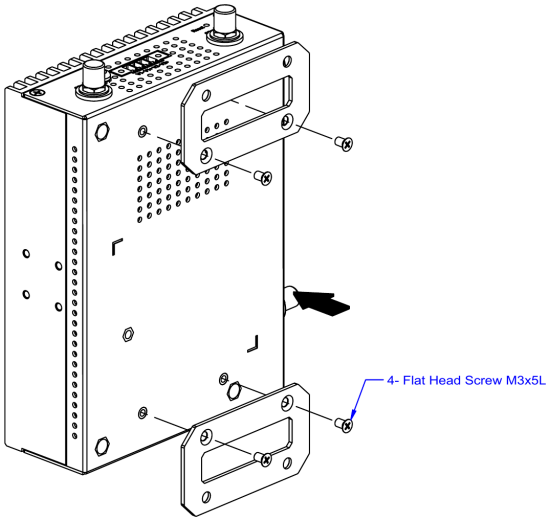


Figure 2.9 Installing Wall Mount Plates

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

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

10. To mount the wall plate, use screws of the size shown in the following illustration.

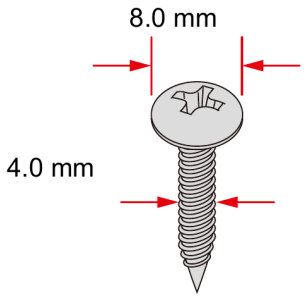


Figure 2.10 Wall Mounting Screw Dimensions

Note!

- *Make sure the screws dimensions are suitable for use with the wall mounting plate.*
- *Do not completely tighten the screws into the wall. A final adjustment may be needed before fully securing the wall mounting plates on the wall.*

11. Align the wall mount plate over the screws on the wall.

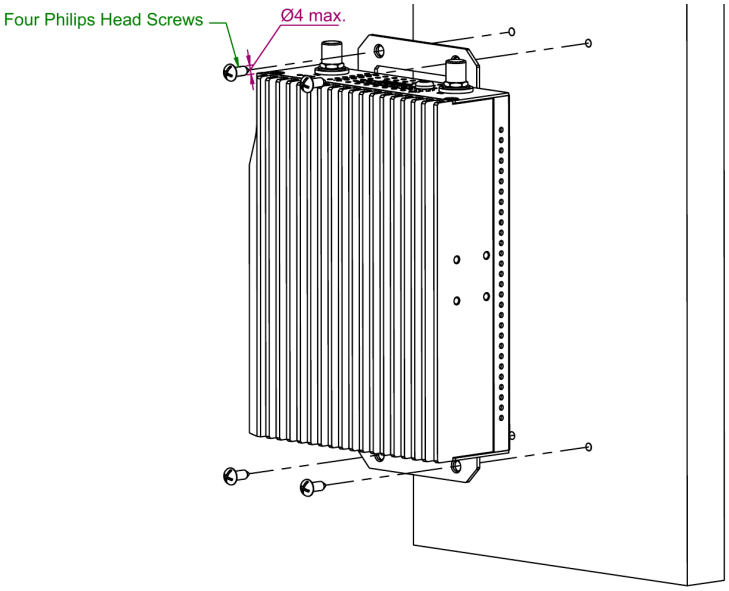


Figure 2.11 Wall Mount Installation

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

2.2.3 Wireless Connection

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

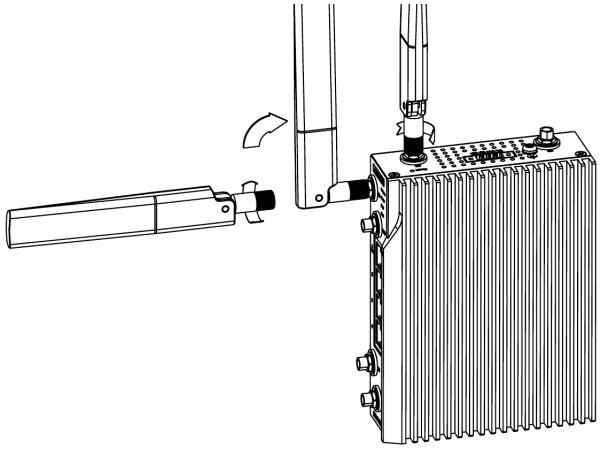


Figure 2.12 Installing the Antenna

2. Position the antenna for optimal signal strength.

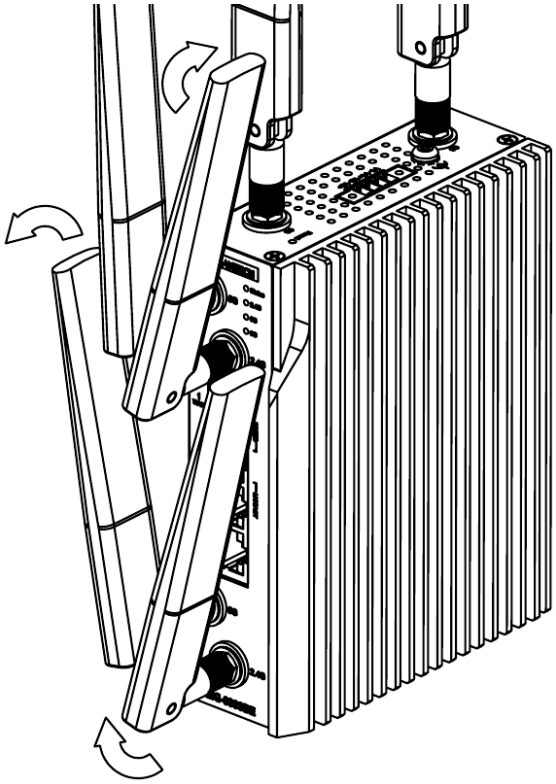


Figure 2.13 Positioning the Antenna

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

2.2.4 Network Connection

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

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

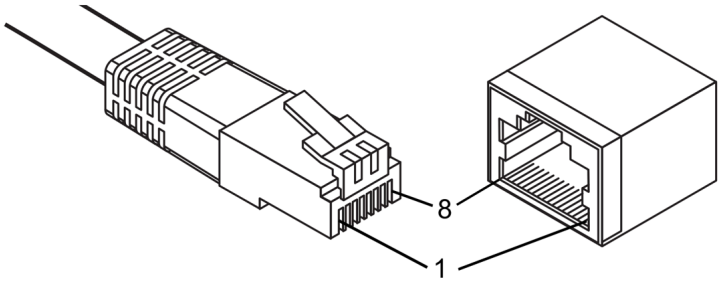


Figure 2.14 Ethernet Plug & Connector Pin Position

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

2.2.5 Power Connection

2.2.5.1 Overview

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



Caution! *Do not disconnect modules or cabling unless the power is first gatewayed 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 gateways can be powered by using the same DC source used to power other devices. A DC voltage range of 12 to 48 V_{DC} must be applied between the V1+ terminal and the V1- terminal (PW1), see the following illustrations. The chassis ground screw terminal should be tied to the panel or chassis ground. A redundant power configuration is supported through a secondary power supply unit to reduce network down time as a result of power loss.

EKI-6333BE-4GD Series support 12 to 48 V_{DC}. Dual power inputs are supported and allow you to connect a backup power source.

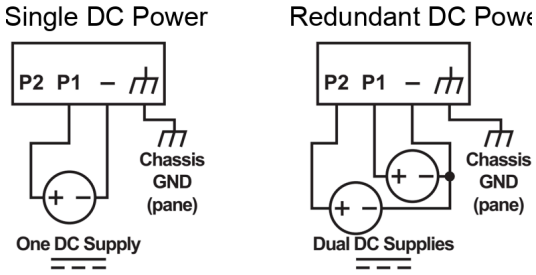


Figure 2.15 Power Wiring for EKI-6333BE-4GD Series

2.2.5.2 Considerations

Take into consideration the following guidelines before wiring the device:

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

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

2.2.5.3 Grounding the Device

Caution! *Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the device.*

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

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

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

Caution! *Do not block air ventilation holes.*

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

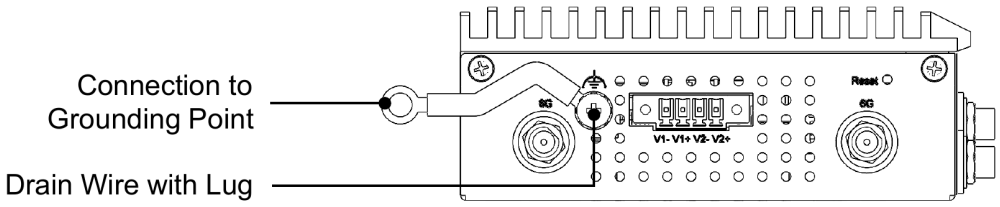


Figure 2.16 Grounding Connection

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

Note! *Before applying power to the grounded gateway, 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 gateway.*

2.2.5.4 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 gateway.*

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

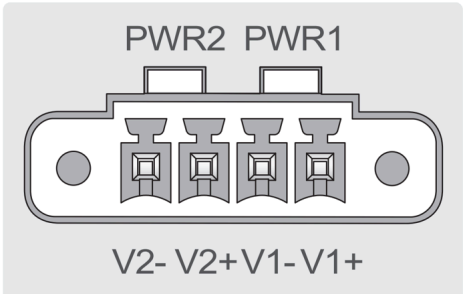


Figure 2.17 Terminal Receptor: Power Input Contacts

To wire the power inputs:

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

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

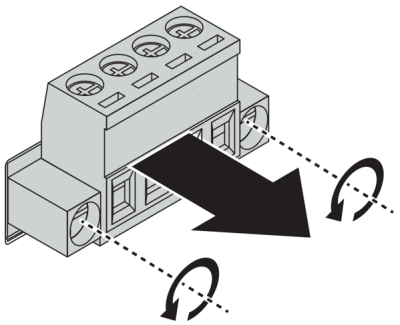


Figure 2.18 Removing a Terminal Block

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

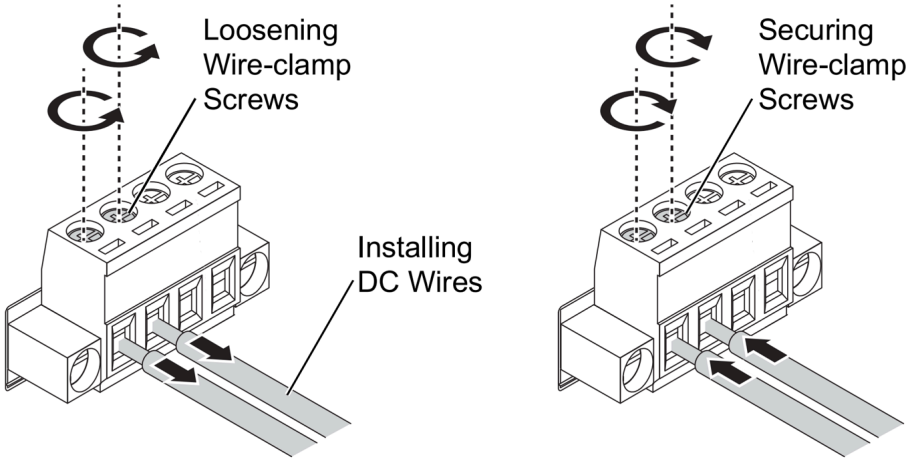


Figure 2.19 Installing DC Wires in a Terminal Block

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

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

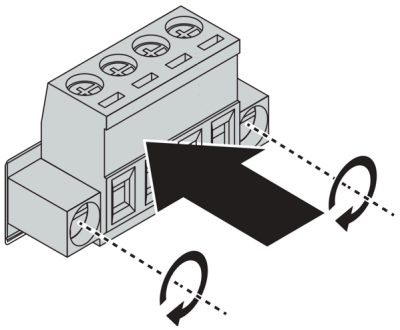


Figure 2.20 Securing a Terminal Block to a Receptor

2.3 Reset Button

Reset configuration to factory default:

Press and hold Reset button for 5 seconds.

System reboot:

Press and hold Reset button for 2 seconds.

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



Chapter 3

Web Interface

3.1 Log In

To access the login window, connect the device to the network, see Section 2.2. 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.

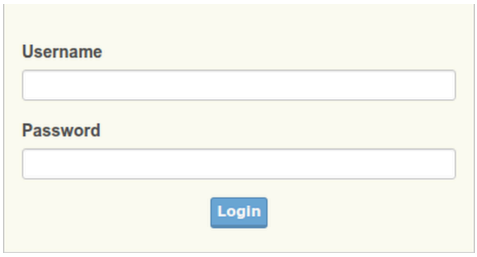


Figure 3.1 Login Screen

Note! *Screen may differ depending on the Web browser.*

5. If this is the first time logging in with the default password, the **Change Password** screen displays automatically. Enter the default password in the **Old Password** field, enter a new password in the **New Password** field, and re-enter it in the **Confirm Password** field.
6. Click **Submit** to change the password and continue to the management interface.

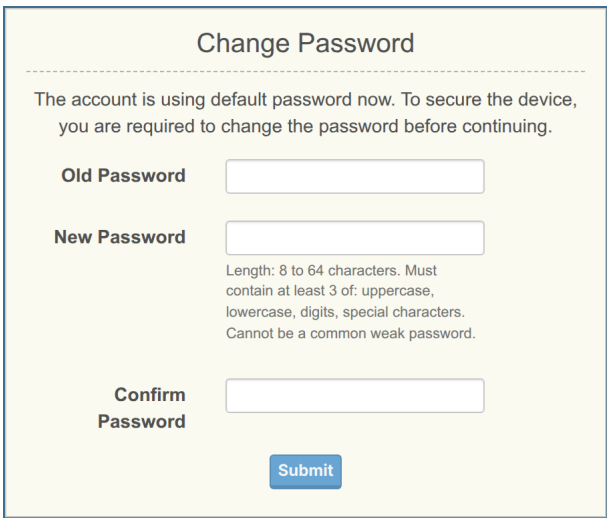


Figure 3.2 Change Password (First Login)

Note! *The new password must be 8 to 64 characters long and contain at least 3 of the following: uppercase letters, lowercase letters, digits, and special characters. Common weak passwords are not accepted.*

3.1.1 Password

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

1. Log in to the user interface menu, see Section 3.1.
2. Navigate to **Home** > **Management** > **Account Manager** . The Account Manager page displays.
3. The profile to change is the current logged in profile. Enter the new password under the Password field.
4. Re-type the same password in the **Confirm Password** field.
5. Click **Apply** to change the current account settings.



Figure 3.3 Management > Account Manager

6. Once completed, the settings must be saved to the firmware to retain them after a reboot. Navigate to **Home** > **Management** > **Apply Configuration** .
7. Click **Apply and Reboot** to save the settings.

3.2 Overview

To access this page, Navigate to **Home** > **Status** and click **Overview** .

System Info

Information Name	Information Value
Firmware Version	1.1.4
Local Hostname	Advantech
System Time	Fri May 8 10:58:41 2026
System Up Time	0 day 17 hr 21 min 29 sec
Model Name	Advantech EKI-6333BE
Serial Number	



Figure 3.4 Status > Overview, System Info and LAN Interface

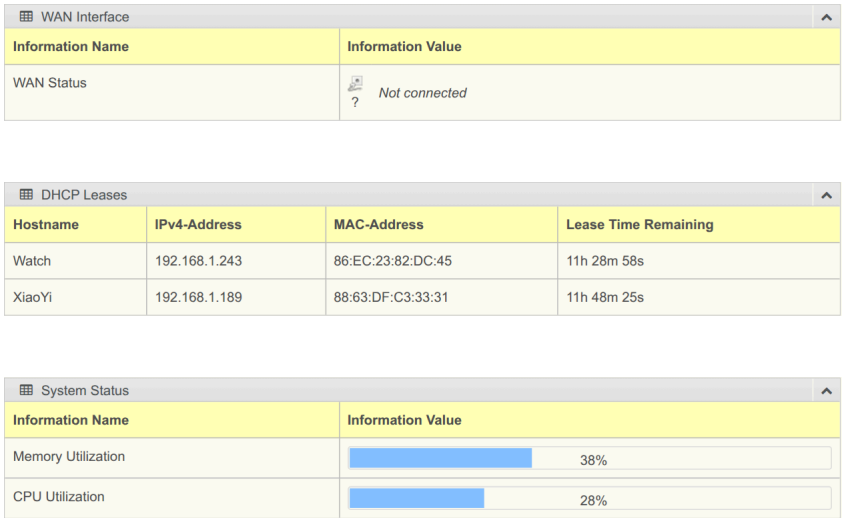


Figure 3.5 Status > Overview, WAN Interface, DHCP Leases, and System Status

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 and time of the device.
System Up Time	Displays the time since the last device reboot.
Model Name	Displays the model name of the device.
Serial Number	Displays the device serial number.

Item	Description
LAN Interface	
LAN Status	Displays the LAN interface address, netmask, RX (KB / packets), TX (MB / packets), and MAC address.
Wireless - 2.4GHz	Displays the current settings for the 2.4 GHz interface, listing the access point mode, SSID name, BSSID, encryption type, wireless channel, TX power and country code.
Wireless - 5GHz	Displays the current settings for the 5 GHz interface, listing the access point mode, SSID name, BSSID, encryption type, wireless channel, TX power and country code.
Wireless - 6GHz	Displays the current settings for the 6 GHz interface, listing the access point mode, SSID name, BSSID, encryption type, wireless channel, TX power and country code.
Wireless - MLO 2.4GHz	Displays the MLO 2.4 GHz link information (mode, SSID, BSSID, encryption, country code).
Wireless - MLO 5GHz	Displays the MLO 5 GHz link information (mode, SSID, BSSID, encryption, country code).
Wireless - MLO 6GHz	Displays the MLO 6 GHz link information (mode, SSID, BSSID, encryption, country code).
WAN Interface	
WAN Status	Displays the WAN address, netmask, gateway, DNS server and protocol when the WAN is connected.
DHCP Leases	
Hostname	Displays the hostname of each DHCP client.
IPv4-Address	Displays the assigned IPv4 address of each DHCP client.
MAC-Address	Displays the MAC address of each DHCP client.
Lease Time Remaining	Displays the remaining lease time before the DHCP entry expires.
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 Address Resolution Protocol

The Address Resolution Protocol (ARP) allows mapping of dynamic Internet Protocol addresses (IP address) to a permanent physical machine address in a local area network (LAN) through the use of the MAC address.

To access this page, Navigate to **Home** > **Status** and click **ARP** .

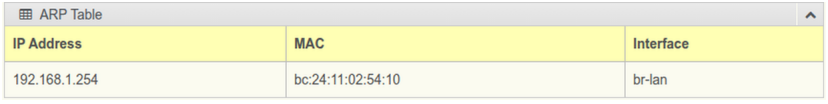


Figure 3.6 Status > ARP

The following table describes the items in the previous figure.

Item	Description
ARP Table	
IP Address	Displays the mapped IP address learned by the device.
MAC	Displays the MAC address of the defined IP list entry.
Interface	Displays the bridge or physical interface (for example, br-lan) on which the entry exists.

3.4 Interface Settings

3.4.1 LAN

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

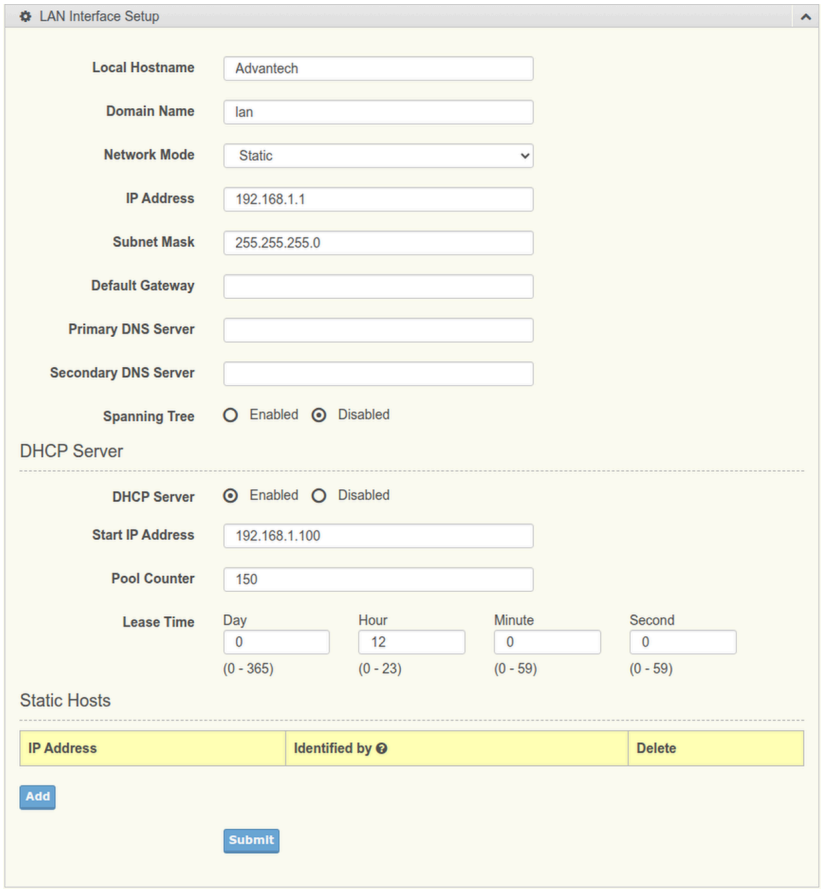


Figure 3.7 Interface > LAN

The following table describes the items in the previous figure.

Item	Description
LAN Interface Setup	
Local Hostname	Enter the device name: up to 16 alphanumeric characters.
Domain Name	Enter the text string to define the name of a domain.
Network Mode	Click the drop-down menu to select the IP Address setting mode: Static (default) or DHCP. When DHCP is selected the IP-related fields below are obtained from a DHCP server.
IP Address	Enter a value to specify the IP address of the interface. The default is 192.168.1.1.
Subnet Mask	Enter a value to specify the IP subnet mask for the interface. The default is 255.255.255.0.
Default Gateway	Enter the gateway IP address. Must be on the same subnet as the LAN IP.
Primary DNS Server	Enter the primary static DNS server IP.
Secondary DNS Server	Enter the secondary static DNS server IP.
Spanning Tree	Click the radio button to enable or disable (default) the spanning tree service.
DHCP Server	

Item	Description
DHCP Server	Click the radio button to enable (default) or disable the DHCP server function.
Start IP Address	Enter a starting IP address for the IP assignment. Must be on the same subnet as the LAN IP and unique within the network.
Pool Counter	Enter the number of IP addresses to be assigned by the DHCP server.
Lease Time	Enter the DHCP lease time in Day / Hour / Minute / Second (must be greater than 30 seconds). Default is 12 hours.
Static Hosts	
IP Address	Enter the static IP address to assign to a specific Hostname or MAC. Must be unique and on the same subnet as the LAN IP.
Identified by	Click the drop-down to select Hostname or MAC. Enter the matching Hostname or MAC (for example, 00:11:22:33:44:55) the static IP entry is bound to.
Add / Delete	Click **Add** to insert a new static host entry; click **Delete** to remove an existing one.
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** > **Apply Configuration** > **Apply and Reboot** .*

3.4.2 WAN

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

The Interface screen allows user to setup the WAN interface and its network function mode.

Disable Mode

When Network Mode is set to Disable (default), the device disables the WAN service and all interfaces (LAN 1, WLAN 2.4G, WLAN 5G, WLAN 6G) are used as local interfaces.



Figure 3.8 Interface > WAN > Network Mode (Disable)

The following table describes the items in the previous figure.

Item	Description
Network Mode	Click the drop-down menu to select the mode type: Disable (default), Static, DHCP, PPPoE.
Submit	Click **Submit** to save the values and update the screen.

Static Mode

When Network Mode is set to Static , the Static WAN Type configuration settings appear.

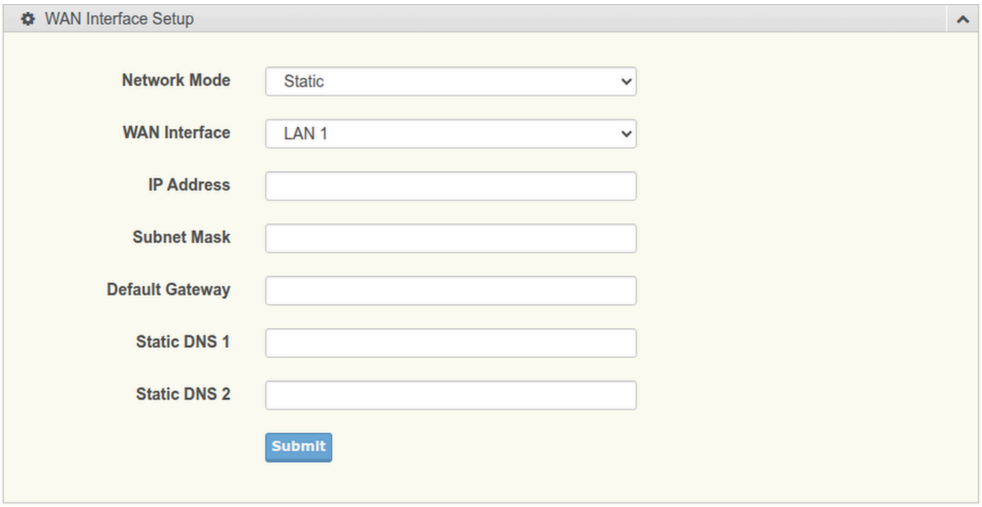


Figure 3.9 Interface > WAN > Network Mode > Static

The following table describes the items in the previous figure.

Item	Description
Network Mode	Click the drop-down menu to select the mode type: Disable (default), Static, DHCP, PPPoE.
WAN Interface	Click the drop-down to select the WAN interface to configure: LAN 1, WLAN 2.4G, WLAN 5G, or WLAN 6G.
IP Address	Enter the WAN IP address given by your service provider.
Subnet Mask	Enter the WAN subnet mask given by your service provider.
Default Gateway	Enter the WAN gateway IP address given by your service provider. Must be on the same subnet as the WAN IP.
Static DNS 1	Enter the primary WAN DNS IP address given by your service provider.
Static DNS 2	Enter the secondary WAN DNS IP address given by your service provider.
Submit	Click **Submit** to save the values and update the screen.

DHCP Mode

When Network Mode is set to DHCP , the WAN obtains its IP and DNS settings automatically from a DHCP server.



Figure 3.10 Interface > WAN > Network Mode > DHCP

The following table describes the items in the previous figure.

Item	Description
Network Mode	Click the drop-down menu to select the mode type: Disable (default), Static, DHCP, PPPoE.
WAN Interface	Click the drop-down to select the WAN interface to configure: LAN 1, WLAN 2.4G, WLAN 5G, or WLAN 6G.
Submit	Click **Submit** to save the values and update the screen.

PPPoE Mode

When Network Mode is set to PPPoE , the PPPoE WAN Type configuration settings appear.

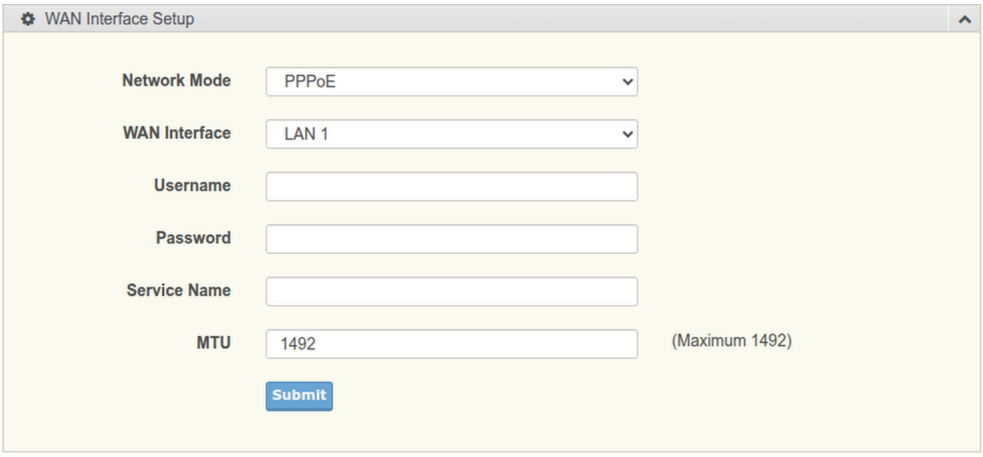


Figure 3.11 Interface > WAN > Network Mode > PPPoE

The following table describes the items in the previous figure.

Item	Description
Network Mode	Click the drop-down menu to select the mode type: Disable (default), Static, DHCP, PPPoE.
WAN Interface	Click the drop-down to select the WAN interface to configure: LAN 1, WLAN 2.4G, WLAN 5G, or WLAN 6G.
Username	Enter the PPPoE user name (account) provided by your service provider.
Password	Enter the PPPoE password provided by your service provider.
Service Name	Enter the service name if your ISP requires it.
MTU	Enter the MTU (Maximum Transmission Unit) for PPPoE encapsulation. Default 1492 (maximum 1492).
Submit	Click **Submit** to save the values and update the screen.

3.4.2.1 Topology

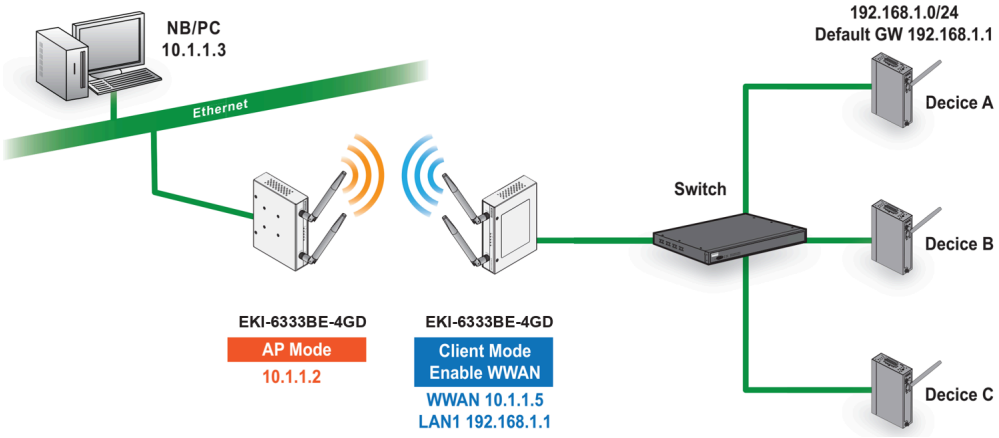


Figure 3.12 Wireless WAN Topology

3.4.3 Wireless 2.4GHz

To access this page, click **Interface** > **Wireless - 2.4GHz** .

3.4.3.1 Basic

Basic wireless settings offer two types of configurable modes, Access Point and Client.

The following descriptions provide further details for each specific mode.

Access Point Mode

To access this page, click **Wireless - 2.4GHz** > **Basic** and select **Access Point** in Operation Mode.

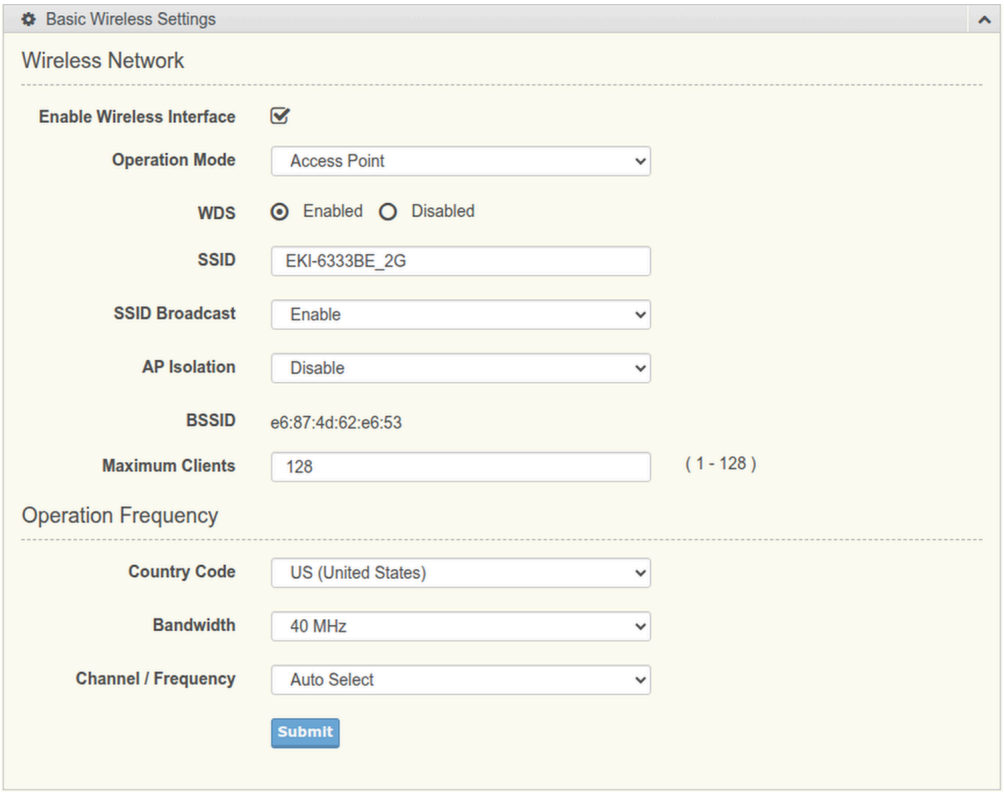


Figure 3.13 Wireless - 2.4GHz > Basic > Access Point

The following table describes the items in the previous figure.

Item	Description
Wireless Network	
Enable Wireless Interface	Click to enable or disable the interface.
Operation Mode	Click the drop-down menu to select an operation mode: Access Point or Client.
WDS	Click the radio button to enable or disable the Wireless Distribution System (WDS) to allow your device to create WDS link with peer devices. Note: For the function to initiate effectively, the wireless devices intended for pairing, must be simultaneously turned on.
SSID	Enter the name to distinguish it from other networks in your neighborhood.
SSID Broadcast	Click the drop-down menu to enable or disable the SSID broadcast function. The function is only enabled when Operation Mode is set to Access Point.
AP Isolation	Click the drop-down menu to enable or disable the AP Isolation function. The function is only enabled when Operation Mode is set to Access Point.
BSSID	Display the MAC address of the device.

Item	Description
Maximum Clients	Enter the value (1 to 128) designating the maximum number of clients per wireless device.
Operation Frequency	
Country Code	Click the drop-down menu to select the country/region. Available channels and transmit power follow the regulatory domain of the selected country.
Bandwidth	Click the drop-down menu to select the channel bandwidth. 2.4 GHz: 20 MHz or 40 MHz. 5 GHz: 20, 40, 80, or 160 MHz. 6 GHz: 20, 40, 80, 160, or 320 MHz (EHT320 Wi-Fi 7).
Channel / Frequency	Click the drop-down menu to select the operating channel and frequency. Default: Auto Select.
Submit	Click **Submit** to save the values and update the screen.

Client Mode

To access this page, click **Wireless - 2.4GHz** > **Basic** and select **Client** in Operation Mode.

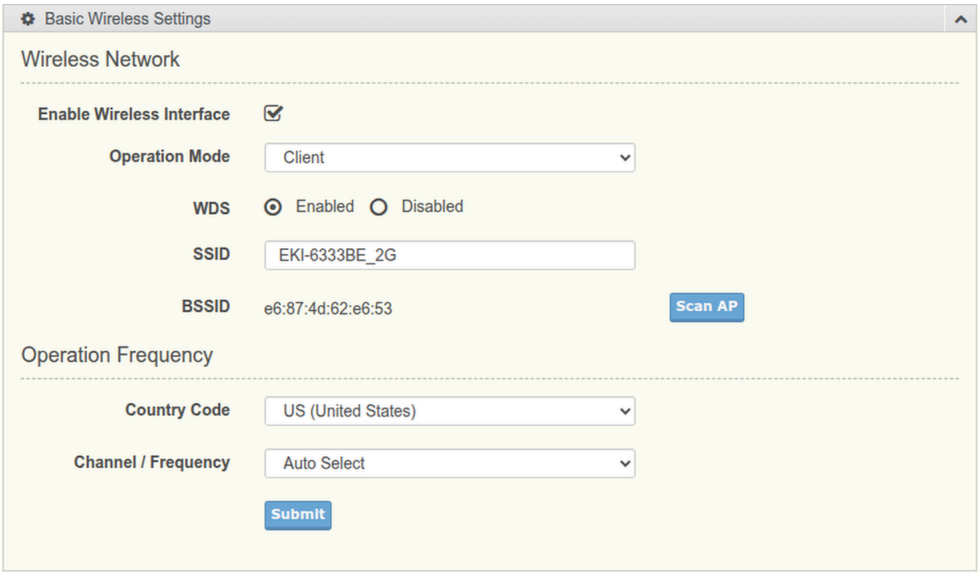


Figure 3.14 Wireless - 2.4GHz > Basic > Client

The following table describes Wireless Network screen.

Item	Description
Wireless Network	
Enable Wireless Interface	Click to enable or disable the interface.
Operation Mode	Click the drop-down menu to select an operation mode: Access Point or Client.
WDS	Click the radio button to enable or disable the Wireless Distribution System (WDS) to allow your device to create WDS link with peer devices.
SSID	Enter the name of the target access point to associate with.
BSSID	Displays the basic service set identifiers (BSSID) for the device.
Scan AP	Click to rescan and detect nearby Access Points.
Operation Frequency	

Item	Description
Country Code	Click the drop-down menu to select the country/region. Available channels and transmit power follow the regulatory domain of the selected country.
Channel / Frequency	Click the drop-down menu to select the operating channel and frequency. Default: Auto Select.
Submit	Click **Submit** to save the values and update the list.

3.4.3.2 Advanced

Access Point Mode

To view the Advanced menu, the Basic Operation Mode must be designated to Access Point Mode.

To access this page, click **Wireless - 2.4GHz** > **Advanced** .

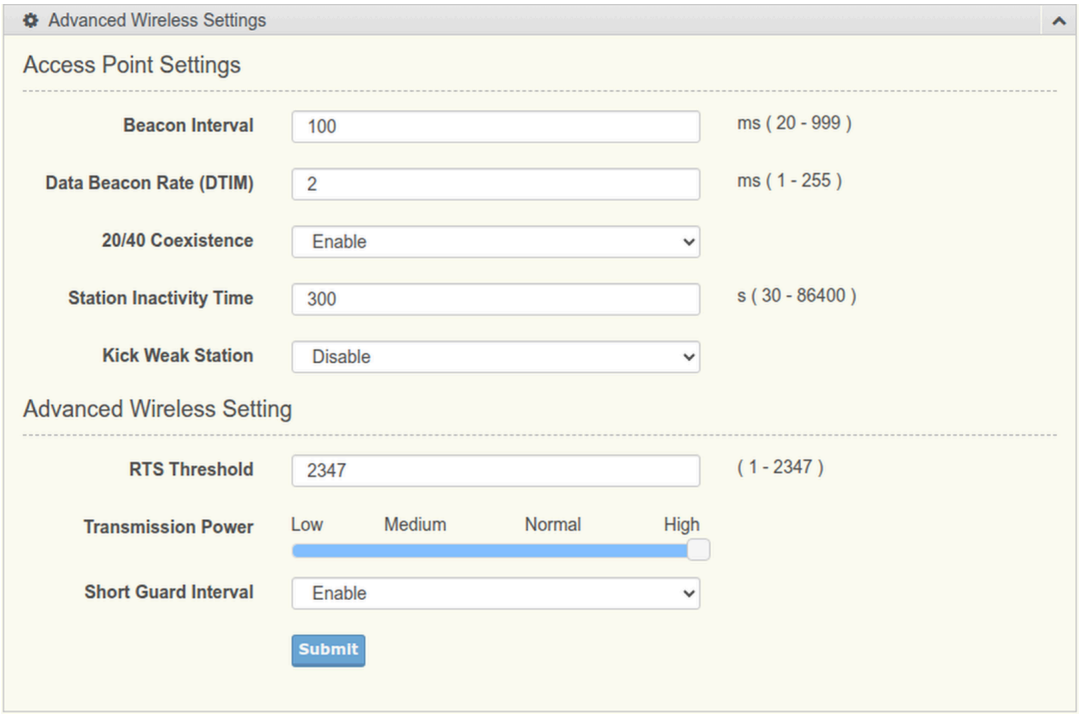


Figure 3.15 Wireless - 2.4GHz > Advanced

The following table describes the items in the previous figure.

Item	Description
Access Point Settings	
Beacon Interval	Enter a value (20-999) to specify the frequency interval to broadcast packets.
Data Beacon Rate (DTIM)	DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 2. Enter a value between 1 and 255.
20/40 Coexistence	Select enable to select 20/40 MHz coexistence. Once enabled, the device allows clients operating only on a single channel (20 MHz) to connect to the wireless network (default: disabled).
Station Inactivity Time	Enter the value in seconds (30 to 86400, default 300) to define the period of traffic inactivity for a client before the AP removes it.

Item	Description
Kick Weak Station	Click the drop-down menu to enable or disable disconnecting clients with a weak signal from the AP (default: disabled).
Advanced Wireless Setting	
RTS Threshold	Enter a value (1-2347) to specify the request time to send threshold.
Transmission Power	Click the slide bar to select the transmission power level: Low, Medium, Normal, or High.
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 Mode

To view the Advanced menu under Client Mode, click **Wireless - 2.4GHz** > **Advanced** . The following Client Settings menu is only available when Basic Operation Mode is set to Client.

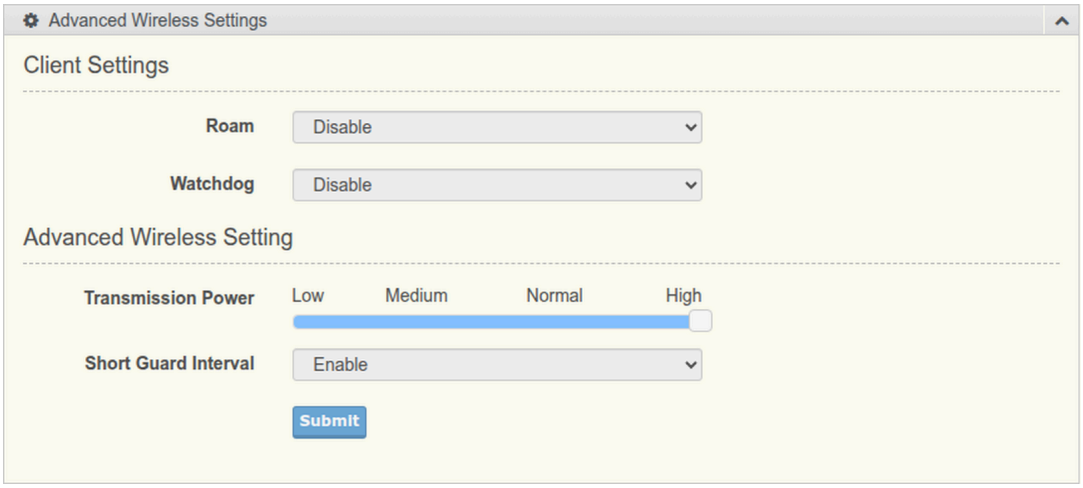


Figure 3.16 Wireless - 2.4GHz > Advanced (Client Mode)

The following table describes the items in the previous figure.

Item	Description
Client Settings	
Roam	Click to enable or disable 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.

Item	Description
Watchdog	Click to set the Watchdog policy to Disable (default), Disassociate, Ping. **Disable:** Select to disable the Watchdog function (Default). **Disassociate:** When EKI-6333BE-4GD disassociates with AP, and doesn't connect with any AP within the seconds specified in the Disassociate Timer field, the device will act according to the Watchdog Action field. **Ping:** Continuously ping a specific remote host for connection status using a user-defined IP address. If the target IP address cannot be pinged the designated action (Restart WLAN, Reboot, Force re-association) will be taken. - Watchdog Action: Designate the action (Restart WLAN, Reboot, Force re-association) when the conditions of Watchdog policy are met. - 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 Wireless Setting	
Transmission Power	Click the slide bar to select the transmission power level: Low, Medium, Normal, or High.
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.

3.4.3.3 Security

To access this page, click **Wireless - 2.4GHz** > **Security** .

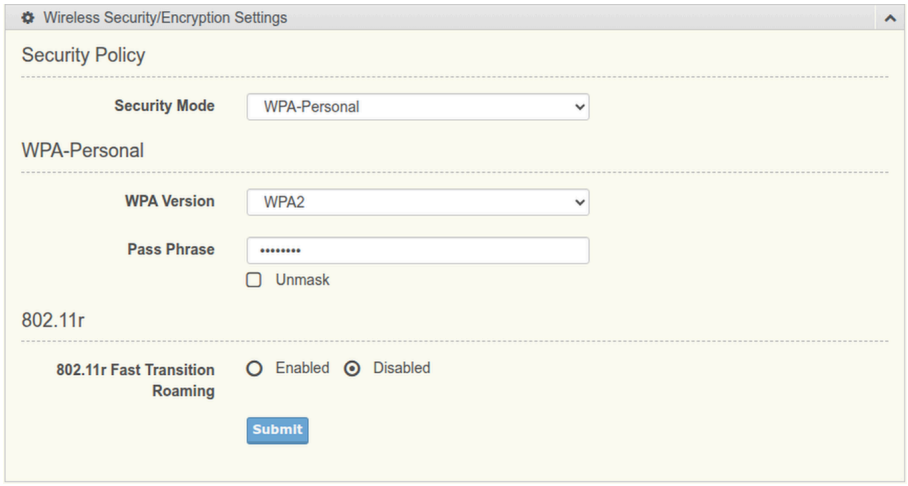


Figure 3.17 Wireless - 2.4GHz > Security

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 used for wireless communication. Available options: None, WPA-Personal, WPA-Enterprise. WPA-Personal supports WPA2, WPA3, and the WPA2+WPA3 transition mode.
Submit	Click **Submit** to save the values and update the screen.

None Mode

To access this page, click **Wireless Settings** > **Security** .

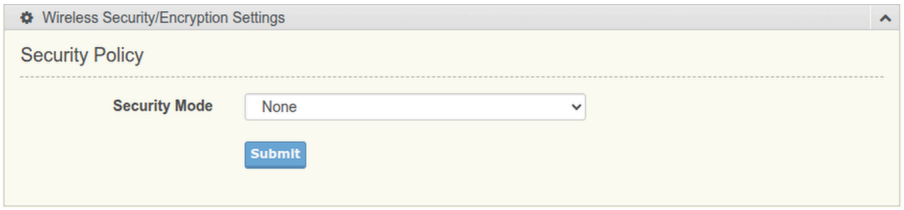


Figure 3.18 Wireless Settings > Security

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 used for wireless communication. Available options: None, WPA-Personal, WPA-Enterprise. With None selected, the wireless network is open (unauthenticated) — recommended only for isolated test deployments.
Submit	Click **Submit** to save the values and update the screen.

WPA-Personal Mode

To access this page, click **Interface** > **Wireless - 2.4** > **Security** > **Security Mode** > **WPA-Personal** .

WPA-Personal uses a pre-shared passphrase (PSK / SAE) for authentication. WPA3 (SAE) is recommended for new deployments; WPA2+WPA3 is a transition mode that accepts both legacy WPA2-PSK and WPA3-SAE clients on the same SSID.

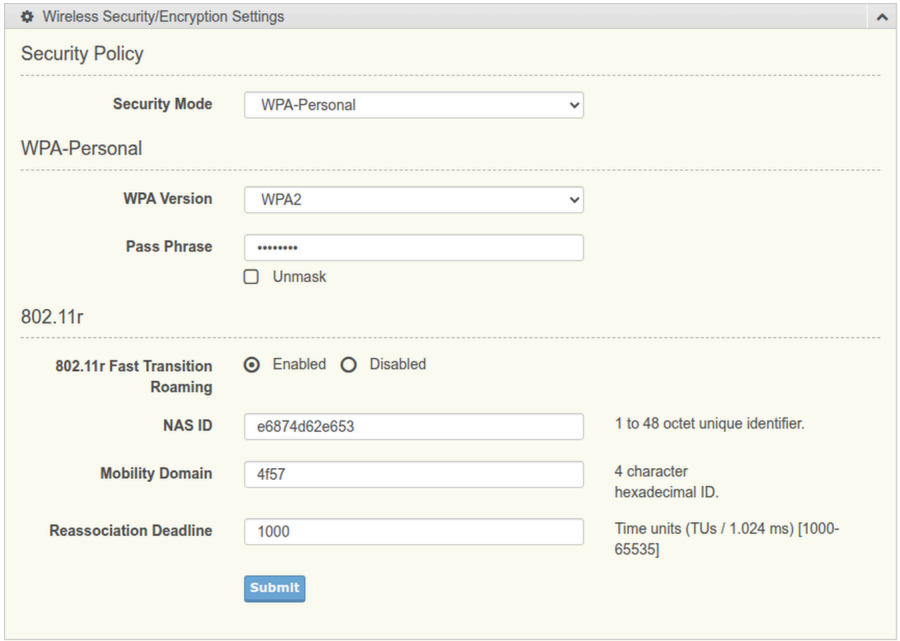


Figure 3.19 Security Mode > WPA-Personal

The following table describes the items in the previous figure.

Item	Description
Security Policy	

Item	Description
Security Mode	Click the drop-down menu to select the encryption used for wireless communication. Available options: None, WPA-Personal, WPA-Enterprise.
WPA Personal	
WPA Version	Click the drop-down menu to designate the authentication standard. Available options: WPA2, WPA3, WPA2+WPA3. Legacy WPA1 / WPA1+WPA2 are no longer supported.
Pass Phrase	Enter a unique password to define the passphrase used for authentication. The passphrase is 8–63 ASCII characters. Click **Unmask** to view the entered value.
802.11r	
802.11r Fast Transition Roaming	Click to enable or disable the 802.11r function allowing clients with WPA-Personal to move faster between APs. The 802.11r function is only available when the device is in AP mode.
NAS ID	Enter the ID (1 to 48 octet unique identifier) to associate to the WLAN. In the 802.11r group, the NAS ID of each AP must different.
Mobility Domain	Enter the corresponding mobility domain identifier (4 character hexadecimal ID) to enable 802.11r roaming. In a network of standalone Instant APs within the same management VLAN, 802.11r roaming does not function due to mobility domain identifiers not matching across Instant APs. The identifiers are auto-generated. Users can set a mobility domain identifier to enable 802.11r. For standalone Instant APs in the same management VLAN, 802.11r, the same value must correspond across the same management VLAN.
Reassociation Deadline	Enter a timeout value in seconds. The range is 1000 to 65535 (default: 1.024 ms). The deadline is the life time that the destination AP will keep the security information of the roaming client. If the client hasn't roamed to the destination AP after the deadline, the destination AP will remove the security information of the client.
Submit	Click **Submit** to save the values and update the screen.

WPA-Enterprise Mode

To access this page, click **Interface** > **Wireless - 2.4** > **Security** > **Security Mode** > **WPA-Enterprise** .

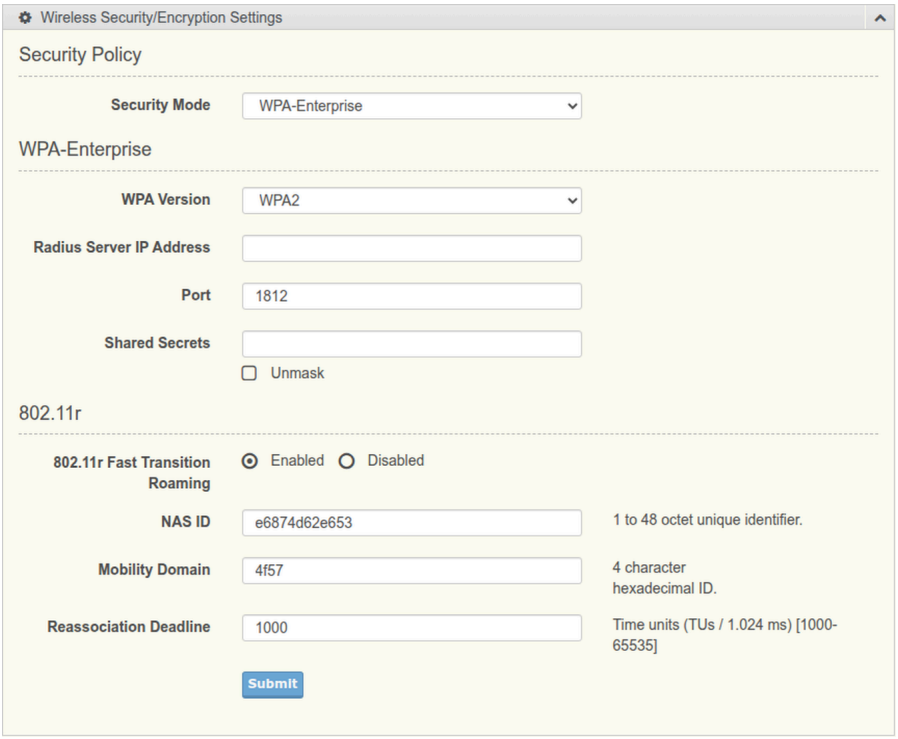


Figure 3.20 Security Mode > WPA-Enterprise

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 used for wireless communication. Available options: None, WPA-Personal, WPA-Enterprise.
WPA-Enterprise	
WPA Version	Click the drop-down menu to select the WPA standard. Available options: WPA2.
Radius Server IP Address	Enter the IP address of the designated RADIUS server used for 802.1X authentication.
Port	Enter the UDP port on which the RADIUS server listens for authentication requests (default 1812).
Shared Secrets	Enter the string used as the shared secret between the access point and the RADIUS server.
802.11r	
802.11r Fast Transition Roaming	Click to enable or disable the 802.11r function allowing clients with WPA-Enterprise to move faster between APs. The 802.11r function is only available when the device is in AP mode.
NAS ID	Enter the ID (1 to 48 octet unique identifier) to associate to the WLAN. In the 802.11r group, the NAS ID of each AP must different.

Item	Description
Mobility Domain	Enter the corresponding mobility domain identifier (4 character hexadecimal ID) to enable 802.11r roaming. In a network of standalone Instant APs within the same management VLAN, 802.11r roaming does not function due to mobility domain identifiers not matching across Instant APs. The identifiers are auto-generated. Users can set a mobility domain identifier to enable 802.11r. For standalone Instant APs in the same management VLAN, 802.11r, the same value must correspond across the same management VLAN.
Reassociation Deadline	Enter a timeout value in seconds. The range is 1000 to 65535 (default: 1.024 ms). The deadline is the life time that the destination AP will keep the security information of the roaming client. If the client hasn't roamed to the destination AP after the deadline, the destination AP will remove the security information of the client.
Submit	Click **Submit** to save the values and update the screen.

3.4.3.4 Multiple SSID

The Multiple SSID feature is only available when the wireless operation mode of the device is set to Access Point mode.

To access this page, click **Wireless - 2.4GHz** > **Multiple SSID** .

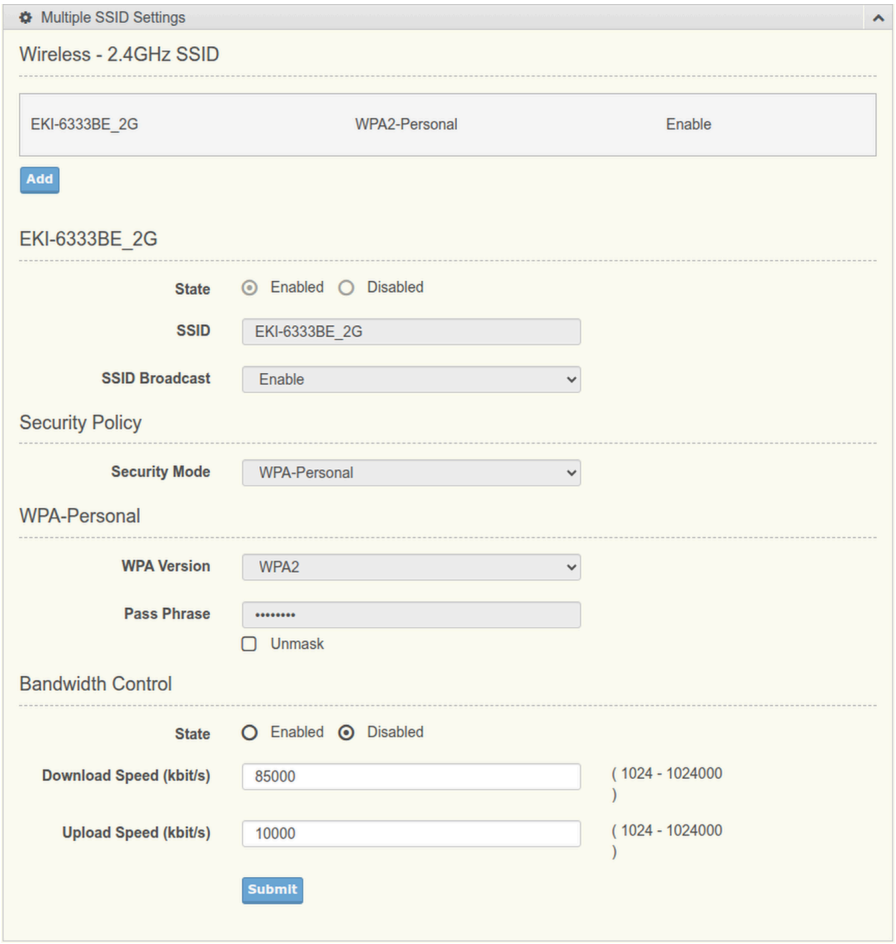


Figure 3.21 Wireless - 2.4GHz > Multiple SSID

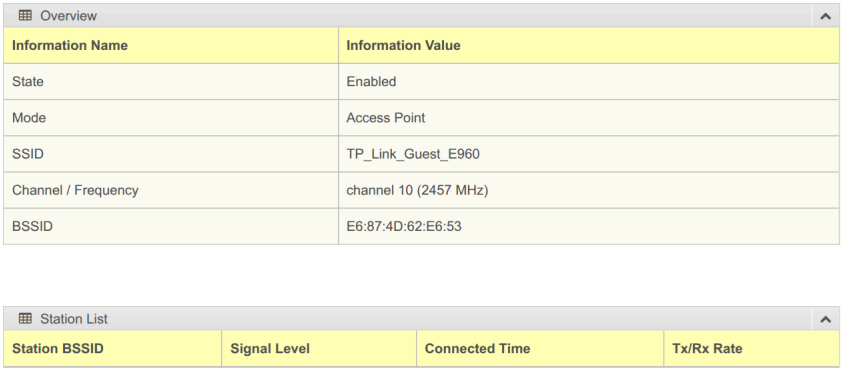
The following table describes the items in the previous figure.

Item	Description
Wireless - 2.4GHz SSID	
Add	Click **Add** after completing the SSID information to create the wireless network and list it in the menu.
<2.4GHz SSID>	
State	Click the radio button to enable or disable the defined SSID.
SSID	Enter the text string identifying the name of the SSID.
SSID Broadcast	Click the drop-down menu to enable (visible) or disable (not broadcasted) the broadcasting of the SSID name.
Security Policy	
Security Mode	Click the drop-down menu to select the encryption used for the additional SSID. Available options: None, WPA-Personal, WPA-Enterprise.
WPA-Personal	
WPA Version	Click the drop-down menu to select the WPA Version: WPA2, WPA3, or WPA2+WPA3 (transition mode). The same options as the primary Security page apply to each additional SSID.
Pass Phrase	Enter the pre-shared key (8–63 ASCII characters or 64 hex digits) used to authenticate clients connecting to this SSID.
Bandwidth Control	
State	Click the radio button to enable or disable per-SSID bandwidth control.
Download Speed (kbits)	Enter the maximum download rate (kbps) for clients on this SSID when Bandwidth Control is enabled.
Upload Speed (kbits)	Enter the maximum upload rate (kbps) for clients on this SSID when Bandwidth Control is enabled.
Submit	Click **Submit** to save the values and update the screen.

3.4.3.5 Statistics

The function provides statistic information about the wireless network reporting on traffic records and station lists.

To access this page, click **Wireless - 2.4GHz** > **Statistics** .



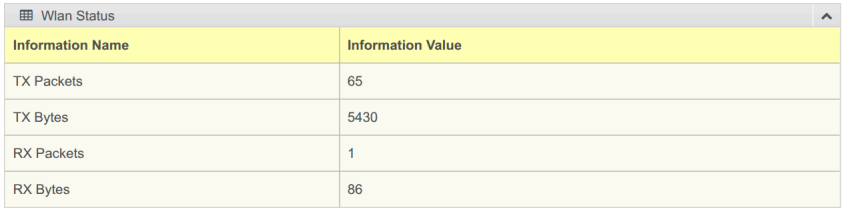


Figure 3.22 Wireless - 2.4GHz > Statistics

The following table describes the items in the previous figure.

Item	Description
Overview	
State	Displays the current state (Enabled / Disabled) of the interface.
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.

3.4.3.6 Access Control

The Access Control feature appoints the authority to wireless clients on accessing EKI-6333BE-4GD Series, providing an additional security mechanism. This function is available only under AP mode.

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

To access this page, click **Wireless - 2.4GHz** > **Access Control** .

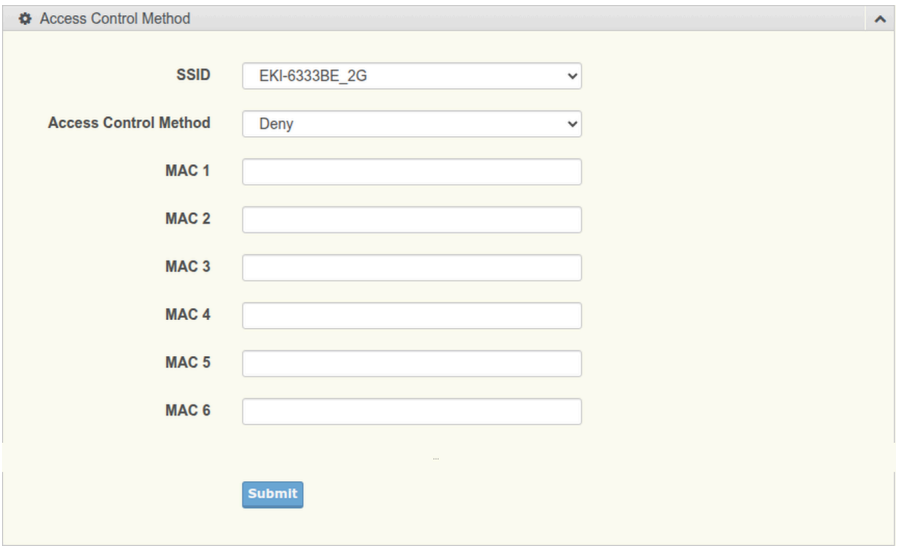


Figure 3.23 Wireless - 2.4GHz > Access Control

The following table describes the items in the previous figure.

Item	Description
SSID	Click the drop-down menu to select the SSID from the list of already created wireless networks.
Access Control Method	Click the drop-down menu to set the access control method: Disable, Deny or Allow.
MAC 1..N	Enter up to 32 MAC addresses to deny or allow. The field count expands automatically as entries are filled.
Submit	Click **Submit** to save the values and update the screen.

3.4.3.7 Traffic Control

The Traffic Control function provides quality connection control to a connected client over the network, mainly limiting the upper or lower speed of the connection. The traffic control function is only available when the device is in AP mode.

To access this page, click **Wireless - 2.4GHz** > **Traffic Control** .

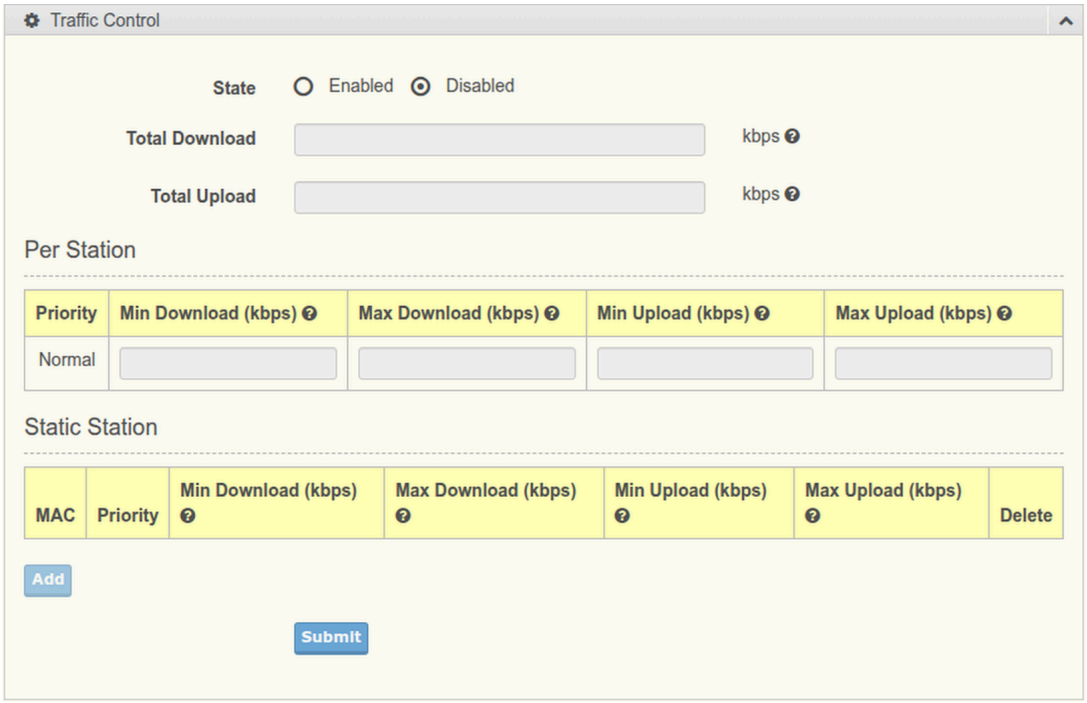


Figure 3.24 Wireless - 2.4GHz > Traffic Control

Item	Description
State	Click to enable or disable the traffic control function.
Total Download	Enter the value to define the total download speed of the WLAN interface. (Range 1-1000000 kbps)
Total Upload	Enter the value to define the total upload speed of the WLAN interface. (Range 1-1000000 kbps)
Per Station	
Priority	Click the drop-down menu to select the priority class (Normal, High, etc.).
Min Download (kbps)	Enter the minimum guaranteed download speed (kbps) per client.
Max Download (kbps)	Enter the maximum download speed (kbps) per client.
Min Upload (kbps)	Enter the minimum guaranteed upload speed (kbps) per client.
Max Upload (kbps)	Enter the maximum upload speed (kbps) per client.
Static Station	
MAC	Enter the target client MAC address.
Priority	Click the drop-down menu to select the priority class for this client.
Min Download (kbps)	Enter the minimum guaranteed download speed (kbps) for this client.
Max Download (kbps)	Enter the maximum download speed (kbps) for this client.
Min Upload (kbps)	Enter the minimum guaranteed upload speed (kbps) for this client.
Max Upload (kbps)	Enter the maximum upload speed (kbps) for this client.
Add / Delete	Click **Add** to insert a new Static Station entry; click **Delete** to remove an existing one.
Submit	Click **Submit** to save the values and update the setting.

3.4.3.8 Site Survey

The Site Survey page is only available when the wireless operation mode of the device is set to Client mode. It scans nearby Access Points on the 2.4 GHz band so the operator can pick a target SSID to associate with.

To access this page, click **Wireless - 2.4GHz** > **Site Survey** .

The page lists every detected AP with **SSID**, **AP BSSID**, **Channel**, and **Security**. Select an entry, then click **Submit** to copy it back to the Basic page (the SSID and BSSID fields are populated automatically) or **Cancel** to discard the selection.

AP List

SSID	BSSID	Channel	Signal Level	Encryption
EKI-1652WT-P	74:FE:48:B0:B9:7D	1 (2.412 GHz)	-79 dBm	WPA/WPA2
xxxxx	1E:8A:6C:C8:8D:67	1 (2.412 GHz)	-76 dBm	WPA2
chungzi_24g	C4:41:1E:4E:08:80	3 (2.422 GHz)	-77 dBm	Open
Hidden Network	5E:EF:68:34:7C:DD	4 (2.427 GHz)	-77 dBm	WPA2
CHT Wi-Fi Home-XWW	54:B7:BD:21:15:A8	6 (2.437 GHz)	-24 dBm	WPA2
Hidden Network	56:B7:BD:21:15:A8	6 (2.437 GHz)	-25 dBm	WPA2/WPA3
QQ_2G	00:D0:C9:FF:68:CE	6 (2.437 GHz)	-76 dBm	WPA/WPA2
EKI-6333AC-2G-2.4G	88:DC:96:7A:97:A6	6 (2.437 GHz)	-78 dBm	Open
Hidden Network	64:09:80:1C:55:23	10 (2.457 GHz)	-72 dBm	WPA/WPA2
EKI-6333AC-2G_chungzi	74:FE:48:28:AA:E2	10 (2.457 GHz)	-81 dBm	Open
Hidden Network	CC:28:AA:F2:C9:70	10 (2.457 GHz)	-78 dBm	WPA2/WPA3
ASUS_2G	9A:28:AA:F2:C9:71	10 (2.457 GHz)	-79 dBm	WPA2/WPA3
TP_Link_Guest_E960	DE:62:79:84:E9:62	10 (2.457 GHz)	-74 dBm	Open
SQA_Enterprise_2G	00:D0:C9:FE:93:94	1 (2.412 GHz)	-80 dBm	WPA/WPA2
AEPOP2	74:FE:48:61:A5:AA	11 (2.462 GHz)	-79 dBm	WPA2
NETGEAR19	E4:F4:C6:12:C5:DD	1 (2.412 GHz)	-78 dBm	WPA/WPA2
VelopCDC_Marcel	58:EF:68:34:7C:DD	4 (2.427 GHz)	-78 dBm	WPA2
AE	30:16:9D:47:52:FE	5 (2.432 GHz)	-81 dBm	WPA2/WPA3

Figure 3.25 Wireless - 2.4GHz > Site Survey

The following table describes the items in the previous figure.

Item	Description
SSID	The network name (SSID) of the detected Access Point.
BSSID	The MAC address of the detected Access Point.
Channel	The radio channel on which the AP is operating, with its centre frequency shown in parentheses.
Signal Level	The received signal strength in dBm. A value closer to 0 indicates a stronger signal.
Encryption	The security/encryption type used by the AP (e.g., WPA2, WPA/WPA2, Open).
Submit	After selecting an entry from the AP List, click **Submit** to copy the SSID and BSSID to the Basic page.
Cancel	Click **Cancel** to discard the selection and close the dialog.

3.4.4 Wireless 5GHz

To access this page, click **Interface** > **Wireless - 5GHz** .

The Wireless - 5GHz sidebar exposes the same leaves as Wireless 2.4GHz — Basic, Advanced, Security, Multiple SSID, Statistics, Access Control, Traffic Control in AP mode; Basic, Advanced, Security, Statistics, Site Survey in Client mode. For per-field descriptions, refer to the corresponding Wireless 2.4GHz subsection.

3.4.4.1 Basic

To access this page, click **Wireless - 5GHz** > **Basic** .

For per-field descriptions, refer to Section 3.4.3.1.

3.4.4.2 Advanced

To access this page, click **Wireless - 5GHz** > **Advanced** .

For per-field descriptions, refer to Section 3.4.3.2.

3.4.4.3 Security

To access this page, click **Wireless - 5GHz** > **Security** .

For per-field descriptions, refer to Section 3.4.3.3.

3.4.4.4 Multiple SSID

To access this page, click **Wireless - 5GHz** > **Multiple SSID** .

For per-field descriptions, refer to Section 3.4.3.4.

3.4.4.5 Statistics

To access this page, click **Wireless - 5GHz** > **Statistics** .

For per-field descriptions, refer to Section 3.4.3.5.

3.4.4.6 Access Control

To access this page, click **Wireless - 5GHz** > **Access Control** .

For per-field descriptions, refer to Section 3.4.3.6.

3.4.4.7 Traffic Control

To access this page, click **Wireless - 5GHz** > **Traffic Control** .

For per-field descriptions, refer to Section 3.4.3.7.

3.4.4.8 Site Survey

To access this page, click **Wireless - 5GHz** > **Site Survey** .

For per-field descriptions, refer to Section 3.4.3.8.

3.4.5 Wireless 6GHz

The Wireless 6GHz radio supports IEEE 802.11ax (Wi-Fi 6E) and IEEE 802.11be (Wi-Fi 7) operation on the U-NII-5 / U-NII-6 / U-NII-7 / U-NII-8 bands. Per Wi-Fi Alliance certification, 6 GHz radios mandate WPA3 (SAE) authentication — WPA-Personal with WPA Version locked to WPA3 — and legacy ciphers (TKIP, WEP) are not available. The IEEE 802.11be (EHT) PHY adds the EHT320 channel bandwidth (320 MHz) on top of EHT20 / EHT40 / EHT80 / EHT160.

To access this page, click **Interface** > **Wireless - 6GHz** .

The 6GHz radio exposes the same configuration leaves as Wireless 2.4GHz and 5GHz — Basic, Advanced, Security, Multiple SSID, Statistics, Access Control, Traffic Control in AP mode; Basic, Advanced, Security, Statistics, Site Survey in Client mode. For per-field descriptions not repeated below, refer to the corresponding Wireless 2.4GHz subsection (Section 3.4.3).

The 6GHz-specific differences are:

- **Channel** — the available channel list is restricted to the U-NII-5/6/7/8 bands and is further filtered by the configured Country code. With Country = US (lab default), channels start from 5 (5.985 GHz) in 20 MHz increments up through channel 213 (7.015 GHz).

- **Channel bandwidth (htmode)** — adds **EHT320** (320 MHz) as a Wi-Fi 7 option, in addition to EHT20 / EHT40 / EHT80 / EHT160.
- **Security Mode** — only WPA-Personal and WPA-Enterprise are available; the WPA Version dropdown is locked to **WPA3** and the cipher to AES (CCMP). WPA2 / WPA2+WPA3 / None cannot be selected on a 6 GHz radio.

3.4.5.1 Basic

To access this page, click **Wireless - 6GHz** > **Basic** .

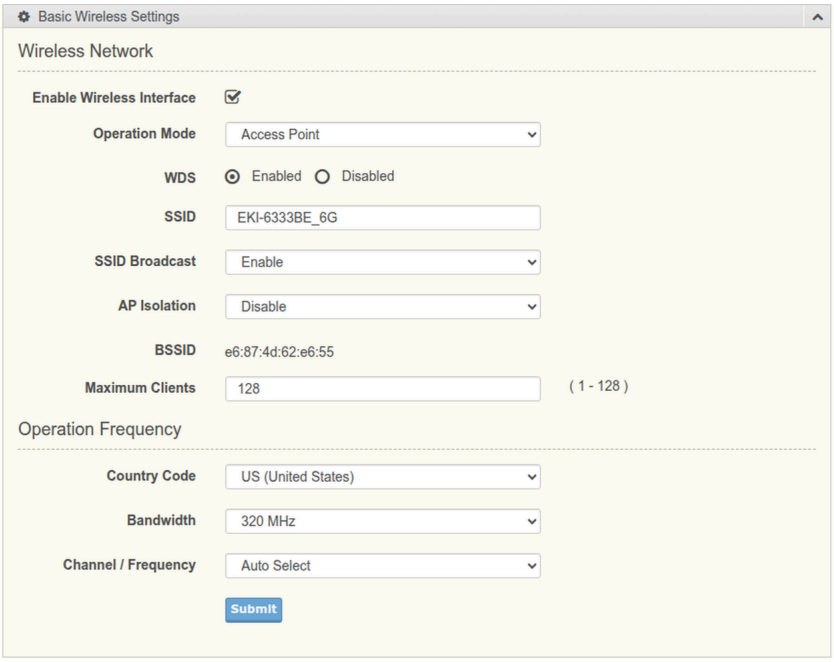


Figure 3.26 Wireless - 6GHz > Basic > Access Point

For per-field descriptions, refer to Section 3.4.3.1. The 6GHz Basic page adds **EHT320** to the Channel bandwidth dropdown and exposes the U-NII-5/6/7/8 channel list described above.

3.4.5.2 Advanced

To access this page, click **Wireless - 6GHz** > **Advanced** .

For per-field descriptions, refer to Section 3.4.3.2.

3.4.5.3 Security

To access this page, click **Wireless - 6GHz** > **Security** .

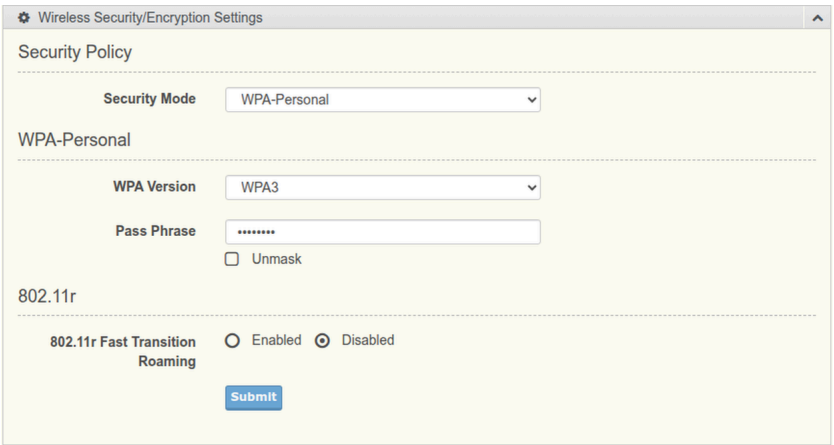


Figure 3.27 Wireless - 6GHz > Security (WPA3 forced)

On 6 GHz radios, Security Mode dropdown options follow the parent radio (None / WPA-Personal / WPA-Enterprise), but the WPA Version dropdown under WPA-Personal is fixed to **WPA3** (no WPA2 fallback). The cipher is automatically set to AES (CCMP). For per-field descriptions of the remaining items (Pass Phrase, 802.11r, RADIUS), refer to Section 3.4.3.3.

3.4.5.4 Multiple SSID

To access this page, click **Wireless - 6GHz** > **Multiple SSID** .

For per-field descriptions, refer to Section 3.4.3.4. WPA3 is mandatory on each additional 6 GHz SSID.

3.4.5.5 Statistics

To access this page, click **Wireless - 6GHz** > **Statistics** .

For per-field descriptions, refer to Section 3.4.3.5.

3.4.5.6 Access Control

To access this page, click **Wireless - 6GHz** > **Access Control** .

For per-field descriptions, refer to Section 3.4.3.6.

3.4.5.7 Traffic Control

To access this page, click **Wireless - 6GHz** > **Traffic Control** .

For per-field descriptions, refer to Section 3.4.3.7.

3.4.6 Wireless MLO

Multi-Link Operation (MLO) is an IEEE 802.11be (Wi-Fi 7) feature that aggregates two or three radios (2.4 GHz, 5 GHz, 6 GHz) into a single STA association. Traffic is scheduled across all active links to increase aggregate throughput and reduce latency, while still supporting non-MLO clients on each individual radio's per-band SSID.

To access this page, click **Interface** > **Wireless - MLO** .

The Wireless - MLO sidebar exposes six leaves: Basic, Advanced, Security, Bandwidth Control, Statistics, and Access Control. Compared with the per-band radios (2.4 GHz, 5 GHz, 6 GHz), MLO replaces the per-SSID **Multiple SSID** page with a single global **Bandwidth Control** page; the MLO sidebar also omits Site Survey and Traffic Control. WPA3 is mandatory on the MLO Security page because 6 GHz is always one of the bonded links.

For per-field descriptions not repeated below, refer to the corresponding Wireless 2.4GHz subsection (Section 3.4.3).

3.4.6.1 Basic

To access this page, click **Wireless - MLO** > **Basic** .

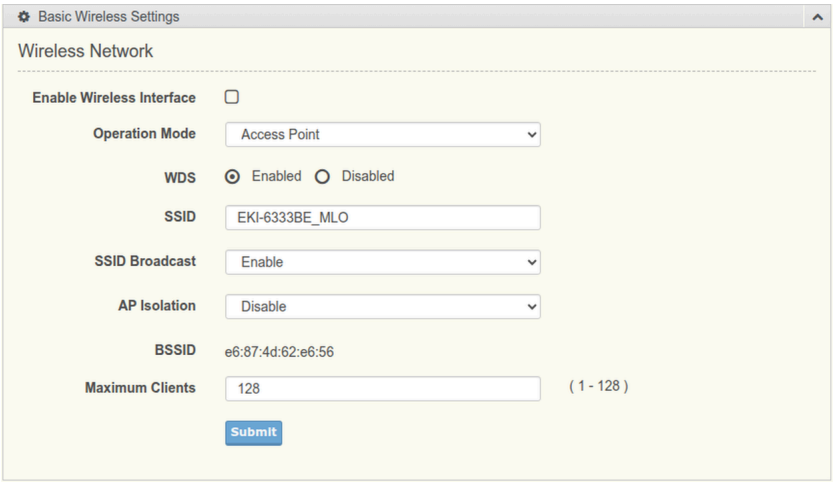


Figure 3.28 Wireless - MLO > Basic

For per-field descriptions, refer to Section 3.4.3.1. Channel and Channel bandwidth are not configurable on the MLO Basic page — those settings are inherited from each bonded radio's own Basic page.

3.4.6.2 Advanced

To access this page, click **Wireless - MLO** > **Advanced** .

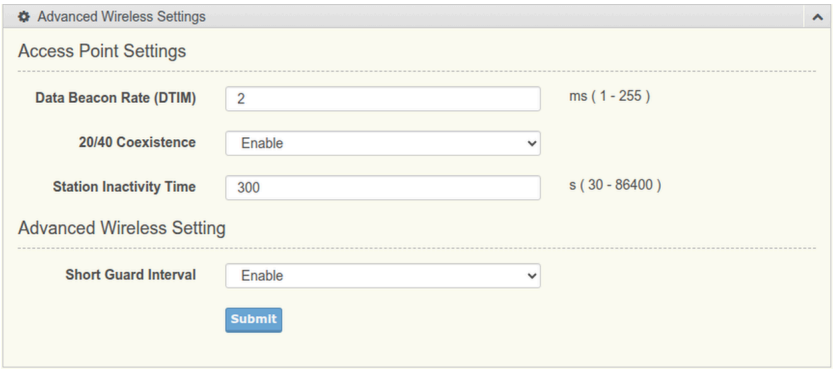


Figure 3.29 Wireless - MLO > Advanced

For per-field descriptions, refer to Section 3.4.3.2.

3.4.6.3 Security

To access this page, click **Wireless - MLO** > **Security** .

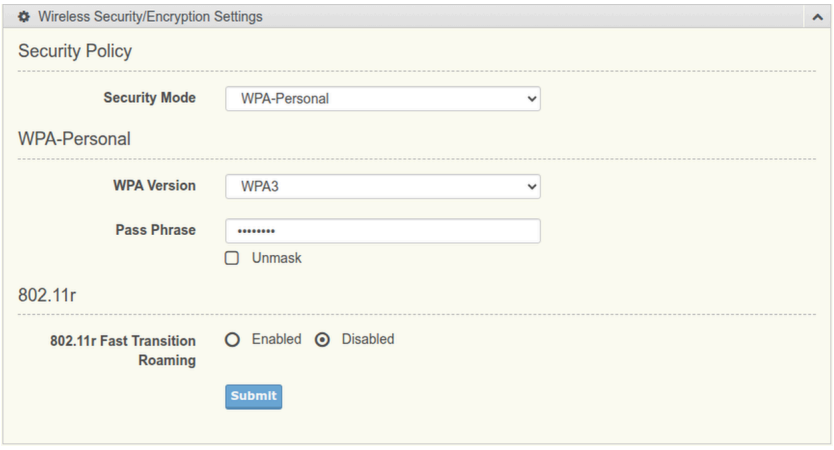


Figure 3.30 Wireless - MLO > Security

For per-field descriptions, refer to Section 3.4.3.3. The MLO Security page locks WPA Version to **WPA3** and cipher to AES (CCMP), reflecting the 6 GHz mandate inherited from the bonded radio set.

3.4.6.4 Bandwidth Control

The Bandwidth Control page sets a single download / upload rate cap that applies to all clients associated to the MLO link, regardless of band. Unlike per-band Traffic Control, MLO Bandwidth Control does not expose per-station rules.

To access this page, click **Wireless - MLO** > **Bandwidth Control** .

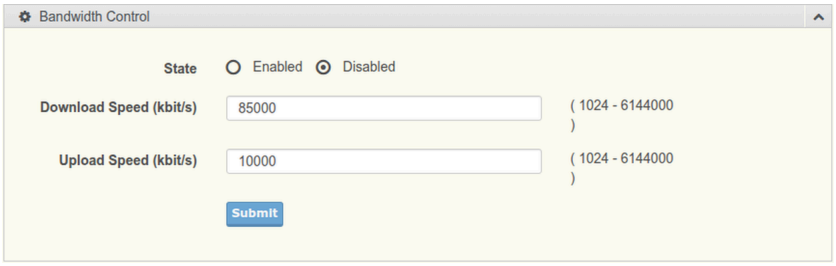


Figure 3.31 Wireless - MLO > Bandwidth Control

The following table describes the items in the previous figure.

Item	Description
State	Click the radio button to enable or disable the bandwidth control function. Default: Disabled.
Download Speed (kbit/s)	Enter the maximum aggregate download speed for the MLO link, in kbit/s. Range 1024 – 6 144 000.
Upload Speed (kbit/s)	Enter the maximum aggregate upload speed for the MLO link, in kbit/s. Range 1024 – 6 144 000.
Submit	Click **Submit** to save the values and update the screen.

3.4.6.5 Statistics

To access this page, click **Wireless - MLO** > **Statistics** .

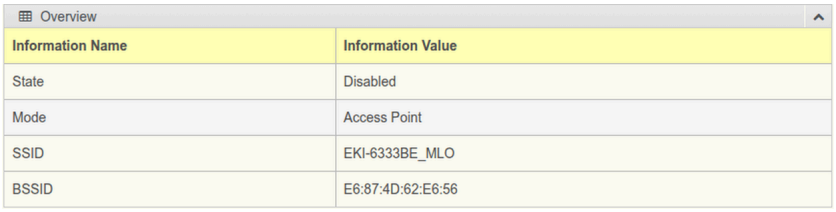


Figure 3.32 Wireless - MLO > Statistics

For per-field descriptions, refer to Section 3.4.3.5.

3.4.6.6 Access Control

To access this page, click **Wireless - MLO** > **Access Control** .



Figure 3.33 Wireless - MLO > Access Control

For per-field descriptions, refer to Section 3.4.3.6.

3.4.7 EasyMesh

EasyMesh allows multiple devices to form a unified wireless mesh network, coordinating Wi-Fi coverage and client roaming across all connected devices without manual configuration on each unit.

Each device in the mesh takes one of two roles. The **Controller** connects to the upstream network, defines the wireless settings for the whole mesh, and manages every Agent that joins it. An **Agent** receives those settings from the Controller and extends wireless coverage to the area around it. A mesh has one Controller and any number of Agents.

The mesh uses two separate SSIDs for two different purposes. The **Backhaul SSID** carries traffic between the mesh devices themselves: it is the wireless link that connects an Agent back to the Controller. It is not intended for user devices.

The **Fronthaul SSID** is the network that laptops, PCs, and phones connect to. Every device in the mesh broadcasts the same Fronthaul SSID, so a client keeps the same network name and password regardless of which device it is connected to, and roams between them automatically.

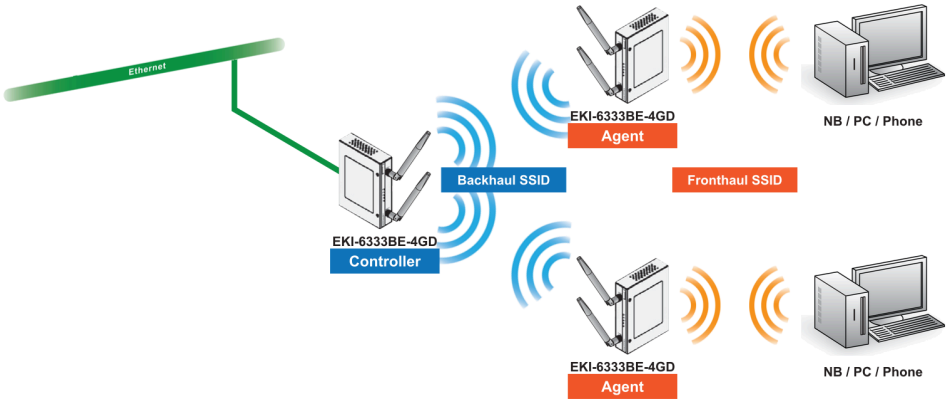


Figure 3.34 EasyMesh Network Topology

Note! *Connect user devices to the Fronthaul SSID. The Backhaul SSID is reserved for the wireless links between mesh devices and should not be used by laptops, PCs, or phones.*

3.4.7.1 Settings

To access this page, click **EasyMesh** > **Settings** .

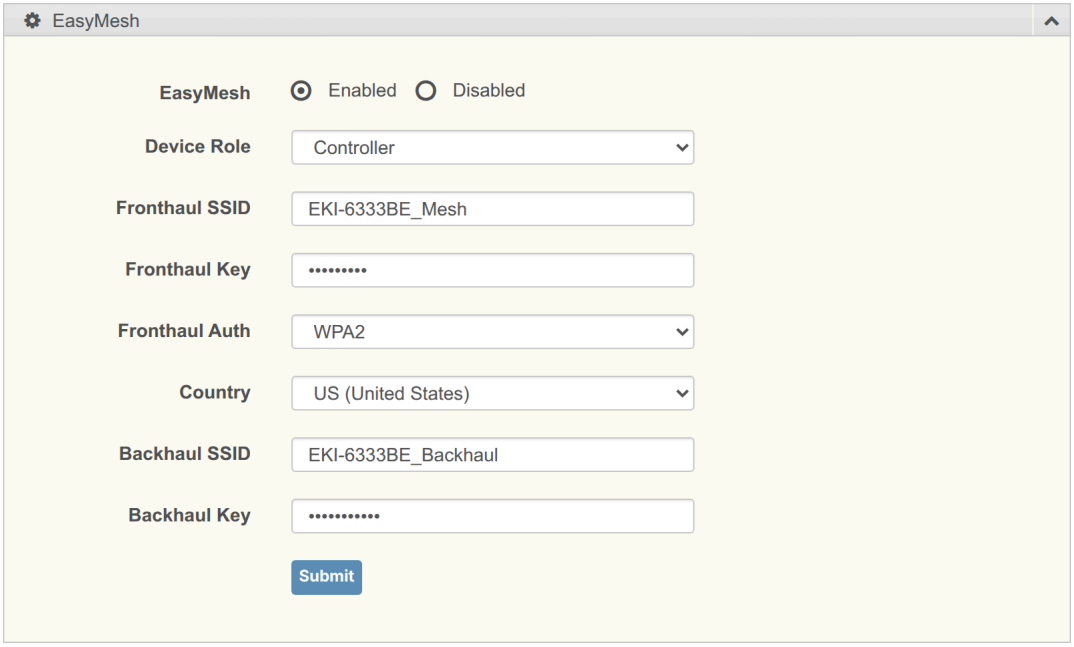


Figure 3.35 EasyMesh > Settings

The following table describes the items in the previous figure.

Item	Description
EasyMesh	Click the radio button to enable or disable the EasyMesh function.
Device Role	Click the drop-down menu to select the device role: **Controller** (coordinates the mesh and manages Agent devices) or **Agent** (joins a mesh managed by a Controller). Only available when EasyMesh is enabled.
Fronthaul SSID	Enter the SSID that laptops, PCs, and phones connect to. Every device in the mesh broadcasts this SSID. Only available when Device Role is set to Controller.
Fronthaul Key	Enter the pre-shared key for the Fronthaul SSID. Only available when Device Role is set to Controller.
Fronthaul Auth	Click the drop-down menu to select the authentication type for the Fronthaul SSID: WPA2 or WPA3. Only available when Device Role is set to Controller.
Country	Click the drop-down menu to select the country/region for the mesh radios. Available channels and transmit power follow the regulatory domain of the selected country.
Backhaul SSID	Enter the SSID used for the wireless link between mesh devices. Do not connect user devices to this SSID.
Backhaul Key	Enter the pre-shared key for the backhaul link.
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** > **Apply Configuration** > **Apply and Reboot** .*

3.4.7.2 Topology

To access this page, click **EasyMesh** > **Topology** .

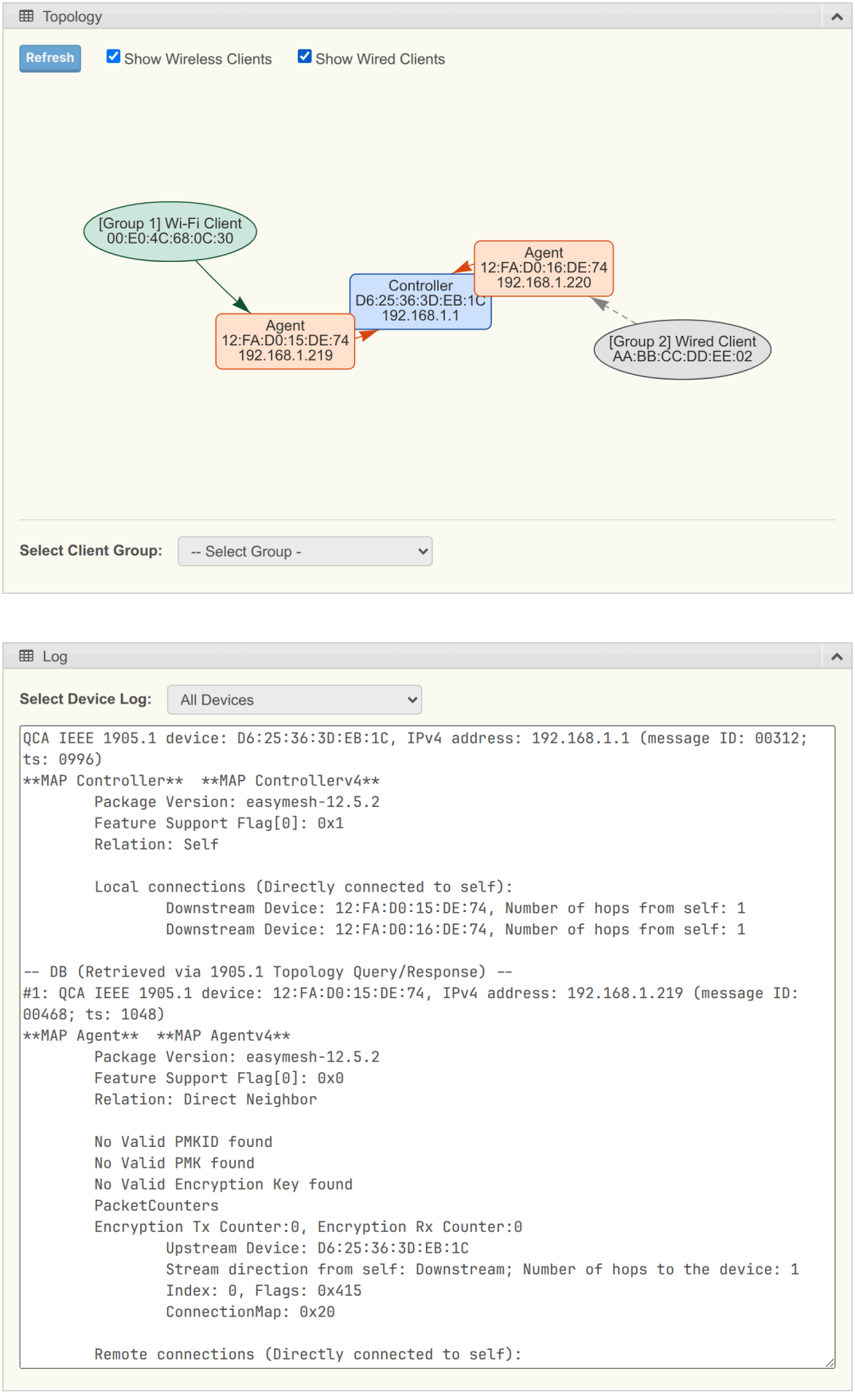


Figure 3.36 EasyMesh > Topology

The following table describes the items in the previous figure.

Item	Description
Topology	
Refresh	Click **Refresh** to redraw the mesh topology diagram with the latest device and client information.
Show Wireless Clients	Click the checkbox to display wireless clients connected to each mesh device in the topology diagram.
Show Wired Clients	Click the checkbox to display wired clients connected to each mesh device in the topology diagram.
Log	
Select Device Log	Click the drop-down menu to select a specific mesh device, or **All Devices**, to display its EasyMesh event log in the text box below.

3.5 Network Settings

3.5.1 Static Route

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

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



Figure 3.37 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, Wireless 5GHz, Wireless 6GHz, or Wireless MLO.
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.

3.5.2 NAT

Network Address Translation (NAT) allows the device to provide an agent function between the public network (Internet) and the private network (local). This allows a single unique IP address to represent a group of connected devices access to the external network.

By the same token, when a packet enters the domain, NAT translates the external (public) unique address into a private local address.

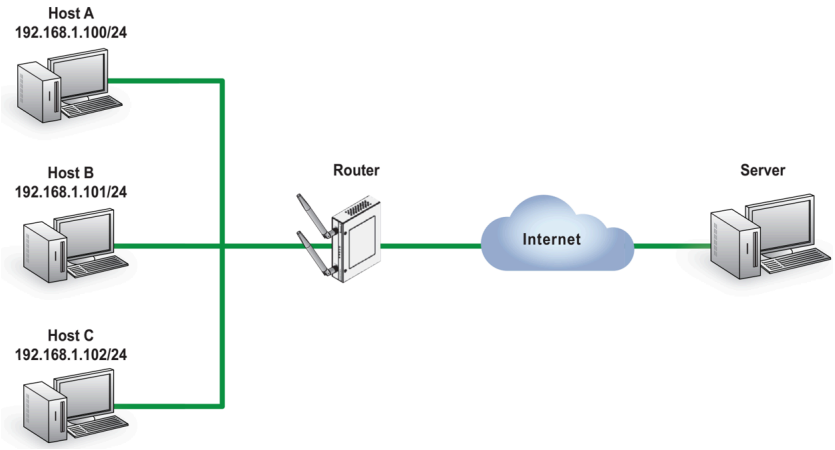


Figure 3.38 NAT Diagram

3.5.3 Forwarding

3.5.3.1 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.

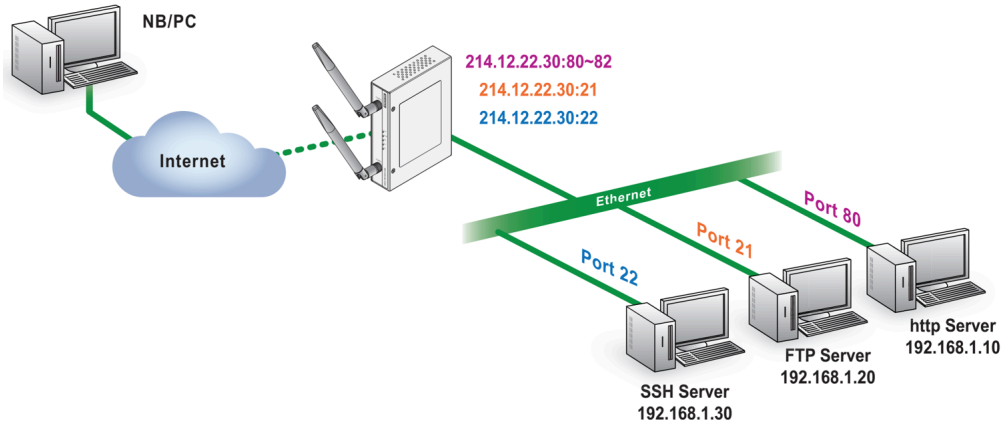


Figure 3.39 Port Forwarding

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

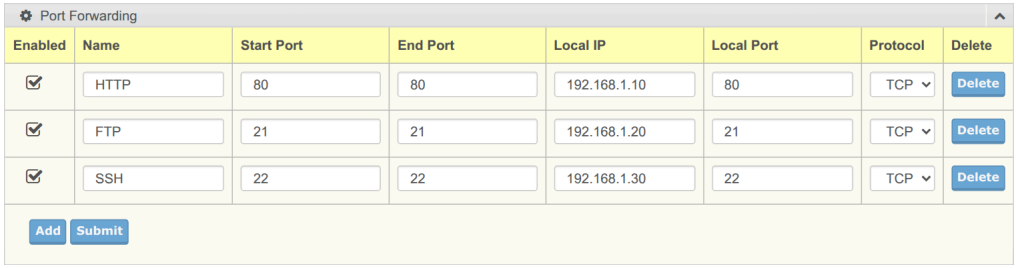


Figure 3.40 Networking > Forwarding > Port Forwarding

The following table describes the items in the previous figure.

Item	Description
Enabled	Tick the checkbox to enable this port forwarding entry.
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.

3.5.3.2 DMZ

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

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

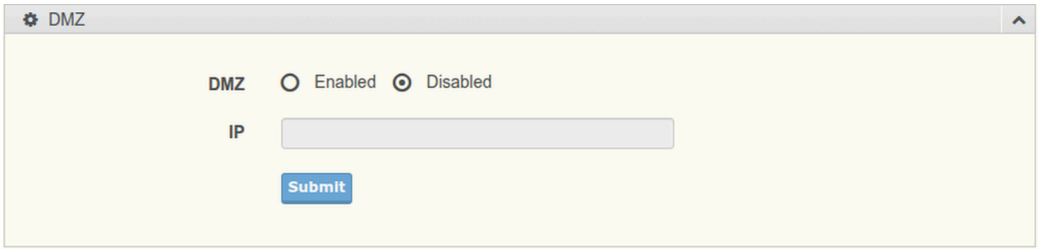


Figure 3.41 Networking > Forwarding > DMZ

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.

3.5.4 Security

3.5.4.1 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 supports Source IP Filtering, Destination IP Filtering, Source Port Filtering, and Destination Port Filtering.

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

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



Figure 3.42 Networking > Security > Filter

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

3.5.4.2 VPN Passthrough

VPN pass-through is a function of the router, which allows the VPN traffic between local PC and remote VPN server. 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** .

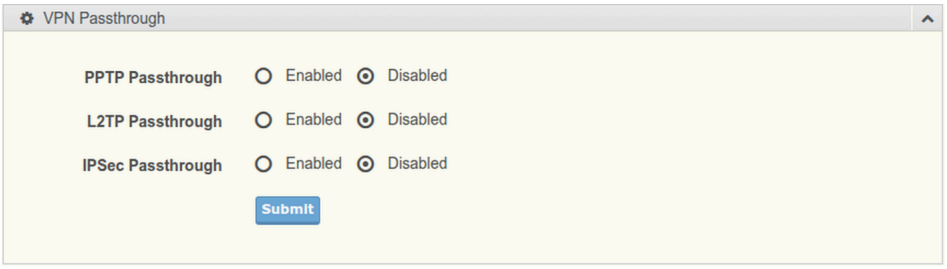


Figure 3.43 Networking > Security > VPN Passthrough

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

Item	Description
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.

3.5.5 IP-QoS

IP-QoS provides per-IP-address rate limiting on traffic forwarded through EKI-6333BE-4GD Series. The feature is split between a global enable / disable switch (Basic) and a rule table that lists each rate-limited IP address (Limit Rate).

To access these pages, click **Networking** > **IP-QoS** .

3.5.5.1 Basic

Enable or disable IP-based QoS rate limiting. When enabled, the rules defined under **Limit Rate** (Section 3.5.5.2) are applied to matched IP addresses; when disabled, all rules are inactive but their entries are preserved for later re-enabling.

To access this page, click **Networking** > **IP-QoS** > **Basic** .

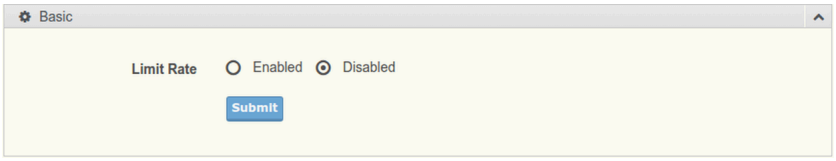


Figure 3.44 Networking > IP-QoS > Basic

The following table describes the items in the previous figure.

Item	Description
Limit Rate	Click the radio button to enable or disable IP-based QoS rate limiting. Default: Disabled.
Submit	Click **Submit** to save the value and update the screen.

3.5.5.2 Limit Rate

Define per-IP rate-limiting rules. Each rule pins a download / upload rate to a specific LAN-side IP address. When the LAN is configured with a static IP, each entry's IP Address must lie on the same subnet as the LAN IP (the WebUI rejects out-of-subnet entries with the alert `IP has to be on the same subnet as the LAN IP.`).

To access this page, click **Networking** > **IP-QoS** > **Limit Rate** .

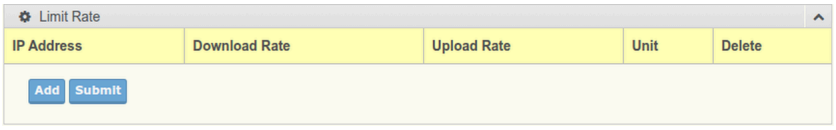


Figure 3.45 Networking > IP-QoS > Limit Rate (empty)

When the table is empty, click **Add** to insert a new row and fill in the IP address and download / upload rate.



Figure 3.46 Networking > IP-QoS > Limit Rate (one entry)

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter the LAN-side IP address whose traffic is rate-limited. Must be on the same subnet as the LAN IP when the LAN is configured with a static address.
Download Rate	Enter the maximum download speed allowed for traffic destined to this IP. Integer value, in the unit selected by the **Unit** column.
Upload Rate	Enter the maximum upload speed allowed for traffic originated from this IP. Integer value, in the unit selected by the **Unit** column.
Unit	Click the drop-down menu to select the rate unit: **Kbit/s** (default) or **Mbit/s**.
Delete	Click **Delete** to remove the entry.
Add	Click **Add** to append a new empty row to the table.
Submit	Click **Submit** to save all rules and update the screen.

3.6 Management

3.6.1 Account Manager

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

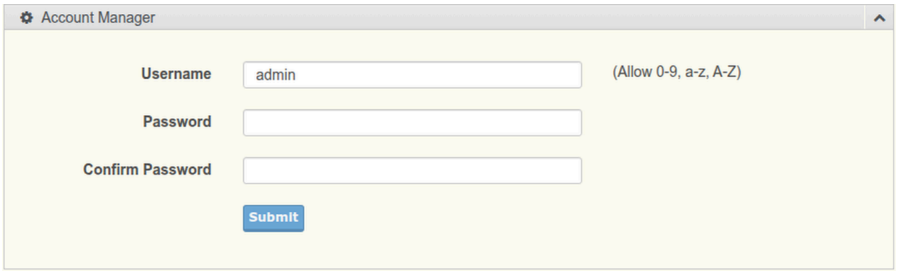


Figure 3.47 Management > Account Manager

The following table describes the items in the previous figure.

Item	Description
Username	Enter the administrator account name. Allowed characters: 0-9, a-z, A-Z. Default: admin.
Password	Enter the text string to define a password for the listed username entry.
Confirm Password	Re-type the text string as identified in the password field to confirm the entry.
Submit	Click **Submit** to save the values and update the screen.

3.6.2 Syslog

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

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

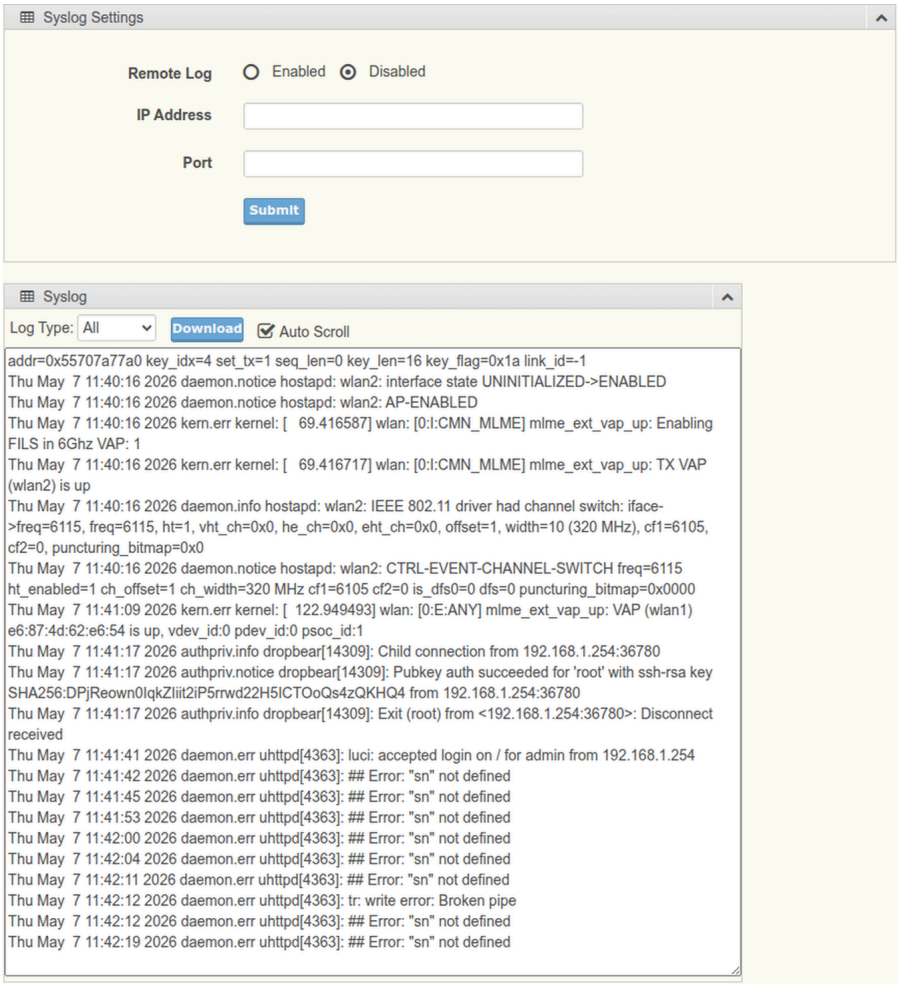


Figure 3.48 Management > Syslog

The following table describes the items in the previous figure.

Item	Description
Remote Log	Click the radio button to enable or disable the remote log function. Enabling the function allows for the saving of log entries on a remote, not local, system.
IP Address	Enter the static address of the remote system used for storing logging information.
Port	Enter the port number of the define static address used for storing logging information.
Submit	Click **Submit** to save the values and update the screen.
Download	Click **Download** to download the log file.
Auto Scroll	Click the option to allow for auto scrolling when the log entries has extended below the page line.

3.6.3 NTP / Time

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

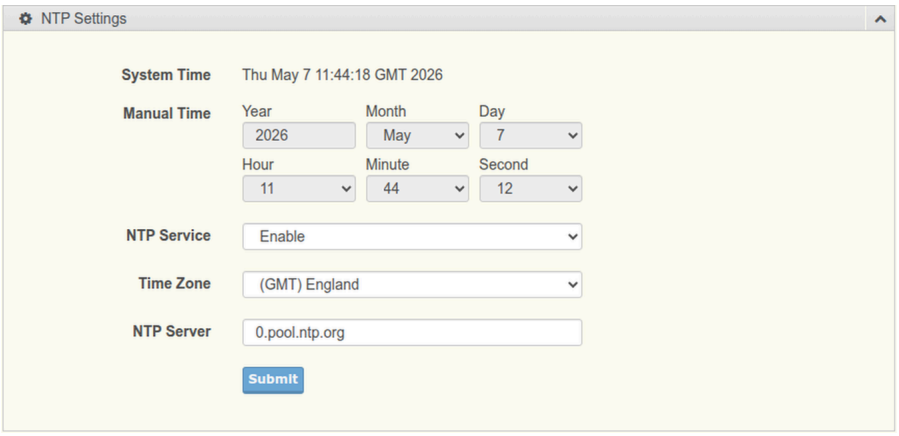


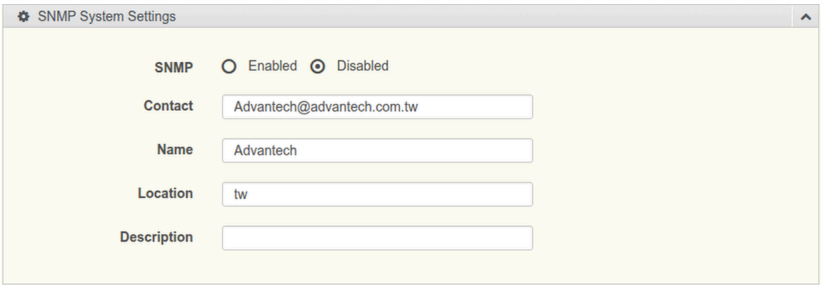
Figure 3.49 Management > NTP / Time

The following table describes the items in the previous figure.

Item	Description
System Time	Displays the current system time settings.
Manual Time	To enable manual configuration, NTP Service option must first be disabled. Manually enter the Year, Month, Day, Hour, Minute, and Second settings to define the system time.
NTP Service	Click the drop-down menu to enable or disable the NTP server. By disabling this function, the Manual Time setting can be configured.
Time Zone	Click the drop-down menu to select a system time zone.
NTP Server	Enter the address of the SNTP server.
Submit	Click **Submit** to save the values and update the screen.

3.6.4 SNMP

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



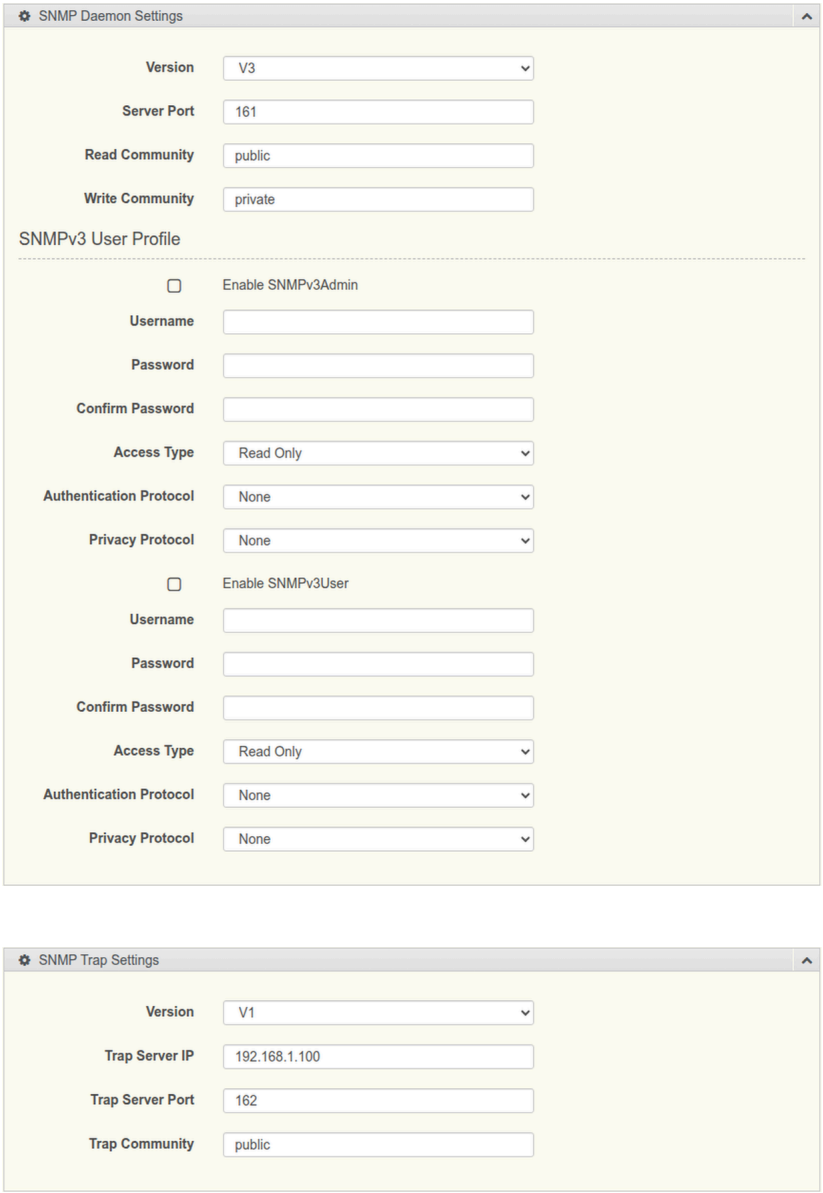


Figure 3.50 Management > SNMP

The following table describes the items in the previous figure.

Item	Description
SNMP System Settings	
SNMP	Click the radio button to enable or disable the Simple Network Management Protocol (SNMP) function used to monitor network devices.
Contact	Enter the contact route in an Email format for use during an SNMP event.
Name	Enter the text string describing the contact entry.
Location	Enter the text string describing the region/location of the contact entry.
Description	Enter a descriptive remark to better identify the contact entry.
SNMP Daemon Settings	
Version	Click the drop-down menu to select the SNMP version (V1, V2c, V3).
Server Port	Enter the port to access on the specified server. Default: 161.

Item	Description
Read Community	Enter the setting to define the level of read access for the defined user, options: private, public (default).
Write Community	Enter the setting to define the level of write access for the defined user, options: private (default), public.
SNMPv3 User Profile	
Enable SNMPv3Admin	Tick the checkbox to activate the SNMPv3 admin account.
Username	Enter the SNMPv3 admin account name.
Password	Enter the password for the SNMPv3 admin account.
Confirm Password	Re-enter the password to confirm.
Access Type	Click the drop-down menu to select the access level: Read Only or Read/Write.
Authentication Protocol	Click the drop-down menu to select the authentication algorithm: None, MD5, or SHA.
Privacy Protocol	Click the drop-down menu to select the privacy/encryption algorithm: None, DES, or AES.
Enable SNMPv3User	Tick the checkbox to activate the SNMPv3 user account.
Username	Enter the SNMPv3 user account name.
Password	Enter the password for the SNMPv3 user account.
Confirm Password	Re-enter the password to confirm.
Access Type	Click the drop-down menu to select the access level: Read Only or Read/Write.
Authentication Protocol	Click the drop-down menu to select the authentication algorithm: None, MD5, or SHA.
Privacy Protocol	Click the drop-down menu to select the privacy/encryption algorithm: None, DES, or AES.
SNMP Trap Settings	
Version	Click the drop-down menu to select the SNMP trap version (V1, V2c, V3).
Trap Server IP	Enter the IP address of the trap server.
Trap Server Port	Enter the port number used by the trap server. Default: 162.
Trap Community	Enter the setting to define the level of access for the defined user, options: private, public.
Submit	Click **Submit** to save the values and update the screen.

3.6.5 Remote Services

To access this page, click **Management** > **Remote Services** .

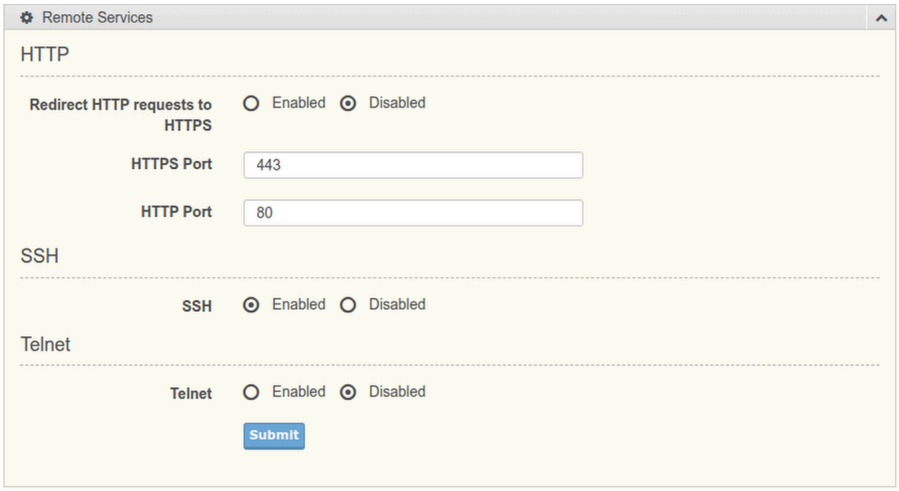


Figure 3.51 Management > Remote Services

The following table describes the items in the previous figure.

Item	Description
HTTP	
Redirect HTTP requests to HTTPS	Click the drop-down menu to enable or disable the function. By default the function is disabled. When enabled, a NAT setting and Open Ports can be setup to direct connection requests to an internal server.
HTTPS Port	Enter the port to forward HTTPS traffic, default: 443.
HTTP Port	Enter the port to forward HTTP traffic, default: 80.
SSH	
SSH	Click the radio button to enable or disable access to SSH function.
Telnet	
Telnet	Click the radio button to enable or disable access to the Telnet function.
Submit	Click **Submit** to save the values and update the screen.

3.6.6 Configuration Manager

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

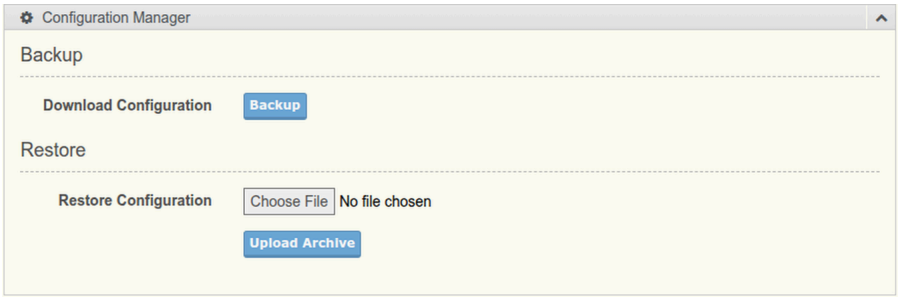


Figure 3.52 Management > Configuration Manager

The following table describes the items in the previous figure.

Item	Description
Backup	
Download Configuration	Click **Backup** to export the current device settings to a local archive file.
Restore	
Restore Configuration	Click **Upload Archive** to select a previously saved configuration file and apply it.

3.6.7 Firmware Upgrade

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

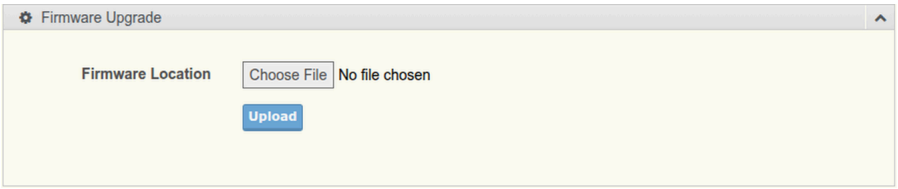


Figure 3.53 Management > Firmware Upgrade

The following table describes the items in the previous figure.

Item	Description
Firmware Location	Click **Choose File** to browse for the firmware image file, then click **Upload** to begin the upgrade.

3.6.8 Reset System

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



Figure 3.54 Management > Reset System

The following table describes the items in the previous figure.

Item	Description
Reset to Defaults	Click **Reset** the device, any changes to settings will be lost unless the Apply Configuration function is executed prior to resetting.

3.6.9 Apply Configuration

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

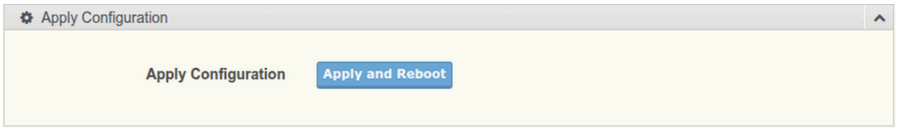


Figure 3.55 Management > Apply Configuration

The following table describes the items in the previous figure.

Item	Description
Apply and Reboot	Click **Apply and Reboot** to save the new configuration settings and reboot the device to permanently save the new settings.

3.6.10 Reboot Device

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



Figure 3.56 Management > Reboot Device

The following table describes the items in the previous figure.

Item	Description
Reboot	Click **Reboot** to reboot the device. Any configuration changes you have made since the last time you issued a save will be lost.

3.7 Tools

3.7.1 Diagnostics

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

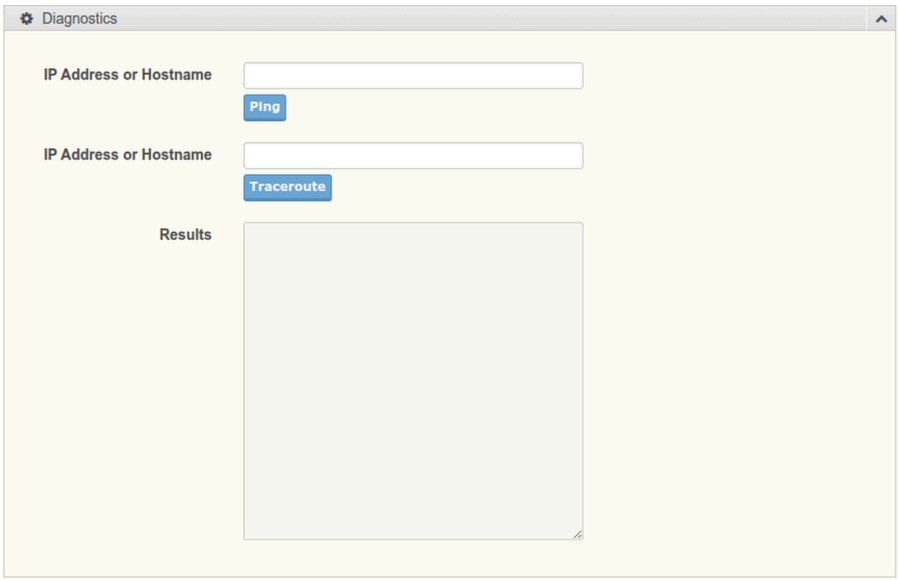


Figure 3.57 Tools > Diagnostics

The following table describes the items in the previous figure.

Item	Description
Ping > **IP Address or Hostname**	Enter the IP address or host name of the station to ping. The value is not retained across a power cycle. Host names are composed of labels concatenated with periods; each label must be 1–63 characters long, with a 64-character maximum overall.
Ping	Click **Ping** to display the ping result for the target.

Item	Description
Traceroute > **IP Address or Hostname**	Enter the IP address or host name of the destination to trace. Same input rules as the Ping field above.
Traceroute	Click **Traceroute** to track the pathway taken by a packet from this device to the destination.
Results	Displays the output of the Ping or Traceroute function.

ADVANTECH

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. 2026