User Manual

EKI-6333AC-2GD Series

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

ADVANTECH

Enabling an Intelligent Planet

Copyright

The documentation and the software included with this product are copyrighted 2022 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 March 2022

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.

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 recommenEKI-6333AC-2GD Seriesded 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-6333AC-2GD Wi-Fi AP
- 2 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 7
2.1.3 Bottom View 7
2.1.4 Left View 8
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 21
3.2 Overview 22
3.3 Address Resolution Protocol 23
3.4 Interface Settings 23
3.4.1 LAN 23
3.4.2 WAN 24
3.4.3 Wireless 2.4GHz 27
3.4.4 Wireless 5GHz 45
3.4.5 Wireless Redundant 45
3.5 Network Settings 50
3.5.1 Static Route 50
3.5.2 NAT 51
3.5.3 Forwarding 51
3.5.4 Security 53
3.6 Management 55
3.6.1 Password Manager 55
3.6.2 Syslog 55
3.6.3 NTP / Time 56
3.6.4 SNMP 57
3.6.5 Remote Services 58
3.6.6 Configuration Manager 59
3.6.7 Firmware Upgrade 59
3.6.8 Reset System 59
3.6.9 Apply Configuration 60
3.6.10 Reboot Device 60
3.7 Tools 61
3.7.1 Diagnostics 61

List of Figures

Figure 1.1 Dimensions 4
Figure 2.1 Front View 6
Figure 2.2 Rear View 7
Figure 2.3 Bottom View as Seen Without a Port Cover 7
Figure 2.4 Left View 8
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-6333AC-2GD Series 15
Figure 2.16 Grounding Connection 17
Figure 2.17 Terminal Receptor: Power Input Contacts 18
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 19
Figure 3.1 Login Screen 21
Figure 3.2 Administration > HTTP 21
Figure 3.3 Status > Overview, System Info and LAN Interface 22
Figure 3.4 Status > Overview, WAN Interface, DHCP Leases, & System Status 22
Figure 3.5 Status > ARP 23
Figure 3.6 **Interface > LAN 23**
Figure 3.7 Interface > WAN > Network Mode 24
Figure 3.8 Interface > WAN > Network Mode > Static 25
Figure 3.9 Interface > WAN > Network Mode > DHCP 25
Figure 3.10 Interface > WAN > Network Mode > PPPoE 26
Figure 3.11 Wireless WAN Topology 26
Figure 3.12 Wireless - 2.4GHz > Basic > Access Point 27
Figure 3.13 Wireless - 2.4GHz > Basic > Client 29
Figure 3.14 Wireless - 2.4GHz > Basic > Bridged Repeater 30
Figure 3.15 Bridged Repeater Mode Topology 31
Figure 3.16 Enabling Bridged Repeater Mode 32
Figure 3.17 Completed Bridged Repeater Mode Setting 32
Figure 3.18 Wireless - 2.4GHz > Advanced 33
Figure 3.19 Wireless - 2.4GHz > Advanced 34
Figure 3.20 Wireless - 2.4GHz > Security 35
Figure 3.21 Wireless - 2.4GHz > Security 36
Figure 3.22 Wireless Settings > Security 36
Figure 3.23 **Security Mode > WEP 37**
Figure 3.24 **Security Mode > WPA-Personal 38**
Figure 3.25 **Security Mode > WPA/WPA2-Enterprise 39**
Figure 3.26 Wireless - 2.4GHz > Multiple SSID 40
Figure 3.27 Wireless - 2.4GHz > Statistics 41
Figure 3.28 Wireless - 2.4GHz > Access Control 42
Figure 3.29 Wireless - 2.4GHz > Site Survey 42
Figure 3.30 Wireless VLAN ID Data Flow Diagram 43
Figure 3.31 Wireless - 2.4GHz > VLAN 43
Figure 3.32 Wireless - 2.4GHz > Traffic Control 44
Figure 3.33 Wireless - 2.4GHz > Log 44
Figure 3.34 Interface > Wireless Redundant > Redundant Status 45
Figure 3.35 Wireless Redundancy Enabled 46

Figure 3.36 Interface > Wireless Redundant > Role Exchange Settings 46
Figure 3.37 Wireless RSSI Detection 48
Figure 3.38 Wireless PING Detection 48
Figure 3.39 Interface > Wireless Redundant > Slave Settings 49
Figure 3.40 Wireless Redundant Auto Selection 49
Figure 3.41 Wireless Redundant Topology 50
Figure 3.42 Networking > **Static Route** **50**
Figure 3.43 NAT Diagram 51
Figure 3.44 Port Forwarding 51
Figure 3.45 Networking > **Forwarding** > Port **Forwarding** **52**
Figure 3.46 Networking > **Forwarding** > DMZ 53
Figure 3.47 Networking > **Security** > Filter 53
Figure 3.48 Networking > **Security** > VPN Passthrough 54
Figure 3.49 Management > **Password Manager** **55**
Figure 3.50 Management > **Syslog** **55**
Figure 3.51 Management > **NTP / Time** **56**
Figure 3.52 **Management** > **SNMP** **57**
Figure 3.53 **Management** > **Remote Services** **58**
Figure 3.54 **Management** > Configuration **Manager** **59**
Figure 3.55 **Management** > Firmware Upgrade 59
Figure 3.56 **Management** > **Apply Configuration** **59**
Figure 3.57 **Management** > **Apply Configuration** **60**
Figure 3.58 **Management** > **Reboot Device** **60**
Figure 3.59 **Tools** > Diagnostics 61

Chapter 1

Introduction

1.1 Overview

The EKI-6333AC-2GD Series is a feature rich wireless AP with din-rail type design which provides a reliable wireless connectivity for industrial environments.

With the support of STP, WMM and IGMP snooping protocols, EKI-6333AC-2GD improves the reliability of wireless connectivity, especially in applications requiring high reliability and throughput data transmission. To secure the wireless connection, EKI-6333AC-2GD implements the latest encryption technologies, including WPA2/ WPA/802.1x for powerful security authentication.

1.2 Device Features

- Support 802.11 a/b/g/n/ac MIMO 2T2R
- WLAN transmission rate up to 867 Mbps
- Supports secure access with WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise
- Provides Web-based configuration
- Support Dual band 2.4 GHz / 5 GHz Concurrent

1.3 Specifications

Specifications	Description	
Interface	I/O Port	2 x RJ45
Physical	Enclosure	Metal shell with solid mounting kits
	Mounting	DIN-rail, Wall
	Dimensions (W x H x D)	30 x 140 x 111.3 mm (1.18" x 5.51" x 4.38")
	Weight	560g
	IP Rating	IP30
LED Display	System LED	System: Power WLAN: Link/Active LAN: Link/Active
	Reboot Trigger	Built-in WDT (watchdog timer)
Environment	Operating Temperature	-20 ~ 70 °C (-4~158°F)
	Storage Temperature	-30 ~ 80°C (-22 ~ 176°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
	Speed	5GHz:867Mbps, 2.4GHz:300Mbps (Max)
	Network Mode	Infrastructure
	Free Space Range	Open space 100 m
	Antenna	2 x reverse SMA connectors Default external 2 Omni antenna
	Wireless Security	WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise
Ethernet Communications	Compatibility	IEEE 802.3
	Speed	10/100/1000 Mbps
	Port Connector	2 x 8-pin RJ45
	Protection	Built-in 1.5 KV magnetic isolation
Power	Consumption	17W
	Input	12 ~ 48 VDC
	Connector	Terminal block
Software	Management	Telnet, FTP, SNMP, Web UI, SSH
	Wireless	Radio on/off, WMM, Output Power Control, Beacon Interval, RTS/ CTS threshold, DTIM Interval
	Operation Modes	AP, Client, Bridged Repeater Mode
	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, FTP Server, QoS
Regulatory Approvals	EMC	CE, FCC Part 15 Subpart B (Class B)

1.4 Dimensions

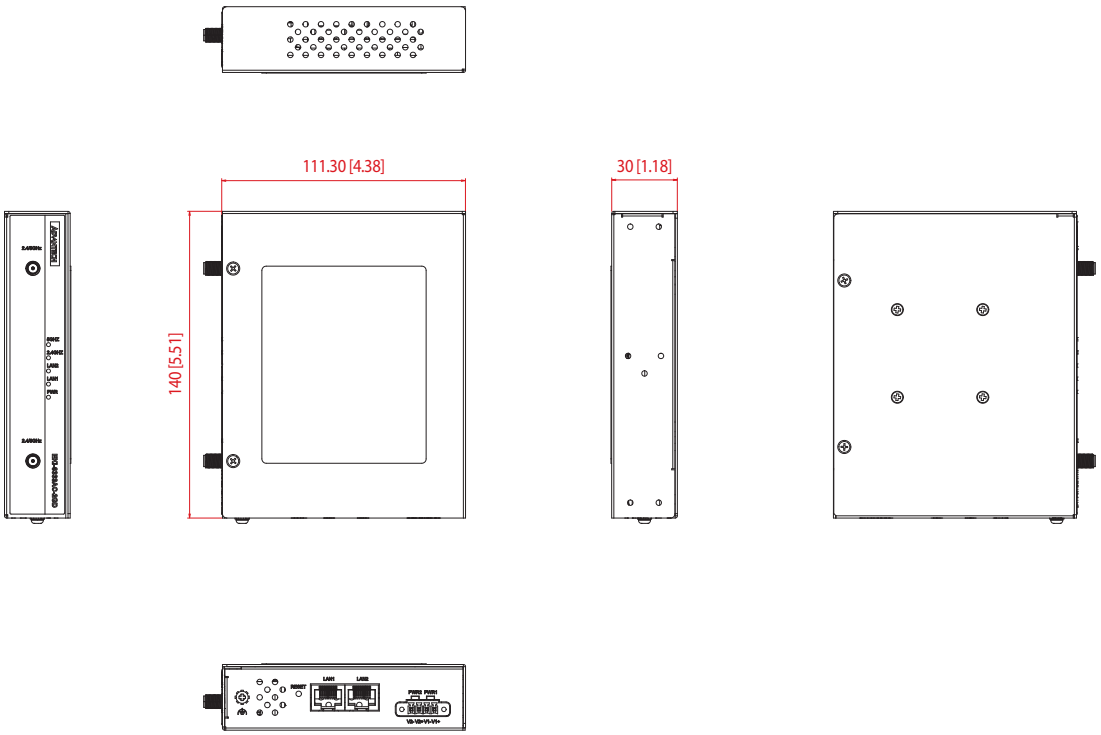


Figure 1.1 Dimensions

Chapter 2

Getting Started

2.1 Hardware

2.1.1 Front View

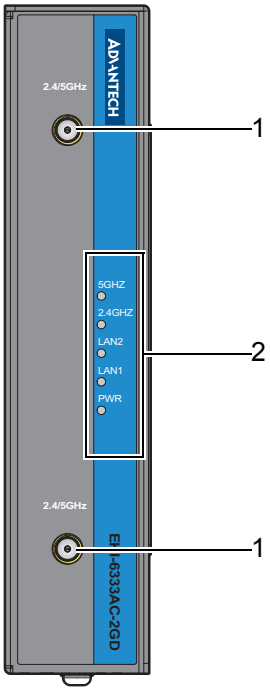


Figure 2.1 Front View

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

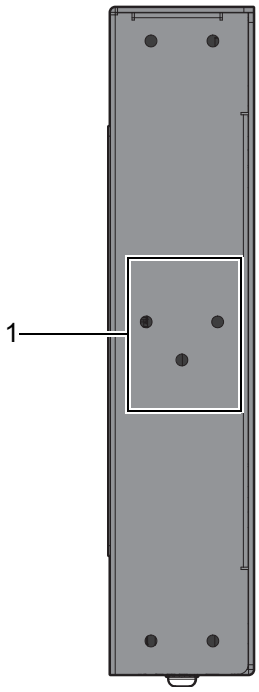


Figure 2.2 Rear View

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

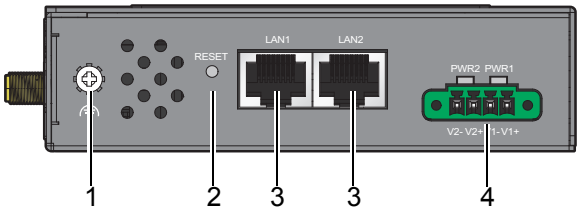


Figure 2.3 Bottom View as Seen Without a Port Cover

No.	Item	Description
1.	GND	Grounding connector
2.	Reset button	Button allows for system soft reset or factory default reset
3.	ETH port	LAN RJ45 port
4.	Terminal block	Connect cabling for power

2.1.4 Left View

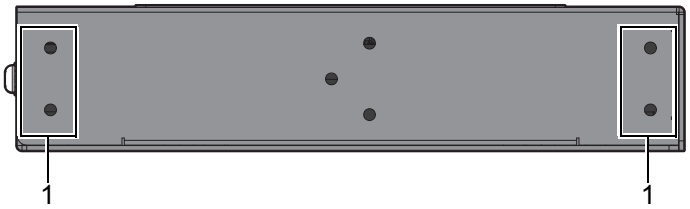


Figure 2.4 Left View

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

2.1.5 LED Indicators

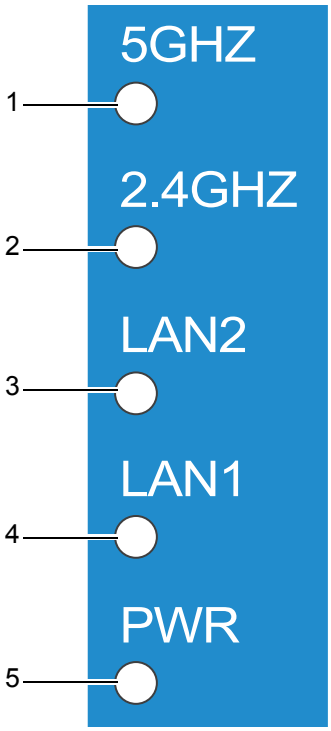


Figure 2.5 System LED Panel

No.	LED Name	LED Color	Description
1.	WLAN (5 GHz)	Green on	Wireless function is active
		Green blinking	Wireless port is transmitting or receiving data
2.	WLAN (2.4 GHz)	Green on	Wireless function is active
		Green blinking	Wireless port is transmitting or receiving data
3.	Ethernet (LAN 2)	Green on	10/100/1000Mbps Ethernet connection
		Green blinking	Ethernet port is transmitting or receiving data
4.	Ethernet (LAN 1)	Green on	10/100/1000Mbps Ethernet connection
		Green blinking	Ethernet port is transmitting or receiving data
5.	PWR	Amber on	Power is on
		Amber blinking	Boot state, firmware update
		Off	Power is off or power error condition exists

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.

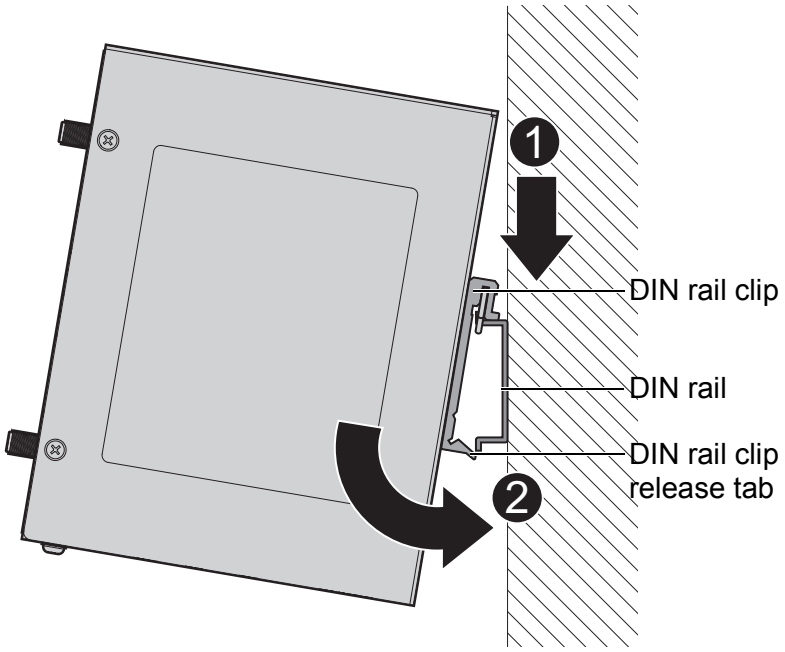


Figure 2.6 Installing the DIN-Rail Mounting Kit

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

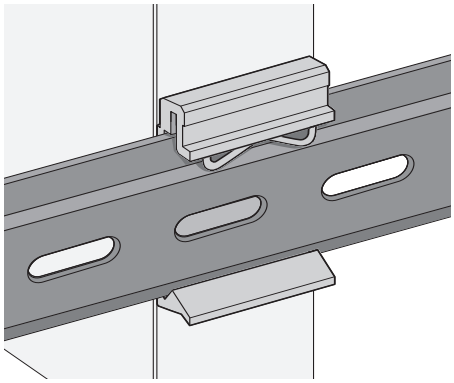


Figure 2.7 Correctly Installed DIN Rail Kit

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.

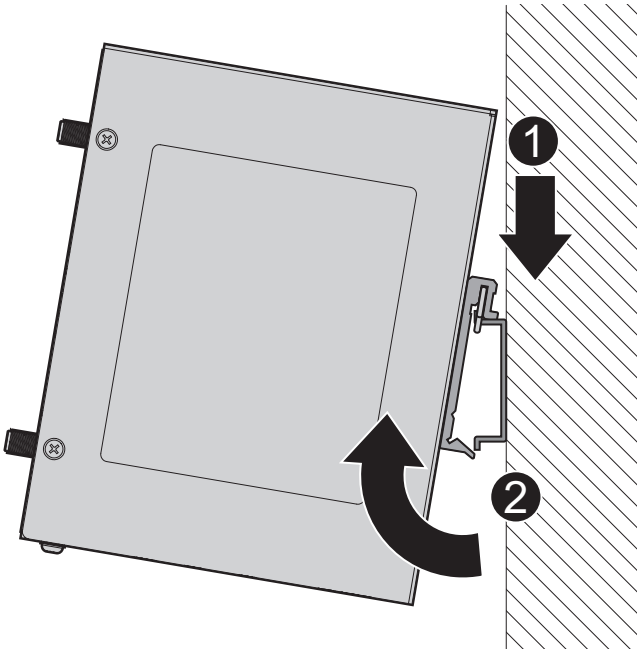


Figure 2.8 Removing the DIN-Rail

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.

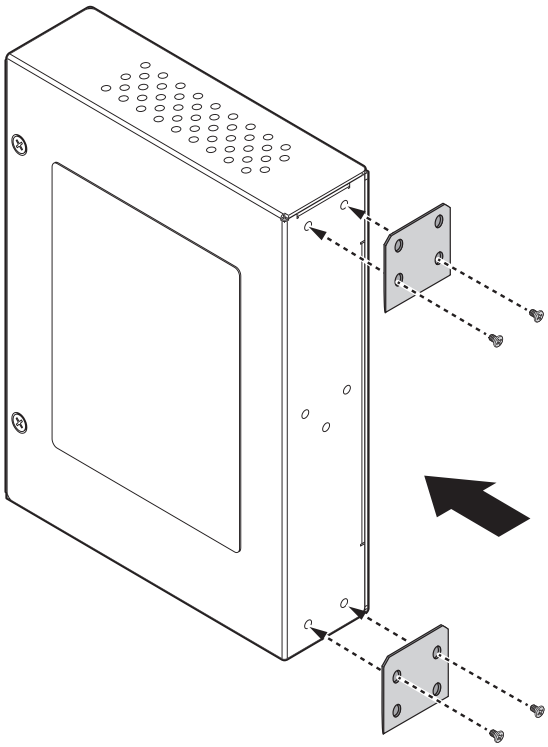


Figure 2.9 Installing Wall Mount Plates

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.

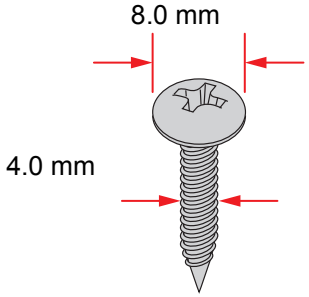


Figure 2.10 Wall Mounting Screw Dimensions

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.

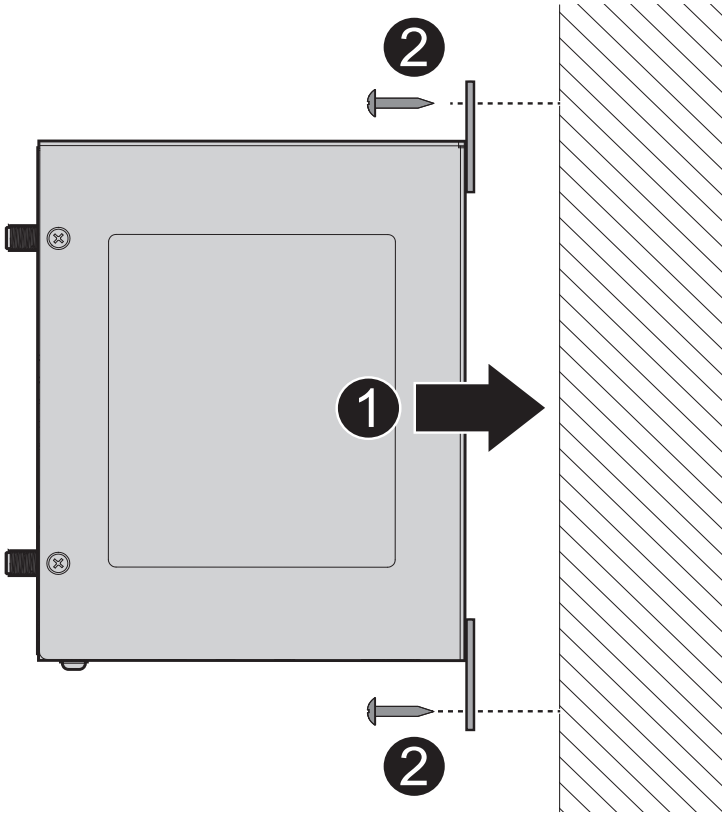


Figure 2.11 Wall Mount Installation

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.

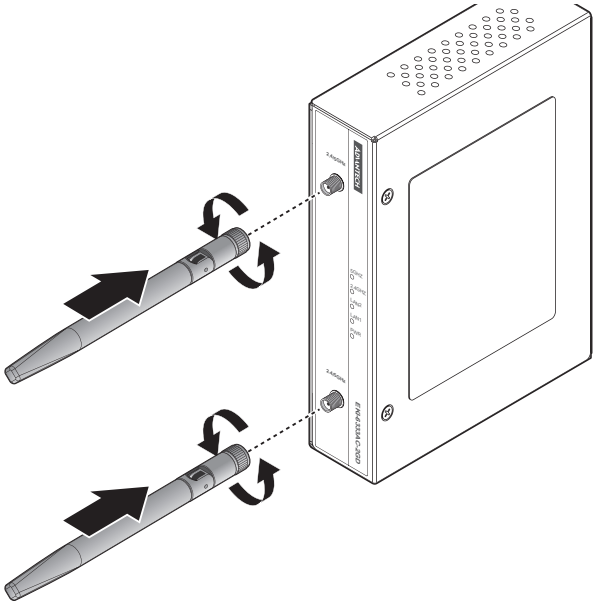


Figure 2.12 Installing the Antenna

2. Position the antenna for optimal signal strength.

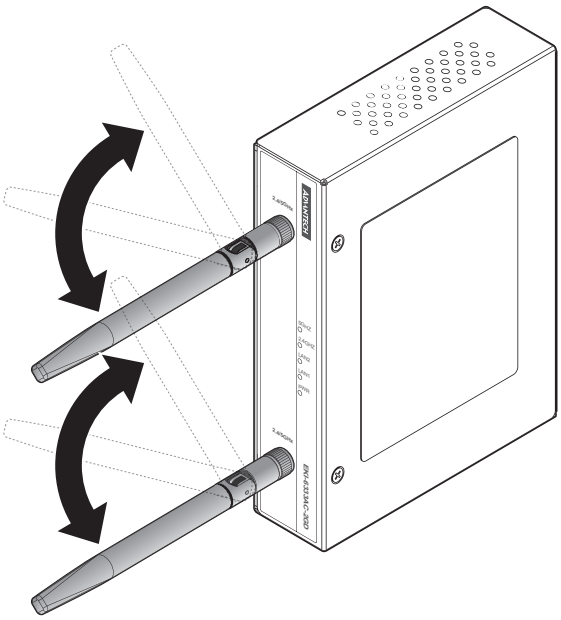


Figure 2.13 Positioning the Antenna

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

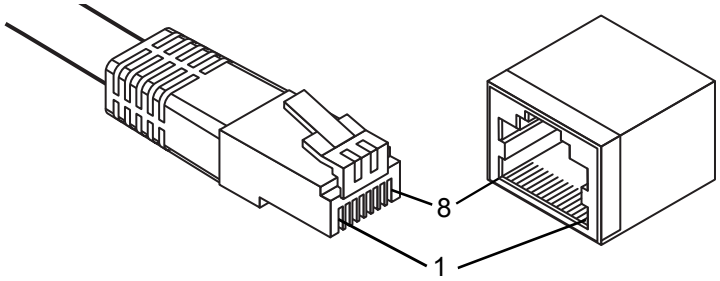


Figure 2.14 Ethernet Plug & Connector Pin Position

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-6333AC-2GD Series support 12 to 48 V_{DC}. Dual power inputs are supported and allow you to connect a backup power source.

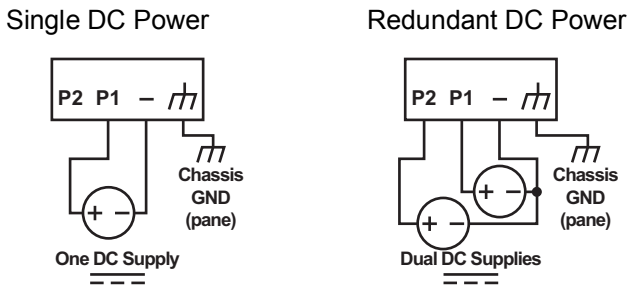


Figure 2.15 Power Wiring for EKI-6333AC-2GD Series

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.

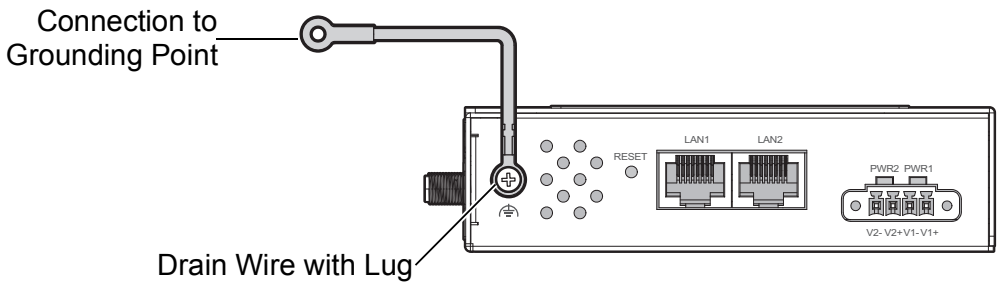


Figure 2.16 Grounding Connection

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.

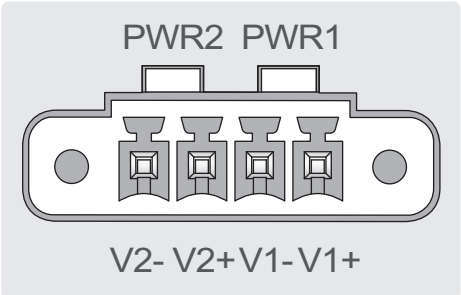


Figure 2.17 Terminal Receptor: Power Input Contacts

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.

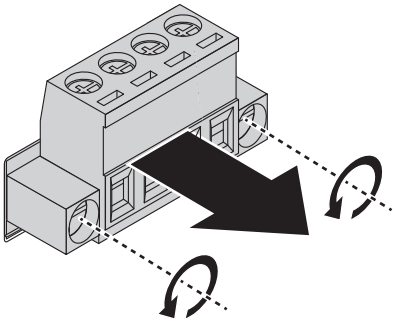


Figure 2.18 Removing a Terminal Block

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.

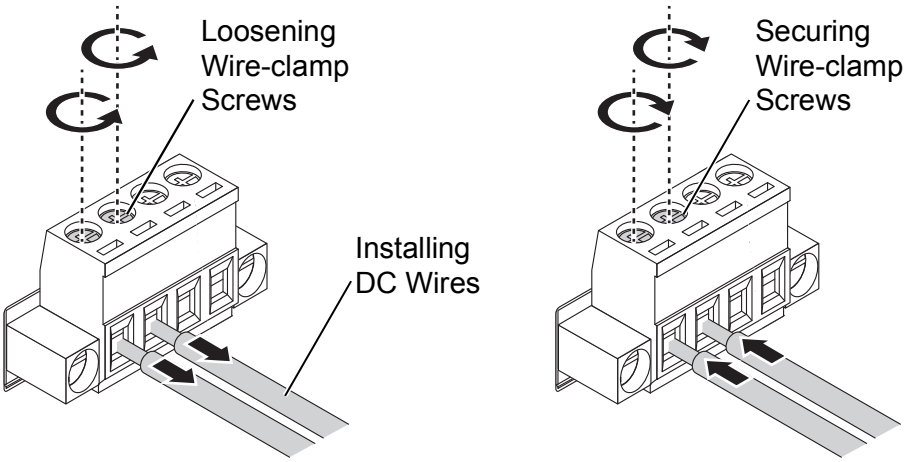


Figure 2.19 Installing DC Wires in a Terminal Block

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.

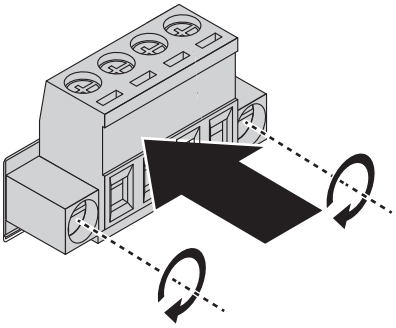


Figure 2.20 Securing a Terminal Block to a Receptor

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 “Connecting Hardware” on page 9. 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.

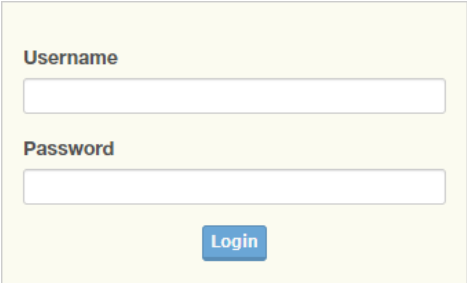


Figure 3.1 Login Screen

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

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 “Log In” on page 21.
2. Navigate to **Home** > **Management** > **Password Manager**. The Password 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.

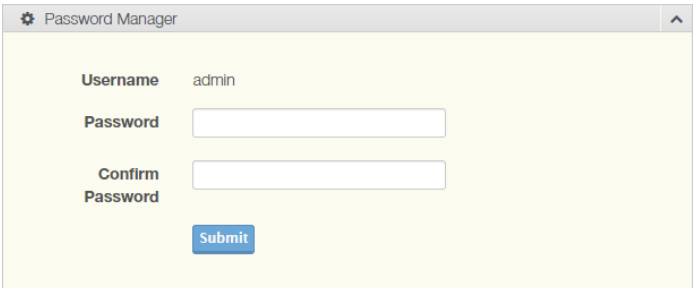


Figure 3.2 Administration > HTTP

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	1.2.4
Local Hostname	Advantech
System Time	Mon Jun 21 08:02:10 2021
System Up Time	0 day 0 hr 2 min 32 sec
Model Name	Advantech EKI-6333AC-2G
Serial Number	IAC2438545

LAN Interface

Information Name	Information Value
LAN Status	**Address:** 192.168.1.165 **Netmask:** 255.255.255.0 **RX:** 81.59 KB (752 Pkts.) **TX:** 1.32 MB (965 Pkts.) **MAC-Address:** 74:FE:48:46:54:68
Wireless - 2.4GHz	**Mode:** Access Point | **SSID:** EKI-6333AC-2G-2.4G **BSSID:** 74:FE:48:46:54:6A | **Encryption:** mixed WPA/WPA2 PSK (TKIP, CCMP) **Channel:** 8 (2.447 GHz) | **Tx-Power:** 30 dBm **Country:** TW
Wireless - 5GHz	**Mode:** Access Point | **SSID:** EKI-6333AC-2G-5G **BSSID:** 74:FE:48:46:54:6B | **Encryption:** mixed WPA/WPA2 PSK (TKIP, CCMP) **Channel:** 44 (5.220 GHz) | **Tx-Power:** 23 dBm **Country:** TW

Figure 3.3 Status > Overview, System Info and LAN Interface

WAN Interface

Information Name	Information Value
WAN Status	*Not connected*

DHCP Leases

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

System Status

Information Name	Information Value
Memory Utilization	84%
CPU Utilization	3%

Figure 3.4 Status > Overview, WAN Interface, DHCP Leases, & System Status

Item	Description
System Info	
Firmware Version	Display the current firmware version of the device.
Local Hostname	Display the current local hostname of the device.
System Time	Displays the current date of the device.
System Up Time	Displays the time since the last device reboot.
Model Name	Displays the model name of the device.
LAN Interface	
LAN Status	Displays the current LAN and MAC settings, TX packets/bytes, and RX packets/bytes.
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 assigned region (country).
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 assigned region (country).
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 3.5 Status > ARP

The following table describes the items in the previous figure.

Item	Description
ARP Table	
IP Address	Displays the mapped IP address.
MAC	Displays the MAC address of the defined IP list entry.
Interface	Displays the defined interface of the mapped address.

3.4 Interface Settings

3.4.1 LAN

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

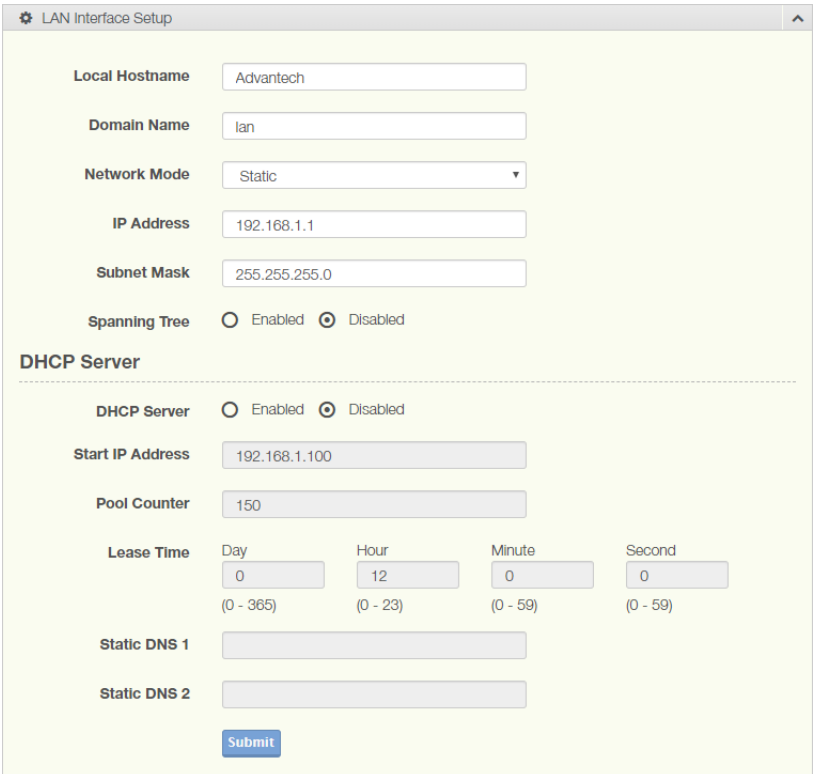


Figure 3.6 Interface > LAN

The following table describes the items in the previous figure.

Item	Description
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 or DHCP.
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.
Spanning Tree	Click the radio button to enable or disable (default) the spanning tree service.
DHCP Server	
DHCP Server	Click the radio button to enabled or disabled the DHCP server function.
Start IP Address	Enter starting a IP address for the IP assignment.
Pool Counter	Enter a variable to define the number of IP addresses for a given network.
Lease Time	Enter in the value designating the lease time for the DHCP server.
Static DNS 1	Enter in the value designating the primary static DNS.
Static DNS 2	Enter in the value designating the secondary static DNS.
Submit	Click **Submit** to save the values and update the screen.

Note! *All new configurations will take effect after rebooting. To reboot the device, click **Management** > **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. When WAN Type (Network Mode) is disabled (default), it means the device disables WAN service, and all interfaces (LAN 1, LAN2, WLAN 2.4G and WLAN 5G) are used as the local interface.

Figure 3.7 Interface > WAN > Network Mode

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 radio button to select the a WAN interface (LAN 1, LAN 2, WLAN 2.4G, or WLAN 5G).
Submit	Click **Submit** to save the values and update the screen.

When WAN Type (Network Mode) is **Static**, the **Static WAN Type** configuration settings appear.

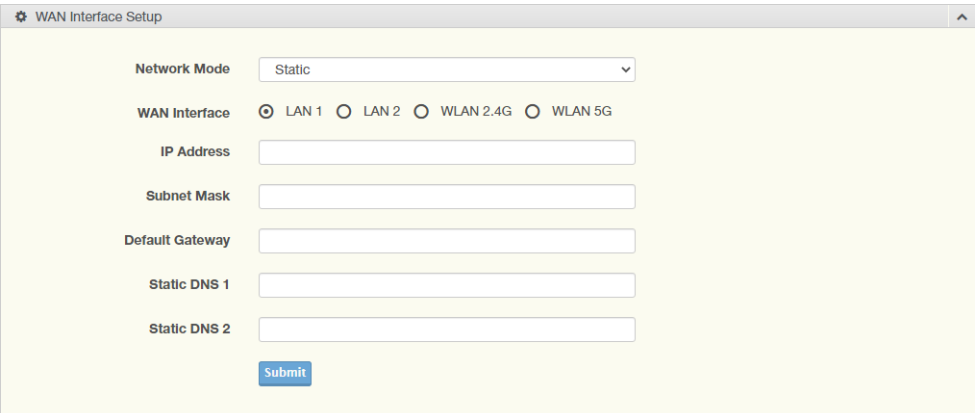


Figure 3.8 Interface > WAN > Network Mode > Static

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 radio button to select the specific interface to configure.
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.
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.

When WAN Type (Network Mode) is **DHCP**, the **DHCP WAN Type** configuration settings appear.

Figure 3.9 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 radio button to select the specific interface to configure.
Submit	Click **Submit** to save the values and update the screen.

When WAN Type (Network Mode) is **PPPoE**, the **PPPoE WAN Type** configuration settings appear.

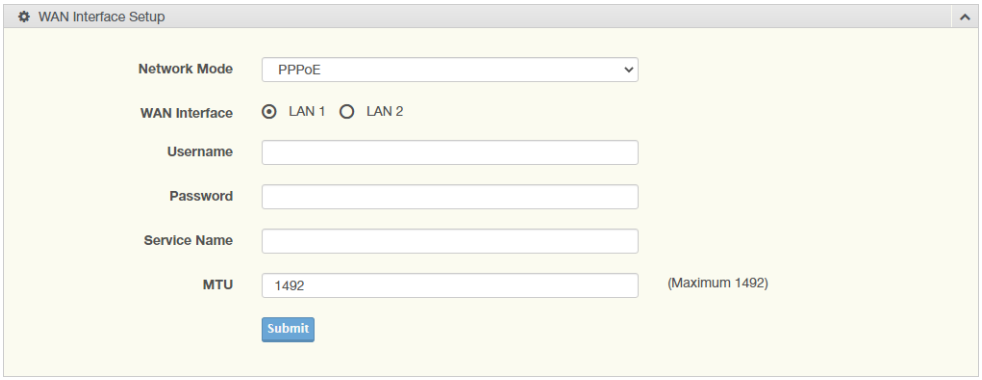


Figure 3.10 Interface > WAN > Network Mode > PPPoE

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 radio button to select the specific interface to configure.
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	MTU refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission.
Submit	Click **Submit** to save the values and update the screen.

3.4.2.1 Topology

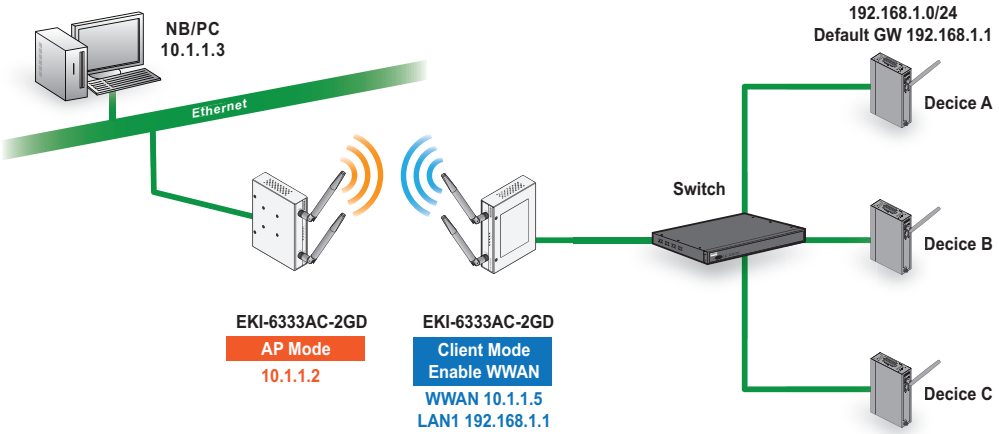


Figure 3.11 Wireless WAN Topology

3.4.3 Wireless 2.4GHz

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

3.4.3.1 Basic

Basic wireless settings offer three types of configurable modes, Access Point, Client, and Bridged Repeater.

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.

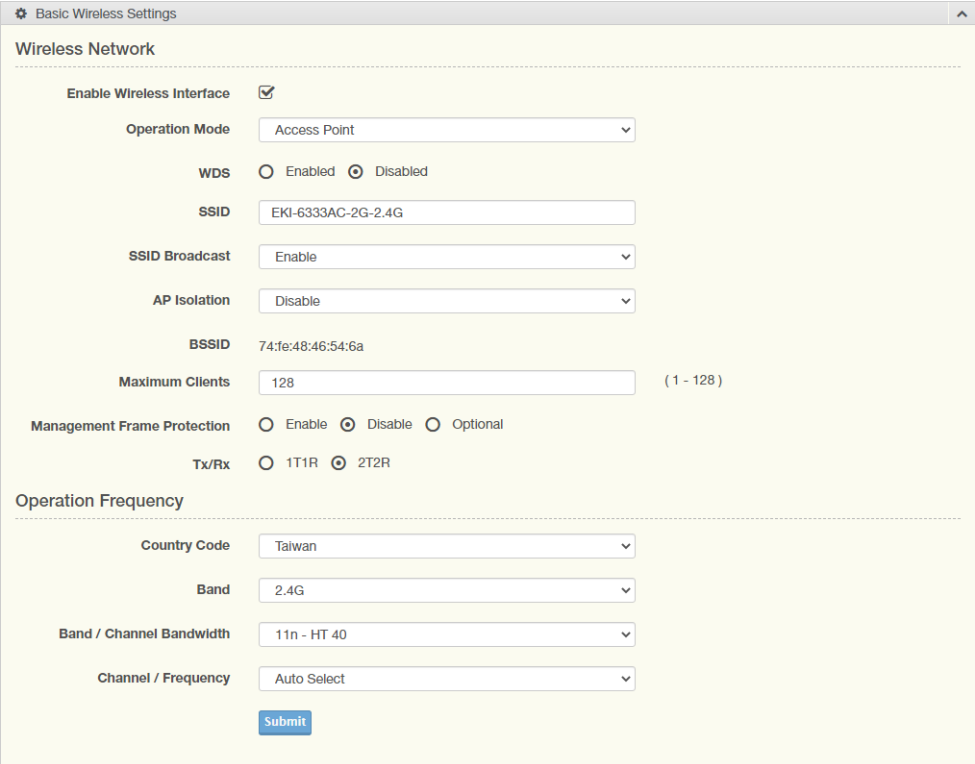


Figure 3.12 Wireless - 2.4GHz > Basic > Access Point

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, Client, Bridged Repeater.
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.

Item	Description
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.
Maximum Clients	Enter the value (1 to 128) designating the maximum number of clients per wireless device.
Management Frame Protection	Click the radio button to enable, disable, or set the function to optional. The wireless feature increases the security of the management frames, standard: IEEE 802.11W-2009.
Tx/Rx	Click to select the transmission signal stream, single or dual stream.
Operation frequency	
Country Code	Click the drop-down menu to select the country code to specify different selectable channels. Some specific channels and/or operational frequency bands are country dependent.
Band	Click the drop-down menu to select the band channel.
Band / Channel bandwidth	Click the drop-down menu to select the band and channel bandwidth: 11b/g - Non-HT (Legacy), 11n - HT20, 11n - HT40, or 11ac - VHT 80 (5GHz only).
Channel / Frequency	Click the drop-down menu to select a wireless channel/frequency: – AutoSelect – Channel 1: 2.412 GHz – Channel 2: 2.417 GHz – Channel 3: 2.422 GHz – Channel 4: 2.427 GHz – Channel 5: 2.432 GHz – Channel 6: 2.437 GHz – Channel 7: 2.442 GHz – Channel 8: 2.447 GHz – Channel 9: 2.452 GHz – Channel 10: 2.457 GHz – Channel 11: 2.462 GHz – Channel 12: 2.467 GHz – Channel 13: 2.472 GHz – Channel 14: 2.484 GHz (802.11b)
Submit	Click **Submit** to save the values and update the screen.

Client Mode

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

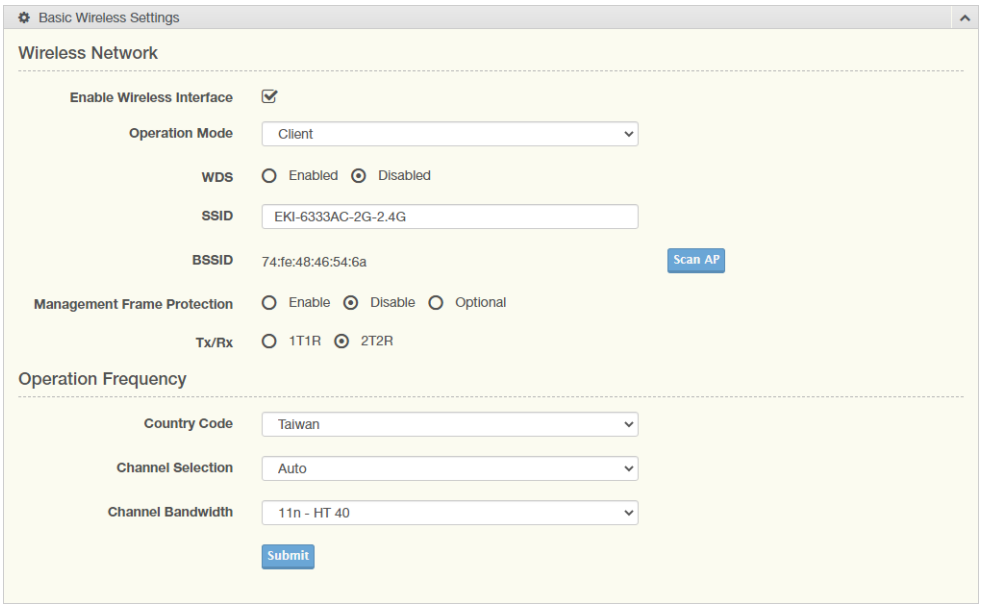


Figure 3.13 Wireless - 2.4GHz > Basic > Client

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, Client, Bridged Repeater.
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 to distinguish it from other networks in your neighborhood.
BSSID	Displays the basic service set identifiers (BSSID) for the device.
Scan AP	Click to rescan and detect nearby Access Points.
Management Frame Protection	Click the radio button to enable, disable, or set the function to optional. The wireless feature increases the security of the management frames, standard: IEEE 802.11W-2009.
Tx/Rx	Click to select the transmission signal stream, single or dual stream.
Operation frequency	
Country Code	Click the drop-down menu to select the country code to specify different selectable channels. Some specific channels and/or operational frequency bands are country dependent.
Channel Selection	Click the drop-down menu to select Auto (default) or Manual. The Auto selection allows the device to select a band. The Manual selection provides access to a selection of the option band (2.4GHz / 5GHz). The function is only enabled when Operation Mode is set to Client.

Item	Description
Channel bandwidth	Click the drop-down menu to select the band and channel bandwidth: 11b/g - Non-HT (Legacy), 11n - HT20, 11n - HT40, or 11ac - VHT 80 (5GHz only).
Submit	Click **Submit** to save the values and update the list.

Bridged Repeater Mode

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

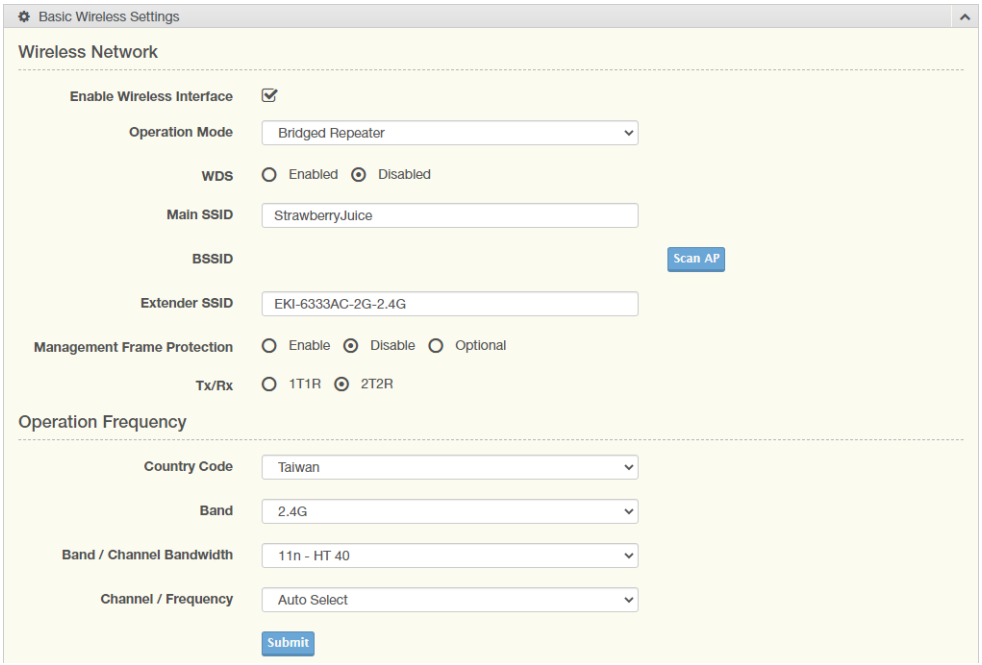


Figure 3.14 Wireless - 2.4GHz > Basic > Bridged Repeater

The following table describes the items in the previous figure.

Item	Description
Wireless Network	
Operation Mode	Click the drop-down menu to select an operation mode: Access Point, Client, Bridged Repeater.
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.
Main SSID	Enter the source SSID network to be repeated.
BSSID	Displays the basic service set identifiers (BSSID) for the device.
Scan AP	Click to rescan and detect nearby Access Points.
Extender SSID	Enter the SSID name to use for transmitting the Main SSID signal. The extender SSID boosts the signal obtained from the Main SSID and allows clients to connect efficiently.
Management Frame Protection	Click the radio button to enable, disable, or set the function to optional. The wireless feature increases the security of the management frames, standard: IEEE 802.11W-2009.
Tx/Rx	Click to select the transmission signal stream, single or dual stream.
Operation frequency	
Country Code	Click the drop-down menu to select the country code to specify different selectable channels. Some specific channels and/or operational frequency bands are country dependent.

Item	Description
Band	Click the drop-down menu to select the band channel.
Band / Channel bandwidth	Click the drop-down menu to select the band and channel bandwidth: 11b/g - Non-HT (Legacy), 11n - HT20, 11n - HT40, or 11ac - VHT 80 (5GHz only).
Channel / Frequency	Click the drop-down menu to select a wireless channel/frequency: – AutoSelect – Channel 1: 2.412 GHz – Channel 2: 2.417 GHz – Channel 3: 2.422 GHz – Channel 4: 2.427 GHz – Channel 5: 2.432 GHz – Channel 6: 2.437 GHz – Channel 7: 2.442 GHz – Channel 8: 2.447 GHz – Channel 9: 2.452 GHz – Channel 10: 2.457 GHz – Channel 11: 2.462 GHz – Channel 12: 2.467 GHz – Channel 13: 2.472 GHz – Channel 14: 2.484 GHz (802.11b)
Submit	Click **Submit** to save the values and update the screen.

Topology

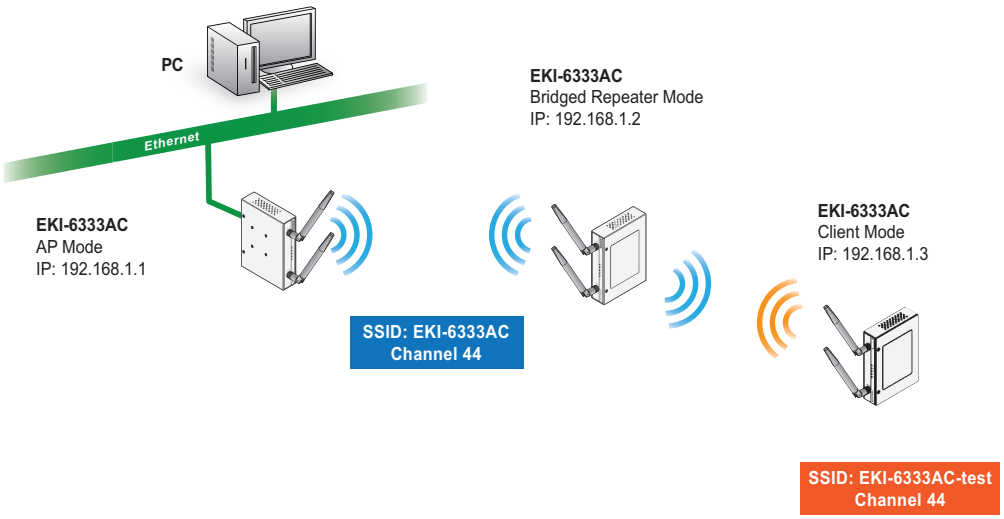


Figure 3.15 Bridged Repeater Mode Topology

Enabling Bridged Repeater Mode

To enable bridged repeater mode on the device navigate to **Interface** > **Wireless - 2.4 GHz** > **Basic**. For the purposes of these guidelines, 2.4 GHz is used. However, bridged repeater mode is also available for the 5 GHz wireless interface.

1. Navigate to the Basic Wireless Settings menu.
2. On Operation Mode, click the drop-down menu to selected **Bridged Repeater**.
3. In the Main SSID field, enter the name of the SSID to use. The SSID field cannot remain empty in Bridged Repeater mode.
4. Click **Scan AP** to select an available AP from the AP list.
5. In the Extender SSID field, enter the client SSID to extend the Main SSID access.

6. Configure the remaining fields to specify your unique settings.
7. Click Submit to save and enable the configuration settings.

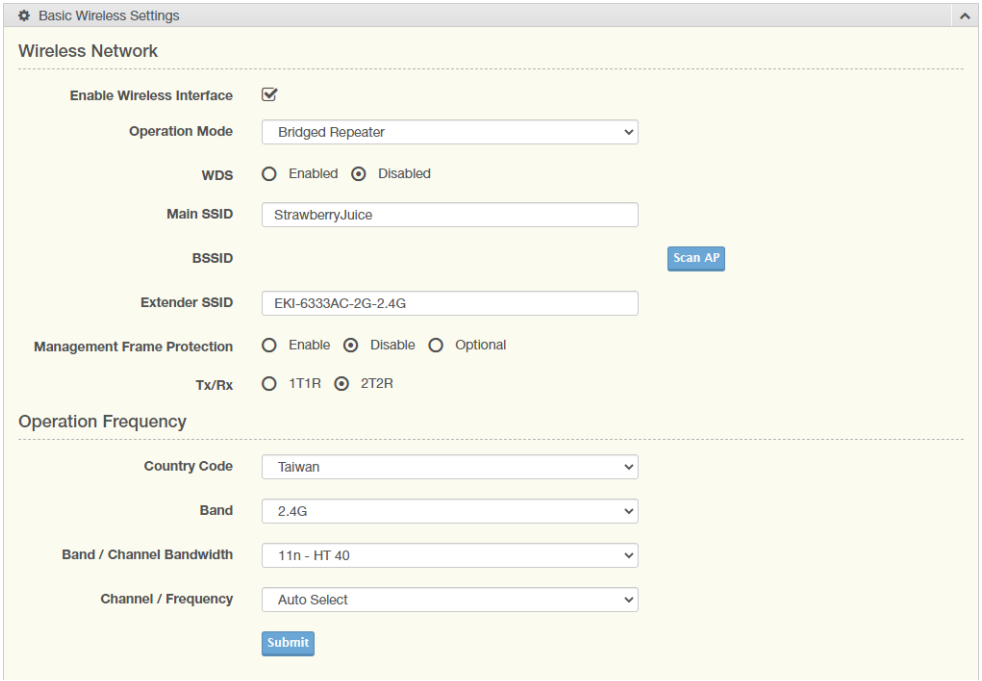


Figure 3.16 Enabling Bridged Repeater Mode

The following figure depicts a completed Bridged Repeater configuration between an AP device (Main SSID), a repeater device, and a client device (extender SSID).

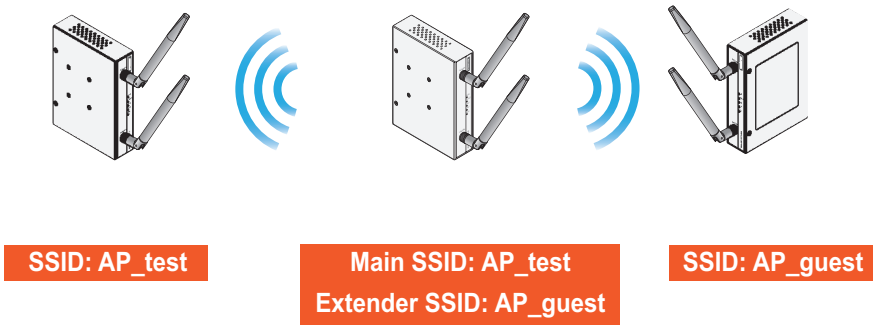


Figure 3.17 Completed Bridged Repeater Mode Setting

3.4.3.2 Advanced

Access Point and Bridge Repeater Modes

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

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

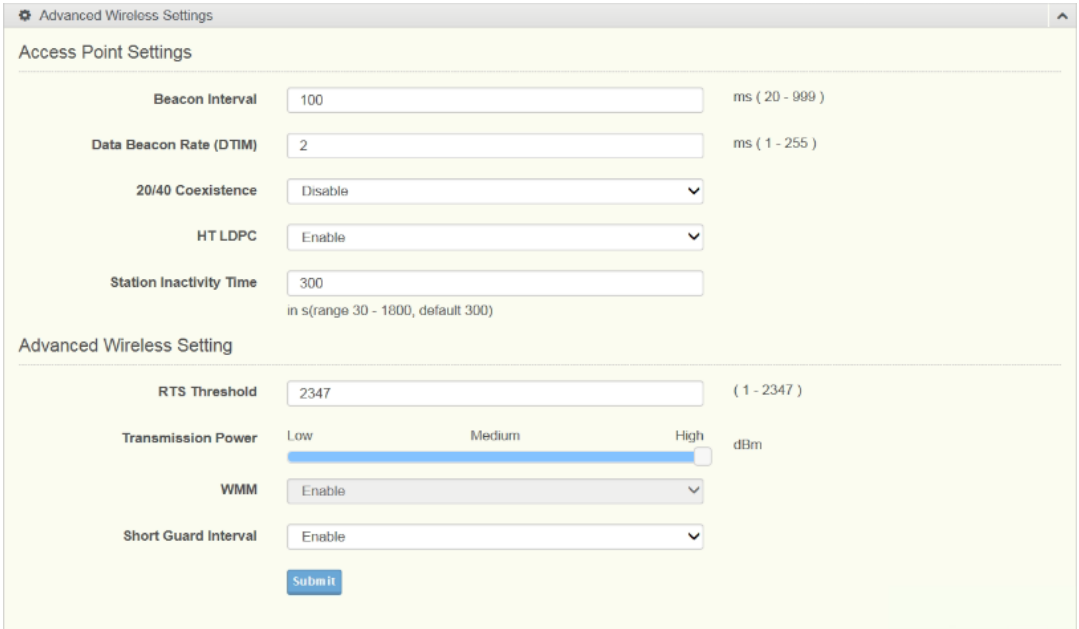


Figure 3.18 Wireless - 2.4GHz > Advanced

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).
HT LDPC	Enable to advertise Low-density Parity Check (LDPC) support. By enabling HT LDPC, the function improves data transmission over channels with a high degree of background noise (default: enabled).
Station Inactivity Time	Enter the value in seconds (30 to 600, default 300) to define the period of traffic inactivity for a client before the AP removes it.
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: High, Medium, or Low.
WMM	Enable WiFi Multimedia (WMM) to enhance the quality of service (QoS) on a network by prioritizing packet data based.

Item	Description
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 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 Mode.

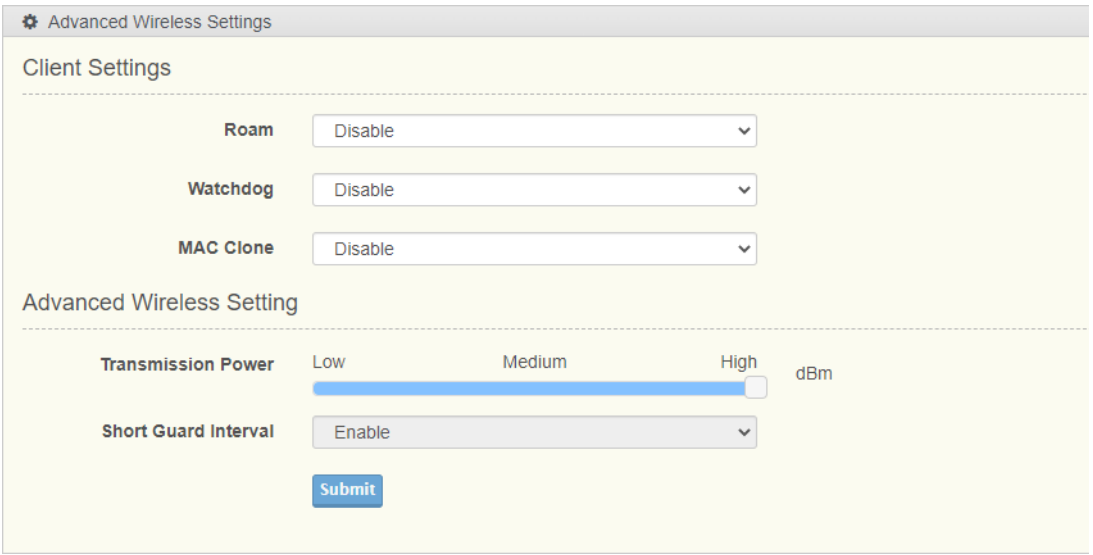


Figure 3.19 Wireless - 2.4GHz > Advanced

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.
RSSI threshold	Enter the value to designate the RSSI threshold (range 1 - 75, default 65). When the RSSI of current connection is poor than RSSI threshold, the device will continue to scan nearby AP according to the interval time in the Scan Interval (Low) field, to look for other AP with better signal.
RSSI hysterisis	Enter the value to indicate how much greater the signal strength of an access point must be to roam to it. Range: 3 to 20 dB (default: 3 dB).
Scan interval (high)	The interval time of background scan during active RSSI > RSSI threshold. The default is 120 seconds.
Scan interval (low)	The interval time of background scan during active RSSI < RSSI threshold. The default is 15 seconds

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-6333AC-2GD 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.
MAC Clone	Click to enable or disable the MAC clone function. ■ Auto: The MAC address of the WLAN interface will be automatically changed to the MAC address of the computer connected to this WEB page. ■ Manual: Specify the new MAC address of the WLAN interface you want.
Advanced Wireless Setting	
Transmission Power	Click the slide bar to select the transmission power level: High, Medium, or Low.
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.

3.4.3.4 Security

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

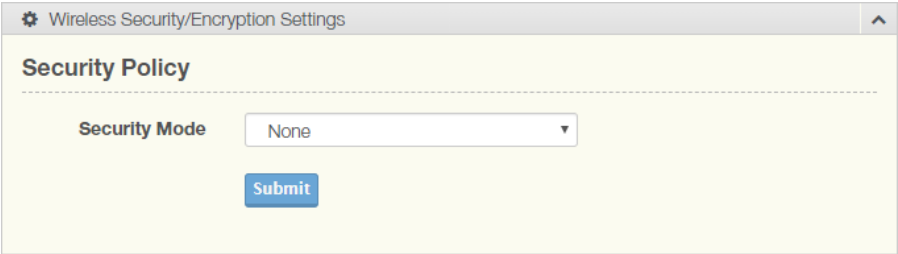


Figure 3.20 Wireless - 2.4GHz > Security

In Bridged Repeater mode, the security / encryption settings are displayed as follows. See the following figure.

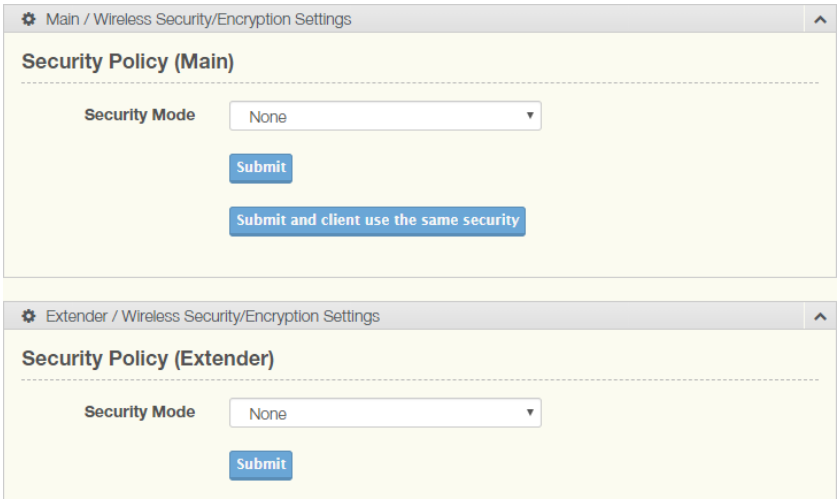


Figure 3.21 Wireless - 2.4GHz > Security

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

Security Mode None

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

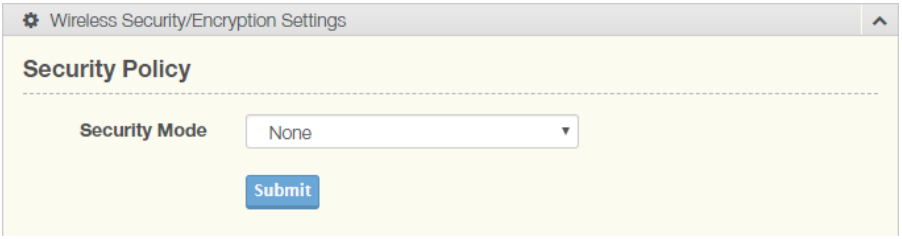


Figure 3.22 Wireless Settings > Security

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

Security Mode WEP

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

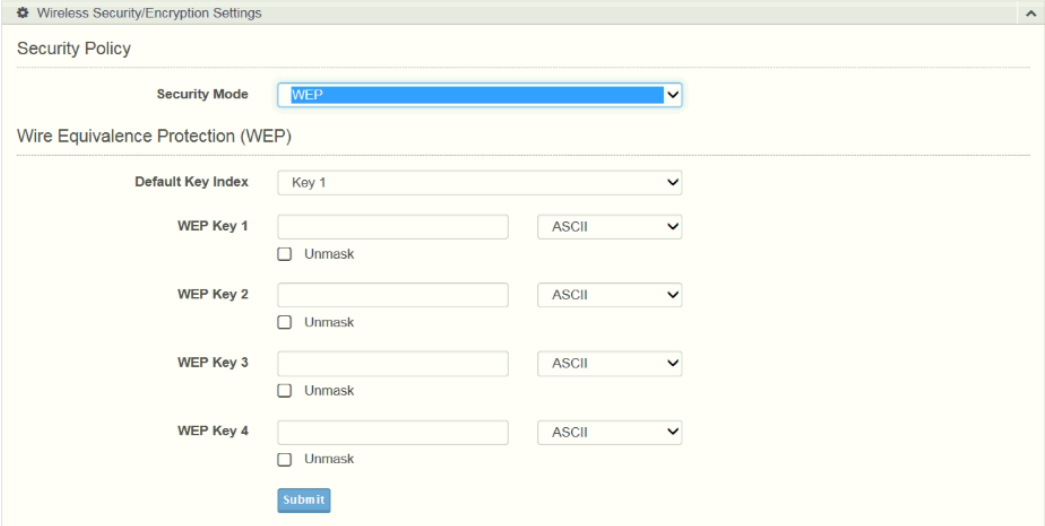


Figure 3.23 Security Mode > WEP

The following table describes the items in the previous figure.

Item	Description
Security Policy	
Security Mode	Click the drop-down menu to select the encryption when communication. Available options: None, WEP, WPA-Personal and WPA/WPA2-Enterprise. If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.
Wire Equivalence Protection (WEP)	
Default Key Index	Click the drop-down menu to select one of the four defined key indexes as defined by the WEP Key # fields in the following
WEP Key 1	Enter up to four WEP keys. Enter a string of characters dependent on the key type: ASCII -- Upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #. Hex -- Digits 0 to 9 and the letters A to F. Click **Unmask** to view the password entry.
WEP Key 2	
WEP Key 3	
WEP Key 4	
Submit	Click **Submit** to save the values and update the screen.

Security Mode WPA-Personal

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

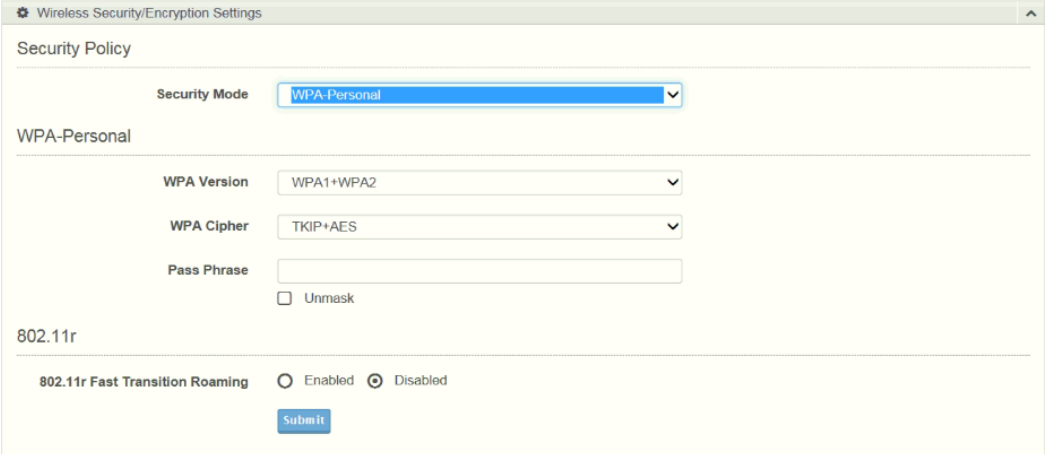


Figure 3.24 Security Mode > WPA-Personal

The following table describes the items in the previous figure.

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

Item	Description
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.

Security Mode WPA/WPA2-Enterprise

To access this page, click **Interface** > **Wireless - 2.4** > **Security** > **Security Mode** > **WPA/WPA2-Enterprise**.

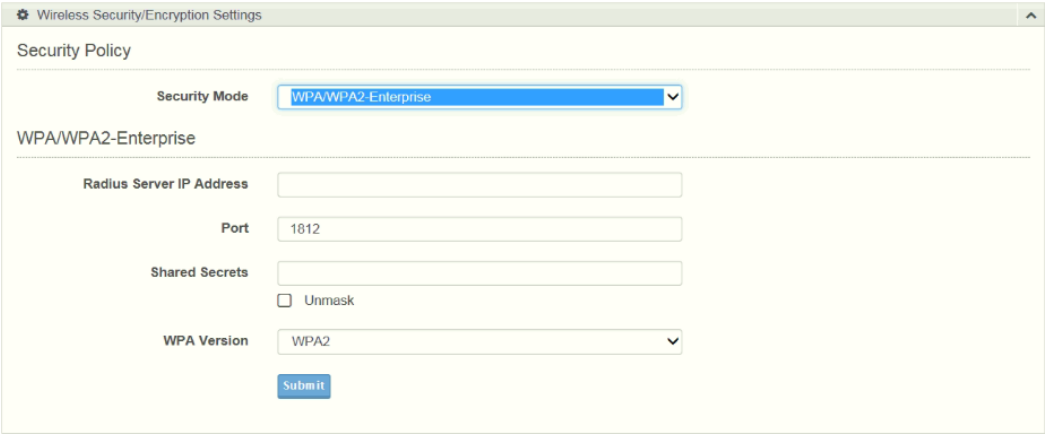


Figure 3.25 Security Mode > WPA/WPA2-Enterprise

The following table describes the items in the previous figure.

Item	Description
Security Policy	
Security Mode	Click the drop-down menu to select the encryption when communication. Available options: None, WEP, WPA-Personal and WPA/WPA2-Enterprise. If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.
WPA/WPA2 Enterprise	
Radius Server IP Address	Enter the IP address of the designated radius server.
Port	Enter the authorized port number corresponding to the designated radius server in previous field.
Shared Secrets	Enter the string variable used as the shared key between client and server.
WPA version	Click the drop down menu to select the designated WPA standard: WPA, WPA2, or WPA+WPA2.
Submit	Click **Submit** to save the values and update the screen.

3.4.3.5 Multiple SSID

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

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

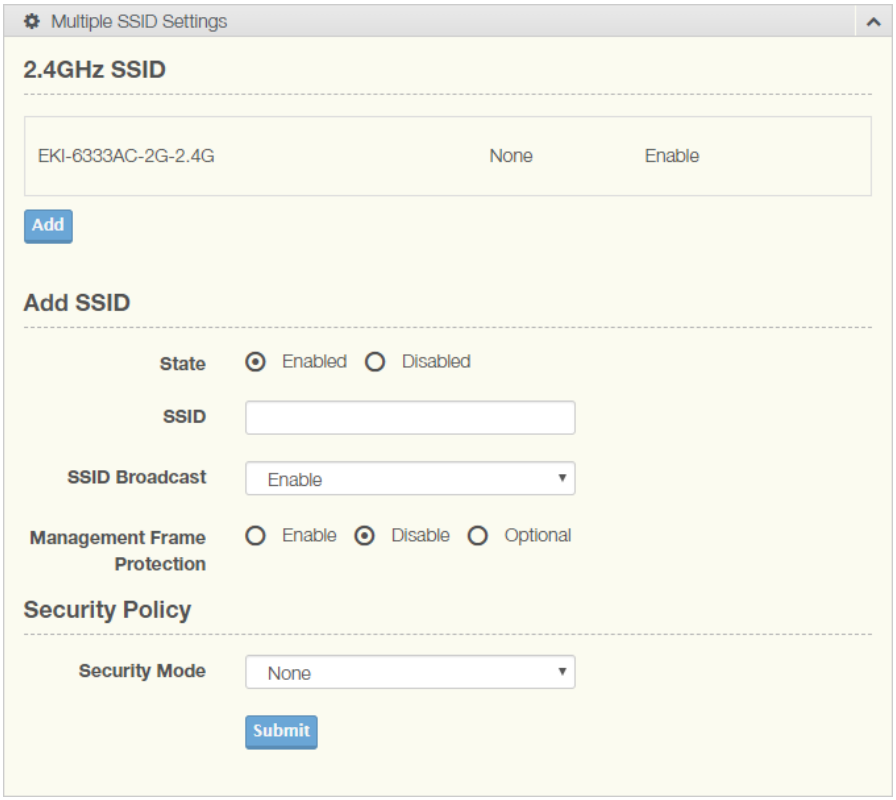


Figure 3.26 Wireless - 2.4GHz > Multiple SSID

The following table describes the items in the previous figure.

Item	Description
Add	Click Add after completing the SSID information to create the wireless network and list it in the menu.
Add SSID	
State	Click the radio button to designate the state (enabled/disabled) of 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
Management Frame Protection	Click the radio button to enable, disable, or set the function to optional. The wireless feature increases the security of the management frames, standard: IEEE 802.11W-2009.
Security Policy	
Security Mode	Click the drop-down menu to select the encryption when communication. Available options: None, WPA-Personal and WPA/ WPA2-Enterprise. If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.
Submit	Click **Submit** to save the values and update the screen.

3.4.3.6 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**.

Overview

Information Name	Information Value
Mode	Access Point
SSID	EKI-6333AC-2G-2.4G
Channel / Frequency	channel 11 (2462 MHz)
BSSID	88:DC:96:80:0F:EA

Station List

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

Wlan Status

Information Name	Information Value
TX Packets	96870
TX Bytes	13474682
RX Packets	0
RX Bytes	0

Figure 3.27 Wireless - 2.4GHz > Statistics

The following table describes the items in the previous figure.

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

3.4.3.7 Access Control

The Access Control appoints the authority to wireless client on accessing EKI-6333AC-2GD Series, thus a further security mechanism is provided. This function is available only under AP mode, see “Management” on page 55.

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

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

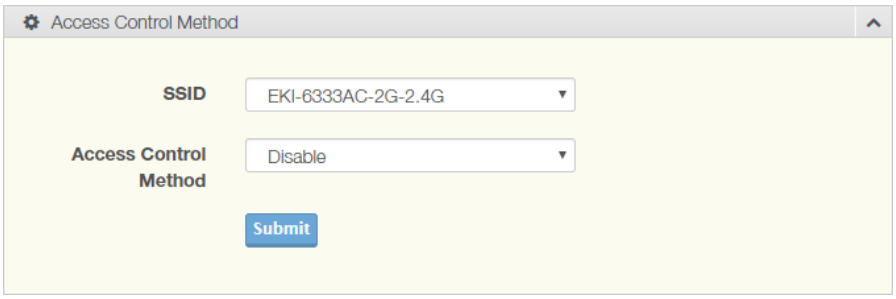


Figure 3.28 Wireless - 2.4GHz > Access Control

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. In the Deny or Allow menu, enter the MAC address of the target device - support for up to 32 target devices.
Submit	Click **Submit** to save the values and update the screen.

3.4.3.8 Site Survey

The Site Survey feature is only available when the wireless mode of the device is set to Client or Bridged Repeater mode, see “Management” on page 55.

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

Figure 3.29 Wireless - 2.4GHz > Site Survey

Item	Description
Refresh	Click to update the displayed AP list table.
AP list	
SSID	Displays the name of the listed AP.
BSSID	Displays the basic service set identifiers (BSSID) used to describe the section of the SSID.
Frequency	Displays the radio frequency of the listed SSID.
Signal level	Displays the signal level of the listed SSID.
Encryption	Displays the encryption type assigned to the listed SSID.

3.4.3.9 VLAN

The VLAN function allows for the processing of data to and from clients in the same manner as data is processed to and from wired connections.

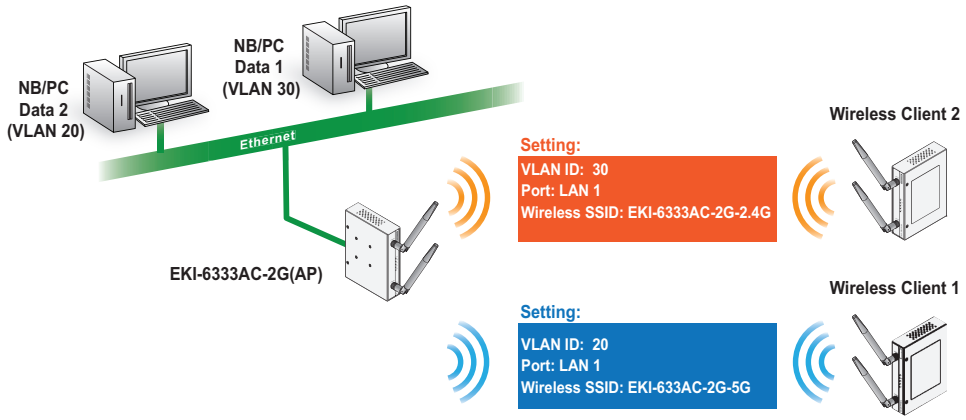


Figure 3.30 Wireless VLAN ID Data Flow Diagram

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

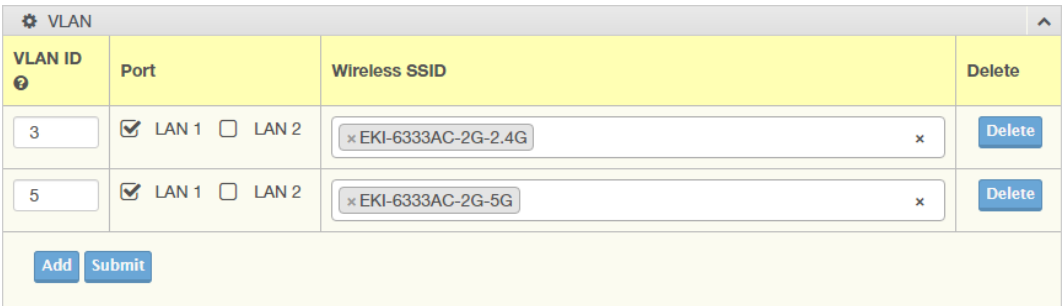


Figure 3.31 Wireless - 2.4GHz > VLAN

Item	Description
VLAN ID	Enter a variable (3 to 127) to identify the VLAN entry.
Port	Click a specific interface (LAN 1 / LAN 2) to designate to the VLAN entry.
Wireless SSID	Click the drop-down menu to select an SSID entry to configure to the VLAN entry.
Delete	Click **Delete** to remove the VLAN entry from the list.
Add	Click **Add** after completing the SSID information to create the wireless network and list it in the menu.
Submit	Click **Submit** to save the values and update the screen.

3.4.3.10 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 or Bridged Repeater mode.

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

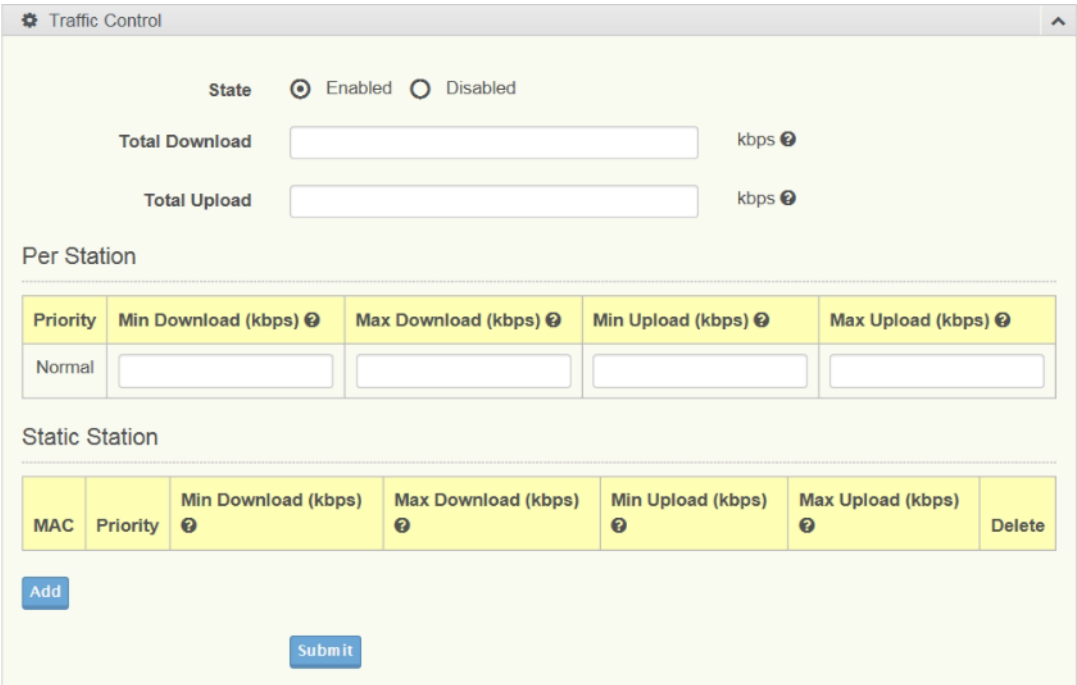


Figure 3.32 Wireless - 2.4GHz > Traffic Control

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	Enter the value to define the default policy for download and upload speed ranges for each connected client.
Static Station	Enter the MAC and speed values to define the download and upload speed ranges for the target client.
Add	Click **Add** after populating a Static Station entry.
Submit	Click **Submit** to save the values and update the setting.

3.4.3.11 Log

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

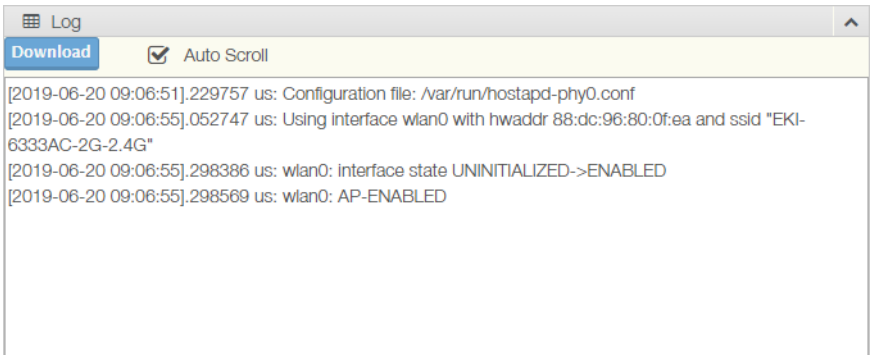


Figure 3.33 Wireless - 2.4GHz > Log

The following table describes the items in the previous figure.

Item	Description
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.

3.4.4 Wireless 5GHz

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

For further details regarding the user interface, refer to the Wireless 2.4GHz section. See “Wireless 2.4GHz” on page 27.

3.4.5 Wireless Redundant

To access this page, click **Interface** > **Wireless Redundant**.

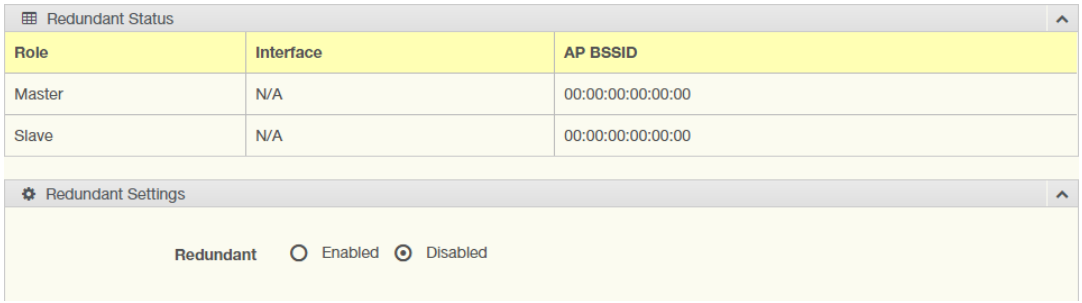


Figure 3.34 Interface > Wireless Redundant > Redundant Status

The following table describes the items in the previous figure.

Item	Description
Redundant Status	
Master	Displays the interface assigned to the master (primary) role.
Slave	Displays the interface assigned to the slave (redundant) role.
Interface	Displays the assigned interface to the device.
AP BSSID	Displays the AP’s SSID identification
Redundant Settings	
Redundant	Click to enable or disable the redundant function. The redundant function is only available when both WLAN interfaces of the device is in client mode.

The following figure displays enabled Redundancy function. The 2.4G and 5G WLAN interfaces of the device will try to connect remote AP at the same time. If both WLAN interface are connected to the AP, one of the WLAN connection will be used as master role, and the other will be used as slave role. The device will only transmit data through the master connection, and slave connection is used just as backup connection. The device can monitor the master connection status. If the quality of master connection is not good, the device will switch the roles of the two WLAN interfaces. The original slave interface will be changed to master interface, and all data will be changed to transferred through this new master interface.

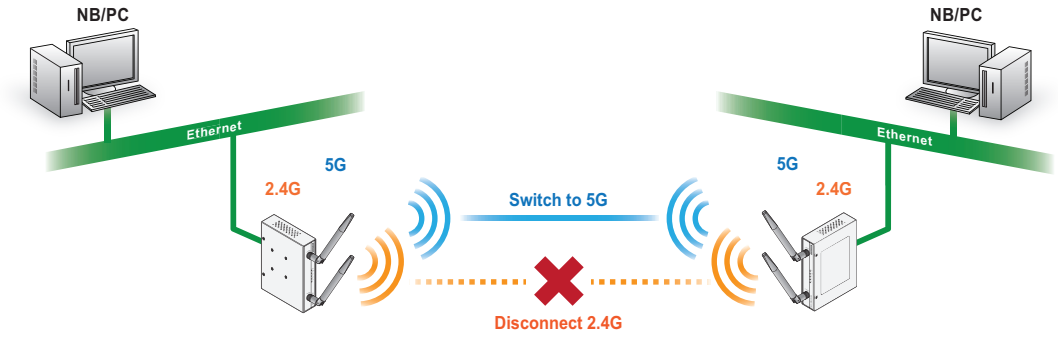


Figure 3.35 Wireless Redundancy Enabled

The Role Exchange Setting menu follows as seen in the following figure.

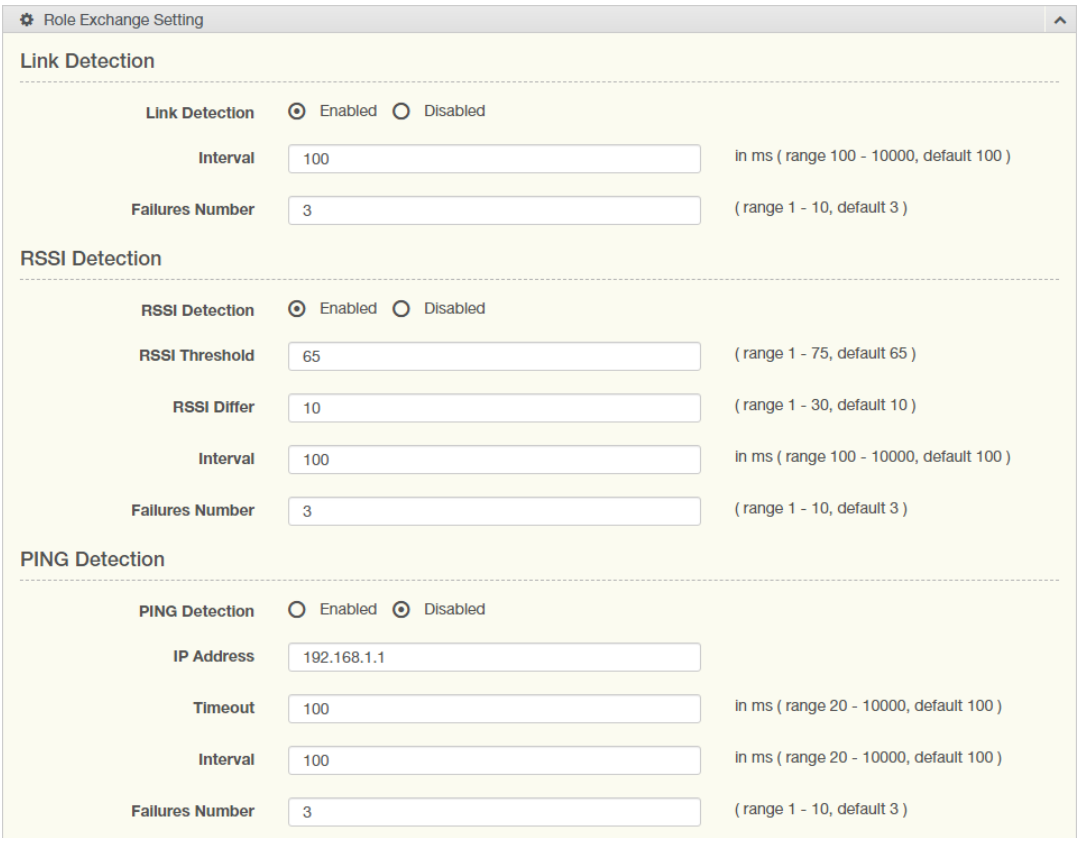


Figure 3.36 Interface > Wireless Redundant > Role Exchange Settings

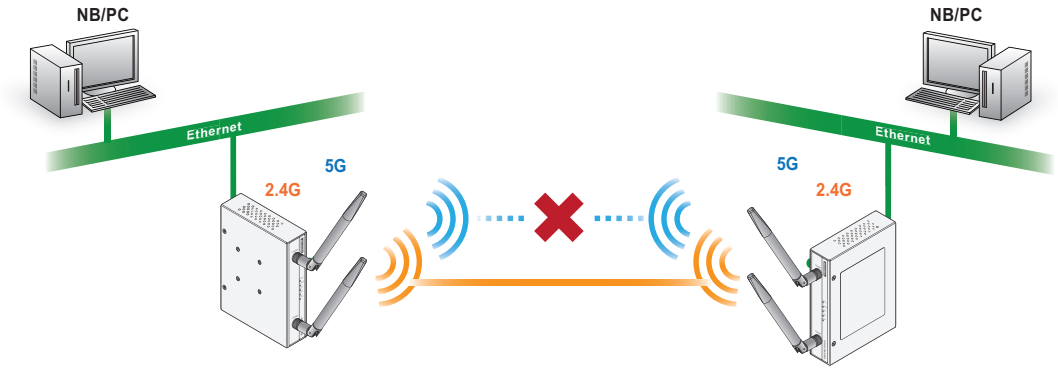
The following table describes the items in the previous figure.

Item	Description
Link Detection	
Link Detection	Click to enable or disable the wireless link detection function. If it is detected that the WLAN interface with master role is in disconnection state straight Failure Number times, the master role will change to another WLAN interface.
Interval	Enter the value in ms to designate the interval time between link queries (range 100 - 10000, default 100).
Failure Number	Enter the value to designate the failure threshold (range 1 - 10, default 3).
RSSI Detection	

Item	Description
RSSI Detection	Click to enable or disable the RSSI detection function. If it is detected that the RSSI of the WLAN interface with master role is poor than RSSI Threshold and is more than RSSI Differ worse than the RSSI of another WLAN interface straight Failure Number times, the master role will change to another WLAN interface.
RSSI Threshold	Enter the value to designate the signal strength setting (range 1 - 75, default 65).
RSSI Differ	If the slave scans and finds that the signal strength is better than the originally connected AP, if it is greater than the set value, it will switch to connect to the AP.(range 1 - 30, default 10)
Interval	Enter the value in ms to designate the interval time between link queries (range 100 - 10000, default 100).
Failures Number	Enter the value to designate the failure threshold (range 1 - 10, default 3).
Ping Detection	
Ping Detection	Click to enable or disable the wireless link detection function. If the device can't ping the specific IP address straight Failure Number times, the master role will change to another WLAN interface.
IP Address	Enter the IP address of the remote device to test connectivity.
Timeout	Enter the value in ms to designate the timeout threshold (range 20 - 10000, default 100).
Interval	Enter the value in ms to designate the interval time between link queries (range 20 - 10000, default 100).
Failures Number	Enter the value to designate the failure threshold (range 1 - 10, default 3).

The following figure displays enabled RSSI detection function.

■ RSSI value > defined threshold



■ RSSI value < defined threshold

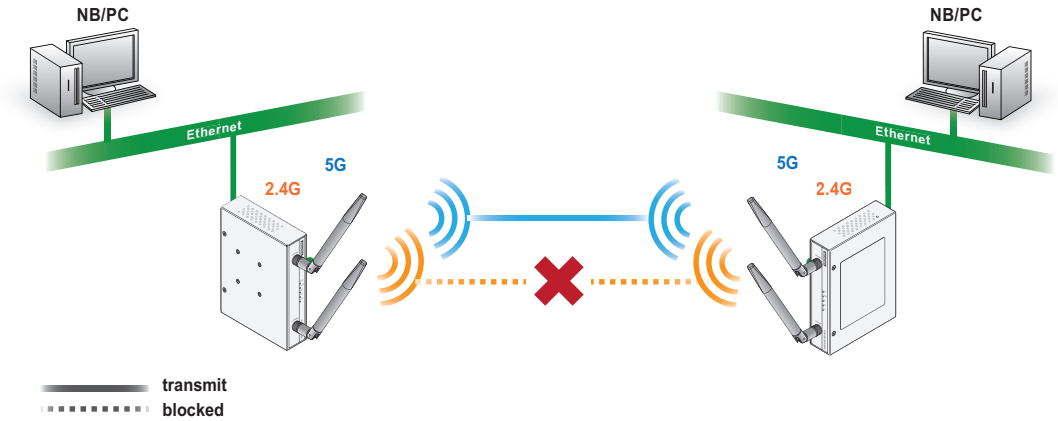


Figure 3.37 Wireless RSSI Detection

■ Ping failed count < defined count

■ Ping failed count > defined count

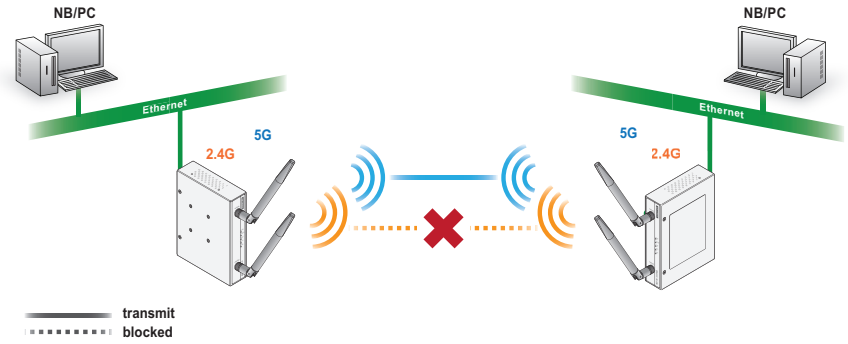


Figure 3.38 Wireless PING Detection

The Slave Settings menu displays as shown in the following figure.

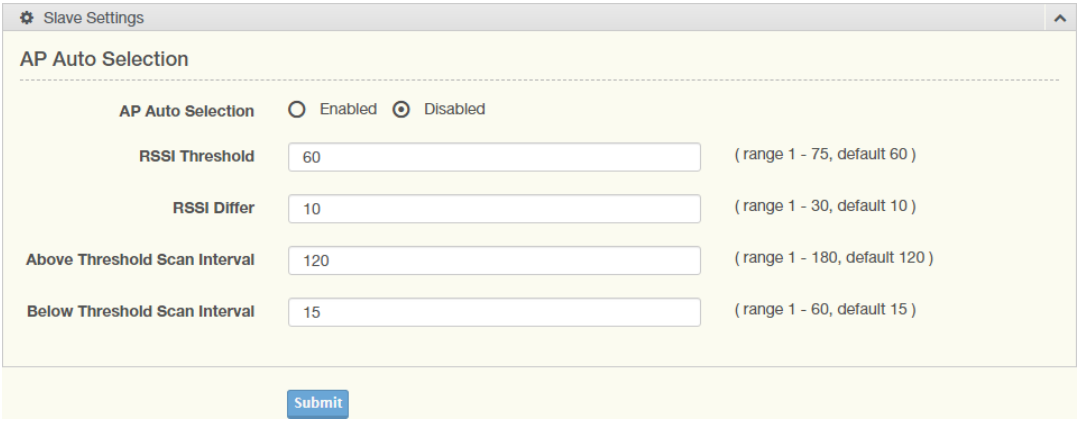


Figure 3.39 Interface > Wireless Redundant > Slave Settings

The following table describes the items in the previous figure.

Item	Description
AP Auto Selection	
AP Auto Selection	Click to enable or disable the AP Auto Selection function.
RSSI Threshold	Set connection quality monitor RSSI threshold.
RSSI Differ	The set value to determine the threshold for selecting an AP connection based on signal strength.
Above Threshold Scan Interval	The interval time during an active RSSI > RSSI threshold scan, background scan. The default is 120 seconds.
Below Threshold Scan Interval	The interval time during a local RSSI <RSSI Threshold scan. The default is 15 seconds
Submit	Click to save the configuration settings.

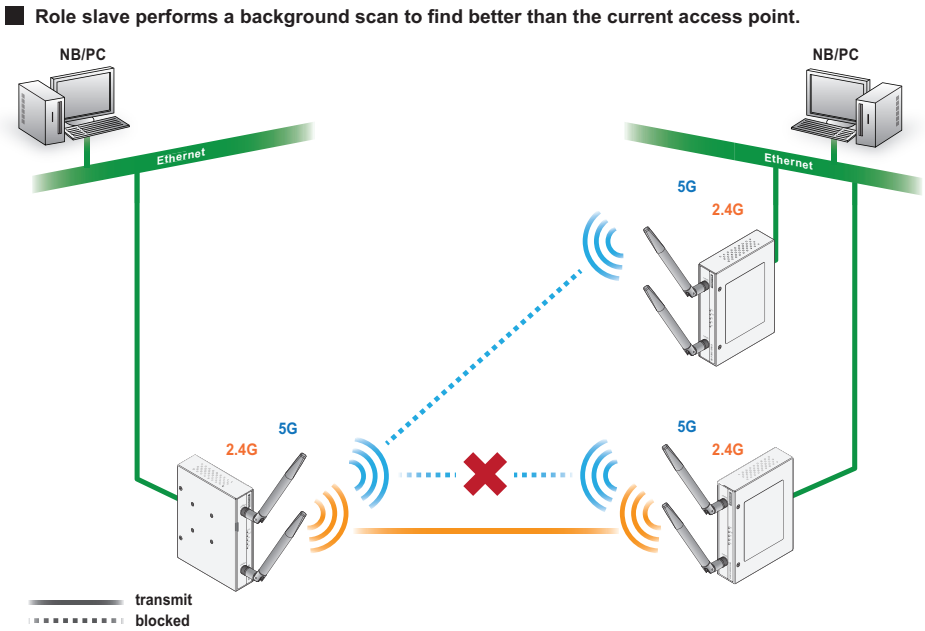


Figure 3.40 Wireless Redundant Auto Selection

3.4.5.1 Topology

In Wireless Redundant mode, two wireless devices are setup. When a disruption or poor signal event occurs and meets the specified conditions, the backup device is initiated.

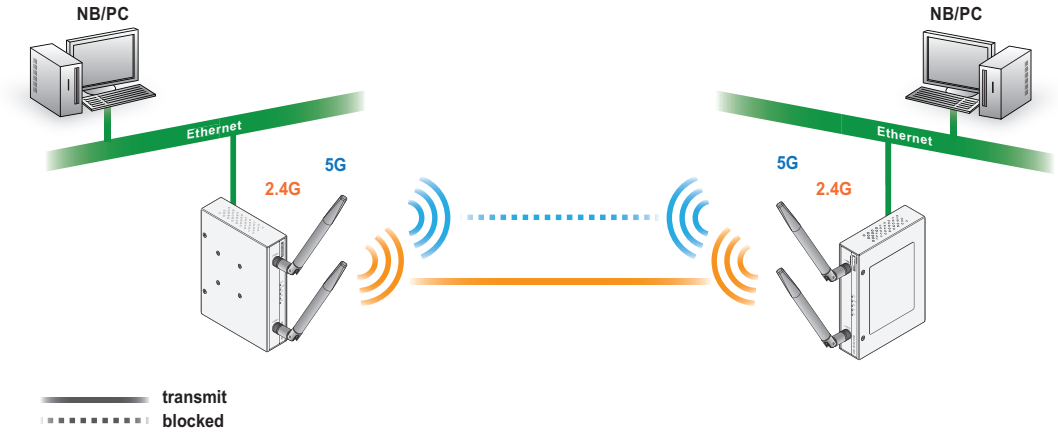


Figure 3.41 Wireless Redundant Topology

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**.

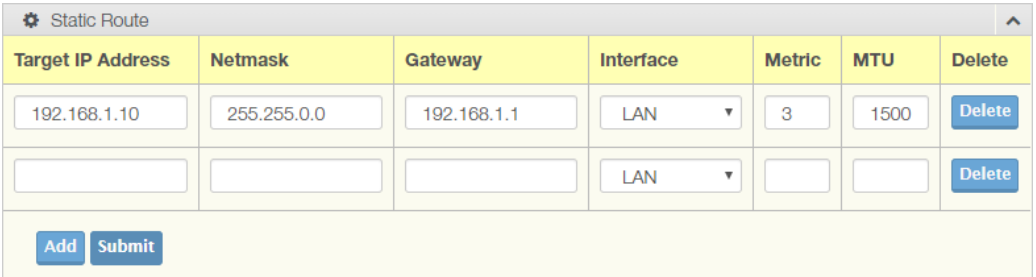


Figure 3.42 Networking > Static Route

The following table describes the items in the previous figure.

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

3.5.2 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.

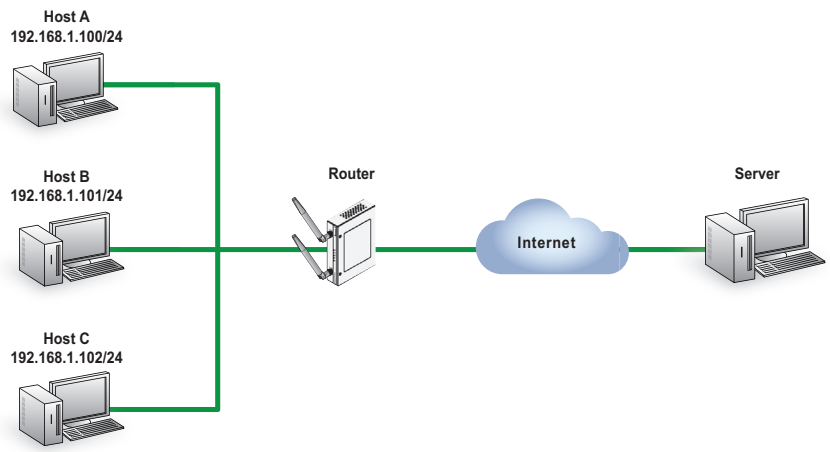


Figure 3.43 NAT Diagram

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.

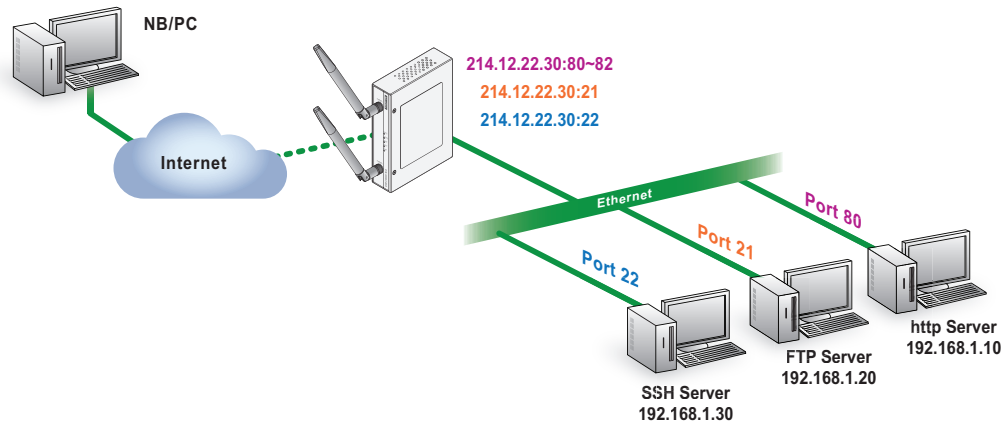


Figure 3.44 Port Forwarding

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

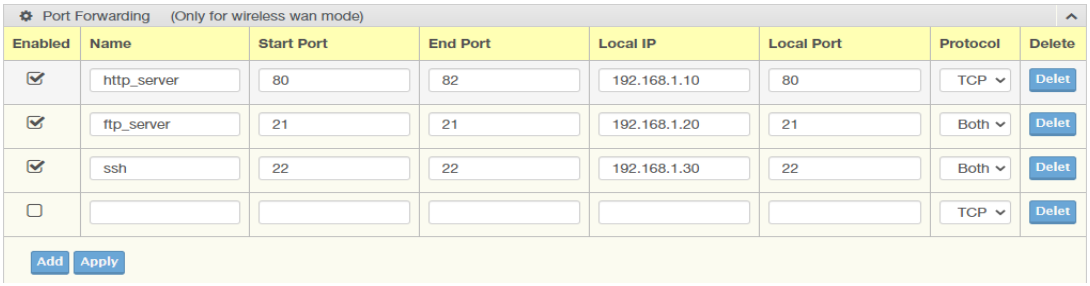


Figure 3.45 Networking > Forwarding > Port Forwarding

The following table describes the items in the previous figure.

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

3.5.3.2 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**.

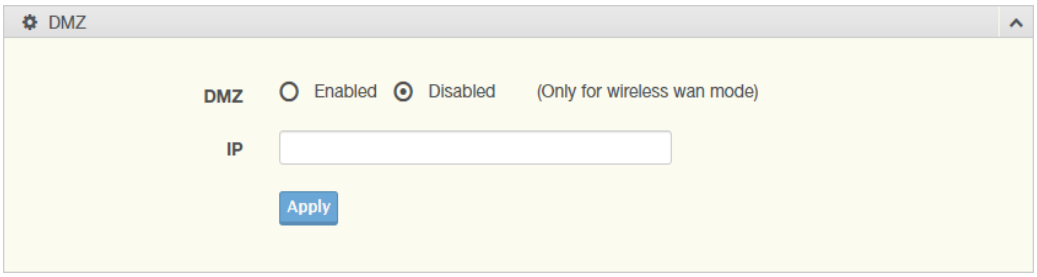


Figure 3.46 Networking > Forwarding > DMZ

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**.

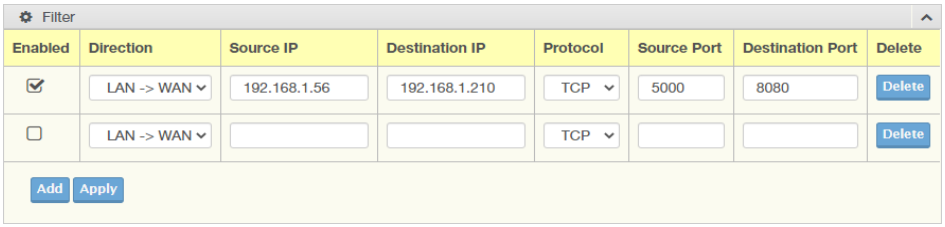


Figure 3.47 Networking > Security > Filter

Item	Description
Filter	Click the radio button to enable or disable the Filter policy.
Enabled	Select to enable the defined filter entry.
Direction	Click the drop-down menu to select the direction of the data packet taffic for the entry: LAN to WAN, WAN to LAN.
Source IP	Enter the IP address of the sender address.
Destination IP	Enter the IP address of the destination address.

Item	Description
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**.

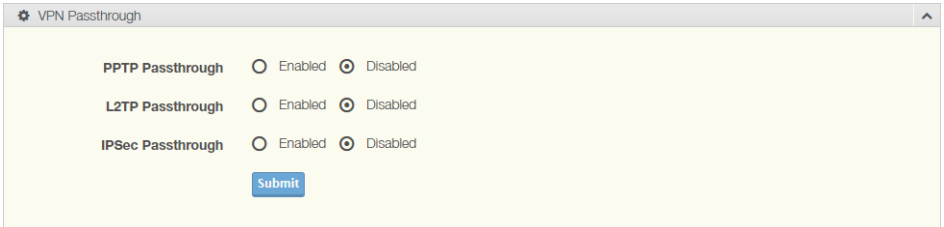


Figure 3.48 Networking > **Security** > **VPN Passthrough**

Item	Description
PPTP Passthrough	Click the radio button to enable or disable PPTP packets to pass through.
L2TP Passthrough	Click the radio button to enable or disable L2TP packets to pass through.
IPSec Passthrough	Click the radio button to enable or disable IPSEC packets to pass through.
Submit	Click **Submit** to save the values and update the policy.

3.6 Management

3.6.1 Password Manager

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

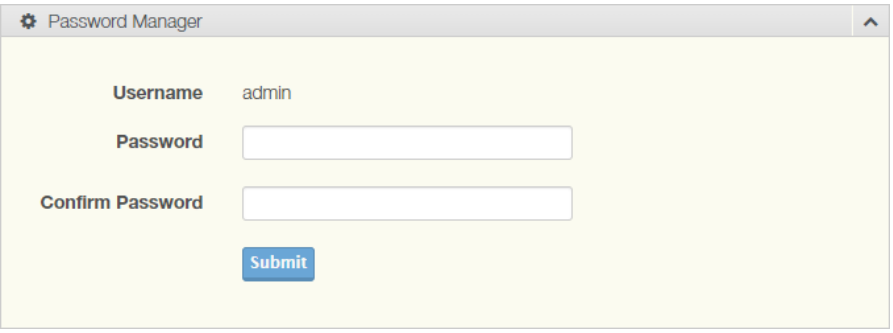


Figure 3.49 Management > Password Manager

The following table describes the items in the previous figure.

Item	Description
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**.

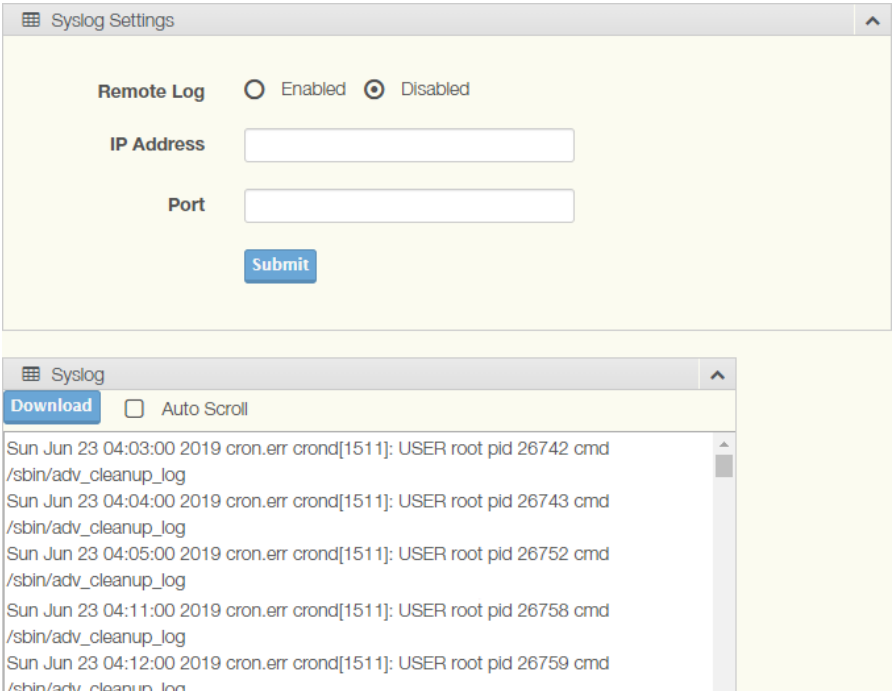


Figure 3.50 Management > Syslog

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**.

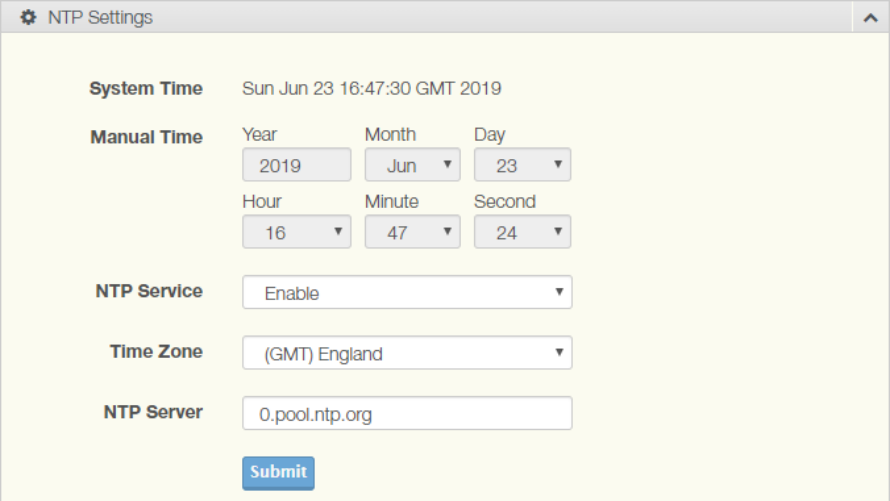


Figure 3.51 Management > NTP / Time

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**.

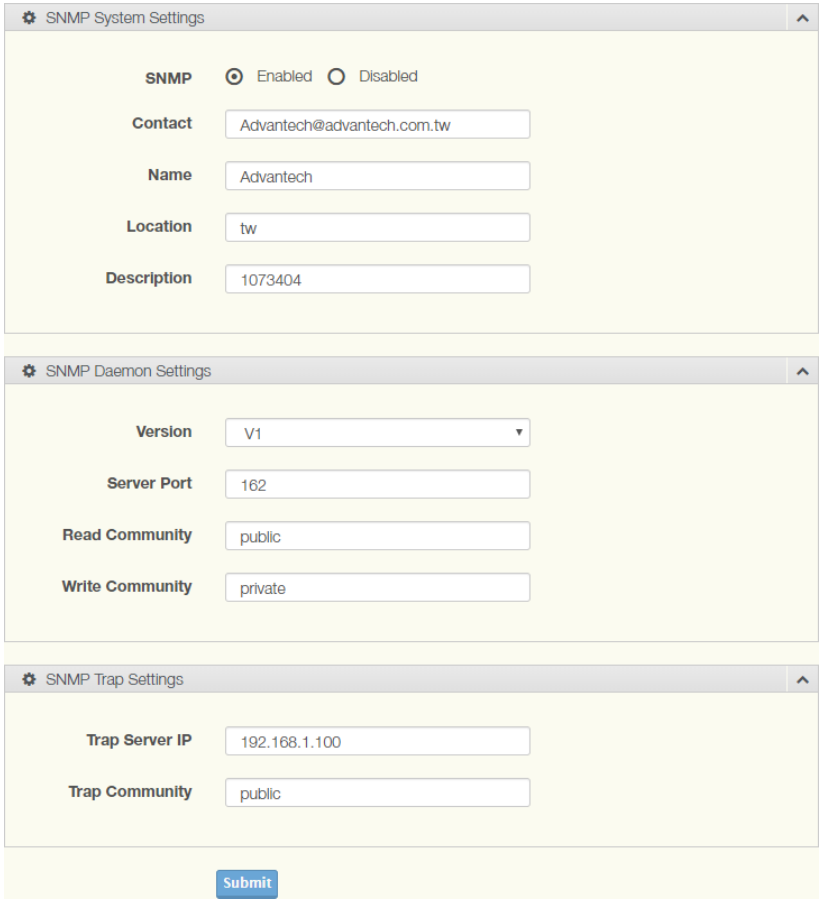


Figure 3.52 Management > SNMP

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 version of the daemon.
Server Port	Enter the port to access on the specified server.
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.
SNMP Trap Settings	
Trap Server IP	Enter the static route to define the trap server used for the defined user.

Item	Description
Trap Community	Enter the setting to define the level of access for the define 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**.

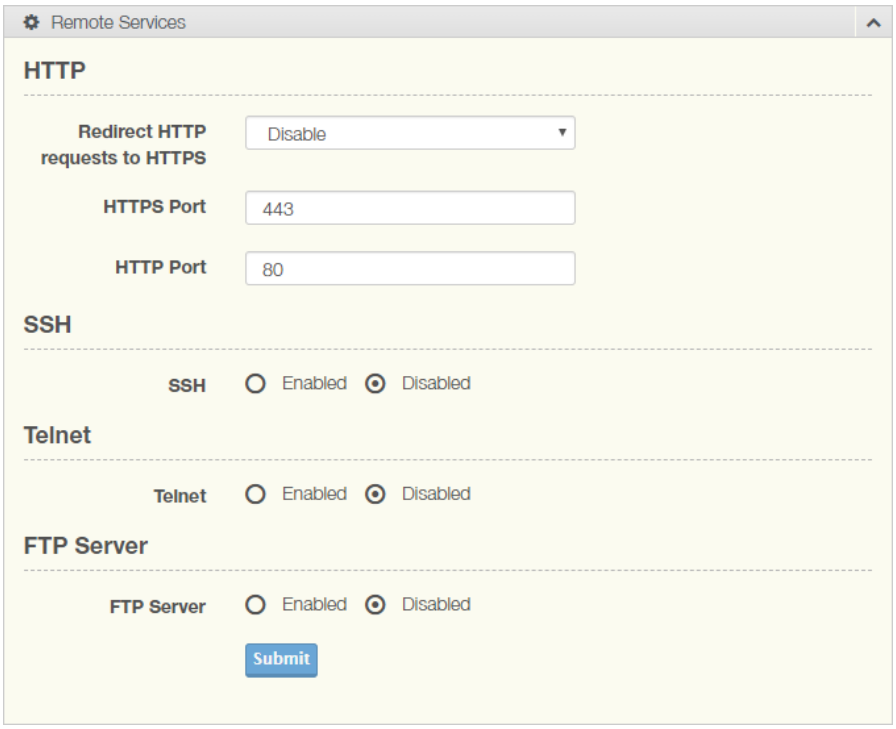


Figure 3.53 Management > Remote Services

The following table describes the items in the previous figure.

Item	Description
HTTP common settings	
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.
FTP Server	
FTP Server	Click the radio button to enable or disable access to the FTP Server 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**.

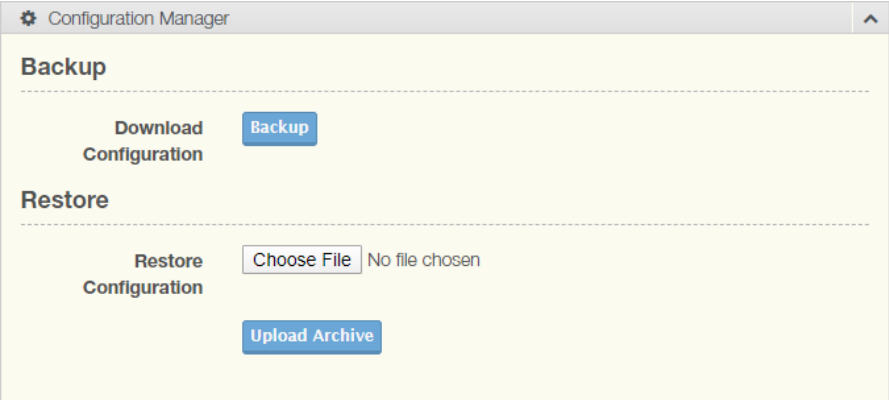


Figure 3.54 Management > Configuration Manager

The following table describes the items in the previous figure.

Item	Description
Backup	
Backup	Click **Backup** to export the device settings.
Restore	
Upload Archive	Click **Upload Archive** to select a previously saved configuration file.

3.6.7 Firmware Upgrade

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

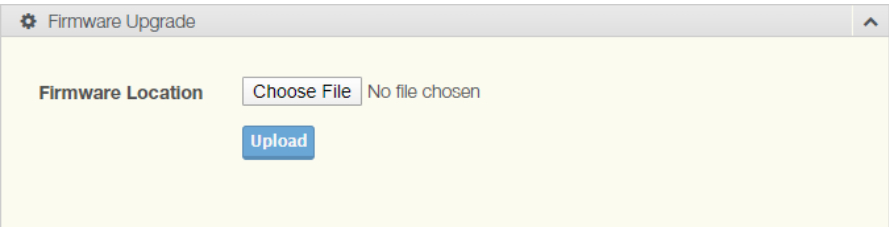


Figure 3.55 Management > Firmware Upgrade

The following table describes the items in the previous figure.

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

3.6.8 Reset System

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

Figure 3.56 Management > Apply Configuration

The following table describes the items in the previous figure.

Item	Description
Reset	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**.

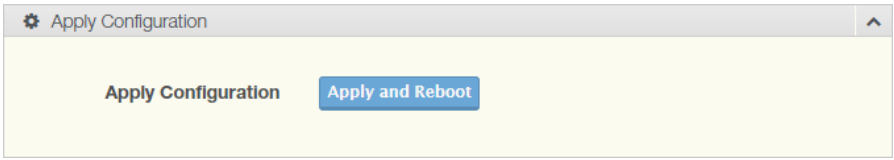


Figure 3.57 Management > Apply Configuration

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 3.58 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**.

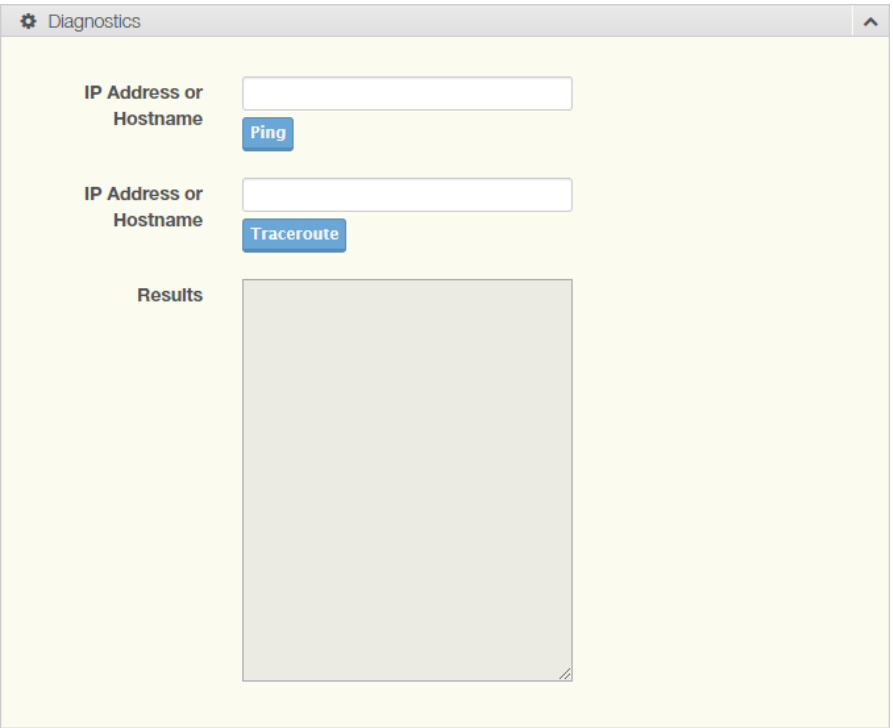


Figure 3.59 Tools > Diagnostics

The following table describes the items in the previous figure.

Item	Description
IP Address or Hostname	Enter the IP address or host name of the station to ping. The initial value is blank. The IP Address or host name you enter is not retained across a power cycle. Host names are composed of series of labels concatenated with periods. Each label must be between 1 and 63 characters long, maximum of 64 characters.
Ping	Click **Ping** to display ping result for the IP address.
IP Address or Hostname	Enter the IP address or host name of the station to ping. The initial value is blank. The IP Address or host name you enter is not retained across a power cycle. Host names are composed of series of labels concatenated with periods. Each label must be between 1 and 63 characters long, maximum of 64 characters.
Traceroute	Click **Traceroute** to track the pathway taken by a packet on the designated network from source to destination.
Results	Displays the results of the Ping or Traceroute function after initializing.

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. 2022