Edge-corE NETWORKS

Transceiver, Cable, Switch
Compatible List For Enterprise Switch

L3 Switch - ECS4620 series

Transceivers	ET4202-SX 1000BASE-SX	ET4202-LX 1000BASE-LX	ET4202-EX 1000BASE-EX	ET4202-ZX 1000BASE-ZX	ET4202-RJ45 1000BASE-T RJ45	ET5402-SR 10G SFP+ SR	ET5402-LR 10G SFP+ LR	ET5402-ER 10G SFP+ ER	ET5402-ZR 10G SFP+ ZR
ECS4620-52T	v	v	v	v	v	v	v	v	v
ECS4620-52P	v	v	v	v	v	v	v	v	v
ECS4620-28T	v	v	v	v	v	v	v	v	v
ECS4620-28P	v	v	v	v	v	v	v	v	v
ECS4620-28F	v	v	v	v	v	v	v	v	v

L3 Switch - ECS4620 series

Cables	ET5402-DAC-xM (1-5m) 10G SFP+ DAC	ET5402-AOC-xM (3-100m) 10G SFP+ AOC
ECS4620-52T	v	v
ECS4620-52P	v	v
ECS4620-28T	v	v
ECS4620-28P	v	v
ECS4620-28F	v	v

L2 Switch -ECS4150 series ECS4130 series, ECS4125 series, ECS4120 series,

Transceivers	ET4202-SX 1000BASE-SX	ET4202-LX 1000BASE-LX	ET4202-EX 1000BASE-EX	ET4202-ZX 1000BASE-ZX	ET4202-RJ45 1000BASE-T RJ45	ET4202-BD43-10-I 1000BASE-BD43	ET4202-BD34-10-I 1000BASE-BD34
ECS4150-28T	v	v					
ECS4150-28P	v	v					
ECS4130-28T	v	v	v	v	v	v	v
ECS4130-28T-DC	v	v	v	v	v	v	v
ECS4125-10P	v	v	v	v	v		
ECS4120-52T	v	v	v	v	v		
ECS4120-28T	v	v	v	v	v		
ECS4120-28Fv2	v	v	v	v	v		

	ET5402-SR 10G SFP+ SR	ET5402-LR 10G SFP+ LR	ET5402-ER 10G SFP+ ER	ET5402-ZR 10G SFP+ ZR	ET5402-RJ45 10GBASE-T RJ45
ECS4150-28T	v	v			v
ECS4150-28P	v	v			v
ECS4130-28T	v	v	v	v	
ECS4130-28T-DC	v	v	v	v	
ECS4125-10P	v	v	v	v	
ECS4120-52T	v	v	v	v	
ECS4120-28T	v	v	v	v	
ECS4120-28Fv2	v	v	v	v	

L2 Switch - ECS4100 series

Transceivers	ET4202-SX 1000BASE-SX	ET4202-LX 1000BASE-LX	ET4202-EX 1000BASE-EX	ET4202-ZX 1000BASE-ZX	ET4202-RJ45 1000BASE-T RJ45
ECS4100-52T	v	v	v	v	v
ECS4100-52P	v	v	v	v	v
ECS4100-28TC	v	v	v	v	v
ECS4100-28T	v	v	v	v	v
ECS4100-28P	v	v	v	v	v
ECS4100-12T	v	v	v	v	v
ECS4100-12PH	v	v	v	v	v

L2 Switch - ECS5520 series, ECS4530-54CSFP, ECS4120-28Fv2-I

Transceivers	ET4202-SX 1000BASE-SX	ET4202-LX 1000BASE-LX	ET4202-EX 1000BASE-EX	ET4202-ZX 1000BASE-ZX	ET4202-RJ45 1000BASE-T RJ45	ET4202-SXI 1000BASE-SX (I-temp)	ET4202-LXI 1000BASE-LX (I-temp)	ET4202-EXI 1000BASE-EX (I-temp)	ET4202-ZXI 1000BASE-ZX (I-temp)
ECS5520-18X	v	v	v	v	v	v	v	v	v
ECS5520-18T									
ECS4530-54CSFP	v	v	v	v	v	v	v	v	v
ECS4120-28Fv2-I	v	v	v	v	v	v	v	v	v

	ET4202-RJ45I 1000BASE-T RJ45 (I-temp)	ET4202-CSFP4310I 1000BASE-CSFP 10KM	ET4202-CSFP4320I 1000BASE-CSFP 20KM	ET4202-CSFP4340I 1000BASE-CSFP 40KM	ET5402-SR 10G SFP+ SR	ET5402-LR 10G SFP+ LR	ET5402-ER 10G SFP+ ER	ET5402-ZR 10G SFP+ ZR	ET5402-SRI 10G SFP+ SR (I-temp)
ECS5520-18X	v				v	v	v	v	v
ECS5520-18T									
ECS4530-54CSFP	v	v	v	v	v	v	v	v	v
ECS4120-28Fv2-I	v				v	v	v	v	v

	ET5402-LRI 10G SFP+ LR (I-temp)	ET5402-ERI 10G SFP+ ER (I-temp)	ET5402-ZRI 10G SFP+ ZR (I-temp)	ET6401-SR4 40G QSFP+ SR4	ET6401-LR4 40G QSFP+ LR4
ECS5520-18X	v	v	v	v	v
ECS5520-18T				v	v
ECS4530-54CSFP	v	v	v		
ECS4120-28Fv2-I	v	v	v		

L2 Switches

Cables	ET5402-DAC-xM (1-5m) 10G SFP+ DAC	ET5402-AOC-xM (3-100m) 10G SFP+ AOC	ET5402-AOC-3MI 10G SFP+ AOC	ET6402-DAC-xM (1-5m) 40G QSFP+ DAC	ET6402-10DAC-xM (1-5m) 40G QSFP+ AOC	ET6402-AOC-xM (3-100m) 40G QSFP+ AOC	ET6402-10AOC-xM (3-100m) 40G QSFP+ AOC
ECS5520-18X	v	v	v	v	v	v	v
ECS5520-18T				v	v	v	v
ECS4530-54CSFP		v					
ECS4150-28T	v	v					
ECS4150-28P	v	v					
ECS4130-28T		v	v				
ECS4130-28T-DC		v	v				
ECS4125-10P	v	v					
ECS4120-52T	v	v					
ECS4120-28T		v					
ECS4120-28Fv2	v	v					
ECS4120-28Fv2-I	v	v					

Web-smart Pro Switch - ECS2100 series

Transceivers	ET4202-SX 1000BASE-SX	ET4202-LX 1000BASE-LX	ET4202-EX 1000BASE-EX	ET4202-ZX 1000BASE-ZX	ET4202-RJ45 1000BASE-T RJ45
ECS2100-52T	v	v	v	v	v
ECS2100-28T	v	v	v	v	v
ECS2100-28P	v	v	v	v	v
ECS2100-28PP	v	v	v	v	v
ECS2100-10T	v	v	v	v	v
ECS2100-10P	v	v	v	v	v
ECS2100-10PE	v	v	v	v	v

Web-smart Switch - ECS2020 series

Transceivers	ET4202-SX 1000BASE-SX	ET4202-LX 1000BASE-LX	ET4202-EX 1000BASE-EX	ET4202-ZX 1000BASE-ZX	ET4202-RJ45 1000BASE-T RJ45
ECS2020-28T	v	v	v	v	v
ECS2020-28P	v	v	v	v	v
ECS2020-10T	v	v	v	v	v
ECS2020-10P	v	v	v	v	v

Industrial Switch - ECIS4500 series

Transceivers	ET4202-SXI 1000BASE-SX	ET4202-LXI 1000BASE-LX	ET4202-EXI 1000BASE-EX	ET4202-ZXI 1000BASE-ZX	ET4202-RJ45I 1000BASE-T RJ45
ECIS4500-8T2F	v	v	v	v	v
ECIS4500-6T2F	v	v	v	v	v
ECIS4500-6T4F	v	v	v	v	v
ECIS4500-4P4T	v	v	v	v	v
ECIS4500-4P2T2F	v	v	v	v	v
ECIS4500-8P4F	v	v	v	v	v
ECIS4500-8P2T4F	v	v	v	v	v

LETTER OF AUTHORIZATION

Date: July 1st, 2025

Re: Letter of Authorization of Official Non-exclusive Project Partner to Padtec SA for Edgecore Product Lines in Brazil.

We, Edgecore Networks Corporation, the developer and manufacturer of wired and wireless networking products.

We, are hereby duly authorized non-exclusive right to Padtec SA, registered office at R. Dr. Ricardo Benetton Martins, 1000, Parque II do Polo de Alta Tecnologia, Campinas - SP, 13086-510, Brazil to use our brand "Edgecore" and product manufactured by us to submit the Tender/RFP/EOI in Brazil as follows. We also state that Edgecore is not established in Brazil.

PREFEITURA DE CÁCERES

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

AV. Brasil, 119, COC, Bairro Jardim Celeste, Cáceres/MT, Cep 78.210-906

Project Title: Processo Administrativo nº 29/2025

Bid No: Pregão Eletrônico 90015/2025

The Letter of Authorization will become effective from now until the termination of the contract or early termination of the foresaid Project/Bid.

Your sincerely,

..... President

Edgecore Networks Corporation

鈺登科技股份有限公司
Edgecore Networks Corporation
www.edge-core.com

NCA-1250

Multi-core x86 Network Appliance With
Intel® Alder Lake N, Amston Lake Or Twin Lake

Images are for refernce only. See ordering information for SKU details.

Features

- Intel® Atom® x7425E/x7405C/x7835RE & Processor N97/N250/N150
- DDR5 4800MT/s, SODIMM, Max. 16GB
- 6x 2.5GbE RJ45 (By SKU), 1x USB 3.0, 1x Console
- 1x M.2 (SATA) 2280, 1x EMMC 16GB Onboard (By SKU)
- 1x M.2 3042/3050/3052 For 5G/LTE (USB3.2), 1x M.2 2230 E Key For Intel AX201 (CNVIo) (SKU A/B)

Specifications

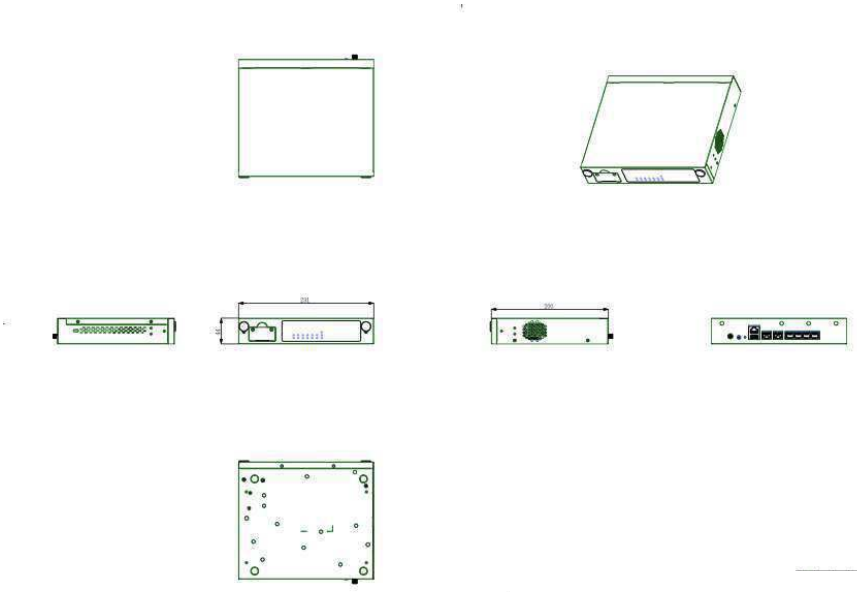
Platform	
Form Factor	Desktop
Processor Options	Intel® Atom® x7425E/N97(Alder Lake N) x7405C/x7835RE (Amston Lake) N250/N150 (Twin Lake)
CPU Socket	Onboard
Chipset	SoC
Security Acceleration	N/A
BIOS	AMI SPI Flash BIOS
System Memory	
Technology	DDR5 4800MT/s SODIMM
Max. Capacity	16GB
Socket	1 x 262-pin SODIMM
Networking	
Ethernet Ports	SKU A: 6 x 2.5GbE RJ45 LAN Ports SKU B: 5 x 2.5GbE RJ45 LAN Ports SKU C: 6 x 2.5GbE RJ45 LAN Ports SKU D: 6 x 2.5GbE RJ45 LAN Ports SKU E: 5 x 2.5GbE RJ45 LAN Ports SKU F: 5 x 2.5GbE RJ45 LAN Ports
Bypass	N/A
NIC Module Slot	N/A
LOM	
IO Interface	N/A
OPMA Slot	N/A
I/O Interface	
Reset Button	1
LED	Power/Status/Storage
Power Button	1
Console	1 x RJ45
USB	1 x USB 3.0
LCD Module	N/A
Display	N/A
Power Input	1 x DC Jack
Storage	
HDD/SSD Support	N/A
Onboard Slots	1 x M.2 (SATA) 2280 1 x EMMC 16GB onboard (SKU A/C/D/E/F)
Expansion	
PCIe	N/A
Mini-PCIe/M.2/SIM	1 x M.2 3042/3050/3052 For 5G/LTE (USB3.2) 1 x M.2 2230 E Key For Intel AX201 (CNVIo, SKU A/B Only) 1 x Nano SIM
PGN Module	N/A
Miscellaneous	
Watchdog	Yes
Internal RTC with Li Battery	Yes
TPM	Yes (SKU A/C/D/E/F)
Cooling	
Processor	Passive CPU Heatsink
System	Fanless
Environmental Parameters	
Temperature	0~40°C Operating -20~70°C Non-Operating
Humidity (RH)	10~90% Operating 5~95% Non-Operating
System Dimensions	
(WxHxD)	231 x 44 x 200 mm
Weight	1.1 kg
Package Dimensions	
(WxHxD)	358 x 290 x 135 mm
Weight	2.3 kg
Power	
Type / Watts	12V 40W Power Adapter
Input	AC 100~240V@50~60Hz
Certification	
Approvals and Compliance	RoHS, CE/FCC Class B

Product I/O View

Images are for refernce only. See ordering information for SKU details.

- **A** DC Jack With Lock
- **B** Power Button
- **C** Reset Button
- **D** Console & USB
- **E** 6x 2.5GbE RJ45 (SKU A/C/D) Or 5x 2.5GbE RJ45 (SKU B/E/F)
- **F** SIM Cover
- **G** LAN LED
- **H** Status LED

Dimensions (WxDxH): 231 x 200 x 44 mm



Ordering Information

NCA-1250A	Intel x7425E 4-Core With 6x 2.5GbE RJ45 LAN Ports, 1x TPM Onboard, Wi-Fi/LTE/5G Modules Support
NCA-1250B	Intel N97 4-Core With 5x 2.5GbE RJ45 LAN Ports, 1x TPM (By Project), Wi-Fi/LTE/5G Modules Support
NCA-1250C	Intel x7405C 4-Core With 6x 2.5GbE RJ45 LAN Ports, 1x TPM Onboard, LTE/5G Modules Support
NCA-1250D	Intel x7835RE 8-Core With 6x 2.5GbE RJ45 LAN Ports, 1x TPM Onboard, LTE/5G Modules Support
NCA-1250E	Intel N250 4-Core With 5x 2.5GbE RJ45 LAN Ports, 1x TPM Onboard, LTE/5G Modules Support
NCA-1250F	Intel N150 4-Core With 5x 2.5GbE RJ45 LAN Ports, 1x TPM Onboard, LTE/5G Modules Support

V1-2025.05.22

Lanner

Lanner

Network Appliance Platform

Hardware Platforms for Network Computing

NCA-1250
User Manual

Version: 1.4

Date of Release: 2025-05-20

About this Document

This manual describes the overview of the various functionalities of this product, and the information you need to get it ready for operation. It is intended for those who are:

- responsible for installing, administering and troubleshooting this system or Information Technology professionals.
- assumed to be qualified in the servicing of computer equipment, such as professional system integrators, or service personnel and technicians.

The latest version of this document can be found on Lanner's official website, available either through the product page or through the Lanner Download Center page with a login account and password.

Icon Description

The icons are used in the manual to serve as an indication of interest topics or important messages. Below is a description of these icons:

Icon	Usage
 **Note or Information**	This mark indicates that there is something you should pay special attention to while using the product.
 **Warning or Important**	This mark indicates that there is a caution or warning and it is something that could damage your property or product.

Online Resources

To obtain additional documentation resources and software updates for your system, please visit the Lanner Download Center. As certain categories of documents are only available to users who are logged in, please be registered for a Lanner Account at http://www.lannerinc.com/ to access published documents and downloadable resources.

Technical Support

In addition to contacting your distributor or sales representative, if there are any technical queries, you could submit a support ticket to our Lanner Technical Support department.

Documentation Feedback

Your feedback is valuable to us, as it will help us continue to provide you with more accurate and relevant documentation. To provide any feedback, comments or to report an error, please email to contact@lannerinc.com. Thank you for your time.

Contact Information

Taiwan Corporate Headquarters

Lanner Electronics Inc.

7F, No.173, Sec.2, Datong Rd.

Xizhi District, New Taipei City 22184,

Taiwan

立端科技股份有限公司

221 新北市汐止區

大同路二段 173 號 7 樓

T: +886-2-8692-6060

F: +886-2-8692-6101

E: contact@lannerinc.com

China

Beijing L&S Lancom Platform Tech. Co., Ltd.

Guodong LOFT 9 Layer No. 9 Huinan Road,

Huilongguan Town, Changping District, Beijing

102208 China

T: +86 010-82795600

F: +86 010-62963250

E: service@ls-china.com.cn

USA

Lanner Electronics Inc.

47790 Westinghouse Drive

Fremont, CA 94539

T: +1-855-852-6637

F: +1-510-979-0689

E: sales_us@lannerinc.com

Canada

Lanner Electronics Canada Ltd

3160A Orlando Drive

Mississauga, ON

L4V 1R5 Canada

T: +1 877-813-2132

F: +1 905-362-2369

E: sales_ca@lannerinc.com

Europe

Lanner Europe B.V.

Wilhelmina van Pruisenweg 104

2595 AN The Hague

The Netherlands

T: +31 70 701 3256

E: sales_eu@lannerinc.com

Copyright and Trademarks

Acknowledgment

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of 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 instruction, 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 or more 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 transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Note

1. An unshielded-type power cord is required in order to meet FCC emission limits and also to prevent interference to the nearby radio and television reception. It is essential that only the supplied power cord be used.
2. Use only shielded cables to connect I/O devices to this equipment.
3. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Important

1. Operations in the 5.15-5.25GHz band are restricted to indoor usage only.
2. This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

Safety Guidelines

Follow these guidelines to ensure general safety:

- Keep the chassis area clear and dust-free during and after installation.
- Do not wear loose clothing or jewelry that could get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Disconnect all power by turning off the power and unplugging the power cord before installing or removing a chassis or working near power supplies
- Do not work alone if potentially hazardous conditions exist.
- Never assume that power is disconnected from a circuit; always check the circuit.

Consignes de sécurité

Suivez ces consignes pour assurer la sécurité générale :

- Laissez la zone du châssis propre et sans poussière pendant et après l'installation.
- Ne portez pas de vêtements amples ou de bijoux qui pourraient être pris dans le châssis. Attachez votre cravate ou écharpe et remontez vos manches.
- Portez des lunettes de sécurité pour protéger vos yeux.
- N'effectuez aucune action qui pourrait créer un danger pour d'autres ou rendre l'équipement dangereux.
- Coupez complètement l'alimentation en éteignant l'alimentation et en débranchant le cordon d'alimentation avant d'installer ou de retirer un châssis ou de travailler à proximité de sources d'alimentation.
- Ne travaillez pas seul si des conditions dangereuses sont présentes.
- Ne considérez jamais que l'alimentation est coupée d'un circuit, vérifiez toujours le circuit. Cet appareil génère, utilise et émet une énergie radiofréquence et, s'il n'est pas installé et utilisé conformément aux instructions des fournisseurs de composants sans fil, il risque de provoquer des interférences dans les communications radio.

Lithium Battery Caution

- There is risk of explosion if the battery is replaced by an incorrect type.
- Dispose of used batteries according to the instructions.
- Installation should be conducted only by a trained electrician or only by an electrically trained person who knows all installation procedures and device specifications which are to be applied.
- Do not carry the handle of power supplies when moving to another place.
- Please conform to your local laws and regulations regarding safe disposal of lithium battery.
- Disposal of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery can result in an explosion.
- Leaving a battery in an extremely high temperature environment can result in an explosion or the leakage of flammable liquid or gas.
- A battery subjected to extremely low air pressure may result in an explosion or the leakage of flammable liquid or gas.

Avertissement concernant la pile au lithium

- Risque d'explosion si la pile est remplacée par une autre d'un mauvais type.
- Jetez les piles usagées conformément aux instructions.
- L'installation doit être effectuée par un électricien formé ou une personne formée à l'électricité connaissant toutes les spécifications d'installation et d'appareil du produit.
- Ne transportez pas l'unité en la tenant par le câble d'alimentation lorsque vous déplacez l'appareil.

Operating Safety

- Electrical equipment generates heat. Ambient air temperature may not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Be sure that the room in which you choose to operate your system has adequate air circulation.
- Ensure that the chassis cover is secure. The chassis design allows cooling air to circulate effectively. An open chassis permits air leaks, which may interrupt and redirect the flow of cooling air from internal components.
- Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. ESD damage occurs when electronic components are improperly handled and can result in complete or intermittent failures. Be sure to follow ESD-prevention procedures when removing and replacing components to avoid these problems.

- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. If no wrist strap is available, ground yourself by touching the metal part of the chassis.
- Periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohms (Mohms).

Sécurité de fonctionnement

- L'équipement électrique génère de la chaleur. La température ambiante peut ne pas être adéquate pour refroidir l'équipement à une température de fonctionnement acceptable sans circulation adaptée. Vérifiez que votre site propose une circulation d'air adéquate.
- Vérifiez que le couvercle du châssis est bien fixé. La conception du châssis permet à l'air de refroidissement de bien circuler. Un châssis ouvert laisse l'air s'échapper, ce qui peut interrompre et rediriger le flux d'air frais destiné aux composants internes.
- Les décharges électrostatiques (ESD) peuvent endommager l'équipement et gêner les circuits électriques. Des dégâts d'ESD surviennent lorsque des composants électroniques sont mal manipulés et peuvent causer des pannes totales ou intermittentes. Suivez les procédures de prévention d'ESD lors du retrait et du remplacement de composants.
- Portez un bracelet anti-ESD et veillez à ce qu'il soit bien au contact de la peau. Si aucun bracelet n'est disponible, reliez votre corps à la terre en touchant la partie métallique du châssis.
- Vérifiez régulièrement la valeur de résistance du bracelet antistatique, qui doit être comprise entre 1 et 10 mégohms (Mohms).

Mounting Installation Precautions

The following should be put into consideration for rack-mount or similar mounting installations:

- Do not install and/or operate this unit in any place that flammable objects are stored or used in.
- The installation of this product must be performed by trained specialists; otherwise, a non-specialist might create the risk of the system's falling to the ground or other damages.
- Lanner Electronics Inc. shall not be held liable for any losses resulting from insufficient strength for supporting the system or use of inappropriate installation components.
- Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
- Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Reliable Grounding - Reliable grounding of rack mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Installation & Operation

- This equipment must be grounded. The power cord for product should be connected to a socket-outlet with earthing connection.
  Cet équipement doit être mis à la terre. La fiche d'alimentation doit être connectée à une prise de terre correctement câblée
- Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75.
  Peut être installé dans des salles de matériel de traitement de l'information conformément à l'article 645 du National Electrical Code et à la NFPA 75.
- The machine can only be used in a restricted access location and must be installed by a skilled person.
  Les matériels sont destinés à être installés dans des EMPLACEMENTS À ACCÈS RESTREINT.
- Some USB devices may not be compatible with the system. If you encounter an error, please remove the USB device and restart the system.
- The unit is to be connected only to PoE networks without routing to the outside plant.

Warning

- Class I Equipment. This equipment must be earthed. The power plug must be connected to a properly wired earth ground socket outlet. An improperly wired socket outlet could place hazardous voltages on accessible metal parts.
- Product shall be used with Class 1 laser device modules.

Avertissement

- Équipement de classe I. Ce matériel doit être relié à la terre. La fiche d'alimentation doit être raccordée à une prise de terre correctement câblée. Une prise de courant mal câblée pourrait induire des tensions dangereuses sur des parties métalliques accessibles.
- Le produit doit être utilisé avec des modules de dispositifs laser de classe 1."

Electrical Safety Instructions

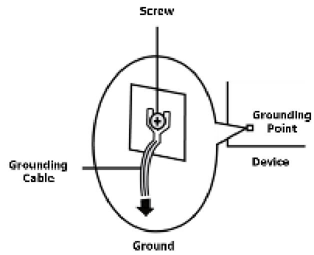
Before turning on the device, ground the grounding cable of the equipment. Proper grounding (grounding) is very important to protect the equipment against the harmful effects of external noise and to reduce the risk of electrocution in the event of a lightning strike. To uninstall the equipment, disconnect the ground wire after turning off the power. A ground wire (green-and-yellow) is required and the part connecting the conductor must be greater than 4 mm2 or 10 AWG.

Consignes de sécurité électrique

- Avant d'allumer l'appareil, reliez le câble de mise à la terre de l'équipement à la terre.
- Une bonne mise à la terre (connexion à la terre) est très importante pour protéger l'équipement contre les effets néfastes du bruit externe et réduire les risques d'électrocution en cas de foudre.
- Pour désinstaller l'équipement, débranchez le câble de mise à la terre après avoir éteint l'appareil.
- Un câble de mise à la terre est requis et la zone reliant les sections du conducteur doit faire plus de 4 mm2 ou 10 AWG.

Grounding Procedure for DC Power Source

- Connect the grounding cable to the ground.
- The protection device for the DC power source must provide 30 A current.
- This protection device must be connected to the power source before DC power.



Procédure de mise à la terre pour source d'alimentation CC

- Branchez le câble de mise à la terre à la terre.
- L'appareil de protection pour la source d'alimentation CC doit fournir 30 A de courant.
- Cet appareil de protection doit être branché à la source d'alimentation avant l'alimentation CC.

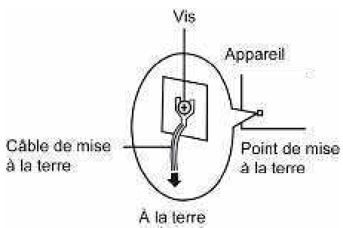


Table of Contents

CHAPTER 1: PRODUCT OVERVIEW

The NCA-1250 offers robust multi-core computing power in a compact desktop form factor. It can be configured with Intel® Atom® Processor X-series and processor N-series, codenamed Alder Lake N, Amston Lake, and Twin Lake platform, making it a cost-effective gateway platform for SMB, retail, branch offices and those looking to deploy any edge security application.

Package Content

Your package contains the following items:

- 1x NCA-1250 Network Appliance
- 1x Power Cable
- 1x Console Cable
- 1x Power Adapter
- 1x Nameplate & 4x rubber foot pads

Note: (1) If any component is missing or damaged, please contact your dealer immediately for assistance. (2) The supplied power adapter and power cable are dedicated to this product only; do not use them with devices other than this model.

Ordering Information

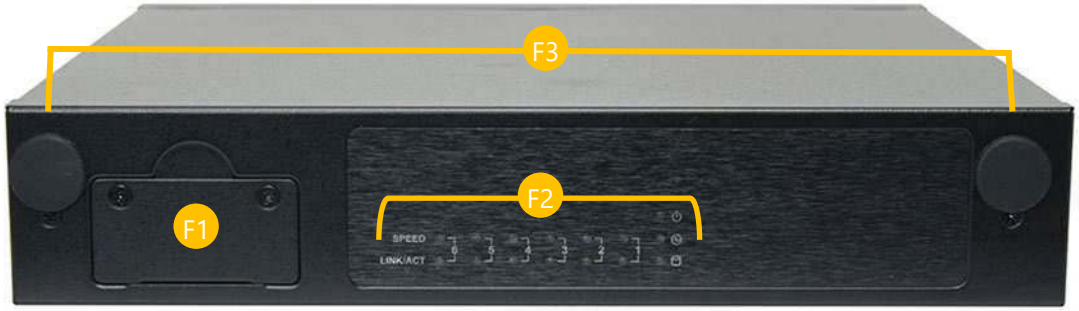
SKU No.	Specification
NCA-1250A	Intel® x7425E/4 Cores with 6x 2.5GbE RJ45 LAN Ports, 1x TPM (Onboard), Wi-Fi/LTE/5G Modules Support
NCA-1250B	Intel® N97/4 Cores with 5x 2.5GbE RJ45 LAN Ports, 1x TPM (By Project), Wi-Fi/LTE/5G Modules Support
NCA-1250C	Intel® x7405C/4Cores with 6x 2.5GbE RJ45 LAN Ports, 1x TPM (Onboard), LTE/5G Module Support
NCA-1250D	Intel® x7835RE/8 Cores with 6x 2.5GbE RJ45 LAN Ports, 1x TPM (Onboard), LTE/5G Module Support
NCA-1250E	Intel® N250/4 Cores with 5x 2.5GbE RJ45 LAN Ports, 1x TPM (Onboard), LTE/5G Modules Support
NCA-1250F	Intel® N150/4 Cores with 5x 2.5GbE RJ45 LAN Ports, 1x TPM (Onboard), LTE/5G Modules Support

System Specifications

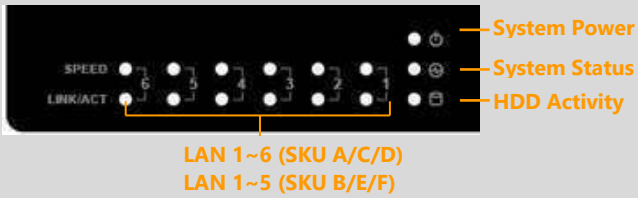
Form Factor		Desktop
Platform	Processor Options	Intel® Atom® x7425E/N97 (Alder Lake N)/ x7405C/x7835RE (Amston Lake)/ N250/N150 (Twin Lake)
	CPU Socket	Onboard
	Chipset	SoC
BIOS		AMI SPI Flash BIOS
System Memory	Technology	DDR5 4800MT/s SODIMM
	Max. Capacity	Up to 16GB
	Socket	1x 262-Pin SODIMM
Networking	Ethernet Ports	SKU A/C/D: 6x 2.5GbE RJ45 LAN Ports; SKU B/E/F: 5x 2.5GbE RJ45 LAN Ports
LOM	IO Interface	N/A
	OPMA slot	N/A
I/O Interface	Reset Button	1x Reset Button
	LED Indicator	Power/Status/Storage LED Indicator
	Power Button	1x Power Button
	Console Port	1x RJ45 Console Port
	USB Port	1x USB 3.0 Port
	Power input	1x DC Power Adaptor
Storage	HDD/SSD Support	N/A
	Onboard Slots	1x M.2 2280 for SATA 1x EMMC 16GB Onboard (SKU A/C/D/E/F)
Expansion	Mini-PCIe/M.2	1x M.2 3042/3050/3052 for 5G/LTE (USB3.2); 1x M.2 2230 E-Key for Wi-Fi6/BT (CNVIO, SKU A/B Only)
	SIM Card Slot	1x Nano SIM Card Slot
Miscellaneous	Watchdog	Yes
	Internal RTC w/ Li-Battery	Yes
	TPM	TPM 2.0 Onboard (SKU A/C/D/E/F Only)
Cooling	Processor	Passive CPU heatsink
	System	Fanless
Environmental Parameters	Temperature	0~40ºC Operating; -20~70ºC Non-Operating
	Humidity (RH)	10% to 90% Operating; 5% to 95% Non-Operating
System Dimensions	(WxDxH)	231 x 44 x 200mm
	Weight	1.1 kg
Package Dimensions	(WxDxH)	358 x 290 x 135mm
	Weight	2.3 kg (8.2kg/3-in-1)
Power	Type/Watts	12V/3.3A, 40W Power Adapter
	Input	AC 100~240V @50~60 Hz
Approvals and Compliance		RoHS, CE/FCC Class B

Front Panel

NCA-1250A/C/D

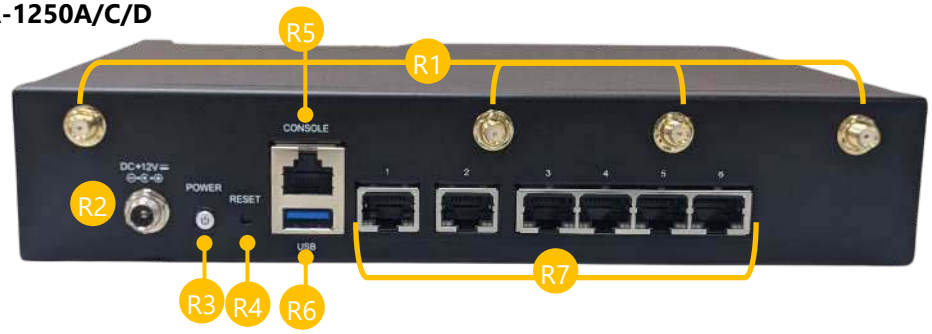


NCA-1250B/E/F

No.	Description	
F1	SIM Card Slot	SIM Card Slot Cover
F2	LED Indicators	
F3	Antenna Port	2x Antenna Holes for 5G Module (Optional)

Rear Panel

NCA-1250A/C/D



NCA-1250B/E/F

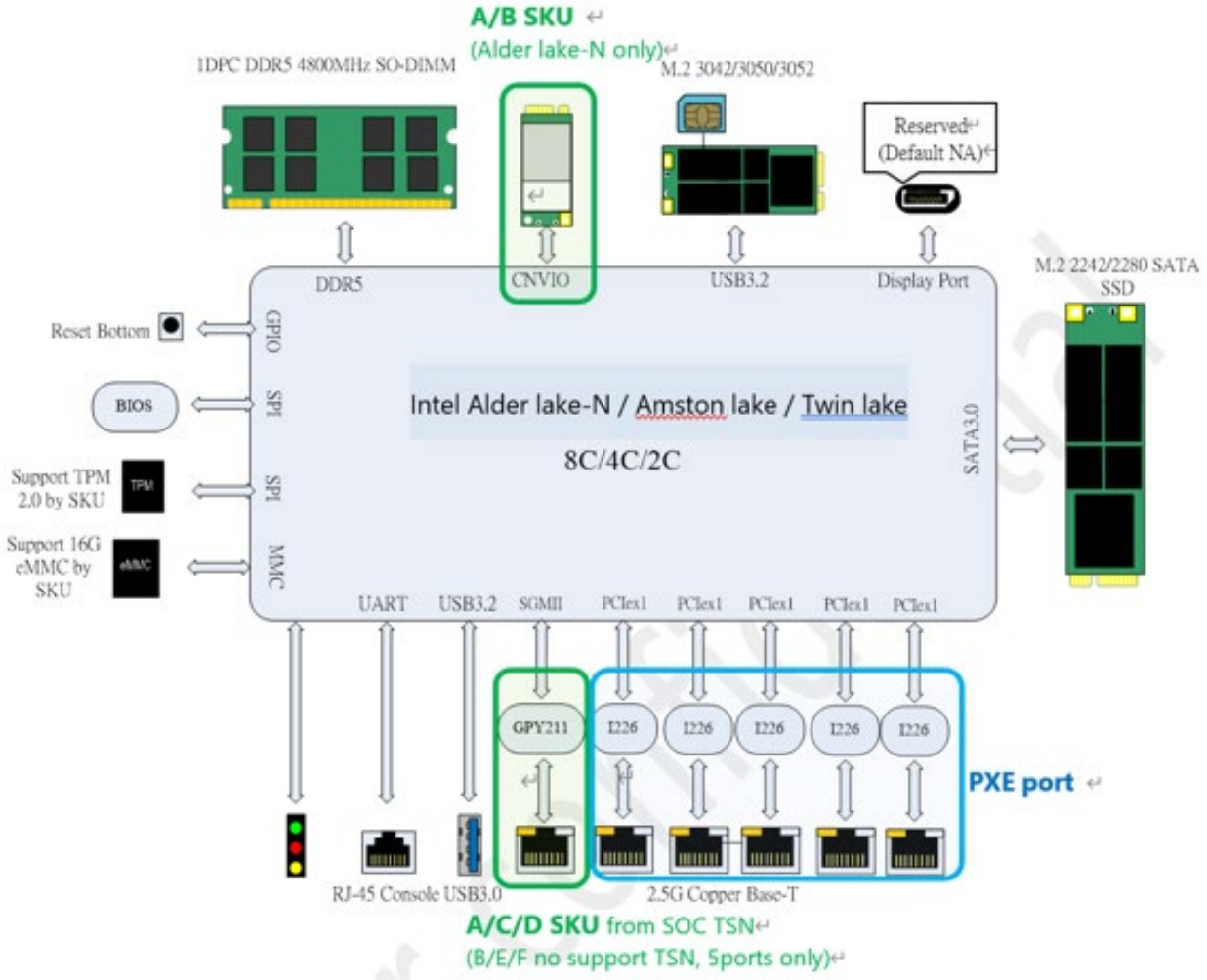
No.	Description	
R1	Antenna Port	SMA Connector for the Wi-Fi and 5G/LTE Module (Optional)
R2	Power Supply	1x DC Jack with Lock
R3	Power Button	1x Power ON/OFF Button
R4	Reset Button	1x Reset Button (Software Reset)
R5	Console Port	1x GbE RJ45 Console Port
R6	USB Port	1x Type A USB 3.0 Port
R7	LAN Port	5x or 6x 2.5GbE RJ45 Ethernet Ports with LED Indicators (By SKU)

NOTE: For LAN ports support PXE function, pls refer to Appendix C.

CHAPTER 2: MOTHERBOARD INFORMATION

Block Diagram

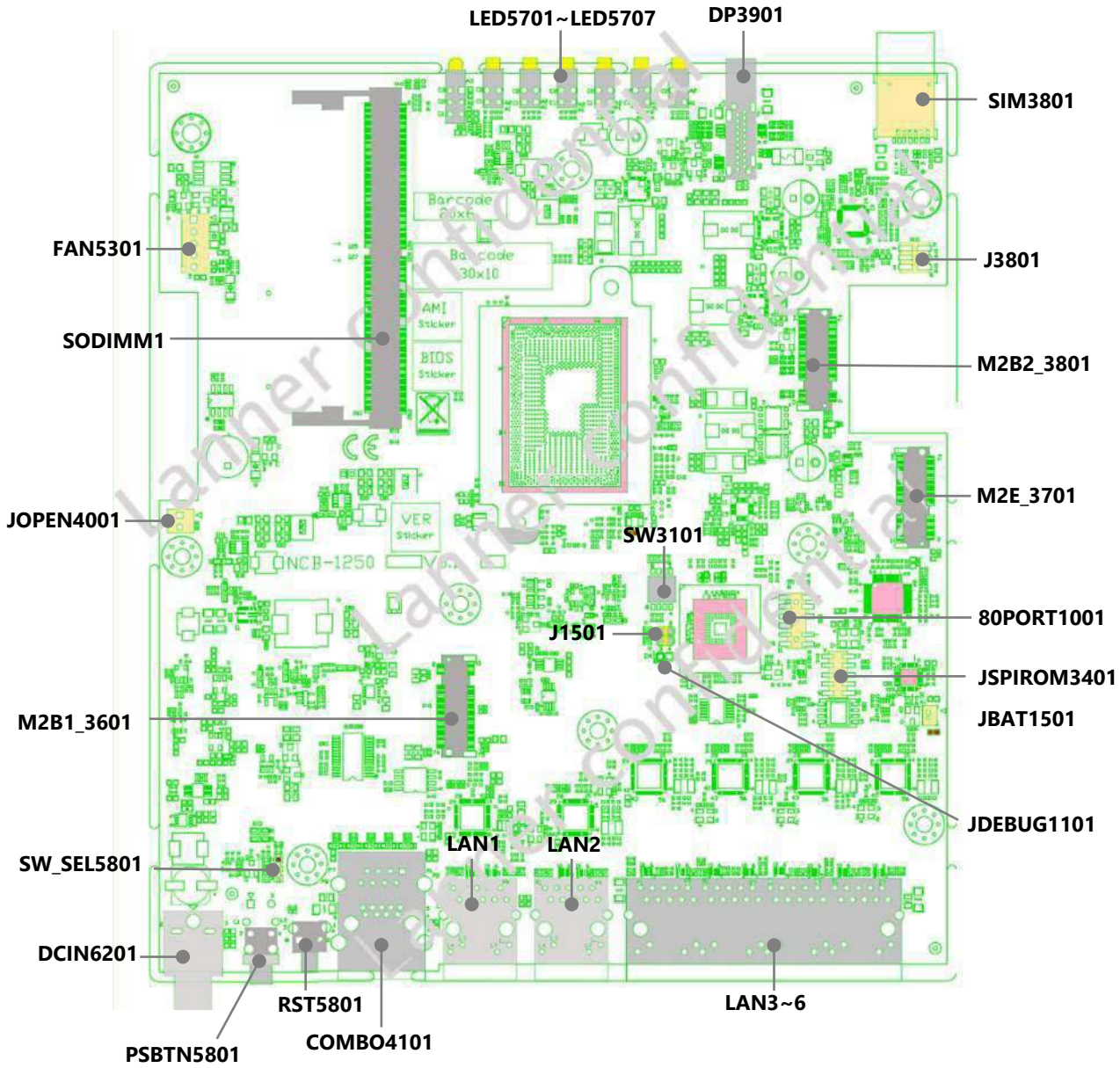
The block diagram indicates how data flows among components on the motherboard. Please refer to the following figure for your motherboard's layout design.



Motherboard Layout

The layout of the motherboard illustrates the positions of connectors and jumpers. Use the accompanying picture for guidance on pin assignments and internal connections.

Top Side of Motherboard



Bottom Side of Motherboard

Jumper Setting and Pin Assignment

J3801: 5G Module Setting

PIN NO.	DESCRIPTION
1	M2B2_OPT_VCC
2	3V3
3	M2B2_P22_VBUS_SENSE
4	3V3
5	M2B2_P20_PCIE_DIS
6	1V8

Matching Table of Jumper Settings and Modules below,

V = install jumper

X = NC

Latch	EM9291	EM9191	Others
(1-2)	V	x	x
(3-4)	x	V	x
(5-6)	x	V	x

SW3101: Debug Setting

PIN NO.	DESCRIPTION
1	SOC_GPP_R2_R
2	SOC_GPP_B18_R
3	NC
4	NC
5	NC
6	NC
7	3V3
8	+P3V3_1V8_VCCPGPPR

Latch 1 (pin 1-8): ON for debug use; OFF for normal operating(default).

Latch 2 (pin 2-7): ON for debug use; OFF for normal operating(default).

Latch 3 (pin 3-6): no function, set switch to OFF as default.

Latch 4 (pin 4-5): no function, set switch to OFF as default

80PORT1001: 80 Port

PIN NO.	DESCRIPTION
1	ESPI_CLK
2	ESPI_IO1
3	ESPI_RST
4	ESPI_IO0
5	ESPI_CS
6	3V3_S0
7	ESPI_IO3
8	LATCH
9	ESPI_IO2
10	GND
11	3V3_SB
12	NC

JSPIROM3401

PIN NO.	DESCRIPTION
1	BIOS1_HOLD
2	NC
3	BIOS1_CS
4	3V3
5	BIOS1_SO
6	NC
7	NC
8	BIOS1_SCK
9	GND
10	BIOS1_SI

JBAT1501

PIN NO.	DESCRIPTION
1	VBAT
2	GND

J1501: CMOS Setting

PIN NO.	DESCRIPTION
1	RTCRST
2	GND
3	SRTCRST
4	GND

(1-2): Short for clear CMOS, NC for normal operating.

(3-4): Short for clear CMOS, NC for normal operating.

JDEBUG1101

PIN NO.	DESCRIPTION
1	SOC_UART0_TXD
2	GND

FAN5301

PIN NO.	DESCRIPTION
1	GND
2	12V
3	FAN_TACH
4	NC
5	FAN_PWM

JOPEN4001

PIN NO.	DESCRIPTION
1	GND
2	SIO_CASEOPEN

JSW_SEL5801

(1-2): SW Reset, Default Setting.

(2-3): HW Reset.

PIN NO.	DESCRIPTION
1	SW_RESET
2	BTN_RESET
3	HW_RESET

DCIN6201

PIN NO.	DESCRIPTION
1	12V
2	GND
3	GND

M2B2_3801

PIN NO.	DESCRIPTION	PIN NO.	DESCRIPTION
1	NC	38	M2B2_P38
2	3V3	39	GND
3	GND	40	NC
4	3V3	41	NC
5	GND	42	NC
6	F_CARD_POWER_OFF_N (default:1V8)	43	NC
7	USB2_TXP	44	NC
8	NC	45	GND
9	USB2_TXN	46	NC
10	NC	47	NC
11	GND	48	NC
12	LATCH	49	NC
13	LATCH	50	NC
14	LATCH	51	GND
15	LATCH	52	NC
16	LATCH	53	NC
17	LATCH	54	NC
18	LATCH	55	NC
19	LATCH	56	NC
20	M2B2_P20_PCIE_DIS	57	GND
21	NC	58	NC
22	M2B2_P22_VBUS_SENSE	59	NC
23	NC	60	NC
24	M2B2_P24	61	NC
25	NC	62	NC
26	GND	63	NC
27	GND	64	NC
28	NC	65	NC
29	USB3_RXN	66	SIM_DETECT (Default: NC)
30	SIM_RST	67	RESET
31	USB3_RXP	68	M2B2_P68
32	SIM_CLK	69	NC
33	GND	70	3V3
34	SIM_DAT	71	GND
35	USB3_TXN	72	3V3

36	SIM_VCC	73	GND
37	USB3_TXP	74	3V3
--	--	75	NC

M2E_3701

PIN NO.	DESCRIPTION	PIN NO.	DESCRIPTION
1	GND	39	GND
2	3V3	40	NC
3	NC	41	NC
4	3V3	42	NC
5	NC	43	NC
6	LED_WIFI_N	44	GND
7	GND	45	NC
8	NC	46	NC
9	CNVi_D1_RXN	47	NC
10	CNVi_RESET	48	NC
11	CNVi_D1_RXP	49	SUSCLK
12	NC	5-	GND
13	GND	51	NC
14	CNVi_CLKREQ_N	52	NC
15	CNVi_D0_RXN	53	NC
16	LED_BT_N	54	NC
17	CNVi_D0_RXP	55	NC
18	GND	56	GND
19	GND	57	NC
20	NC	58	CNVi_D1_TXN
21	CNVi_CLK_RXN	59	NC
22	CNVi_BRI_RSP	60	CNVi_D1_TXP
23	CNVi_CLK_RXP	61	NC
24	LATCH	62	GND
25	LATCH	63	NC
26	LATCH	64	CNVi_D0_TXN
27	LATCH	65	NC
28	LATCH	66	CNVi_D0_TXP
29	LATCH	67	NC
30	LATCH	68	GND
31	LATCH	69	NC
32	CNVi_RGI_DT	70	CNVi_CLK_TXN
33	GND	71	3V3
34	CNVi_RGI_RSP	72	CNVi_CLK_TXP
35	NC	73	3V3
36	CNVi_BRI_DT	74	GND
37	NC	75	GND
38	NC	--	--

M2B1_3601

PIN NO.	DESCRIPTION	PIN NO.	DESCRIPTION
1	NC	39	GND
2	3V3	40	NC
3	GND	41	SATA3_RXP
4	3V3	42	NC
5	GND	43	SATA3_RXN

6	NC	44	NC
7	NC	45	GND
8	NC	46	NC
9	NC	47	SATA3_TXN
10	NC	48	NC
11	NC	49	SATA3_TXP
12	LATCH	5-	NC
13	LATCH	51	GND
14	LATCH	52	NC
15	LATCH	53	NC
16	LATCH	54	NC
17	LATCH	55	NC
18	LATCH	56	NC
19	LATCH	57	GND
20	NC	58	NC
21	NC	59	NC
22	NC	60	NC
23	NC	61	NC
24	NC	62	NC
25	NC	63	NC
26	NC	64	NC
27	GND	65	NC
28	NC	66	NC
29	NC	67	NC
30	NC	68	NC
31	NC	69	NC
32	NC	70	3V3
33	GND	71	GND
34	NC	72	3V3
35	NC	73	GND
36	NC	74	3V3
37	NC	75	GND
38	GND	--	--

CHAPTER 3 HARDWARE INSTALLATION

For your safety and to prevent electric shock or damage to the system, ensure all power connections are disconnected to completely power off the device. Additionally, wear ESD protection gloves while performing the procedures outlined in this chapter.

Opening the Chassis

1. Power off the system and remove all power connections.
2. Locate and remove the six (6) screws on the right, left, and bottom side.

Right Side

Left Side

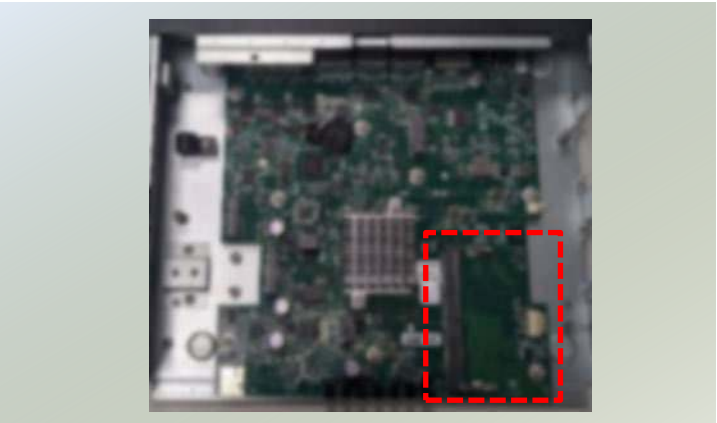
Bottom Side

3. Gently slide the chassis cover away from the system and lift the cover to remove.

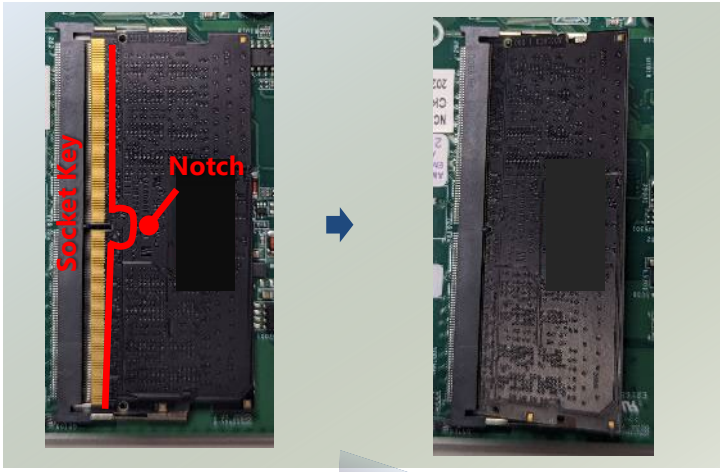
Installing System Memory

The motherboard supports one DDR5 SODIMM with speeds of up to 4800MT/s. Please follow the steps for installation

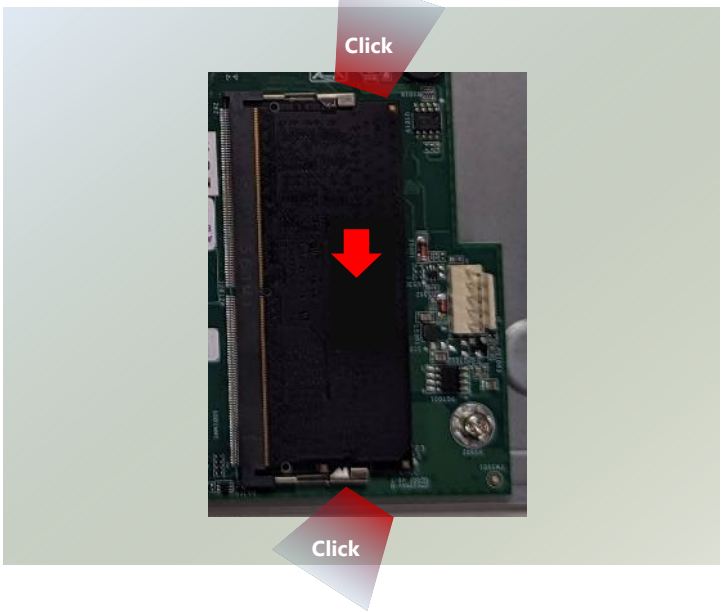
1. Power off the system and open the bottom chassis cover.
2. Locate the system memory slot.



3. Align the notch of module with the socket key in the slot. Insert the pins at 30 degrees into the socket key until it is fully seated.



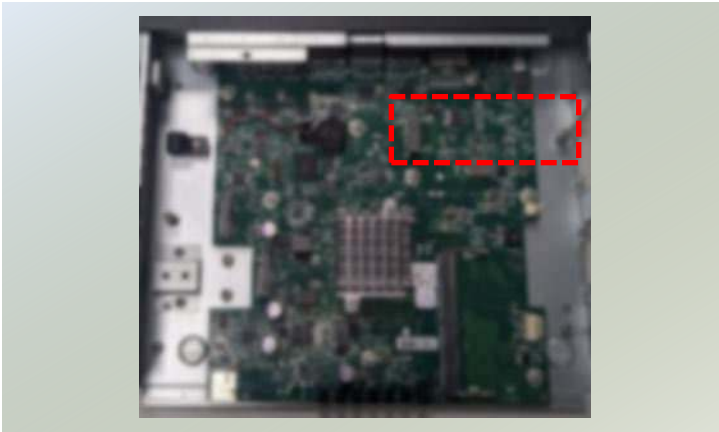
4. Push down on the module until the slot latch catches and clicks into place.



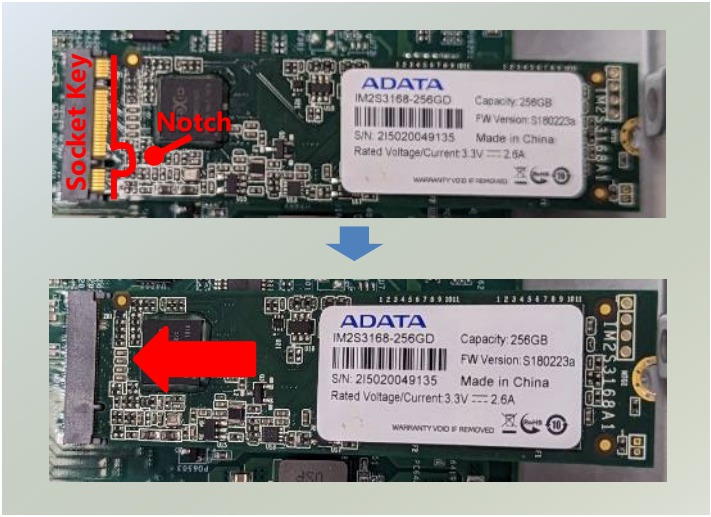
Installing M.2 Storage (Optional)

The motherboard supports one M.2 storage slot for additional SATA storage. Please follow the steps for installation.

1. Power off the system and open the bottom chassis cover.
2. Locate the M.2 slot on the motherboard.



3. Align the notch of the M.2 storage module with the socket key in the pin slot.
4. Insert the M.2 storage module card pins at 30 degrees into the socket until it is fully seated.

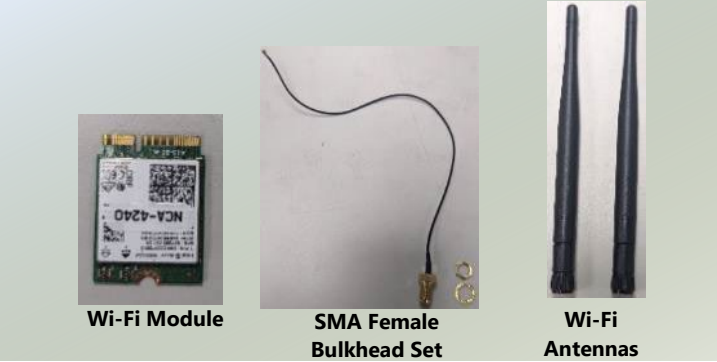


5. Push down on the module card and secure it with a screw.

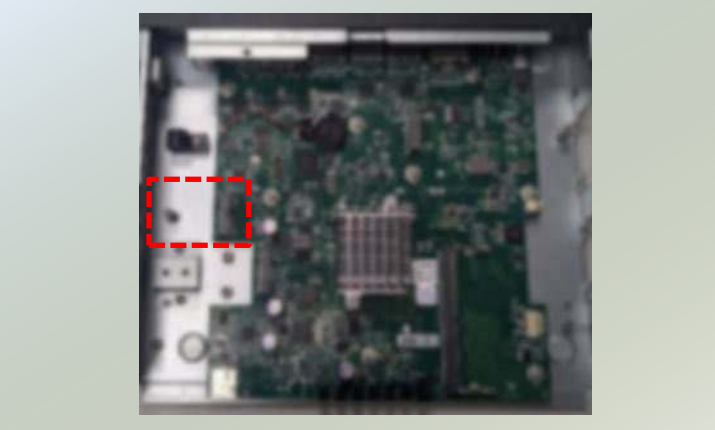
Installing Wi-Fi Module Card (Optional)

The system provides one M.2 2230 E-Key slot for Wi-Fi module. The Wi-Fi module will require two (2) antennas. Follow the steps for installation.

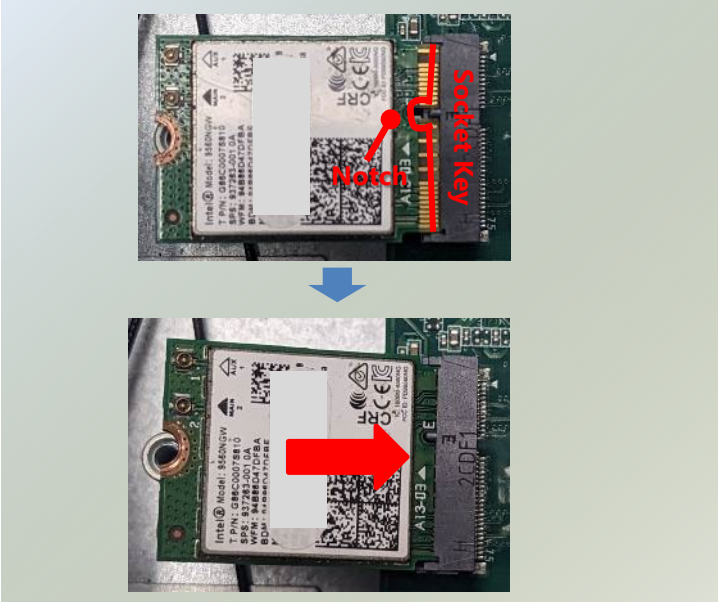
1. The Wi-Fi Module Kit includes:
   - 1x Wi-Fi Module Card
   - 2x SMA Female Cable Sets
   - 2x Wi-Fi Antennas



2. Power off the system and open the bottom chassis cover.
3. Locate the M.2 slot on the motherboard.



4. Align the notch of the Wi-Fi module card with the socket key in the pin slot.
5. Angle the Wi-Fi module card pins at 30 degrees and insert them into the socket until the card is fully seated.

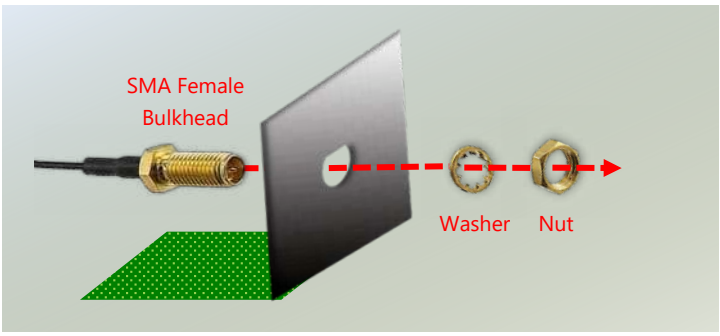


6. Push down on the module card and secure with a screw.

Installing Wi-Fi Antennas

1. Locate the two (2) antenna hole placements (A1, A2). Locate the two (2) IPEX connectors on the Wi-Fi module card.

2. From inside the chassis, insert the SMA Female Bulkhead through the antenna hole on the rear panel.
3. From the outside of the system, affix the Washer and Nut, then securely tighten the Nut using an SMA Torque Wrench.



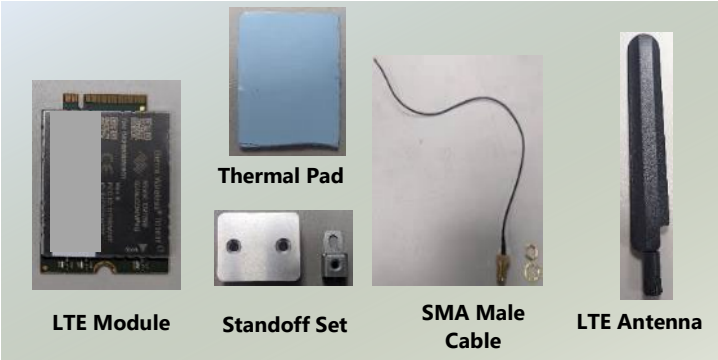
4. Connect the antenna cables to the IPEX connectors on the Wi-Fi module card.

5. Lastly, fasten the antennas onto the bulkhead located on the system's exterior.

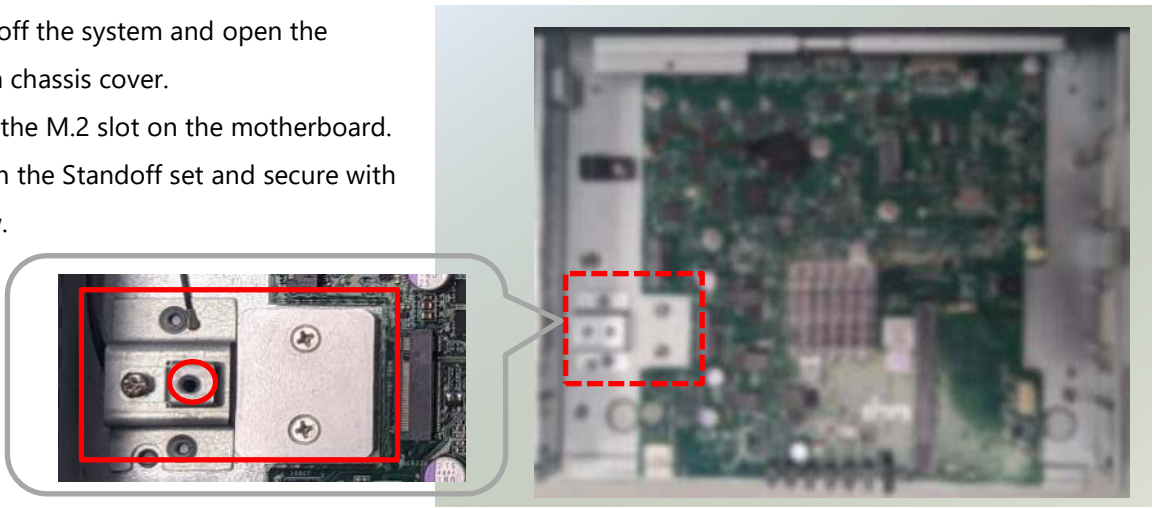
Installing LTE Module Card (Optional)

The motherboard provides one M.2 3042/3050/3052 slot for LTE/5G expansion. LTE module requires two (2) antennas, and 5G module requires four (4) antennas. Therefore, only one LTE module or one 5G module can be installed. Please follow the procedures for LTE module card expansion installation.

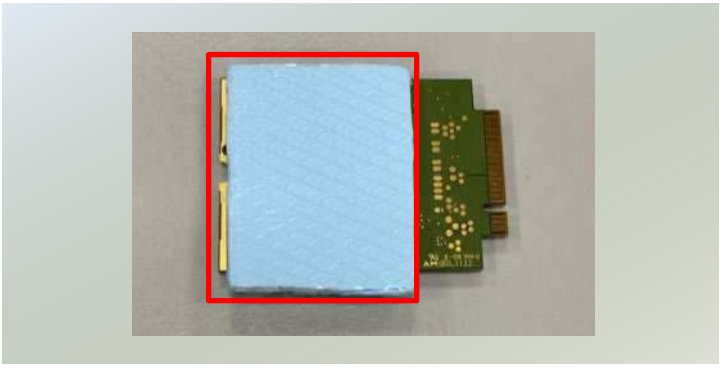
1. The LTE Module Kit includes:
   - 1x LTE Module Card
   - 2x SMA Male Cable Sets
   - 2x LTE Antennas
   - 1x Standoff Set
   - 1x Thermal pad



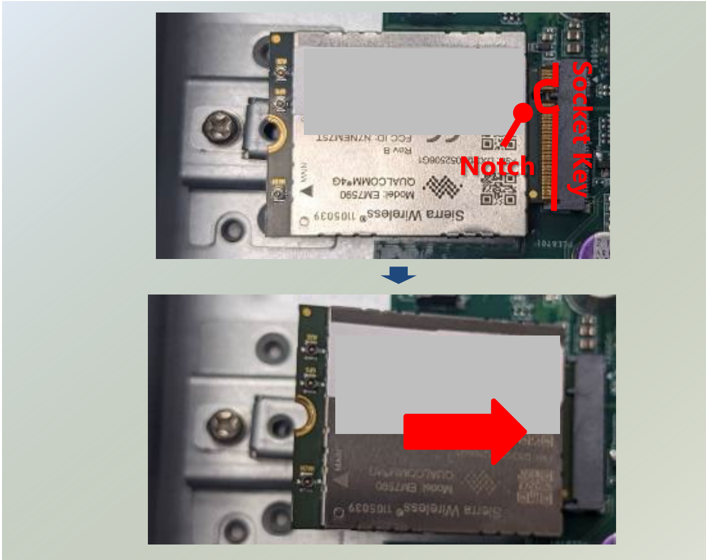
2. Power off the system and open the bottom chassis cover.
3. Locate the M.2 slot on the motherboard. Position the Standoff set and secure with a screw.



4. Next, thermal pad placement. Place the thermal pad on the bottom of the LTE module card.



4. Align the notch of the LTE module card with the socket key in the pin slot.
5. Position the LTE module card pins at a 30-degree angle and insert them into the socket until the card is completely seated.

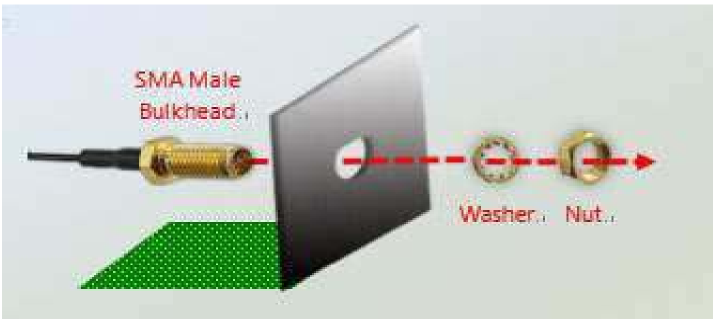


6. Push down on the module card and secure it with a screw.

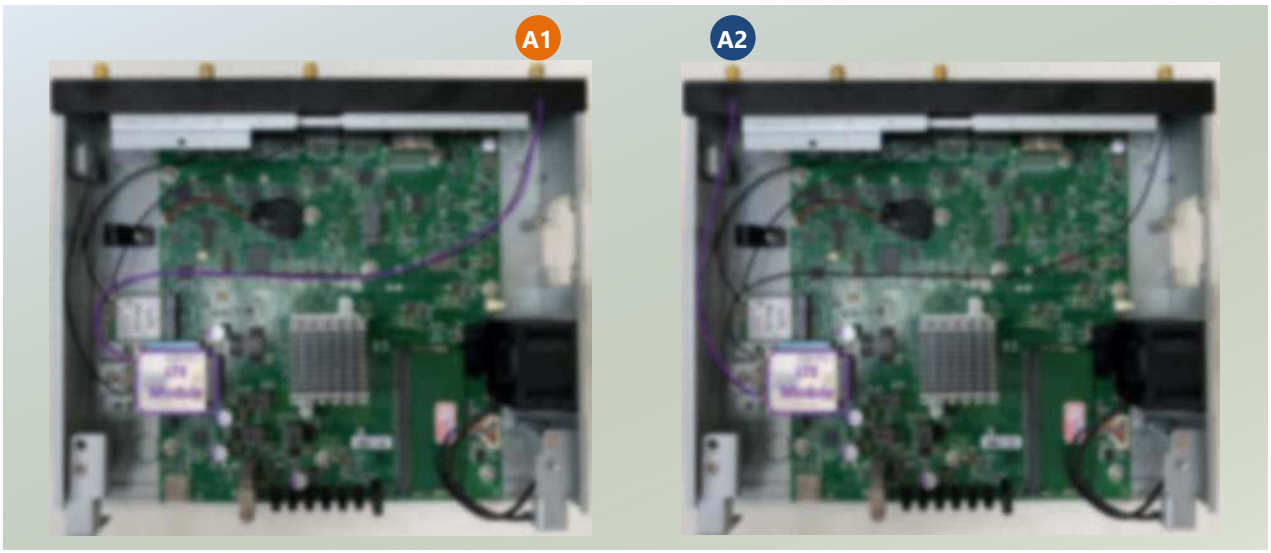
Installing LTE Antennas

1. Locate the two (2) antenna hole placements (A1, A2). Locate the two (2) IPEX connectors on the LTE module card.

2. From inside the chassis, insert the SMA Male Bulkhead through the antenna hole on the panel.
3. On the outside of the system, attach the Washer and Nut, and tighten the Nut using an SMA Torque Wrench.



4. Connect the antenna cables to the IPEX connectors on the LTE module card.

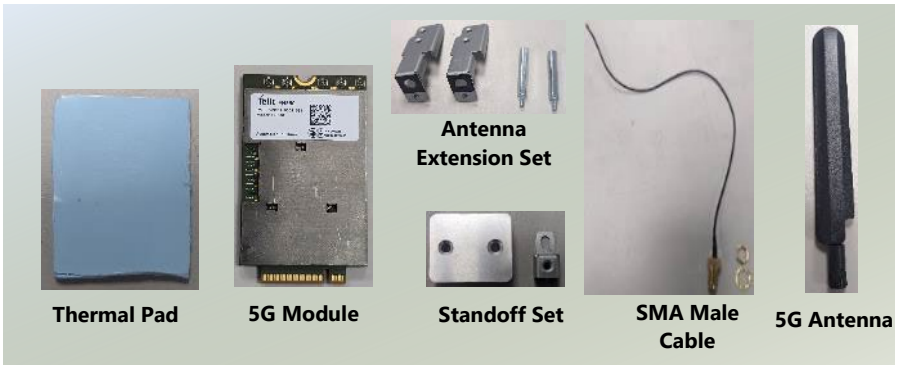


5. Lastly, fasten the antennas onto the bulkhead located on the system's exterior.

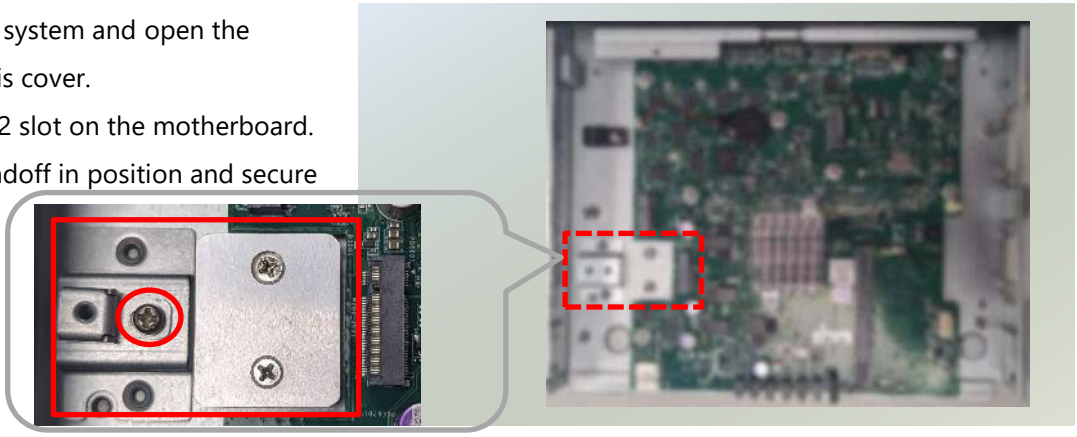
Installing 5G Module Card (Optional)

The motherboard provides one M.2 slot for 5G/LTE expansion. LTE module requires two (2) antennas, and 5G module requires four (4) antennas. Therefore, only one LTE module or one 5G module can be installed. Please follow the procedures for 5G module card expansion installation.

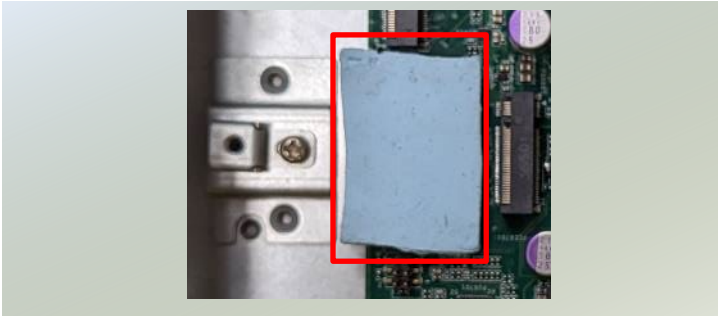
1. The 5G Module Kit includes:
   - 1x 5G Module Card
   - 4x SMA Male Cable Sets
   - 2x Antenna Extension Set
   - 4x 5G Antennas
   - 1x Standoff Set
   - 1x Thermal Pad



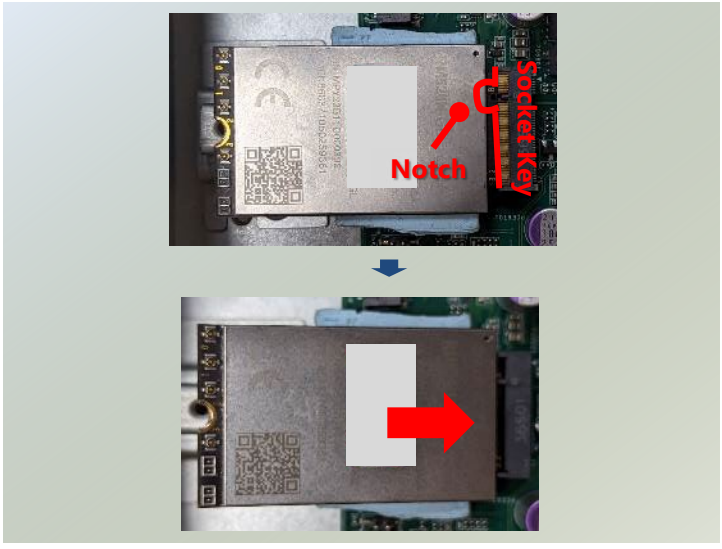
2. Power off the system and open the bottom chassis cover.
3. Locate the M.2 slot on the motherboard. Place the Standoff in position and secure with a screw.



4. Next, thermal pad placement. Place the thermal pad over the standoff.



5. Align the notch of the5G module card with the socket key in the pin slot.
6. Position the 5G module card pins at a 30-degree angle and insert them into the socket until the card is completely seated.

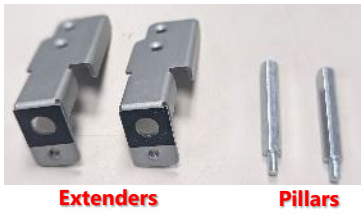


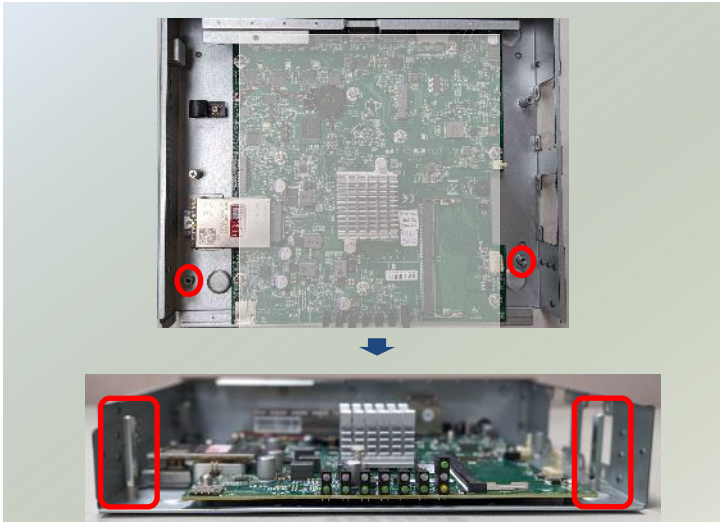
5. Push down on the module card and secure it with a screw.

Installing 5G Antennas

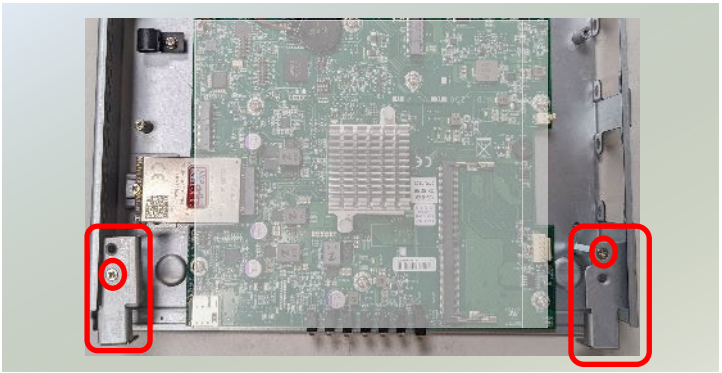
1. First, antenna extension setup. Locate the metal pillars placement on the motherboard. Then screw in the two metal pillars.

Antenna Extension Set

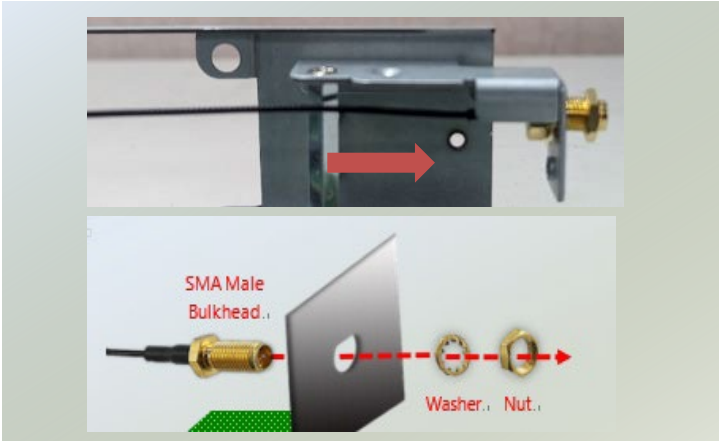




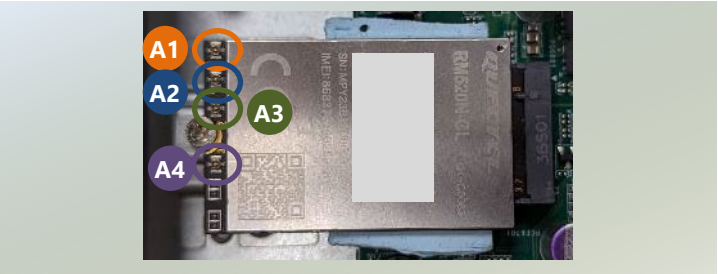
2. Then place the Extenders on top of the pillars, and secure with screws.



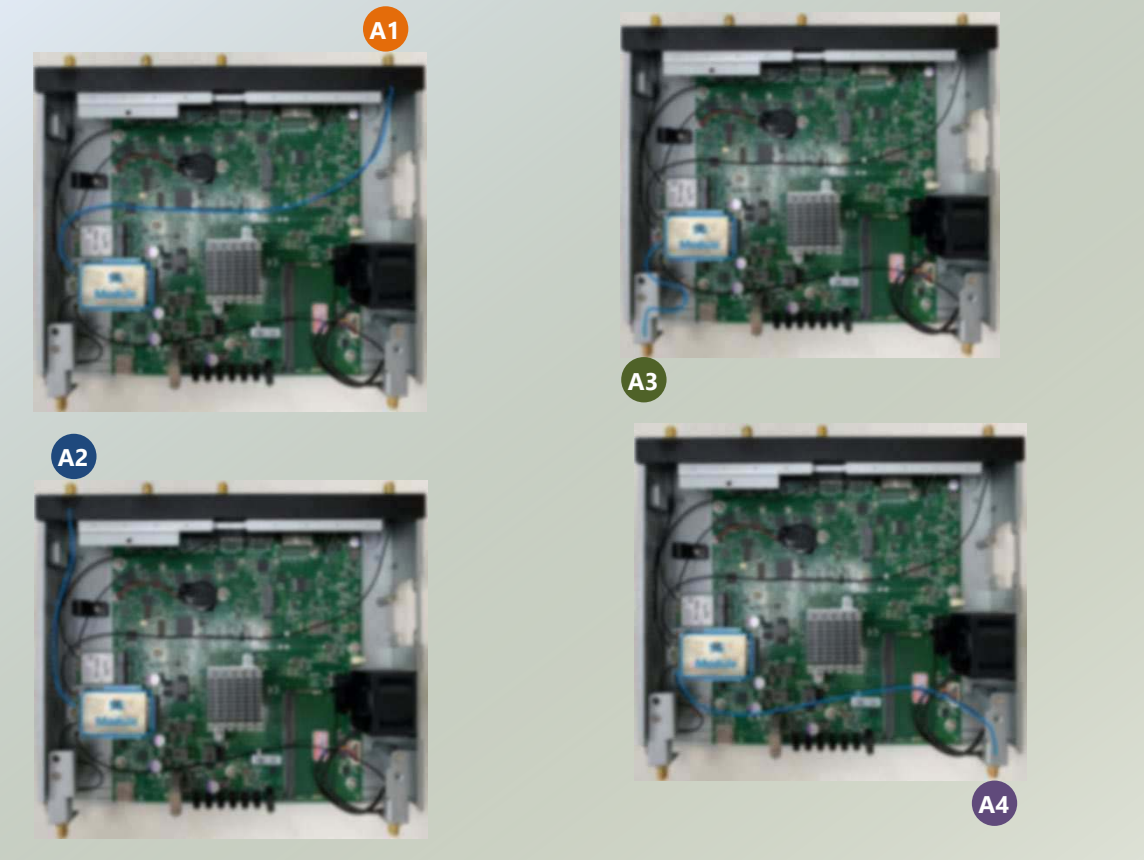
3. Then insert the SMA Male Bulkhead through Extender Antenna Hole. From the outside of the system, affix the Washer and Nut, then securely tighten the Nut using an SMA Torque Wrench.



4. Locate the four (4) IPEX connectors on the 5G module card.



5. Connect the antenna cables to the IPEX connectors on the 5G module card.



6. Lastly, fasten the antennas onto the bulkhead located on the system's exterior.

Installing SIM Card (Optional)

The SIM slot on the front panel supports an LTE/5G module (optional). The SIM socket support push-push mechanism, allowing inserting and ejecting the SIM card to be as easy as one push.

1. Locate the SIM card slot cover on the front panel. Loosen the two screws that secure the SIM slot cover and remove the slot cover. With the gold contacts on the SIM card facing downwards and the cut edge of the SIM card on the left side, push the SIM card all the way in until it clicks into place.

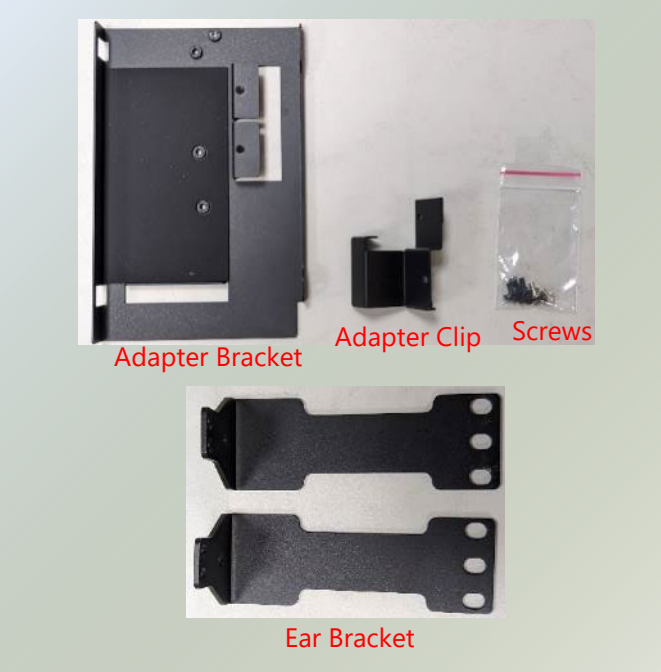
2. To remove the SIM card, use your fingertip to push it a little to have the card automatically ejected.

Rackmount the System (Optional)

With the rackmount kit, this system can be fixed onto rack posts. Please contact Lanner 's sales representative for purchasing this kit.

The Rackmount Kit includes:

- 2x Ear Bracket
- 1x Adapter Bracket
- 1x Adapter Clip
- 1x Screws Pack
  (For bracket and rack-mounting)



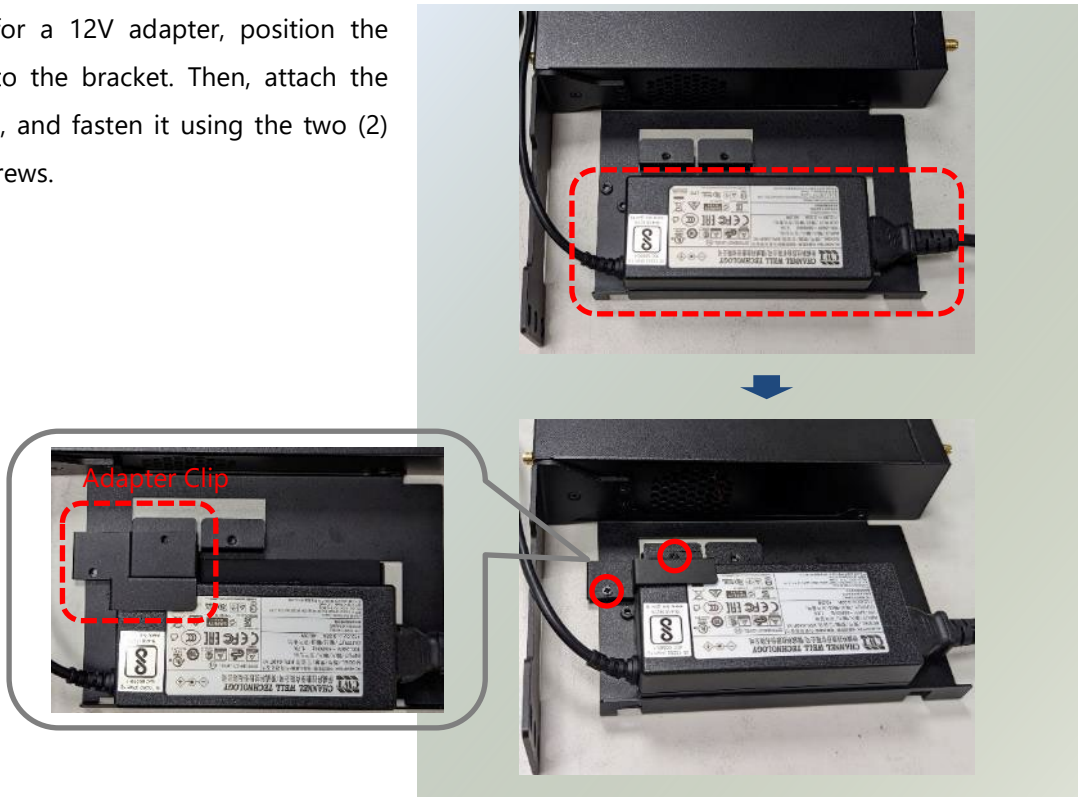
Attaching the Assembly to the Chassis

1. Align the ear bracket with the side panel's screw holes on one side of the system and secure it using three (3) screws.

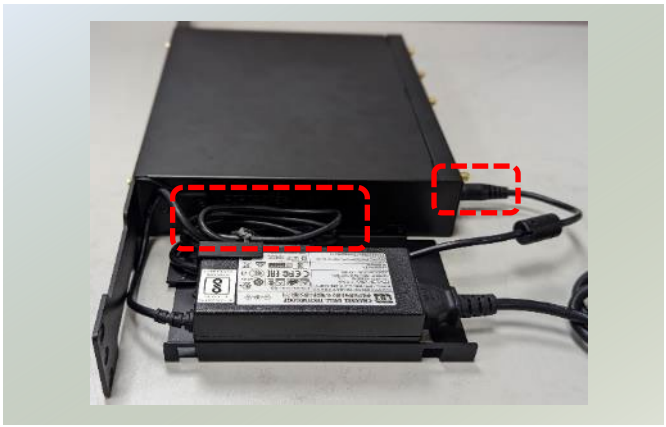
2. Secure the other ear bracket to the other side of the system.

3. Attach the adapter holder to the left side panel with two screws.

4. Designed for a 12V adapter, position the adapter onto the bracket. Then, attach the adapter clip, and fasten it using the two (2) provided screws.



5. Arrange the adapter's cables within the adapter bracket.
6. Connect the power adapter's connector to the system's rear panel power supply jack.



Installing the System to the Rack

1. Install a shelf in the rack to support the system (recommended). Hold the system with the front facing you, lift it gently and place it into the rack. Secure the brackets to the rack rails using rack-mounting screws.

Wallmount the System (Optional)

With the Wall-mount Kit, this system can be fixed on the wall surface. Please contact Lanner's sales representative for purchasing this kit.

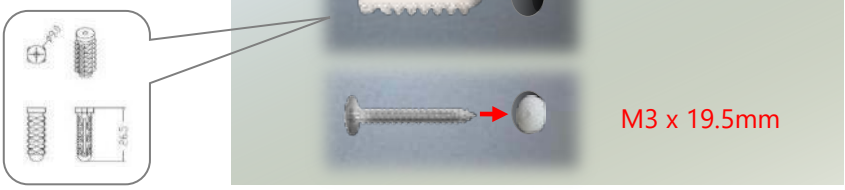
1. The Wallmount Kit includes:
   - 1x pair of Wall Brackets
   - 1x Screw Pack

2. Turn the system over, and attach the wall brackets to its underside, fastening them securely using the four provided screws.

3. Measure and mark the exact location on the wall for the system. Drill four (4) holes to align with the bracket's mounting holes.

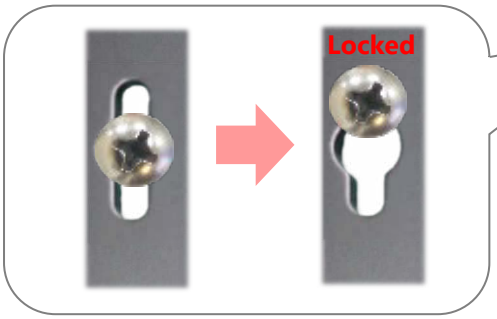
Note: The demonstrated screw type can fit in general drywall or shelves. Please identify the wall type and select a suitable fixing approach to fix this system to the wall and consult qualified trained person if you are unsure.

4. Insert the wall plugs into the drilled holes, then insert the long screws into the wall plugs.

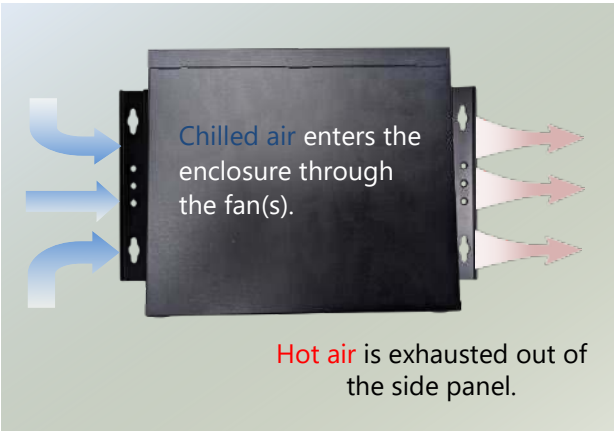


5. Position the system's wall brackets to line up with the four screws on the wall.

6. Attach the system by aligning its bracket holes with the wall screws, then press downward on the system to secure.



7. Ensure optimal airflow ventilation for the system by clearing obstructions around its intake and exhaust openings, and by organizing cables effectively to create sufficient space.



CHAPTER 4 SOFTWARE SETUP

BIOS Setup

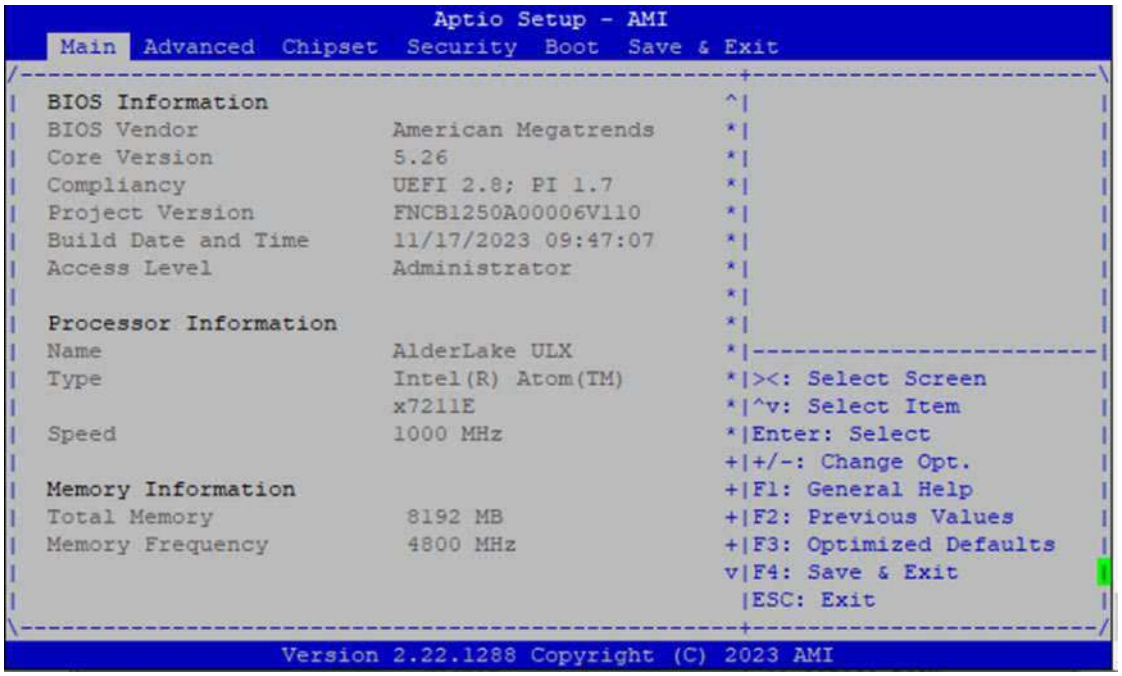
To enter the BIOS setup utility, simply follow the steps below:

1. Boot up the system.
2. The system has AMI BIOS built-in, with a SETUP utility that allows users to configure required settings or to activate certain system features. Pressing the **<Tab>** or **<Del>** key immediately allows you to enter the Setup utility.

Control Keys	Description
→←	select a setup screen, for instance, [Main], [Advanced],[IntelRCSetup], [Security], [Boot], and [Save & Exit]
↑↓	select an item/option on a setup screen
<Enter>	select an item/option or enter a sub-menu
+/-	to adjust values for the selected setup item/option
F1	to display General Help screen
F2	to retrieve previous values, such as the parameters configured the last time you had entered BIOS.
F3	to load optimized default values
F4	to save configurations and exit BIOS
<Esc>	to exit the current screen

Main Menu

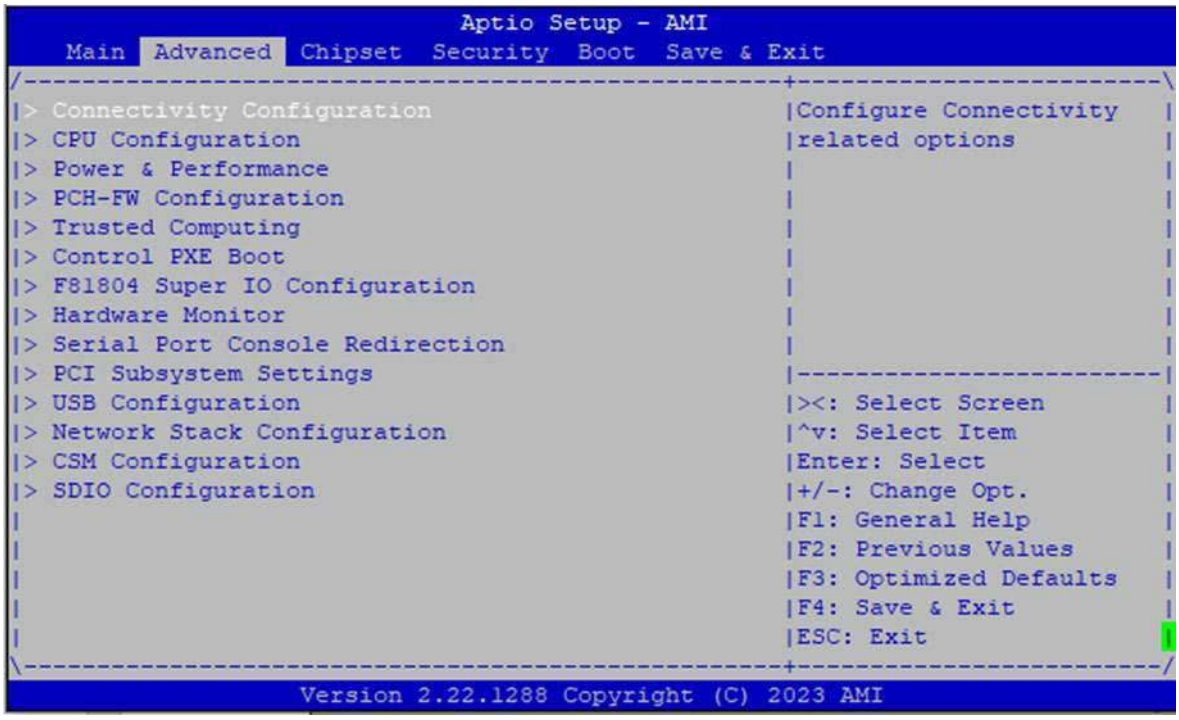
Setup main page contains BIOS information and project version information.



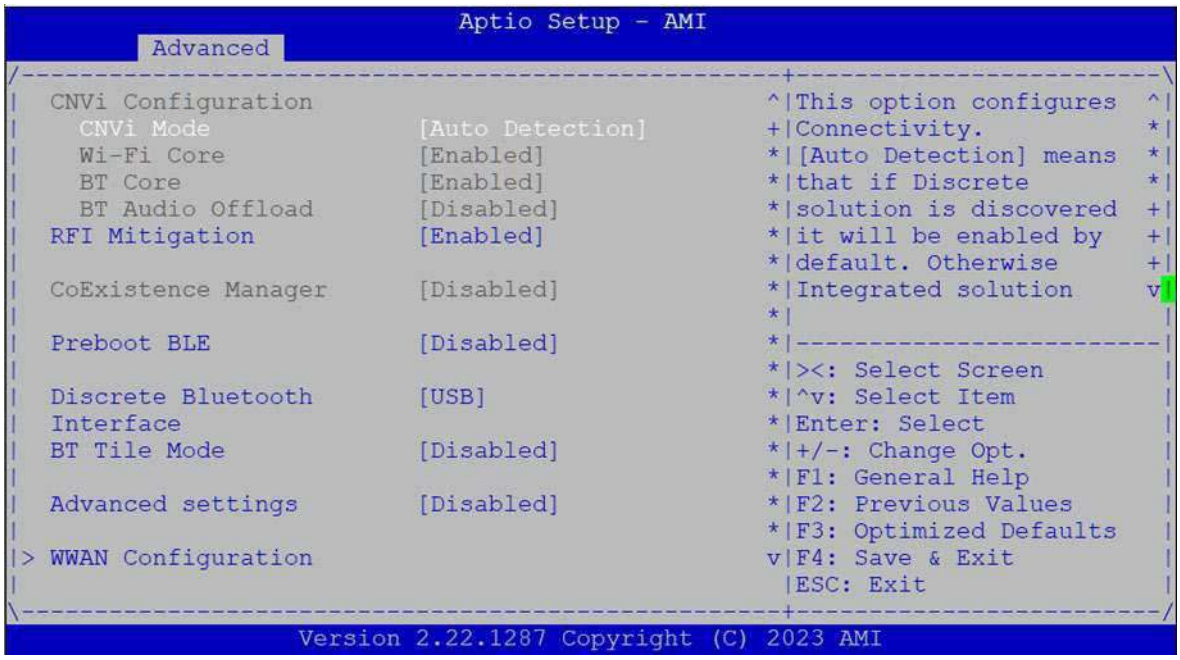
Feature	Description
BIOS Information	BIOS Vendor: American Megatrends Core Version: AMI Kernel version, CRB code base, X64 Compliancy: UEFI version, PI version Project Version: BIOS release version Build Date and Time: MM/DD/YYYY Access Level: Administrator / User
Processor Information	Information of platform processor
Memory Information	Information of memory
PCH Information	Information of platform pch
System Date	To set the Date, use **<Tab>** to switch between Date elements. Default Range of Year: 1998-9999 Default Range of Month: 1-12 Days: dependent on Month.
System Time	To set the Date, use **<Tab>** to switch between Date elements.

Advanced Menu

Select the **Advanced** menu item from the BIOS setup screen to enter the "Advanced" setup screen. Users can select any of the items in the left frame of the screen.



Connectivity Configuration



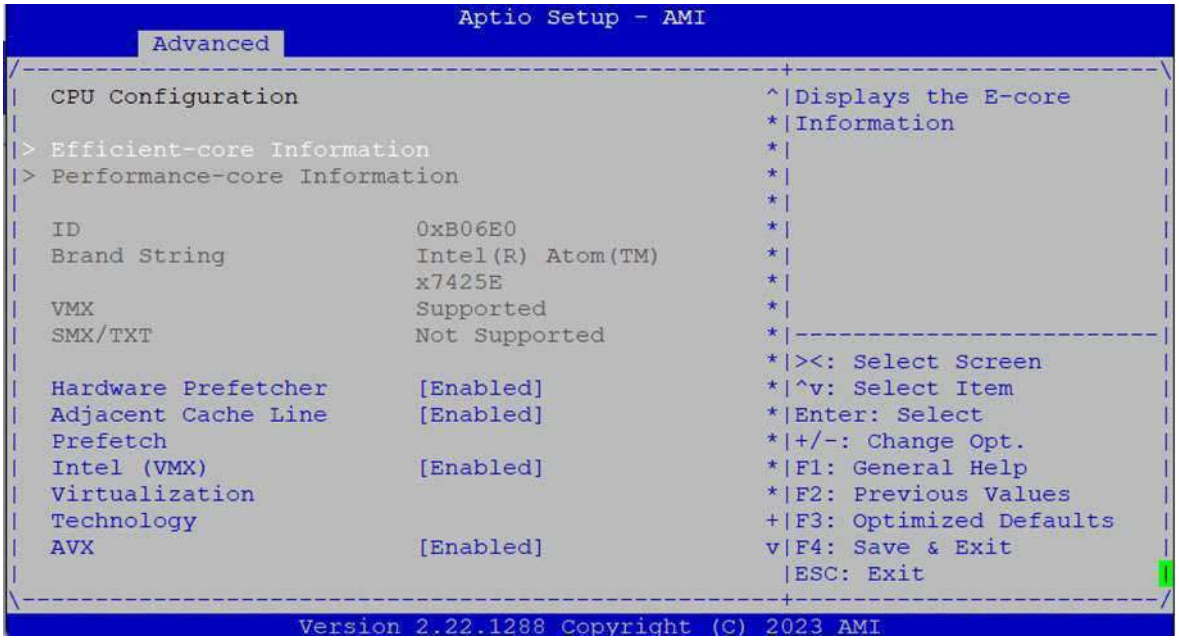
Feature	Options	Description
CNVi Mode	Disable Integrated Auto Detection	This option configures Connectivity. **[Auto Detection]** means that if Discrete solution is discovered it will be enabled by default. Otherwise Integrated solution (CNVi) will be enabled; **[Disable Integrated]** disables Integrated Solution. **NOTE:** When CNVi is present, the GPIO pins that are used for radio interface cannot be assigned to the other native function.
Wi-Fi Core	Enabled Disabled	This is an option intended to Enable/Disable Wi-Fi Core in CNVi
BT Core	Enabled Disabled	This is an option intended to Enable/Disable BT Core in CNVi
BT Audio Offload	Disabled Enabled	This is an option to Enable/Disable BT Audio Offload which enables audio input from BT device in HFP format to the audio DSP and enables power efficient audio output to BT device via A2DP format. This feature only support with Intel(R) Wireless-AX 22560
RFI Mitigation	Enabled Disabled	This is an option intended to Enable/Disable DDR-RFIM feature for Connectivity This RFI mitigation feature may result in temporary slowdown of the DDR speed.
Preboot BLE	Disabled Enabled	This will be used to enable Preboot Bluetooth function
Discrete Bluetooth Interface	Disabled USB	Serial IO UART0 needs to be enabled to select BT interface

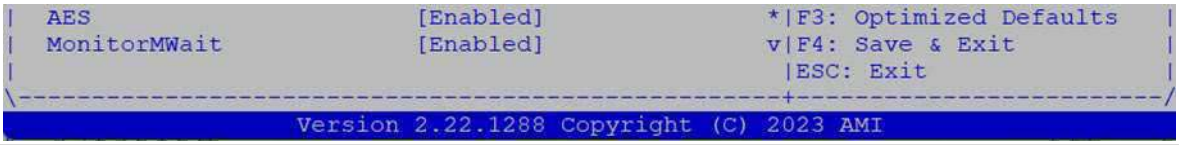
BT Tile Mode	Disabled Enabled	Enable/Disable Tile
Advanced settings	Disabled Enabled	Configure ACPI objects for wireless devices

WWAN Configuration

Feature	Options	Description
WWAN Device	Disabled 4G - 7360/7560 5G - M80	Select the M.2 WWAN Device options to enable 4G - 7360/7560 (Intel), 5G - M80 (MediaTek) Modems

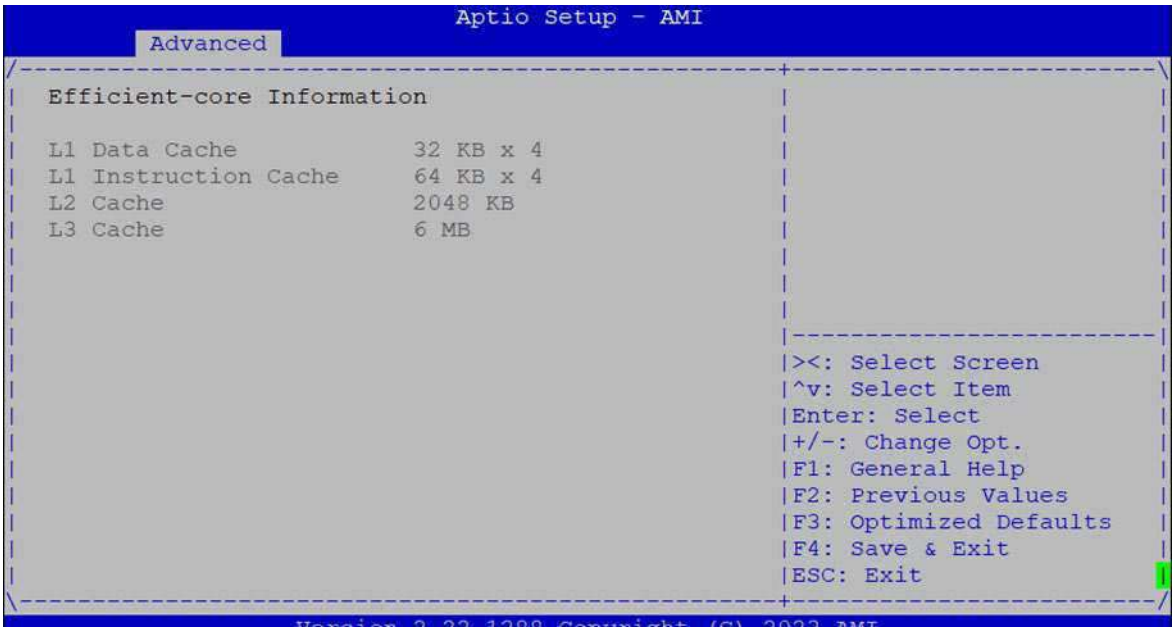
CPU Configuration





Feature	Options	Description
Hardware Prefetcher	Disabled Enabled	To turn on/off the MLC streamer prefetcher.
Adjacent Cache Line Prefetch	Disabled Enabled	To turn on/off prefetching of adjacent cache lines.
Intel (VMX) Virtualization Technology	Disabled Enabled	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
AES	Disabled Enabled	Enable/Disable AES (Advanced Encryption Standard)
MonitorMWait	Disabled Enabled	Enable/Disable MonitorMWait, if Disable MonitorMwait, the AP threads Idle Manner should not set in MWAIT Loop

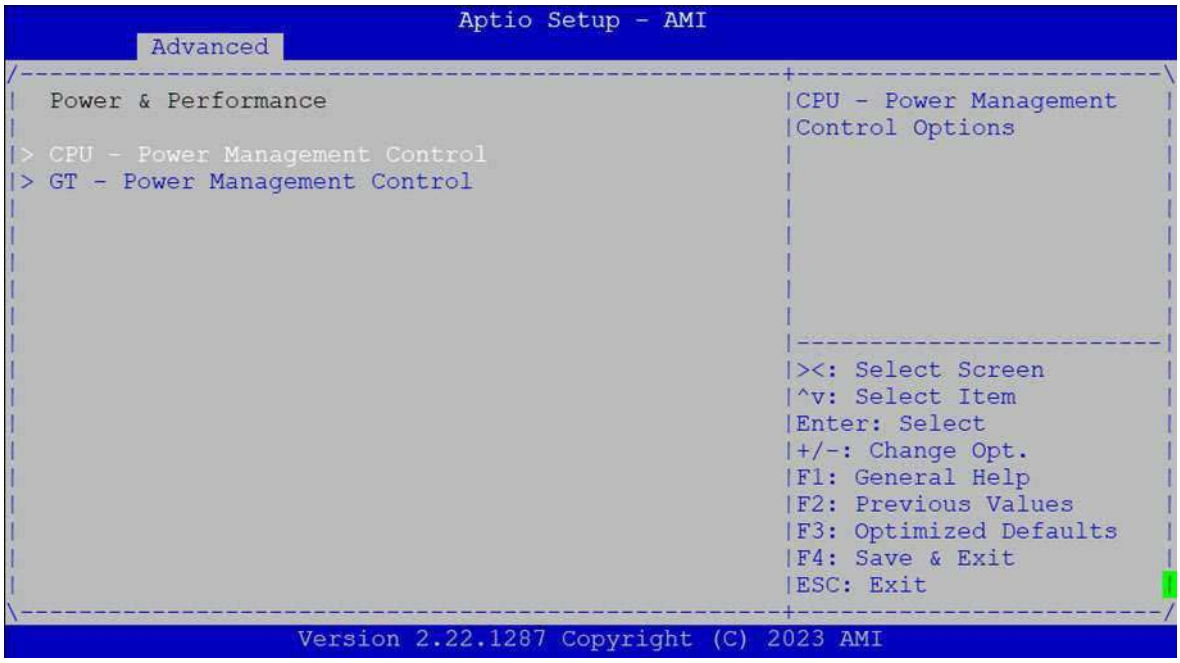
Efficient-Core Information



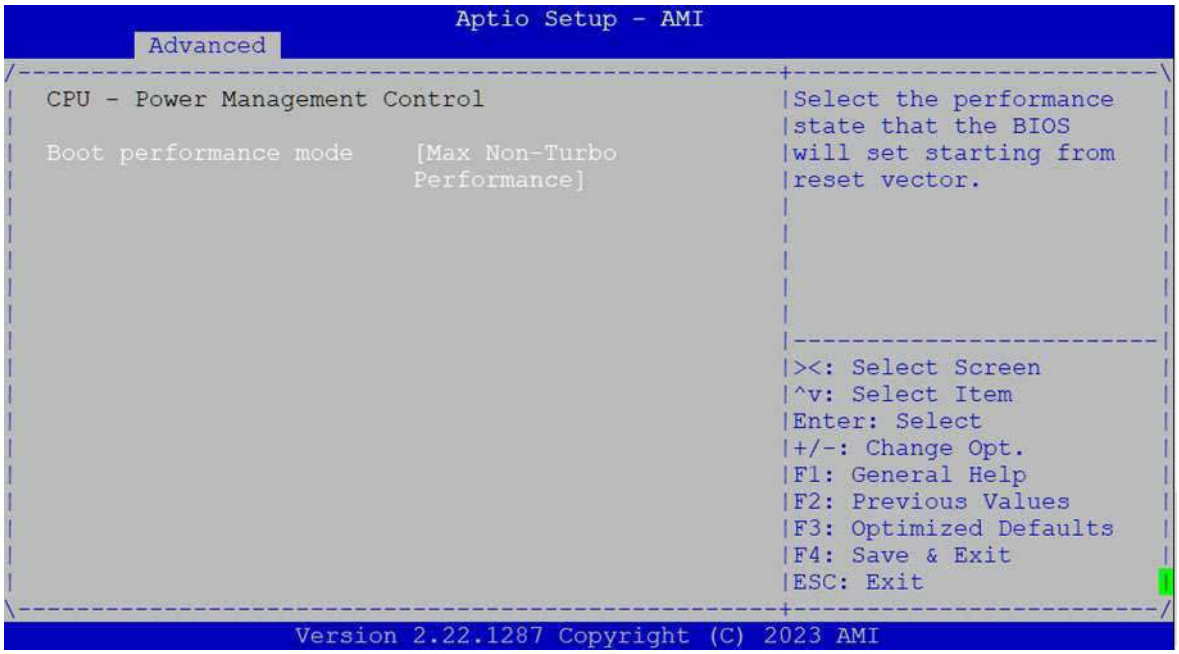
Performance-Core Information

NA

Power & Performance

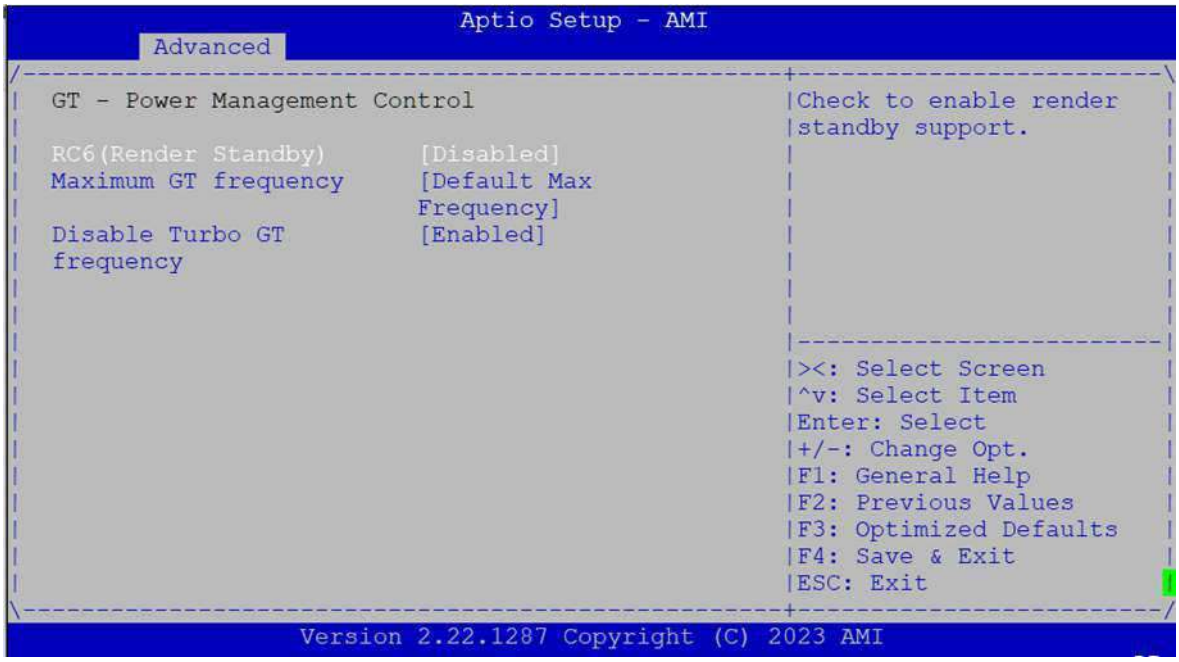


CPU – Power Management Control



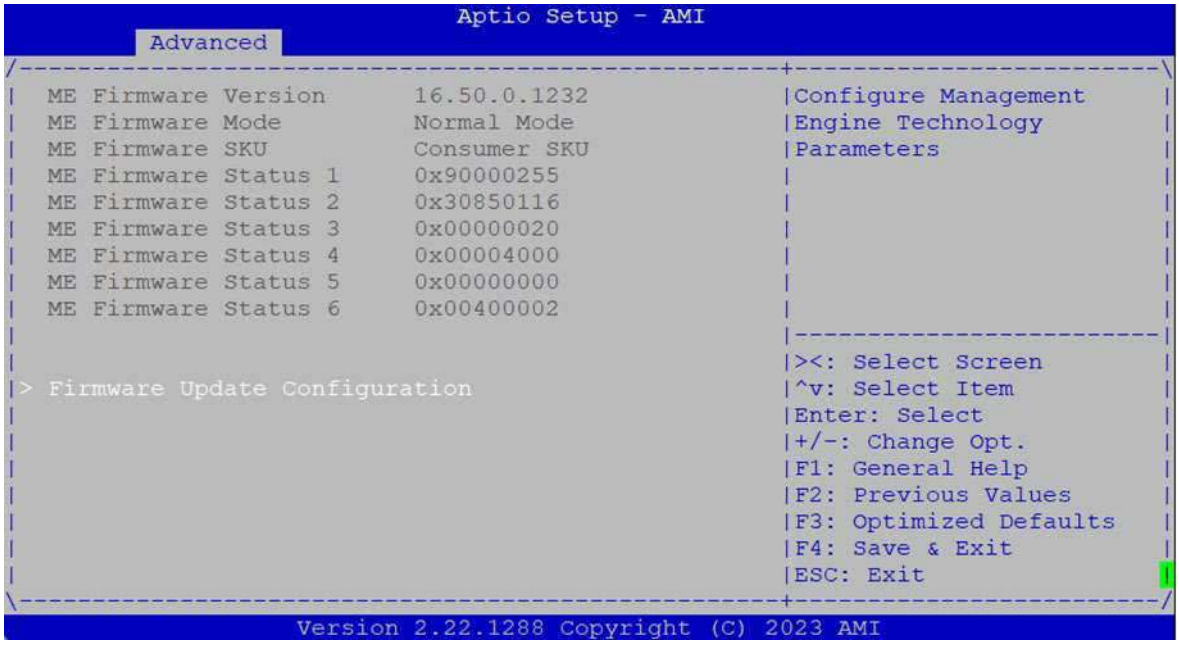
Feature	Options	Description
Boot performance mode	Max Battery Max Non-Turbo Performance Turbo Performance	Select the performance state that the BIOS will set starting from reset vector.

GT – Power Management Control

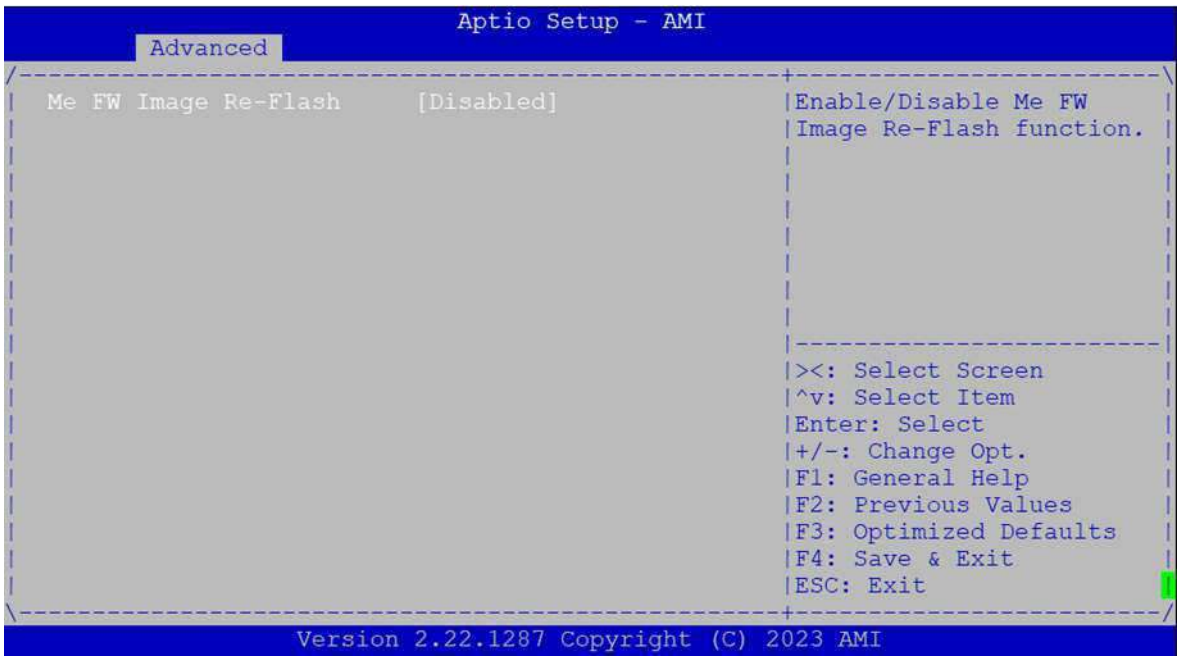


Feature	Options	Description
RC6 (Render Standby)	Disabled Enabled	Check to enable render standby support.
Maximum GT frequency	Default Max Frequency	Maximum GT frequency limited by the user. Choose between 300MHz (RPN) and 1550MHz (RP0). Value beyond the range will be clipped to min/max supported by SKU
Disable Turbo GT frequency	Enabled Disabled	Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited

PCH-FW Configuration

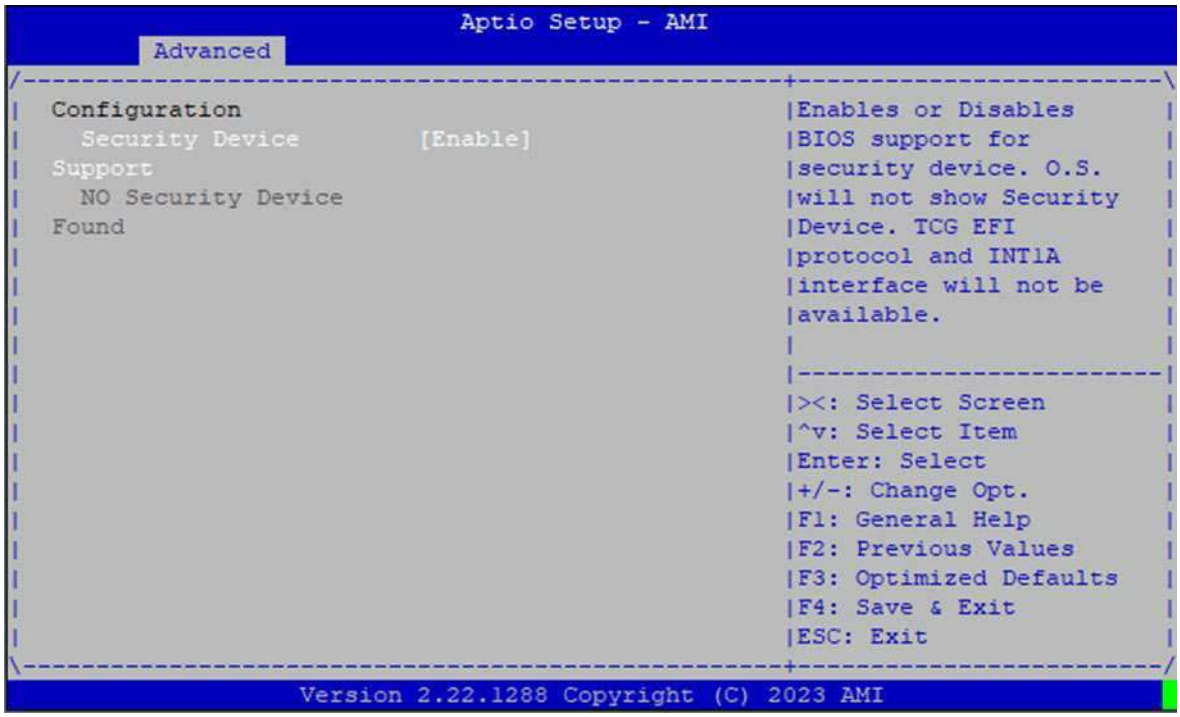


Firmware Update Configuration



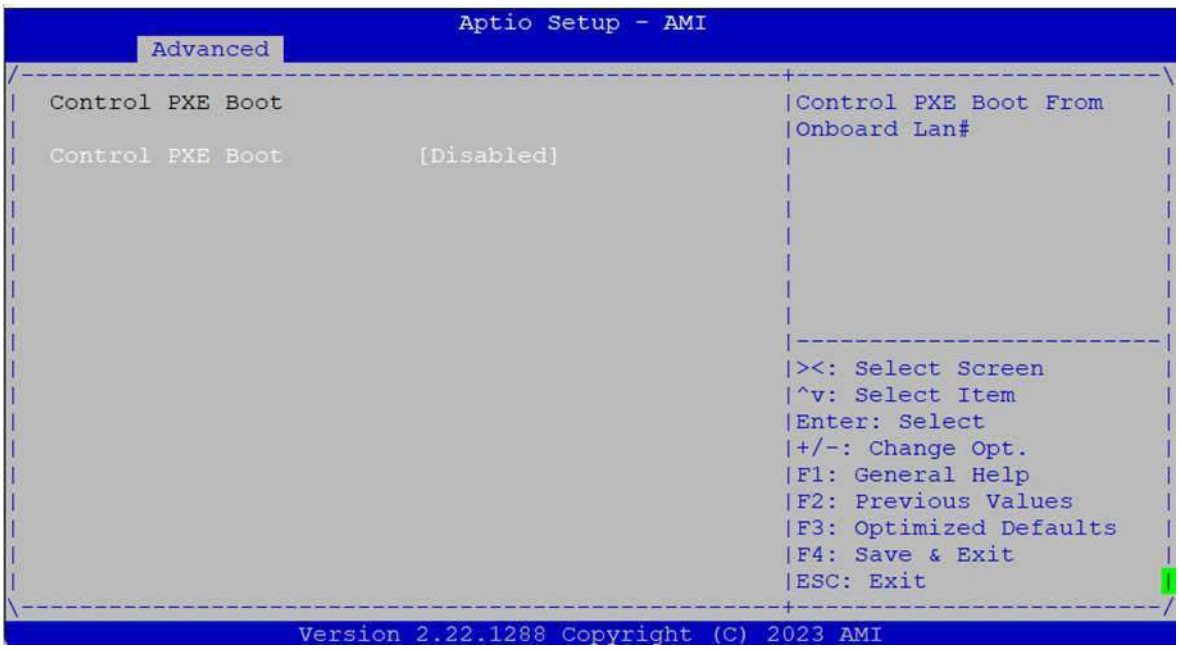
Feature	Options	Description
Me FW Image Re-Flash	Disabled Enabled	Enable/Disable Me FW Image Re-Flash function.

Trusted Computing



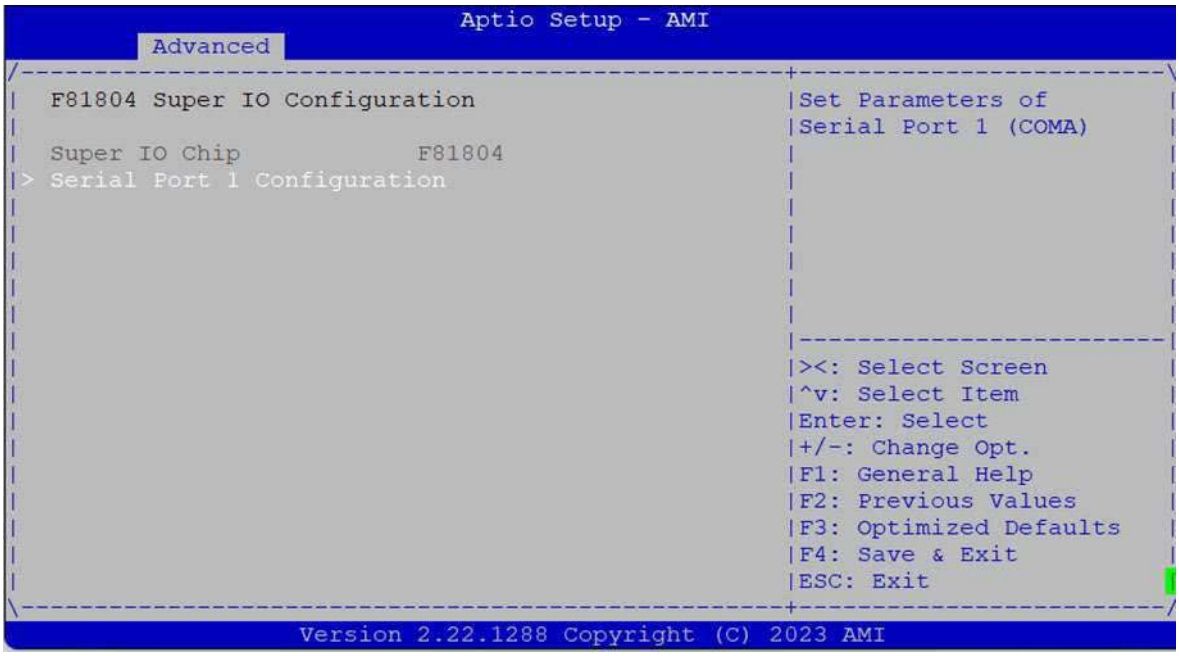
Feature	Options	Description
Security Device Support	Disable Enable	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

Control PXE Boot

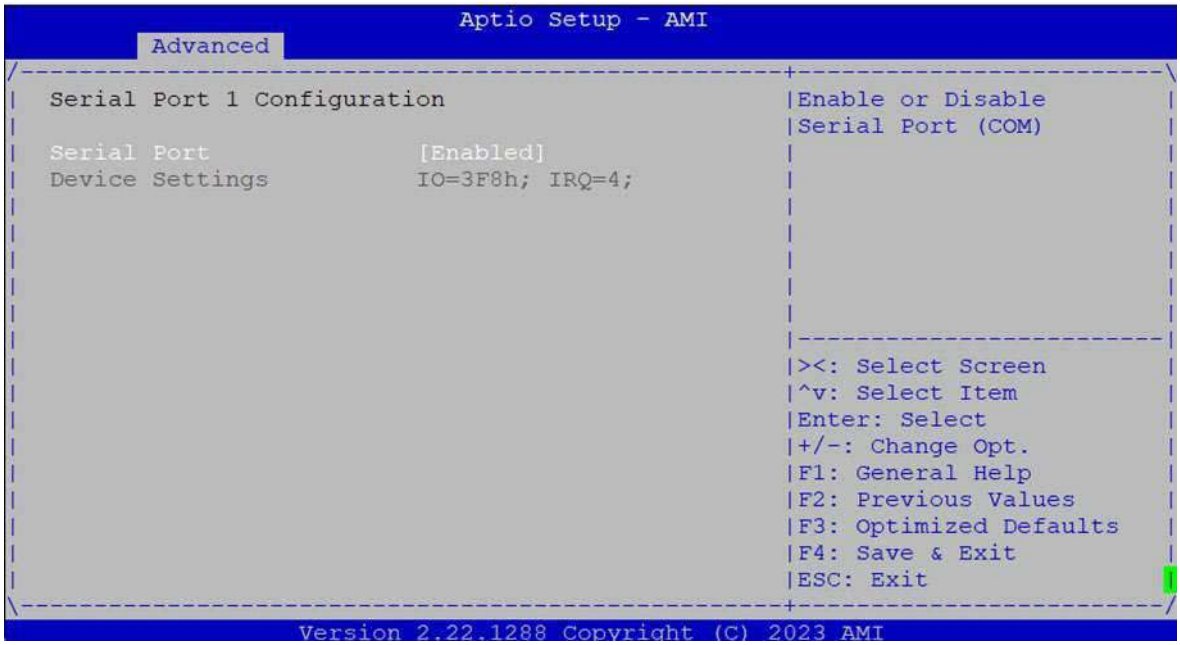


Feature	Options	Description
Control PXE Boot	Disabled LAN2 LAN3 LAN4 LAN5 LAN6	Control PXE Boot from I226 Lan#

F81804 Super IO Configuration

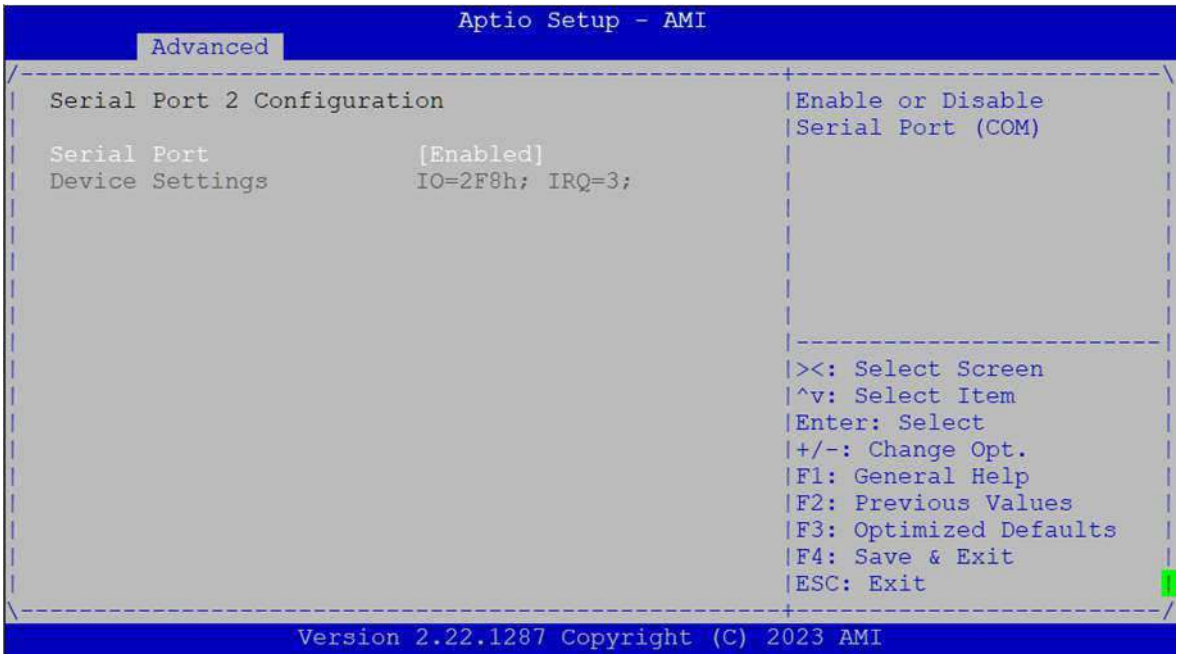


Serial Port 1 Configuration



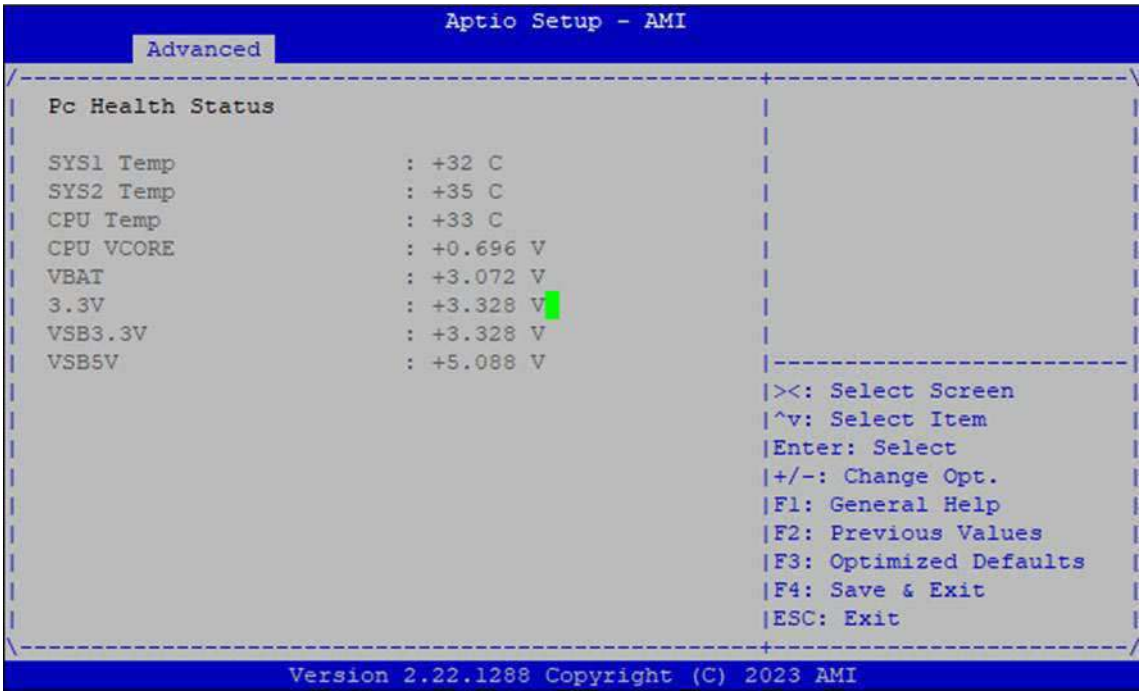
Feature	Options	Description
Serial Port	Disabled Enabled	Enable or Disable Serial Port (COM)
Device Settings	N/A	IO=3F8h; IRQ=4;

Serial Port 2 Configuration



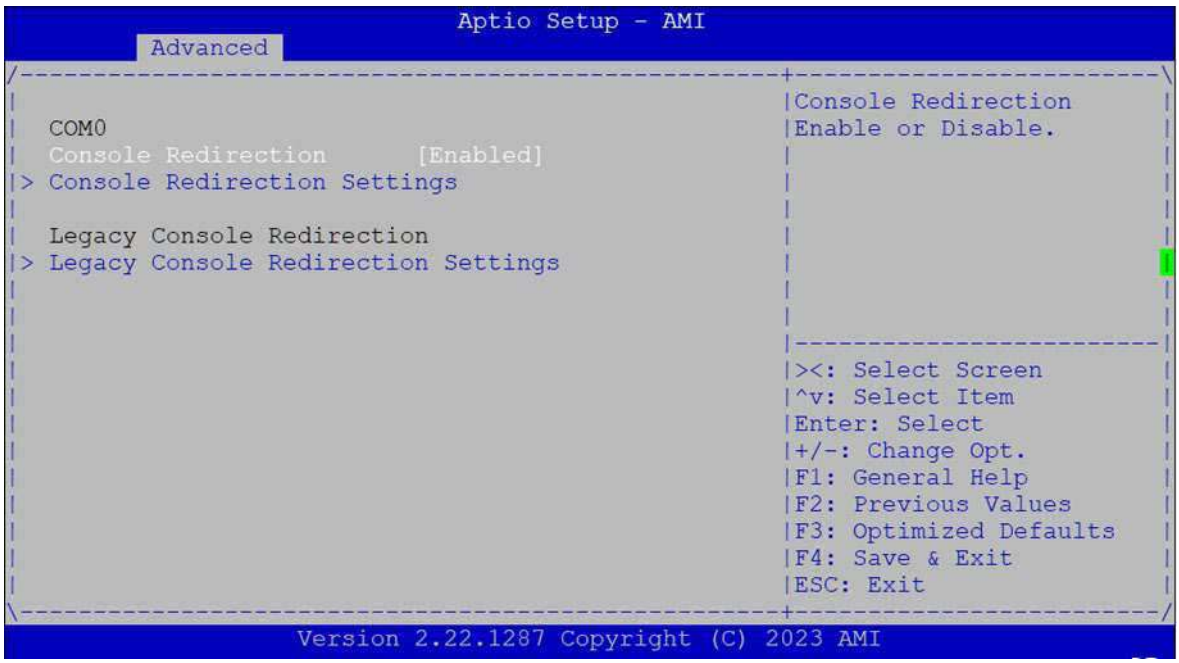
Feature	Options	Description
Serial Port	Disabled Enabled	Enable or Disable Serial Port (COM)
Device Settings	N/A	IO=2F8h; IRQ=3;

Hardware Monitor



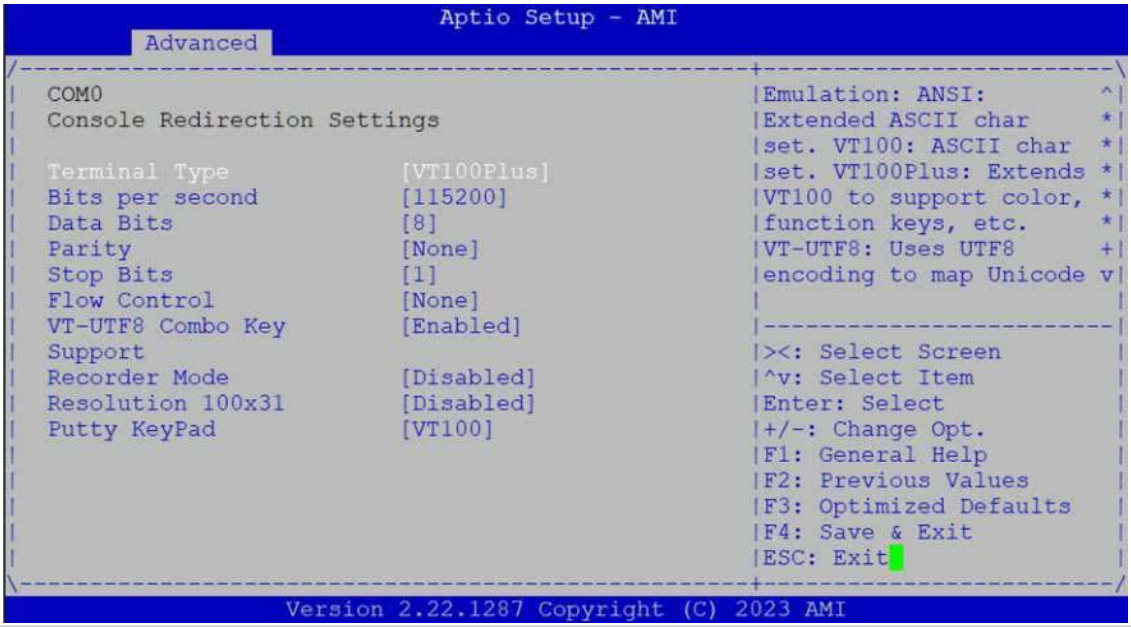
Feature	Description
SYS1 Temp	This value reports the System temperature
SYS2 Temp	This value reports the System temperature (Close to CPU)
CPU Temp	This value reports the CPU temperature
FAN1 Speed	This value reports the Fan1 speed
CPU VCORE	This value reports the CPU VCORE Input voltage
VBAT	This value reports the VBAT Input voltage
3.3V	This value reports the 3.3V Input voltage
VSB3.3V	This value reports the VSB3.3V Input voltage
VSB5V	This value reports the VSB5V Input voltage

Serial Port Console Redirection



Feature	Options	Description
Console Redirection	Disabled Enabled	Console Redirection Enable or Disable.

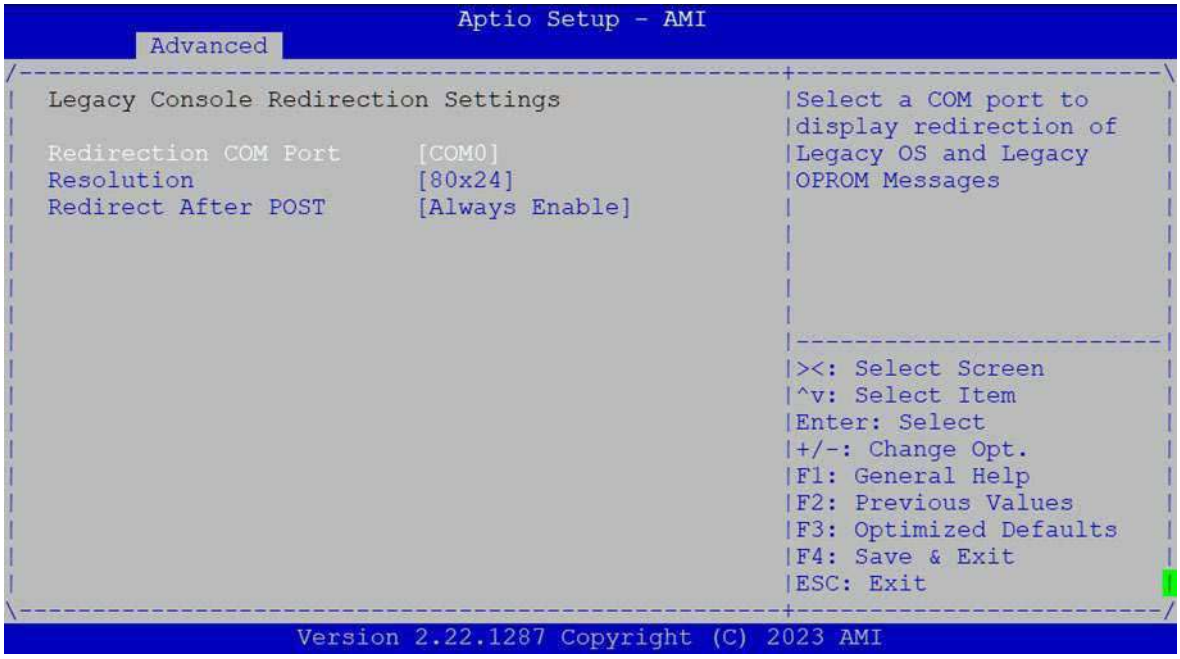
Console Redirection Settings



Feature	Options	Description
Terminal Type	VT100 VT100+ VT-UTF8 ANSI	Emulation: **ANSI:** Extended ASCII char set. **VT100:** ASCII char set. **VT100+:** Extends VT100 to support color, function keys, etc. **VT-UTF8:** Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 115200	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 8	Data Bits
Parity	None Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors.
Stop Bits	1 2	Stop bits indicate the end of a serial data packet.
Flow Control	None Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow.

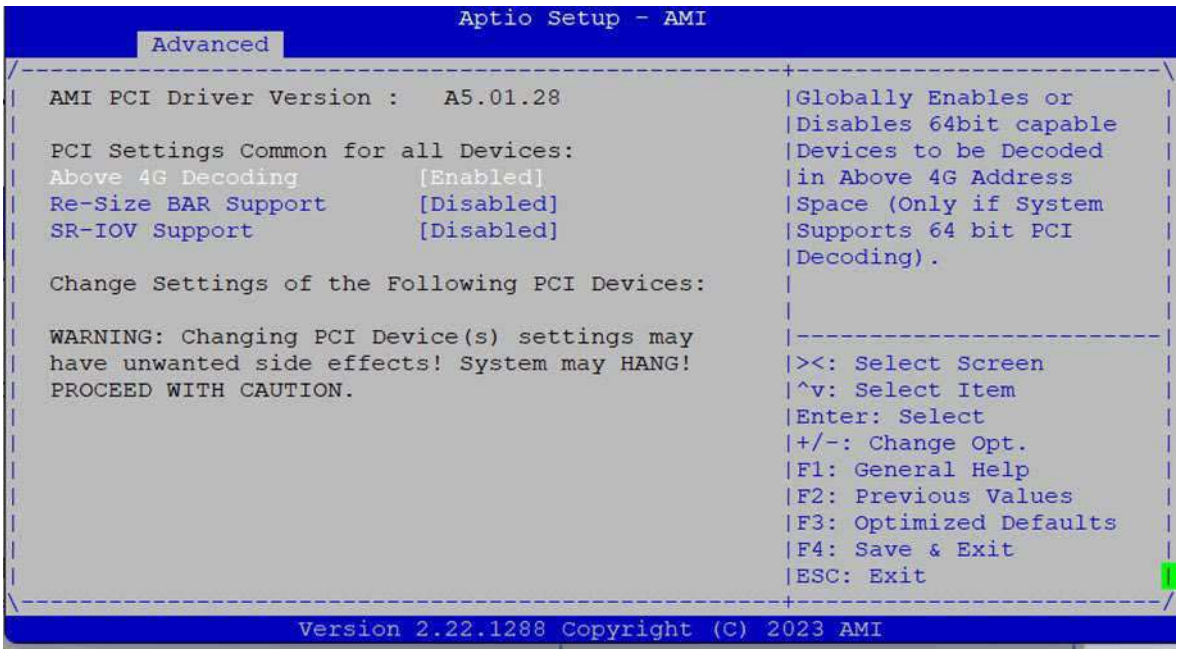
VT-UTF8 Combo Key Support	Disabled Enabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	Disabled Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	Disabled Enabled	Enables or disables extended terminal resolution.
Putty KeyPad	VT100 LINUX XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.

Legacy Console Redirection Settings



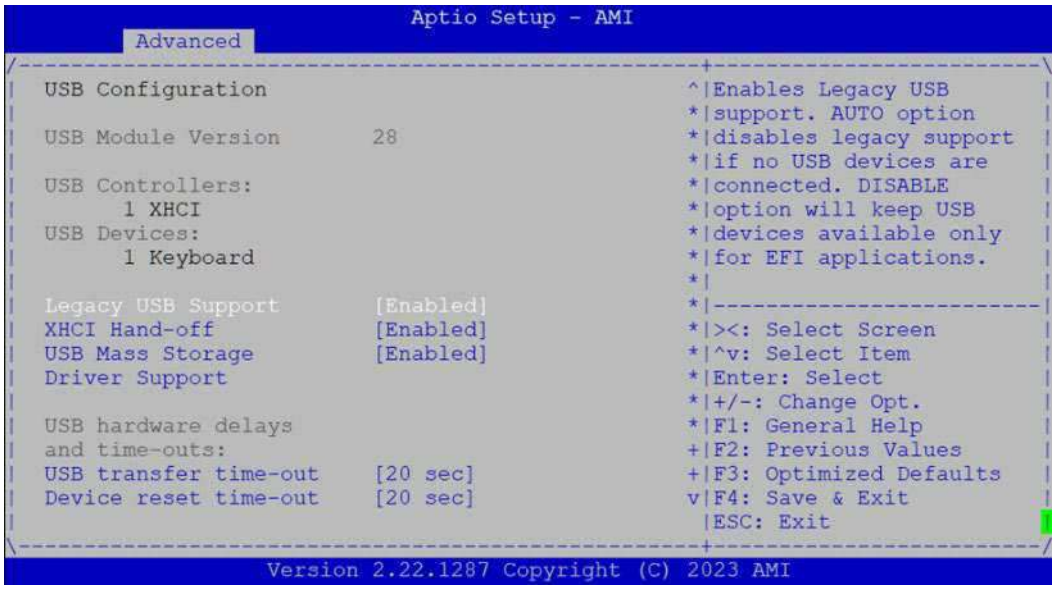
Feature	Options	Description
Redirection COM Port	COM0	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages
Resolution	80x24 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Redirect After POST	Always Enable BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

PCI Subsystem Settings



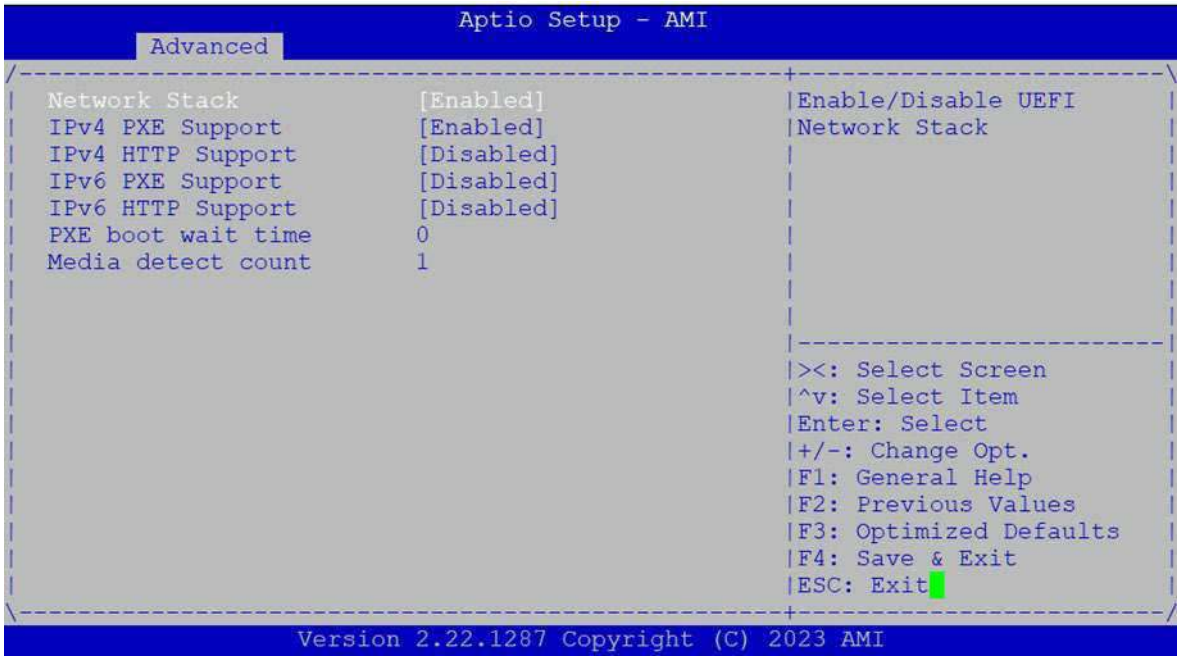
Feature	Options	Description
Above 4G Decoding	Disabled Enabled	Disables 64bit capable Device Resources to be Allocated in Above 4G Address Space.
SR-IOV Support	Disabled Enabled	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support.
Re-Size BAR Support	Disabled Enabled	If system has Resizable BAR capable PCIe Devices, this option Enables or Disables Resizable BAR Support.

USB Configuration



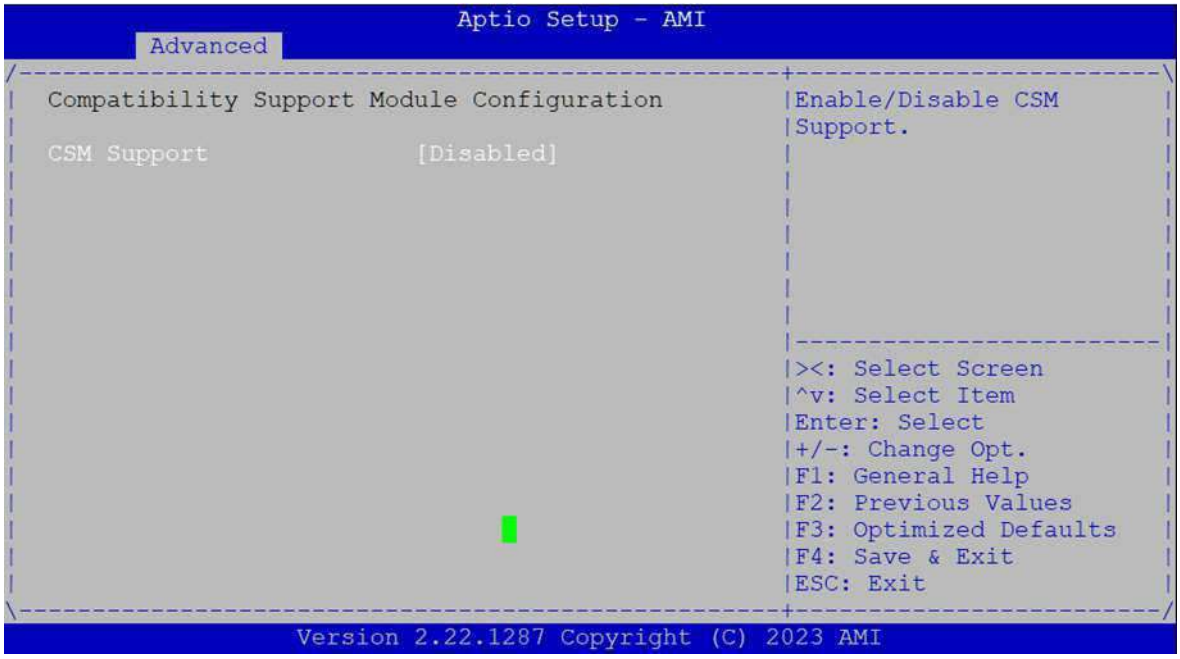
Feature	Options	Description
Legacy USB Support	Enabled Disabled Auto	Enables Legacy USB support. **Auto** option disables legacy support if no USB devices are connected. **Disabled** option will keep USB devices available only for EFI applications.
XHCI Hand-off	Enabled Disabled	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Disabled Enabled	Enable/Disable USB Mass Storage Driver Support.
USB transfer time-out	1 sec 5 sec 10 sec 20 sec	The time-out value for Control, Bulk, and Interrupt transfers
Device reset time-out	10 sec 20 sec 30 sec 40 sec	USB mass storage device Start Unit command time-out
Device power-up delay	Auto Manual	Maximum time the device will take before it properly reports itself to the Host Controller. **Auto** uses default value: for a Root port, it is 100 ms, for a Hub port the delay is taken from Hub descriptor.

Network Stack Configuration



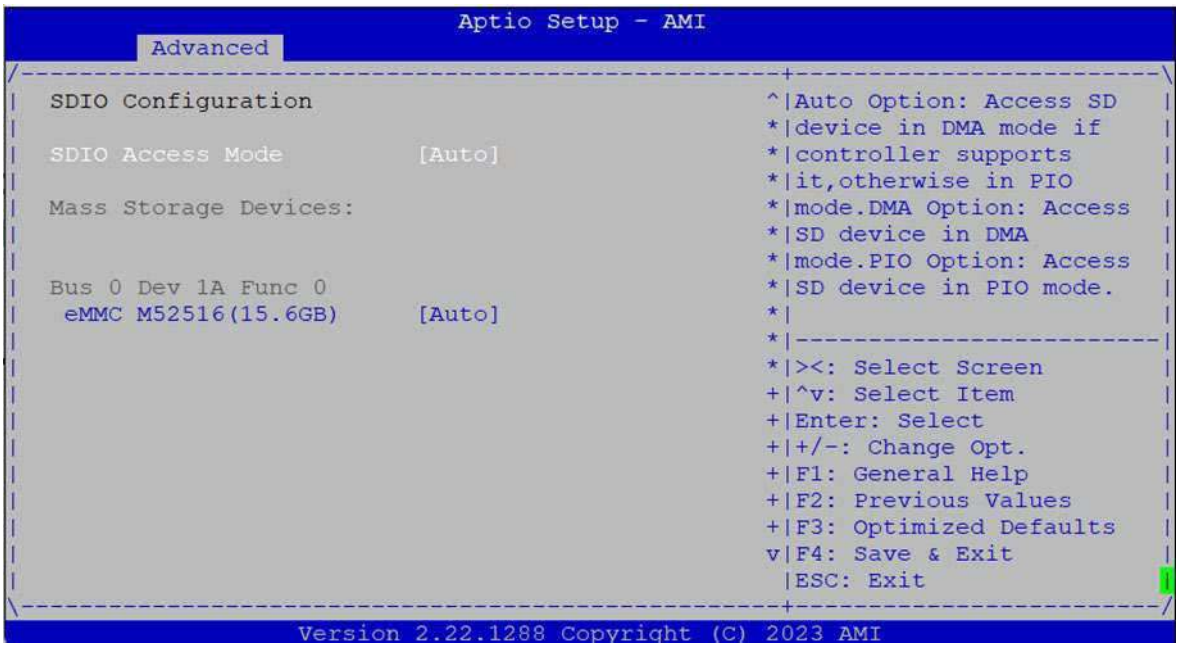
Feature	Options	Description
Network Stack	Disabled Enabled	Enable/Disable UEFI Network Stack
IPv4 PXE Support	Disabled Enabled	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	Disabled Enabled	Enable/Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.
IPv6 PXE Support	Disabled Enabled	Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.
IPv6 HTTP Support	Disabled Enabled	Enable/Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available.
PXE boot wait time	0	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.
Media detect count	1	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

CSM Configuration



Feature	Options	Description
CSM Support	Disabled Enabled	Enable/Disable CSM Support.

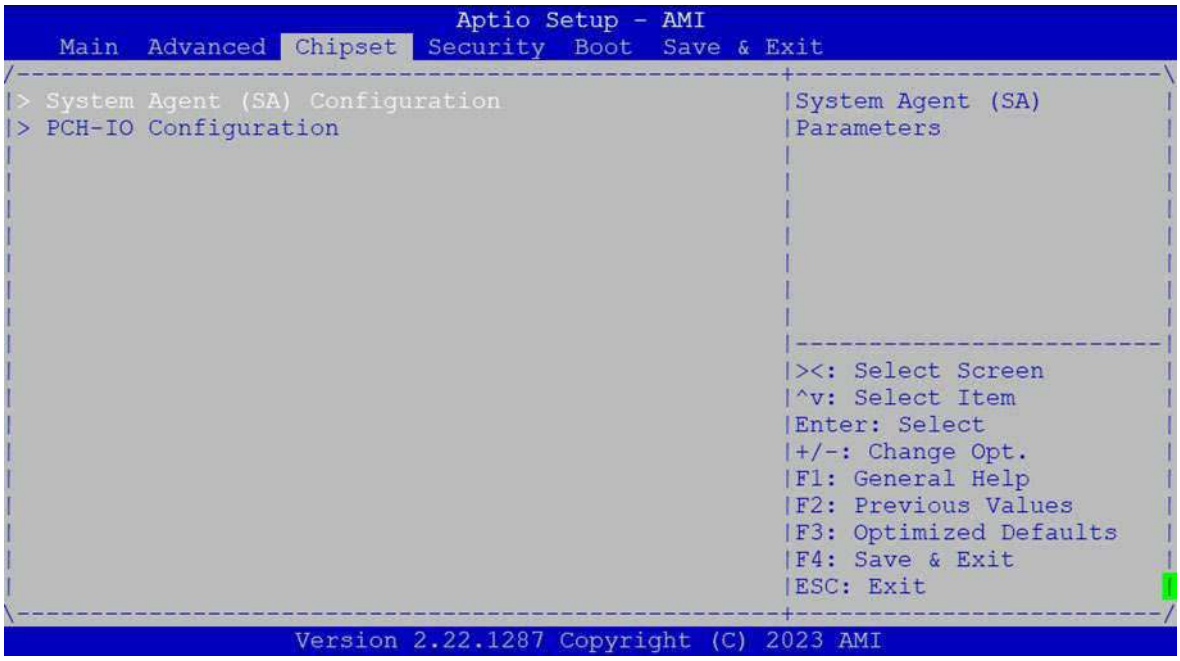
SDIO Configuration



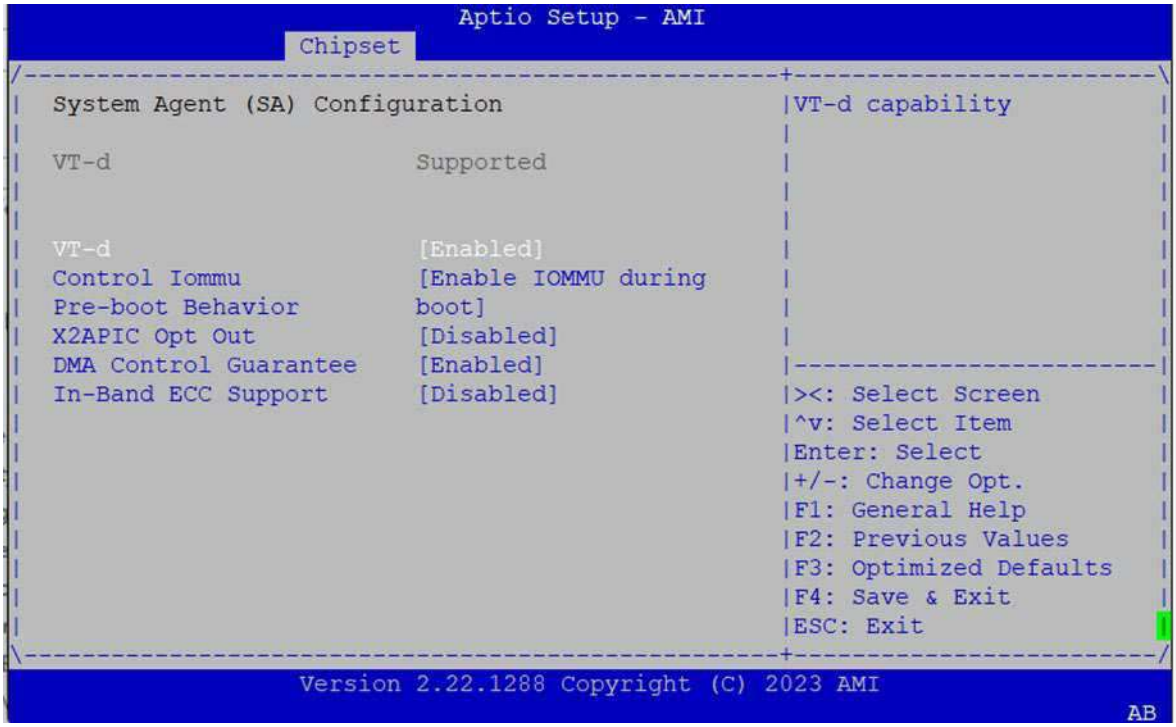
Feature	Options	Description
SDIO Access Mode	Auto ADMA SDMA PIO	Auto Option: Access SD device in DMA mode if controller supports it, otherwise in PIO mode. DMA Option: Access SD device in DMA mode. PIO Option: Access SD device in PIO mode.

Chipset Page

Select the "Chipset" item from the BIOS setup screen to enter the Chipset page. Users can select any of the items in the left frame of the screen.

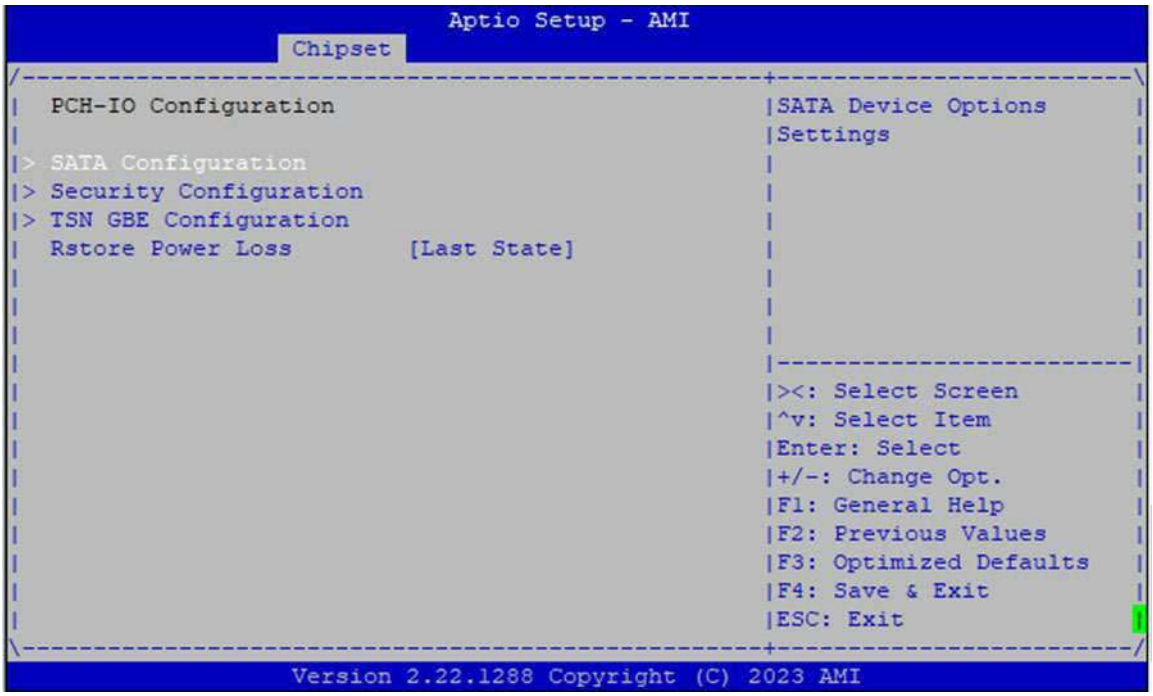


System Agent (SA) Configuration



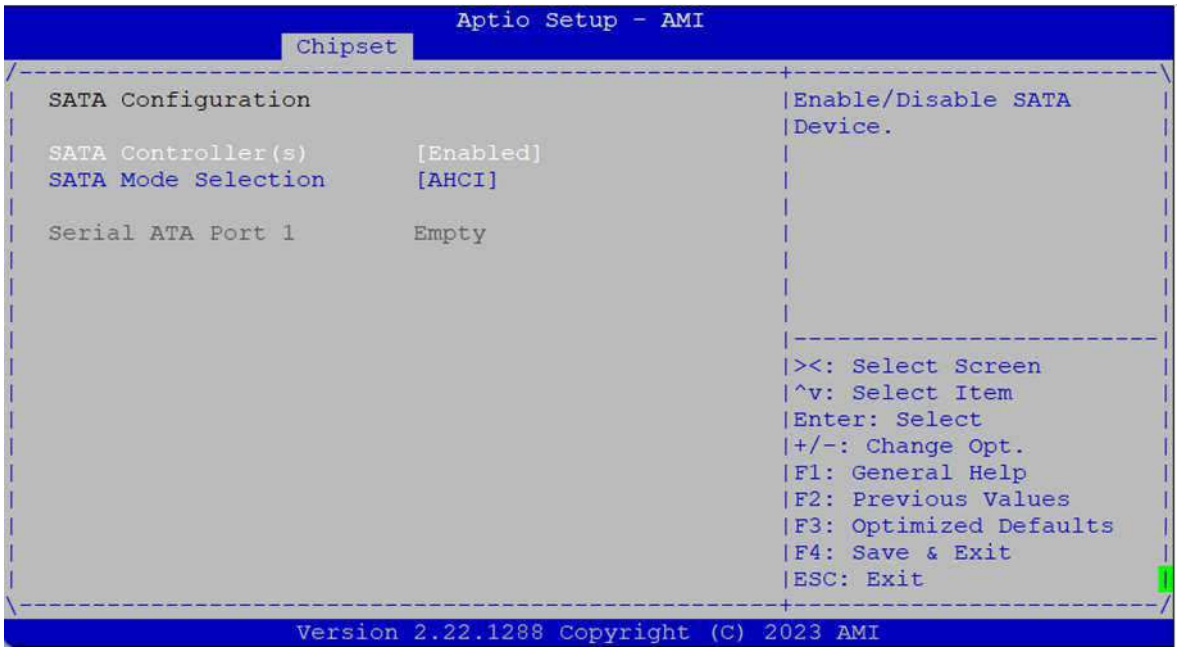
Feature	Options	Description
VT-d	Disabled Enable	VT-d capability
Control Iommu	Disable IOMMU Enable IOMMU during boot	Enable IOMMU in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)
X2APIC Opt Out	Enabled Disabled	Enable/Disable X2APIC_OPT_OUT bit
DMA Control Guarantee	Enabled Disabled	Enable/Disable DMA_CONTROL_GUARANTEE bit
In-Band ECC Support	Enabled Disabled	Enable/Disable In-Band ECC. Will be enabled if memory has symmetric configuration

PCH-IO Configuration



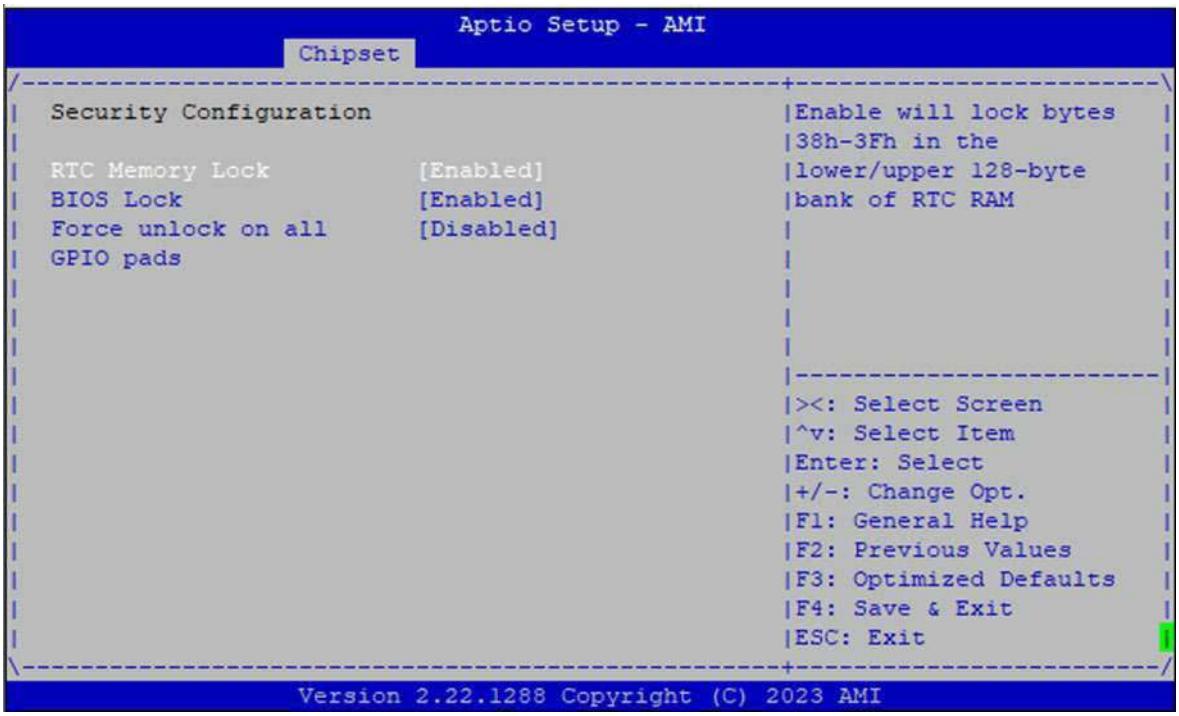
Feature	Options	Description
Restore AC Power Loss	Power On Power Off Last State	Specify what state to go to when power is re-applied after a power failure (G3 state).

SATA Configuration



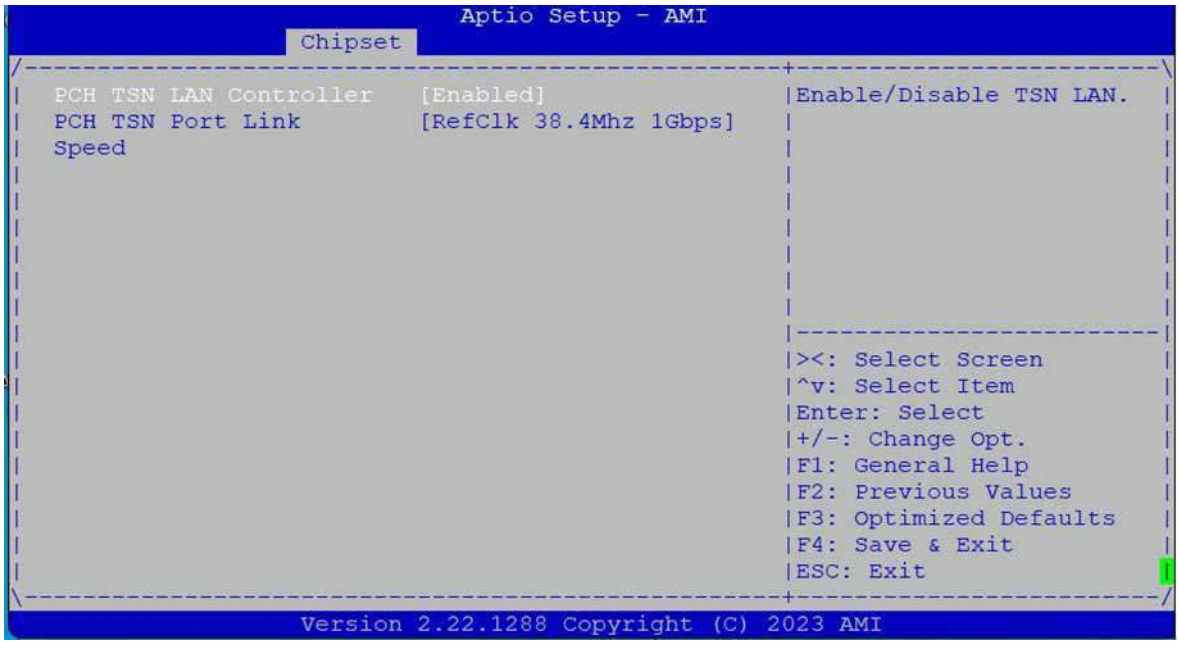
Feature	Options	Description
SATA Controller(s)	Enabled Disabled	Enable/Disable SATA Device.
SATA Mode Selection	AHCI	Determines how SATA controller(s) operate.

Security Configuration



Feature	Options	Description
RTC Memory Lock	Enabled Disabled	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM.
Bios Lock	Enabled Disabled	Enable/Disable the PCH BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.
Force unlock on all GPIO pads	Enabled Disabled	If Enabled BIOS will force all GPIO pads to be in unlocked state

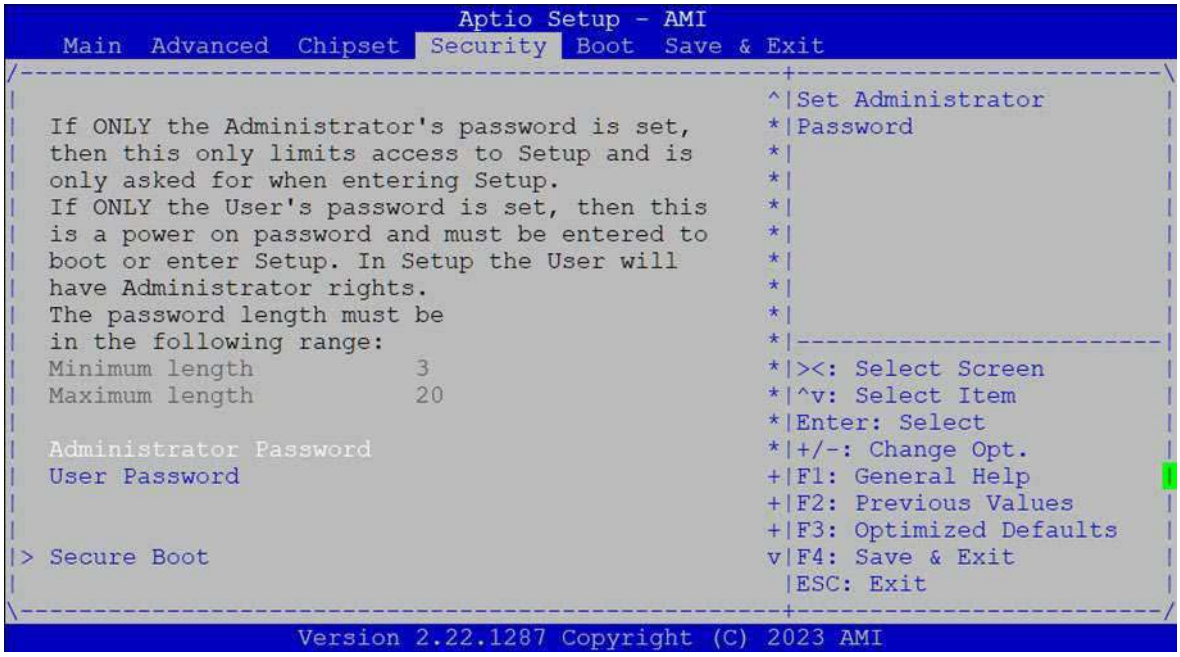
TSN GBE Configuration



Feature	Options	Description
PCH TSN LAN Controller	Enabled Disabled	Enable/Disable TSN LAN Device.
PCH TSN Port Link Speed	RefClk 38.4Mhz 1Gbps RefClk 38.4Mhz 2.5Gbps	Select TSN LANLink Speed

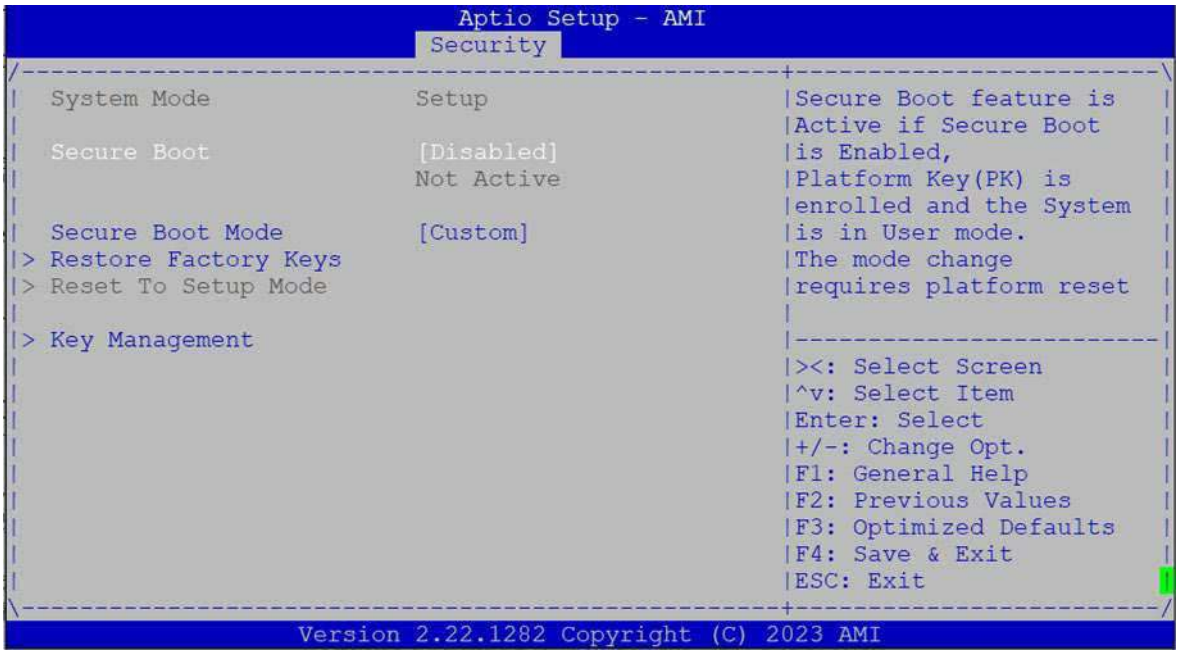
Security page

Select the "Security" item from the BIOS setup screen to enter the Security page. Users can select any of the items in the left frame of the screen.



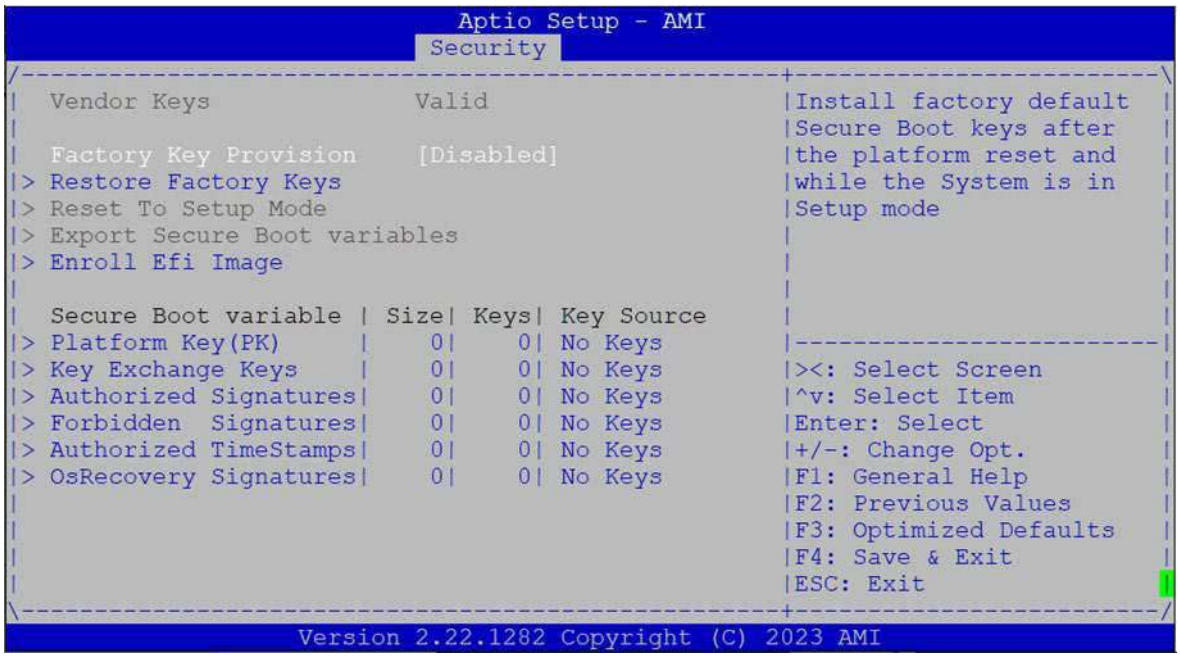
Feature	Description
Setup Administrator Password	If ONLY the Administrator's password is set, it only limits access to Setup and is only asked for when entering Setup.
User Password	If ONLY the User's password is set, it serves as a power-on password and must be entered to boot or enter Setup. In Setup, the User will have Administrator rights.

Secure Boot



Feature	Options	Description
Secure Boot	Disabled Enabled	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled and the System is in User mode. The mode change requires platform reset
Secure Boot Mode	Standard Custom	Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication

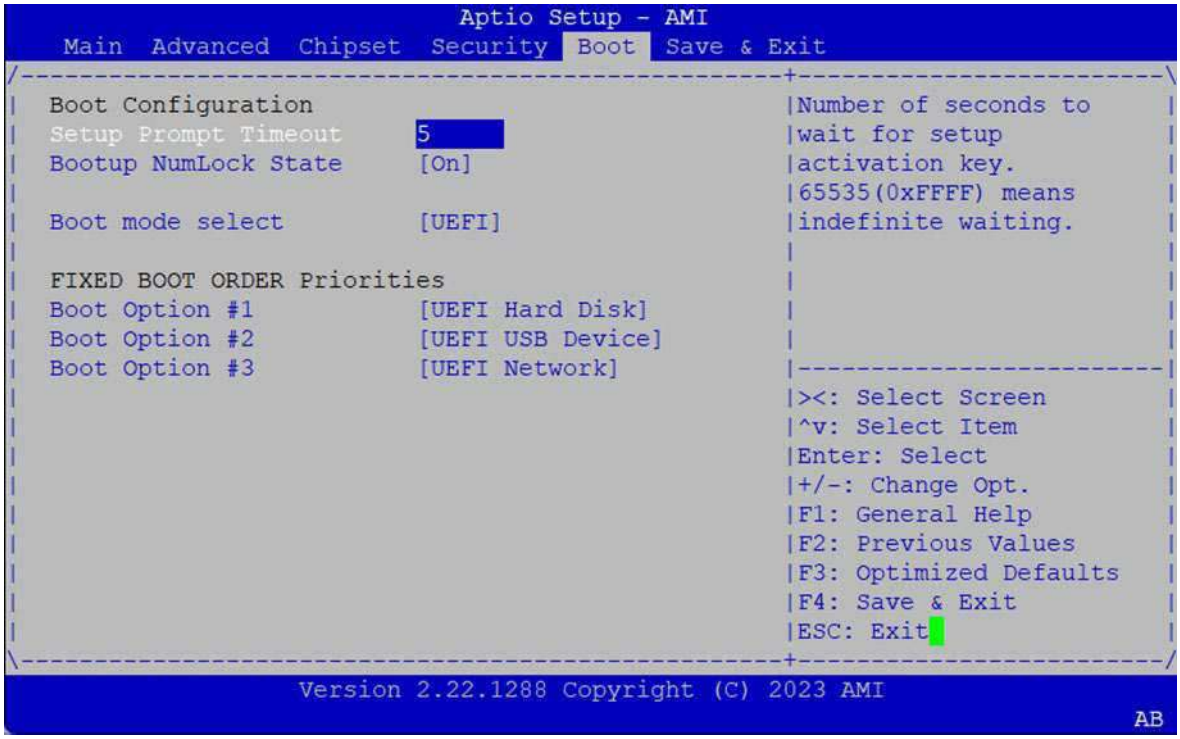
Key Management



Feature	Options	Description
Factory Key Provision	Disabled Enabled	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode
Restore Factory Keys	None	Force System to User Mode. Install factory default Secure Boot key databases
Reset To Setup Mode	None	Delete all Secure Boot key databases from NVRAM
Export Secure Boot variables	None	Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device
Enroll Efi Image	None	Allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db)

Boot Page

Select the "Boot" item from the BIOS setup screen to enter the Boot page. Users can select any of the items in the left frame of the screen.

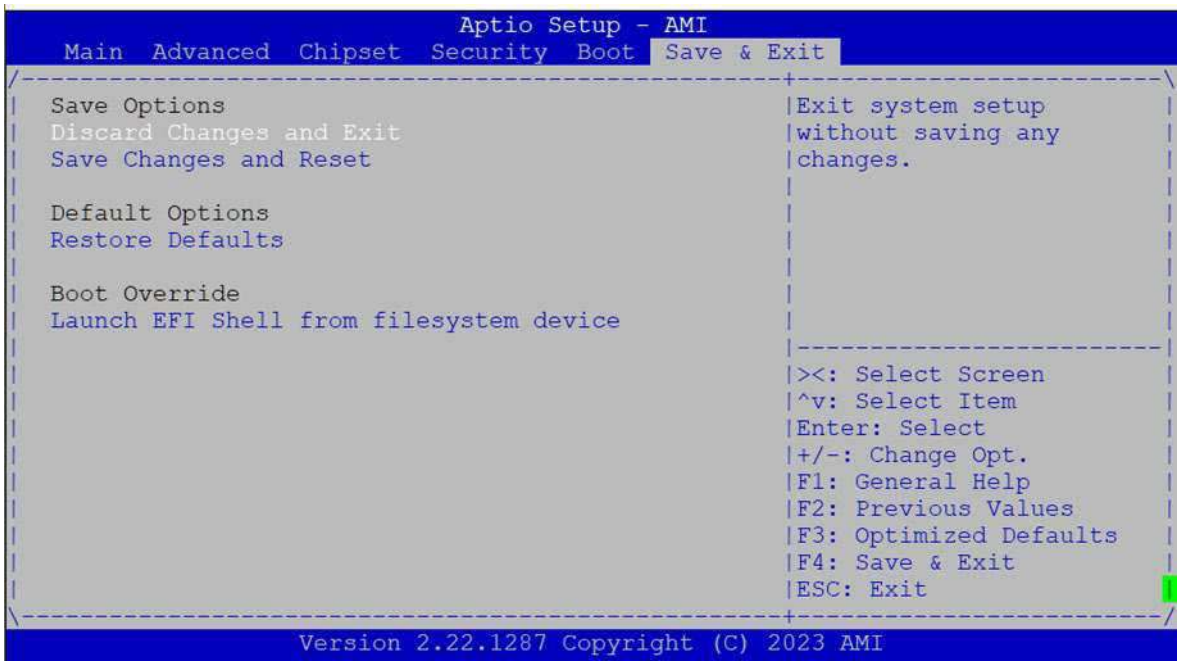


Feature	Options	Description
Setup Prompt Timeout	5	The number of seconds to wait for setup activation key. 65535 means indefinite waiting.
Bootup NumLock State	On Off	Select the keyboard NumLock state
Boot mode select	LEGACY UEFI DUAL	Select boot mode LEGACY/UEFI

- Default Boot Priority: **Hard Disk → USB → Network**
- Choose specifies boot device priority sequence from available Group device.
- Choose boot priority from boot option group.

Save and Exit Page

Select the "Save and Exit" item from the BIOS setup screen to enter the Save and Exit page. Users can select any of the items in the left frame of the screen.

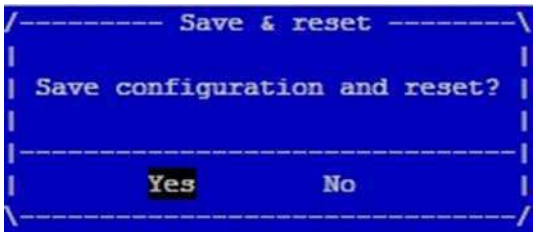


■ Discard Changes and Exit

Select this option to quit Setup without saving any modifications to the system configuration. The following window will appear after the "**Discard Changes and Exit**" option is selected. Select "**Yes**" to Discard changes and Exit Setup.

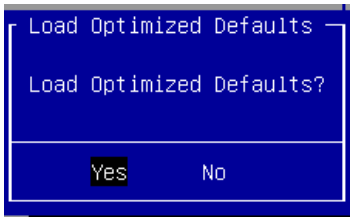
■ Save Changes and Reset

When Users have completed the system configuration changes, select this option to save the changes and reset from BIOS Setup in order for the new system configuration parameters to take effect. The following window will appear after selecting the "**Save Changes and Reset**" option is selected. Select "**Yes**" to Save Changes and reset.



■ Restore Defaults

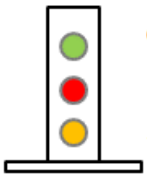
Restore default values for all setup options. Select "**Yes"** to load Optimized defaults.



PS: The items under Boot Override will depend on devices connected on the system.

APPENDIX A: LED INDICATOR EXPLANATIONS

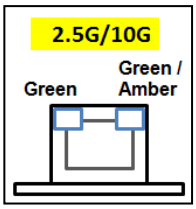
▸ System Power / Status / HDD Activity



Green : Power
Green / Red : Status
Amber : HDD

LED	COLOR ON LCM	COLOR ON BOARD	LED ACTION	DESCRIPTION
POWER	**Green**	**Green**	Steady	When system power on
	Off	Off	N/A	No power on
STATUS	**Green**	**Green**	Steady	control by GPIO
	Amber	**Red**	Steady	control by GPIO
	Off	Off	N/A	control by GPIO (Default) or No power on
HDD	**Amber**	**Amber**	Blinking	Blinking indicates HDD activity, Include SATA / NVME
	Off	Off	N/A	No data access or No power on

▸ RJ-45 LAN LED



2.5Gb RJ-45 Define:

Speed	Green (Active)	Green/Amber (Link)
10/100M	Blinking / Data access	OFF
1G	Blinking / Data access	ON (Amber)
2.5G	Blinking / Data access	ON (Green)
1. When cable is plug-in and network is linked. Both LED lights will be bright. The behavior is as defined. 2. Without the Cable plug-in, the LED should be off 3. If LAN Driver controls the LED, the behavior will follow the driver		

APPENDIX B: ENABLE 2.5GBE LAN FUNCTIONALITY

The NCA-1250 features the Intel® i226 Ethernet Controller. To activate the Intel® i226 2.5GbE LAN capabilities, ensure your Linux Kernel is updated to version 5.16.18 or later.

The OS Support matrix can be found here.

Open Source support for 2.5 GbE Intel® Ethernet Network Controllers (igc)

Product Specifications	Linux Driver	Linux*										FreeBSD*	VMware*	DPDK*	
		Kernel 5.4	Kernel 5.8	Kernel 5.16.18	RHEL 7.9	RHEL 8.1	RHEL 8.3	RHEL 8.6	Ubuntu* 18.04 LTS	Ubuntu* 20.04 LTS	Ubuntu* 22.04 LTS	13.0	ESXi8.0	20.05	22.07
I226-LM	igc	-	-	Yes	-	-	-	Yes	-	-	-	-	Yes	-	Yes
I226-V	igc	-	-	Yes	-	-	-	Yes	-	-	-	-	Yes	-	Yes
I226-IT	igc	-	-	Yes	-	-	-	Yes	-	-	-	-	Yes	-	Yes

If a customer requires assistance with a Kernel that is not mentioned in the table above, kindly contact our technical support team.

The NCA-1250A LAN1 (from GPY211 via SOC TSN) does not support auto-switching between 1G and 2.5G. Considering that most equipment is focused on 1G, the default setting for device port1 is 1G.

Users can manually change the LAN1 setting to 2.5G by following these steps:

Step 1. Press the <Tab> or <Del> key to enter the BIOS Setup utility.

Step 2. Select the Chipset page.

Step 3. Choose PCH-IO Configuration.

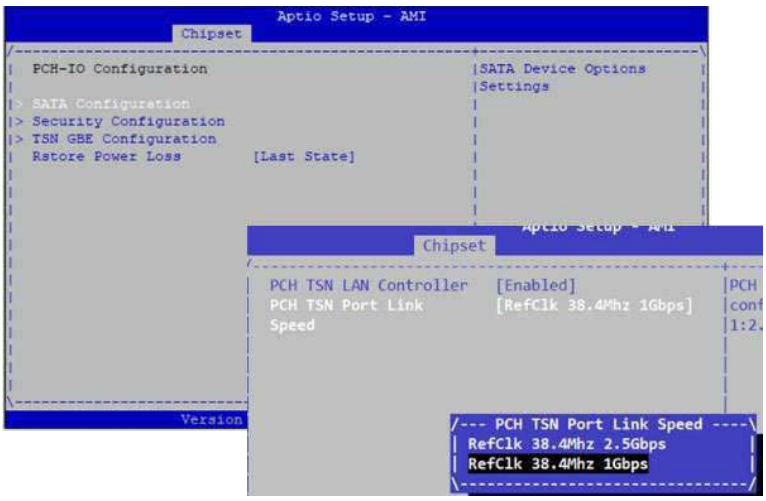
Step 4. Select TSN GBE Configuration.

Step 5. Choose RefC1k 38.4Mhz 1Gbps.

Step 6. Press F4: Save & Exit.

Notes: After adjusting the BIOS to 2.5G, if LAN1 is connected to 1G, the device will not automatically slow down to 2.5G. It's important to understand that 2.5G means only 2.5G; 1G or below must be set to 1G. The inability to auto-convert is due to the characteristics of the Intel® IC.

BIOS page → Chipset → PCH-IO Configuration → TSN GBE Configuration

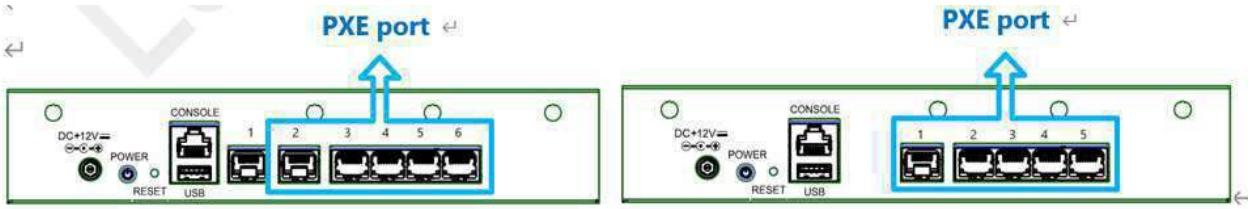


APPENDIX C: ENABLE PXE FUNCTIONALITY

The NCA-1250 is equipped with the Intel® i226 Ethernet Controller, which supports PXE (Preboot Execution Environment) functionality. By default, PXE is disabled in the BIOS. To use PXE boot, ensure that it is manually enabled in the BIOS settings.

PXE Support Details:

- LAN0 (from GPY211): PXE not supported
- LAN 1~5 (via Intel® i226): PXE supported



NCA-1250A/C/D SKU

NCA-1250B/E/F SKU

APPENDIX D: TERMS AND CONDITIONS

Warranty Policy

1. All products are under warranty against defects in materials and workmanship for a period of one year from the date of purchase.
2. The buyer will bear the return freight charges for goods returned for repair within the warranty period; whereas the manufacturer will bear the after service freight charges for goods returned to the user.
3. The buyer will pay for the repair (for replaced components plus service time) and transportation charges (both ways) for items after the expiration of the warranty period.
4. If the RMA Service Request Form does not meet the stated requirement as listed on "RMA Service," RMA goods will be returned at customer's expense.
5. The following conditions are excluded from this warranty:
   - Improper or inadequate maintenance by the customer
   - Unauthorized modification, misuse, or reversed engineering of the product
   - Operation outside of the environmental specifications for the product.

RMA Service

Requesting an RMA#

1. To obtain an RMA number, simply fill out and fax the "RMA Request Form" to your supplier.
2. The customer is required to fill out the problem code as listed. If your problem is not among the codes listed, please write the symptom description in the remarks box.
3. Ship the defective unit(s) on freight prepaid terms. Use the original packing materials when possible.
4. Mark the RMA# clearly on the box.

Note: Customer is responsible for shipping damage(s) resulting from inadequate/loose packing of the defective unit(s). All RMA# are valid for 30 days only; RMA goods received after the effective RMA# period will be rejected.

RMA Service Request Form

When requesting RMA service, please fill out the following form. Without this form enclosed, your RMA cannot be processed.

RMA No:	Reasons to Return: ▫ Repair(Please include failure details) ▫ Testing Purpose
Company:	Contact Person:
Phone No.	Purchased Date:
Fax No.:	Applied Date:
Return Shipping Address: _____ Shipping by: ▫ Air Freight ▫ Sea ▫ Express_____ ▫ Others:_____	

Item	Model Name	Serial Number	Configuration

Item	Problem Code	Failure Status

*Problem Code:

01:D.O.A.	07: BIOS Problem	13: SCSI	19: DIO
02: Second Time R.M.A.	08: Keyboard Controller Fail	14: LPT Port	20: Buzzer
03: CMOS Data Lost	09: Cache RMA Problem	15: PS2	21: Shut Down
04: FDC Fail	10: Memory Socket Bad	16: LAN	22: Panel Fail
05: HDC Fail	11: Hang Up Software	17: COM Port	23: CRT Fail
06: Bad Slot	12: Out Look Damage	18: Watchdog Timer	24: Others (Pls specify)

Request Party

Authorized Signature / Date

Confirmed By Supplier

Authorized Signature / Date

NCA-4240

1U 19" Rackmount Appliance With
Intel® 12th/13th/14th Gen Core™ i9/i7/i5/i3, Pentium®
Or Celeron® Processor

Images are for refernce only. See ordering information for SKU details.

Features

- Intel® 12th/13th/14th Gen Core™ i9/i7/i5/i3, Pentium® Or Celeron® Processor With H610E/Q670E Chipset (Codenamed Alder Lake S/Raptor Lake S/Raptor Lake Refresh)
- 1x GbE RJ45, 8x 2.5GbE RJ45, 1x NIC Module
- 3x Pairs Of Gen 3 SE LAN Bypass
- 2x 288-pin DIMM DDR5 Up To 5600MT/s (Max. 64GB)
- 2x USB 3.0 Ports, 2x 2.5" HDD/SSD
- 1x PCIe*8, 1x M.2 2230 Wifi
- 1x M.2 2280 NVMe, 1x M.2 2242 SATA

Specifications

Platform	
Form Factor	1U 19" Rackmount
Processor Options	Intel® 12th/13th/14th Gen Core™ i9/i7/i5/i3, Pentium® Or Celeron® Processor
CPU Socket	1 x LGA1700
Chipset	SKU A: Intel® H610E SKU B: Intel® Q670E
Security Acceleration	N/A
BIOS	AMI SPI Flash BIOS
System Memory	
Technology	DDR5 Up To 5600 MT/s Non-ECC UDIMM
Max. Capacity	64GB
Socket	2 x 288-pin DIMM
Networking	
Ethernet Ports	1 x GbE RJ45 With LED MGMT Via i219 8 x 2.5GbE RJ45 With LED Via i226
Bypass	3 Pairs Gen3 SE
NIC Module Slot	1
LOM	
IO Interface	N/A
OPMA Slot	N/A
I/O Interface	
Reset Button	1
LED	Power/Status/Storage
Power Button	1 x ATX Power Switch
Console	1 x RJ45
USB	2 x USB 3.0
LCD Module	2 x 20 Character LCM 4 x Keypads
Display	N/A
Power Input	AC Power Inlet on PSU

Storage	
HDD/SSD Support	2 x 2.5" HDD/SSD
Onboard Slots	SKU A: 1 x M.2 2242 (M Key) SATA SKU B: 1 x M.2 2242 (M Key) SATA & 1 x M.2 2280 (M Key) NVME (PCIe Gen4 x 4)
Expansion	
PCIe	1 x PCIE x8 Gen4 FH/HL (SKU B Only, Additional Riser Card Kit Required)
mini-PCIe or M.2	1 x M.2 2230 E Key (SKU B Only)
Miscellaneous	
Watchdog	Yes
Internal RTC with Li Battery	Yes
TPM	Optional
Cooling	
Processor	Passive CPU Heatsink
System	3 x Cooling Fans With Smart Fan
Environmental Parameters	
Temperature	0~40°C Operating -40~70°C Non-Operating
Humidity (RH)	5~90% Operating 5~95% Non-Operating
System Dimensions	
(WxDxH)	438 x 321 x 44 mm
Weight	4.71 kg
Package Dimensions	
(WxDxH)	588 x 494 x 185 mm
Weight	8.55 kg
Power	
Type / Watts	220W ATX Single PSU
Input	AC 100~240V, 4-2A, 60~50Hz
Certification	
Approvals and Compliance	RoHS, CE/FCC Class A, UKCA, UL

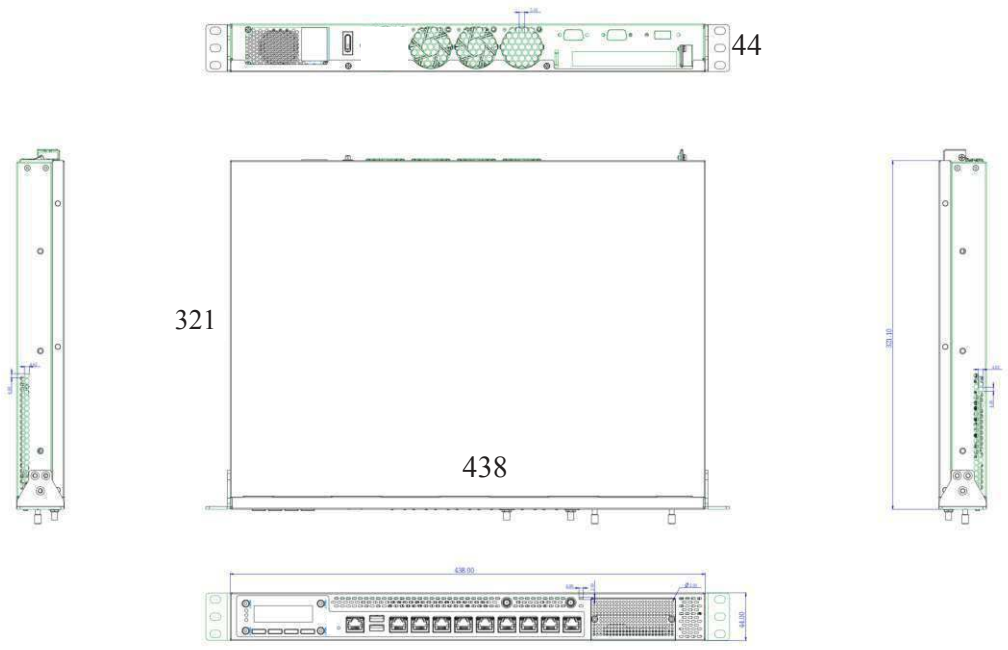
Network Appliance

Product I/O View

Images are for refernce only. See ordering information for SKU details.

- A LED
- B LCM & Keys
- C Reset Button
- D Console Port
- E USB 3.0
- F LAN Ports
- G NIC Slot
- H PCIe Slot
- I Cooling Fans
- J Power On/Off
- Power Inlet

Dimensions (WxDxH) 438 x 321 x 44 mm



Ordering Information

NCA-4240A	Intel® 12th/13th/14th Gen Core™ i9/i7/i5/i3 Processor With H610E, 2x DDR5 UDIMM, 8x 2.5GbE RJ45 With 3 Pairs Of Bypass, 1x 1GbE RJ45 MGMT, 1x NIC (PCIEx8 Only), 1x M.2 2242 SATA, 1x M.2 2230 (CNVIO Only), 1x LCM, 220W Single PSU
NCA-4240B	Intel® 12th/13th/14th Gen Core™ i9/i7/i5/i3 Processor With Q670E, 2x DDR5 UDIMM, 8x 2.5GbE RJ45 With 3 Pairs Of Bypass, 1x 1GbE RJ45 MGMT, 1x NIC (PCIEx8 Only), 1x M.2 2242 SATA, 1x M.2 2280 NVMe, 1x M.2 2230 (PCIE/CNVIO), 1x LCM, 220W Single PSU

Lanner

connect@lannerinc.com | www.lannerinc.com

Lanner

Network Appliance Platform

Hardware Platforms for Network Computing

NCA-4240
User Manual

Version: 1.6

Date of Release:2024-12-12

About this Document

This manual describes the overview of the various functionalities of this product, and the information you need to get it ready for operation. It is intended for those who are:

- responsible for installing, administering and troubleshooting this system or Information Technology professionals.
- assumed to be qualified in the servicing of computer equipment, such as professional system integrators, or service personnel and technicians.

The latest version of this document can be found on Lanner's official website, available either through the product page or through the Lanner Download Center page with a login account and password.

Icon Descriptions

The icons are used in the manual to serve as an indication of interest topics or important messages.

Icon	Usage
Note or Information	This mark indicates that there is something you should pay special attention to while using the product.
Warning or Important	This mark indicates that there is a caution or warning and it is something that could damage your property or product.

Online Resources

To obtain additional documentation resources and software updates for your system, please visit the Lanner Download Center. As certain categories of documents are only available to users who are logged in, please be registered for a Lanner Account at http://www.lannerinc.com/ to access published documents and downloadable resources.

Technical Support

In addition to contacting your distributor or sales representative, you could submit a request at our Lanner Technical Support and fill in a support ticket to our technical support department.

Documentation Feedback

Your feedback is valuable to us, as it will help us continue to provide you with more accurate and relevant documentation. To provide any feedback, comments or to report an error, please email contact@lannerinc.com. Thank you for your time.

Copyright and Trademarks

Contact Information

Taiwan Corporate Headquarters

Lanner Electronics Inc.

7F, No.173, Sec.2, Datong Rd.

Xizhi District, New Taipei City 22184,

Taiwan

立端科技股份有限公司

221 新北市汐止區

大同路二段 173 號 7 樓

T: +886-2-8692-6060

F: +886-2-8692-6101

E: contact@lannerinc.com

China

Beijing L&S Lancom Platform Tech. Co., Ltd.

Guodong LOFT 9 Layer No. 9 Huinan Road,

Huilongguan Town, Changping District, Beijing

102208 China

T: +86 010-82795600

F: +86 010-62963250

E: service@ls-china.com.cn

USA

Lanner Electronics Inc.

47790 Westinghouse Drive

Fremont, CA 94539

T: +1-855-852-6637

F: +1-510-979-0689

E: sales_us@lannerinc.com

Canada

Lanner Electronics Canada Ltd

3160A Orlando Drive

Mississauga, ON

L4V 1R5 Canada

T: +1 877-813-2132

F: +1 905-362-2369

E: sales_ca@lannerinc.com

Europe

Lanner Europe B.V.

Wilhelmina van Pruisenweg 104

2595 AN The Hague

The Netherlands

T: +31 70 701 3256

E: sales_eu@lannerinc.com

Acknowledgment

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of 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 instruction, 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 or more 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 transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Note

1. An unshielded-type power cord is required in order to meet FCC emission limits and also to prevent interference to the nearby radio and television reception. It is essential that only the supplied power cord be used.
2. Use only shielded cables to connect I/O devices to this equipment.
3. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Important

1. Operations in the 5.15-5.25GHz band are restricted to indoor usage only.
2. This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

Safety Guidelines

Follow these guidelines to ensure general safety:

- Keep the chassis area clear and dust-free during and after installation.
- Do not wear loose clothing or jewelry that could get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Disconnect all power by turning off the power and unplugging the power cord before installing or removing a chassis or working near power supplies
- Do not work alone if potentially hazardous conditions exist.
- Never assume that power is disconnected from a circuit; always check the circuit.

Consignes de sécurité

Suivez ces consignes pour assurer la sécurité générale :

- Laissez la zone du châssis propre et sans poussière pendant et après l'installation.
- Ne portez pas de vêtements amples ou de bijoux qui pourraient être pris dans le châssis. Attachez votre cravate ou écharpe et remontez vos manches.
- Portez des lunettes de sécurité pour protéger vos yeux.
- N'effectuez aucune action qui pourrait créer un danger pour d'autres ou rendre l'équipement dangereux.
- Coupez complètement l'alimentation en éteignant l'alimentation et en débranchant le cordon d'alimentation avant d'installer ou de retirer un châssis ou de travailler à proximité de sources d'alimentation.
- Ne travaillez pas seul si des conditions dangereuses sont présentes.
- Ne considérez jamais que l'alimentation est coupée d'un circuit, vérifiez toujours le circuit. Cet appareil génère, utilise et émet une énergie radiofréquence et, s'il n'est pas installé et utilisé conformément aux instructions des fournisseurs de composants sans fil, il risque de provoquer des interférences dans les communications radio.

Lithium Battery Caution

- There is risk of explosion if the battery is replaced by an incorrect type.
- Dispose of used batteries according to the instructions.
- Installation should be conducted only by a trained electrician or only by an electrically trained person who knows all installation procedures and device specifications which are to be applied.
- Do not carry the handle of power supplies when moving to another place.
- Please conform to your local laws and regulations regarding safe disposal of lithium battery.
- Disposal of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery can result in an explosion.
- Leaving a battery in an extremely high temperature environment can result in an explosion or the leakage of flammable liquid or gas.
- A battery subjected to extremely low air pressure may result in an explosion or the leakage of flammable liquid or gas.

Avertissement concernant la pile au lithium

- Risque d'explosion si la pile est remplacée par une autre d'un mauvais type.
- Jetez les piles usagées conformément aux instructions.
- L'installation doit être effectuée par un électricien formé ou une personne formée à l'électricité connaissant toutes les spécifications d'installation et d'appareil du produit.
- Ne transportez pas l'unité en la tenant par le câble d'alimentation lorsque vous déplacez l'appareil.

Operating Safety

- Electrical equipment generates heat. Ambient air temperature may not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Be sure that the room in which you choose to operate your system has adequate air circulation.
- Ensure that the chassis cover is secure. The chassis design allows cooling air to circulate effectively. An open chassis permits air leaks, which may interrupt and redirect the flow of cooling air from internal components.
- Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. ESD damage occurs when electronic components are improperly handled and can result in complete or intermittent failures. Be sure to follow ESD-prevention procedures when removing and replacing components to avoid these problems.

- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. If no wrist strap is available, ground yourself by touching the metal part of the chassis.
- Periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohms (Mohms).

Sécurité de fonctionnement

- L'équipement électrique génère de la chaleur. La température ambiante peut ne pas être adéquate pour refroidir l'équipement à une température de fonctionnement acceptable sans circulation adaptée. Vérifiez que votre site propose une circulation d'air adéquate.
- Vérifiez que le couvercle du châssis est bien fixé. La conception du châssis permet à l'air de refroidissement de bien circuler. Un châssis ouvert laisse l'air s'échapper, ce qui peut interrompre et rediriger le flux d'air frais destiné aux composants internes.
- Les décharges électrostatiques (ESD) peuvent endommager l'équipement et gêner les circuits électriques. Des dégâts d'ESD surviennent lorsque des composants électroniques sont mal manipulés et peuvent causer des pannes totales ou intermittentes. Suivez les procédures de prévention d'ESD lors du retrait et du remplacement de composants.
- Portez un bracelet anti-ESD et veillez à ce qu'il soit bien au contact de la peau. Si aucun bracelet n'est disponible, reliez votre corps à la terre en touchant la partie métallique du châssis.
- Vérifiez régulièrement la valeur de résistance du bracelet antistatique, qui doit être comprise entre 1 et 10 mégohms (Mohms).

Mounting Installation Precautions

The following should be put into consideration for rack-mount or similar mounting installations:

- Do not install and/or operate this unit in any place that flammable objects are stored or used in.
- The installation of this product must be performed by trained specialists; otherwise, a non-specialist might create the risk of the system's falling to the ground or other damages.
- Lanner Electronics Inc. shall not be held liable for any losses resulting from insufficient strength for supporting the system or use of inappropriate installation components.
- Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
- Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Reliable Grounding - Reliable grounding of rack mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
- Instruction for the installation of the conductor to building earth by a skilled person.

Electrical Safety Instructions

Before turning on the device, ground the grounding cable of the equipment. Proper grounding (grounding) is very important to protect the equipment against the harmful effects of external noise and to reduce the risk of electrocution in the event of a lightning strike. To uninstall the equipment, disconnect the ground wire after turning off the power. A ground wire (green-and-yellow) is required and the part connecting the conductor must be greater than 6 mm2 or 8AWG.

Consignes de sécurité électrique

- Avant d'allumer l'appareil, reliez le câble de mise à la terre de l'équipement à la terre.
- Une bonne mise à la terre (connexion à la terre) est très importante pour protéger l'équipement contre les effets néfastes du bruit externe et réduire les risques d'électrocution en cas de foudre.
- Pour désinstaller l'équipement, débranchez le câble de mise à la terre après avoir éteint l'appareil.
- Un câble de mise à la terre est requis et la zone reliant les sections du conducteur doit faire plus de 6 mm2 ou 8 AWG.

Table of Contents

CHAPTER 1: PRODUCT OVERVIEW

The NCA-4240 features LGA 1700 socket, up to 64GB of DDR5 memory capacity at 4800MHz, comprehensive Intel® H610E/Q670E chipset, 1x Gbe RJ45, 8x 2.5 Gbe RJ45 with 3 pairs of bypass, 1x RJ45 console and 1x NIC slot.

Main Features

- Intel® Alder Lake S/Raptor Lake S/Raptor Lake S Refresh Processor with H610E/Q670E Chipset
- 1x GbE RJ45, 8x 2.5GbE RJ45, 1x NIC Module
- 3x Pairs of Gen 3 SE LAN Bypass
- 2x 288-pin DIMM DDR5 4800/5600 MHz (Max.64GB)
- 2x USB 3.0 Ports, 2x 2.5" HDD/SSD

Package Content

- 1x NCA-4240 Network Security Platform
- 1x Power Cable
- 1x RJ45 Console Cable; 2x SATA Cables
- 1x CPU Heatsink; 1x Air Duct
- 2x Short Ear Rack Mount Kit with Screws

Optional Kits

Model	Description
TPM Kit	IAC-TPM04A TPM Module
Riser Card Kit	PCIE Gen 3 Riser Card Kit for rear FH/HL PCIe expansion card
IO Card Kit	Upper-layer expansion card support for 2x 10G SFP **NOTE**: To install this IO Card Kit, the chassis must be replaced with the NCC-4240B chassis (By Project Only)
Wi-Fi Kit NCA-4240	AX201, Wi-Fi Module Kit with Antenna (CNVIO) and RF cover
Wi-Fi Kit NCA-4240	AX210, Wi-Fi Module Kit with Antenna (PCIe) and RF cover
Slide Rail Kit	Standard Slide Rail Kit, 438mm
Case Open Kit NCA-4240	Case Open Kit with 10cm cable and bracket

Note
For assistance in finding specific compatible components or kits, please inquire to your dealer or sales representative.

Ordering Information

SKU No.	Main Features
NCA-4240A	Intel® Alder Lake-S/Raptor Lake S/Raptor Lake S Refresh Processor, PCH H610E, 2x DDR5 U-DIMM, 1x Gbe RJ45, 8x 2.5 GbE RJ45 with 3 Pairs of Bypass, 1x RJ45 Console, 1x NIC Module Slot (1x PCIE*8), Single PSU
NCA-4240B	Intel® Alder Lake-S/Raptor Lake S/Raptor Lake S Refresh Processor, PCH Q670E, 2x DDR5 U-DIMM, 1x Gbe RJ45, 8x 2.5 GbE RJ45 with 3 Pairs of Bypass, 1x RJ45 Console, 1x NIC Module Slot (1x PCIE*8), Single PSU

System Specifications

Form Factor		1U 19" Rackmount
Platform	Processor Options	Intel® Alder Lake S/Raptor Lake S/Raptor Lake S Refresh
	CPU Socket	1x LGA1700 socket
	Chipset	SKU A: Intel® H610E SKU B: Intel® Q670E
BIOS		AMI SPI Flash BIOS
System Memory	Technology	DDR5 4800/5600 Non-ECC UDIMM
	Max. Capacity	Up to 64GB
	Socket	2x 288-pin DIMM
Networking	Ethernet Ports	1x GbE RJ45 w/ LED MGMT via i219; 8x 2.5GbE RJ45 w/ LED via i226
	Bypass	3 Pairs Gen3 SE
	NIC Module Slot	1x NIC Slot
LOM	IO Interface	N/A
	OPMA slot	N/A
I/O Interface	Reset Button	1x Reset Button
	LED Indicators	Power/Status/Storage LED Indicators
	Power Button	1x ATX Power Switch
	Console Port	1x RJ45 Console Port
	USB Port	2x USB 3.0 Port
	LCD Module	2x20 Character LCM, 4x Keypads
	Power input	AC Power Inlet on PSU
Storage	HDD/SSD Support	2x 2.5" Internal HDD/SSD Bays
	Onboard Slots	SKU A: 1x M.2 2242 M-Key SATA SKU B: 1x M.2 2242 M-Key SATA & 1x M.2 2280 M-Key NVME (PCIe Gen4x4)
Expansion	PCIe	1x PCIe x8 Gen4 FH/HL (SKU B only)
	Mini-PCIe	1x M.2 2230 E-Key (SKU B only)
Miscellaneous	Watchdog	Yes
	Internal RTC with Li Battery	Yes
	TPM	N/A; TPM 2.0 (Optional)
Cooling	Processor	Passive CPU Heatsink
	System	3x Cooling Smart Fans
Environmental Parameters	Temperature	0~40°C Operating; -40~70°C Non-Operating
	Humidity (RH)	5~90% Operating; 5~ 95% Non-Operating
System Dimensions	(WxDxH)	438mm x 321mm x 44mm
	Weight	19.3kg
Package Dimensions	(WxDxH)	533mm x 494mm x 185mm
	Weight	TBA
Power	Type/Watts	220W ATX Single PSUs
	Input	AC 90-264V@ 47~63 Hz
Approvals and Compliance		RoHS, CE/FCC Class A, UKCA, UL

Front Panel

No.	Description	
F1	LED Indicators	 System Power System Status HDD Activity
F2	Control Panel	2x20 Character LCM & 4x Keypad
F3	Reset Button	1x Reset Button
F4	Console Port	1x RJ45 Console Port
F5	USB Ports	2x USB 3.0 Ports
F6	LAN Port	1x 1GbE RJ45; 8x 2.5GbE RJ45
F7	NIC Slot	1x PCIe x8 for Front Slim Type NIC module (Slot1) NOTE: Unable to support dual PCIe*4 configuration

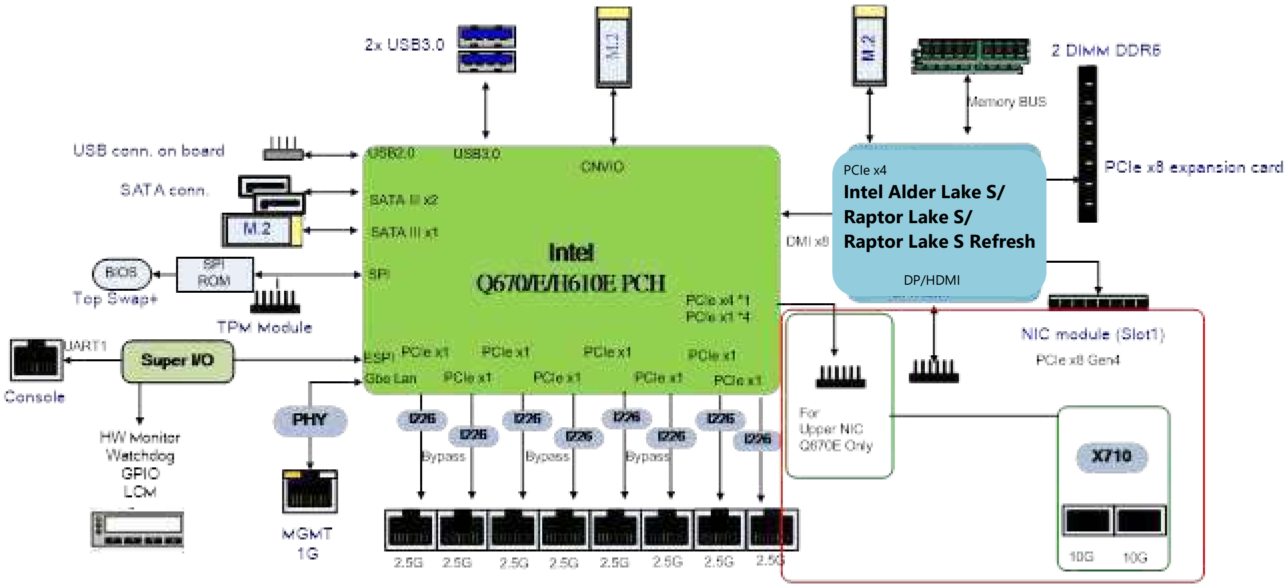
Rear Panel

No.	Description	
R1	PCIe Expansion Slot	FH/HL Size PCIe Slot for 1x PCIE*8 (Optional)
R2	Cooling Fan	3x Smart Fans
R3	Power Button	1x Power On/Off Switch
R4	Power Inlet	AC Power Inlet on PSU

Motherboard Information

Block Diagram

The block diagram indicates how data flows among components on the motherboard. Please refer to the following figure for your motherboard's layout design.

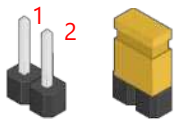
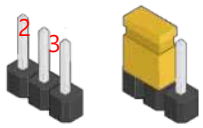
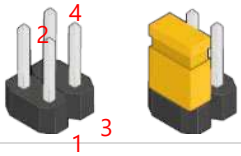


Internal Jumpers

The pin headers on the motherboard play a crucial role in controlling key functions. By placing a shunt (jumper) over the specified pins (whose numbers are labeled on the circuit board around the pin header), you can enable or disable specific features. Always ensure that your system is powered off before adjusting the jumpers.

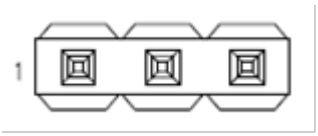
Jumper Setting

To short the designated pins, push the jumper down on them so that they become **SHORT**. To make the pins setting **OPEN**, simply remove the jumper cap.

2-pin Header	3-pin Header	4-pin Header
		
Open Short	Open (1-2) Jumped	Open (1-2) Jumped

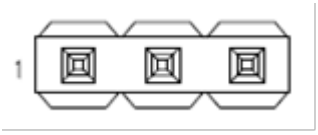
1. JRTC1：RTC Reset

Jumper	Description
1-2 (Default)	Normal
2-3	Reset register bits in the RTC well



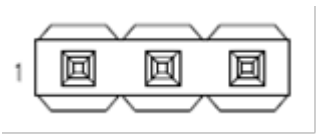
2. JCMOS1: Secured RTC Reset

Jumper	Description
1-2 (Default)	Normal
2-3	Reset the manageability register bits in the RTC well



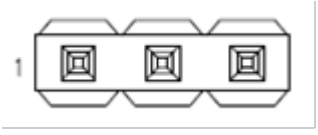
3. JRST1: HW/SW Reset Selection

Jumper	Description
1-2	Hardware Reset
2-3 (Default)	Software Reset



4. JMCU1: Update LPC844 FW

Jumper	Description
1-2 (Default)	Normal
2-3	ISP Mode



Connectors Pin Assignment

1. JOPEN1: Case Open Wafer

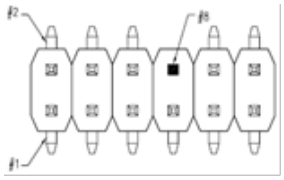
Pin No.	Description	Pin No.	Description
1	GND	2	PCH_INTRUDER_HDR_N

2. JPWR1: Power On/Off Wafer

Pin No.	Description	Pin No.	Description
1	PWRBTN_N	2	GND

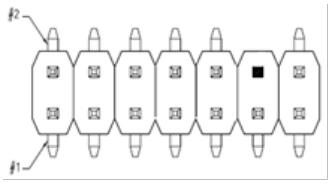
3. JESPI1: ESPI Debug 80 Port Pin Header

Pin No.	Description	Pin No.	Description
1	ESPI_CLK_SIO	2	ESPI_IO1_SIO
3	ESPI_RST_SIO_N	4	ESPI_IO0_SIO
5	ESPI_CS0_SIO_N	6	+V3P3S
7	ESPI_IO3_SIO	-	--
9	ESPI_IO2_SIO	10	GND
11	+V3P3DSW	12	NC



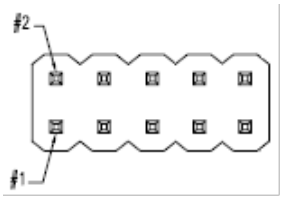
4. JSPI_TPM1: SPI and TPM Pin Header

Pin No.	Description	Pin No.	Description
1	SPI_HD#	2	NC
3	SPI_CS0_SF_N	4	+V3P3A_TPM
5	SPI_MISO_TPM	6	SPI_HOLD_SF_N
7	NC	8	SPI_CLK_TPM
9	GND	10	SPI_MOSI_TPM
11	IRQ_TPM_N	-	--
13	SPI_CS2_TPM_N	14	PLTRST_TPM_N



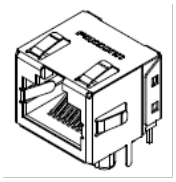
5. JGPIO1: GPIO Pin Header

Pin No.	Description	Pin No.	Description
1	GPO_B_1	2	GPI_B_1
3	GPO_B_2	4	GPI_B_2
5	GPO_B_3	6	GPI_B_3
7	GPO_B_4	8	GPI_B_4
9	GND	10	GND



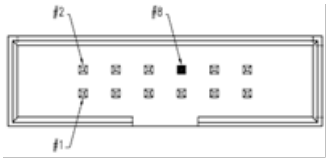
6. COM1: Console RJ45

Pin No.	Description	Pin No.	Description
1	COM1_RTS_N	5	GND
2	COM1_DTR_N	6	COM1_RXD
3	COM1_TXD	7	COM1_DSR_N
4	GND	8	COM1_CTS_N



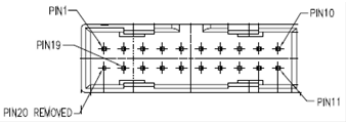
7. COM2: Serial Port 2 Box Header

Pin No.	Description	Pin No.	Description
1	+V5S	2	HDD_LED_N
3	COM2_DCD_N	4	COM2_DSR_N
5	COM2_RXD	6	COM2_RTS_N
7	COM2_TXD	-	--
9	COM2_DTR_N	10	COM2_CTS_N
11	GND_COM	12	COM2_RI_N



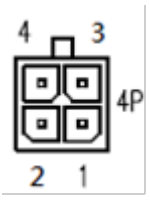
8. JUSB1: Internal USB Box Header

Pin No.	Description	Pin No.	Description
1	+USB3_PW	11	USB2_4+
2	USB3_R3-	12	USB2_4-
3	USB3_R3+	13	GND_USB2
4	GND_USB2	14	USB3_T4+
5	USB3_T3-	15	USB3_T4-
6	USB3_T3+	16	GND_USB2
7	GND_USB2	17	USB3_R4+
8	USB2_3-	18	USB3_R4-
9	USB2_3+	19	+USB4_PW
10	NC	-	--



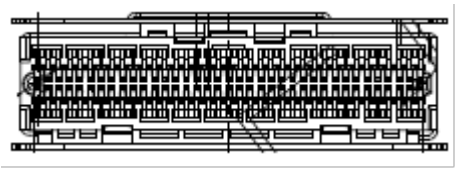
9. ATX3: IO Power Connector

Pin No.	Description
1	GND
2	GND
3	+V3P3S
4	+V12S



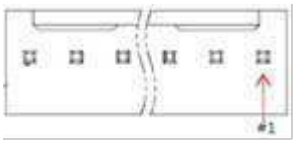
10. JSL1: IO Slim SAS Connector

Pin No.	Description	Pin No.	Description	Pin No.	Description	Pin No.	Description
A1	GND	A20		B1	GND	B20	
A2	CLK_SLIM_DP	A21		B2	PCIE21_TX_C_DP	B21	
A3	CLK_SLIM_DN	A22	GND	B3	PCIE21_TX_C_DN	B22	GND
A4	GND	A23		B4	GND	B23	
A5	PCIE21_RX_DP	A24		B5	PCIE22_TX_C_DP	B24	
A6	PCIE21_RX_DN	A25	GND	B6	PCIE22_TX_C_DN	B25	GND
A7	GND	A26		B7	GND	B26	
A8	PCIE22_RX_DP	A27		B8	PCIE23_TX_C_DP	B27	
A9	PCIE22_RX_DN	A28	GND	B9	PCIE23_TX_C_DN	B28	GND
A10	GND	A29		B10	GND	B29	SMB_CLK
A11	PCIE23_RX_DP	A30		B11	PCIE24_TX_C_DP	B30	SMB_DATA
A12	PCIE23_RX_DN	A31	GND	B12	PCIE24_TX_C_DN	B31	GND
A13	GND	A32		B13	GND	B32	PCH_WAKE_N
A14	PCIE24_RX_DP	A33		B14		B33	PCIE1_PRSNT1_N
A15	PCIE24_RX_DN	A34	GND	B15		B34	GND
A16	GND	A35	PCIE1_PRSNT0_N	B16	GND	B35	+V3P3_DUAL
A17		A36	PLTRST_PCIE3_N	B17		B36	+V3P3_DUAL
A18		A37	GND	B18		B37	GND
A19	GND			B19	GND		



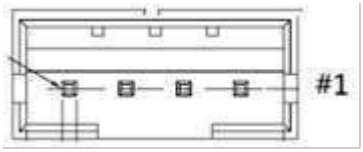
11. FAN1 ~ FAN3: FAN Connector

Pin No.	Description
1	GND
2	+V12S
3	HM_FAN_TECH_IN1
4	HM_FAN_TECH_IN2
5	HM_PWMOUT1



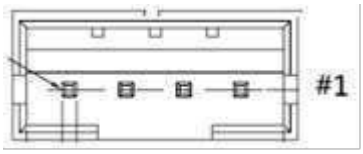
12. CON1: LPC844 Flash Write Wafer

Pin No.	Description
1	+V3P3DSW
2	MCU_RXD
3	GND
4	MCU_TXD



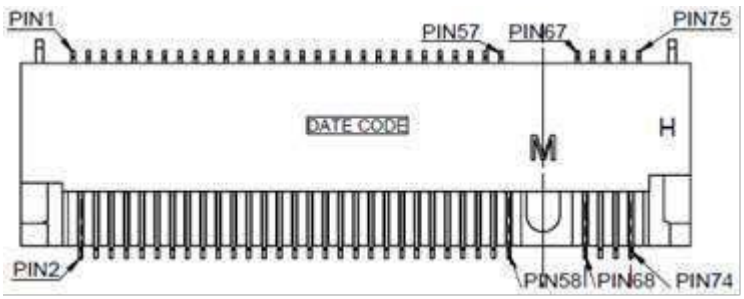
13. CON2: LPC844 SW Debug Wafer

Pin No.	Description
1	+V3P3DSW
2	GND
3	MCU_CLK
4	MCU_DIO



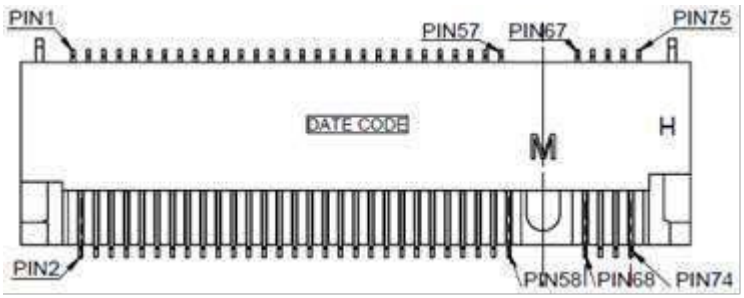
14. NGFF1: PCIe M.2 M-Key Connector

Pin No.	Description	Pin No.	Description	Pin No.	Description	Pin No.	Description
1	GND	39	GND	2	+P3V3	40	NC
3	GND	41	NGFF_CRX_DTX_N0	4	+P3V3	42	NC
5	NGFF_CRX_DTX_N3	43	NGFF_CRX_DTX_P0	6	NC	44	NC
7	NGFF_CRX_DTX_P3	45	GND	8	NC	46	NC
9	GND	47	NGFF_CTX_DRX_N0	10	M2_ACT_LED_L	48	NC
11	NGFF_CTX_DRX_N3	49	NGFF_CTX_DRX_P0	12	+V3P3S	50	RST_M2_N
13	NGFF_CTX_DRX_P3	51	GND	14	+V3P3S	52	M2_CLKREQ_N
15	GND	53	CLK_CPU_M2_DN	16	+V3P3S	54	M2_PEWAKE_N
17	NGFF_CRX_DTX_N2	55	CLK_CPU_M2_DP	18	+V3P3S	56	NC
19	NGFF_CRX_DTX_P2	57	GND	20	NC	58	NC
21	GND	59	KEY	22	NC	60	KEY
23	NGFF_CTX_DRX_N2	61	KEY	24	NC	62	KEY
25	NGFF_CTX_DRX_P2	63	KEY	26	NC	64	KEY
27	GND	65	KEY	28	NC	66	KEY
29	NGFF_CRX_DTX_N1	67	NC	30	NC	68	CLK32K_M2_R
31	NGFF_CRX_DTX_P1	69	M2_PEDET	32	NC	70	+V3P3S
33	GND	71	GND	34	NC	72	+V3P3S
35	NGFF_CTX_DRX_N1	73	GND	36	NC	74	+V3P3S
37	NGFF_CTX_DRX_P1	75	GND	38	NC	-	--



15. NGFF2: SATA M.2 M-Key Connector

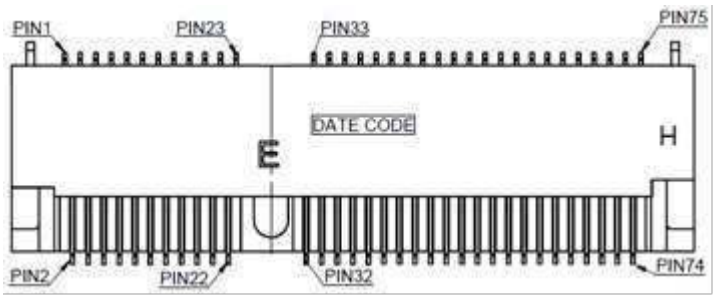
Pin No.	Description	Pin No.	Description	Pin No.	Description	Pin No.	Description
1	GND	39	GND	2	+V3P3S	40	NC
3	GND	41	SATA_RX6_P	4	+V3P3S	42	NC
5	NC	43	SATA_RX6_N	6	NC	44	NC
7	NC	45	GND	8	NC	46	NC
9	GND	47	SATA_TX6_N	10	NC	48	NC
11	NC	49	SATA_TX6_P	12	+V3P3S	50	NC
13	NC	51	GND	14	+V3P3S	52	NC
15	GND	53	NC	16	+V3P3S	54	NC
17	NC	55	NC	18	+V3P3S	56	NC
19	NC	57	GND	20	NC	58	NC
21	GND	59	KEY	22	NC	60	KEY
23	NC	61	KEY	24	NC	62	KEY
25	NC	63	KEY	26	NC	64	KEY
27	GND	65	KEY	28	NC	66	KEY
29	NC	67	NC	30	NC	68	NC
31	NC	69	M2_PEDET	32	NC	70	+V3P3S
33	GND	71	GND	34	NC	72	+V3P3S
35	NC	73	GND	36	NC	74	+V3P3S
37	NC	75	GND	38	NC	-	--



16. NGFF3: CNVio M.2 E-Key Connector

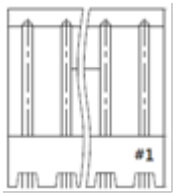
Pin No.	Description	Pin No.	Description	Pin No.	Description	Pin No.	Description
1	GND	39	GND	2	+V3P3_WIFI	40	CLINK_DATA
3	USB2_DP14	41	PCIE16_RX_DP	4	+V3P3_WIFI	42	CLINK_CLK
5	USB2_DN14	43	PCIE16_RX_DN	6	WLAN_LED1	44	M2_COEX3
7	GND	45	GND	8	M.2_PCMCLK	46	M2_COEX2
9	CNV_WR_1_DN	47	CLK_PCH_M2_DP	10	M.2_RST_N	48	M2_COEX1
11	CNV_WR_1_DP	49	CLK_PCH_M2_DN	12	M.2_PCMIN	50	M2_E_SUSCLK
13	GND	51	GND	14	M.2_PCMOUT	52	M2_E_RST#
15	CNV_WR_0_DN	53	E_CLKREQ_N	16	WLAN_LED2	54	M.2_BT_RF_KILL_N

17	CNV_WR_0_DP	55	PCH_WAKE_N	18	GND	56	M.2_WIFI_RF_KILL_N
19	GND	57	GND	20	UART_BT_WAKE_N	58	NC
21	CNV_WR_CLK_DN	59	CNV_WT_1_DN	22	CNV_BRI_RSP	60	NC
23	CNV_WR_CLK_DP	61	CNV_WT_1_DP	24	KEY	62	NC
25	KEY	63	GND	26	KEY	64	NC
27	KEY	65	CNV_WT_0_DN	28	KEY	66	NC
29	KEY	67	CNV_WT_0_DP	30	KEY	68	NC
31	KEY	69	GND	32	CNV_RGI_DT	70	NC
33	GND	71	CNV_WT_CLK_DN	34	CNV_RGI_RSP	72	+V3P3_WIFI
35	PCIE16_TX_C_DP	73	CNV_WT_CLK_DP	36	CNV_BRI_DT	74	+V3P3_WIFI
37	PCIE16_TX_C_DN	75	GND	38	CLINK_RST_N		



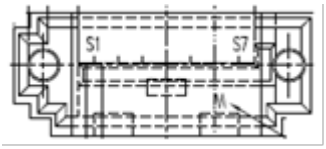
17. PWR1 ~ PWR2: SATA Power Wafer

Pin No.	Description
1	+V12S
2	GND
3	GND
4	+V5S



18. SATA1~SATA2: SATA Signal

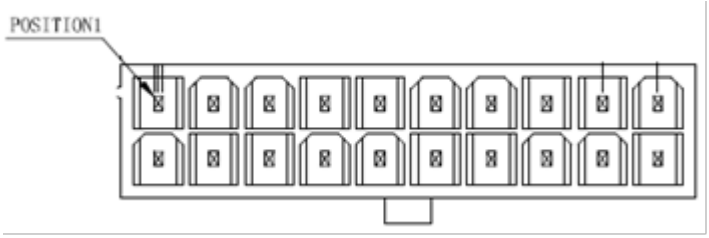
Pin No.	Description	Pin No.	Description
1	GND	5	SATA_RX_DN
2	SATA_TX_DP	6	SATA_RX_DP
3	SATA_TX_DN	7	GND
4	GND		



19. ATX1: ATX Power Connector

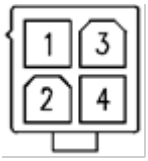
Pin No.	Description	Pin No.	Description	Pin No.	Description	Pin No.	Description
1	+V3P3S	39	GND	2	+V3P3S	40	GND
3	+V3P3S	41	POK	4	NC	42	NC
5	GND	43	+V5DSW	6	GND	44	+V5S
7	+V5S	45	+V12S	8	PSON#	46	+V5S

9	GND	47	+V12S	10	GND	48	+V5S
11	+V5S	49	+V3P3S	12	GND	50	GND



20. ATX2: ATX Power Connector

Pin No.	Description
1	+GND
2	+P12V
3	GND
4	+P12V



CHAPTER 2: HARDWARE SETUP

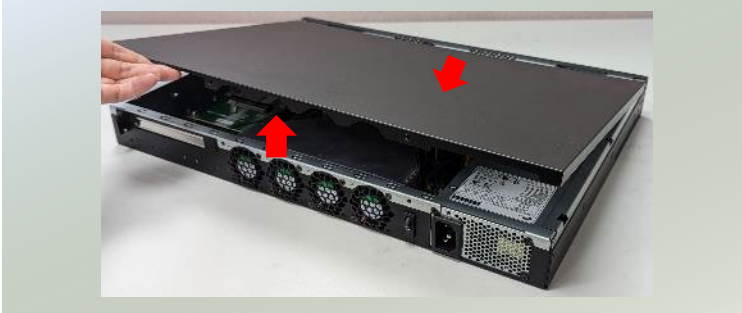
To reduce the risk of personal injury, electric shock, or damage to the system, please remove all power connections to shut down the device completely, and wear ESD protection gloves when handling the installation steps.

Opening the Chassis

1. Power off the system and remove all power connections.

2. Locate and remove the two (2) screws on the chassis cover.

3. Gently slide the chassis cover away from the system and lift the cover to remove.



Installing the System Memory

The motherboard supports two memory slots for DDR5 UDIMM. Please follow the steps below to install the DIMM memory modules.

Supported System Memory Summary

Total Slots	2
Number of Channels	2 (2 DIMMs per channel)
Supported DIMM Capacity	4GB, 8GB, 16GB, 32GB
Memory Size	Maximum 64GB (32GB*2)
Memory Type	DDR5 Non-ECC UDIMM 4800/5600MHz
Minimum DIMM Installed	At least 1 memory modules to boot and run from

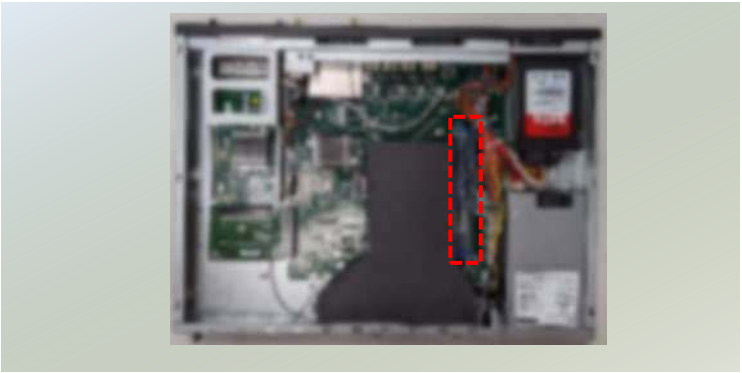
DIMM Population Guidelines

- The CPU requires at least 1 memory module to boot and run from.
- Use memory modules of the same capacity, speed, and from the same manufacturer to avoid compatibility issues and to achieve optimal CPU performance.

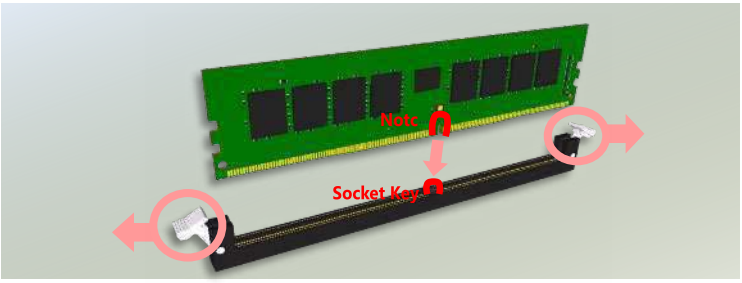
Memory Module Installation Instructions

Please follow the steps below to install the DIMM memory modules.

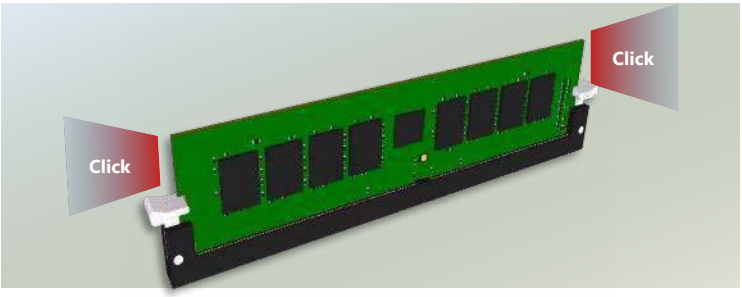
1. Power off the system and open the chassis cover.
2. Locate the DIMM memory slots.



3. Pull open the DIMM slot latches.
4. Align the notch of the module with the socket key in the slot and carefully insert the card into the slot.



5. Push the module down into the slot until it is firmly seated. Press vertically on both corners of the card until it clicks into place.



Installing the TPM Module (Optional)

The system provides one slot for a TPM module card for hardware-based security related functions. Follow the steps below for installation.

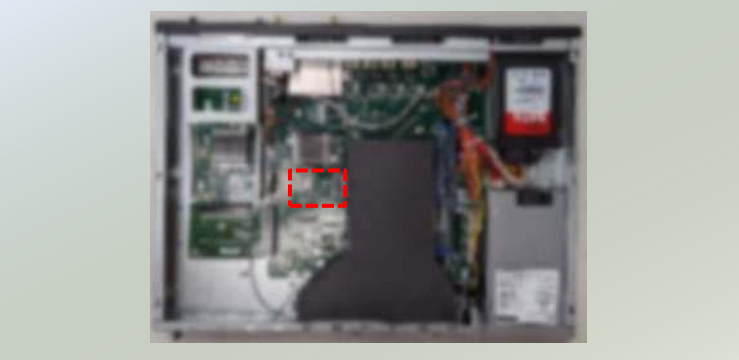
1. Power off the system and open the chassis cover.
2. Locate the TPM connector pins on the motherboard.

3. Insert the module card pins with the connector pins, until the module card is firmly seated.

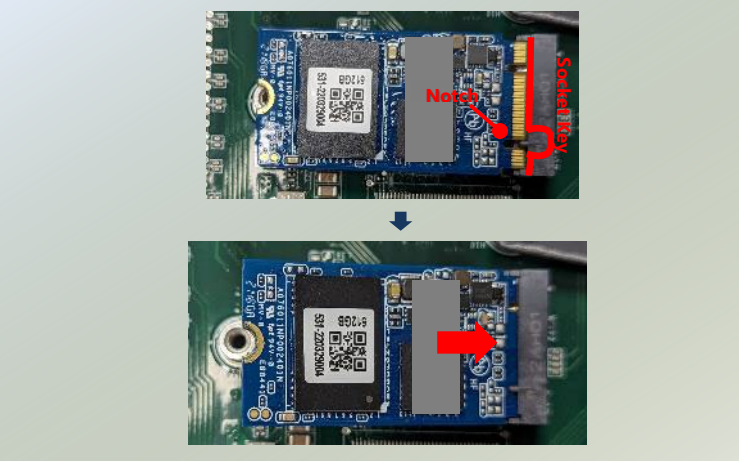
Installing the M.2 Storage (Optional)

The system supports one M.2 slot for additional data storage. Please follow the steps for installation.

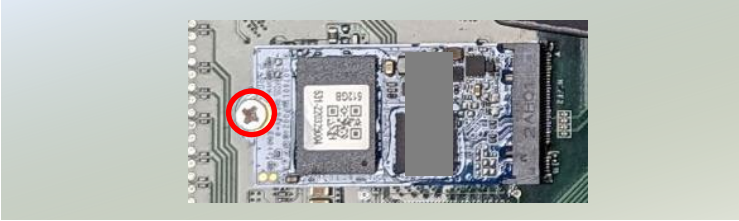
1. Power off the system and open the chassis cover.
2. Locate the M.2 2242 M-Key slot on the motherboard.



3. Align the notch of the storage card with the socket key in the pin slot.
4. Insert the module card pins at 30 degrees into the socket until it is fully seated.



5. Push down on the module card and secure with a screw.

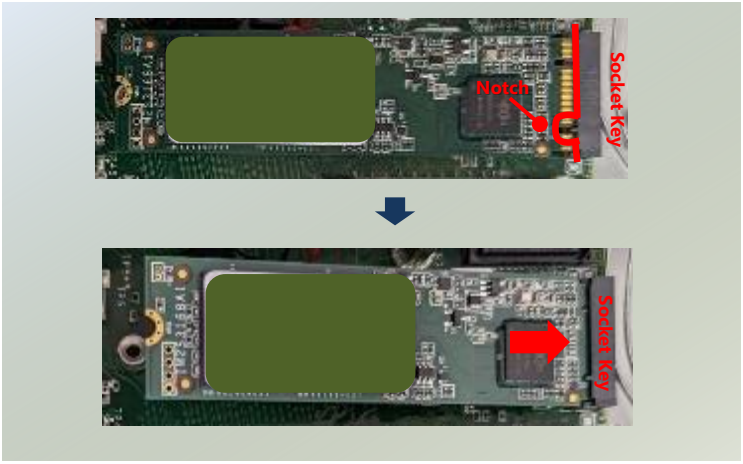


Installing the M.2 NVMe Storage (SKU B Only, Optional)

NCA-4240 SKU B also supports an additional M.2 2280 M-Key slot for NVMe storage. Please follow the steps for installation.

1. Power off the system and open the chassis cover.
2. Locate the M.2 2280 M-Key slot on the motherboard.

3. Align the notch of the storage card with the socket key in the pin slot.
4. Insert the module card pins at 30 degrees into the socket until it is fully seated.



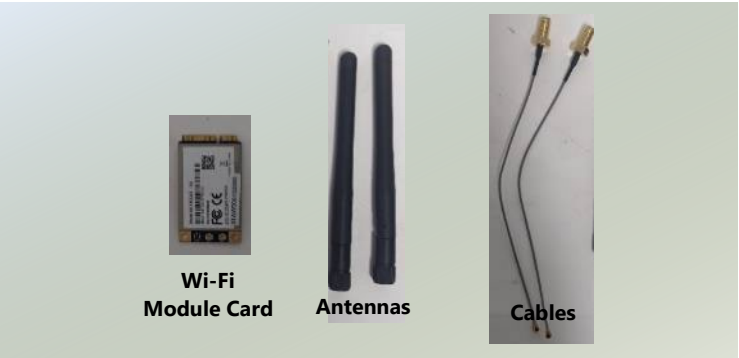
5. Push down on the module card and secure with one (1) screw.

Installing the Wi-Fi Module Card (SKU B Only, Optional)

NCA-4240 SKU B supports one M.2 2230 E-Key for a Wi-Fi or BT module card. Wi-Fi module requires two antennas. Please follow the steps to install the Wi-Fi module card.

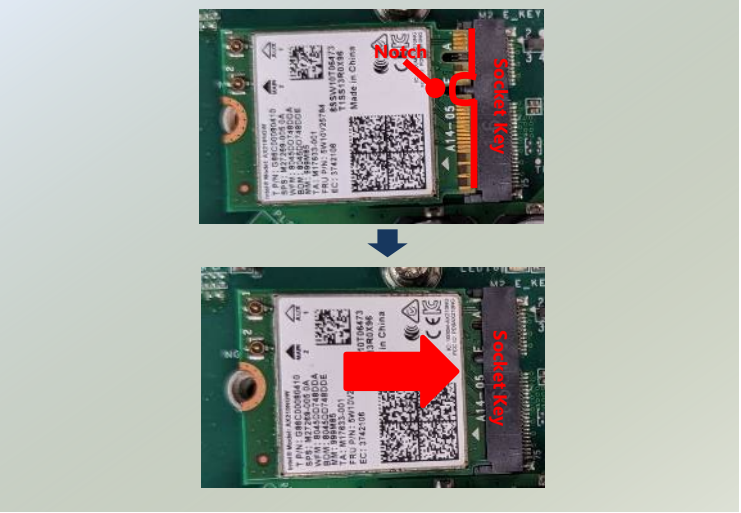
The Wi-Fi Module Card kit contains the following items:

- 1x Wi-Fi Module Card
- 2x SMA to IPEX cable
- 2x Antennas



1. Power off the system and open the chassis cover.
2. Locate the M.2 2230 E-Key slot on the motherboard.

3. Align the notch of the Wi-Fi module with the socket key in the pin slot.
4. Insert the Wi-Fi module card pins at 30 degrees into the socket until it is fully seated.

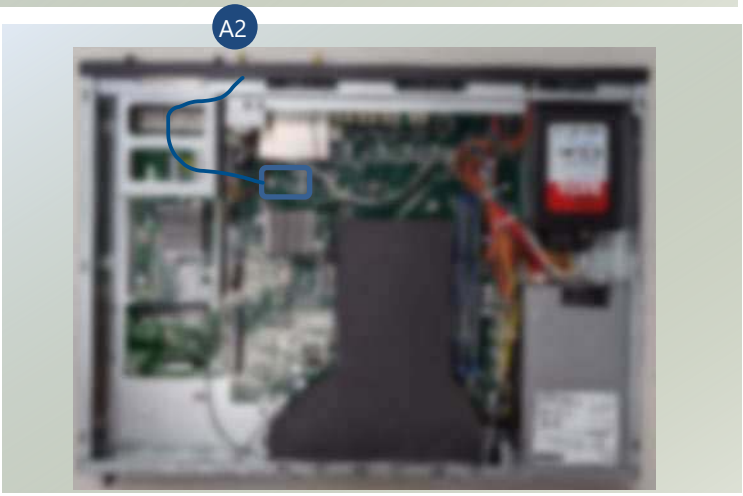


5. Push down on the module card and secure with a screw.

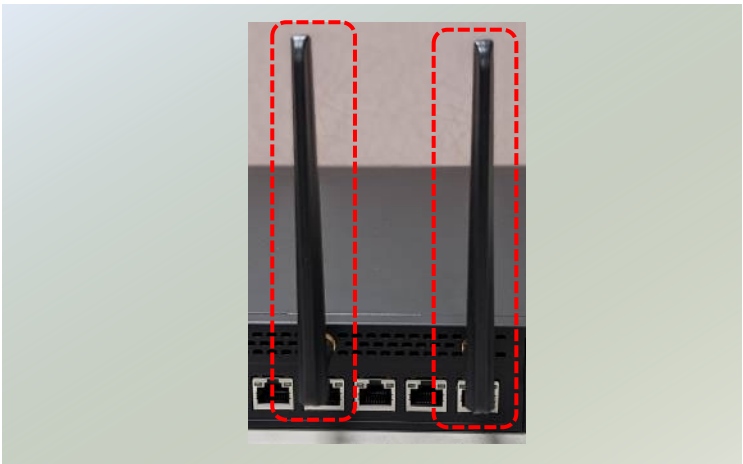
Installing Wi-Fi Antennas

1. Locate the two (2) antenna hole placements (A1, A2). Locate the two (2) IPEX connectors on the Wi-Fi module card.

2. Connect the RF cables to the IPEX connectors on the Wi-Fi module card and screw the other end of the cables in the antenna holes.



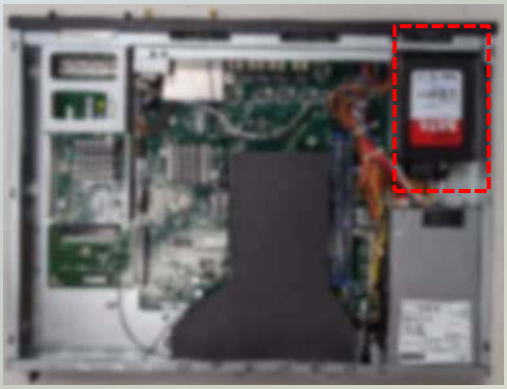
3. Then, screw on the antennas on the outside of the system.



Installing the Disk Drives (Optional)

The HDD/SSD bay supports two 2.5" SATA HDDs or SSD for additional data storage. Follow the steps for installation.

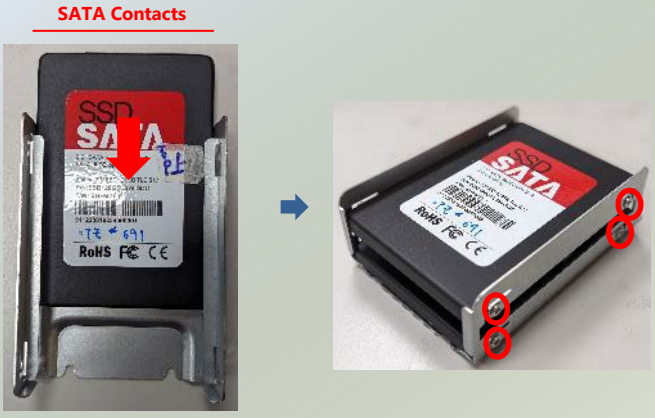
1. Power off the system and open the chassis cover.
2. Locate the 2.5" disk tray inside the system.



3. Loosen the one (1) screw that secures the tray. Remove the screw, take the tray out and prepare to install the disk drives.

NOTE: Make sure to watch out for the notches (circled in blue) on the sides of the tray, especially when placing the tray back in the system.

4. Mount the disk drives in the tray, make sure the SATA Contacts (SATA data cables and power cable connectors) are facing outwards. Apply two (2) screws on each side of the disk drive.



NOTE: When installing two disk drives, begin with the one in the lower (bottom) slot.

5. Attach the SATA data cable and power cable to the HDD/SSD disk.

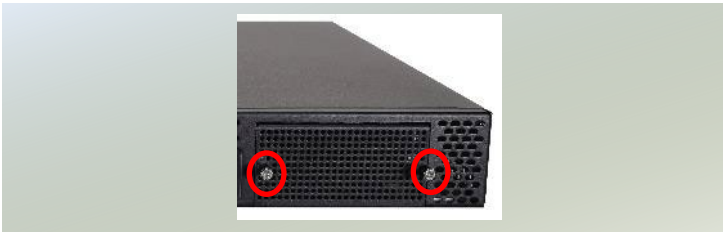
6. Place the tray (with the disk drives now installed) back to its original place inside the system. Secure with the original one (1) screw.

Installing the NIC Modules

The system comes with one NIC module slot for expansion. Follow the steps for installation.

1. Locate the NIC module slot on the front panel of the system.

2. Rotate clockwise and loosen the two lock-screws, and remove the NIC module slot door.



3. Insert your NIC module. (The module shown here is for reference only.)

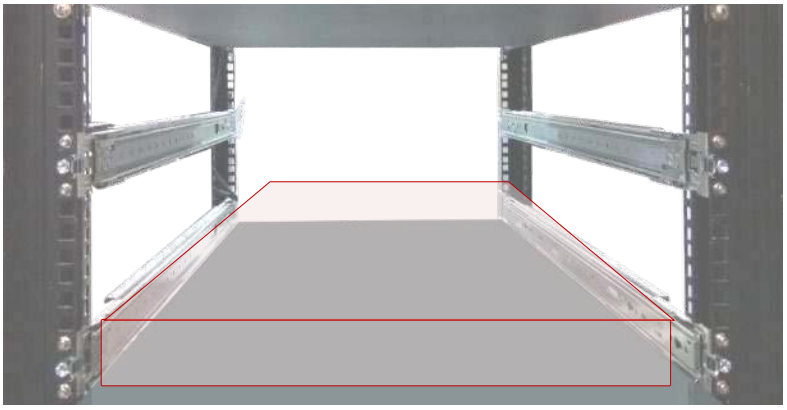
4. Once the module is firmly seated, rotate counter-clockwise and tighten the two lock-screws.

Mounting the System

This system offers multiple mounting options to suit your application and environment. It includes two types of mounting kits: one for standard rack or enclosure installations and another for integrating this system into a rack.

- **Ear Brackets**

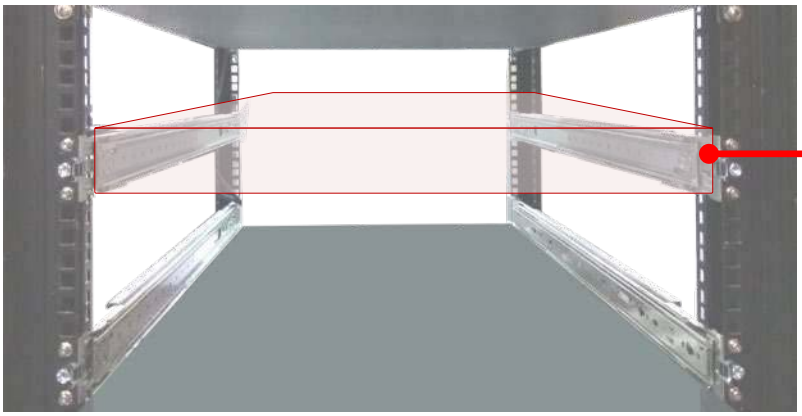
This quick and straightforward method involves attaching the system to the rack's front posts. To prevent the chassis from tipping over, it's crucial to pair this method with a shelf or slide rails for added stability.



Note: The system should be installed on the rack using a shelf or slide rails, as the "Mounting Ears" are designed for securing the system, not supporting it.

- **Slide Rail Kit + Short Ear Brackets**

The sliding rack-mount rails provide easy access to the system while ensuring it is securely fastened to the rack.



The Slide Rail Kit ensures the system is securely held in place while providing adequate weight support for the device.

CHAPTER 3: SOFTWARE SETUP

BIOS Setup

BIOS is a firmware embedded on an exclusive chip on the system's motherboard. Lanner's BIOS firmware offering including market-proven technologies such as Secure Boot and Intel Boot Guard technology deliver solid commitments for the shield protection against malware, uncertified sequences and other named cyber threats.

Main Setup

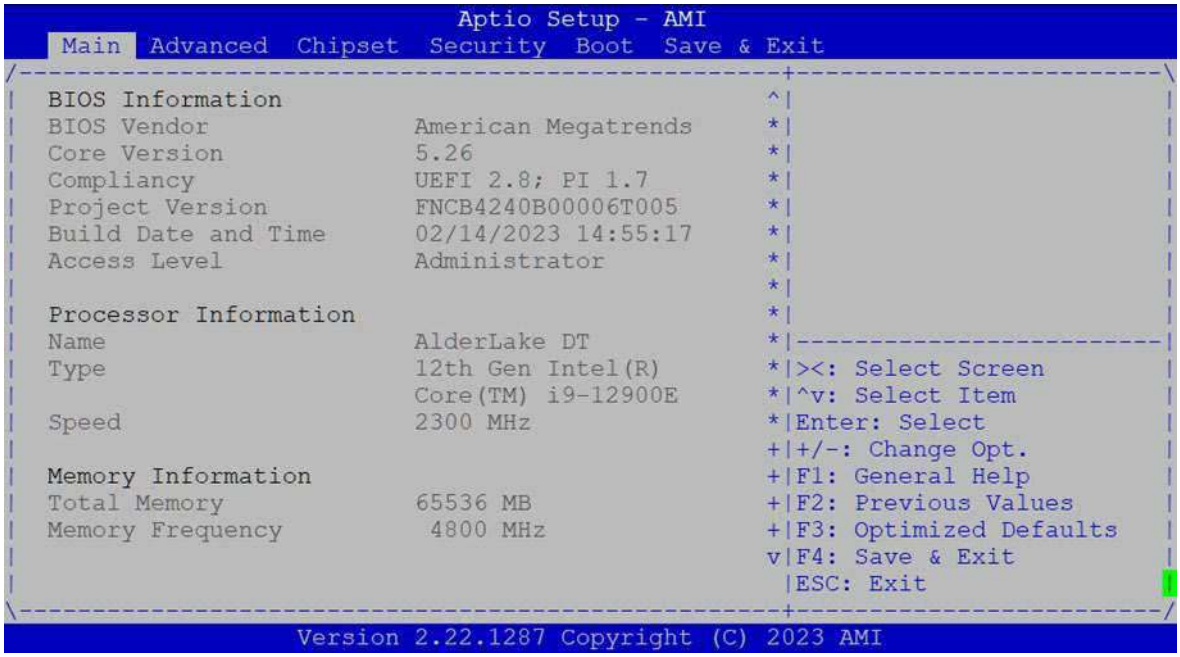
To enter the BIOS setup utility, simply follow the steps below:

1. Boot up the system.
2. Pressing the **<Tab>** or **<Del>** key immediately allows you to enter the Setup utility, and then you will be directed to the BIOS main screen. The instructions for BIOS navigations are as below:

Control Keys	Description
→←	select a setup screen
↑↓	select an item/option on a setup screen
<Enter>	select an item/option or enter a sub-menu
+/-	adjust values for the selected setup item/option
F1	display General Help screen
F2	retrieve previous values, such as the last configured parameters during the last time you entered BIOS
F3	load optimized default values
F4	save configurations and exit BIOS
<Esc>	exit the current screen

Main Page

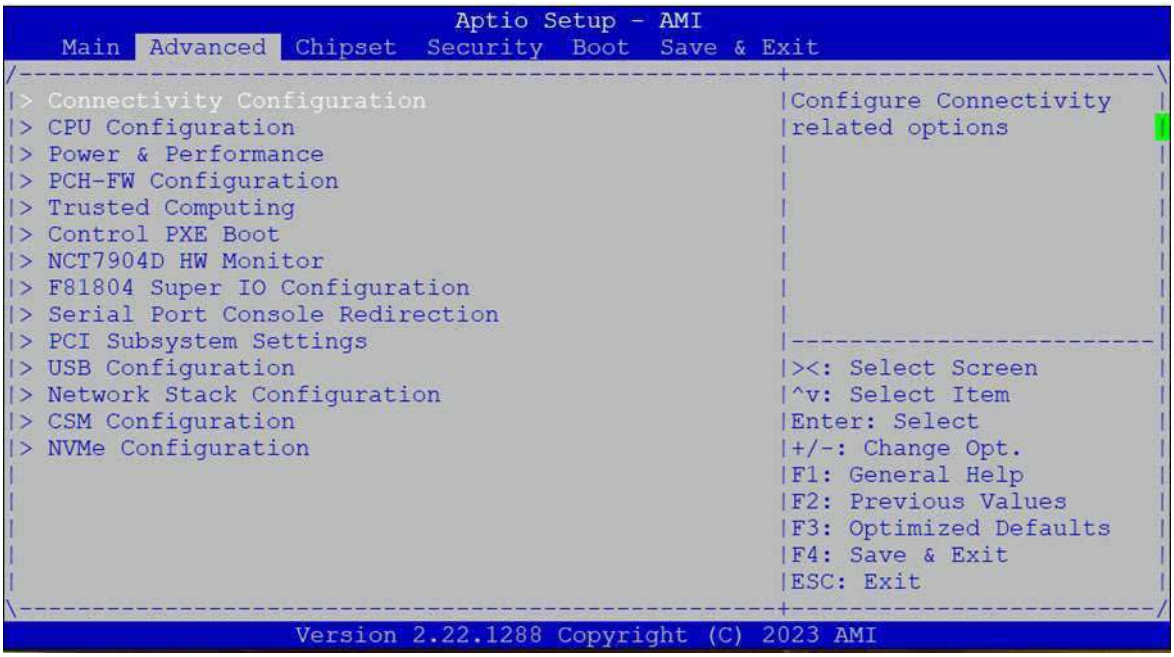
Setup main page contains BIOS information and project version information.



Feature	Description
BIOS Information	BIOS Vendor: American Megatrends Core Version: AMI Kernel version, CRB code base, X64 Compliancy: UEFI version, PI version Project Version: BIOS release version Build Date and Time: MM/DD/YYYY Access Level: Administrator / User
Processor Information	Information of platform processor
Memory Information	Information of memory
PCH Information	Information of platform pch
System Date	To set the Date, use **<Tab>** to switch between Date elements. Default Range of Year: 1998-9999 Default Range of Month: 1-12 Days: dependent on Month.
System Time	To set the Date, use **<Tab>** to switch between Date elements.

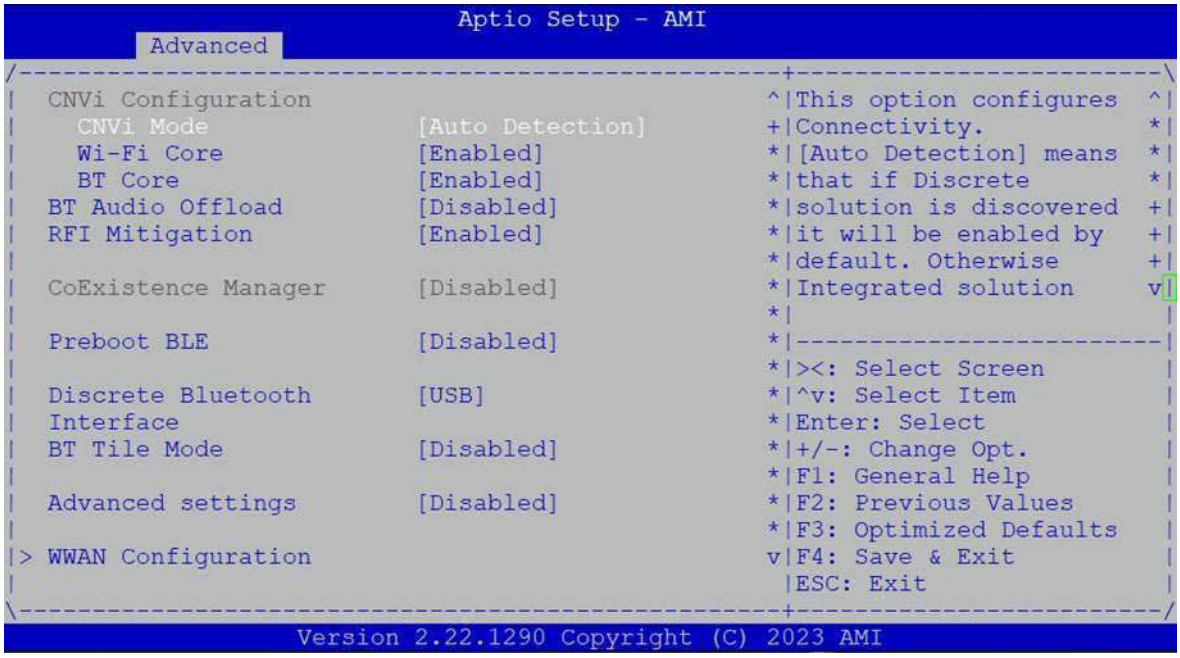
Advanced Page

Select the **Advanced** menu item from the BIOS setup screen to enter the **Advanced** setup screen. Users can select any of the items in the left frame of the screen.



Feature	Options	Description
Restore AC Power Loss	Power On Power Off Last State	Specify what state to go to when power is reapplied after a power failure (G3 state).

Connectivity Configuration



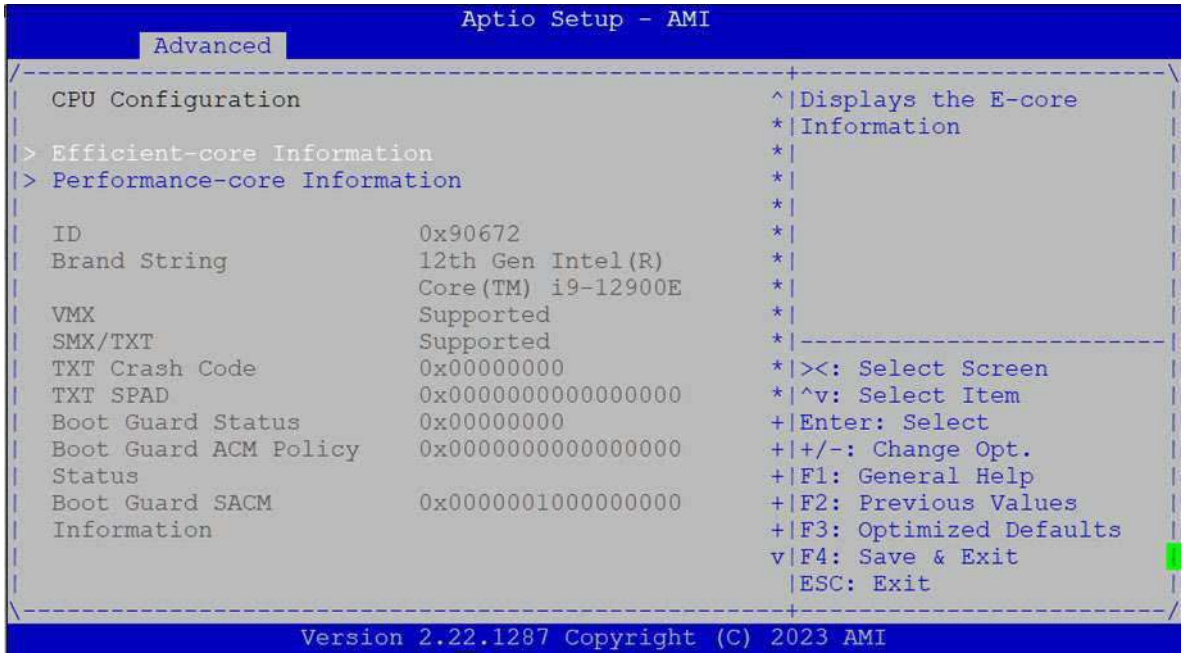
Feature	Options	Description
CNVi Mode	Disable Integrated Auto Detection	This option configures Connectivity. **[Auto Detection]** means that if Discrete solution is discovered it will be enabled by default. Otherwise Integrated solution (CNVi) will be enabled; **[Disable Integrated]** disables Integrated Solution. **NOTE**: When CNVi is present, the GPIO pins that are used for radio interface cannot be assigned to the other native function.
Wi-Fi Core	Enabled Disabled	This is an option intended to Enable/Disable Wi-Fi Core in CNVi
BT Core	Enabled Disabled	This is an option intended to Enable/Disable BT Core in CNVi
BT Audio Offload	Disabled Enabled	This is an option to Enable/Disable BT Audio Offload which enables audio input from BT device to the audio DSP and enables power efficient audio output to BT device.
RFI Mitigation	Enabled Disabled	This is an option intended to Enable/Disable DDR-RFIM feature for Connectivity This RFI mitigation feature may result in temporary slowdown of the DDR speed.
Preboot BLE	Disabled Enabled	This will be used to enable Preboot Bluetooth function
Discrete Bluetooth Interface	Disabled USB	Serial IO UART0 needs to be enabled to select BT interface
BT Tile Mode	Disabled Enabled	Enable/Disable Tile

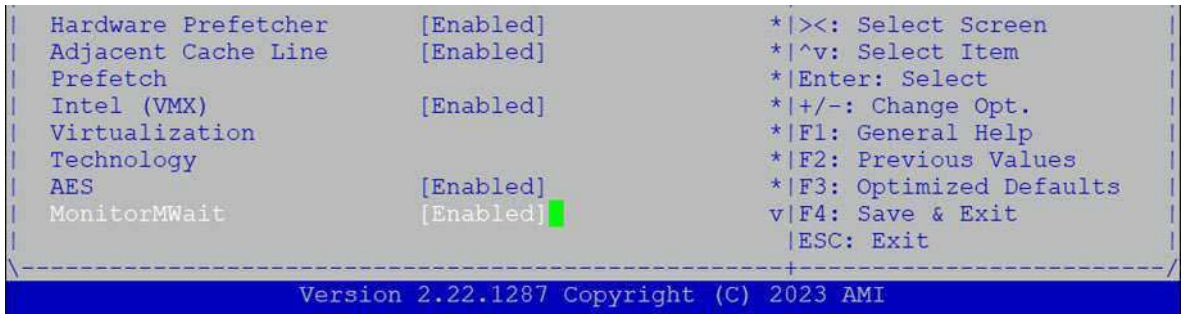
Advanced Setting	Disabled Enabled	Configure ACPI objects for wireless devices

WWAN Configuration

Feature	Options	Description
WWAN Device	Disabled 4G-730/7560 5G-M80	Select the M.2 WWAN Device options to enable 4G - 7360/7560 (Intel), 5G - M80 (MediaTek) Modems

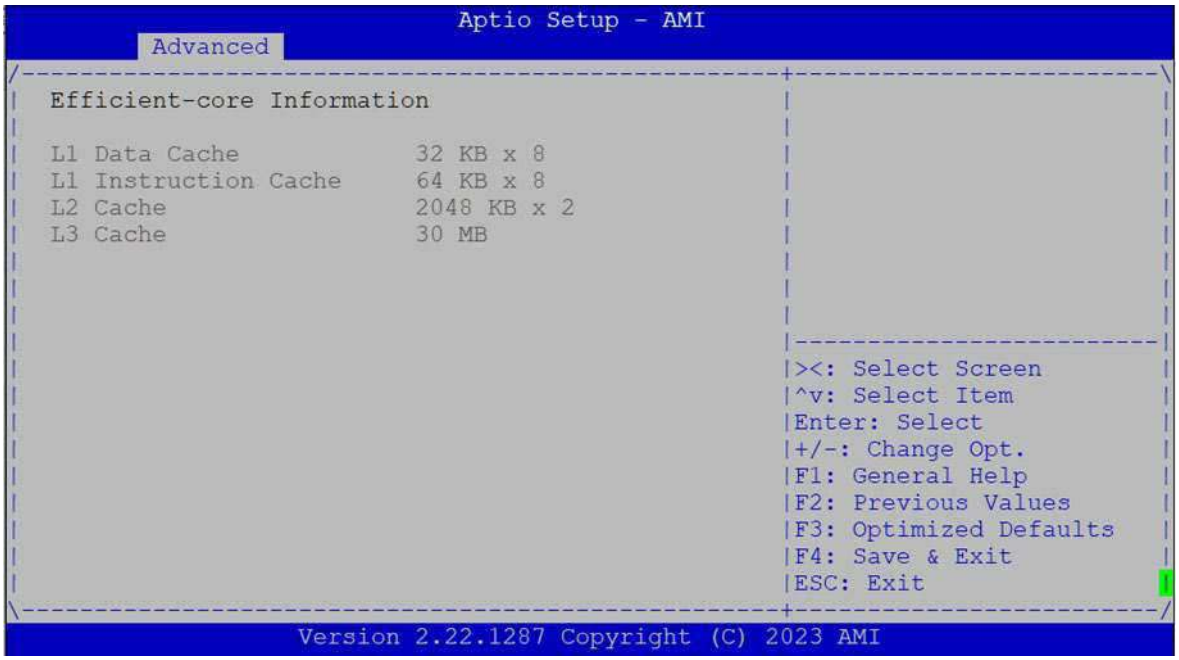
CPU Configuration



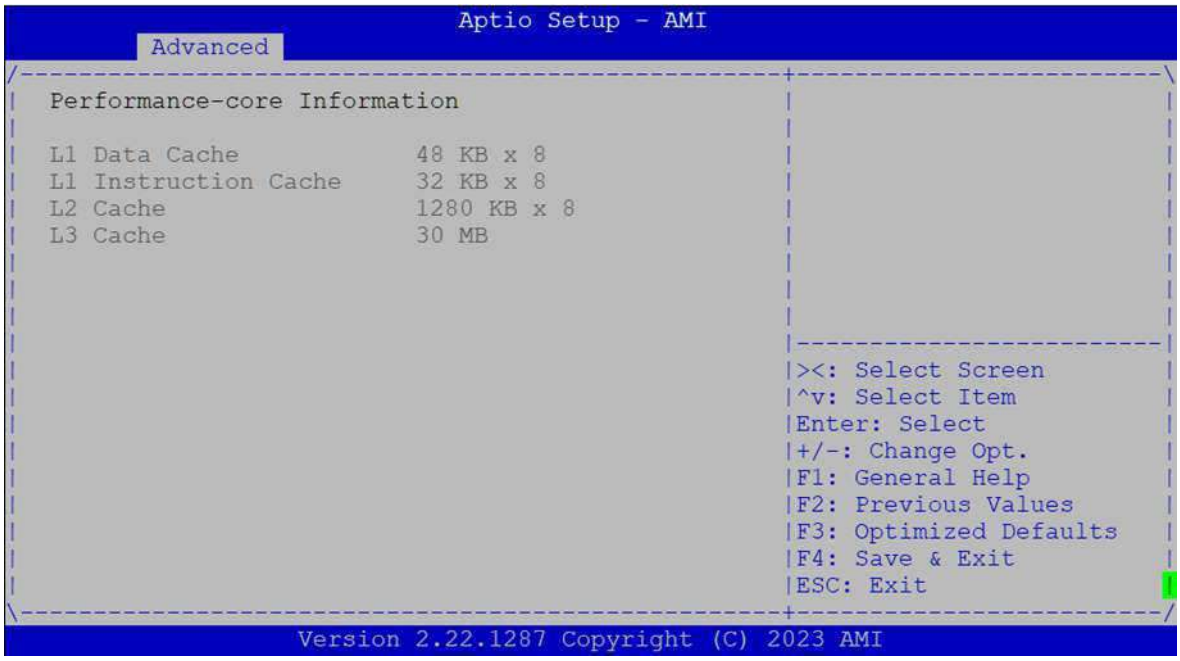


Feature	Options	Description
Hardware Prefetcher	Disabled Enabled	To turn on/off the MLC streamer prefetcher.
Adjacent Cache Line Prefetch	Disabled Enabled	To turn on/off prefetching of adjacent cache lines.
Intel (VMX) Virtualization Technology	Disabled Enabled	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
AES	Disabled Enabled	Enable/Disable AES (Advanced Encryption Standard)
MonitorMWait	Disabled Enabled	Enable/Disable MonitorMWait, if Disable MonitorMwait, the AP threads Idle Manner should not set in MWAIT Loop

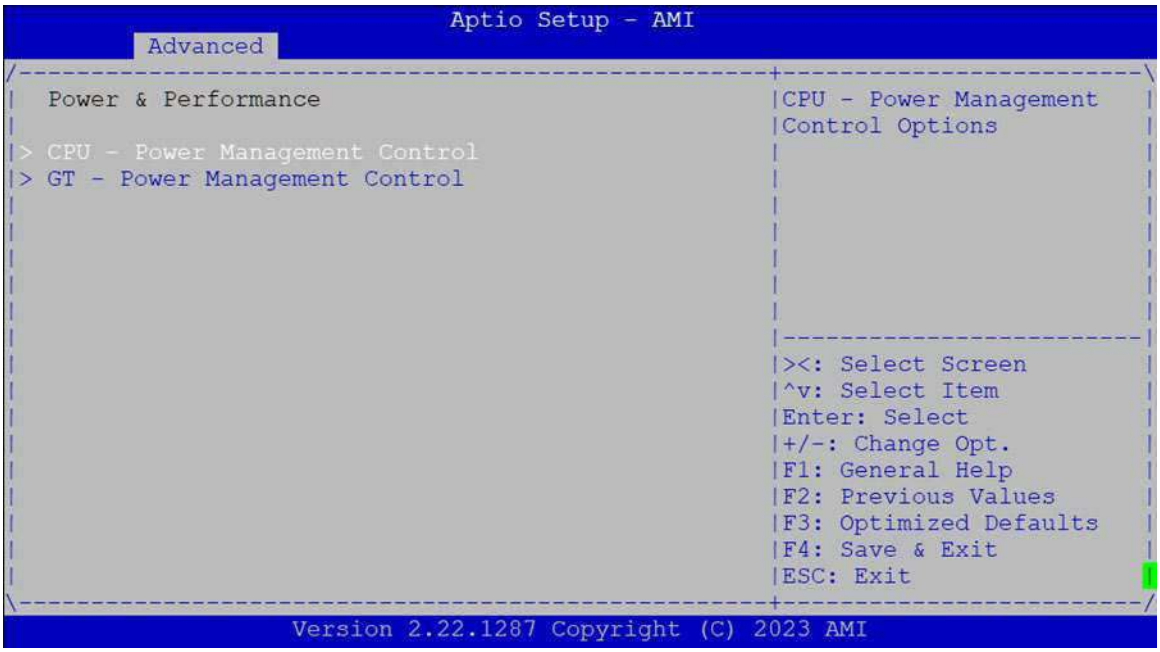
Efficient-Core Information



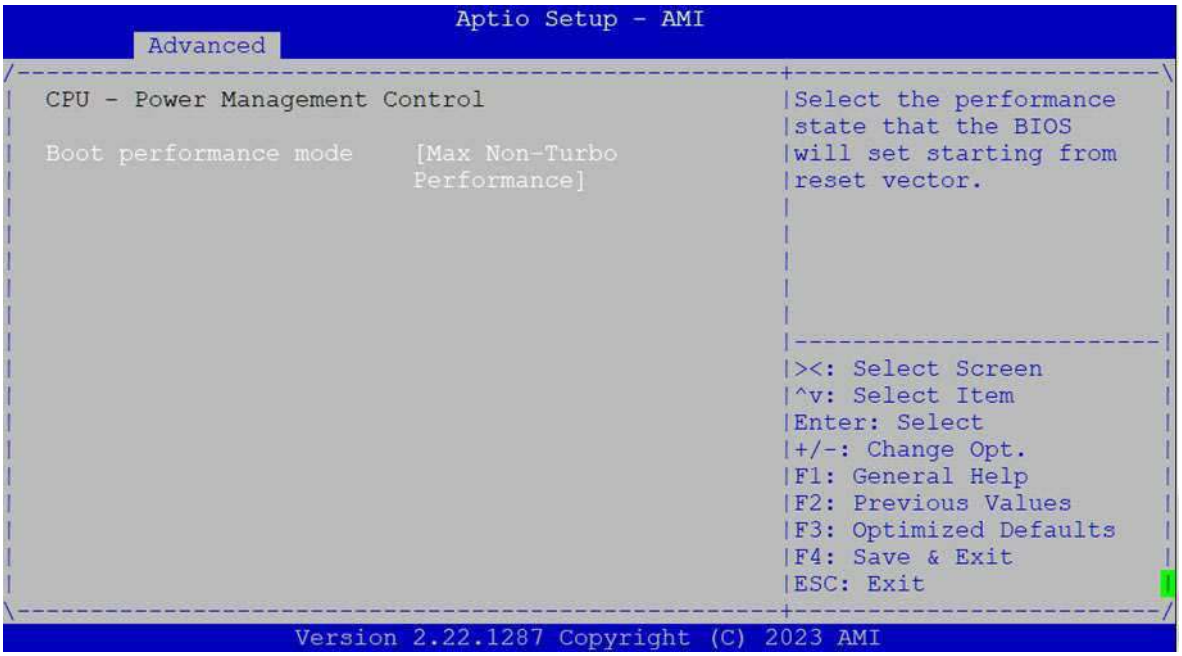
Performance-Core Information



Power & Performance

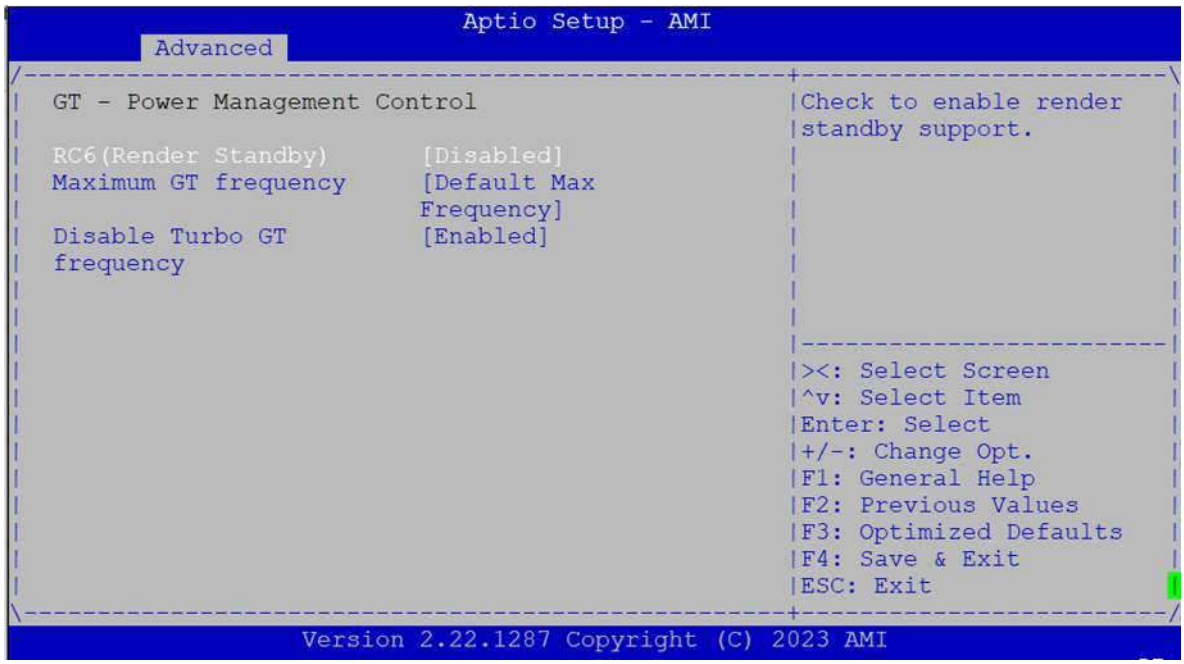


CPU – Power Management Control



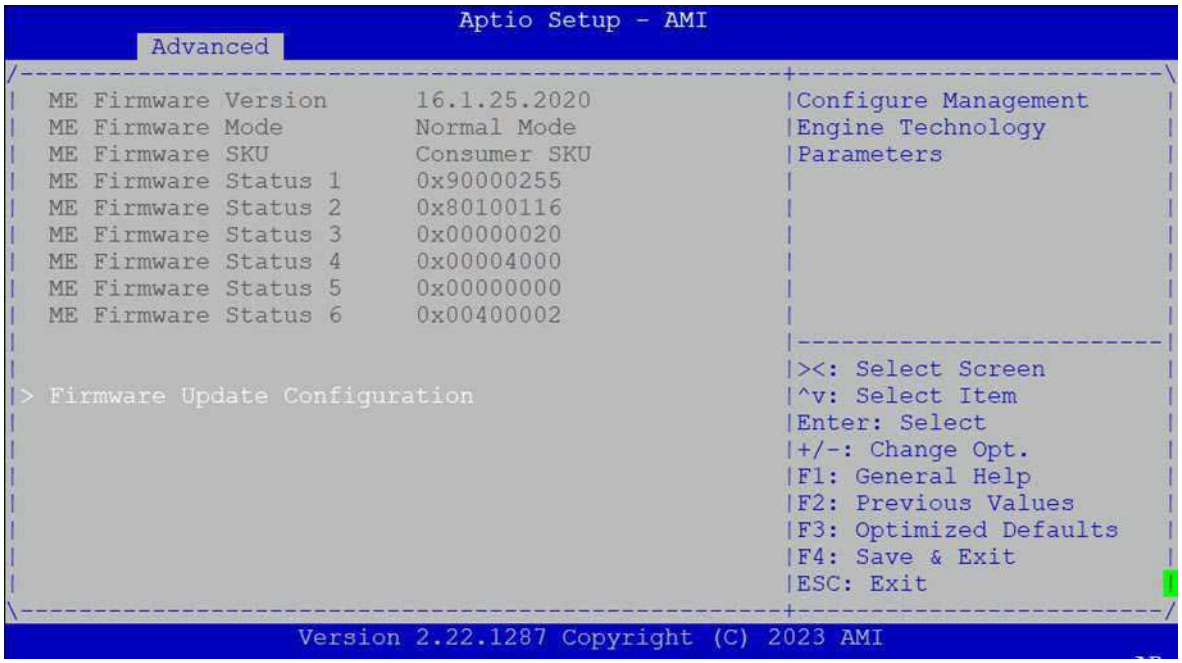
Feature	Options	Description
Boot Performance Mode	Max Battery Max Non-Turbo Performance Turbo Performance	Select the performance state that the BIOS will set starting from reset vector.

GT – Power Management Control

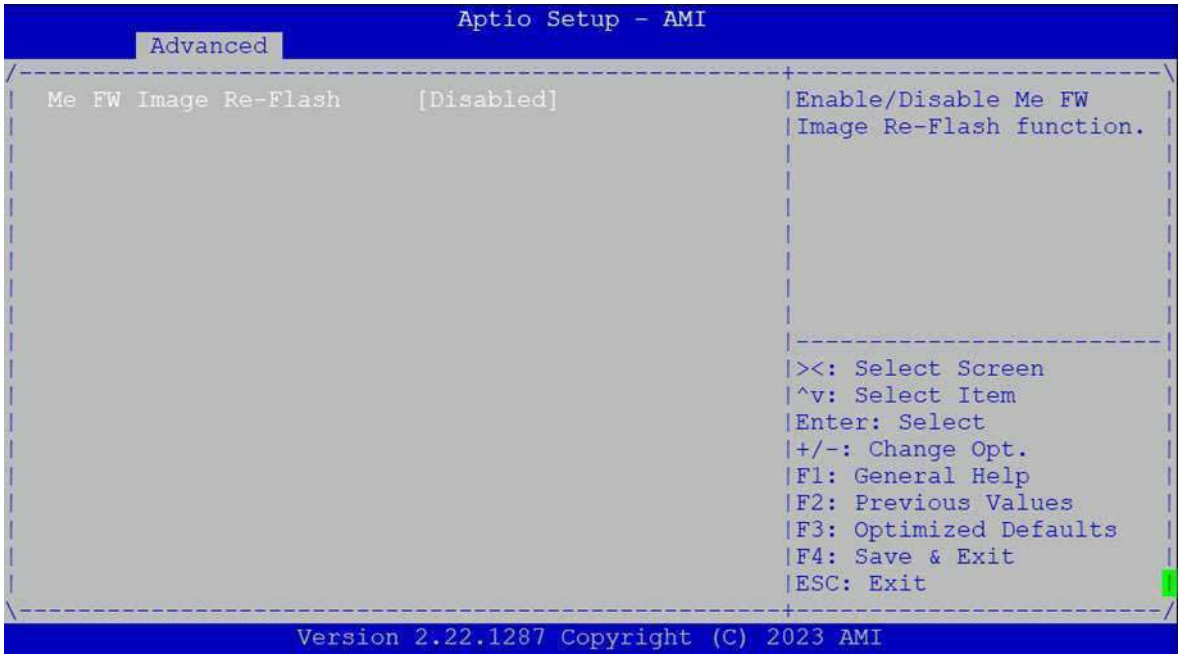


Feature	Options	Description
RC6 (Render Standby)	Disabled Enabled	Check to enable render standby support.
Maximum GT Frequency	Default Max Frequency	Maximum GT frequency limited by the user. Choose between 300MHz (RPN) and 1550MHz (RP0). Value beyond the range will be clipped to min/max supported by SKU
Disable Turbo GT Frequency	Enabled Disabled	Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited

PCH-FW Configuration

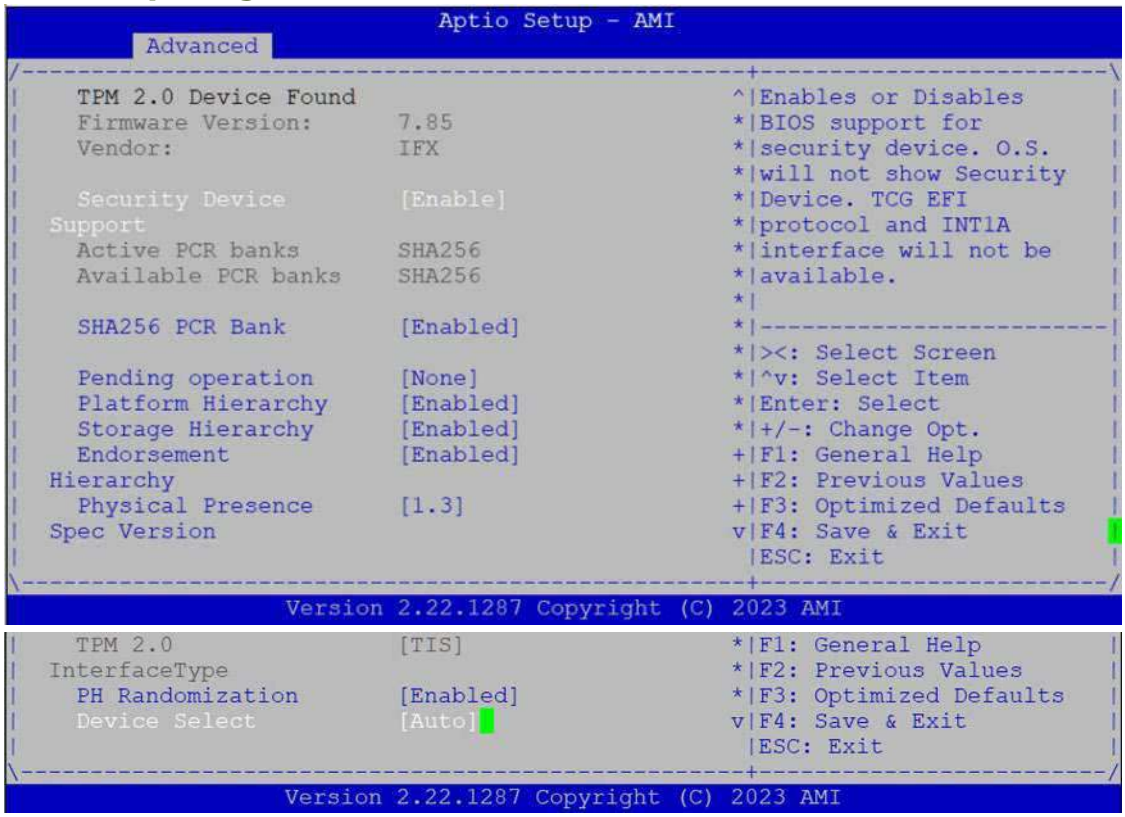


Firmware Update Configuration



Feature	Options	Description
Me FW Image Re-Flash	Disabled Enabled	Enable/Disable Me FW Image Re-Flash function.

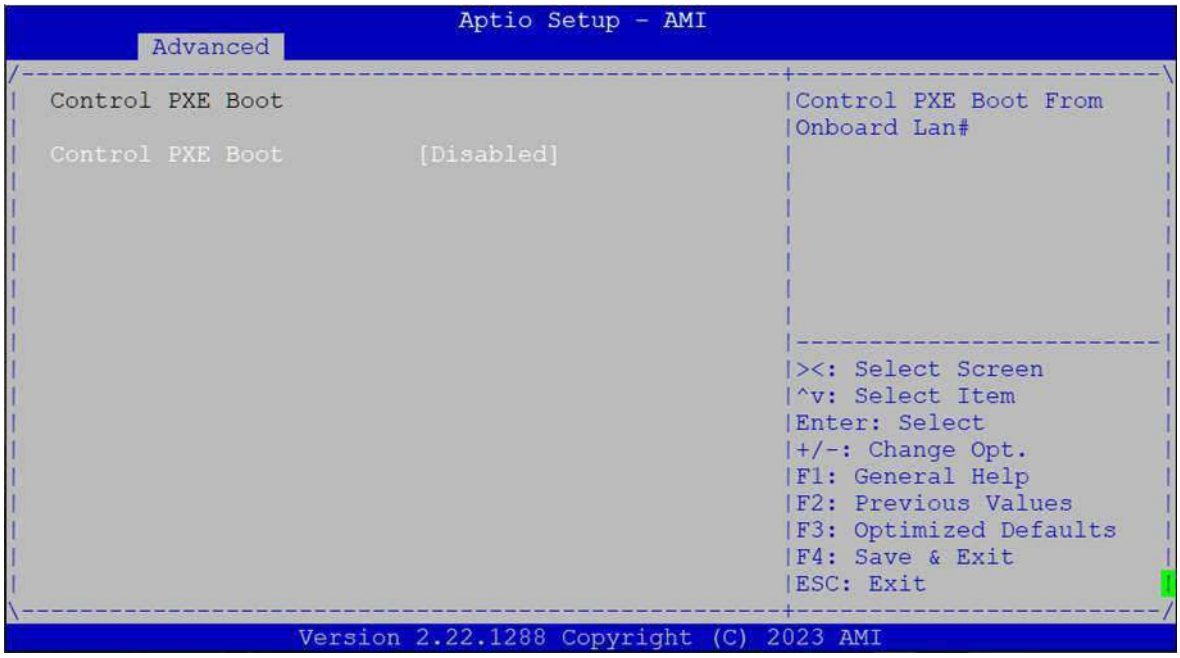
Trusted Computing



Feature	Options	Description
Security Device Support	Disable Enable	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
SHA256 PCR Bank	Disable Enable	Enable or Disable SHA256 PCR Bank
Pending Operation	None TPM Clear	Schedule an Operation for the Security Device. **NOTE:** Your Computer will reboot during restart to change State of Security Device.
Platform Hierarchy	Disabled Enabled	Enable or Disable Platform Hierarchy
Storage Hierarchy	Disabled Enabled	Enable or Disable Storage Hierarchy
Endorsement Hierarchy	Disabled Enabled	Enable or Disable Endorsement Hierarchy
Physical Presence Spec Version	1.2 1.3	Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. **NOTE:** some HCK tests might not support 1.3.
PH Randomization	Disabled Enabled	Enables or Disables Platform Hierarchy randomization. DO NOT ENABLE THIS QUESTION IN PRODUCTION PLATFORMS. THIS IS FOR DEVELOPMENT TESTING. OVERRIDE ChangePlatformAuth ELINK for production platforms supporting TXT.

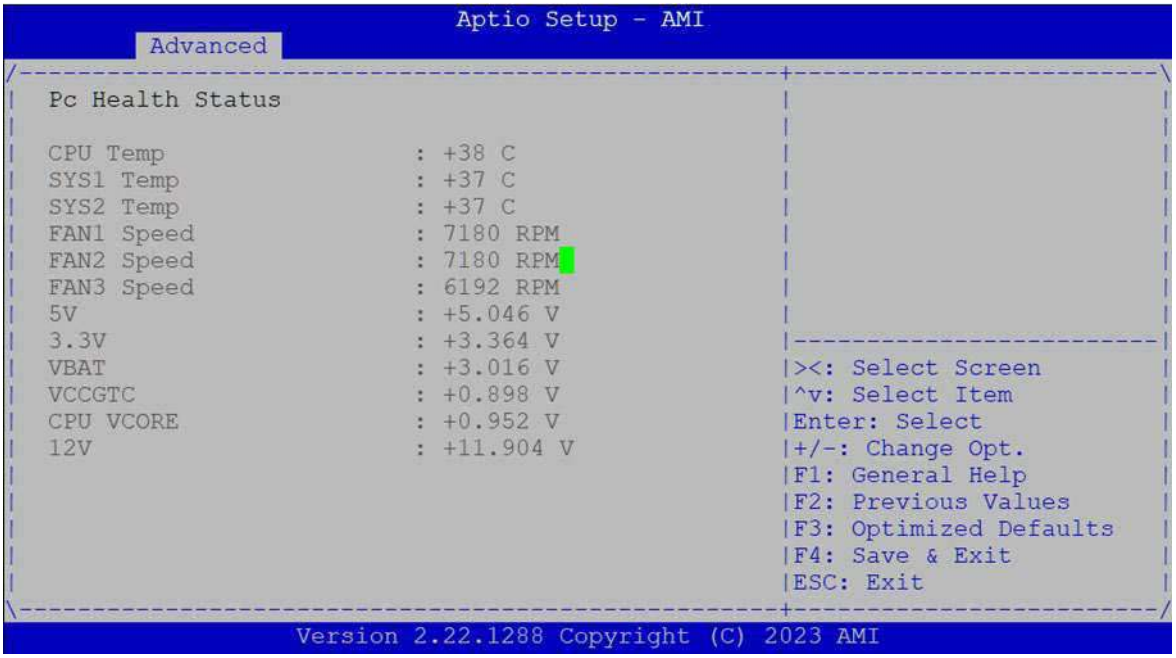
Device Select	TPM 1.2 TPM 2.0 Auto	**TPM 1.2** will restrict support to TPM 1.2 devices, **TPM 2.0** will restrict support to TPM 2.0 devices, **Auto** will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated

Control PXE Boot



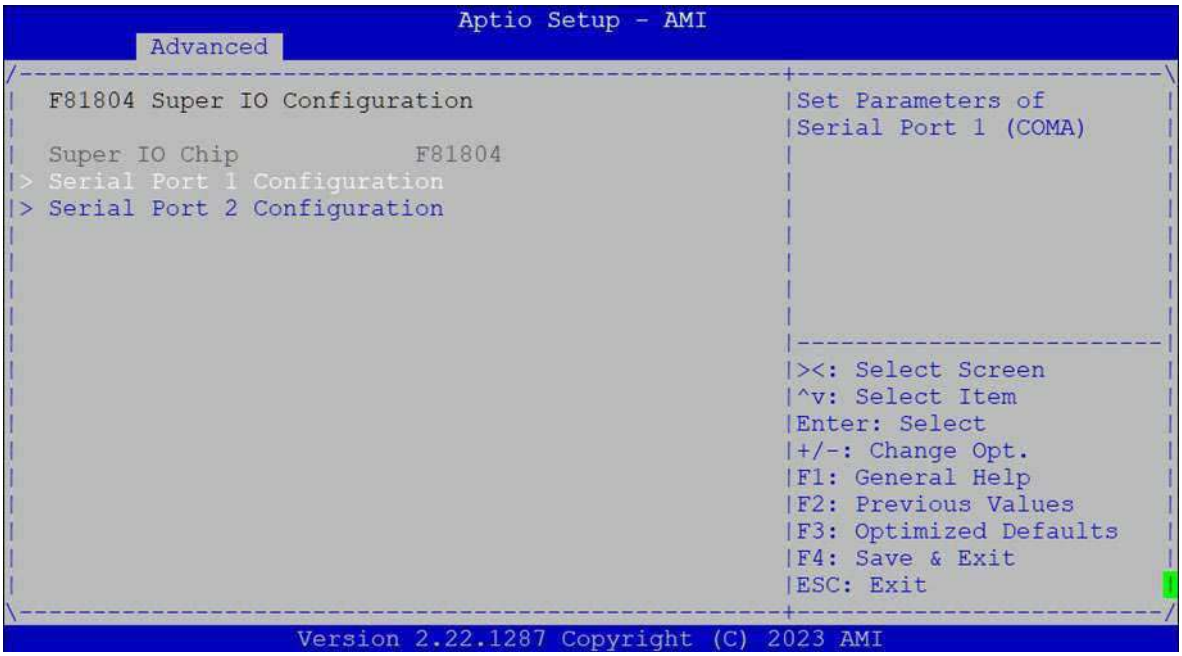
Feature	Options	Description
Control PXE Boot	Disabled Lan0	Control PXE Boot from onboard Lan#.

NCT7904D HW Monitor

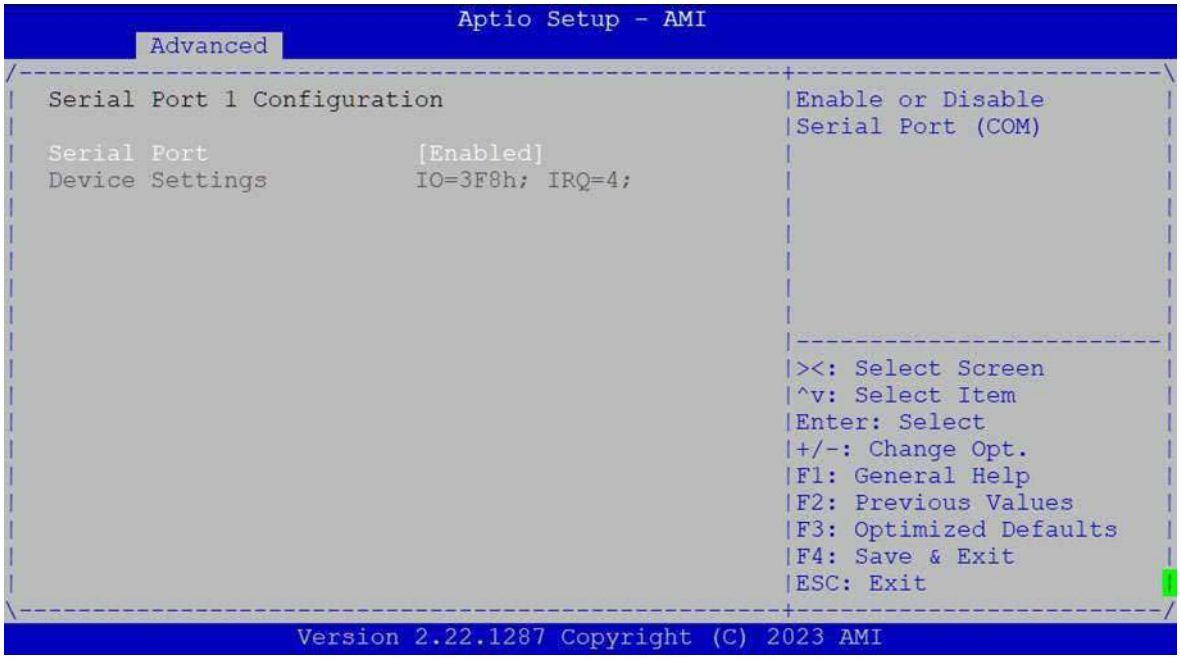


Feature	Description
CPU Temp	This value reports the CPU temperature
SYS1 Temp	This value reports the System temperature
SYS2 Temp	This value reports the System temperature (Close CPU)
FAN1 Speed	This value reports the Fan1 speed
FAN2 Speed	This value reports the Fan2 speed
FAN3 Speed	This value reports the Fan3 speed
5V	This value reports the 5V Input voltage
3.3V	This value reports the 3.3V Input voltage
VBAT	This value reports the VBAT Input Voltage
VCCGTC	This value reports the VCCGT Input voltage
CPU VCORE	This value reports the CPU VCORE Input voltage
12V	This value reports the 12V Input voltage

F81804 Super IO Configuration

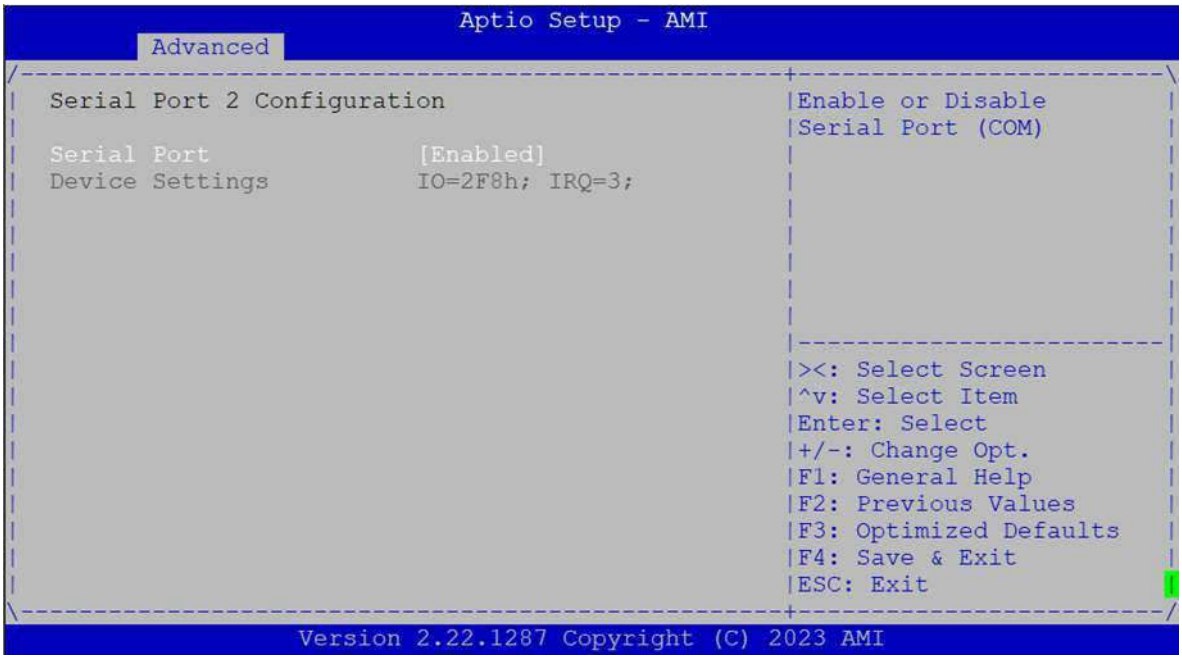


Serial Port 1 Configuration



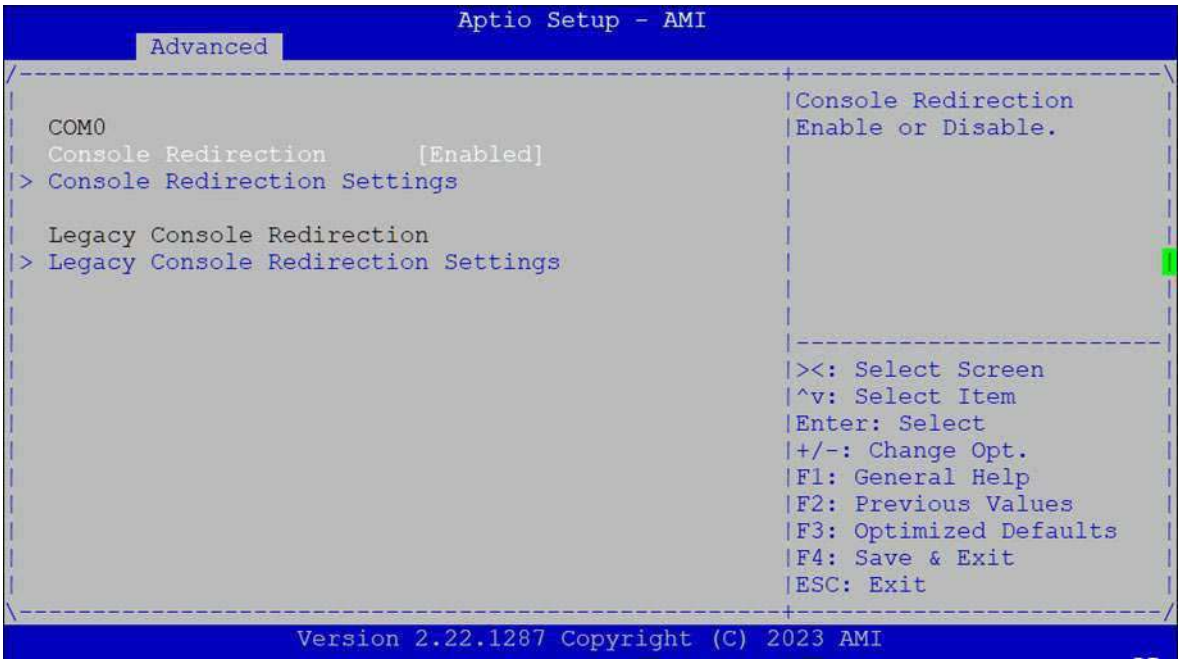
Feature	Options	Description
Serial Port	Disabled Enabled	Enable or Disable Serial Port (COM)
Device Settings	N/A	IO=3F8h; IRQ=4;

Serial Port 2 Configuration



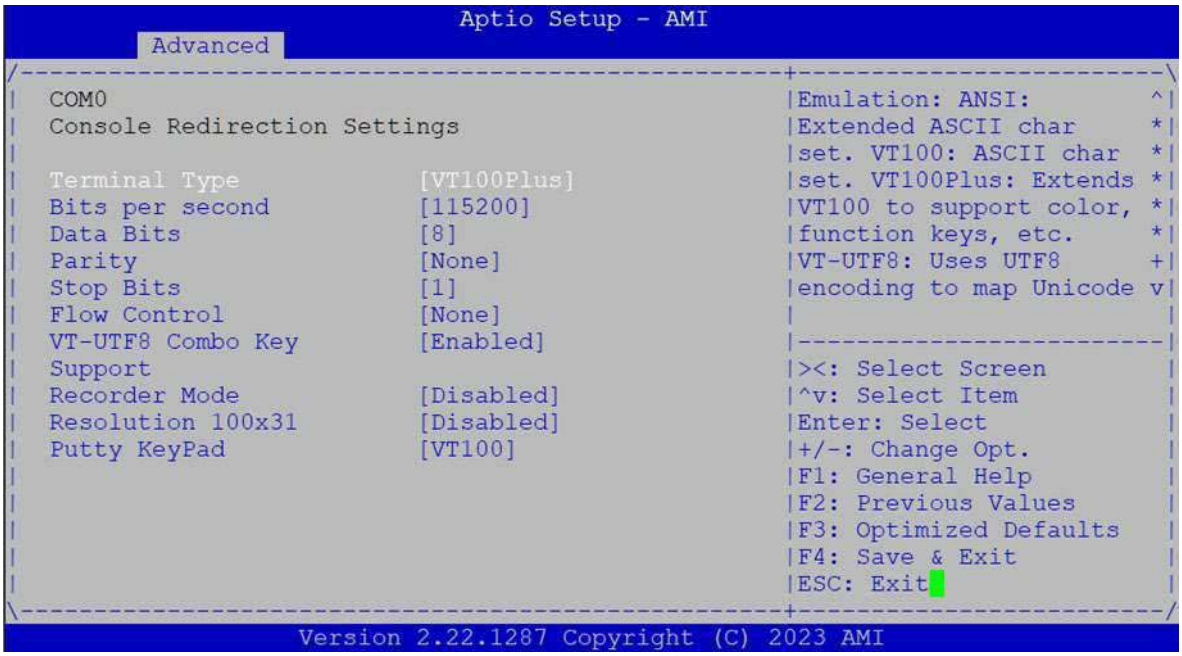
Feature	Options	Description
Serial Port	Disabled Enabled	Enable or Disable Serial Port (COM)
Device Settings	N/A	IO=2F8h; IRQ=3;

Serial Port Console Redirection



Feature	Options	Description
Console Redirection	Disabled Enabled	Console Redirection Enable or Disable.

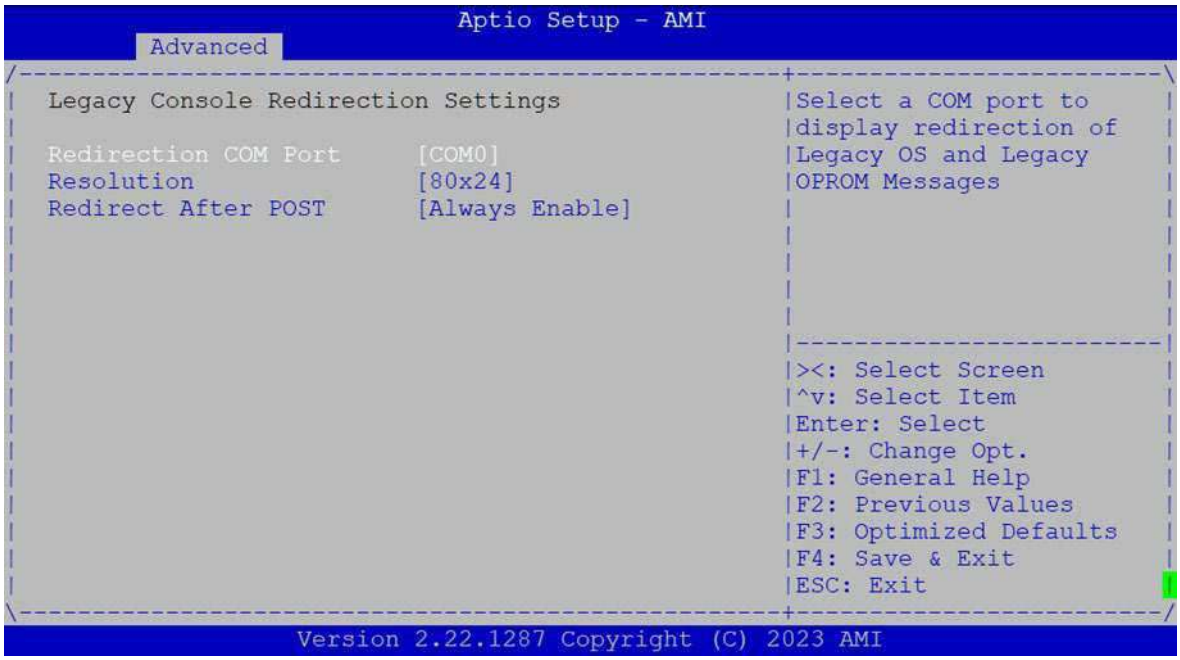
Console Redirection Settings



Feature	Options	Description
Terminal Type	VT100 VT100+ VT-UTF8 ANSI	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 115200	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 8	Data Bits
Parity	None Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors.
Stop Bits	1 2	Stop bits indicate the end of a serial data packet.
Flow Control	None Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow.

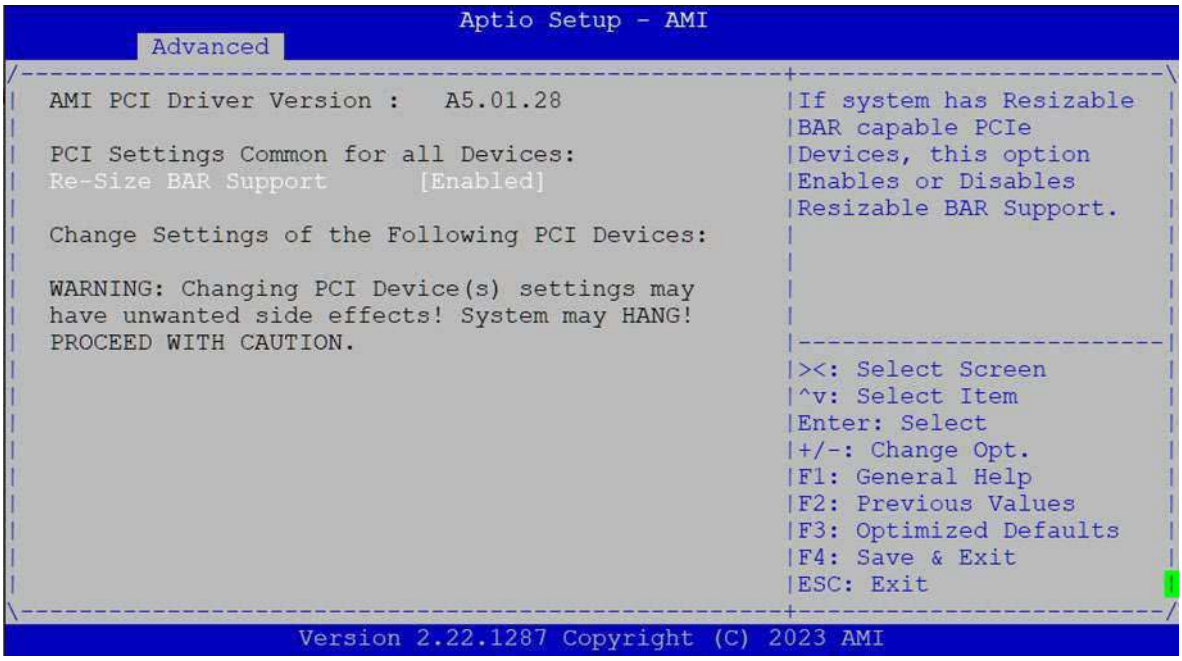
VT-UTF8 Combo Key Support	Disabled Enabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	Disabled Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	Disabled Enabled	Enables or disables extended terminal resolution.
Putty Keypad	VT100 LINUX XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.

Legacy Console Redirection Settings



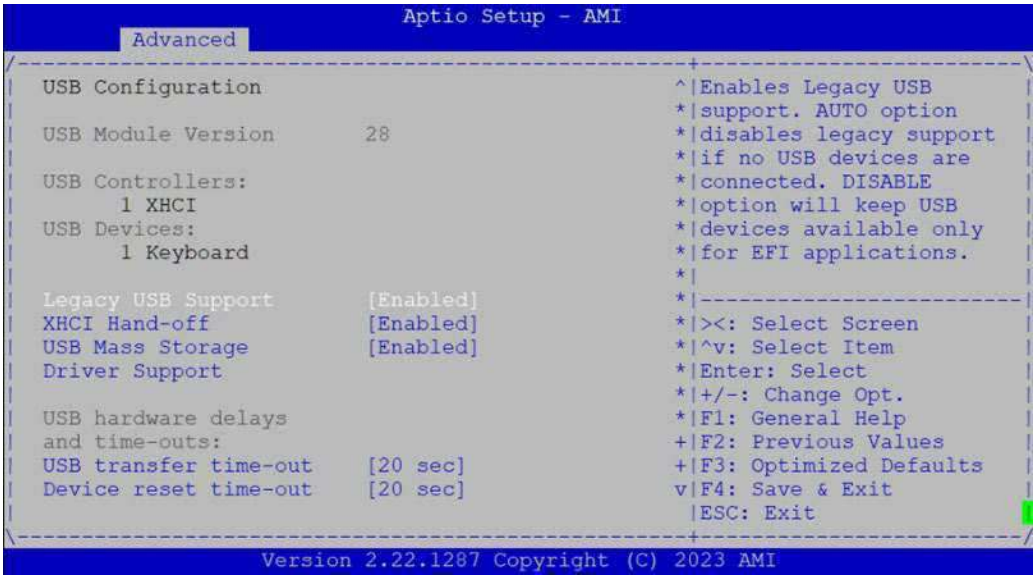
Feature	Options	Description
Redirection COM Port	COM0	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages
Resolution	80x24 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Redirect After POST	Always Enable BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

PCI Subsystem Settings



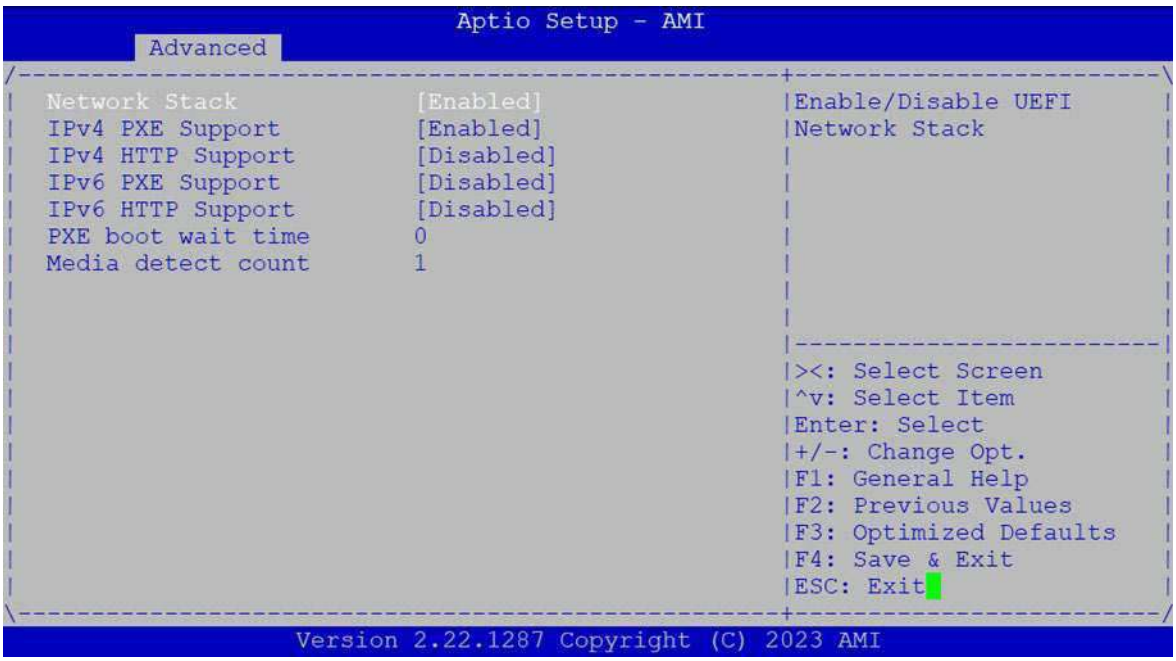
Feature	Options	Description
Re-Size BAR Support	Disabled Enabled	If system has Resizable BAR capable PCIe Devices, this option Enables or Disables Resizable BAR Support

USB Configuration



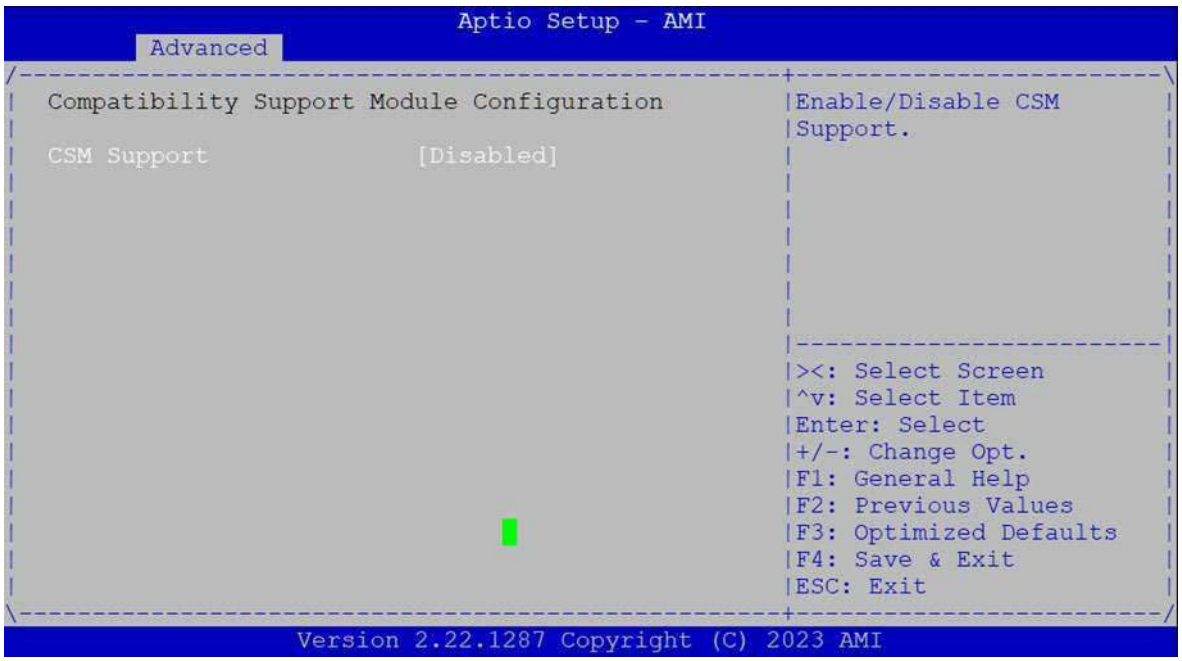
Feature	Options	Description
Legacy USB Support	Enabled Disabled Auto	Enables Legacy USB support. **Auto** option disables legacy support if no USB devices are connected. **Disabled** option will keep USB devices available only for EFI applications.
XHCI Hand-off	Enabled Disabled	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Disabled Enabled	Enable/Disable USB Mass Storage Driver Support.
USB transfer time-out	1 sec 5 sec 10 sec 20 sec	The time-out value for Control, Bulk, and Interrupt transfers
Device reset time-out	10 sec 20 sec 30 sec 40 sec	USB mass storage device Start Unit command time-out
Device power-up delay	Auto Manual	Maximum time the device will take before it properly reports itself to the Host Controller. **Auto** uses default value: for a Root port, it is 100 ms, for a Hub port the delay is taken from Hub descriptor.

Network Stack Configuration



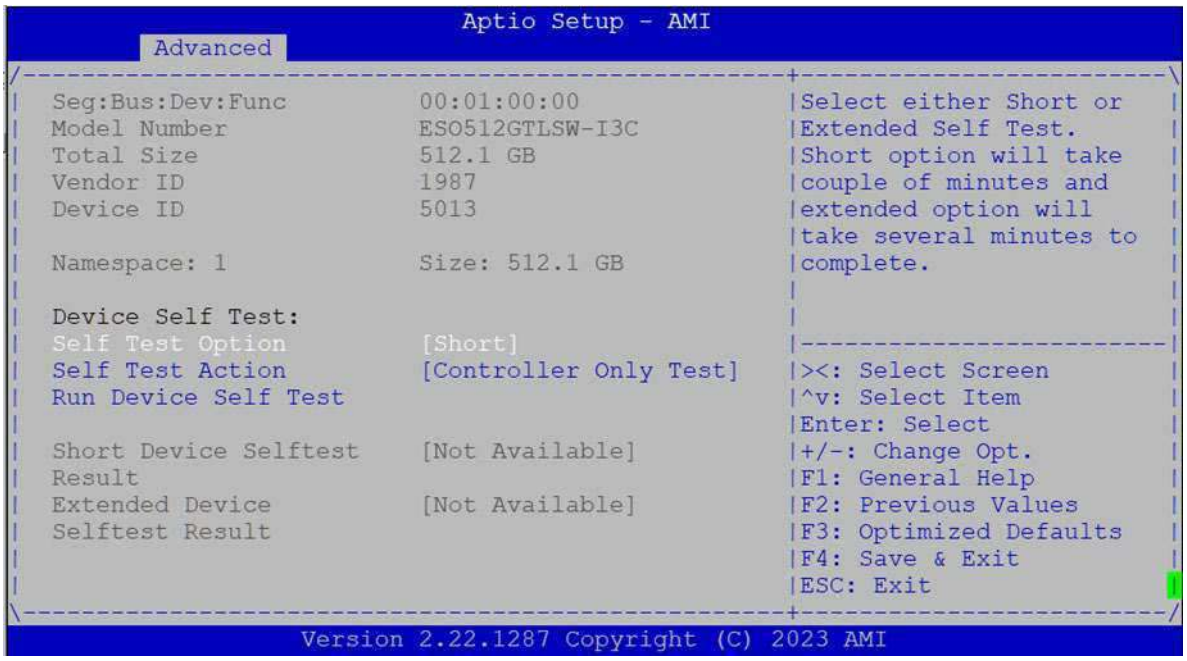
Feature	Options	Description
Network Stack	Disabled Enabled	Enable/Disable UEFI Network Stack
IPv4 PXE Support	Disabled Enabled	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	Disabled Enabled	Enable/Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.
IPv6 PXE Support	Disabled Enabled	Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.
IPv6 HTTP Support	Disabled Enabled	Enable/Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available.
PXE Boot Wait Time	0	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.
Media Detect Count	1	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

CSM Configuration



Feature	Options	Description
CSM Support	Disabled Enabled	Enable/Disable CSM Support

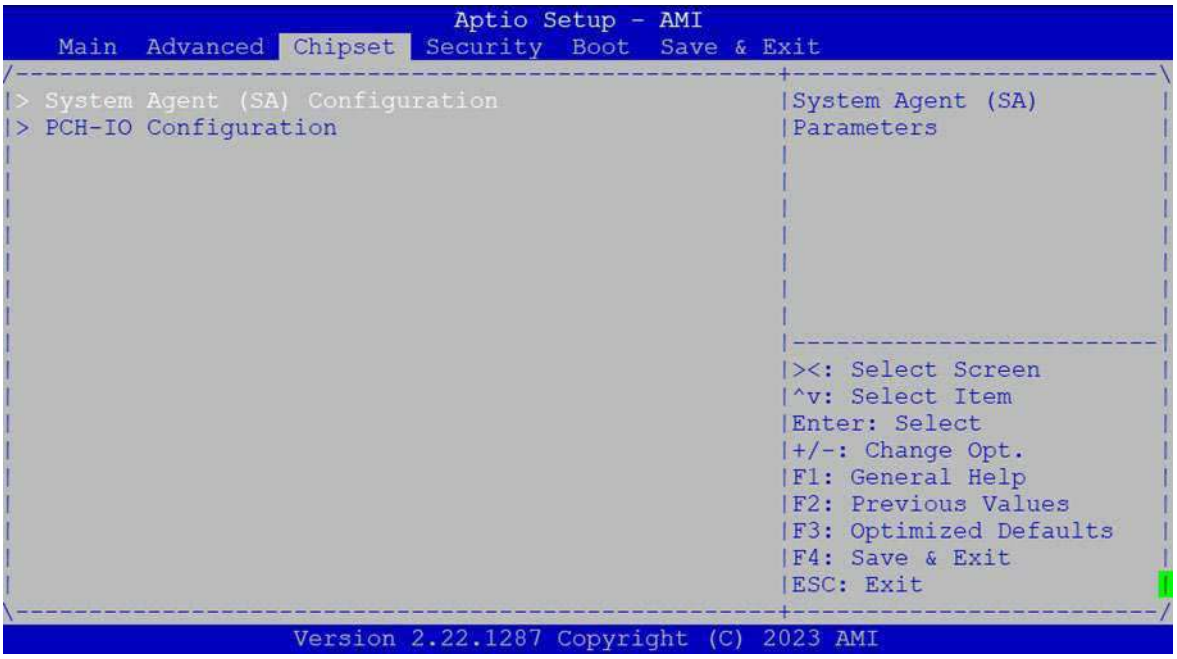
NVMe Configuration



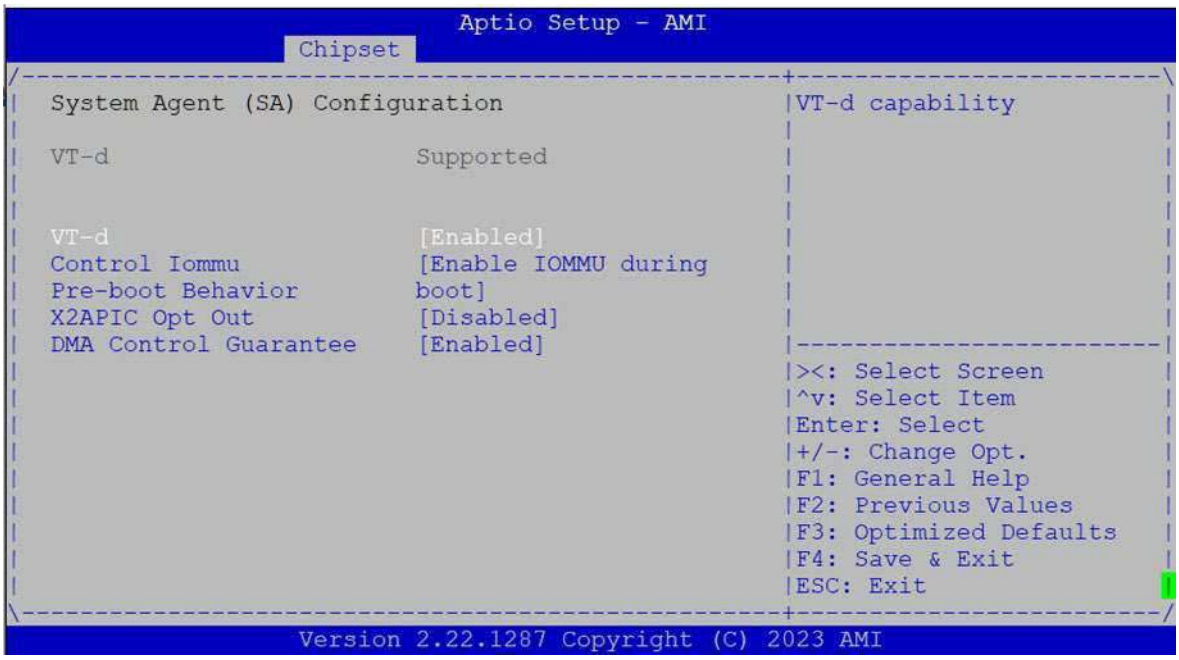
Feature	Options	Description
Self-Test Option	Short Extended	Select either Short or Extended Self-Test. Short option will take couple of minutes and extended option will take several minutes to complete.
Self-Test Action	Controller Only Test Controller and NameSpace Test	Select either to test Controller alone or Controller and NameSpace. Selecting Controller and Namespace option will take lot longer to complete the test.
Run Device Self-Test	N/A	Perform device self-test for the corresponding Option and Action selected by user. Pressing 'Esc' key will abort the test. Result shown below is the recent result logged in the device.

Chipset Page

Select the **Chipset** item from the BIOS setup screen to enter the **Chipset** page. Users can select any of the items in the left frame of the screen.

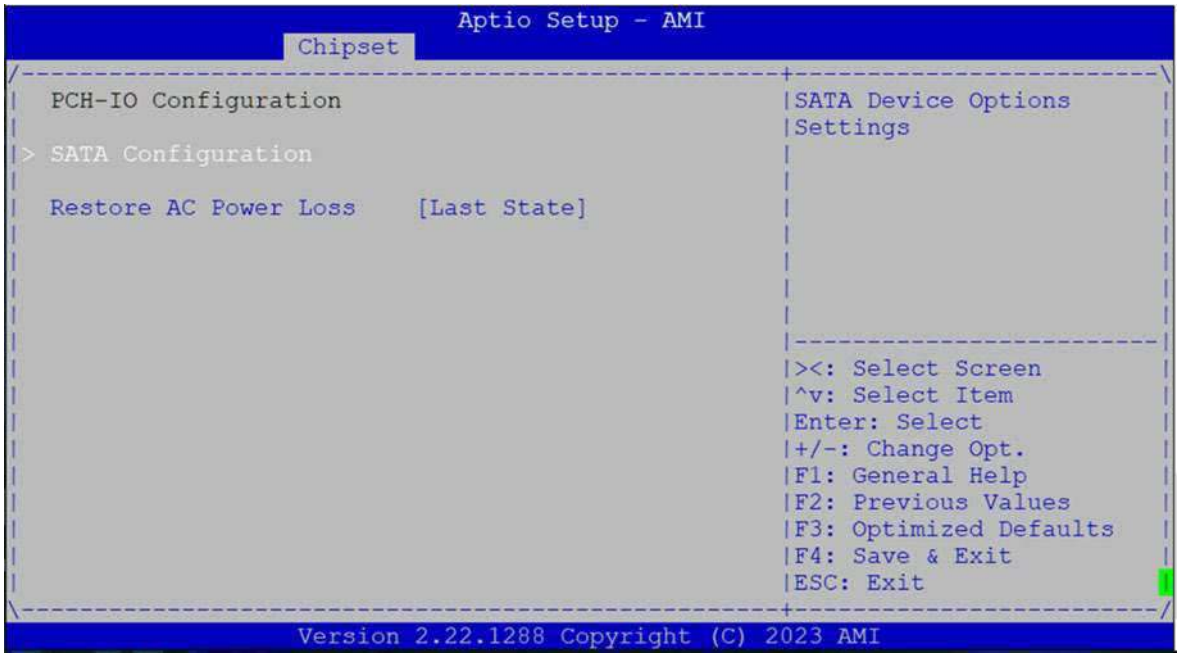


System Agent (SA) Configuration



Feature	Options	Description
VT-d	Disabled Enable	VT-d capability
Control Iommu	Disable IOMMU Enable IOMMU during Boot	Enable IOMMU in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)
X2APIC Opt Out	Enabled Disabled	Enable/Disable X2APIC_OPT_OUT bit
DMA Control Guarantee	Enabled Disabled	Enable/Disable DMA_CONTROL_GUARANTEE bit

PCH-IO Configuration



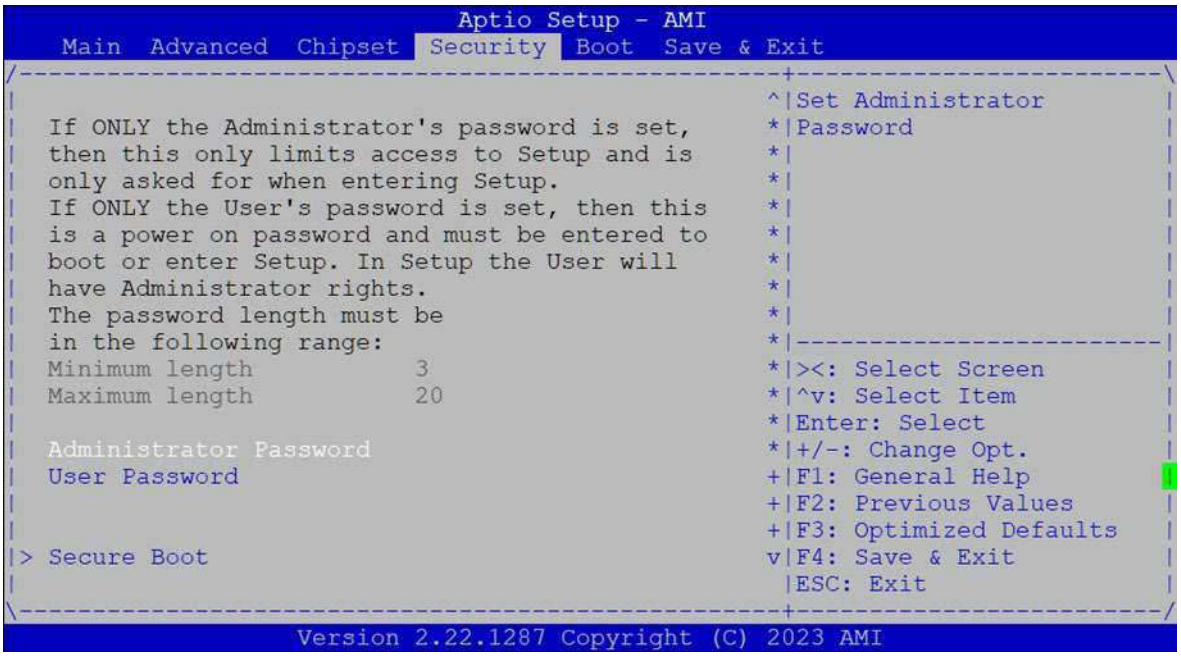
Feature	Options	Description
Restore AC Power Loss	Power On Power Off Last State	Specify what state to go to when power is re-applied after a power failure (G3 state).

SATA Configuration

Feature	Options	Description
SATA Controller(s)	Enabled Disabled	Enable/Disable SATA Device
SATA Mode Selection	AHCI	Determines how SATA controller(s) operate.

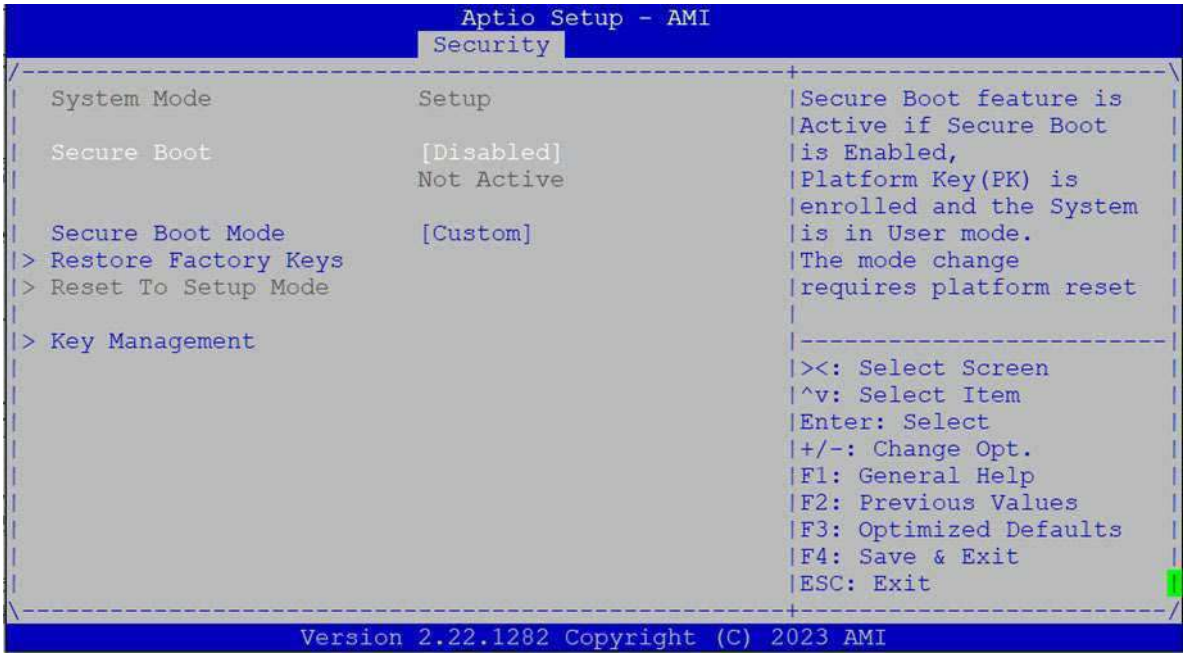
Security Page

Select the **Security** item from the BIOS setup screen to enter the **Security** page. Users can select any of the items in the left frame of the screen.



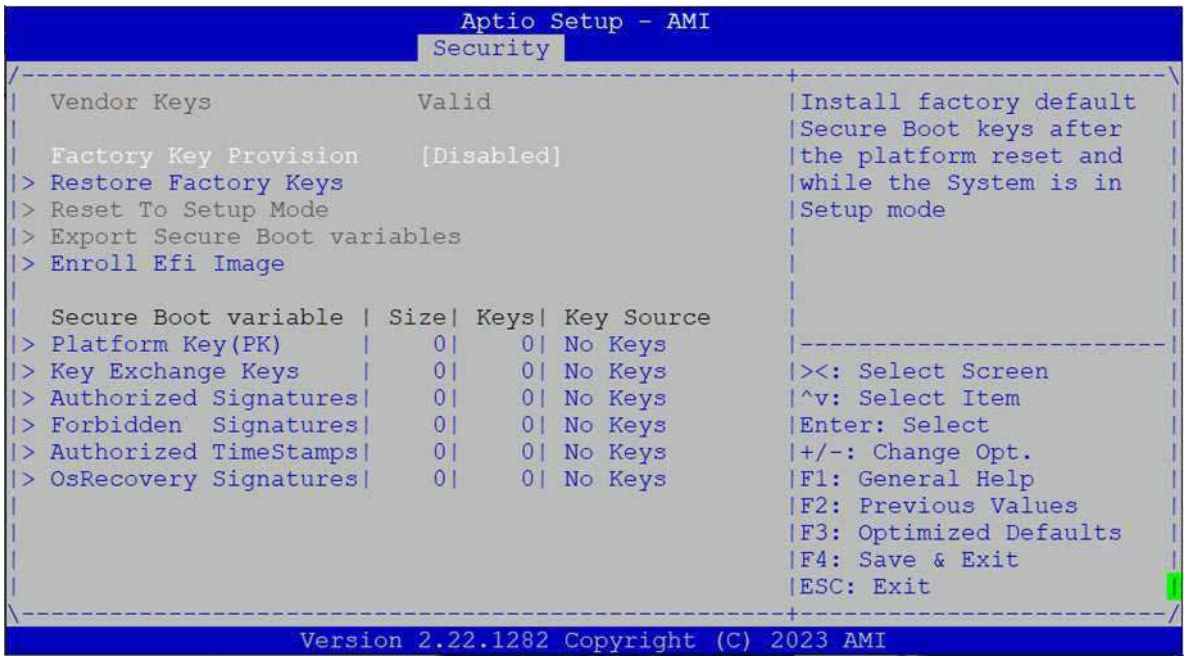
Feature	Description
Setup Administrator Password	If ONLY the Administrator's password is set, it only limits access to Setup and is only asked for when entering Setup.
User Password	If ONLY the User's password is set, it serves as a power-on password and must be entered to boot or enter Setup. In Setup, the User will have Administrator rights.

Secure Boot



Feature	Options	Description
Secure Boot	Disabled Enabled	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled and the System is in User mode. The mode change requires platform reset
Secure Boot Mode	Standard Custom	Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication

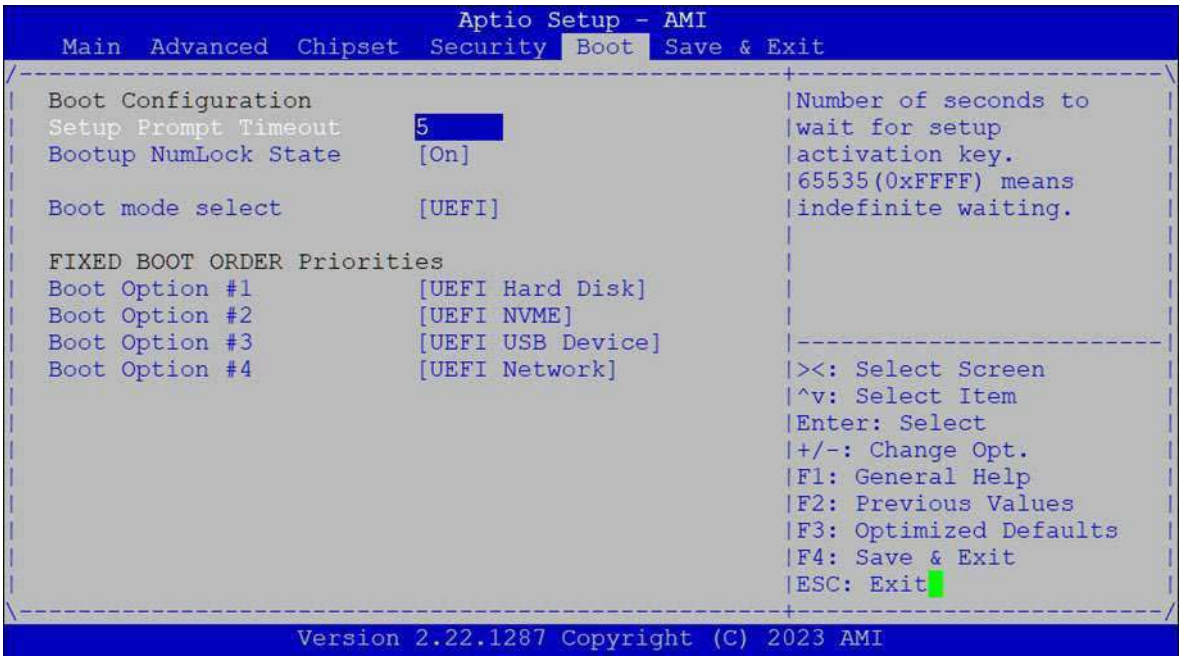
Key Management



Feature	Options	Description
Factory Key Provision	Disabled Enabled	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode
Restore Factory Keys	None	Force System to User Mode. Install factory default Secure Boot key databases
Reset to Setup Mode	None	Delete all Secure Boot key databases from NVRAM
Export Secure Boot Variables	None	Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device
Enroll Efi Image	None	Allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db)

Boot Page

Select the **Boot** item from the BIOS setup screen to enter the **Boot** page. Users can select any of the items in the left frame of the screen.

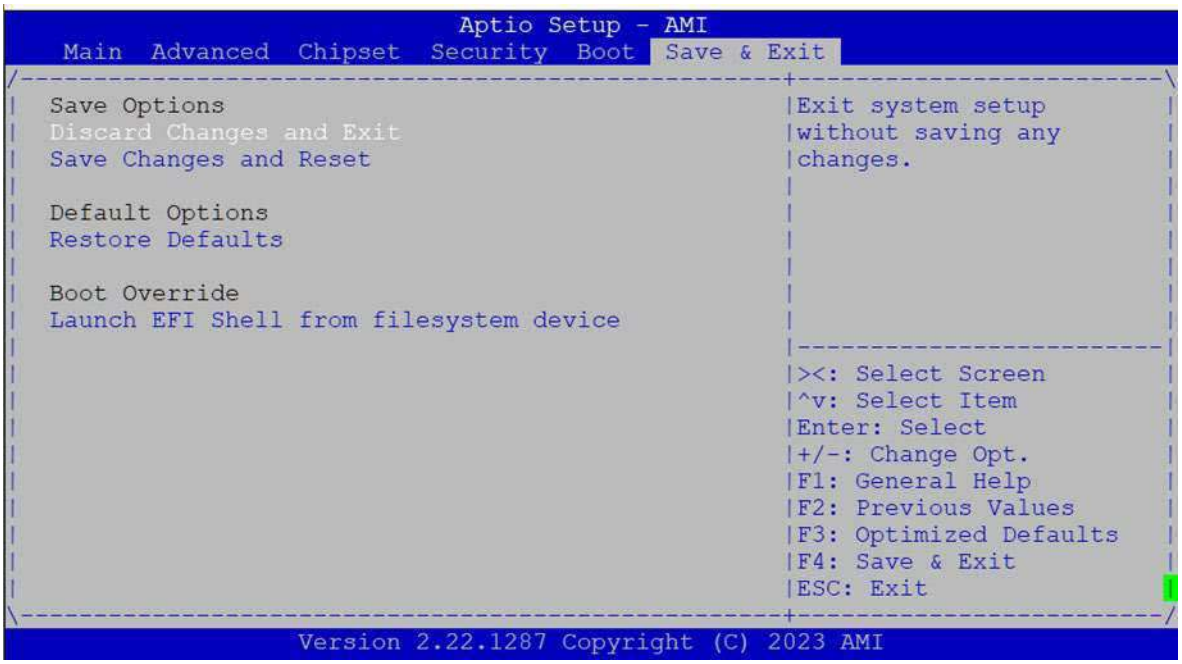


Feature	Options	Description
Setup Prompt Timeout	5	The number of seconds to wait for setup activation key. 65535 means indefinite waiting.
Bootup NumLock State	On Off	Select the keyboard NumLock state
Boot Mode Select	LEGACY UEFI DUAL	Select boot mode LEGACY/UEFI

- Default boot priority: **Hard Disk -> NVME -> USB -> Network**
- Choose specifies boot device priority sequence from available Group device.
- Choose boot priority from boot option group.

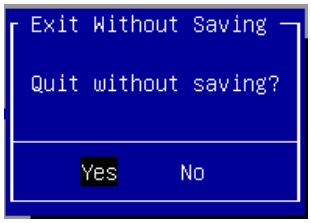
Save and Exit Page

Select the **Save and Exit** item from the BIOS setup screen to enter the **Save and Exit** page. Users can select any of the items in the left frame of the screen.



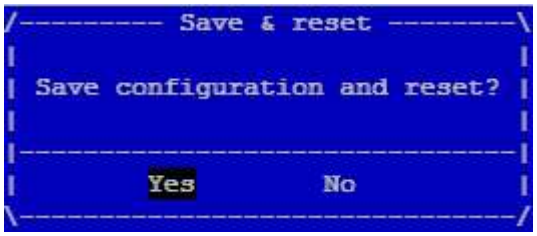
- **Discard Changes and Exit**

Select this option to quit Setup without saving any modifications to the system configuration. The following window will appear after the "**Discard Changes and Exit**" option is selected. Select "**Yes"** to Discard changes and Exit Setup.



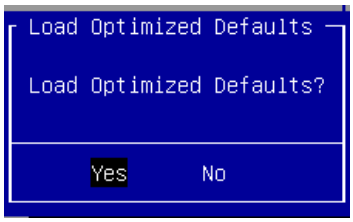
- **Save Changes and Reset**

When Users have completed the system configuration changes, select this option to save the changes and reset from BIOS Setup in order for the new system configuration parameters to take effect. The following window will appear after selecting the "**Save Changes and Reset**" option is selected. Select "**Yes**" to Save Changes and reset.



- **Restore Defaults**

Restore default values for all setup options. Select "**Yes"** to load Optimized defaults.

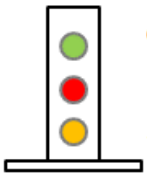


Note

The items under Boot Override may not be the same image as above. It should depend on the actual devices connect on system.

APPENDIX A: LED INDICATOR EXPLANATIONS

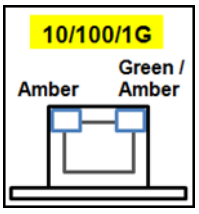
▸ System Power / Status / HDD Activity

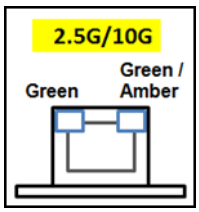


Green : Power
Green / Red : Status
Amber : HDD

LED	COLOR ON LCM	COLOR ON BOARD	LED ACTION	DESCRIPTION
POWER	**Green**	**Green**	Steady	When system power on
	Off	Off	N/A	No power on
STATUS	**Green**	**Green**	Steady	control by GPIO
	Amber	**Red**	Steady	control by GPIO
	Off	Off	N/A	control by GPIO (Default) or No power on
HDD	**Amber**	**Amber**	Blinking	Blinking indicates HDD activity Include SATA / NVME
	Off	Off	N/A	No data access or No power on

▸ RJ45 LAN LED





1Gb RJ-45 Define:

Speed	Amber (Active)	Green/Amber (Link)
10M	Blinking / Data access	OFF
100M	Blinking / Data access	ON (**Green**)
1G	Blinking / Data access	ON (**Amber**)
1. When cable is plugged-in and network is linked. Both LED will be bright. The behavior is as defined. 2. Without the Cable plug-in, the LED should be off. 3. If LAN Driver controls the LED, the behavior will follow the driver		

2.5Gb RJ-45 Define:

Speed	Green (Active)	Green/Amber (Link)
10/100M	Blinking / Data access	OFF
1G	Blinking / Data access	ON (**Amber**)
2.5G	Blinking / Data access	ON (**Green**)
1. When cable is plug-in and network is linked. Both LED lights will be bright. The behavior is as defined. 2. Without the Cable plug-in, the LED should be off 3. If LAN Driver controls the LED, the behavior will follow the driver		

APPENDIX B: TERMS AND CONDITIONS

Warranty Policy

1. All products are under warranty against defects in materials and workmanship for a period of one year from the date of purchase.
2. The buyer will bear the return freight charges for goods returned for repair within the warranty period, whereas the manufacturer will bear the after service freight charges for goods returned to the user.
3. The buyer will pay for the repair (for replaced components plus service time) and transportation charges (both ways) for items after the expiration of the warranty period.
4. If the RMA Service Request Form does not meet the stated requirement as listed on the "RMA Service," RMA goods will be returned at customer's expense.
5. The following conditions are excluded from this warranty:
   - Improper or inadequate maintenance by the customer
   - Unauthorized modification, misuse, or reversed engineering of the product
   - Operation outside of the environmental specifications for the product.

RMA Service

Requesting an RMA#

1. To obtain an RMA number, simply fill out and fax the "RMA Request Form" to your supplier.
2. The customer is required to fill out the problem code as listed. If your problem is not among the codes listed, please write the symptom description in the remarks box.
3. Ship the defective unit(s) on freight prepaid terms. Use the original packing materials when possible.
4. Mark the RMA# clearly on the box.

Note: The customer is responsible for shipping damage(s) resulting from inadequate/loose packing of the defective unit(s). All RMA# are valid for 30 days only; RMA goods received after the effective RMA# period will be rejected.

RMA Service Request Form

When requesting RMA service, please fill out the following form. Without this form enclosed, your RMA cannot be processed.

RMA No:	Reasons to Return: ▫ Repair(Please include failure details) ▫ Testing Purpose
Company:	Contact Person:
Phone No.	Purchased Date:
Fax No.:	Applied Date:
Return Shipping Address: _____ Shipping by: ▫ Air Freight ▫ Sea ▫ Express_____ ▫ Others:_____	

Item	Model Name	Serial Number	Configuration

Item	Problem Code	Failure Status

*Problem Code:

01:D.O.A.	07: BIOS Problem	13: SCSI	19: DIO
02: Second Time R.M.A.	08: Keyboard Controller Fail	14: LPT Port	20: Buzzer
	09: Cache RMA Problem	15: PS2	21: Shut Down
03: CMOS Data Lost	10: Memory Socket Bad	16: LAN	22: Panel Fail
04: FDC Fail	11: Hang Up Software	17: COM Port	23: CRT Fail
05: HDC Fail	12: Out Look Damage	18: Watchdog Timer	24: Others (Pls specify)
06: Bad Slot			

Request Party

Authorized Signature / Date

Confirmed By Supplier

Authorized Signature / Date

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Relatório Nível III - Regularidade Fiscal e Trabalhista Federal

Dados do Fornecedor

CNPJ: **44.122.701/0001-79**
Razão Social: **SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA**
Nome Fantasia: **G2Z**
Situação do Fornecedor: **Credenciado** Data de Vencimento do Cadastro: **21/01/2026**

Dados do Nível

Situação do Nível: **Cadastrado**

Comprovante de Regularidade da Receita Federal e PGFN

Tipo de Comprovante: **Certidão** Data de Validade: **12/10/2025**
Código de Controle: **B49B3452D6366B1B**

Comprovante de Regularidade do FGTS

Tipo de Comprovante: **Certidão** Data de Validade: **25/07/2025**
Código de Controle: **2025062609486413755566**

Comprovante de Regularidade do TST

Tipo de Comprovante: **Certidão** Data de Validade: **30/12/2025**
Código de Controle: **374612622025**

OAP101

Wi-Fi 6 OUTDOOR Access Point

INTRODUCTION

The OAP101 is an enterprise-grade, dual-band Wi-Fi 6 outdoor access point, designed to withstand harsh weather conditions in outdoor and industrial environments with an IP68 rated, rust-resistant housing. The OAP101 features 2x2:2 uplink and downlink MU-MIMO that can each transmit data to multiple clients simultaneously, and together have a combined data rate of up to almost 3 Gbps. The OAP101's integration with Bluetooth Low Energy (BLE) enables value-added applications such as iBeacon and Matter applications.

The OAP101 can be operated in a standalone mode or managed by Edgecore ecCLOUD, ecCLOUD-VPC, or EWS/VEWS Series controllers.

HIGHLIGHTS

Wi-Fi

- Concurrent dual-band 2.4 and 5 GHz
- Wi-Fi 6 2x2:2 UL and DL MU-MIMO supporting up to 3 Gbps data rate
- Supports up to 32 ESSIDs
- High-density Wi-Fi deployment
- Bluetooth Low Energy (BLE)

Physical

- Wall and pole mountable
- IP68 weatherproof plastic housing
- Industrial temperature range
- RJ-45 console for troubleshooting and debug

SPECIFICATIONS

PHYSICAL	
Power	• DC Input: 48 VDC (DC terminal block) • PoE: 802.3at compliant (PSE injector is not included in standard package)
Dimensions	• 283.4 mm (L) x 293.4 mm (W) x 71 mm (H)
Weight	• 1.725 kg (excluding mounting bracket)
Interfaces	• Uplink (PoE In): 1 x 10/100/1000/2.5GBase-T Ethernet, Auto MDIX, RJ-45 with 802.3at PoE • LAN: 1 x 10/100/1000Base-T Ethernet, Auto MDIX, RJ-45 • Console: 1 x RJ-45
LED Indicator	• 1 x tri-color LED (Power, Cloud, Uplink)
Buttons	• 1 x Restart / Reset
Environmental Conditions	• Operating Temperature: -40˚C (-40˚F) to 60˚C (140˚F) • Operating Humidity: 5% to 95% non-condensing • IP66, IP68 rating
Power Consumption	• 21.12 W
Antenna	• 5 dBi (2.4 GHz, built-in omni-directional antennas with 20-degree down tilt) • 6 dBi (5 GHz, built-in omni-directional antennas with 20-degree down tilt) • 4.5 dBi (BLE, built-in)
Mounting	• Pole mount (standard bracket including hose clamp) • Wall mount (standard bracket)
Protective Vent	• Yes

WI-FI	
Standards	• 802.11 a/b/g/n/ac/ax • Concurrent dual-band 2.4 and 5 GHz
Support Data Rates	• 802.11b: 1, 2, 5.5, 11 Mbps • 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps • 802.11n: 6.5 – 300 Mbps (20 / 40 MHz) • 802.11ac: 6.5 – 867 Mbps (20 / 40 / 80 MHz) • 802.11ax: 3.6 – 574 Mbps (2.4 GHz, 20 / 40 MHz) • 802.11ax: 3.6 – 2402 Mbps (5 GHz, 20 / 40 / 80 /160 MHz)
Radio Chains	• 2.4 GHz: 2x2 • 5 GHz: 2x2
Spatial Streams	• 2; MU-MIMO support
Aggregate Conducted Transmit Power RF output power aggregates across MIMO chains and does not contain antenna gain.	• 2.4 GHz: up to 26 dBm • 5 GHz: up to 25 dBm Maximum power is limited by local regulations
Channelization	• 2.4 GHz: 20 / 40 MHz • 5 GHz: 20 / 40 / 80 / 160 MHz
Frequency Range	• 2.401 – 2.483 GHz • 5.170 – 5.835 GHz

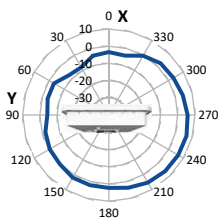
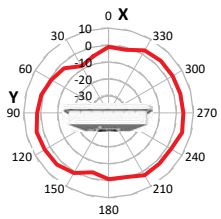
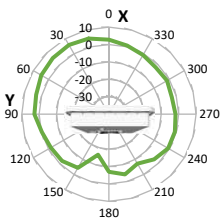
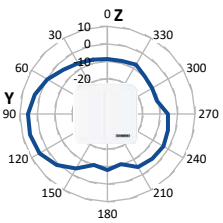
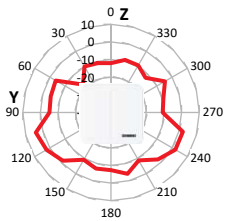
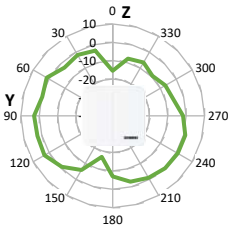
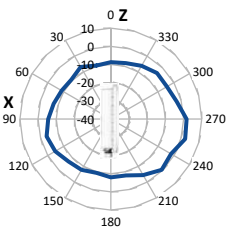
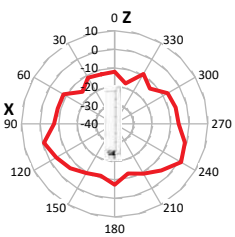
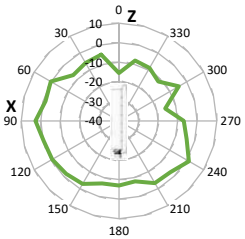
WI-FI	
Operating Channels Channels are restricted by local regulatory and product certifications	• 2.4 GHz: 1 – 11 (US), 1 – 13 (Europe) , 1-13 (Japan) • 5 GHz: 36 – 165 (US), 36 – 140 (Europe), 100-144 (Japan)
ESSID	• Up to 16 per radio (32 in total)
Certification	• FCC, CE, TELEC, VCCI
Physical Data Rate	• Up to 574 Mbps (2.4 GHz) • Up to 2402 Mbps (5 GHz)

FEATURES	
Wireless	• 802.11 k/v/r • Orthogonal Frequency Division Multiple Access (OFDMA) • Client isolation • Open Mesh • BSS Coloring • Band Steering • Wi-Fi Enhanced Open (OWE) • Wireless site survey
Network	• Spanning Tree Protocol (STP) • Dynamic Host Configuration Protocol (DHCP) • DHCP Relay • 802.1q • Access Control List (ACL) • Network Address Translation (NAT) • Dynamic VLAN • Link Layer Discovery Protocol (LLDP) • Smart isolation • IPv6 compatible • Proxy ARP
Security	• WPA-Personal (AES) • WPA-Enterprise (AES) • WPA2-Personal (AES) • WPA2-Enterprise (AES) • WPA3-Personal (AES) • WPA3-Personal Transition (AES) • WPA3-Enterprise (AES) • WPA3-Enterprise transition (AES) • MAC Address Authentication • Multi Pre-Shared Key (MPSK) • Dynamic Pre-Shared Key (DPSK) • MAC Address Authentication • DHCP Snooping • ARP Inspection • L3 Firewall

FEATURES

Maintenance	• Network Time Protocol (NTP) • Standalone • Management by ecCLOUD • Management by ecCLOUD-VPC • Management by EWS/VEWS Series Controller (Complete Tunnel/Split Tunnel) • SSH • QR code onboarding • SNMP v1/v2c/v3 • Remote Syslog • Discovery tool • Zero Touch Provisioning (ZTP)
QoS	• RSSI threshold (optimal client filtering) • Multicast-to-Unicast conversion • WME
Mobility	• OpenRoaming (Hotspot 2.0 R1)
Others	• iBeacon • Target Wake Time (TWT) • Hotspot captive portal • Dynamic Authorization (DAE)

SIGNAL COVERAGE PATTERN

	2.4 GHz	5 GHz	Bluetooth
Azimuth			
Elevation ZY			
Elevation ZX			

ORDERING INFORMATION

Part Number	Description	Remark
FI2WL0101009A	OAP101 (WW)	Edgecore OAP101
131500000206A	POE29U-560	30W PSE injector

TEL: 886-3-5638888 FAX: 886-3-6686111
1, Creation Rd. III, Hsinchu Science Park, Taiwan 30077
sales@edge-core.com
www.edge-core.com

Quick Start Guide

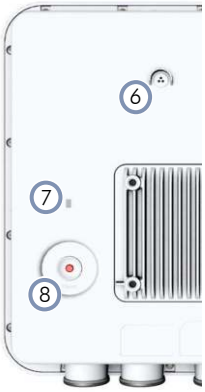
Outdoor Access Point

OAP101 | OAP101-6E

Package Contents

1. OAP101 or OAP101-6E access point
2. Mounting bracket and 4 x M6 screws
3. DC terminal plug
4. 3 x Cable glands
5. 2 x Steel-band clamps for pole mount (2.5 inch diameter max.)
6. Screw kit—4 screws and 4 plugs
7. QR code card

Overview



1. Grounding point
2. DC In port: 48 VDC
3. Uplink (PoE) port: RJ-45 2.5GBASE-T connection to 802.3at PoE
4. LAN port: 1 Gbps LAN connection
5. Console port
6. Moisture protective vent
7. Power/Status LED:
   - Yellow green: On (power OK), Blinking (boot up)
   - Blue: On (cloud managed)
   - Purple: Blinking (uplink activity in cloud managed mode)
   - Orange: Blinking (uplink activity in stand-alone mode)
8. Restart/Reset button:
   - A quick press restarts the system.
   - Press and hold for 5 seconds resets to factory defaults.

Installation

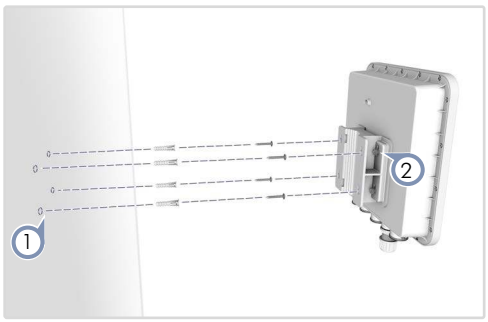
Warning: For a safe and reliable installation, use only the accessories and screws provided with the device. Use of other accessories and screws could result in damage to the unit. Any damages incurred by using unapproved accessories are not covered by the warranty.

Warning: To ensure compliance with IP66 and IP68 standards, maintain a cap or a cable gland on all ports.

Note: The drawings in this document are for illustration only and may not match your particular model.

1 Mount the Device

a. Mounting on a Wall



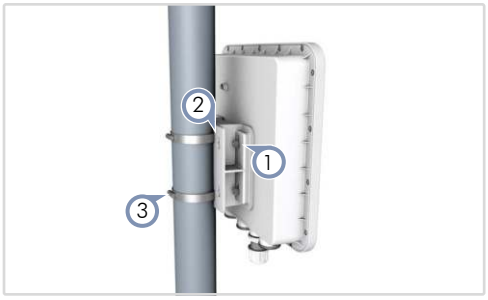
1. At the installation location on the wall, use the mounting bracket to mark four holes for the wall plugs and screws. The bracket must be installed with the marking “UP” at the top.

   Drill four holes for the wall plugs, and then insert the plugs and tap them flush with the wall surface.

   Note: Drill 2.5 mm (±0.2 mm) holes for M3 self-tapping screws, or 4.5 mm (±0.2 mm) holes for nylon wall plugs.

2. Use the included M6 screws to attach the mounting bracket to the device.
3. With its ports facing down, slide the device down onto the pre-installed screws until it snaps into its secured position. Do not let go of the device until you confirm that it is secure.

b. Mounting on a Pole



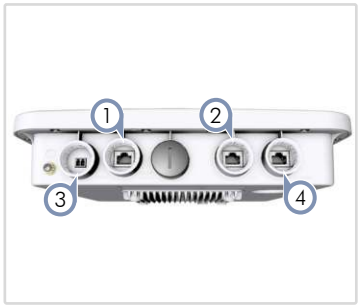
1. Use the included M6 screws to attach the mounting bracket to the device.
2. Feed the two steel-band clamps through the pole-mount bracket mounting points.
3. Fasten the steel-band clamps around the pole to secure the AP to the pole.

2 Ground the Device

1. Ground the device by connecting a ground wire to the grounding point on the device and to nearby good earth.

3 Connect Cables

a. Connect Ethernet Cables



Note: Port covers and cable glands should be tightened to a torque of 10 kgf.cm.

1. Connect Category 5e or better cable to the Uplink (PoE In) 2.5GBASE-T RJ-45 port. When connected to a PoE source, the Uplink (PoE In) port connection provides power to the unit.
2. (Optional) Connect a local LAN switch or computers to the LAN 1000BASE-T RJ-45 port.

b. (Optional) Connect DC Power

3. Wire the included DC terminal plug to a 48 VDC, 0.5 A source to provide power to the device. Follow the wiring scheme shown on the panel with the negative pole (-) on the left and the positive pole (+) on the right.

c. (Optional) Management Connection

4. Connect an RJ-45 to DB9 straight-through console cable and then configure the serial connection: 115200 bps, 8 characters, no parity, one stop bit, 8 data bits, and no flow control.

4 Check AP LED

1. When operating normally, the Power/Status LED should be on yellow green. Blinking indicates the device is booting up.

5 Initial Setup and AP Registration

There are three options for setting up the AP for your network:

- If your network is already managed by ecCLOUD, you can just register the AP on your network by entering the MAC address and serial number on ecCLOUD.
- Connect to the AP's web interface through a network connection to one of the AP's LAN ports. See section "Connecting to the Web Interface".
- Use QR-Code Onboarding to connect to the AP through a web browser on a phone. See section "QR Code Onboarding".

The first-time you access the AP's web management interface, it automatically runs the Setup Wizard for initial AP configuration. Follow the Setup Wizard steps to configure the AP for management by ecCLOUD or in a stand-alone mode.

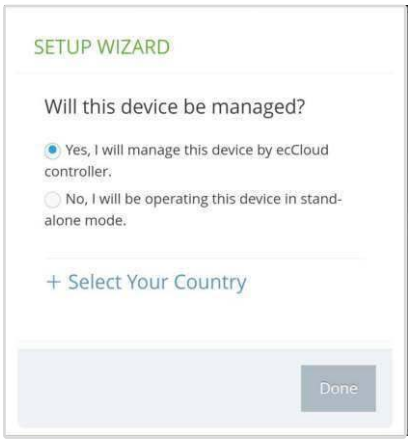
Connecting to the Web Interface

Follow these steps to connect to the AP's web interface through a network connection to one of the AP's LAN ports.

1. Connect a PC directly to one of the AP's LAN ports.
2. Set the PC IP address to be on the same subnet as the AP LAN port default IP address. (The PC address must start 192.168.2.x with subnet mask 255.255.255.0.)
3. Enter the AP's default IP address of 192.168.2.1 into the web browser address bar.

Note: To connect to the web interface using the Uplink (PoE) port, the IP address is automatically assigned through DHCP by default. If a DHCP server is unreachable, the Uplink (PoE) port reverts to a fallback IP address of 192.168.1.10.

4. On first-time log in to the web interface, the Setup Wizard starts and you must select how the AP will be managed using the ecCLOUD controller or in stand-alone mode.



5. Continue with the Setup Wizard to make other settings:
   - **Cloud-Managed Mode:** Select the country of operation.
   - **Stand-Alone Mode:** Use the default wireless network setting or customize the network name, then set a password (the default user name is "admin" with password "admin"), and select the country of operation.
6. Click "Done" to finish the setup wizard.

Note: For more information on the Setup Wizard and AP configuration, refer to the *User Manual*.

QR Code Onboarding

For quick set up and registration of your AP with the ecCLOUD controller, you can scan the QR code on the AP using a phone.

Follow these steps:

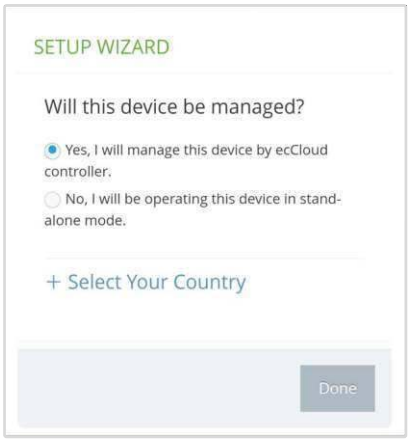
1. Make sure the AP is powered on and connected to the Internet.
2. Use the camera or a barcode app on your phone to scan the AP's QR code. The QR code is printed on a label next to the AP's ports.

3. When a message pops up, tap "yes" to join the Wi-Fi network (iPhone requires you to go to Settings > Wi-Fi or open the browser for the message to pop up).

   The web browser should open and redirect to the Setup Wizard page.

Note: If the phone cannot connect to the Wi-Fi network, type the SSID (network name) and password manually. The SSID name is the AP serial number (for example, EC0123456789), and the password is the AP MAC address (for example, 903CB3BC1234).

4. After setting a new password and the regulatory country, select to manage the AP using the ecCLOUD controller or to manage the AP in stand-alone mode.

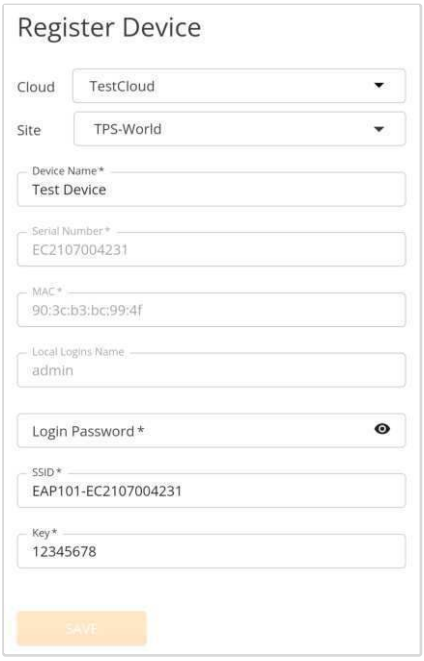


   a. **Stand-Alone Mode:** Use the default wireless network setting or customize the network name and password. Tap "Done" to finish the Setup Wizard.

      Wait about two minutes for the AP configuration to update, and then connect to the wireless network name configured in the setup wizard. The browser is then redirected to the login page of the AP.

   b. **Cloud-Managed Mode:** Tap "Done" to finish the setup wizard and the browser is redirected to the ecCLOUD login page.

If you already have an ecCLOUD account, log in and select a site for the AP. The AP is automatically registered for cloud management. After you tap "Save," wait about two minutes for the cloud controller to configure the AP.



If you do not have an ecCLOUD account, tap "I want to register" and first set up an account. Create a cloud and site before confirming the regulatory country. After tapping "Next," the AP is then automatically registered for cloud management. After you tap "Save," wait about two minutes for the cloud controller to configure the AP.

Note: Refer to the Edgecore *ecCLOUD Controller User Manual* for more information on setting up and configuring APs through ecCLOUD.

Safety and Regulatory Information

FCC Interference Statement

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.

For product available in the USA/Canada market, only channel 1–11 can be operated. Selection of other channels is not possible.

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft.

Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 59 cm between the radiator and your body.

1. Installation personnel

This product is designed for specific applications and should be installed by qualified personnel who have knowledge of RF and its related regulations. A general user shall not attempt to install or modify the equipment configuration.

2. Installation location

To meet regulatory RF exposure requirements, this product shall be installed at a location where, during normal operations, the radiating antenna is at least 59 cm away from any nearby persons.

3. External antenna

Use only the antennas which have been approved by the applicant. Using non-approved antenna(s) is prohibited and may produce unwanted spurious or excessive RF transmitting power which may lead to a violation of FCC limits.

4. Installation procedure

Please refer to this equipment's user manual for the procedure details.

FCC Warning: The installation position must be carefully selected so that the final output power does not exceed the limit set forth in relevant regulations. Violation of output power regulations could lead to serious federal penalties.

CE Statement

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

All operational modes:

2.4 GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ax (HE20), 802.11ax (HE40)

5 GHz: 802.11a, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ac (VHT80), 802.11ax (HE20), 802.11ax (HE40), 802.11ax (HE80), 802.11ax (HE160)

BLE 2.4 GHz: 802.15.1

The frequency and maximum transmitted power limit in EU are listed as below:

2412-2472 MHz: 20 dBm
5470-5725 MHz: 30 dBm

AT	BE	BG	CH	CY	CZ
DE	DK	EE	EL	ES	FI
FR	HR	HU	IE	IS	IT
LI	LT	LU	LV	MT	NL
NO	PL	PT	RO	SE	SI
SK	TR	UK			

The abbreviations of the countries, as prescribed in above table, where any restrictions on putting into service or any requirements for authorization of use exist.

CE Mark Declaration of Conformance for EMI and Safety (EEC)

This information technology equipment is in compliance with the Directive 2014/53/EU and Directive 2014/35/EU.

The Declaration of Conformity (DoC) can be obtained from www.edge-core.com -> support -> download.

Japan - VCCI Statement

この装置は、クラスB機器です。この装置は、住宅環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。 VCCI－B

Applies to OAP101 only.

NCC Statement (Taiwan)

NCC 警語

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通

信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。 應避免影響附近雷達系統之操作。

MPE

本產品電磁波曝露量 (MPE) 標準值 1mW/cm2，送測產品實測值為 0.12152 mW/cm2，建議使用時至少距離人體 51 cm。

BSMI (Taiwan)

電氣方面的安全性

- 為避免可能的電擊造成嚴重損害，搬動產品之前，請先將產品電源線暫時從電源插座中拔掉。
- 當您要加入硬體裝置到系統中或者要移除系統中的硬體裝置時，請務必先連接該裝置的訊號線，然後再連接電源線。可能的話，在安裝硬體裝置之前先拔掉產品的電源供應器電源線。
- 當您要從主機板連接或拔除任何的訊號線之前，請確定所有電源線已事先拔掉。
- 請確定電源供應器的電壓設定已調到本國 / 本區域所使用的電壓標準值。若您不確定您所屬區域的供應電壓值為何，那麼請就近詢問當地的電力公司人員。
- 如果電源供應器已損壞，請不要嘗試自行修復。請將之交給專業技術服務人員或經銷商來處理。

操作方面的安全性

- 在使用產品之前，請確定所有的排線、電源線都已正確地連接好。若您發現有重大的瑕疵，請盡速連絡您的經銷商。
- 為避免發生電氣短路情形，請務必將所有沒用到的螺絲、迴紋針及其他零件收好，不要遺留在主機板上或產品主機中。
- 灰塵、溼氣以及劇烈的溫度變化都會影響主機板的使用壽命，因此請盡量避免放置在這些地方。
- 請勿將產品主機放置在容易搖晃的地方。
- 若在本產品的使用上有任何的技術性問題，請和經過檢定或有經驗的技術人員聯絡。

使用注意事項

- 在您開始操作本系統之前，請務必詳閱以下注意事項，以避免因為人為的疏失造成系統損傷甚至人體本身的安全。
- 使用前，請檢查產品各部份組件是否正常，以及電源線是否有任破損，或是連接不正確的情形發生。
- 如果有任何破損情形，請盡速與您的授權經銷商連絡，更換良好的線路。
- 產品放置的位置請遠離灰塵過多，溫度過高，太陽直射的地方。
- 保持機器在乾燥的環境下使用，雨水、溼氣、液體等含有礦物質將會腐蝕電子線路。
- 使用時，請務必保持周遭散熱空間，以利散熱。
- 使用前，請檢查各項周邊設備是否都已經連接妥當再開機。
- 避免邊吃東西邊使用，以免污染機件造成故障。
- 請避免讓紙張碎片、螺絲及線頭等小東西靠近產品之連接器、插槽、孔位等處，避免短路及接觸不良等情況發生。
- 請勿將任何物品塞入產品內，以避免引起機件短路或電路損毀。
- 產品開機一段時間之後，散熱片及部份 IC 表面可能會發熱、發燙，請勿用手觸摸，並請檢查系統是否散熱不良。
- 在安裝或移除周邊產品時請先關閉電源。
- 電源供應器如果發生損壞，切勿自行修理，請交由授權經銷商處理。
- 產品的機殼、鐵片大部份都經過防割傷處理，但是您仍必須注意避免被某些細部鐵片尖端及邊緣割傷，拆裝機殼時最好能夠戴上手套。

當你有一陣子不使用產品時，休假或是颱風天，請關閉電源之後將電源線拔掉。

限用物質含有情況標示聲明書
Declaration of the Presence Condition of the Restricted Substances Marking

設備名稱：戶外型無線基地台 Equipment Name			型號 (型式) : OAP101 Type Designation (Type)			
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr^{+6})	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
電路板組件 PCBA	—	○	○	○	○	○
組合線 Cable ass'y	—	○	○	○	○	○
天線 Antenna	○	○	○	○	○	○
機殼 Chassis	○	○	○	○	○	○

備　考 1.	" 超出 0.1 wt %" 及 " 超出 0.01 wt %" 係指限用物質之百分比含量超出百分比含量基準值。
Note 1:	"Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.
備　考 2.	" ○ " 係指該項限用物質之百分比含量未超出百分比含量基準值。
Note 2:	" ○ " indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.
備　考 3.	" — " 係指該項限用物質為排除項目。
Note 3:	The " — " indicates that the restricted substance corresponds to the exemption.

Warnings and Cautionary Messages

Warning: This product does not contain any serviceable user parts.
Warning: Installation and removal of the unit must be carried out by qualified personnel only.

Caution: Wear an anti-static wrist strap or take other suitable measures to prevent electrostatic discharge when handling this equipment.
Caution: Do not plug a phone jack connector in the RJ-45 port. This may damage this device.
Caution: Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Hardware Specifications

AP Chassis

Size (LxWxH)	293.4 x 283.4 x 71 mm (11.55 x 11.16 x 2.80 in.)
Weight	1725 g (3.80 lb)
Waterproof Rating	IP66 and IP68
Temperature	Operating: -40° C to 60° C (-40° F to 140° F) Storage: -40° C to 70° C (-40° F to 158° F)
Humidity	Operating: 5% to 95% (non-condensing)

Network Interfaces

Ports	Uplink(PoE) RJ-45: 2.5GBASE-T, PoE PD LAN1 RJ-45: 1000BASE-T
2.4 GHz Radio	IEEE 802.11b/g/n/ax
5 GHz Radio	IEEE 802.11a/ac/n/ax
6 GHz Radio	IEEE 802.11a/ac/n/ax (OAP101-6E only)
Bluetooth Radio	IEEE 802.15.1
Radio Frequencies	US and TW: 2.4–2.4835 GHz 5.15–5.85 GHz 5.925-6.425 GHz (OAP101-6E only) 6.525-6.875 GHz (OAP101-6E only) EU: 2.4–2.4835 GHz 5.47–5.725 GHz Japan: 2.4–2.4835 GHz 5.47–5.730 GHz

Power Specifications

PoE Input Power	25.5 W max 802.3at-compliant
DC Power	DC Input: 48 VDC, 0.5 A

Regulatory Compliances

Radio	EN 300 328 V2.2.2 (2.4G/BT-LE) EN 301 893 V2.1.1 (5G) EN 303 413 V1.1.1 (GPS) EN 50385 / EN 62311: 2017 (MPE) 47 CFR FCC Part 15.247 47 CFR FCC Part 15.407 MIC Certification Rule, Article 2 Paragraph 1 Item 19 and 19-3 (OAP101 only) MIC Terminal Equipment Design Certification, Articles 3, 4, 6, 9, and 34 (OAP101 only) NCC LP002 (OAP101 only)
Emissions	EN 301 489-1 V2.1.1 (2017-02) EN 301 489-17 V3.1.1 (2017-02) EN 55032:2015 47 CFR FCC Rules and Regulations Part 15 Subpart B, Class B Digital Device VCCI CISPR 32:2016 Class B ITE (OAP101 only) BSMI CNS 15936 (OAP101 only)
Safety	EN 62368-1: 2014 + A11: 2017 EN 60950-22: 2017 IEC 62368-1: 2014 (Second Edition) IEC 60529: 1989+AMD1: 1999+ AMD2: 2013CSV (IP68) BSMI CNS 15598-1 (OAP101 only)

Quick Start Guide

Outdoor Access Point

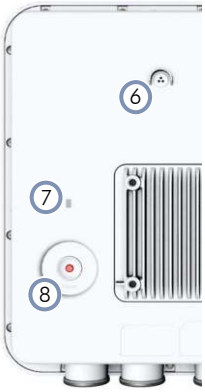
OAP101 (T) | OAP101-6E (T)

Edge-corE®

Package Contents

1. OAP101 (T) or OAP101-6E (T) access point
2. Mounting bracket and 4 x M6 screws
3. DC terminal plug
4. 3 x Cable glands
5. 2 x Steel-band clamps for pole mount (2.5 inch diameter max.)
6. Screw kit—4 screws and 4 plugs
7. QR code card

Overview



1. Grounding point
2. DC In port: 48 VDC
3. Uplink (PoE) port: RJ-45 2.5GBASE-T connection to 802.3at PoE
4. LAN port: 1 Gbps LAN connection
5. Console port
6. Moisture protective vent
7. Power/Status LED:
   - Yellow green: On (power OK), Blinking (boot up)
   - Blue: On (cloud managed)
   - Purple: Blinking (uplink activity in cloud managed mode)
   - Orange: Blinking (uplink activity in stand-alone mode)
8. Restart/Reset button:
   - A quick press restarts the system.
   - Press and hold for 5 seconds resets to factory defaults.

Installation

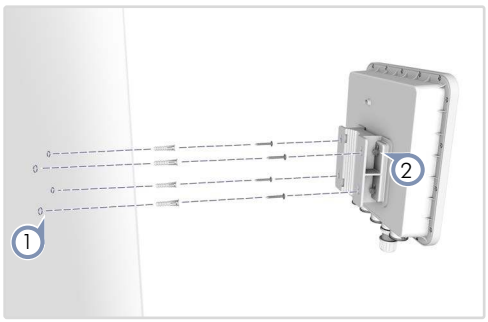
Warning: For a safe and reliable installation, use only the accessories and screws provided with the device. Use of other accessories and screws could result in damage to the unit. Any damages incurred by using unapproved accessories are not covered by the warranty.

Warning: To ensure compliance with IP66 and IP68 standards, maintain a cap or a cable gland on all ports.

Note: The drawings in this document are for illustration only and may not match your particular model.

1 Mount the Device

a. Mounting on a Wall



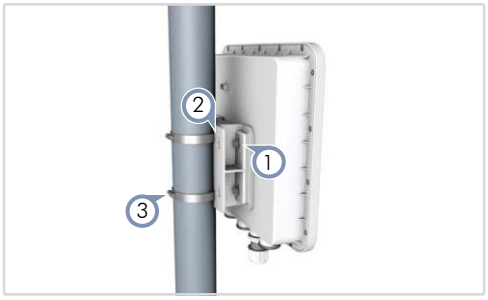
1. At the installation location on the wall, use the mounting bracket to mark four holes for the wall plugs and screws. The bracket must be installed with the marking “UP” at the top.

   Drill four holes for the wall plugs, and then insert the plugs and tap them flush with the wall surface.

   Note: Drill 2.5 mm (±0.2 mm) holes for M3 self-tapping screws, or 4.5 mm (±0.2 mm) holes for nylon wall plugs.

2. Use the included M6 screws to attach the mounting bracket to the device.
3. With its ports facing down, slide the device down onto the pre-installed screws until it snaps into its secured position. Do not let go of the device until you confirm that it is secure.

b. Mounting on a Pole



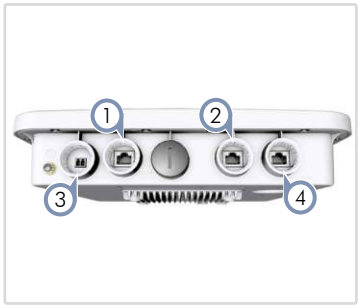
1. Use the included M6 screws to attach the mounting bracket to the device.
2. Feed the two steel-band clamps through the pole-mount bracket mounting points.
3. Fasten the steel-band clamps around the pole to secure the AP to the pole.

2 Ground the Device

1. Ground the device by connecting a ground wire to the grounding point on the device and to nearby good earth.

3 Connect Cables

a. Connect Ethernet Cables



Note: Port covers and cable glands should be tightened to a torque of 10 kgf.cm.

1. Connect Category 5e or better cable to the Uplink (PoE In) 2.5GBASE-T RJ-45 port. When connected to a PoE source, the Uplink (PoE In) port connection provides power to the unit.
2. (Optional) Connect a local LAN switch or computers to the LAN 1000BASE-T RJ-45 port.

b. (Optional) Connect DC Power

3. Wire the included DC terminal plug to a 48 VDC, 0.5 A source to provide power to the device. Follow the wiring scheme shown on the panel with the negative pole (-) on the left and the positive pole (+) on the right.

c. (Optional) Management Connection

4. Connect an RJ-45 to DB9 straight-through console cable and then configure the serial connection: 115200 bps, 8 characters, no parity, one stop bit, 8 data bits, and no flow control.

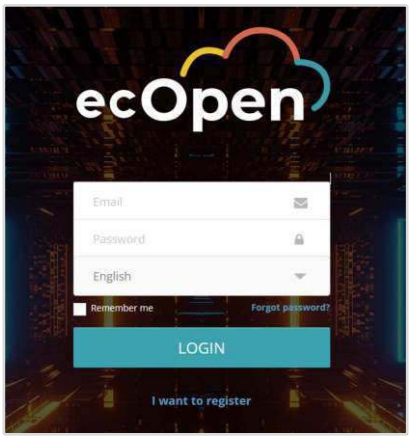
4 Check AP LED

1. When operating normally, the Power/Status LED should be on yellow green. Blinking indicates the device is booting up.

5 Initial Setup and AP Registration

There are two options for setting up the AP for your network:

- When the AP is first connected to the Internet through the Uplink port, it is automatically redirected to ecOpen (https://cloud.openwifi.ignitenet.com/). Enter the AP's MAC address and serial number for device registration.



- By default, the AP is assigned an IP address through DHCP. If the AP cannot connect to ecOpen, access the AP's web interface through one of the AP's LAN ports to make configuration changes (for example, to change from DHCP to a static IP). See section "Connecting to the Web Interface".

Connecting to the Web Interface

Note that you can only connect to the AP's web interface when the AP is not connected to the Internet.

Follow these steps to connect to the AP's web interface through a network connection to one of the AP's LAN ports.

1. Connect a PC directly to one of the AP's LAN ports.
2. Set the PC IP address to be on the same subnet as the AP LAN port default IP address. (The PC address must start 192.168.1.x with subnet mask 255.255.255.0.)
3. Enter the AP's default IP address of 192.168.1.1 into the web browser address bar.
4. Log in to the web interface using the default user name "root" and password "openwifi".

Note: The TIP OpenWiFi SDK default URL of the DigiCert certificate is set to ecOpen: (https://cloud.openwifi.ignitenet.com). If you want to register the AP to your own TIP OpenWiFi SDK, contact oxherd@edge-core.com to change the default URL.

Safety and Regulatory Information

FCC Interference Statement

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.

For product available in the USA/Canada market, only channel 1–11 can be operated. Selection of other channels is not possible.

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft.

Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 59 cm between the radiator and your body.

1. Installation personnel

This product is designed for specific applications and should be installed by qualified personnel who have knowledge of RF and its related regulations. A general user shall not attempt to install or modify the equipment configuration.

2. Installation location

To meet regulatory RF exposure requirements, this product shall be installed at a location where, during normal operations, the radiating antenna is at least 59 cm away from any nearby persons.

3. External antenna

Use only the antennas which have been approved by the applicant. Using non-approved antenna(s) is prohibited and may produce unwanted spurious or excessive RF transmitting power which may lead to a violation of FCC limits.

4. Installation procedure

Please refer to this equipment's user manual for the procedure details.

FCC Warning: The installation position must be carefully selected so that the final output power does not exceed the limit set forth in relevant regulations. Violation of output power regulations could lead to serious federal penalties.

CE Statement

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

All operational modes:

2.4 GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ax (HE20), 802.11ax (HE40)

5 GHz: 802.11a, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ac (VHT80), 802.11ax (HE20), 802.11ax (HE40), 802.11ax (HE80), 802.11ax (HE160)

BLE 2.4 GHz: 802.15.1

The frequency and maximum transmitted power limit in EU are listed as below:

2412-2472 MHz: 20 dBm
5470-5725 MHz: 30 dBm

AT	BE	BG	CH	CY	CZ
DE	DK	EE	EL	ES	FI
FR	HR	HU	IE	IS	IT
LI	LT	LU	LV	MT	NL
NO	PL	PT	RO	SE	SI
SK	TR	UK			

The abbreviations of the countries, as prescribed in above table, where any restrictions on putting into service or any requirements for authorization of use exist.

CE Mark Declaration of Conformance for EMI and Safety (EEC)

This information technology equipment is in compliance with the Directive 2014/53/EU and Directive 2014/35/EU.

The Declaration of Conformity (DoC) can be obtained from www.edge-core.com -> support -> download.

Japan - VCCI Statement

この装置は、クラスB機器です。この装置は、住宅環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。 **VCCI ー B**

Applies to OAP101 (T) only.

NCC Statement (Taiwan)

NCC 警語

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受

合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。 應避免影響附近雷達系統之操作。

MPE

本產品電磁波曝露量 (MPE) 標準值 1mW/cm2，送測產品實測值為 0.12152 mW/cm2，建議使用時至少距離人體 51 cm。

BSMI (Taiwan)

電氣方面的安全性

- 為避免可能的電擊造成嚴重損害，搬動產品之前，請先將產品電源線暫時從電源插座中拔掉。
- 當您要加入硬體裝置到系統中或者要移除系統中的硬體裝置時，請務必先連接該裝置的訊號線，然後再連接電源線。可能的話，在安裝硬體裝置之前先拔掉產品的電源供應器電源線。
- 當您要從主機板連接或拔除任何的訊號線之前，請確定所有電源線已事先拔掉。
- 請確定電源供應器的電壓設定已調到本國 / 本區域所使用的電壓標準值。若您不確定您所屬區域的供應電壓值為何，那麼請就近詢問當地的電力公司人員。
- 如果電源供應器已損壞，請不要嘗試自行修復。請將之交給專業技術服務人員或經銷商來處理。

操作方面的安全性

- 在使用產品之前，請確定所有的排線、電源線都已正確地連接好。若您發現有重大的瑕疵，請盡速連絡您的經銷商。
- 為避免發生電氣短路情形，請務必將所有沒用到的螺絲、迴紋針及其他零件收好，不要遺留在主機板上或產品主機中。
- 灰塵、溼氣以及劇烈的溫度變化都會影響主機板的使用壽命，因此請盡量避免放置在這些地方。
- 請勿將產品主機放置在容易搖晃的地方。
- 若在本產品的使用上有任何的技術性問題，請和經過檢定或有經驗的技術人員聯絡。

使用注意事項

- 在您開始操作本系統之前，請務必詳閱以下注意事項，以避免因為人為的疏失造成系統損傷甚至人體本身的安全。
- 使用前，請檢查產品各部份組件是否正常，以及電源線是否有任破損，或是連接不正確的情形發生。
- 如果有任何破損情形，請盡速與您的授權經銷商連絡，更換良好的線路。
- 產品放置的位置請遠離灰塵過多，溫度過高，太陽直射的地方。
- 保持機器在乾燥的環境下使用，雨水、溼氣、液體等含有礦物質將會腐蝕電子線路。
- 使用時，請務必保持周遭散熱空間，以利散熱。
- 使用前，請檢查各項周邊設備是否都已經連接妥當再開機。
- 避免邊吃東西邊使用，以免污染機件造成故障。
- 請避免讓紙張碎片、螺絲及線頭等小東西靠近產品之連接器、插槽、孔位等處，避免短路及接觸不良等情況發生。
- 請勿將任何物品塞入產品內，以避免引起機件短路或電路損毀。
- 產品開機一段時間之後，散熱片及部份IC表面可能會發熱、發燙，請勿用手觸摸，並請檢查系統是否散熱不良。
- 在安裝或移除周邊產品時請先關閉電源。
- 電源供應器如果發生損壞，切勿自行修理，請交由授權經銷商處理。
- 產品的機殼、鐵片大部份都經過防割傷處理，但是您仍必須注意避免被某些細部鐵片尖端及邊緣割傷，拆裝機殼時最好能夠戴上手套。

當你有一陣子不使用產品時，休假或是颱風天，請關閉電源之後將電源線拔掉。

限用物質含有情況標示聲明書
Declaration of the Presence Condition of the Restricted Substances Marking

設備名稱：戶外型無線基地台 Equipment Name			型號 (型式) : OAP101 Type Designation (Type)			
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr^{+6})	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
電路板組件 PCBA	—	○	○	○	○	○
組合線 Cable ass'y	—	○	○	○	○	○
天線 Antenna	○	○	○	○	○	○
機殼 Chassis	○	○	○	○	○	○

備　考 1.	" 超出 0.1 wt %" 及 " 超出 0.01 wt %" 係指限用物質之百分比含量超出百分比含量基準值。
Note 1:	"Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.
備　考 2.	" ○ " 係指該項限用物質之百分比含量未超出百分比含量基準值。
Note 2:	" ○ " indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.
備　考 3.	" — " 係指該項限用物質為排除項目。
Note 3:	The " — " indicates that the restricted substance corresponds to the exemption.

Warnings and Cautionary Messages

Warning: This product does not contain any serviceable user parts.
Warning: Installation and removal of the unit must be carried out by qualified personnel only.

Caution: Wear an anti-static wrist strap or take other suitable measures to prevent electrostatic discharge when handling this equipment.
Caution: Do not plug a phone jack connector in the RJ-45 port. This may damage this device.
Caution: Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Hardware Specifications

AP Chassis

Size (LxWxH)	293.4 x 283.4 x 71 mm (11.55 x 11.16 x 2.80 in.)
Weight	1725 g (3.80 lb)
Waterproof Rating	IP66 and IP68
Temperature	Operating: -40° C to 60° C (-40° F to 140° F) Storage: -40° C to 70° C (-40° F to 158° F)
Humidity	Operating: 5% to 95% (non-condensing)

Network Interfaces

Ports	Uplink(PoE) RJ-45: 2.5GBASE-T, PoE PD LAN1 RJ-45: 1000BASE-T
2.4 GHz Radio	IEEE 802.11b/g/n/ax
5 GHz Radio	IEEE 802.11a/ac/n/ax
6 GHz Radio	IEEE 802.11a/ac/n/ax (OAP101-6E (T) only)
Bluetooth Radio	IEEE 802.15.1
Radio Frequencies	US and TW: 2.4–2.4835 GHz 5.15–5.85 GHz 5.925-6.425 GHz (OAP101-6E (T) only) 6.525-6.875 GHz (OAP101-6E (T) only) EU: 2.4–2.4835 GHz 5.47–5.725 GHz Japan: 2.4–2.4835 GHz 5.47–5.730 GHz

Power Specifications

PoE Input Power	25.5 W max 802.3at-compliant
DC Power	DC Input: 48 VDC, 0.5 A

Regulatory Compliances

Radio	EN 300 328 V2.2.2 (2.4G/BT-LE) EN 301 893 V2.1.1 (5G) EN 303 413 V1.1.1 (GPS) EN 50385 / EN 62311: 2017 (MPE) 47 CFR FCC Part 15.247 47 CFR FCC Part 15.407 MIC Certification Rule, Article 2 Paragraph 1 Item 19 and 19-3 (OAP101 (T) only) MIC Terminal Equipment Design Certification, Articles 3, 4, 6, 9, and 34 (OAP101 (T) only) NCC LP002 (OAP101 (T) only)
Emissions	EN 301 489-1 V2.1.1 (2017-02) EN 301 489-17 V3.1.1 (2017-02) EN 55032:2015 47 CFR FCC Rules and Regulations Part 15 Subpart B, Class B Digital Device VCCI CISPR 32:2016 Class B ITE (OAP101 (T) only) BSMI CNS 15936 (OAP101 (T) only)
Safety	EN 62368-1: 2014 + A11: 2017 EN 60950-22: 2017 IEC 62368-1: 2014 (Second Edition) IEC 60529: 1989+AMD1: 1999+ AMD2: 2013CSV (IP68) BSMI CNS 15598-1 (OAP101 (T) only)

Quick Start Guide

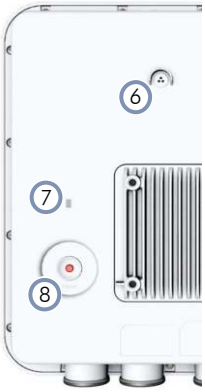
Outdoor Access Point

OAP101 (P)

Package Contents

1. OAP101 (P) access point
2. Mounting bracket and 4 x M6 screws
3. DC terminal plug
4. 3 x Cable glands
5. 2 x Steel-band clamps for pole mount (2.5 inch diameter max.)
6. Screw kit—4 screws and 4 plugs
7. QR code card

Overview



1. Grounding point
2. DC In port: 48 VDC
3. Uplink (PoE) port: RJ-45 2.5GBASE-T connection to 802.3at PoE
4. LAN port: 1 Gbps LAN connection
5. Console port
6. Moisture protective vent
7. Power/Status LED:
   - Yellow green: On (power OK), Blinking (boot up)
   - Blue: On (cloud managed)
   - Purple: Blinking (uplink activity in cloud managed mode)
   - Orange: Blinking (uplink activity in stand-alone mode)
8. Restart/Reset button:
   - A quick press restarts the system.
   - Press and hold for 5 seconds resets to factory defaults.

Installation

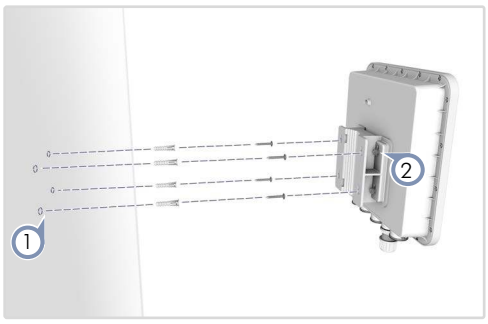
Warning: For a safe and reliable installation, use only the accessories and screws provided with the device. Use of other accessories and screws could result in damage to the unit. Any damages incurred by using unapproved accessories are not covered by the warranty.

Warning: To ensure compliance with IP66 and IP68 standards, maintain a cap or a cable gland on all ports.

Note: The drawings in this document are for illustration only and may not match your particular model.

1 Mount the Device

a. Mounting on a Wall



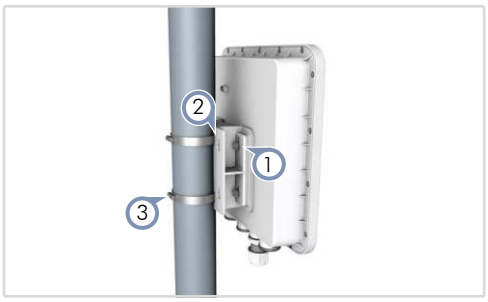
1. At the installation location on the wall, use the mounting bracket to mark four holes for the wall plugs and screws. The bracket must be installed with the marking “UP” at the top.

   Drill four holes for the wall plugs, and then insert the plugs and tap them flush with the wall surface.

   Note: Drill 2.5 mm (±0.2 mm) holes for M3 self-tapping screws, or 4.5 mm (±0.2 mm) holes for nylon wall plugs.

2. Use the included M6 screws to attach the mounting bracket to the device.
3. With its ports facing down, slide the device down onto the pre-installed screws until it snaps into its secured position. Do not let go of the device until you confirm that it is secure.

b. Mounting on a Pole



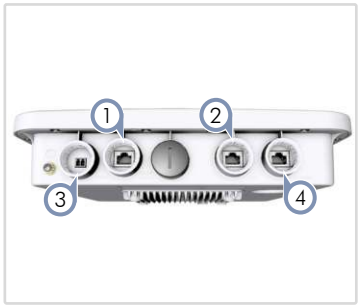
1. Use the included M6 screws to attach the mounting bracket to the device.
2. Feed the two steel-band clamps through the pole-mount bracket mounting points.
3. Fasten the steel-band clamps around the pole to secure the AP to the pole.

2 Ground the Device

1. Ground the device by connecting a ground wire to the grounding point on the device and to nearby good earth.

3 Connect Cables

a. Connect Ethernet Cables



Note: Port covers and cable glands should be tightened to a torque of 10 kgf.cm.

1. Connect Category 5e or better cable to the Uplink (PoE In) 2.5GBASE-T RJ-45 port. When connected to a PoE source, the Uplink (PoE In) port connection provides power to the unit.
2. (Optional) Connect a local LAN switch or computers to the LAN 1000BASE-T RJ-45 port.

b. (Optional) Connect DC Power

3. Wire the included DC terminal plug to a 48 VDC, 0.5 A source to provide power to the device. Follow the wiring scheme shown on the panel with the negative pole (-) on the left and the positive pole (+) on the right.

c. (Optional) Management Connection

4. Connect an RJ-45 to DB9 straight-through console cable and then configure the serial connection: 115200 bps, 8 characters, no parity, one stop bit, 8 data bits, and no flow control.

4 Check AP LED

1. When operating normally, the Power/Status LED should be on yellow green. Blinking indicates the device is booting up.

5 Connect to Plume Cloud

The AP can be connected to Plume Cloud via the Plume mobile app and the OAP101 (P) BLE function, or manually by adding the NODE_ID (the OAP101 (P)'s serial number) into your Plume Cloud website when the AP is in the Plume Cloud inventory.

Safety and Regulatory Information

FCC Interference Statement

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.

For product available in the USA/Canada market, only channel 1–11 can be operated. Selection of other channels is not possible.

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft.

Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 59 cm between the radiator and your body.

1. Installation personnel

This product is designed for specific applications and should be installed by qualified personnel who have knowledge of RF and its related regulations. A general user shall not attempt to install or modify the equipment configuration.

2. Installation location

To meet regulatory RF exposure requirements, this product shall be installed at a location where, during normal operations, the radiating antenna is at least 59 cm away from any nearby persons.

3. External antenna

Use only the antennas which have been approved by the applicant. Using non-approved antenna(s) is prohibited and may produce unwanted spurious or excessive RF transmitting power which may lead to a violation of FCC limits.

4. Installation procedure

Please refer to this equipment's user manual for the procedure details.

FCC Warning: The installation position must be carefully selected so that the final output power does not exceed the limit set forth in relevant regulations. Violation of output power regulations could lead to serious federal penalties.

CE Statement

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

All operational modes:

2.4 GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ax (HE20), 802.11ax (HE40)

5 GHz: 802.11a, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ac (VHT80), 802.11ax (HE20), 802.11ax (HE40), 802.11ax (HE80), 802.11ax (HE160)

BLE 2.4 GHz: 802.15.1

The frequency and maximum transmitted power limit in EU are listed as below:

2412-2472 MHz: 20 dBm
5470-5725 MHz: 30 dBm

AT	BE	BG	CH	CY	CZ
DE	DK	EE	EL	ES	FI
FR	HR	HU	IE	IS	IT
LI	LT	LU	LV	MT	NL
NO	PL	PT	RO	SE	SI
SK	TR	UK			

The abbreviations of the countries, as prescribed in above table, where any restrictions on putting into service or any requirements for authorization of use exist.

CE Mark Declaration of Conformance for EMI and Safety (EEC)

This information technology equipment is in compliance with the Directive 2014/53/EU and Directive 2014/35/EU.

The Declaration of Conformity (DoC) can be obtained from www.edge-core.com -> support -> download.

Japan - VCCI Statement

この装置は、クラスB機器です。この装置は、住宅環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。 VCCI－B

NCC Statement (Taiwan)

NCC 警語

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受

合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。 應避免影響附近雷達系統之操作。

MPE

本產品電磁波曝露量 (MPE) 標準值 1mW/cm2，送測產品實測值為 0.12152 mW/cm2，建議使用時至少距離人體 51 cm。

BSMI (Taiwan)

電氣方面的安全性

- 為避免可能的電擊造成嚴重損害，搬動產品之前，請先將產品電源線暫時從電源插座中拔掉。
- 當您要加入硬體裝置到系統中或者要移除系統中的硬體裝置時，請務必先連接該裝置的訊號線，然後再連接電源線。可能的話，在安裝硬體裝置之前先拔掉產品的電源供應器電源線。
- 當您要從主機板連接或拔除任何的訊號線之前，請確定所有電源線已事先拔掉。
- 請確定電源供應器的電壓設定已調到本國 / 本區域所使用的電壓標準值。若您不確定您所屬區域的供應電壓值為何，那麼請就近詢問當地的電力公司人員。
- 如果電源供應器已損壞，請不要嘗試自行修復。請將之交給專業技術服務人員或經銷商來處理。

操作方面的安全性

- 在使用產品之前，請確定所有的排線、電源線都已正確地連接好。若您發現有重大的瑕疵，請盡速連絡您的經銷商。
- 為避免發生電氣短路情形，請務必將所有沒用到的螺絲、迴紋針及其他零件收好，不要遺留在主機板上或產品主機中。
- 灰塵、溼氣以及劇烈的溫度變化都會影響主機板的使用壽命，因此請盡量避免放置在這些地方。
- 請勿將產品主機放置在容易搖晃的地方。
- 若在本產品的使用上有任何的技術性問題，請和經過檢定或有經驗的技術人員聯絡。

使用注意事項

- 在您開始操作本系統之前，請務必詳閱以下注意事項，以避免因為人為的疏失造成系統損傷甚至人體本身的安全。
- 使用前，請檢查產品各部份組件是否正常，以及電源線是否有任破損，或是連接不正確的情形發生。
- 如果有任何破損情形，請盡速與您的授權經銷商連絡，更換良好的線路。
- 產品放置的位置請遠離灰塵過多，溫度過高，太陽直射的地方。
- 保持機器在乾燥的環境下使用，雨水、溼氣、液體等含有礦物質將會腐蝕電子線路。
- 使用時，請務必保持周遭散熱空間，以利散熱。
- 使用前，請檢查各項周邊設備是否都已經連接妥當再開機。
- 避免邊吃東西邊使用，以免污染機件造成故障。
- 請避免讓紙張碎片、螺絲及線頭等小東西靠近產品之連接器、插槽、孔位等處，避免短路及接觸不良等情況發生。
- 請勿將任何物品塞入產品內，以避免引起機件短路或電路損毀。
- 產品開機一段時間之後，散熱片及部份IC表面可能會發熱、發燙，請勿用手觸摸，並請檢查系統是否散熱不良。
- 在安裝或移除周邊產品時請先關閉電源。
- 電源供應器如果發生損壞，切勿自行修理，請交由授權經銷商處理。
- 產品的機殼、鐵片大部份都經過防割傷處理，但是您仍必須注意避免被某些細部鐵片尖端及邊緣割傷，拆裝機殼時最好能夠戴上手套。

當你有一陣子不使用產品時，休假或是颱風天，請關閉電源之後將電源線拔掉。

限用物質含有情況標示聲明書
Declaration of the Presence Condition of the Restricted Substances Marking

設備名稱：戶外型無線基地台 Equipment Name			型號 (型式) : OAP101 Type Designation (Type)			
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr^{+6})	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
電路板組件 PCBA	—	○	○	○	○	○
組合線 Cable ass'y	—	○	○	○	○	○
天線 Antenna	○	○	○	○	○	○
機殼 Chassis	○	○	○	○	○	○

備　考 1.	" 超出 0.1 wt %" 及 " 超出 0.01 wt %" 係指限用物質之百分比含量超出百分比含量基準值。
Note 1:	"Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.
備　考 2.	" ○ " 係指該項限用物質之百分比含量未超出百分比含量基準值。
Note 2:	" ○ " indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.
備　考 3.	" — " 係指該項限用物質為排除項目。
Note 3:	The " — " indicates that the restricted substance corresponds to the exemption.

Warnings and Cautionary Messages

Warning: This product does not contain any serviceable user parts.
Warning: Installation and removal of the unit must be carried out by qualified personnel only.

Caution: Wear an anti-static wrist strap or take other suitable measures to prevent electrostatic discharge when handling this equipment.
Caution: Do not plug a phone jack connector in the RJ-45 port. This may damage this device.
Caution: Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Hardware Specifications

AP Chassis

Size (LxWxH)	293.4 x 283.4 x 71 mm (11.55 x 11.16 x 2.80 in.)
Weight	1725 g (3.80 lb)
Waterproof Rating	IP66 and IP68
Temperature	Operating: -40° C to 60° C (-40° F to 140° F) Storage: -40° C to 70° C (-40° F to 158° F)
Humidity	Operating: 5% to 95% (non-condensing)

Network Interfaces

Ports	Uplink(PoE) RJ-45: 2.5GBASE-T, PoE PD LAN1 RJ-45: 1000BASE-T
2.4 GHz Radio	IEEE 802.11b/g/n/ax
5 GHz Radio	IEEE 802.11a/ac/n/ax
Bluetooth Radio	IEEE 802.15.1
Radio Frequencies	US and TW: 2.4–2.4835 GHz 5.15–5.85 GHz EU: 2.4–2.4835 GHz 5.47–5.725 GHz Japan: 2.4–2.4835 GHz 5.47–5.730 GHz

Power Specifications

PoE Input Power	25.5 W max 802.3at-compliant
DC Power	DC Input: 48 VDC, 0.5 A

Regulatory Compliances

Radio	EN 300 328 V2.2.2 (2.4G/BT-LE) EN 301 893 V2.1.1 (5G) EN 303 413 V1.1.1 (GPS) EN 50385 / EN 62311: 2017 (MPE) 47 CFR FCC Part 15.247 47 CFR FCC Part 15.407 MIC Certification Rule, Article 2 Paragraph 1 Item 19 and 19-3 MIC Terminal Equipment Design Certification, Articles 3, 4, 6, 9, and 34 NCC LP002
Emissions	EN 301 489-1 V2.1.1 (2017-02) EN 301 489-17 V3.1.1 (2017-02) EN 55032:2015 47 CFR FCC Rules and Regulations Part 15 Subpart B, Class B Digital Device VCCI CISPR 32:2016 Class B ITE BSMI CNS 15936
Safety	EN 62368-1: 2014 + A11: 2017 EN 60950-22: 2017 IEC 62368-1: 2014 (Second Edition) IEC 60529: 1989+AMD1: 1999+ AMD2: 2013CSV (IP68) BSMI CNS 15598-1

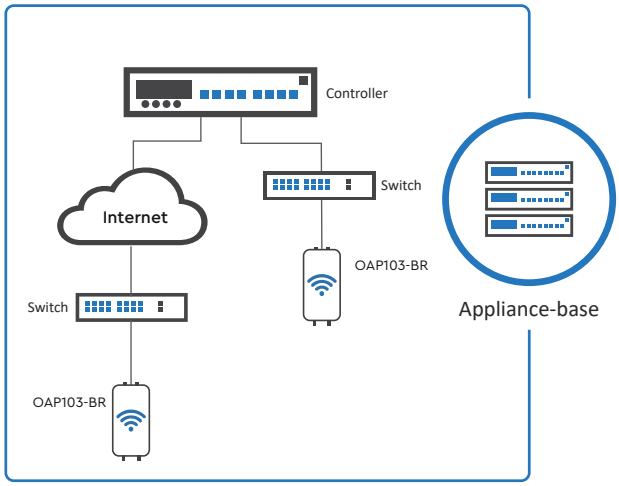
OAP103-BR

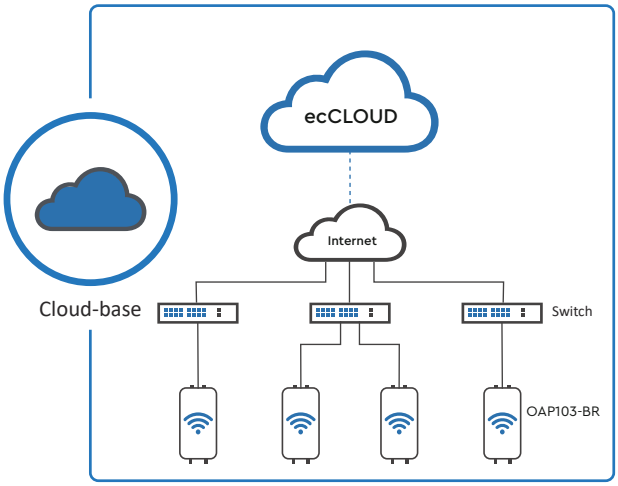
OUTDOOR WI-FI 6 ACCESS POINT

INTRODUCTION

OAP103-BR is an enterprise-grade, concurrent dual-band Wi-Fi 6 outdoor access point. OAP103-BR supports 5G 4 x 4 : 4 uplink and downlink MU-MIMO between the AP and multiple clients, with up to 2.9 Gbps aggregated data rate.

OAP103-BR can be operated as standalone mode or managed by Edgecore ecCLOUD and EWS-Series controller.





HIGHLIGHTS

- Concurrent Dual-Band 2.4GHz & 5GHz
- 802.11ax 4x4:4 UL MU-MIMO supporting up to 2.9 Gbps data rate
- Support up to 32 ESSIDs.
- Enterprise-Grade Wireless Security
- 802.3at Power over Ethernet (PoE)

SPECIFICATIONS

PHYSICAL	
Power	• PoE: 802.3at compliant
Dimensions	• 45.0 cm (L) x 23.0 cm (W) x 7 cm (H)
Weight	• 2.10 kg (4.63 lbs)
Interfaces	• Uplink: 1 x 10/100/1000/2.5GBase-T Ethernet, Auto MDIX, RJ-45 with 802.3at PoE • LAN: 1 x 10/100/1000/2.5GBase-T Ethernet, Auto MDIX, RJ-45
LED Indicator	• Power / System / Uplink / LAN / 2.4G / 5G
Environmental Conditions	• Operating Temperature: -20°C (-4°F) to 50°C (122°F) • Humidity: 10% to 95% non-condensing • IP68 Rating
Power Consumption	• 25W max*2
Antenna	• Type: Omni directional antenna (2.4 GHz & 5 GHz) • Gain: 5 dBi (2.4 GHz), 6 dBi (5 GHz)
Mounting	• Pole mount hose clamp, wall, ceiling
Protective Vent	
WI-FI	
Standards	• 802.11a/b/g/n/ac/ax • Concurrent dual-band 2.4 GHz & 5 GHz
Supported Data Rates	• 802.11b: 1, 2, 5.5, 11 Mbps • 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps • 802.11n: 6.5 –300 Mbps (20 / 40 MHz) • 802.11ac: 6.5 –1733 Mbps (20 / 40 / 80 MHz) • 802.11ax: 3.6 –574 Mbps (2.4 GHz, 20 / 40 MHz) • 802.11ax: 3.6 –2400 Mbps (5 GHz, 20 / 40 / 80 MHz)
Radio Chains	• 2.4 GHz: 2 x 2 • 5 GHz: 4 x 4
Spatial Streams	• 2.4 GHz: 2; MU-MIMO support • 5 GHz: 4; MU-MIMO support
Aggregate Conducted Transmit Power*3	• 2.4 GHz: Up to 23dBm*4 • 5 GHz: Up to 26dBm*4
Channelization	• 2.4 GHz: 20 / 40 MHz • 5 GHz: 20 / 40 / 80Mhz
Frequency Range	• 2.400 –2.483 GHz • 5.150 –5.850 GHz
Operating Channels	• 2.4 GHz: 1 –11 (US), 1 –13 (Europe) • 5 GHz*5: 36 –165 (US), 36 –140 (Europe)
ESSIDs	• Up to 16 per radio (32 total)
Certifications	• ANATEL, WIFI Alliance (Sub-category: Enterprise/Service Provider Access Point, Switch/Controller or Router)
PERFORMANCE	
Physical Data Rate	• Up to 574 Mbps (2.4 GHz) • Up to 2,400 Mbps (5 GHz)
Supported Clients	• 512 clients

*1: One USB port work at a time
*2: 22W when powered by DC
*3: RF output power aggregates across MIMO chains and doesn't contain antenna gain
*4: Maximum power is limited by local regulatory requirements
*5: Some channels are restricted by local regulatory requirements and certifications

FEATURES	
Wireless	• 802.11 k/r • Orthogonal Frequency Division Multiple Access (OFDMA) • Client Isolation • OpenMesh • Auto Channel Selection • Support up to 1024 QAM Modulation
Network	• Spanning Tree Protocol (STP) • Dynamic Host Configuration Protocol (DHCP) • 802.1q • Access Control List (ACL) • Network Address Translation (NAT) • Dynamic VLAN • Link Layer Discovery Protocol (LLDP)
Security	• WPA-Personal (AES) • WPA-Enterprise (AES) • WPA2-Personal (AES) • WPA2-Enterprise (AES) • WPA3-Personal (AES) • WPA3-Personal Transition (AES) • WPA3-Enterprise (AES) • WPA3-Enterprise transition (AES) • MAC Address Authentication • 802.1X • Support MPSK
Maintenance	• Network Time Protocol (NTP) • Standalone • Management by ecCLOUD • Management by EWS-Series Controller (Complete tunnel) • SSH • QR Code Onboarding • SNMP v2c • Remote Syslog
QoS	• RSSI Threshold (Optimal Client Filtering)
Others	• 16 VLANs • Static IP addressing • DHCP client for automatic network configuration • Bluetooth Low-Energy (BLE) • SSID propagation • Dynamic Power Level Adjustment • Operation in Mesh mode • Target Wake Time (TWT) • BSS Coloring

TEL: 886-3-5638888 FAX: 886-3-6686111
1 Creation Rd. II, Hsinchu Science Park, Taiwan 30077
sales@edge-core.com
www.edge-core.com

PROCURAÇÃO

A empresa **SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA**, Inscrita no CNPJ sob o n° **44.122.701/0001-79**, sediada na Setor SRTVS Qd 701 bloco O - Sala 122, Multiempresarial, Asa Sul, Brasília-DF – Cep: 70.340-000, por intermédio de seu representante legal, Roselane Gonzalez do Nascimento Almeida, portadora da CNH sob nº 01375790968, CPF sob nº 078.944.777-02, nomeia e constitui sua bastante procuradora , **Paola Derriaux Chastagnier,** inscrita no CPF sob o número **093.870.557-10**, residente e domiciliado na cidade de Nova Friburgo, Rio de Janeiro, doravante denominada OUTORGADA, para representar a OUTORGANTE como se presente fosse, em qualquer instância, em portais de licitações, certames licitatórios, pregões e congêneres, de qualquer entidade de direito público ou privado, incluindo autarquias, sociedades de economia mista, fundações, empresas públicas e agências governamentais, podendo também, assinar, acordar, declarar, transigir, formular ofertas, lances e propostas verbais, assinar documentos, assinar comerciais, desistir verbalmente de formular ofertas, lances e propostas verbais, negociar redução de preços, recorrer, impugnar, esclarecer, tomar qualquer decisão durante todas as fases da licitação ou pregão, inclusive apresentar a declaração de que a OUTORGANTE licitante cumpre os requisitos de habilitação, apresentar envelopes de propostas de preços e documentação de habilitação, desistir expressamente da intenção de interpor recurso administrativo ao final da sessão, assinar a ata da sessão, prestar todos os esclarecimentos solicitados pelo pregoeiro ou pela comissão de licitação , praticando, enfim, todos os atos pertinentes permitidos em Direito, por mais especiais que seja, em nome da OUTORGANTE, em todo o território Nacional, o que tudo dará por firme, e valioso, a bem deste mandato.

A presente terá validade até 31 de dezembro de 2025.

Brasília, 03 de julho de 2025.

ROSELANE GONZALEZ DO NASCIMENTO ALMEIDA:07894477702

Assinado de forma digital por ROSELANE GONZALEZ DO NASCIMENTO ALMEIDA:07894477702
Dados: 2025.07.03 12:10:28 -03'00'

ROSELANE GONZALEZ DO NASCIMENTO ALMEIDA

CPF 078.944.777-02

PROPOSTA COMERCIAL

Ao Estimado Órgão: PREFEITURA MUNICIPAL DE CACERES - MT

UASG: 989047

Processo nº: Nº N° 90015/2025

Pregão Eletrônico n°: Processo Administrativo n° 29/2025

Objeto: Registro de Preço para futura e eventual contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres, conforme condições e exigências estabelecidas neste instrumento

Sobre a Sh7:

A Sh7 é uma empresa brasileira de cibersegurança com DNA em telecomunicações e um propósito claro: proteger governos, instituições e empresas contra ameaças digitais, promovendo soberania e segurança da informação em todo o território nacional.

Soluções de Cibersegurança Sh7:

- **SOC** – Security Operations Center
  Monitoramento contínuo e resposta a incidentes em tempo real.
- **NOC** – Network Operations Center
  Sustentação de infraestrutura com foco em disponibilidade e performance.
- **NDR** – Network Detection and Response
  Detecção e resposta a ameaças com base em análise comportamental da rede.
- **ZTNA** – Zero Trust Network Access
  Controle de acesso seguro baseado no modelo de confiança zero.
- **CTI** – Cyber Threat Intelligence
  Inteligência contra ameaças em surface, deep e under web.
- **Gestão de Credenciais**
  Controle e proteção de acessos privilegiados e sensíveis.
- **Reputação de Terceiros**
  Avaliação contínua da postura de segurança de parceiros e fornecedores.
- **LGPD** – Conformidade com a Lei Geral de Proteção de Dados
  Soluções técnicas e administrativas para adequação legal e governança de dados.
- **Blindagem Digital com Netsensor**
  Tornamos a rede invisível para atacantes, protegendo contra ameaças desconhecidas (zero day).

Parceiros:

APRESENTAÇÃO DA PROPOSTA

Razão Social: SH7 Proteção e Inteligência Cibernética Ltda
CNPJ: 44.122.701/0001-79 **Inscrição Estadual**: 0809456400111
Endereço: Setor SRTVS Qd 701 bloco O - Sala 122, Multiempresarial, Asa Sul, Brasília-DF – Cep: 70.340-000
Telefone: 11 97825-8402 **e-mail:** paola@tycheconsultoria.com.br

Item	Especificação	Marca	Modelo	Unidade	Qtd	Vlr Unit (R$)	Vlr Total Anual R$
1	Serviço de provimento de solução de Firewall de Nova Geração e SD- WAN (Alta Disponibilidade)	Blockbit	BBX 40 BBX 80 BBX 140 BBX 200- Cluster	unid	2076	564,99	1.172.919,24
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Netsensor	Magic	unid	24	8.999,99	215.999,76
3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso	Rede EXS Bertasso	ASN EXS ASN NItro	Unid	24	3.399,99	81.599,76
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Bertasso	n/a	link	2052	214,99	441.159,48
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	EXS	n/a	link	2052	164,66	337.882,32
6	Implantação da Solução	n/a	n/a	Ativação	1	269.999,99	269.999,99
7	Capacitação especializada da equipe com emissão de certificação.	n/a	n/a	Turma	1	8.416,67	8.416,67
8	Consultoria Política de Segurança	n/a	n/a	Serviço	1	35.666,67	35.666,67

Valor negociado total: R$ 2.563.643,8900

O preço total desta proposta é de R$ 2.563.643,8900 (dois milhões quinhentos e sessenta e três mil e seiscentos e quarenta e três reais e oitenta e nove centavos). Foi o total de descontos que ofertamos em decorrência da disputa. Portanto, não há mais descontos possíveis para estes itens.

Data: 03/07/2025
Validade da proposta: 90 (noventa) dias, a contar da data de sua apresentação.

DECLARAMOS QUE ESTAMOS DE ACORDO COM TODAS AS CONDIÇÕES ESTABELECIDAS NO EDITAL E SEUS ANEXOS.

Estão incluídos nos preços todos os custos da mão de obra, encargos sociais, trabalhistas e previdenciários, uniformes, tributos, taxas, contribuições, insumos, equipamentos e quaisquer outros encargos que incidam sobre a prestação do serviço a ser executado.

Declaramos, que estamos cientes da responsabilidade de manter nossos dados cadastrais atualizados junto ao Contratante, bem como se compromete a informar qualquer alteração que venha a ser realizada.

PAOLA DERRIAUX CHASTAGNIER:09387055710

Assinado de forma digital por PAOLA DERRIAUX CHASTAGNIER:09387055710
Dados: 2025.07.03 12:15:58 -03'00'

Paola Derriaux Chastagnier
Diretora de Licitações - CPF: 093.870.557-10

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Declaração

Declaramos para os fins exigidos na legislação, conforme documentação registrada no SICAF, que a situação do fornecedor no momento é a seguinte:

Dados do Fornecedor

CNPJ:	**44.122.701/0001-79**
Razão Social:	**SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA**
Nome Fantasia:	**G2Z**
Situação do Fornecedor:	**Credenciado** Data de Vencimento do Cadastro: **21/01/2026**
Natureza Jurídica:	**SOCIEDADE EMPRESÁRIA LIMITADA**
MEI:	**Não**
Porte da Empresa:	**Micro Empresa**

Ocorrências e Impedimentos

Ocorrência:	**Nada Consta**
Impedimento de Licitar:	**Nada Consta**

Níveis cadastrados:

Documento(s) assinalado(s) com "*" está(ão) com prazo(s) vencido(s).

Automática: a certidão foi obtida através de integração direta com o sistema emissor. Manual: a certidão foi inserida manualmente pelo fornecedor.

I - Credenciamento

II - Habilitação Juridica

III - Regularidade Fiscal e Trabalhista Federal

Receita Federal e PGFN		Validade:	**12/10/2025**	**Automática**
FGTS		Validade:	**25/07/2025**	**Automática**
Trabalhista	**(http://www.tst.jus.br/certidao)**	Validade:	**30/12/2025**	**Automática**

IV - Regularidade Fiscal Estadual/Distrital e Municipal

Receita Estadual/Distrital	Validade:	**27/07/2025**	
Receita Municipal	(Isento)		

VI - Qualificação Econômico-Financeira

Validade: **30/06/2026**

Esta declaração é uma simples consulta e não tem efeito legal

CPF: 093.XXX.XXX-10 Nome: PAOLA DERRIAUX CHASTAGNIER

Ass: _____

Comprovante de Pagamento Pix

Valor: R$ 7.460,00

Realizado em: 11/06/2025 - 14:05:17

Solicitante: ROSELANE GONZALEZ DO NASCIMENT

Cooperativa e conta origem: 3953/36087-6

Nome do destinatário: G2Z

CNPJ do destinatário: 44.122.701/0001-79

Instituição do destinatário: NU PAGAMENTOS - IP

Agência e conta do destinatário: 1 / 160626821-5

Nome do pagador: Rede Exs Telecomunicacoes Ltda

CNPJ do pagador: 23.935.457/0001-93

Instituição do pagador: BANCO COOPERATIVO SICREDI S.A.

ID da transação: E10736214202506111705O1kTrODMo1k

Autenticação Eletrônica: E107.3621.4202.5061.1170.501k.TrOD.Mo1k

Número de Controle: 12532167101

Emitido em: 03/07/2025 - 17:19:43

* A transação acima foi realizada no nosso Aplicativo Sicredi conforme as condições especificadas neste comprovante.
* Os dados digitados são de responsabilidade do usuário.
Serviços por telefone 3003 4770 (Capitais e Regiões Metropolitanas) / 0800 724 4770 (Demais Regiões)
SAC 0800 724 7220 / Ouvidoria 0800 646 25 19

Comprovante de Pagamento Pix

Valor: R$ 20.000,00

Realizado em: 03/07/2025 - 18:15:16

Solicitante: ROSELANE GONZALEZ DO NASCIMENT

Cooperativa e conta origem: 3953/36087-6

Nome do destinatário: G2Z

CNPJ do destinatário: 44.122.701/0001-79

Instituição do destinatário: NU PAGAMENTOS - IP

Agência e conta do destinatário: 1 / 160626821-5

Nome do pagador: Rede Exs Telecomunicacoes Ltda

CNPJ do pagador: 23.935.457/0001-93

Instituição do pagador: BANCO COOPERATIVO SICREDI S.A.

ID da transação: E10736214202507032114 32J8CBvC6q3

Autenticação Eletrônica: E107.3621.4202.5070.3211.432J.8CBv.C6q3

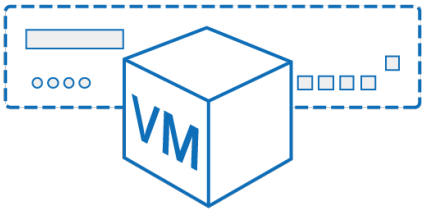
Número de Controle: 12731695532

Emitido em: 03/07/2025 - 18:15:19

* A transação acima foi realizada no nosso Aplicativo Sicredi conforme as condições especificadas neste comprovante.
* Os dados digitados são de responsabilidade do usuário.
Serviços por telefone 3003 4770 (Capitais e Regiões Metropolitanas) / 0800 724 4770 (Demais Regiões)
SAC 0800 724 7220 / Ouvidoria 0800 646 25 19

VEWS-Series

VIRTUAL WIRELESS LAN CONTROLLER

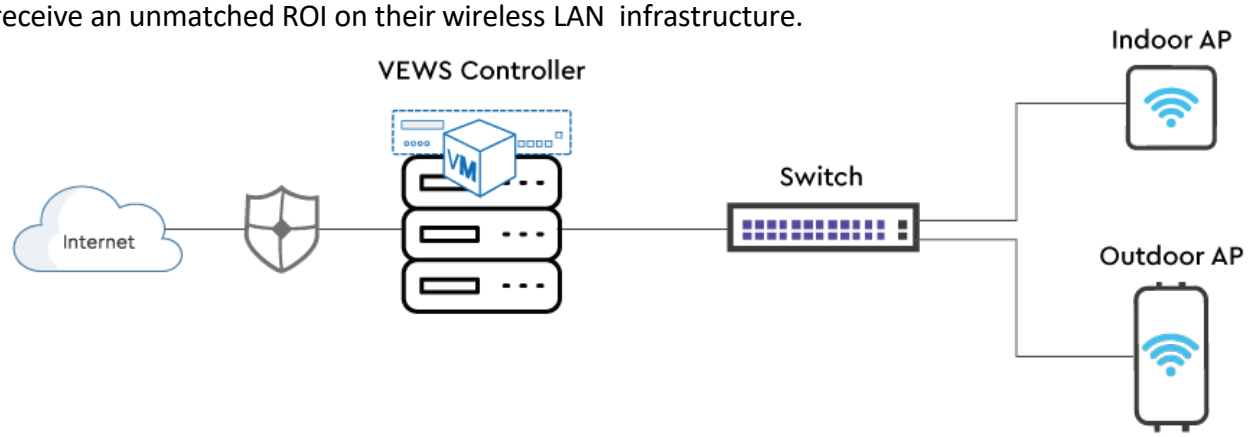


INTRODUCTION

The Edgecore VEWS Virtual Wireless LAN Controller allows to run on any VMware infruscture such as servers, personal computers, and cloud computing resource to provide much-needed hardware independence while offering the same functionality as the physical controller. With AP management, user authentication, policy assignment, traffic shaping, firewall features, and much more all packaged into a single windowpane, the VEWS-series Controller provides network administrators with a reliable, easy-to-use, and centralized management console for an entire organization's wireless network infrastructure, including Edgecore Access Points and Switches and the communication among Controllers, Switches and Access Points are encrypted.

The VEWS-series Controller can be deployed and configured easily, even non-wireless savvy users. For example, automated AP discovery prevents network administrators from having to go through the hassle of individually adding and configuring each access point. Access points as well as connected Wi-Fi devices can then be monitored and managed from a centralized point, with extensive logging & reporting features to assist in troubleshooting and maintenance and it is compatible on VMware 6.7 version. Besides, VEWS-series Controller supports maps functionality allowing the administrator to view and monitor the wireless network coverage map.

For user management, the VEWS-series supports from 3,000 to 100,000 connected clients, according to different models. Moreover, as Wi-Fi-enabled handheld devices, such as smartphones and tablets, become ever so prevalent in our daily lives, businesses and network operators alike are faced with a mind-boggling dilemma – how to simultaneously address the needs of BYOD (Bring Your Own Device), manage Wi-Fi users, and maintain network service quality for mission-critical applications. The VEWS-series is designed exactly with these requirements in mind, and with a total cost of ownership that satisfies even the most price conscious, organizations are guaranteed to receive an unmatched ROI on their wireless LAN infrastructure.



FEATURES

SECURITY

Security is often one of the most important concerns when it comes to enterprise wireless networks. From the most basic need of preventing network access by unauthorized users to performing rogue AP detection and enforcing network isolation, the Edgecore VEWS-series Controller provides a complex set of features that prevent malicious activities in an organization's network.

For deployment flexibility, the Edgecore VEWS-series Controller supports user authentication via both the industry standard 802.1X as well as web-based captive portals. The highly customizable captive portals with integrated walled garden capability can be adapted to suit the needs of hotels, schools, and other public venues. For unregistered users without an account, guest access can be provided by simply entering an e-mail address, logging in with social media accounts, or purchasing a data plan through PayPal.

With various account generation methods, the Edgecore VEWS-series Controller is able to identify users and track user activities, ensuring network security in public Wi-Fi.

The Edgecore VEWS-series Controller also supports remote access via VPN, which is crucial for travelling businessmen. At the same time, site-to-site VPN establishes secure connections between corporate headquarters and branch offices.

USER SECURITY	
Authentication Types	• 802.1X • UAM (browser-based) • IP or MAC-based
Authentication Servers	• Local • On-Demand • Guest • RADIUS • LDAP • NT Domain • SIP • POP3
Customizable Captive Portal	• Yes
Customizable Wild Card Walled Garden	• Yes
User Blacklisting	• Yes

ACCOUNT GENERATION	
On-demand Account	• SMS registration • Purchase via PayPal • Hotel PMS integration • Selectable Billing Plans • Account Ticket Printer
Guest Wi-Fi Account	• Limitation by duration and volume • Configurable reactivation time • E-mail registration and activation
Social Media Login	• Yes

NETWORK SECURITY	
VPN	• Remote • Site-to-Site
Tunneling Protocols	• IPSec • PPTP
Network Isolation	• Intra-VLAN or Port • Inter-VLAN or Port
Rogue AP Detection	• Yes
Certificates	• Built-in Root CA

MOBILITY

The advent of the era of smartphones and tablets has opened a chasm between how the Internet is used and how organizations provide Internet connectivity. Wireless networks have transformed from a luxury to a necessity, in order to support devices that don't have legacy wired capability. Furthermore, additional features need to be provided in order to address the rapidly changing usage behavior.

The Edgecore VEWS-series Controller supports a variety of mobility features that aim to make enterprise Wi-Fi both easier to use and simpler to manage. For example, by supporting fast roaming, users on mobile devices can be on-the-go without worrying about interrupted connections. It is also not uncommon to see a single user with multiple handheld devices - with the Edgecore VEWS-series Controller all of the devices can login to Wi-Fi using the same username and password. Finally, mobile-optimized captive portals and ticket-printed QR code automatic login are both easy methods for a user to get online from their mobile device.

DEVICE MOBILITY	
Fast Roaming Between Access Points	• Yes
Cross Gateway Roaming	• Yes
WISPr Smart Client	• Yes
Mobile Device Recognition for Optimized Captive Portal	• Yes
Multiple Device Logins Per Account	• Yes
QR Code Automatic Login	• Yes
Device Plug-and-Play	• Yes

MANAGEMENT

In a wireless LAN, the Edgecore VEWS-series Controller is the central point of management for network administrators, whether it is monitoring current online users or troubleshooting network connectivity issues. The management console of the Edgecore VEWS-series Controller is a browser-based GUI that is simple and intuitive to operate. From this interface, network administrators can configure traffic shaping profiles, track previous network usage, perform system backup and restore, and much more.

From the user management perspective, one of the core benefits of the Edgecore VEWS-series Controller is its ability to enforce different traffic profiles based on both the location (Service Zone) of the user and the time of access. For example, the profiles applied during work hours can be different from that of during after-work hours. From bandwidth limitations to specific routing rules, network administrators gain fine-grained control over Wi-Fi users.

For access points, Edgecore VEWS-series Controller supports automatic discovery and provisioning, eliminating many repetitive and cumbersome tasks often faced during initial network deployment. Centralized AP configuration and monitoring also greatly reduces maintenance overhead for IT staff.

SYSTEM MANAGEMENT	
Browser-Based Configuration	• Yes
Administrator Accounts	• Multiple tiered access privileges • Monitor each admin's current accessed page • Local database and RADIUS authentication
System Time	• NTP synchronization • Manually configured
System Backup & Restore	• Yes
SNMP	• Yes; v2c
Network Utilities	• Yes; built-in packet capture

AP MANAGEMENT	
Automatic AP Discovery	• Yes
Automatic AP Provisioning	• Yes; template-based
AP Configuration Backup & Restore	• Yes
AP Firmware Batch Upgrade	• Yes
Tunneled AP Management	• Yes; both L2 & L3 APs
AP Load Balancing	• Yes
Automatic AP Firmware Upgrade	• Yes
Individual AP Information	• Associated Clients • Power & Channel • SNR report

INVENTORY MANAGEMENT	
AP Planning Type	• New Stock • Pre-configured • Configured-in-use • Not-to-use
AP Entry Preparation	• CSV file uploadable • Manual added

USER MANAGEMENT

User Policy Assignment	• Role-based • Time & location dependent
Bandwidth Limitation	• Yes
Traffic Classification / Remarking	• Yes; 802.1p / DSCP
Stateful Firewall	• Yes; each rule with individual enforcement schedules
Static Route Assignment	• Yes
Concurrent Session Limit	• Yes
IP Address Reassignment	• Allow clients to obtain different IP addresses after authentication

SERVICE

As wireless networks increasingly become the primary network used by organizations, it is crucial to take into consideration fundamental network services, such as DHCP, NAT, and routing. In addition to providing these functions, the Edgecore VEWS-series Controller also implements the concept of a "Service Zone", which essentially segments the controller into multiple virtual controllers, each with its own associated network services, user policies, authentication settings, etc.

On the reliability end, the Edgecore VEWS-series Controller supports WAN port failover, which helps businesses reduce the chance of network downtime and prevents lost productivity and revenue. Furthermore, load balancing between the WAN ports increases overall performance by alleviating congestion and distributing traffic between the two outgoing links.

Finally, the Edgecore VEWS-series Controller provides unique value- added capabilities, such as a direct integration with Micros Opera PMS that greatly simplifies the overhead of providing managed Wi-Fi in hotels.

NETWORK SERVICES

Redundancy (High Availability)	• N+1 with automatic synchronization
Internet Protocols Supported	• IPv4 • IPv6
DHCP Server / DHCP Relay	• Yes
Network Address Translation	• Yes
Built-in HTTP Proxy Server	• Yes
WAN Port Load Balancing	• Yes
Dynamic Routing	• Yes
Local DNS Records	• Yes
Hotel PMS Integration	• Oracle Hospitality OPERA
Integrated Billing & Accounting System	• Yes
Billing Quota Types	• By duration • By traffic volume

REPORTING

Whether it is real-time monitoring of network activity or tracking the usage of previous Wi-Fi users, network administrators need the appropriate tools at their disposal to increase efficiency and reduce workload. The Edgecore VEWS-series Controller have an extensive set of logging and reporting features that allow network administrators to easily find any information related to the wireless network.

The built-in system dashboard provides a quick overview of the current system status, along with graphical reports of network traffic and system performance. In addition, there is a simple interface for viewing online devices and their associated detailed statistics, including but not limited to the roles they belong to, enforced network policies, and packets transferred.

Alongside network monitoring, the Edgecore VEWS-series Controller also performs detailed logging of all network activity. For example, the User HTTP Web Log allows network administrators to track users who visited malicious websites, while the DHCP Lease Log can assist in troubleshooting clients who cannot receive an IP address. Lastly, the Configuration Change Log shows administrators which settings have been modified in the past, in case there are configuration errors that need to be reverted.

SYSTEM & NETWORK STATUS	
System Dashboard	• Yes
Dashboard Customization	• Yes
Graphical System Performance Reports	• Yes
Traffic Volume Reports	• Yes
System Process Monitor	• Yes
Online Device Monitoring	• Yes
Active Sessions List	• Yes
Configurable SYSLOG Severity	• Yes
SMTP (E-mail) Notifications	• Yes
Multiple Concurrent E-mail Notification Receivers	• Yes

NETWORK ACTIVITY LOGS	
System Log (SYSLOG)	• Yes
CAPWAP Log	• Yes
Configuration Change Log	• Yes; History View
RADIUS Server Log	• Yes
User Events Log	• Yes
User HTTP Web Log	• Yes
Firewall Log	• Yes
DHCP Server/Lease Log	• Yes
PMS Interface Log	• Yes
On-Demand Billing Report	• Yes
AP Status E-mail Notification	• Yes
Logging to External FTP	• Yes
Configurable Logs & Reporting Intervals	• Yes

VEWS MODELS

	VEWS5203	VEWS5204	VEWS5207	VEWS1000
Managed APs	Up to 300	Up to 1,000	Up to 3,000	Up to 10,000
Local Accounts	Up to 10,000	Up to 30,000	Up to 50,000	Up to 120,000
On-Demand Accounts	Up to 10,000	Up to 30,000	Up to 50,000	Up to 120,000
Max. Number of Online Users	3,000	10,000	30,000	100,000
Installation Hardware Requirement				
CPU	4 cores	8 cores	16 cores	40 cores
Memory	4 GB	8 GB	16 GB	32 GB
HDD	512 GB	512 GB	512 GB	512 GB

TEL: 886-3-5638888 FAX: 886-3-6686111
1, Creation Rd. III, Hsinchu Science Park, Taiwan 30077
sales@edge-core.com
www.edge-core.com

Wi-Fi 6 Access Point

Software Release 12.5.3

User Manual

www.edge-core.com

User Manual

Wi-Fi 6 Access Point

Cloud-Enabled Enterprise Access Points
EAP101
EAP102
EAP104
EAP104 (WL)
EAP111
OAP101

E032024-CS-R14

How to Use This Guide

This guide includes detailed information on Edgecore access point (AP) software, including how to operate and use the management functions of APs. To deploy APs effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all software features.

Who Should Read This Guide?

This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks) and the Internet Protocol (IP).

How This Guide is Organized

The organization of this guide is based on the AP's web management interface. An introduction and initial configuration information is also provided.

The guide includes these sections:

- Section I "Getting Started" — Includes an introduction to AP management and initial configuration settings.
- Section II "Web Configuration" — Includes all management options available through the web interface.
- Section III "Appendices" — Includes information on troubleshooting AP management access.

Related Documentation

This guide focuses on AP software configuration, it does not cover hardware installation of an AP. For specific information on how to install an AP, see the following guide:

Quick Start Guide

For all safety information and regulatory statements, see the following documents:

Quick Start Guide

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Revision History

This section summarizes the changes in each revision of this guide.

March 2024 Revision

This is the 14th revision of this guide. It is valid for software release v12.5.3 and includes the following changes:

- Minimum Signal Allowed setting for each SSID, see "Wireless Networks — General Settings" on page 69
- Added Device OS Blacklist, see "Wireless Networks — General Settings" on page 69

January 2024 Revision

This is the 13th revision of this guide. It is valid for software release v12.5.0 and includes the following changes:

- Added support for EAP111
- Added RADIUS NAS ID, see "Wireless Networks — Security Settings" on page 70
- Modified Minimum Signal Allowed default, see "Physical Radio Settings" on page 65
- Added OpenRoaming captive portal, see "OpenRoaming" on page 58
- Added OpenRoaming NAI Realm List Method/Authentication, see "OpenRoaming" on page 58
- Added Syslog Level, see "System Settings" on page 83

September 2023 Revision

This is the 12th revision of this guide. It is valid for software release v12.4.3 and includes the following changes:

- Added support for OAP101

- Added SSID isolation, see "Physical Radio Settings" on page 65
- Multiple PSK enhancement, see "Wireless Networks — Security Settings" on page 70

July 2023 Revision

This is the 11th revision of this guide. It is valid for software release v12.4.1 and includes the following changes:

- Added OpenRoaming, see "OpenRoaming" on page 58 and "Wireless Networks — OpenRoaming" on page 78
- Modified broadcast rate, see "Physical Radio Settings" on page 65
- Access Control List enhancement, see "Wireless Networks — Security Settings" on page 70
- Hostname enhancement, see "System Settings" on page 83
- Moved the language setting to the System page, see "System Settings" on page 83
- Firmware upgrade enhancement, see "Upgrading Firmware" on page 88
- Account username enhancement, see "User Accounts" on page 89

May 2023 Revision

This is the 10th revision of this guide. It is valid for software release v12.4.0 and includes the following changes:

- Added WAN port auto-detection to QR code Onboarding, see "QR Code Onboarding" on page 27
- Added automatic mesh AP configuration, see "Mesh AP Configuration" on page 30
- Removed Mark and Notrack from firewall rules, see "Firewall Rules" on page 51
- Modified Minimum Signal Allowed, see "Physical Radio Settings" on page 65
- Added RF Isolation, see "Physical Radio Settings" on page 65
- Modified Dynamic VLAN, see "Wireless Networks — Network Settings" on page 76
- Modified HotSpot 2.0 settings, see "Wireless Networks — Network Settings" on page 76
- Added Log Level, see "System Settings" on page 83

- Added SNMPv3 User, see "SNMP" on page 94
- Modified Diagnostics and added Speed Test, see "Diagnostics" on page 98

January 2023 Revision

This is the ninth revision of this guide. It is valid for software release v12.3.0 and includes the following changes:

- Updated QR code Onboarding, see "QR Code Onboarding" on page 27
- Updated wireless status, see "Wireless Status" on page 38
- Added support for dynamic PSK, see "Wireless Networks — Security Settings" on page 70
- Updated Hotspot 2.0 settings, see "Wireless Networks — Network Settings" on page 76
- Added CAPWAP Tunnel Interface to Ethernet Settings, see "Ethernet Settings" on page 46

November 2022 Revision

This is the eighth revision of this guide. It is valid for software release v12.2.0 and includes the following changes:

- Added Airtime Fairness, see "Physical Radio Settings" on page 65
- Modified the value range of BSS Coloring, see "Physical Radio Settings" on page 65
- Modified wireless security default, see "Wireless Networks — Security Settings" on page 70
- Added 802.11v, see "Wireless Networks — Security Settings" on page 70
- Added SNMP Trap, see "SNMP" on page 94
- Added BLE Scan, see "BLE" on page 97

November 2022 Revision

This is the seventh revision of this guide. It is valid for software release v12.1.0 and includes the following changes:

- Updated SNMP read/write community settings, see "SNMP" on page 94
- Added BLE radio Tx Power, see "BLE" on page 97
- Added Interference Detection, see "Physical Radio Settings" on page 65

- Added zero-touch provisioning information, see "Zero-Touch Provisioning" on page 20
- Modified the default value for Minimum Signal Allowed, see "Physical Radio Settings" on page 65
- Added 160MHz channel bandwidth option, see "Physical Radio Settings" on page 65
- Removed uCentral cloud option from the Setup Wizard.

July 2022 Revision

This is the sixth revision of this guide. It is valid for software release v12.0.0 and includes the following changes:

- Updated Setup Wizard for uCentral cloud, see "AP Setup Wizard" on page 22
- Added Proxy ARP, see "Wireless Networks — Network Settings" on page 76
- Added Multicast-to-Unicast Conversion, see "Wireless Networks — General Settings" on page 69
- Added Bandsteering, see "Physical Radio Settings" on page 65
- Added WPA3 Enterprise 192-bit and OWE security, see "Wireless Networks — Security Settings" on page 70
- Added multiple PSK keys, see "Wireless Networks — Security Settings" on page 70
- Added Short Guard Interval (SGI), see "Wireless Networks — Advanced Radio Settings" on page 79
- Added Multicast/Broadcast Rate, see "Physical Radio Settings" on page 65
- Added UPnP, see "LAN Settings" on page 49
- Added DHCP Snooping, see "DHCP Snooping" on page 61
- Added ARP Inspection, see "ARP Inspection" on page 62
- Added DHCP Relay, see "DHCP Relay" on page 63
- Added IPv6 for Internet access, see "IPv6 Settings" on page 46
- Added Hotspot 2.0, see "Wireless Networks — Network Settings" on page 76
- Added Device Discovery Tool, see "Device Discovery" on page 99

- Added Discovery Agent settings, see "Edgecore Networks Discovery Tool" on page 91
- Added Reset button and LED enable, see "System Settings" on page 83
- Added PoE Out setting, see "Ethernet Settings" on page 46
- Added caution on firmware upgrades in uCentral mode, see "Upgrading Firmware" on page 88

April 2022 Revision

This is the fifth revision of this guide. It is valid for software release v11.6.0 and includes the following changes:

- Added Client mode, see "Physical Radio Settings" on page 65
- Added Site Survey, see "Wireless Networks — General Settings" on page 69
- Added Custom LAN, see "LAN Settings" on page 49
- Added WME configuration, see "Physical Radio Settings" on page 65
- Added BSS Coloring, see "Physical Radio Settings" on page 65
- Added OFDMA, see "Physical Radio Settings" on page 65
- Added Target Wake Time, see "Physical Radio Settings" on page 65
- Added HTTPS captive portal, see "Captive Portal Settings" on page 56
- Added HTTPS certificate upload, see "Upload Certificate" on page 88

December 2021 Revision

This is the fourth revision of this guide. It is valid for software release v11.4.0 and includes the following changes:

- Updated QR code onboarding, see "QR Code Onboarding" on page 27
- Added mesh traffic graph to the dashboard, see "Traffic Graphs" on page 40
- Added MSP mode, see "System Settings" on page 83

November 2021 Revision

This is the third revision of this guide. It is valid for software release v11.3.1 and includes the following changes:

- Updated the Setup Wizard, see "AP Setup Wizard" on page 22
- Updated the Dashboard, see "Status Information" on page 33

- Added Smart Isolation, see "LAN Settings" on page 49
- Added Hotspot Settings, see "Hotspot Settings" on page 53
- Updated wireless network settings, see "Wireless Networks — Network Settings" on page 76
- Updated wireless open mesh settings, see "Wireless Networks — Open Mesh Settings" on page 78
- Added Telnet settings, see "Telnet" on page 91
- Added web server settings, see "Web Server" on page 91
- Added multicast DNS, see "Multicast DNS" on page 95
- Added firewall settings, see "Firewall Rules" on page 51
- Added a guest network, see "LAN Settings" on page 49

July 2021 Revision

This is the second revision of this guide. It is valid for software release v11.2.0 and includes the following changes:

- Added WPA3-Personal transition, WPA3-Enterprise, and WPA3-Enterprise transition. See "Wireless Networks — Security Settings" on page 70
- Support for IEEE 802.11 k/r, see "Wireless Networks — Security Settings" on page 70
- Added Minimum signal allowed (RSSI Threshold), see "Physical Radio Settings" on page 65
- Support for Open Mesh, see "Wireless Networks — Open Mesh Settings" on page 78
- SNMP v2 support, see "SNMP" on page 94
- Support for remote Syslog, see "Remote System Log Setup" on page 92
- Support for LLDP, see "LLDP" on page 96
- Support for management by an EWS-Series Controller, see "System Settings" on page 83

April 2021 Revision

This is the first revision of this guide. It is valid for software release v11.1.1.

Contents

Figures

Figures

Tables

Section I

Getting Started

This section provides an overview of the access point, and introduces some basic concepts about wireless networking. It also describes the basic settings required to access the management interface.

This section includes these chapters:

1 Introduction

The access point (AP) runs software that includes a network management agent. The agent offers a variety of management options, including a web-based interface. The AP can also be accessed through Secure Shell (SSH) for configuration using a command line interface (CLI).

Note: This manual describes the configuration interface for stand-alone mode. Refer to the Edgecore *ecCLOUD Controller User Manual* for information on configuring the AP through the cloud interface.

This chapter includes the following sections:

Configuration Options

The access point's web agent allows you to configure AP parameters, monitor wireless connections, and display statistics using a standard web browser. The AP's web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed remotely by a Secure Shell (SSH) connection over the network. The CLI is used primarily for technical support.

The AP's web interface allows you to perform management functions such as:

- Set management access user names and passwords
- Configure IP settings
- Configure 2.4 GHz, and 5 GHz radio settings
- 5 GHz, and 6 GHz radio settings
- Control access through wireless security settings
- Filter packets using Access Control Lists (ACLs)
- Download system firmware
- Download or upload configuration files
- Display system information

Zero-Touch Provisioning

APs can be automatically managed by the Edgecore ecCLOUD controller or an EWS-Series controller. If an AP is already registered with the ecCLOUD controller, it will be automatically managed when the WAN port of the AP is connected to the Internet.

When an AP is connected to a local LAN with an EWS-Series controller, the AP can be configured with the controller IP address through DHCP Option 138 and then automatically managed by the controller.

As an alternative to zero-touch provisioning, you can manually set the preferred management method from the web interface, see "System Settings" on page 83.

Connecting to the Web Interface

For first-time access to the AP's web management interface, you can connect a PC directly to one of the AP's LAN ports or use the quick-setup QR code (printed on a label next to the AP's ports). The first-time you access the web interface, it automatically runs the Setup Wizard for initial AP configuration.

For information on the Setup Wizard, see "AP Setup Wizard" on page 22.

For information on using the QR code, see "QR Code Onboarding" on page 27.

LAN Port Connection

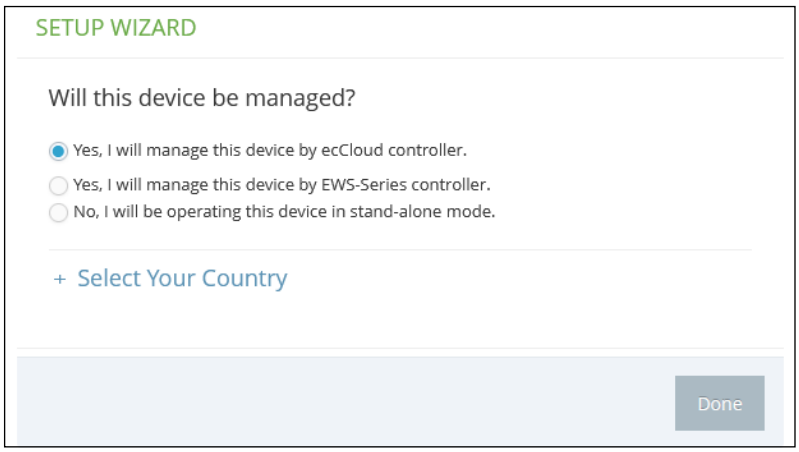
When connecting to the web management interface through one of the AP's LAN ports, the AP has a default management IP address of 192.168.2.1 and a subnet mask of 255.255.255.0. Therefore, you must set your PC IP address to be on the same subnet as the AP (that is, the PC and AP addresses must both start with192.168.2.x).

Note: To connect to the web interface using the Uplink(PoE) port, the IP address is automatically assigned through DHCP by default. If a DHCP server is unreachable, the Uplink(PoE) port reverts to a fallback IP address of 192.168.1.10.

To access the AP's web management interface, use your web browser to connect to the management interface by entering the default IP address of 192.168.2.1.

For first-time access, there is no user login and the Setup Wizard starts automatically. Follow the steps described in "AP Setup Wizard" on page 22.

Figure 1: Web Management Login



Note: To configure the AP with a different management IP address that is compatible with your network, see "LAN Settings" on page 49.

AP Setup Wizard

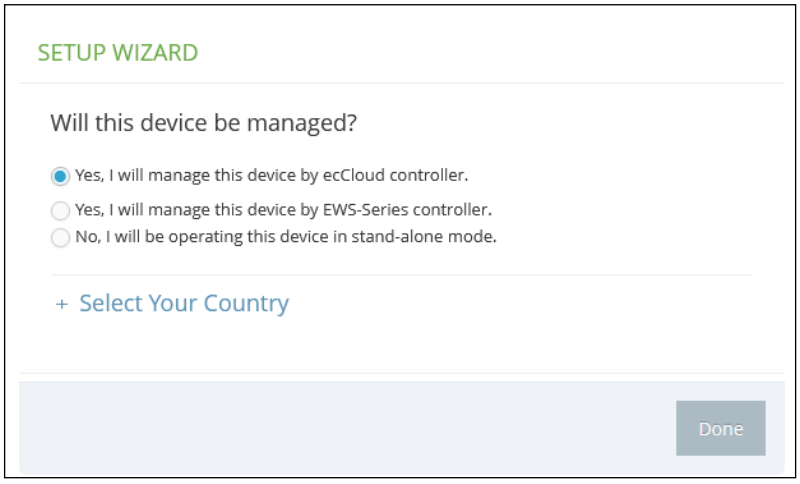
The Setup Wizard is designed to help you configure the basic settings required to get the AP up and running.

Step 1 Select How the AP will be Managed — To manage the AP using the Edgecore ecCLOUD controller, select "Yes, I will manage this device by ecCloud controller," and then continue to Step 6.

To manage the AP using the an Edgecore EWS-series controller, select "Yes, I will manage this device by EWS-Series controller," and then continue to Step 2.

Otherwise, select "No, I will be operating this device in stand-alone mode" and continue to Step 3.

Figure 2: Select ecCloud, EWS Controller, or Stand-Alone



If you select to manage the AP using the Edgecore ecCLOUD controller, go to cloud.ignitenet.com to register your AP. Log in and select Devices from the menu. Click Add Device and enter the AP serial number and MAC address to register the AP with your cloud network. The serial number and MAC address can be found on the product packaging or label.

Note: This manual describes the configuration interface for stand-alone mode. Refer to the Edgecore *ecCLOUD Controller User Manual* for information on configuring the AP through the cloud interface or the *EWS-Series Controller User Manual* for information on managing the AP through an EWS controller.

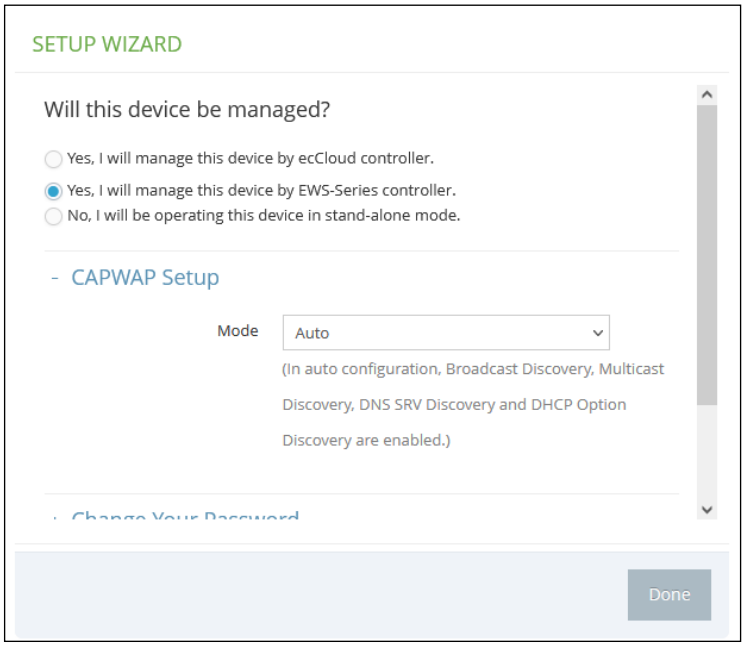
Step 2 CAPWAP Setup — When EWS-Series Controller management is selected, you can set the mode for discovering the controller. Once the AP has discovered the controller on the network it can then send a CAPWAP (Control And Provisioning of Wireless Access Points) join request.

In Auto mode, the AP uses four methods to discover the controller. These methods require no further configuration.

In manual mode, two options are available. Specify the Domain Name Suffix so that the AP can use DNS server records to discover the EWS controller. Or, just specify a static IP address for the controller.

For more information on CAPWAP setup, see "System Settings" on page 83.

Figure 3: CAPWAP Setup

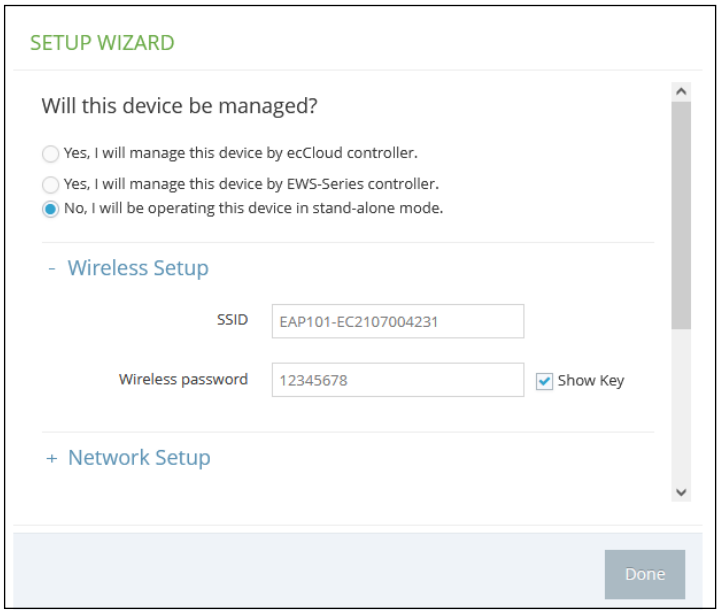


After completing the CAPWAP setup, continue with Step 5.

Step 3 Wireless Setup — If you select to manage the AP in stand-alone mode, you can configure the default wireless network.

The default wireless network name (SSID) consists of the AP model and its serial number, and there is a default wireless password. You have the option to modify the wireless network name and password to your preferred configuration. The wireless name must be 1-32 ASCII characters, and the password must be 8 to 63 ASCII characters (no special characters are allowed).

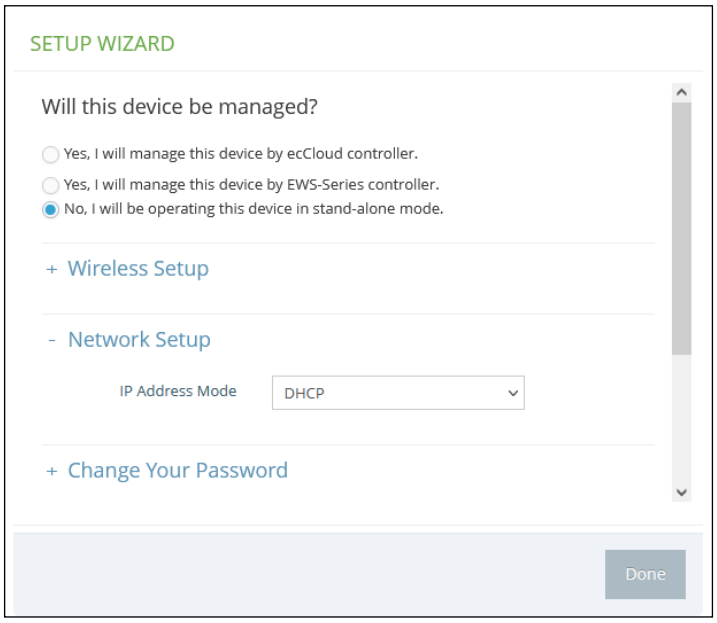
Figure 4: Wireless Setup



Step 4 Network Setup — For AP stand-alone mode, you also have the option to configure the IP address mode used to provide an IP address for the Internet access port.

The default IP Address Mode is DHCP and other options include Static IP and PPPoE. For more information, see "Internet Settings" on page 43.

Figure 5: Network Setup



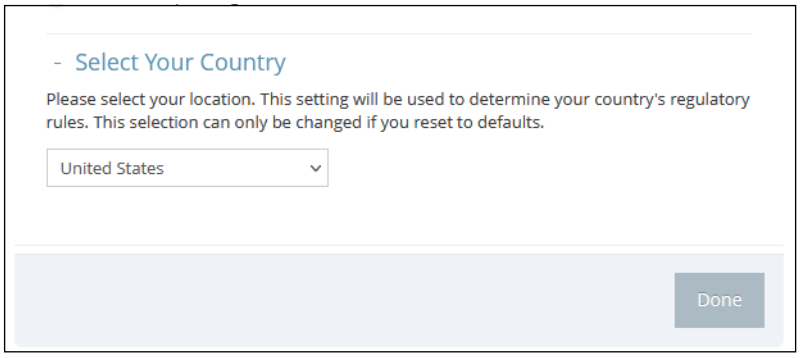
Step 5 Change Your Password — Set a new password for management access to the AP (the default user name is "admin" with password "admin"). The password must be 6-20 ASCII characters (case sensitive with no special characters).

Figure 6: Change Password

Note: For information on changing user names and passwords, see "User Accounts" on page 89.

Step 6 Select Your Country — Select the access point's country of operation from the drop-down menu. You must set the AP's country code to be sure that the radios operate according to permitted local regulations. That is, setting the country code restricts operation of the AP to the radio channels and transmit power levels permitted for wireless networks in the specified country.

Figure 7: Select Country



Caution: You must set the country code to the country of operation. Setting the country code ensures that the radios operate within the local regulations specified for wireless networks.

Note: The country code selection is for non-US models only and is not available to any US models. Per FCC regulation, all Wi-Fi products marketed in the US must be fixed to US operation channels only.

Step 7 After completing the Setup Wizard, click "Done."

QR Code Onboarding

For quick set up and registration of your AP with the ecCLOUD controller, you can scan the QR code on the AP using a phone.

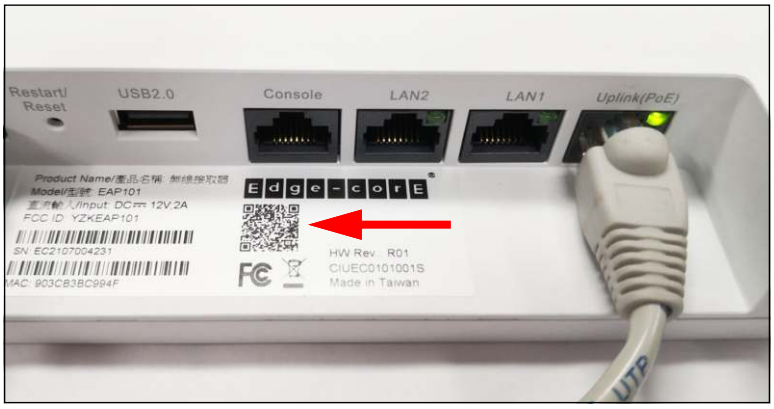
Follow these steps:

1. Power on the AP.

2. Connect the AP to the Internet. Connect your network or Internet access device to the AP's RJ-45 Uplink port.

3. Use the camera or a barcode app on your phone to scan the AP's QR code. The QR code is printed on a label next to the AP's ports.

Figure 8: Scanning the AP QR Code



4. When a message pops up, tap "yes" to join the Wi-Fi network. (iPhone requires you to go to Settings > Wi-Fi or open the browser for the message to pop up.)

   The web browser should open and redirect to the Setup Wizard page.

Note: If the phone cannot connect to the Wi-Fi network, type the SSID (network name) and password manually. The SSID name is the AP serial number (for example, EC0123456789), and the password is the AP MAC address (for example, 903CB3BC1234).

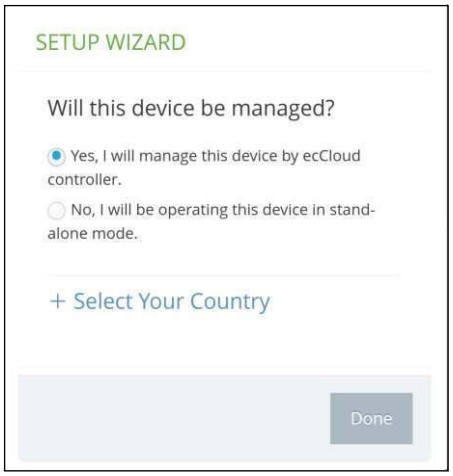
5. Wait for the auto-detection of the WAN port configuration (DHCP, Static IP, or PPPoE).

   When DHCP is detected, the AP automatically continues with the Setup Wizard.

Figure 9: Setup Wizard - Detect Network

6. Select to manage the AP using the ecCLOUD controller or to manage the AP in stand-alone mode.

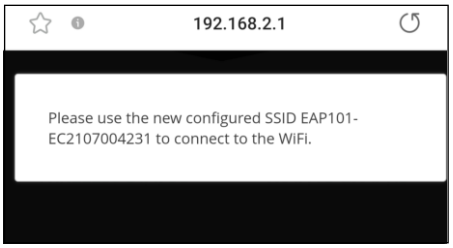
Figure 10: Setup Wizard - Device Management



a. Stand-Alone Mode: Use the default wireless network setting or customize the network name and password. Change the login password and set the country of operation. Tap "Done" to finish the setup wizard.

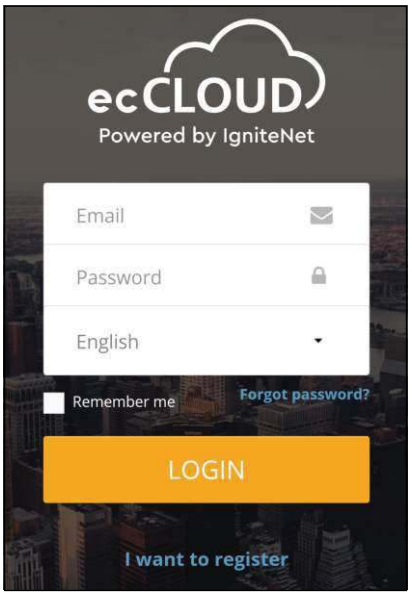
Wait about two minutes for the AP configuration to update, and then connect to the wireless network name configured in the Setup Wizard.

Figure 11: Connect to New SSID



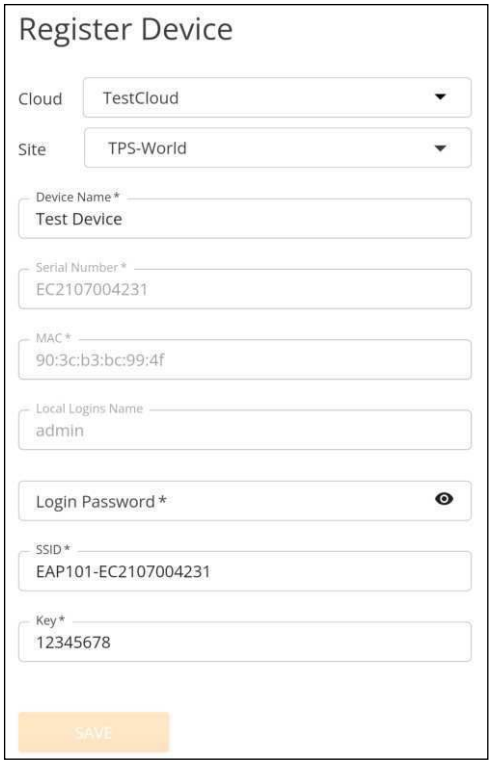
b. Cloud-Managed Mode: Set the country of operation and then tap "Done" to finish the Setup Wizard. The browser is redirected to the ecCLOUD login page.

Figure 12: ecCLOUD Login Page



If you already have an ecCLOUD account, log in and select a site for the AP. The AP is automatically registered for cloud management. Modify the device name, login password, SSID, and security key. After you tap "Save," wait about five minutes for the cloud controller to configure the AP.

Figure 13: ecCLOUD Device Registration



If you do not have an ecCLOUD account, tap "I want to register" and set up an account. Create a cloud and site before confirming the regulatory

country. After tapping “Next,” the AP is then automatically registered for cloud management.

After you tap “Save,” wait about five minutes for the cloud controller to configure the AP.

Note: Refer to the Edgecore *ecCLOUD Controller User Manual* for more information on setting up and configuring APs through ecCLOUD.

Mesh AP Configuration

The first AP can be managed either through ecCLOUD or in stand-alone mode. If a second AP needs to establish a mesh connection with the first AP, follow these steps:

1. Connect the LAN port of the first AP (Mesh Portal Point) to the LAN port of the second AP (Mesh Access Point), which then allows the second AP to synchronize its configuration with the first AP.
2. After unplugging the LAN port, the mesh connection will be established automatically.

Main Menu

The web interface Main Menu provides access to all the configuration settings available for the AP.

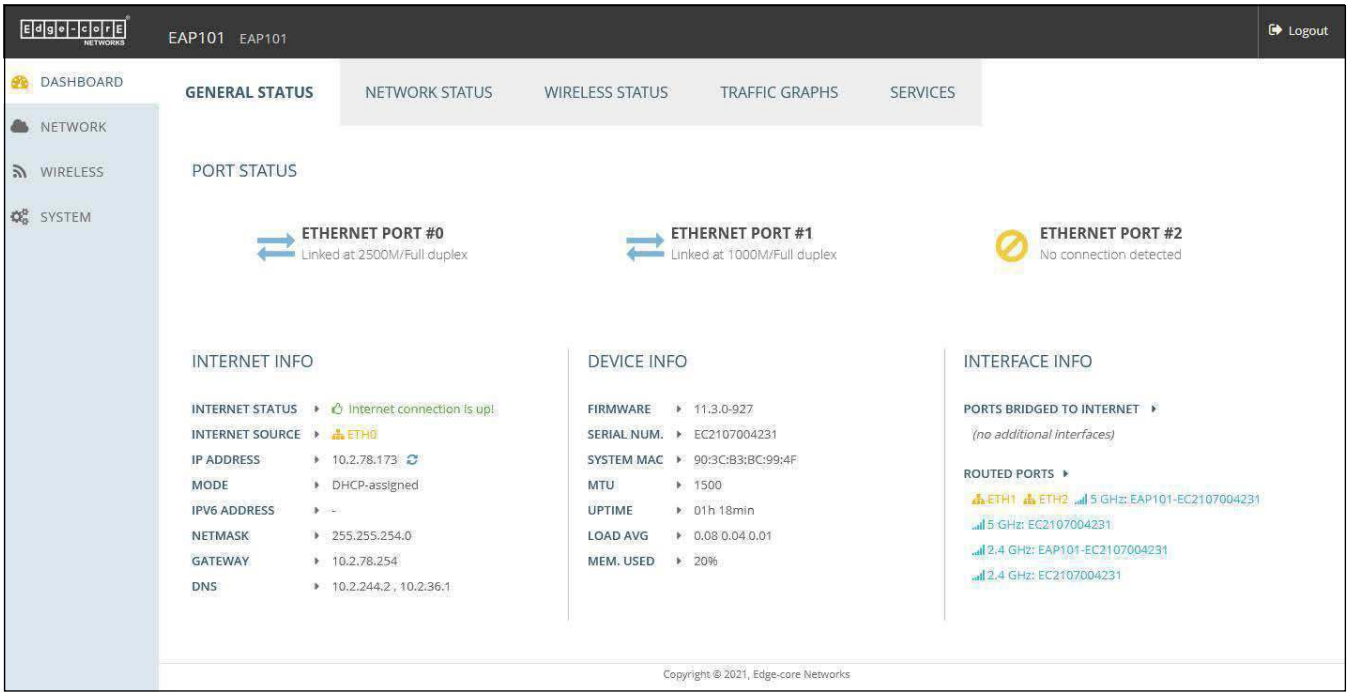
To configure settings, click the relevant Main Menu item. Each Main Menu item is summarized below with links to the relevant section in this guide where the configuration parameters are described in detail:

- **Dashboard** — The dashboard shows basic settings for the AP, including general status, local network settings, and wireless radio status. See “Status Information” on page 33.
- **Network** — Configures Internet, Ethernet, and LAN settings. See “Network Settings” on page 42.
- **Wireless** — Configures 2.4 GHz Radio, 5 GHz Radio, and VLAN settings. See “Wireless Settings” on page 64
- **System** — Configures System (including cloud agent and various system settings), Maintenance (such as view log, reboot, reset defaults, backup defaults, restore defaults, and firmware upgrade), User Accounts, Services (network time), and Diagnostics (including ping, traceroute).

Dashboard

After logging in to the web interface, the dashboard displays. The dashboard shows basic settings for the AP, including Internet status, local network settings, and wireless radio status.

Figure 14: The Dashboard



Common Web Page Buttons

The list below describes the common buttons found on many of the web management pages:

- **Save** – Applies the new parameters and saves them to temporary RAM memory. Also displays a message at the top of the screen to inform you that the changes have not yet been saved to Flash memory. The running configuration will not be saved upon a reboot unless you click the "Save & Apply" button.

Figure 15: Saving Configuration Changes

- **Save & Apply** – Saves the changes made on a page and then applies them so that the configuration is retained after a restart.
- **Revert** – Cancels newly entered settings and restores the originals.
- **Logout** – Ends the web management session.

Section II

Web Configuration

This section provides details on configuring the access point using the web browser interface.

This section includes these chapters:

2 Status Information

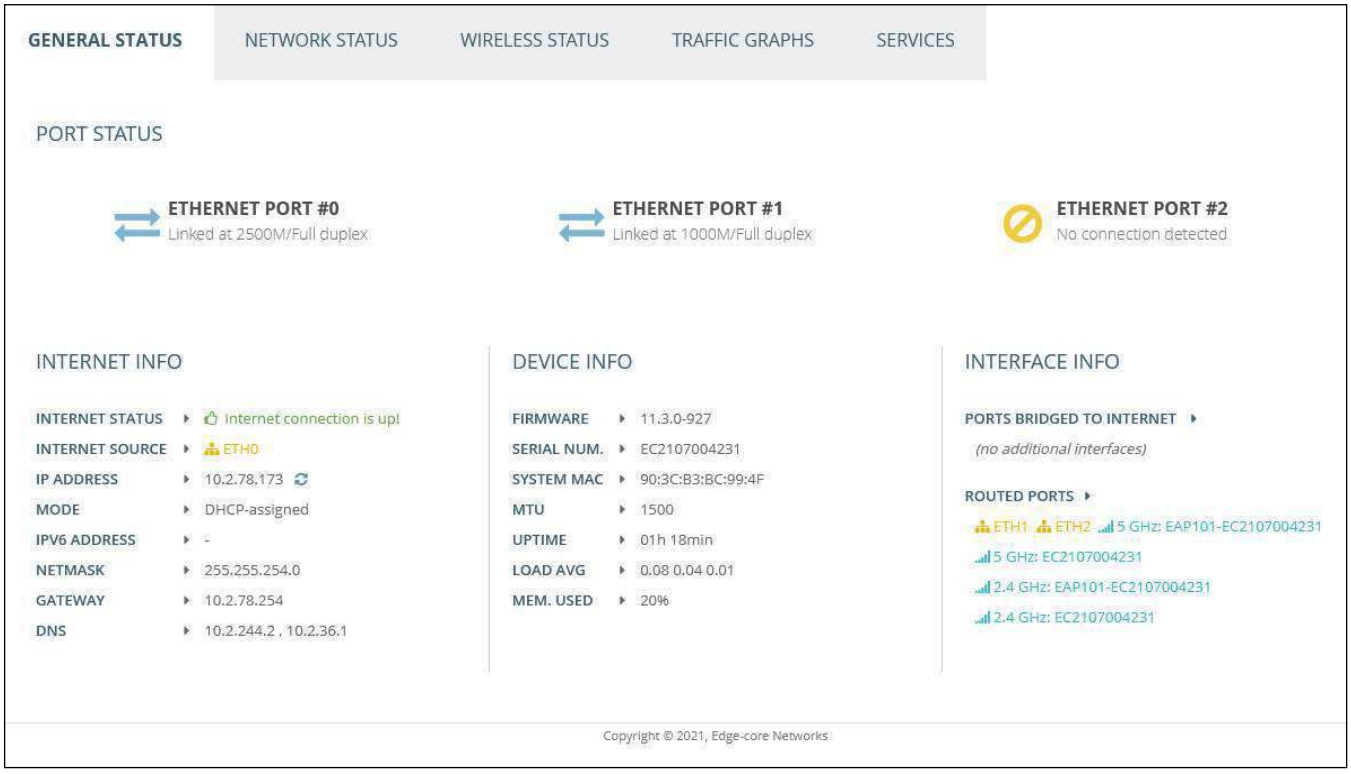
The Dashboard displays information on the current system configuration, including Internet status, local network settings, wireless radio status, traffic graphs, and services.

This chapter includes the following sections:

General Status

The General Status section shows descriptive information about the AP.

Figure 16: General Status Information



The following items are displayed in the “Port Status” section:

- **Ethernet Port #0** — Shows the status of the WAN Ethernet port, including link-up state, speed, and duplex mode.
- **Ethernet Port #1** — Shows the status of the LAN Ethernet port 1, including link-up state, speed, and duplex mode.
- **Ethernet Port #2** — Shows the status of the LAN Ethernet port 2, including link-up state, speed, and duplex mode.

The following items are displayed in the “Internet Info” section:

- **Internet Status** — Shows whether or not the Internet connection is up.
- **Internet Source** — The Ethernet port connected to the Internet. By default, this is Ethernet Port 0.
- **IP Address** — IP address of the Internet connection.

- **Mode** — Shows if the IP address is a static setting or set by DHCP.
- **IPv6 Address** — The IPv6 address of the Internet connection.
- **Netmask** — The subnet mask of the IP address.
- **Gateway** — The IP address of the gateway router that is used when a destination address is not on the local subnet.
- **DNS** — The IP address of the Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

The following items are displayed in the “Device Info” section:

- **Firmware** — The software version number.
- **Serial Number** — The serial number of the physical access point.
- **System MAC** — The system MAC address of the access point.
- **MTU** — The maximum transmission unit for packets sent on the network.
- **Uptime** — Length of time the management agent has been up.
- **Load Average** — The last 1-minute, 5-minute and 15-minute CPU load average.
- **Memory Used** — The percentage of memory being used.

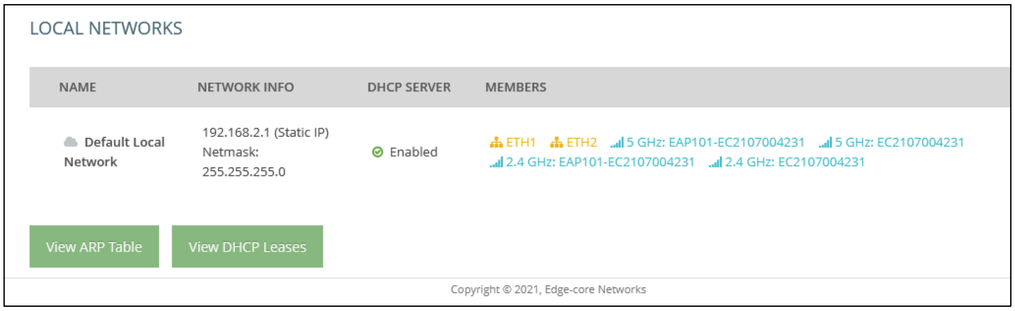
The following items are displayed in the “Interface Info” section:

- **Ports Bridged to Internet** — Additional interfaces attached directly to the Internet. Lists interfaces attached to the WAN (that is, the Internet).
- **Routed Ports** — By default, all interfaces are configured as a member of the LAN. Traffic from these interfaces is routed across the access point through Ethernet Port 0 to the Internet. (This is also called route to Internet.)

Network Status

The Network Status section shows information about local network connections.

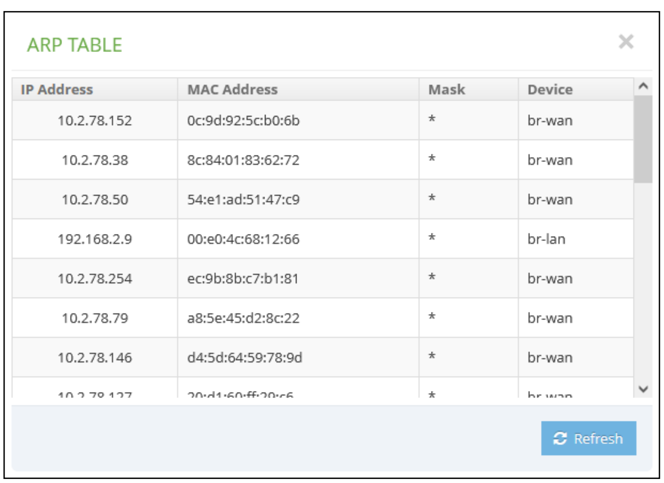
Figure 17: Local Networks



The following items are displayed in this section:

- **Name** — Shows information on the name of the local network.
- **Network Info** — Shows whether the local network uses static or dynamic configuration, and the network mask.
- **DHCP Server** — Shows if DHCP service is enabled on this network.
- **Members** — Shows the ports and wireless radios attached to this network. (Click on any of these interfaces to open the corresponding configuration page.)
- **View ARP Table** — Shows the ARP cache.

Figure 18: ARP Table



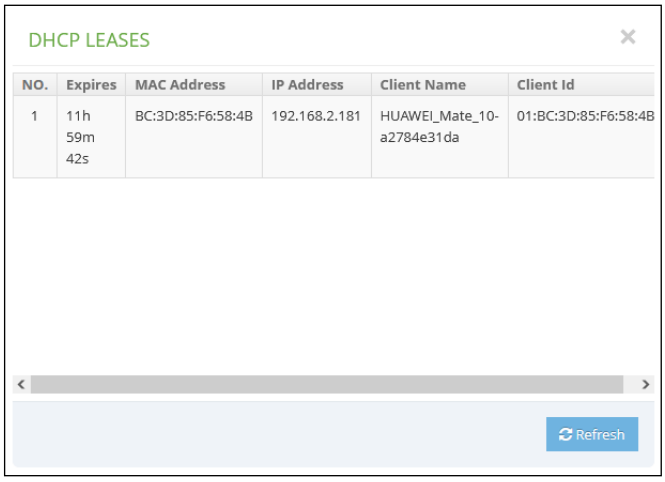
ARP TABLE

IP Address	MAC Address	Mask	Device
10.2.78.152	0c:9d:92:5c:b0:6b	*	br-wan
10.2.78.38	8c:84:01:83:62:72	*	br-wan
10.2.78.50	54:e1:ad:51:47:c9	*	br-wan
192.168.2.9	00:e0:4c:68:12:66	*	br-lan
10.2.78.254	ec:9b:8b:c7:b1:81	*	br-wan
10.2.78.79	a8:5e:45:d2:8c:22	*	br-wan
10.2.78.146	d4:5d:64:59:78:9d	*	br-wan

Refresh

- **View DHCP Leases** — Shows DHCP leases.

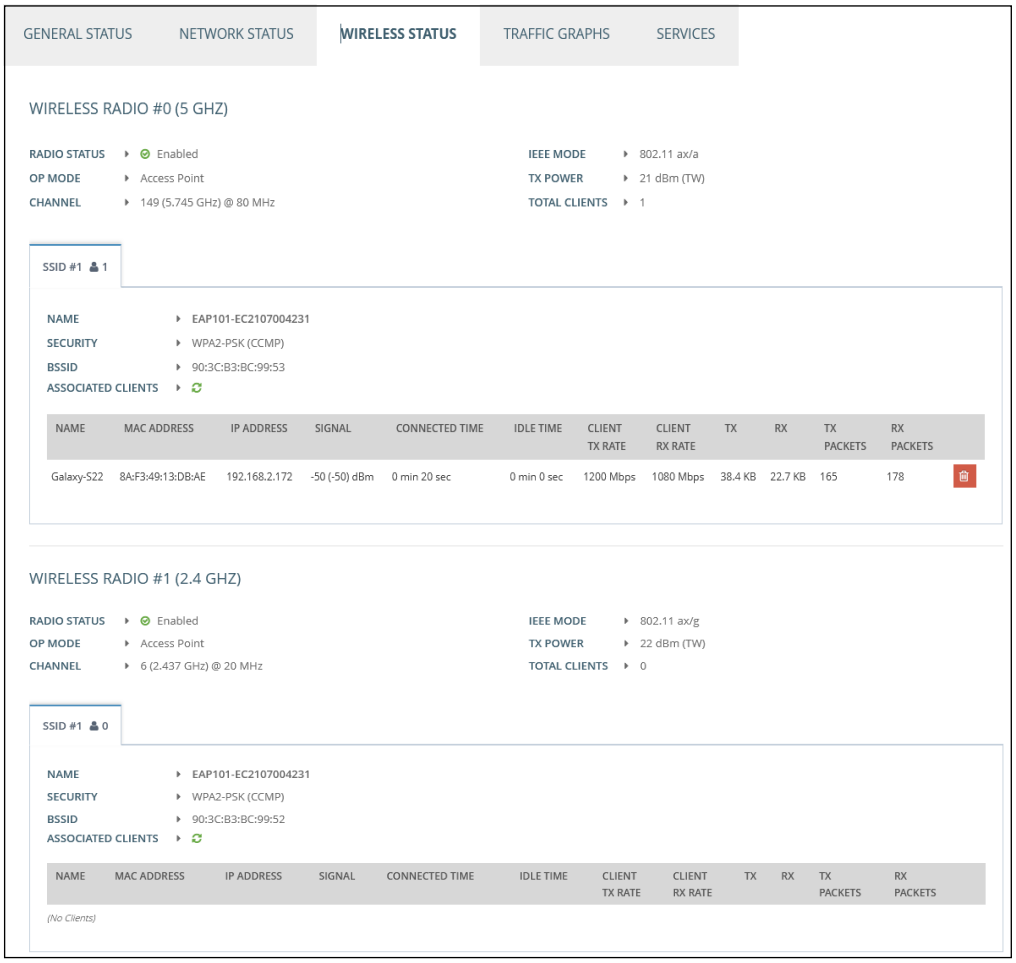
Figure 19: Active DHCP Leases



Wireless Status

The Wireless Status section shows information about the radio settings and associated clients.

Figure 20: Wireless Status



Note that you can click the red button next to an associated client to force disconnection.

The following items are displayed in this section:

- **Wireless Radio 5 GHz/2.4 GHz** — Indicates the 2.4 GHz or 5 GHz wireless interface.
  - **Radio Status** — Shows if the wireless interface is enabled or disabled.
  - **IEEE Mode** — The 802.11 wireless LAN standards supported by the AP.
  - **Op Mode** — Shows if the wireless interface is configured to operate in an access point mode or client mode.

- **Tx Power** — The power of the radio signals transmitted from the AP.
- **Channel** — The radio channel the access point uses to communicate with wireless clients. The available channels depend on the 802.11 Mode, Channel Bandwidth, and Country Code settings.
- **Total Clients** — The total number of clients attached to this interface.

- **SSID #** — Service set identifier. Clients that want to connect to the wireless network through an access point must set their SSIDs to the same as that of the access point.
  - **Name** — A unique identifier for the local wireless network.
  - **Security** — Shows whether or not security has been enabled.
  - **BSSID** — The basic service set identifier. This is the MAC address of the AP generated by combining the 24 bit Organization Unique Identifier (OUI, the manufacturer's identity) and the manufacturer's assigned 24-bit identifier for the radio chipset in the AP.
  - **Associated Clients** — Shows detailed information about associated wireless clients.
    - **Name** — Client name.
    - **MAC Address** — The MAC address of the wireless client.
    - **IP Address** — The IP address assigned to the wireless client.
    - **Signal** — The signal strength (TX/RX) in dBm.
    - **Connected Time** — The time the wireless client has been associated.
    - **Idle Time** — The time the wireless client has been inactive.
    - **Client TX Rate** — The data transmit rate to the wireless client.
    - **Client RX Rate** — The data receive rate from the wireless client.
    - **TX** — The number of bytes transmitted to the wireless client.
    - **RX** — The number of bytes received from the wireless client.
    - **TX Packets** — The number of packets transmitted to the wireless client.
    - **RX Packets** — The number of packets received from the wireless client.

Traffic Graphs

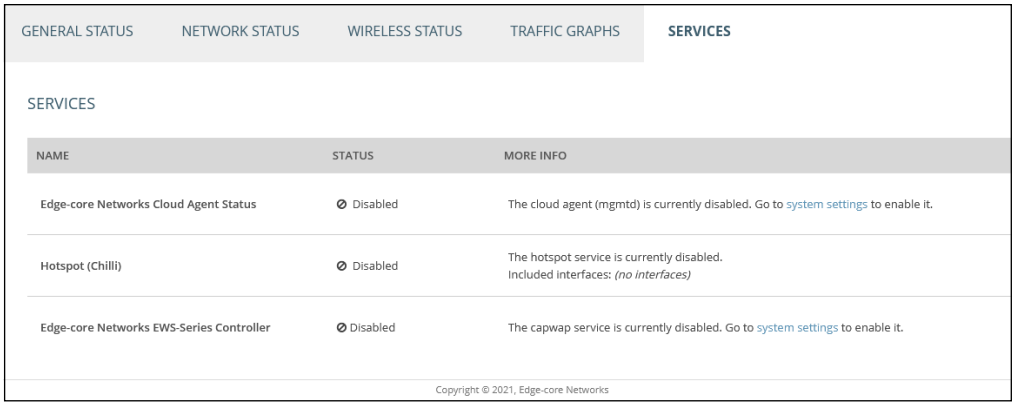
The Traffic Graphs section shows the data rate for the Ethernet ports, wireless interfaces, and mesh interface.

Figure 21: Traffic Graphs

Services

The Services section shows the status of the Edgecore cloud management agent.

Figure 22: Services



- **Edge-core Networks Cloud Agent Status** — Shows whether or not the agent for the cloud controller is enabled.

- **Hotspot (Chilli)** — Shows whether or not hotspot services are enabled. Click on this field to open the Hotspot Settings menu.

- **Edge-core Networks EWS-Series Controller** — Shows if the CAPWAP service is enabled for management of the AP through an EWS-Series controller.

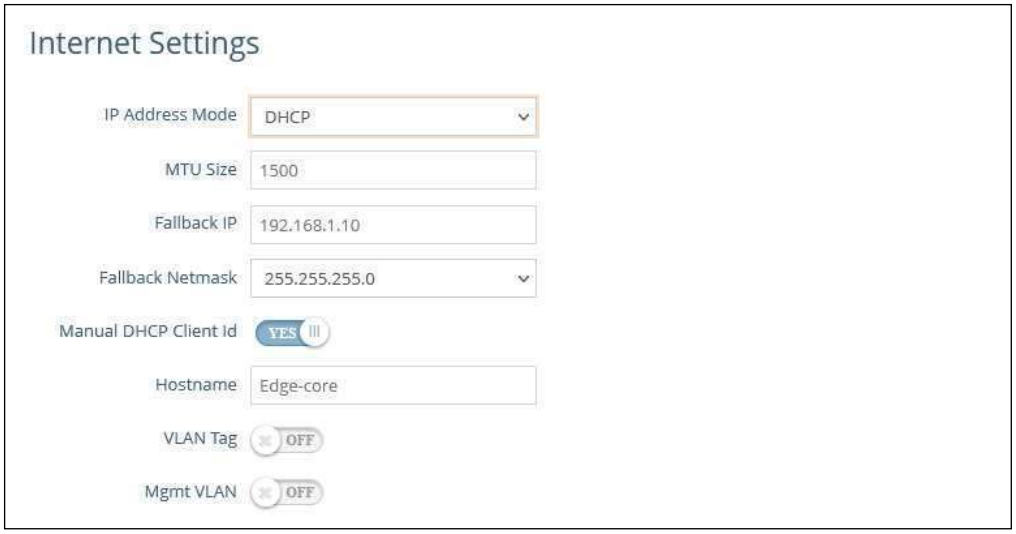
3 Network Settings

This chapter describes basic network settings on the access point. It includes the following sections:

Internet Settings

The Internet Settings page configures the basic Internet settings for the AP, such as the source port, IP aliases, as well as the host name and maximum MTU size.

Figure 23: Internet Settings



The following items are displayed on this page:

- **IP Address Mode** — The method used to provide an IP address for the Internet access port. (Default: DHCP; Options: DHCP, Static IP, PPPoE)
  - **DHCP** — Configuration options displayed for DHCP are shown in Figure 23.
    - **Fallback IP** — This IP address is used if the DHCP service is unavailable or fails. (Default: 192.168.1.10)
    - **Fallback Netmask** — The network mask associated with the fallback IP address. (Default: 255.255.255.0)
    - **Manual DHCP Client Id** — An option to manually enter the hostname for the DHCP client.

Figure 24: IP Address Mode – Static IP

- **Static IP** — To configure a static IP address for the selected Ethernet interface, the following items must be specified.
  - **IP Address** — Specifies an IP address for the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.1.1)
  - **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
  - **Default Gateway** — The IP address of the default gateway, which is used if the requested destination address is not on the local subnet.

    If you have management stations, DNS, RADIUS, or other network servers located on another subnet, type the IP address of the default gateway router in the text field provided.
  - **DNS Servers** — The IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

    If you have a DNS servers located on the local network, type the IP address in the text fields provided.

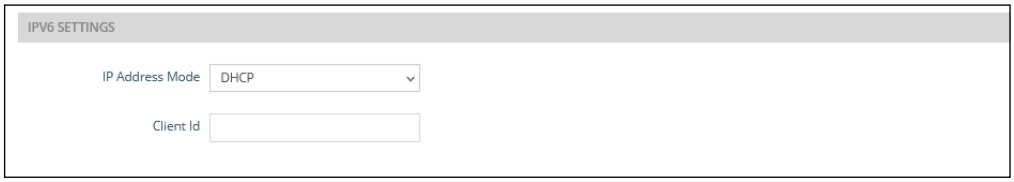
Figure 25: IP Address Mode – PPPoE

- **PPPoE** — To obtain an IP address for the selected Ethernet interface using PPPoE, the following items must be specified.
  - **Service Name** — The service name assigned for the PPPoE connection. The service name is normally optional, but may be required by some service providers. (Range: 1-32 alphanumeric characters)
  - **User Name** — The user name specified by the service provider. (Range: 1-32 characters)
  - **Password** — The password specified by the service provider. (Range: 1-32 characters)
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this interface. (Range: 1400-1500 bytes; Default 1500 bytes)
- **VLAN Tag** — Enable to activate tagging on this port and choose a tagging ID value between 2 and 4094, inclusive.
- **Mgmt VLAN** — Select this option to enable a management VLAN on this device. Once you enable this option, you will no longer be able to access this device on any of built-in the local networks (like 192.168.2.1 for example). You will only be able to access the device from the specified VLAN network. If this device's IP mode is set to DHCP, it will also request a new IP address in the subnet range assigned to the VLAN network.

IPv6 Settings

Enables you to configure the method used to provide an IPv6 address for the Internet access port.

Figure 26: IPv6 Settings



The following items are displayed on this section of the page:

- **IP Address Mode** — The method used to provide an IPv6 address for the Internet access port. (Default: DHCP; Options: DHCP, Static IP)
  - **DHCP** — If you configure DHCP, the Client Id must be specified.
    - **Client Id** — Manually enter the client ID for the DHCP client.
  - **Static IP** — To configure a static IPv6 address for the Internet access port, the following items must be specified.
    - **IP Address** — Specifies an IPv6 address for the access point. An IPv6 address must be configured according to RFC 2373 using 8 colon separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
    - **Default Gateway** — The IPv6 address of the default gateway, which is used if the requested destination address is not on the local subnet.
    - **DNS** — The IPv6 address of Domain Name Servers on the network. A DNS maps numerical IPv6 addresses to domain names and can be used to identify network hosts by familiar names instead of the IPv6 addresses. If you have a DNS server located on the local network, type the IPv6 address in the text field provided.

Ethernet Settings

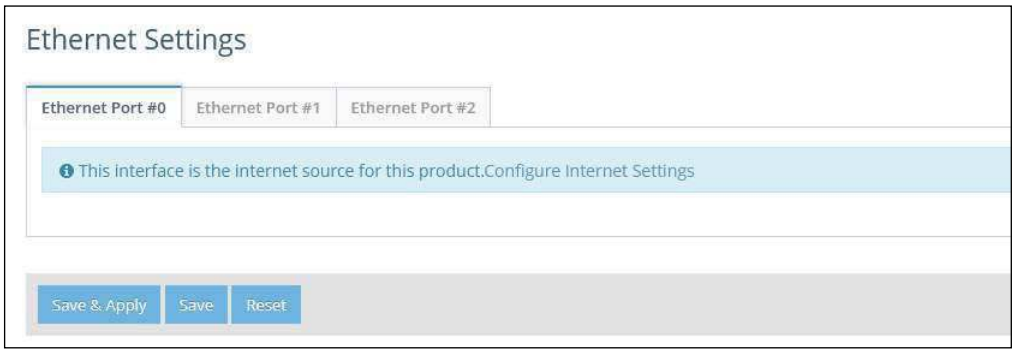
The Ethernet Settings page configures the network behavior of the Ethernet ports, indicating that a port provides an Internet connection for wireless clients attached to the local network (routed to the Internet), or is bridged directly to the Internet.

The following items are common for all pages under Ethernet Settings:

- **Ethernet Port #0** — Shows the status of the WAN Ethernet port.

- **Ethernet Port #1** — Shows the status of the LAN Ethernet port 1.
- **Ethernet Port #2** — Shows the status of the LAN Ethernet port 2.

Figure 27: Ethernet Settings – Internet Source

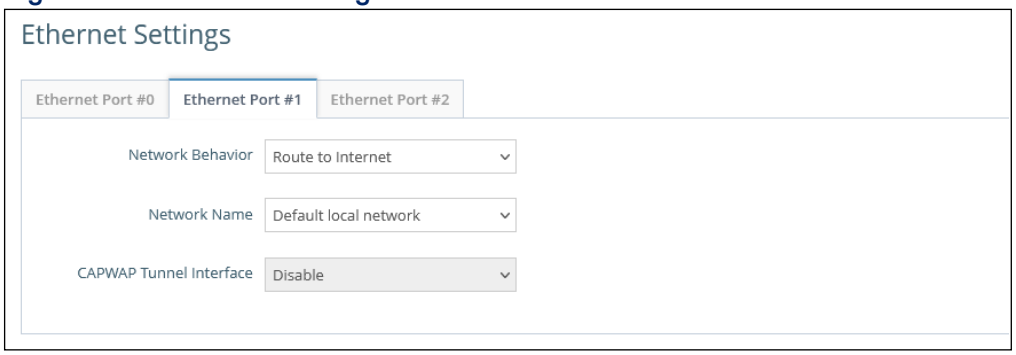


The following status message is displayed if an interface is set as the Internet source:

- "This interface is the internet source for this product. Configure Internet Settings"

  If more than one interface is connected to the Internet, only the last configured interface is used.

Figure 28: Ethernet Settings – Network Behavior



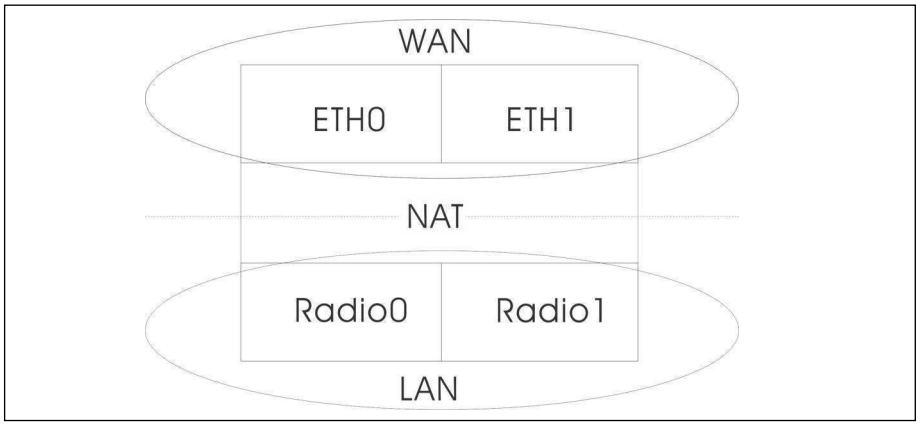
The following items are displayed on this page:

- **Network Behavior** — For the Ethernet port which is not providing Internet access, one of the following connection methods must be specified. (Default: Route to Internet)

  - **Bridge to Internet** — Configures an interface to be attached to the WAN. Traffic from this interface is directly bridged into the Internet. If an Ethernet port is bridged to the Internet, management access cannot be made by a direct connection to this port. However, if another Ethernet port or radio interface is within the LAN (routed to the Internet) the access point can be managed through this interface by a PC which is configured with an IP address in the same subnet.

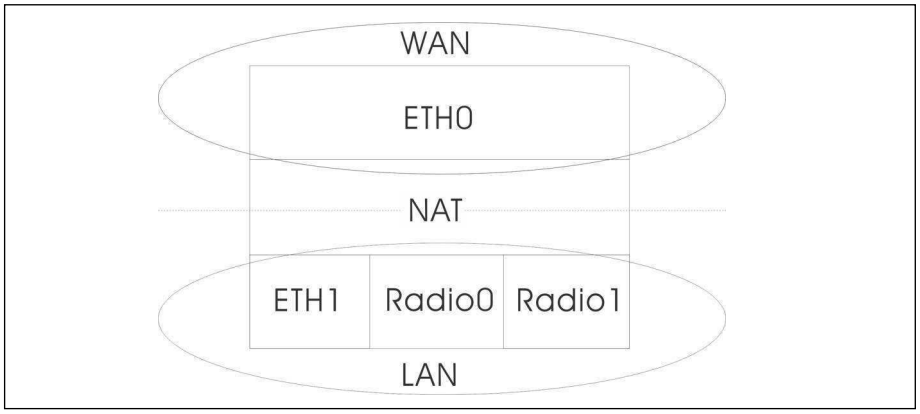
In the following figure, Ethernet Port 0 and Ethernet Port 1 are both attached to the WAN.

Figure 29: Bridge to Internet



- **Route to Internet** — Configures an interface to be a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged directly to the Internet. By default, Ethernet Port 1 is routed to Internet, allowing management access via a direct connection to a PC configured with an address in the same subnet.

Figure 30: Route to Internet



  - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Networks.

- **Add to Guest Network** — This port can only support the guest network.

- **Hotspot Controlled** — This port can only access hotspot services. Click the link to open the Hotspot Settings page. See "Hotspot Settings" on page 53.

- **VLAN Tag Traffic** — This port transmits tagged traffic from a specified VLAN. Select the VLAN ID from the configured list, or click the link to open

the Wireless VLAN Settings page and create a VLAN ID. See "VLAN Settings" on page 80.

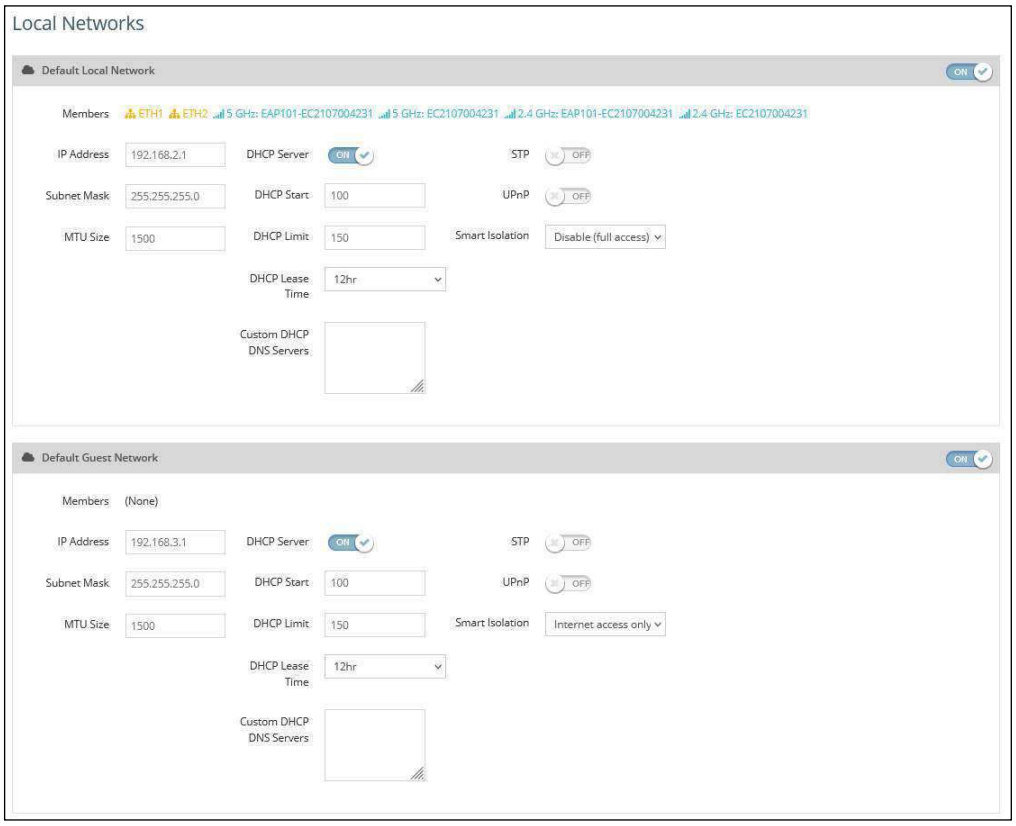
- **PoE Out** — (EAP104 only) Enables the PoE Out feature when the PoE source is detected as 802.3at, otherwise the PoE Out feature is disabled. When set to "Off," PoE Out is always disabled. (Default: On)

- **CAPWAP Tunnel Interface** — When the AP system management is set to EWS-Series Controller mode (see "System Settings" on page 83), the CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode can be configured for the Ethernet port from the controller template. The options are "Disable" or "Complete." A Complete tunnel sends all management, authentication, and data traffic from the AP back to the controller. (Default: Disable)

LAN Settings

The LAN Settings page configures the LAN settings for the local and guest networks, including IP interface setting, DHCP server settings, and STP administrative status.

Figure 31: Network – LAN Settings



The following items are displayed on this page:

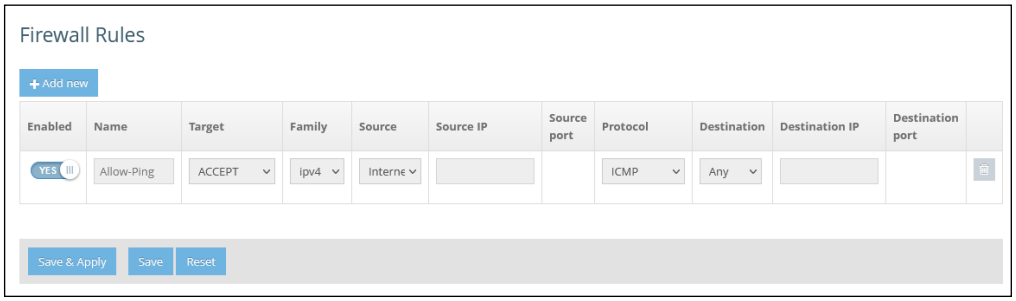
- **IP Address** — Specifies the IP address for the local network or guest network. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.2.1)
- **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this network. (Range: 1400-1500 bytes; Default 1500 bytes)
- **DHCP Server** — Enables/disables DHCP on this network. (Default: Enabled)
  - **DHCP Start** — First address in the address pool. (Range: 1-256; Default: x.x.x.100)
  - **DHCP Limit** — Maximum number of addresses in the address pool. (Range: 1-254; Default: 150)
  - **DHCP Lease Time** — The duration that an IP address is assigned to a DHCP client.
  - **Custom DHCP DNS Servers** — Specify the addresses or hostnames of custom DNS servers to be used.
- **STP** — Enables or disables processing of Spanning Tree Protocol messages. (Default: Disabled)
- **UPnP** — Enables or disables Universal Plug-and-Play broadcast messages. (Default: Disabled)
- **Smart Isolation** — Enables network traffic to be restricted to the specified network:
  - **Disable (full access)** — There is no traffic isolation. Clients can access the Internet and other devices on the local LAN.
  - **Internet access only** — Traffic from this network can only be routed to and from the Internet.
  - **LAN access only** — Traffic from this network is restricted to local LAN devices only.
  - **Internet access strict** — Traffic from this network can only be routed to and from the Internet, but with the additional restriction that users cannot access resources or devices on any private network (such as 192.168.0.0, 172.16.0.0, 10.0.0.0 etc.).
- **Add Custom LAN** — Click this button to create additional networks with their own custom settings. You can create up to 5 custom LANs.

Firewall Rules

Firewall filtering restricts connection parameters to limit the risk of intrusion. The firewall settings allow you to define a sequential list of rules that filter traffic based on source and destination IP addresses and ports. Ingress packets are tested against the filter rules one by one. As soon as a packet matches a rule, the configured target action is implemented.

One rule, "Allow-Ping," is pre-configured to allow Ping packets from the Internet. You can enable or disable this rule, but it cannot be modified or deleted. Click the "Add new" button to add a new firewall rule.

Figure 32: Firewall Rules



The following items are displayed on this page:

- **Enabled** — Enables or disables the rule.
- **Name** — A user-defined name for the filtering rule. (Range: 1-30 characters)
- **Target** — The action to take when a packet is matched. (Options: Accept, Reject, Drop; Default: Accept)
  - **Accept** — Accepts matching packets.
  - **Reject** — Drops matching packets and returns an error packet in response.
  - **Drop** — Drops matching packets.
- **Family** — The IP address family. (Options: Any, IPv4; Default: Any)
- **Source** — The source interface. (Options: Guest Network, Hotspot Network, Default Local Network, Internet, Any)
- **Source IP** — The source IPv4 address in CIDR notation. Includes an IPv4 address followed by a slash (/) and a decimal number to define the network mask.
- **Source port** — The source protocol port. (Range: 0-65535)

- **Protocol** — The protocol type. (Options: Any, TCP+UDP, TCP, UDP, ICMP; Default: TCP+UDP)
- **Destination** — The destination interface. (Options: Guest Network, Hotspot Network, Default Local Network, Internet, Any)
- **Destination IP** — The destination IP address.
- **Destination port** — The destination protocol port. (Range: 0-65535)

Port Forwarding

Port Forwarding can be used to map an inbound protocol type (TCP/UDP) and port to an "internal" IP address and port. The internal (local) IP addresses are the IP addresses assigned to local devices at the edge of a network, and the external IP address is the IP address assigned to the AP interface. This allows remote users to access different servers on your local network using your single public IP address.

Remote users accessing services such as web or FTP at your local site through your public IP address, are redirected (mapped) to other local server IP addresses and TCP/UDP port numbers. For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.3.9/80, then all HTTP requests from outside users are forwarded to 192.168.3.9 on port 80. Therefore, by just using your external IP address provided by your ISP, Internet users can access the services they need at the local addresses to which you redirect them.

Figure 33: Port Forwarding

The following items are displayed on this page:

- **Enabled** — Enables port forwarding.
- **Name** — User defined name. (Range: 1-30 characters)
- **Protocol** — Set the protocol to which port forwarding is applied. (Options: TCP, UDP, TCP+UDP)
- **External Port** — The TCP/UDP port number. (Range: 1-65535)

  The more common TCP service port numbers include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

- **Internal IP address** — The internal destination IP address.
- **Internal Port** — The internal destination protocol port. (Range: 1-65535)

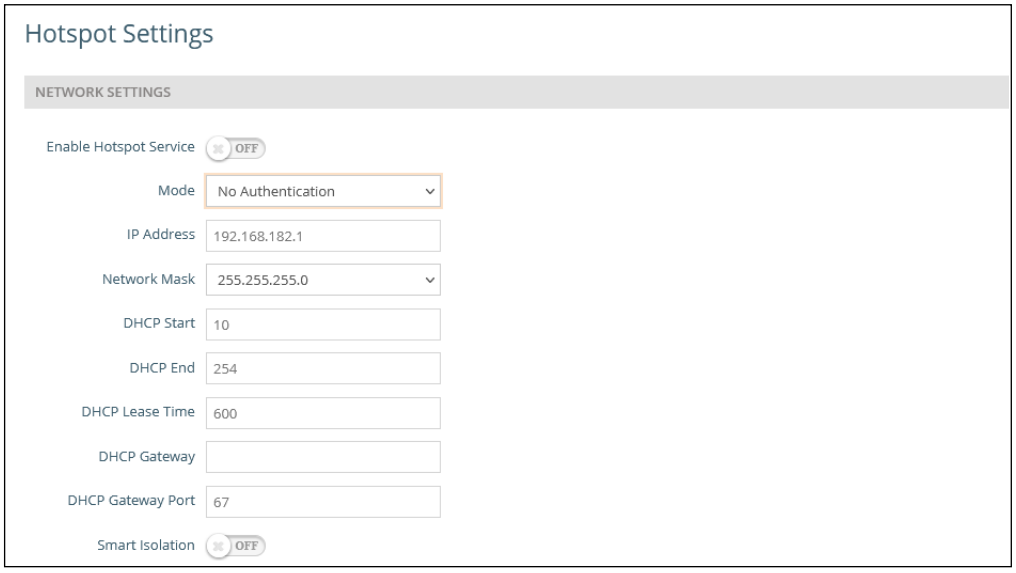
Hotspot Settings

The Hotspot Settings page can configure Internet access to the general public in places such as coffee houses, libraries and hospitals. Specific access rights may also be defined through a RADIUS server.

Network Settings

This section includes the option to enable or disable hotspot service, hotspot mode options, and network settings.

Figure 34: Hotspot Settings (Network Settings)



The following items are displayed on this page:

- **Enable Hotspot Service** — Enables or disables hotspot service. A hotspot is a physical location where people may obtain Internet access, typically using Wi-Fi technology, via a wireless local area network using a router connected to an Internet service provider.
- **Mode** — Hotspot service types include the following options:
  - **External Captive Portal Service** — This option will show the hotspot guest an externally hosted captive portal splash page and may prompt them to login, depending on how you've configured your service settings. Choose this option if you've signed up with a third-party captive portal service provider such as Cloud4Wi or HotSpotSystem.

- **No Authentication** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will not require the guest to login before accessing the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

- **Simple Password-Only Splash Page** — This option will show the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a simple password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

- **Local Spash Page with External RADIUS** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a valid RADIUS username and password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

- **Network IP** — Specifies the IP address for the hotspot. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.182.1)

  If your WAN subnet conflicts with any of the local networks (even the custom ones you create), the AP will automatically change the subnet of the local network.

- **Network Mask** — Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

- **DHCP Start** — Starting number of (last numeric field) in address pool. (Range: 1-254; Default: 10)

- **DHCP End** — Ending number of (last numeric field) in address pool. (Range: 1-254; Default: 254)

- **DHCP Lease Time** — The duration that an IP address is assigned to a DHCP client. (Range: 600-43200 seconds; Default: 600 seconds)

- **DHCP Gateway** — Configure the DHCP gate IP address if you want to use an external DHCP server instead of the internal one.

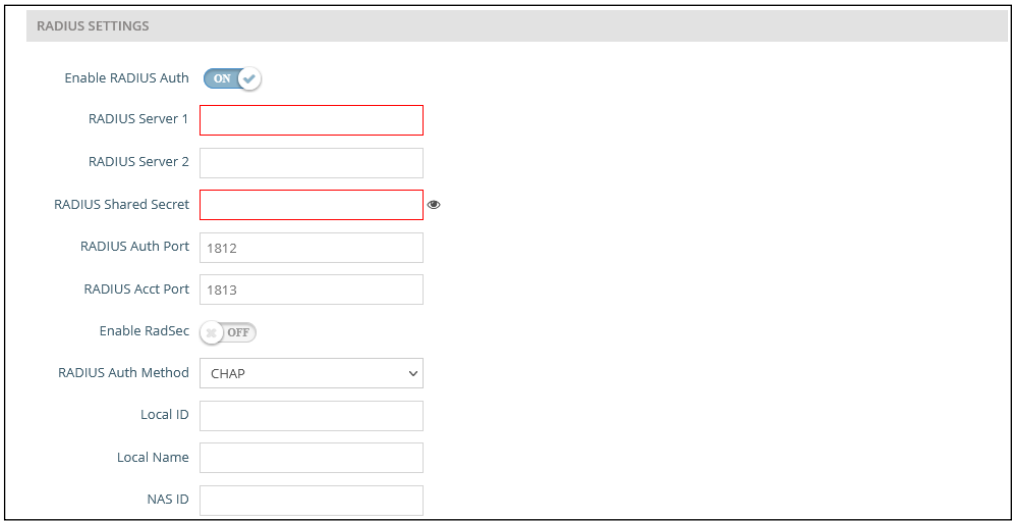
- **DHCP Gateway Port** — The listening port used by the DHCP gateway.

- **Smart Isolation** — Activate to prevent Hotspot users to possibly access WAN resources.

RADIUS Server

If you click set the mode to External Captive Portal Service or Local Splash page with External RADIUS, the following section is displayed.

Figure 35: Hotspot Settings (RADIUS Settings)



The following items are displayed on this page:

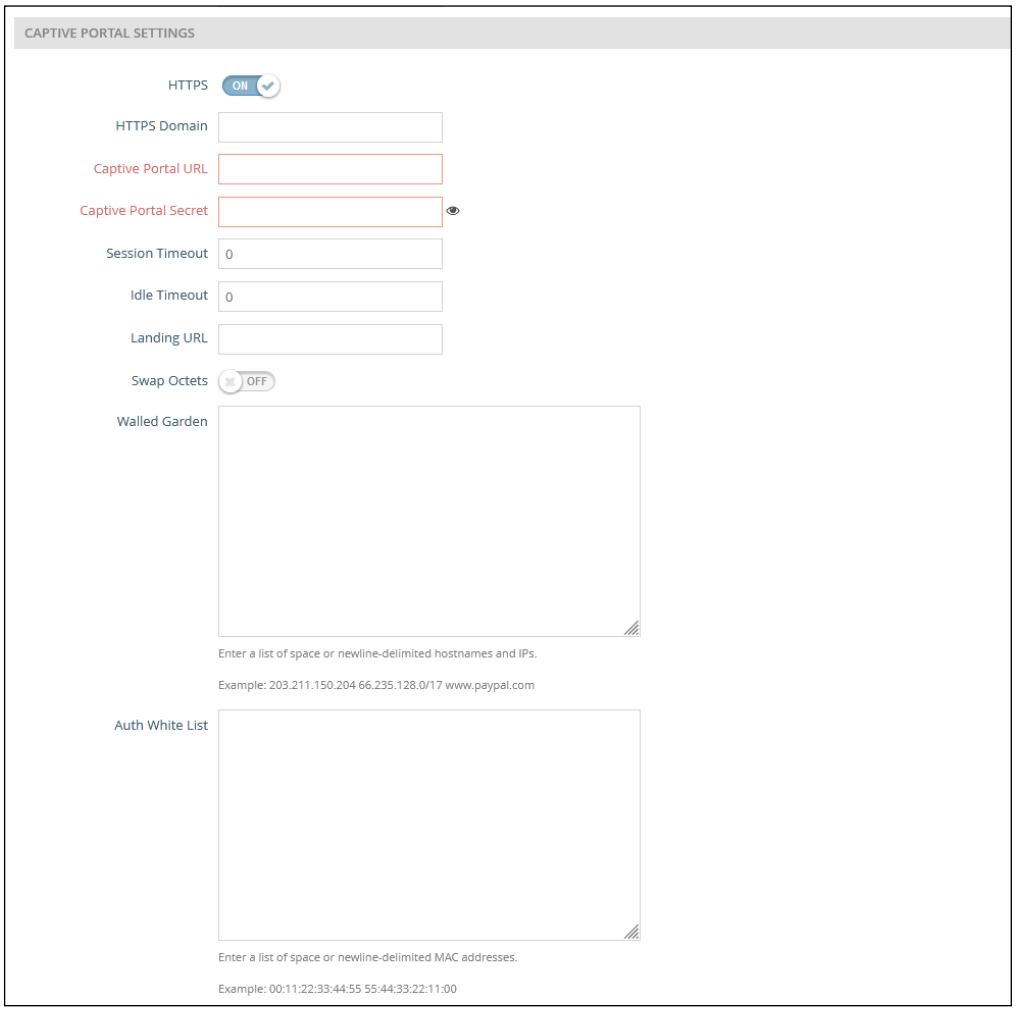
- **Enable RADIUS Auth** — Enables or disables client authentication via a RADIUS server.
- **RADIUS Server 1** — IP address or host name of the primary RADIUS server.
- **RADIUS Server 2** — IP address or host name of the secondary RADIUS server.
- **RADIUS Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Range: 1-255 characters).
- **RADIUS Auth Port** — RADIUS server UDP port used for authentication messages. (Range: 1-65535, Default: 1812)
- **RADIUS Acct Port** — RADIUS server UDP port used for accounting messages. (Range: 1-65535, Default: 1813)
- **Enable RadSec** — An authentication and authorization protocol for transporting RADIUS datagrams over TCP and TLS. RadSec replaces UDP used in the initial RADIUS design, providing a reliable transport protocol and more extensive security for the packet payload.
- **RADIUS Auth Method** — Selects the encryption method to use for messages between the AP and the RADIUS server; CHAP, PAP, or MSCHAPv2. The encryption method must match that used by the RADIUS server.

- **Local ID** — Local RADIUS server identifier.
- **Local Name** — Local RADIUS server name
- **NAS ID** — Local RADIUS server operation identifier.

Captive Portal Settings

The following section is displayed for all hotspot mode options.

Figure 36: Hotspot Settings (Captive Portal Settings)



The following items are displayed on this page:

- **HTTPS** — Enables HTTPS for the captive portal. (Default: Disabled)

Note: To upload a unique security certificate from a trusted certification authority for the HTTPS captive portal, see "Upload Certificate" on page 88.

- **HTTPS Domain** — The domain name of the HTTPS captive portal.
- **Captive Portal URL** — Host name of Internet service portal for the hotspot.

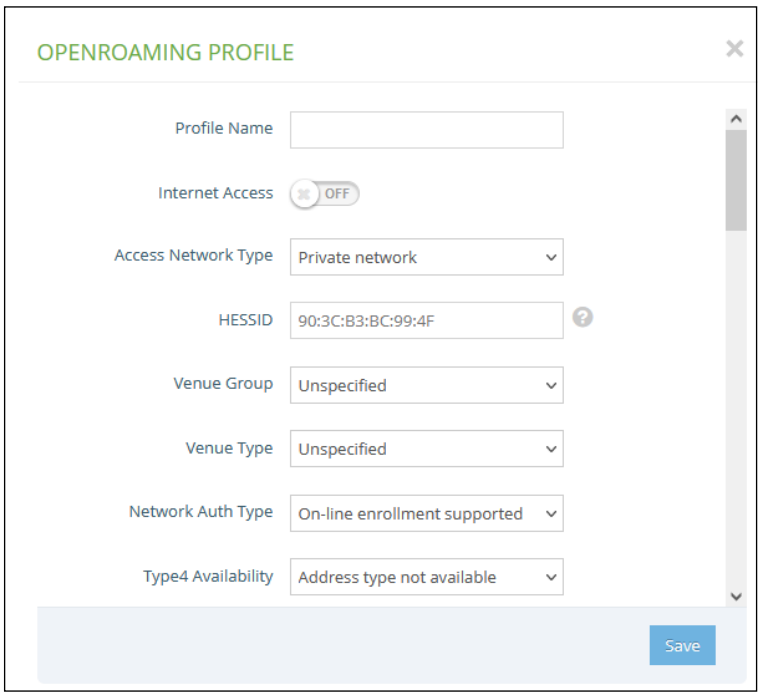
  The captive portal forces a hotspot client to access a welcome web page (normally used for authentication) before gaining further access to the Internet. The welcome page may require authentication and/or payment.
- **Captive Portal Secret** — The password used for logging into the hotspot.
- **Customize Splash Page** — This option is shown for all hotspot service options other than External Captive Portal Service. If enabled, fill in information for the title, background color, logo image file, and optional terms and conditions.
- **Session Timeout** — The maximum time a client can stay attached to the hotspot. (Range: 0-86400 seconds)
- **Idle Timeout** — The maximum a connection can remain inactive before it is closed. (Range: 0-86400 seconds)
- **Landing URL** — Indicates the URL to which the user is directed after logging in to the captive portal.
- **Swap Octets** — Swap the values of the reported “input octets” and “output octets.” This option only appears under External Captive Portal Service.
- **Walled Garden** — A list of web sites to which unauthenticated users are allowed to navigate.
- **Auth White List** — A list of MAC addresses that are allowed to bypass the captive portal to access the Internet.

OpenRoaming

OpenRoaming provides a standard for public-access Wi-Fi networks to support seamless roaming between wireless networks. An OpenRoaming network advertises its public Wi-Fi capabilities and services so that clients can decide if they want to connect to the network.

Up to 32 OpenRoaming profiles can be configured and applied to specific wireless networks (see "OpenRoaming" under "Wireless Networks — Network Settings" on page 76). Click "Add New" to configure a profile.

Figure 37: OpenRoaming Profile



The following items are displayed on this page:

- **Profile Name** — A name that identifies the profile.
- **Internet Access** — Enable if this network provides access to the Internet.
- **Access Network Type** — Select one from the predefined list.
  - **Private network** — Home and enterprise networks that unauthorized users cannot access.
  - **Private network with guest access** — A private network that provides for guest access. A typical example would be an enterprise network that offers guest access.

- **Chargeable public network** — A network that is available to all users, but requires a fee.
- **Free Public Network** — A network that is available to all users without any fees.
- **Personal device network** — A network for peripheral connectivity in an ad-hoc mode. For example, a camera that connects to a printer.
- **Emergency services only network** — A network that is dedicated for access to emergency services only.
- **Test or experimental** — A network for tests or experimental work.
- **Wildcard** — When selected, the AP will reply to clients regardless of the network type requested by the client query.

- **HESSID** — The Homogenous Extended Service Set Identifier (HESSID) for the OpenRoaming network. When configured, the HESSID (a MAC address) uniquely identifies all APs belonging to the same network.
- **Venue Group** — Identifies the general class of the venue. Select from the predefined list.
- **Venue Type** — Identifies the specific type of venue within each group.
- **Network Auth Type** — Specifies the authentication required for the network. Select an option from the predefined list. (Default: "Acceptance of terms and conditions")
- **Type4 Availability** — Specifies the IPv4 address type available from the network.
- **Type6 Availability** — Specifies the IPv6 address type available from the network
- **Operating Class** — A standard index (based on IEEE Std 802.11-2012 Annex E) that specifies the AP supported operating channels.
- **Captive Portal** — Enables the Captive Portal feature. (Default: Disabled)
  - **Captive Portal URL** — Host name of Internet service portal (HTTP or HTTPS).

    A captive portal forces a client to access a welcome web page (normally used for authentication) before gaining further access to the Internet. The welcome page may require authentication and/or payment.

- **Wall Garden** — A list of web sites to which unauthenticated users are allowed to navigate. Enter a list of space or newline-delimited host names and IP addresses.

- **Venue Name Information** — Configures a list of up to 10 venue names.
  - **Language Code** — Select a language from the list. (Default: English)
  - **Venue Name** — The name of the network venue. Multiple names can be added to the list.
  - **Venue URL** — Specifies a URL that provides additional venue information to users.

- **Cellular Network Information List (PLMN)** — (Optional) Identifies the 3GPP cellular networks available through the AP. Specifically, this field identifies the Public Land Mobile Network (PLMN) ID, comprised of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the mobile operator. Up to 10 PLMN IDs can be configured. Input the pair of MCC, MNC.
  For example: 400, 00
  MCC: Three decimal digits (000-999)
  MNC: Two (00-99) or three decimal digits (000-999)

- **Operator Friendly Name** — The name of the network operator and the specified language. Up to 10 names can be configured.

- **Roaming Consortium List** — (Optional) A roaming consortium is a group of service providers (SP) with which a user's credentials can be used for authentication. Each roaming consortium is identified by an organization identifier (OI) that is assigned by the IEEE. An OI is often 24 bits in length, but can also be 36 bits. Up to 10 identifiers can be configured.

- **Domain Name List** — Lists one or up to 10 domain names for the entity operating the AP. This is critical for OpenRoaming network selection policy, as it identifies the operator of the network. It indicates to the mobile device whether they are at a home hotspot or a visited hotspot.

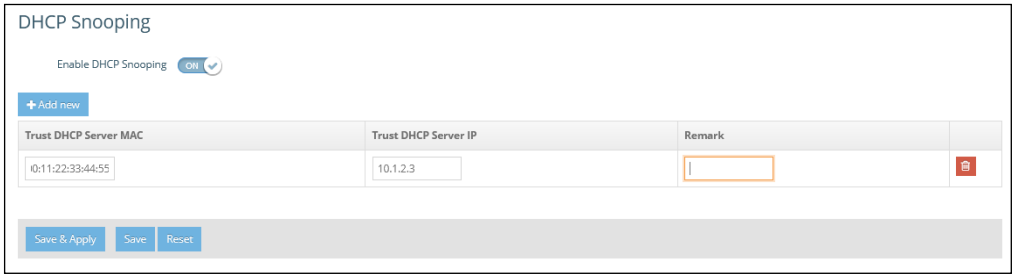
- **NAI Realm List** — (Optional) The network access identifier (NAI) realm list identifies those service provider or other networks that are accessible through the AP. By discovering which authentication realms are supported by a network, a mobile device can selectively authenticate to its preferred network. Up to 10 identifiers can be configured.
  - **Method/Authentication** — Specifies EAP methods and authentication for each service provider added to the NAI Realm List.

DHCP Snooping

DHCP snooping is used to validate and filter DHCP messages received by the AP. When DHCP snooping is enabled, DHCP messages received from a device not listed in the DHCP snooping table are dropped.

You can add known and trusted DHCP servers to the table by specifying their MAC and IP addresses.

Figure 38: DHCP Snooping



The following items are displayed on this page:

- **Enable DHCP Snooping** — Enables DHCP Snooping on the AP.
- **Trust DHCP Server MAC** — The MAC address of a known and trusted DHCP server.
- **Trust DHCP Server IP** — The IP address of a known and trusted DHCP server.
- **Remark** — A comment relating to the DHCP server configured.

ARP Inspection

ARP Inspection is a security feature that validates the MAC Address bindings for Address Resolution Protocol packets. It provides protection against ARP traffic with invalid MAC-to-IP address bindings, which forms the basis for certain "man-in-the middle" attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

Figure 39: ARP Inspection

The following items are displayed on this page:

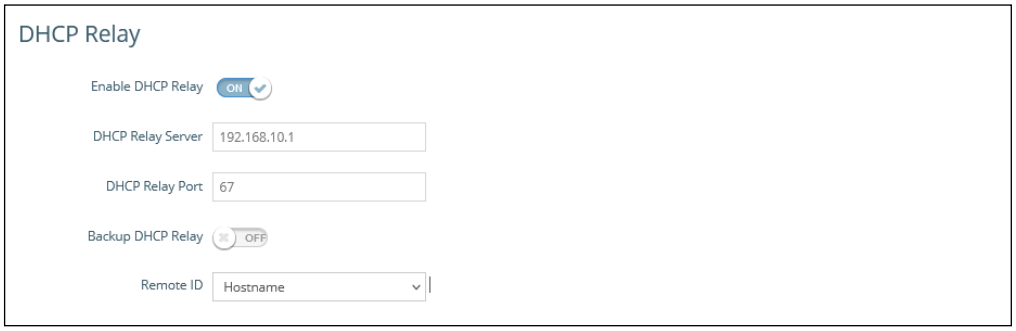
- **ARP Inspection** — When enabled, ARP packets are validated against ARP spoofing.
- **Force DHCP** — Allows the AP to only learn MAC/IP pair information through DHCP packets. Since devices configured with static IP address do not send DHCP traffic, any clients with static IP addresses will be blocked by the AP unless their MAC/IP pair is listed and enabled in the Static Trust List.
- **Trust List Broadcast** — Lets other APs learn the trusted MAC/IP pairs to issue ARP requests.
- **Static Trust List** — Adds the MAC or MAC/IP pairs of devices that are trusted to issue ARP requests. Other network nodes can still send their ARP requests, but if their IP appears in the static list with a different MAC, their ARP requests will be dropped.

DHCP Relay

When DHCP relay is enabled, the AP as an agent for all clients and sends all broadcast DHCP requests directly to a specified DHCP server. The DHCP server IP address and port must be configured, and optionally a backup server.

With DHCP relay enabled, the circuit ID can be set on the VLAN settings or LAN settings page. IP addresses of clients are then obtained by the DHCP relay server and the IP range is determined by the remote ID and circuit ID.

Figure 40: DHCP Relay



The following items are displayed on this page:

- **Enable DHCP Relay** — Enables the DHCP relay feature on the AP.
- **DHCP Relay Server** — Specifies the IP address of the DHCP server.
- **DHCP Relay Port** — Specifies the port of the DHCP server.
- **Backup DHCP Relay** — Optionally specifies a backup DHCP server IP address and port to use if there is no response from the primary server.
- **Remote ID** — Use the hostname as the remote ID, or manually configure a text string as the remote ID.

4 Wireless Settings

This chapter describes the wireless settings on the access point. It includes the following sections:

Radio Settings

The IEEE 802.11 wireless interfaces include configuration options for radio signal characteristics and wireless security features.

The access point can operate in several radio modes, 802.11b+g+n/ax (2.4 GHz) or 802.11a/a+n/ac+a+n/ax (5 GHz). Note that the dual-band access points can operate at 2.4 GHz and 5 GHz at the same time. The web interface identifies the radio configuration pages as:

- **Radio 2.4 GHz** — the 2.4 GHz 802.11b/g/n/ax radio interface
- **Radio 5 GHz** — the 5 GHz 802.11a/n/ac/ax radio interface

Each radio supports 16 virtual access point (VAP) interfaces based on the SSIDs, referred to as SSID1 ~ SSID16. Each VAP functions as a separate access point, and can be configured with its own Service Set Identification (SSID) and security settings. However, most radio signal parameters apply to all VAP interfaces. Traffic to specific VAPs can be segregated based on user groups or application traffic. The clients associate with each VAP in the same way as they would with separate physical access points.

Physical Radio Settings

Figure 41: Physical Settings for Radio 5 GHz

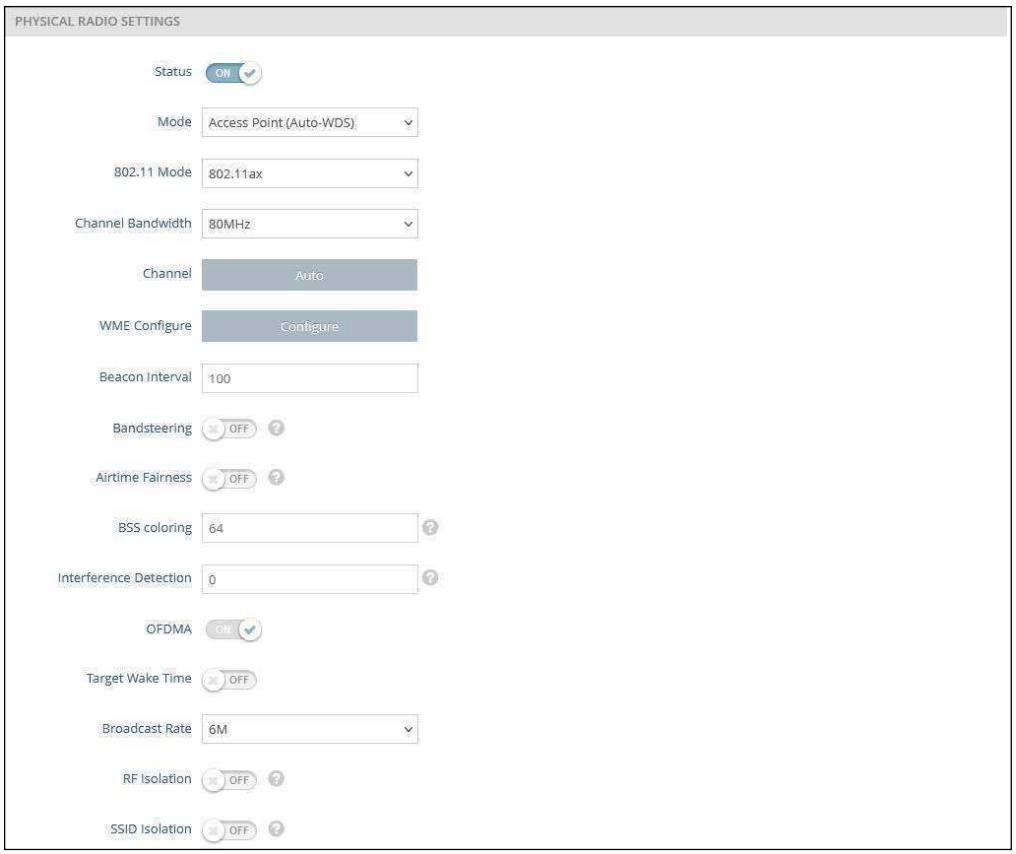
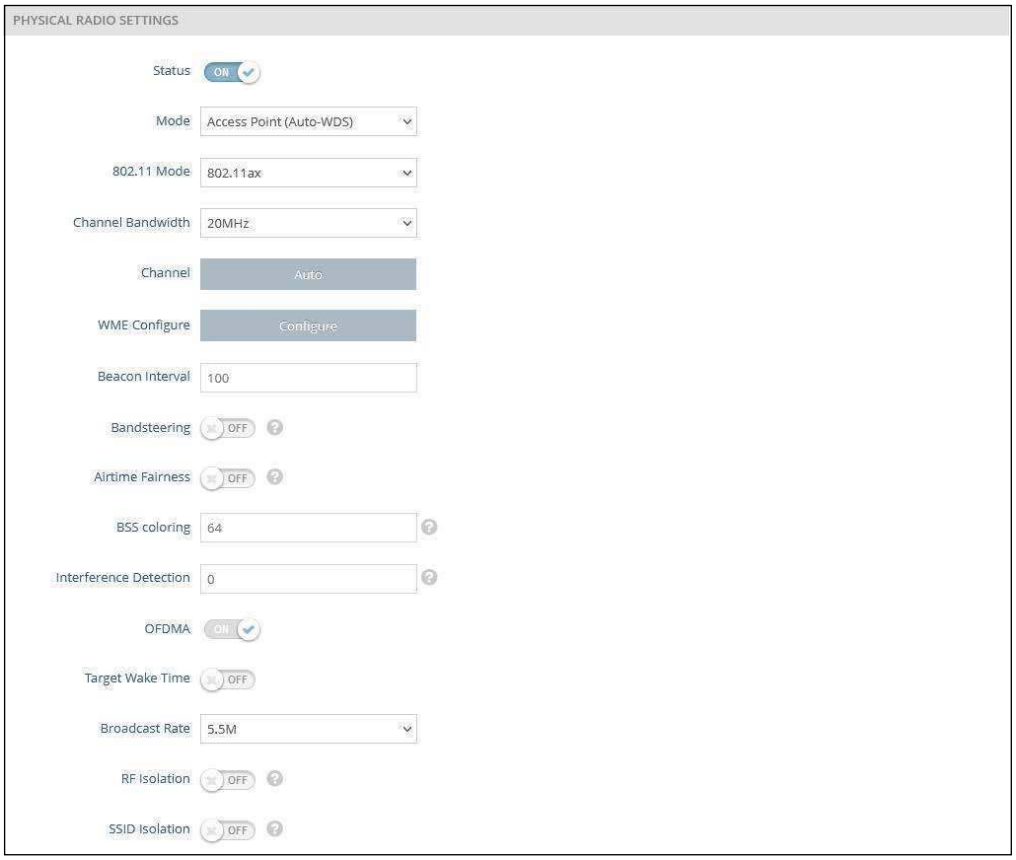


Figure 42: Physical Settings for Radio 2.4 GHz



The following items are displayed on this page:

- **Status** — Enables or disables the wireless service on this interface.
- **Mode** — Selects the mode in which the AP will function.
  - **Access Point (Auto-WDS)** — The AP operates as an access point in WDS mode, which accepts connections from APs in Client WDS mode. (This is the default setting.)

    In this mode, the AP provides services to clients as a normal access point. WDS is used to automatically search for and connect to other AP nodes using the same SSID and security settings.
  - **Client** — The AP can provide a wireless connection to another AP, as well as pass information from or to locally wired hosts and wireless clients.
- **802.11 Mode** — Defines the radio operation mode.
  - **Radio 2.4 GHz** — Default: 11ax; Options: 11b+g+n/ax
  - **Radio 5 GHz** — Default: 11ax; Options: 11a, 11a+n, 11ac+a+n, 11ax

- **Channel Bandwidth** — The AP options for channel bandwidth include 20, 40 80, and 160 MHz. The available channel bandwidth is dependent on the 802.11 Mode. (Default: 20 MHz on 2.4 GHz Radio, 80 MHz on 5 GHz Radio; Options: 20 MHz, 40 MHz, 80MHz, 160MHz)
  - **20MHz** — For 802.11b+g+n and 802.11ax
  - **40MHz** — For 802.11b+g+n, 802.11a, 802.11a+n, 802.11ac+a+n and 802.11ax
  - **80MHz** — For 802.11ac+a+n and 802.11ax
  - **160MHz** — (Supported only on EAP104, EAP111, and OAP101 5 GHz radio) For 802.11ac+a+n and 802.11ax
- **Channel** — The radio channel that the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, for 11g/n 20 MHz mode you can deploy up to three access points in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the access point to which it is linked. (The available channels are dependent on the 802.11 Mode, Channel Bandwidth, and Country Code settings.)

  Selecting Auto enables the access point to automatically select an unoccupied radio channel. (Default: Auto)
- **WME Configuration** — Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features for IEEE 802.11 networks. Access priority can be configured for four "Access Category"(AC) types using the following parameters:
  - **CW Min (Minimum Contention Window)** – The initial upper limit of the random backoff wait time before wireless medium access can be attempted. The initial wait time is a random value between zero and the CWMin value. Specify the CWMin value in the range 0-15 microseconds. Note that the CWMin value must be equal or less than the CWMax value.
  - **CW Max (Maximum Contention Window)** – The maximum upper limit of the random backoff wait time before wireless medium access can be attempted. The contention window is doubled after each detected collision up to the CWMax value. Specify the CWMax value in the range 0-15 microseconds. Note that the CWMax value must be greater or equal to the CWMin value.
  - **AIFS (Arbitration Inter-Frame Space)** – The minimum amount of wait time before the next data transmission attempt. Specify the AIFS value in the range 0-15 microseconds.

  - **TXOP Limit (Transmit Opportunity Limit)** – The maximum time an AC transmit queue has access to the wireless medium. When an AC queue is granted a transmit opportunity, it can transmit data for a time up to the TXOP Limit. This data bursting greatly improves the efficiency for high data-rate traffic. Specify a value in the range 0-8192 microseconds.

- **Beacon Interval** — The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They also carry power-management and other information. (Range: 100-1024 TUs; Default: 100 TUs)

- **Bandsteering** — When enabled, clients that support 2.4 GHz and 5 GHz are first connected to the 5 GHz radio. This feature helps balance the client load over the two radio bands. Note that both radios must have configured SSIDs and security settings that match for this feature to fully operate. (Default: Off)

- **Airtime Fairness** — Enabling this feature improves the overall performance of the wireless network. (Default: Disabled)

- **BSS coloring** — In 802.11ax (Wi-Fi 6) mode, BSS coloring allows nearby APs operating at the same frequency to identify traffic belonging to their own Basic Service Set (BSS). The BSS coloring enables Wi-Fi 6 networks to operate more efficiently in high-density environments where neighboring AP and client transmissions overlap. Assign a color value (a number from 1 to 63) to identify the radio BSS, or enter value 64 to allow the AP to randomly select a color value. (Range: 1-63, 64 random; Default: 64)

- **Interference Detection** — When the utilization in current channel reaches the configured threshold (as a percentage), the AP switches to a different channel. (Range: 0 - 100%; Default: 0, disabled)

- **OFDMA** — The 802.11ax (Wi-Fi 6) mode supports Orthogonal Frequency Division Multiple Access (OFDMA) and this cannot be disabled.

- **Target Wake Time** — In 802.11ax (Wi-Fi 6) mode, the AP can allow clients to request a specific Target-Wakeup Time (TWT) to transmit or receive frames, rather than rely on periodic beacons. This feature enables client devices to have much longer sleep states and results in significant power savings. In addition, the AP can control and schedule client TWTs to both manage contention in the network and accommodate delay-sensitive traffic. (Default: Disabled)

- **Broadcast Rate** — Allows a limit to be placed on the wireless bandwidth consumed by broadcast packets.

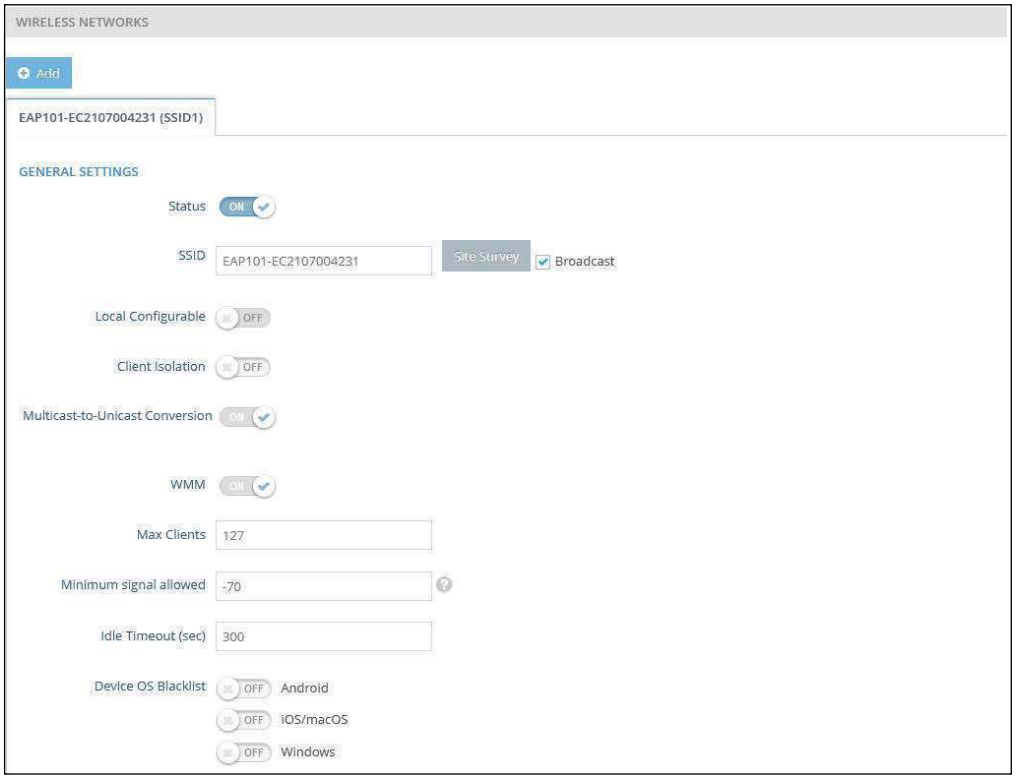
  - **Radio 2.4 Ghz** — Options: 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 5.5M

  - **Radio 5 Ghz** — Options: 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 6M

- **RF Isolation** — When enabled, clients are isolated between different radio cards.
- **SSID Isolation** — When enabled, clients are isolated between different SSIDs on the same radio cards.

Wireless Networks — General Settings

Figure 43: Radio Settings (General Settings)



The following items are displayed in this section of the Wireless Settings page:

- **Status** — Enables or disables the wireless service on this VAP.
- **SSID** — The name of the basic service set provided by a Virtual Access Point (VAP) interface. Clients that want to connect to the network through the access point must set their SSID to the same as that of the access point's VAP interface. (Default: Edgecore5G-# (where # is 1-16) for 5 GHz, Edgecore2.4G-# (where # is 1-16) for 2.4 GHz; Range: 1-32 characters)
- **Site Survey** — Scans for all wireless networks that are broadcasting their SSID.
- **Broadcast** — The SSID can be broadcast at regular intervals so that wireless stations searching for a network connection can discover it. This allows wireless clients to dynamically discover and roam between WLANs. This feature also makes it easier for hackers to break into your home network. Because SSIDs are not encrypted, it is easy to grab one by snooping the WLAN looking for SSID broadcast messages coming from the AP. (Default: Enabled)

- **Local Configurable** — Enables the SSID to be user configurable when the system is operating in MSP mode (see "System Settings" on page 83). (Default: Disabled)
- **Client Isolation** — When enabled, wireless clients can talk to the LAN, and reach the Internet if such connection is available, but they cannot communicate with one another. (Default: Disabled)
- **Multicast-to-Unicast Conversion** — When enabled, the AP converts multicast traffic to unicast traffic and sends it to each associated client. This feature provides a network throughput enhancement, since the AP transmits multicast traffic at a low basic rate, whereas unicast traffic can be transmitted at HT, VHT, or HE rates.
- **Max Clients** — The maximum number of clients that can associate to this SSID at the same time. (Default: 127; Range: 1-256)
- **Minimum signal allowed** — Only allows clients to connect to the radio interface if their signal strength (RSSI) is equal or greater than the specified value. Setting the value to -100 disables this feature. Clients already connected are checked periodically. (Range: -1 to -100; Default: -100)

  This forces clients to associate with an AP that has a better signal strength (also called assisted roaming). Suggested value is -70 to -80 depending on access point density and coverage.
- **Idle Timeout (sec)** — The AP disconnects a client when there is no activity for the configured amount of time. (Default: 300 seconds; Range: 60-60000 seconds)
- **Device OS Blacklist** — Denies access to the SSID from client devices with either Android, iOS/macOS, or Windows operating systems. Set to ON to prevent a client OS from connecting to the SSID. Set to OFF to allow a client OS to connect to the SSID.

Wireless Networks — Security Settings

Figure 44: Wireless Security Settings

The following items are displayed in this section of the Wireless Settings page:

- **Method** — Sets the wireless security method for each VAP, including association mode, encryption, and authentication. (Default: WPA2-PSK)
  - **No Security** — The VAP broadcasts a beacon signal including the configured SSID. Wireless clients with an SSID setting of "any" can read the SSID from the beacon and automatically set their SSID to allow immediate connection.
  - **WPA-PSK** — For enterprise deployment, WPA requires a RADIUS authentication server to be configured on the wired network. However, for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access. The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the access point and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks.
    - **Encryption** — Data encryption uses one of the following methods:
      - **CCMP (AES)** — AES-CCMP is used as the multicast encryption cipher. AES-CCMP is the standard encryption cipher required for WPA2. (This is the default setting.)
      - **Auto: TKIP + CCMP (AES)** — The encryption method used by the client is discovered by the access point.
    - **Key Method** — Uses one of the following PSK methods:
      - **Single PSK** — Enables the entry of a single PSK key.
        - **Key** — WPA is used to encrypt data transmitted between wireless clients and the VAP. WPA uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

          String length must be 8 to 63 ASCII characters (letters and numbers). No special characters are allowed.
      - **Multiple PSK** —Enables the entry of multiple PSK keys. Up to 128 keys can be configured.
        - **Multiple Keys** — Enter multiple keys, one per line. Entering a key with a specific MAC address limits the key for use by a single client. Entering a key without a MAC address enables the key to be used by all clients.

Multiple keys are supported for WPA-PSK, WPA2-PSK, and WPA3 Personal Transition security.

- **Dynamic PSK** — Enables the use of dynamic PSK keys that are periodically generated and updated by a RADIUS authentication server. The RADIUS server IP address, UDP port, and secret text string must be specified. (See "RADIUS Settings" below for details.)

  Dynamic keys are supported only for WPA2-PSK security.

- **WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication.

  WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

  Refer to WPA-PSK for a description of encryption methods and the key.

- **WPA-EAP** — WPA employs a combination of several technologies to provide an enhanced security solution for 802.11 wireless networks. A RADIUS server is used for authentication, and can also be used for accounting.

  Refer to WPA-PSK for a description of encryption methods.

- **RADIUS Settings** — A RADIUS server must be specified for the access point to implement IEEE 802.1X network access control and Wi-Fi Protected Access (WPA) wireless security.

  In addition, you can configure a RADIUS Accounting server to receive user-session accounting information from the access point. RADIUS Accounting can be used to provide valuable information on user activity in the network.

Note: This guide assumes that you have already configured RADIUS server(s) to support the access point. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

  - **Radius Auth Server** — Specifies the IP address or host name of the RADIUS authentication server.

  - **Radius Auth Port** — The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)

- **Radius Auth Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS authentication server. Do not use blank spaces in the string. (Maximum length: 255 characters)

- **NAS ID** — The RADIUS NAS identifier for the SSID interface This value must be between 1 and 48 characters long.

- **Backup Radius Auth** — Enables the support of a backup RADIUS authentication server.

  - **Radius Auth Server** — Specifies the IP address or host name of the backup RADIUS authentication server.

  - **Radius Auth Port** — The UDP port number used by the backup RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)

  - **Radius Auth Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the backup RADIUS authentication server. Do not use blank spaces in the string. (Maximum length: 200 characters)

- **Use Radius Accounting** — Enables the support of a RADIUS accounting server.

  - **Acct Server** — Specifies the IP address or host name of the RADIUS accounting server.

  - **Acct Port** — The UDP port number used by the RADIUS server for accounting messages. (Range: 1024-65535; Default: 1813)

  - **Acct Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS accounting server. Do not use blank spaces in the string. (Maximum length: 200 characters)

  - **Acct Interim Interval** — The time (in seconds) between each accounting update sent to the server. (Range: 60-600 seconds; Default: 60 seconds)

- **WPA2-EAP** — WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

A RADIUS server is used for authentication, and can also be used to accounting.

Refer to WPA-PSK for a description of encryption methods.

Refer to WPA-EAP for a information on configuring the RADIUS server.

- **WPA3 Personal** — Clients using WPA3 with Simultaneous Authentication of Equals (SAE) are accepted for authentication.

  WPA3 provides more robust password-based authentication called Simultaneous Authentication of Equals (SAE), which replaces Pre-Share Key (PSK) in WPA2-Personal. This technology prevents offline dictionary attacks so that data traffic can be transmitted securely.

- **WPA3 Personal Transition** — Clients using WPA3 with SAE or clients using WPA2 with PSK are accepted for authentication. The AP negotiates the supported authentication and encryption with each client before allowing access to the network.

- **WPA3 Enterprise** — An enhanced version of WPA2-EAP security that uses more robust encryption. Clients must support one of the stronger WPA3 encryption options and use Protected Management Frames (PMF) to be able to access the network. The use of IEEE 802.1X network access control and a RADIUS server is required.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **WPA3 Enterprise Transition** — Allows WPA3 and WPA2 clients to access the network. Encryption options and the use of Protected Management Frames (PMF) are negotiated with each client before allowing access to the network.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **WPA3 Enterprise 192-bit** — WPA3 Enterprise security uses a standard 128-bit encryption. For a network handling more sensitive data, there is an option to use 192-bit encryption for additional protection.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **OWE** — Opportunistic Wireless Encryption (OWE) is the WPA3 open network security that allows users of public Wi-Fi networks to gain secure access without using a password. OWE provides individual encryption of data communications between the AP and each client, but does not provide authentication of user identities.

- **PMF** — Protected Management Frames (PMF) provide WPA2/WPA3 security for unicast and multicast management frames between the AP and clients. The "Optional" setting allows clients that do not support PMF to access the network.

The "Mandatory" setting allows only clients that support PMF to access the network. (Default: Optional)

- **802.11k** — Provides clients with information on neighbor APs when roaming. As a client is about to roam from an AP, it sends a request for a "Neighbor Report" that includes a list of available APs and associated information. The client can then quickly identify the best AP to which it can roam without having to scan all channels. (Default: Disabled)

- **802.11r** — Provides a method for fast transition roaming between APs. Before clients roam to a new AP, the initial handshake and encryption calculations are performed in advance, which results in a fast hand off without the need for re-authentication. (Default: Disabled)

- **802.11v** — Provides information to associated clients that facilitates the overall improvement of the wireless network. Also helps clients to improve battery life by setting the idle period. (Default: Disabled)

- **Radius MAC Auth** — The MAC address of the associating station is sent to a configured RADIUS server for authentication. (Default: Disabled)

- **Dynamic Authorization** — The Dynamic Authorization Extensions (DAE) to RADIUS enable a server to disconnect or change the authorization of clients that are already connected to the network. (Default: Disabled)

  - **DAE Port** — The UDP port number to use for DAE messages. (Default: 3799)

  - **DAE Client** — Specifies the IPv4 address of the RADIUS server.

  - **DAE Secret** — The shared text string used to encrypt DAE messages between the access point and the RADIUS server.

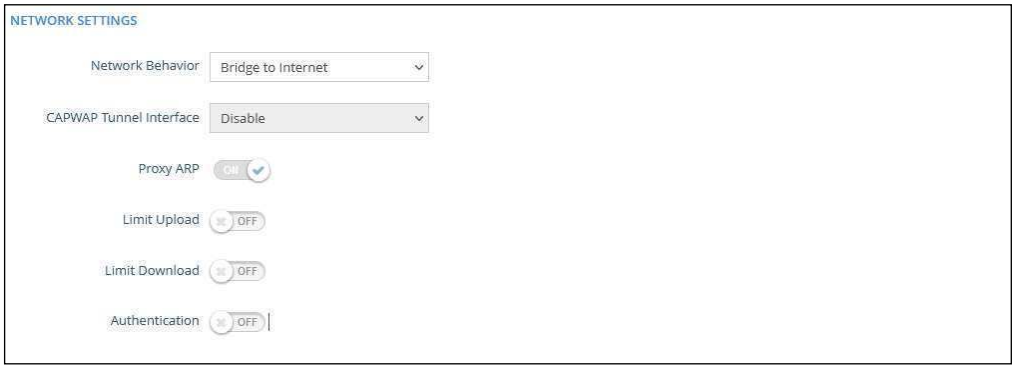
- **Access Control List** — Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point. (Default: OFF)

  - **Policy** — The MAC list can be configured to either allow or deny network access to specified clients. (Default: Allow all MACs on list)

  - **Filtered MACs** — List of client MAC addresses. Up to 512 MAC addresses can be configured.

Wireless Networks — Network Settings

Figure 45: Wireless Network Settings



The following items are displayed in this section of the Wireless Settings page:

- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
  - **Bridge to Internet** — Configures an interface as attached to the WAN. Traffic from this interface is directly bridged into the Internet. (See Figure 29, "Bridge to Internet", on page 48.)
  - **Route to Internet** — Configures an interface as a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged to the Internet. (See Figure 30, "Route to Internet", on page 48.)
    - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.
  - **Add to Guest Network** — This interface can only support the guest network.
  - **Hotspot Controlled** — This interface can only support hotspot services.
    - **Configure Hotspot** — Opens Hotspot Settings page.
    - **Walled Garden** — Configures the Walled Garden list on the Hotspot Settings page.
  - **VLAN Tag Traffic** — Tags any packets passing from this VAP (virtual access point) to the associated Ethernet port with a VLAN ID configured under "VLAN Settings" on page 80.
    - **VLAN Id** — Selects the configured VLAN ID with which to tag the VAP traffic.
    - **VLAN Settings** — Opens the VLAN Settings page.

- **Dynamic VLAN** — The RADIUS server provides the access point with the user VLAN information. The access point assigns the associated user to the related VLAN.
  - **Default VLAN Behavior** — Specifies the behavior (Accept or Reject) when a client's VLAN ID is not defined on the RADIUS server. The default setting is Reject.
    - **Reject** — A client cannot connect to the SSID when the client's VLAN ID is not defined on the RADIUS server.
    - **Accept** — A client can connect to the SSID with an assigned or untagged VLAN ID when the client's VLAN ID is not defined on the RADIUS server.

- **CAPWAP Tunnel Interface** — When the AP system management is set to EWS-Series Controller mode (see "System Settings" on page 83), the CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode can be configured. The options are "Disable," "Complete," or "Split." A Complete tunnel sends all management, authentication, and data traffic from the AP back to the controller. A Split tunnel only sends the management and authentication traffic to the controller. (Default: Disable)

- **Proxy ARP** — When Proxy ARP is enabled, the AP maintains its own ARP lookup table and replies to ARP requests on behalf of downstream stations, avoiding network inefficiencies. This feature is automatically enabled when client isolation is disabled, and disabled when client isolation is enabled. The feature cannot be configured manually. Proxy ARP is supported when the network behavior is "Bridge to Internet" or "VLAN Tag Traffic."

- **Limit Upload** — Enables rate limiting of traffic from the VAP interface as it is passed to the wired network. You can set a maximum rate in Kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

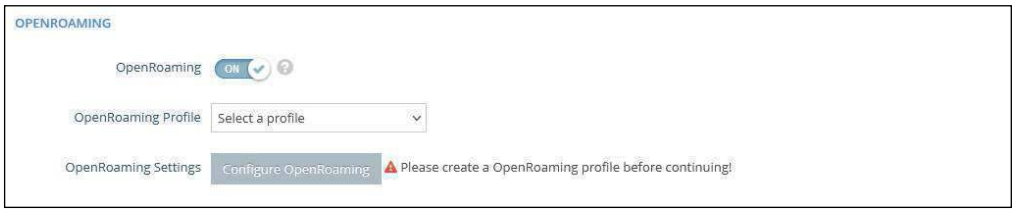
- **Limit Download** — Enables rate limiting of traffic from the wired network as it is passed to the VAP interface. You can set a maximum rate in kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

- **Authentication** — When the AP system management is set to ecCLOUD mode (see "System Settings" on page 83), this options authenticates the AP communications with the ecCLOUD controller. (Default: Disabled)

Wireless Networks — OpenRoaming

Available when WPA2-EAP security is selected, OpenRoaming (Hotspot 2.0) provides a standard for public-access Wi-Fi networks to support seamless roaming between wireless networks. A OpenRoaming AP advertises its public Wi-Fi capabilities and services so that clients can decide if they want to connect to the network.

Figure 46: OpenRoaming Settings



The following items are displayed in this section of the Wireless Settings page:

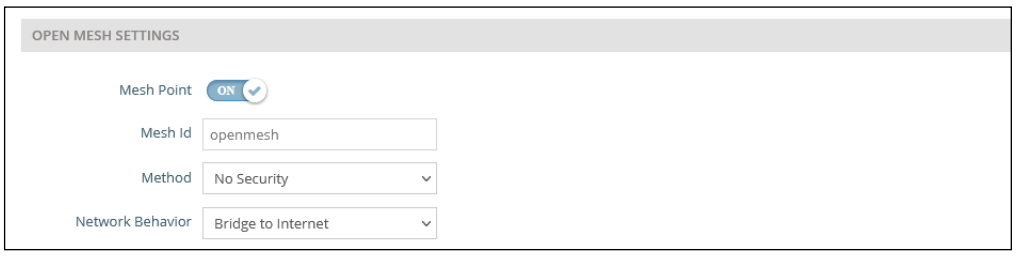
- **OpenRoaming** — Enables OpenRoaming when WPA2-EAP security is selected. (Default: Disabled)
- **OpenRoaming Profile** — Selects the profile to apply to the wireless network. See "OpenRoaming" on page 58 for profile configuration.
- **OpenRoaming Settings** — Click to access the OpenRoaming profile settings page. See "OpenRoaming" on page 58 for profile configuration.

Wireless Networks — Open Mesh Settings

Open Mesh is a network of interconnected node APs, of which only one has a wired connection to the network (and the Internet). The other AP nodes provide wireless links to each other and some support connections to wireless clients. The mesh network not only extends wireless connectivity over a greater distance, but also provides backup links should one node in the network fail.

When setting up an AP to be a node in a mesh network, select one radio interface (2.4 GHz or 5 GHz) and configure it to operate on a specific channel (do not select Auto).Set up other AP nodes to operate on the same radio interface, channel, and with the same SSID.

Figure 47: Open Mesh Settings



The following items are displayed in this section of the Wireless Settings page:

- **Mesh Point** — Enables Open Mesh support on the SSID interface.

- **Mesh ID** — Name of the mesh network.
- **Method** — Security applied on Open Mesh links.
  - **No Security** — None.
  - **WPA3-Personal** — Uses WPA3 with Simultaneous Authentication of Equals (SAE) on mesh links to other APs.
- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
  - **Bridge to Internet** — Configures an interface as attached to the WAN. Traffic from this interface is directly bridged into the Internet. (See Figure 29, "Bridge to Internet", on page 48.)
  - **Route to Internet** — Configures an interface as a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged to the Internet. (See Figure 30, "Route to Internet", on page 48.)
    - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.

Wireless Networks — Advanced Radio Settings

Figure 48: Advanced Radio Settings

The following items are displayed in this section of the Wireless Settings page:

- **Tx Power** — Adjusts the power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the AP model and the Country setting.)
- **SGI** — Enables the Short Guard Interval (SGI) in the following 802.11 modes:
  5 GHz radio; 802.11a, 802.11a+ n, 802.11ac+a+n.
  2.4 GHz radio; 802.11 b g+ n.

  The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns Short Guard Interval is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to

propagation delays, echoes, and reflections to which digital data is normally very sensitive. Enabling SGI sets it to 400ns. (Default: Disabled)

VLAN Settings

VLANs (virtual local area networks) are turned off by default. If turned on they will automatically tag any packets passed to the LAN port from the relevant VAP (virtual access point).

The access point can employ VLAN tagging to control access to network resources and increase security. VLANs separate traffic passing between the access point, associated clients, and the wired network. You can create up to 16 VLAN tagged networks.

Note the following points about the access point's VLAN support:

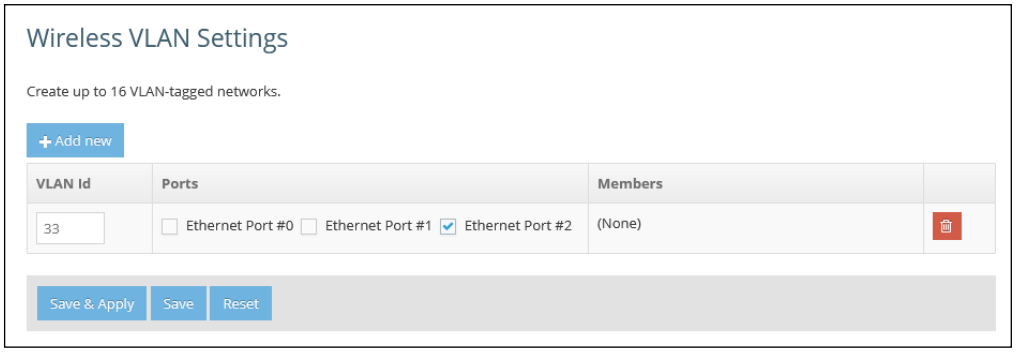
- If an Ethernet LAN port on the access point is assigned a VLAN ID, any traffic entering that port must be also tagged with the same VLAN ID.
- Wireless clients associated to the access point can be assigned to a VLAN. Wireless clients are assigned to the VLAN for the VAP interface with which they are associated. The access point only allows traffic tagged with correct VLAN IDs to be forwarded to associated clients on each VAP interface.
- When VLAN support is enabled on the access point, traffic passed to the wired network is tagged with the appropriate VLAN ID. When an Ethernet port on the access point is configured as a VLAN member, traffic received from the wired network must also be tagged with the same VLAN ID. Received traffic that has an unknown VLAN ID or no VLAN tag is dropped.
- When VLAN support is disabled, the access point does not tag traffic passed to the wired network and ignores the VLAN tags on any received frames.
- Network IP range conflict detection and resolution — The AP has two built-in local networks - one "main" network, and the more secure "guest" network. By default, the subnet ranges of these networks is set to 192.168.2.1 and 192.168.3.1, respectively.

  If your network is already configured to use one of these subnets, when you plug in your network cable to the WAN port of your AP, there would normally be an IP conflict in the local AP's network and your upstream network.

  However, if your WAN subnet conflicts with any of the local networks (even the custom ones you create), the AP will automatically change the subnet of the local network.

Note: Before enabling VLAN tagging on the access point, be sure to configure the attached network switch port to support tagged VLAN frames for the VLAN IDs configured on the access point. Otherwise, connectivity to the access point will be lost when you enable the VLAN feature.

Figure 49: Configuring VLANs



The following items are displayed on this page:

- **VLAN ID** — A VLAN identifier to be assigned. (Range: 2-4094) (VLANs 1 is reserved for internal use.)
- **Ports** — The Ethernet ports assigned to the specified VLAN.
- **Members** — The SSID of a VAP configured to be a member of the specified VLAN. This option is configured under Radio Settings (Network Settings – Network Behavior).

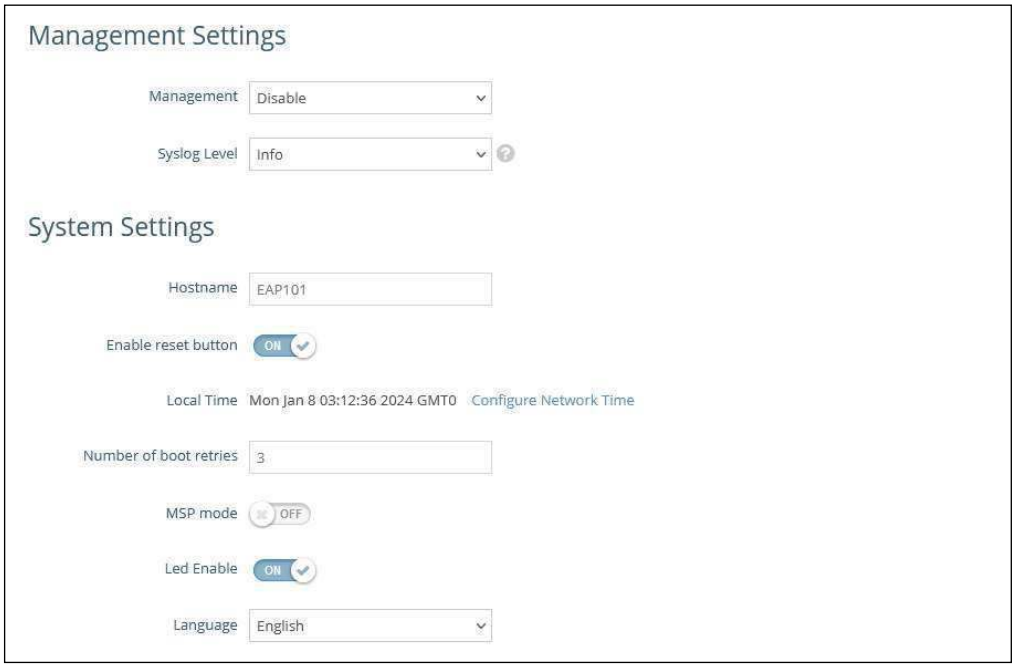
5 System Settings

This chapter describes maintenance settings on the access point. It includes the following sections:

System Settings

The System Settings page can be used to enable the AP to be managed from the Edgecore ecCLOUD controller or EWS-Series Controller, and configure general descriptive information about the AP.

Figure 50: System Settings



The following items are displayed on this page:

- **Management** — Set to "ecCLOUD" to manage this AP from the Edgecore ecCLOUD controller. Set to "EWS-Series Controller" to manage this AP from an Edgecore EWS-Series controller in the local network. Set to disable to manage the AP through the web interface in a stand-alone mode.
  - **ecCLOUD** — When selected, the following parameters are displayed:
    - **Controller URL** — Provides a URL link to the Edgecore ecCLOUD controller management site.
    - **Enable agent** — Enables the AP to be managed from the ecCLOUD controller.
      - **Registration URL** — Specifies the URL for device registration.
    - **Log Level** — Adjusts the system log level for the ecCLOUD daemon (mgmtd). The default value is Info. The standard ranking of log levels is as follows: Trace < Debug < Info < Warn < Error.

- **EWS-Series Controller** — When selected, the following parameters are displayed:
  - **CAPWAP** — Enables CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode.
  - **DNS SRV Discovery** — The AP uses DNS server records to discover the EWS controller to which it can send a CAPWAP join request.
    - **Domain Name Suffix** — Specifies the domain suffix of the controller.
  - **DHCP Option Discovery** — The AP uses the DHCP server to obtain an IP address in the same subnet as the EWS controller, which it can then discover and send a CAPWAP join request.
  - **Broadcast Discovery** — The AP sends broadcast requests to discover the EWS controller in the same subnet.
  - **Multicast Discovery** — The AP sends multicast discover packets across the network to find the EWS controller. This option requires routing paths to be properly configured in the network.
  - **Static Discovery** — Provides a manual method to reach an EWS controller by entering IP addresses that the AP uses to send a CAPWAP join request.
- **Syslog Level** — Limits system log messages based on severity. The standard ranking of log levels is as follows: Debug < Info < Notice < Warning < Error < Critical < Alert < Emergency. (Default: Info)
- **Hostname** — An alias for the AP, enabling the device to be uniquely identified on the network. (Default: EAP101; Range: 1-63 ASCII characters. Only accepts A-Z, a-z, 0-9, and dash "-".)
- **Enable Reset Button** — Enables the AP's hardware reset button. (Default: Enabled)
- **Local Time** — The local time, given as day of week, month, time, year.
- **Number of boot retries** — The maximum number of bootup retries before switching to the next boot bank. (Range: 1-254; Default: 3)
- **MSP Mode** — Enables the Managed Service Provider (MSP) mode that prevents end-users from accessing and modifying most device settings from user-defined user accounts. Management access from "root" and "admin" accounts still provide full access to all device settings. (Default: Disabled)

  With MSP mode enabled, service providers have the option of making specific wireless SSID settings available for user configuration by enabling the "Local

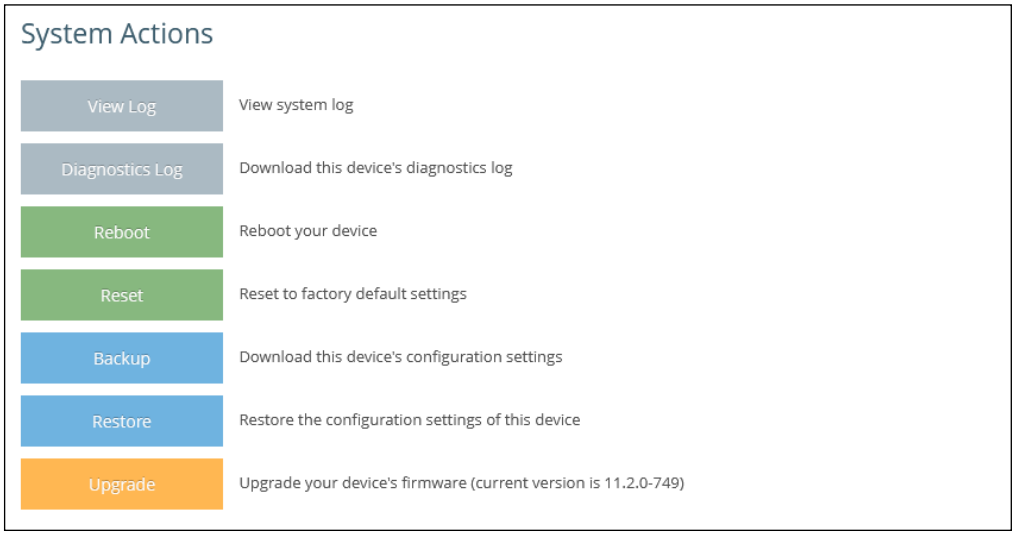
Configurable" setting. See "Wireless Networks — General Settings" on page 69.

- **LED Enable** — Enables the LED indicators on the AP. (Default: Enabled)
- **Language** — Selects the web interface language. (Options: English, Japanese; Default: English)

Maintenance

The Maintenance page supports general maintenance tasks including displaying the system log, downloading a diagnostics log, rebooting the device, restoring factory defaults, backing up or restoring configuration settings, and upgrading firmware.

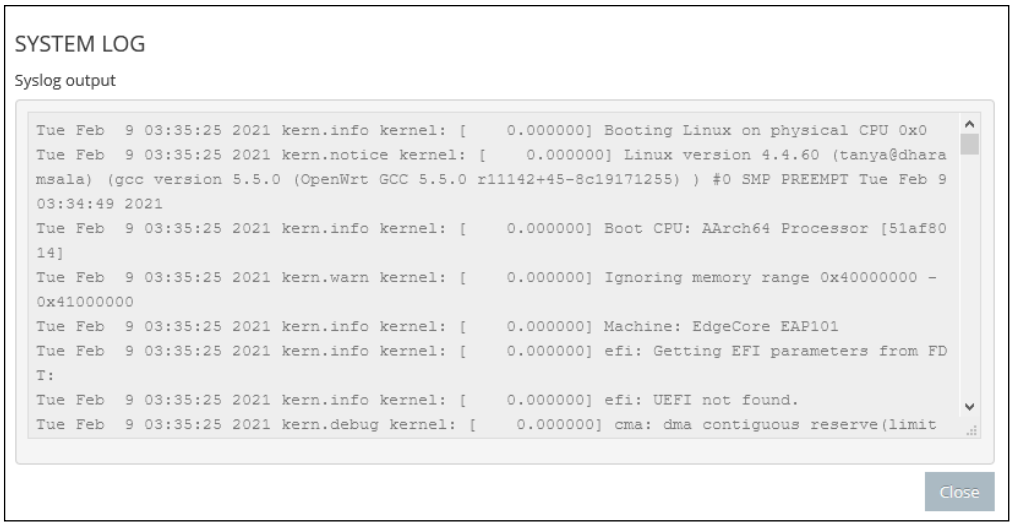
Figure 51: Maintenance



Displaying System Logs

The access point saves event and error messages to a local system log database. The log messages include the date and time, device name, message type, and message details.

Figure 52: System Log



Downloading the Diagnostics Log

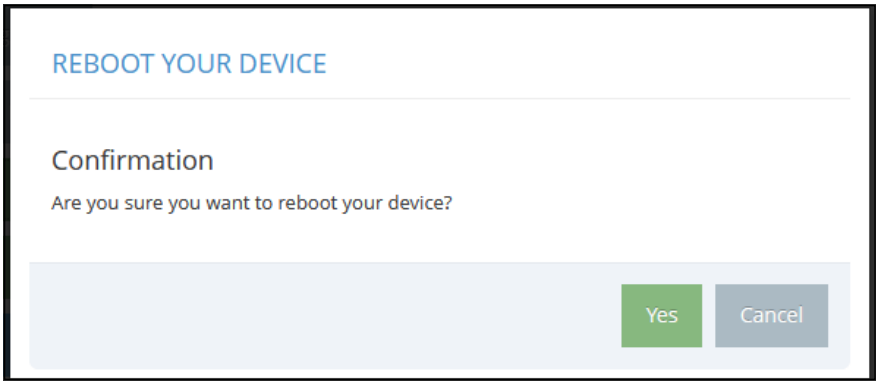
Click “Diagnostics Log” to download the log file to the management workstation. In Windows, a GNU Zip (*.tar.gz) file is stored in the Downloads folder.

The diagnostics log file contains information that can help Edgecore resolve technical issues with the AP.

Rebooting the Access Point

The Reboot page allows you to reboot the access point.

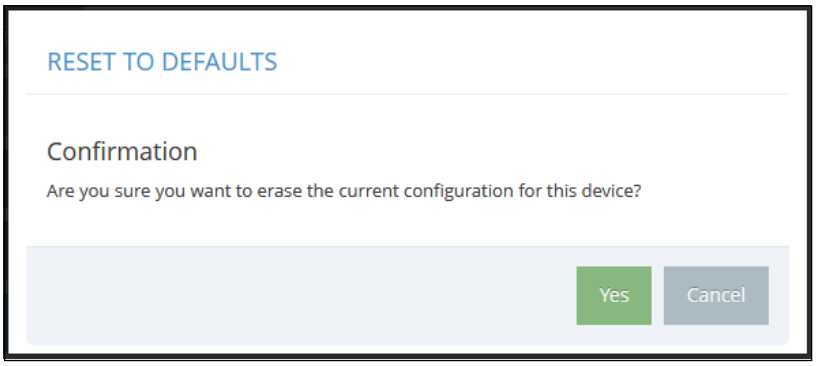
Figure 53: Rebooting the Access Point



Resetting the Access Point

The Reset page allows you to reset the access point to the factory defaults. Note that all user configured information will be lost. You will have to re-enter the default user name and password to re-gain management access to this device.

Figure 54: Resetting to Defaults



Note: It is also possible to reboot or reset the access point by inserting a pin in the pin hole labeled "Reset" on the connector panel of the access point and:

- give a quick press to reboot the access point;
- press and hold for 5 seconds to reset the access point to factory defaults.

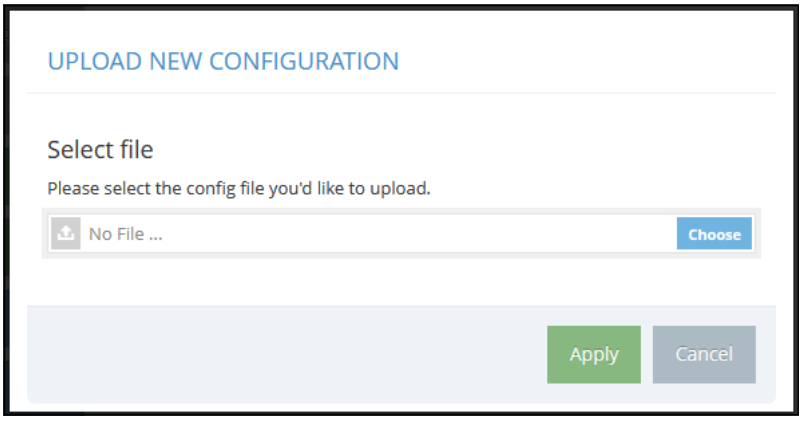
Backing Up Configuration Settings

The Backup function allows you to back up the access point's configuration to a management workstation. In Windows, a GNU Zip (*.tar.gz) file will be stored in the Downloads folder. This is a sample file name: backup-EAP101-2021-02-09.tar.gz

Restoring Configuration Settings

The Restore page allows you to upload configuration settings from a management workstation. The specified file must be one that was previously backed up from the access point.

Figure 55: Restoring Configuration Settings



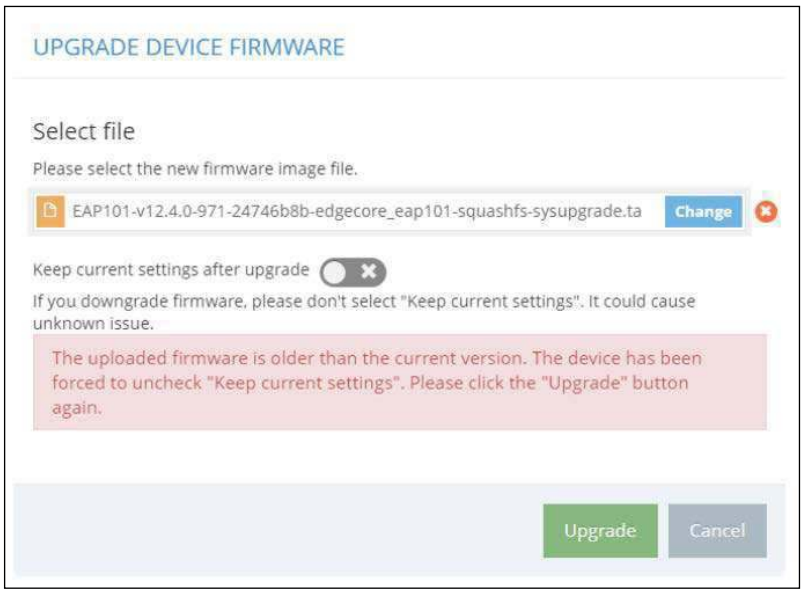
Upgrading Firmware

You can upgrade new access point software from a local file on the management workstation. New software may be provided periodically from Edgecore.

After upgrading new software, you must reboot the access point to implement the new code. Until a reboot occurs, the access point will continue to run the software it was using before the upgrade started. The access point supports dual software images, so if newly loaded software is corrupted, the alternate image will be used on the next reboot. Configuration settings are stored separately from the software, so the current settings will always be used for any new software. However, note that if the current configuration settings are corrupted, the system defaults will be used.

Note: If the uploaded firmware is older than the current version, the device forces the "Keep current settings after upgrade" option to unchecked.

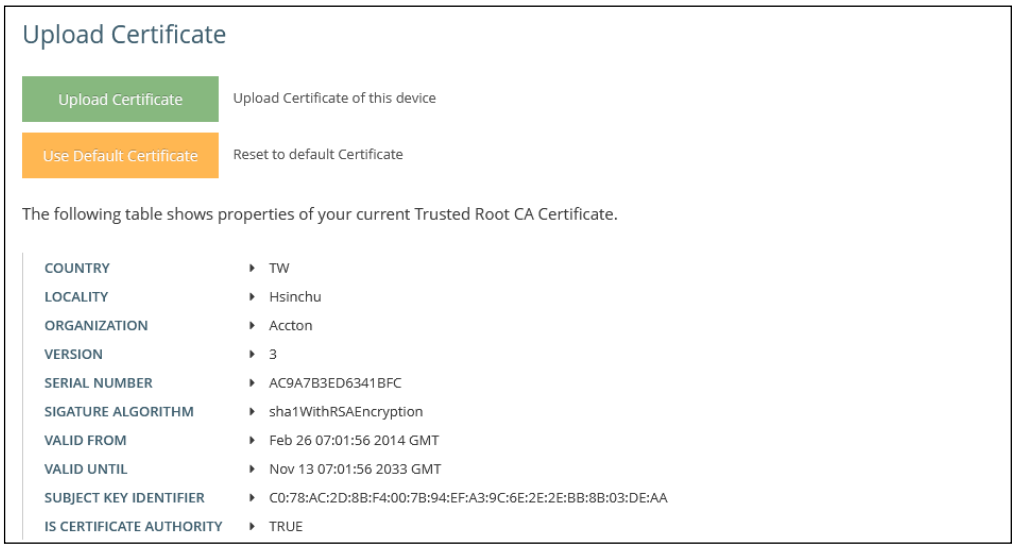
Figure 56: Upgrading Firmware



Upload Certificate

The Upload Certificate page allows you to upload a unique security certificate from a trusted certification authority for secure access (an encrypted connection) to a configured HTTPS captive portal. Alternatively, you can also reset to use the default certificate.

Figure 57: Upload Certificate



The following items are displayed on this page:

- **Upload Certificate** — Click to upload a security certificate and private key from a trusted certification authority.
- **Use Default Certificate** — Click to reset to use the AP's default certificate.

User Accounts

The User Accounts page allows you to control management access to the AP based on manually configured user names and passwords.

Figure 58: User Accounts

The following items are displayed on this page:

- **Enabled** — Click to enable or disable the user account.
- **Username** — The name of the user. (Range: 1-32 ASCII characters. Only accepts A-Z, a-z, 0-9, period ".", underscore "_", and hyphen "-". Usernames cannot begin with a hyphen "-" or period ".".)

- **Password** — The user password. (Range: 6-20 ASCII characters, case sensitive, no special characters)

Services

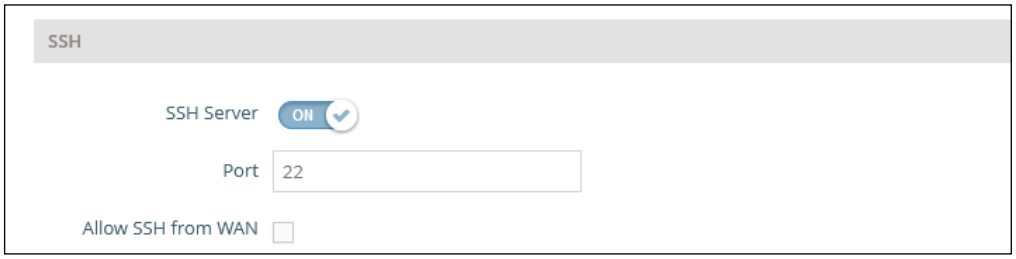
The Services page allows you to control SSH management access to the AP, configure NTP time servers, and configure iBeacon settings.

SSH

The Secure Shell (SSH) can act as a secure replacement for Telnet. The SSH protocol uses generated public keys to encrypt all data transfers passing between the access point and SSH-enabled management station clients and ensures that data traveling over the network arrives unaltered. Clients can then securely use the local user name and password for access authentication.

Note that SSH client software needs to be installed on the management station to access the access point for management via the SSH protocol.

Figure 59: SSH Settings



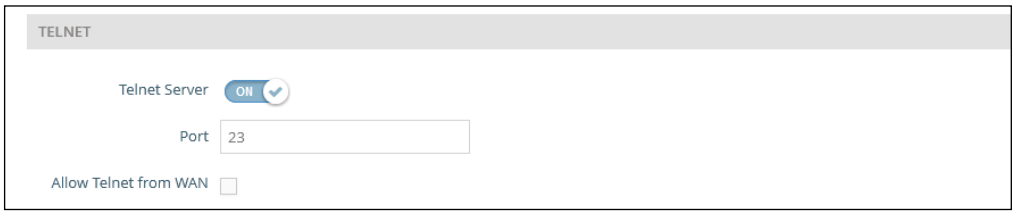
The following items are displayed on this page:

- **SSH Server** — Enables or disables SSH access to the access point. (Default: Enabled)
- **Port** — Sets the TCP port number for the SSH server on the access point. (Range: 1-65535; Default: 22)
- **Allow SSH from WAN** — Allows SSH management access from the WAN.

Telnet

Telnet is a remote management tool that can be used to configure the access point from anywhere in the network. However, note that Telnet is not secure from hostile attacks.

Figure 60: Telnet Server Settings



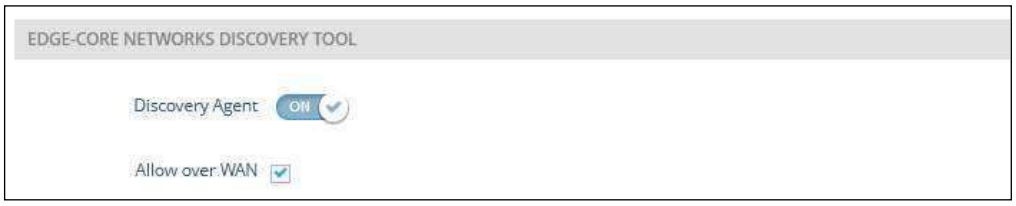
The following items are displayed on this page:

- **Telnet Server** — Enables or disables Telnet access to the access point. (Default: Enabled)
- **Port** — Sets the TCP port number for the Telnet server on the access point. (Range: 1-65535; Default: 23)
- **Allow Telnet from WAN** — Allows Telnet management access from the WAN.

Edgecore Networks Discovery Tool

The Discovery Tool agent enables the AP to find other Edgecore devices in the same Layer 2 network. See "Device Discovery" on page 99 to scan the network for devices.

Figure 61: Discovery Agent Settings



The following items are displayed on this page section:

- **Discovery Agent** — Enables the discovery agent. (Default: Enabled)
- **Allow over WAN** — Enables the discovery agent to operate over the port connected to the Internet source. (Default: Enabled)

Web Server

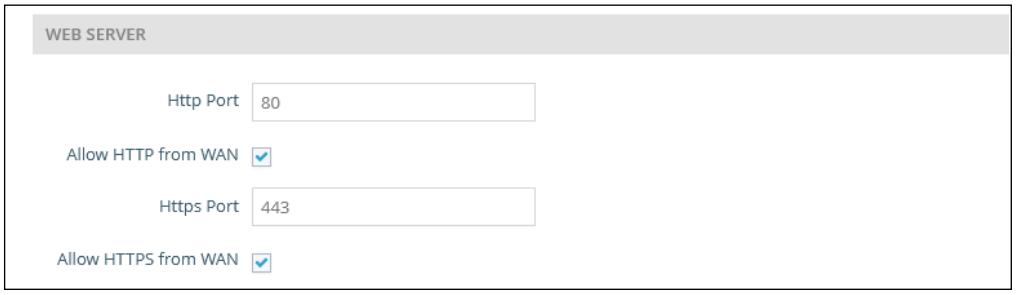
A Web browser provides the primary method of managing the access point. Both HTTP and HTTPS service can be accessed independently. If you enable HTTPS, you must indicate this in the URL: https://device:port_number]

When you start HTTPS, the connection is established in this way:

- The client authenticates the server using the server's digital certificate.

- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
- A padlock icon should appear in the status bar for most browsers.

Figure 62: Web Server Settings



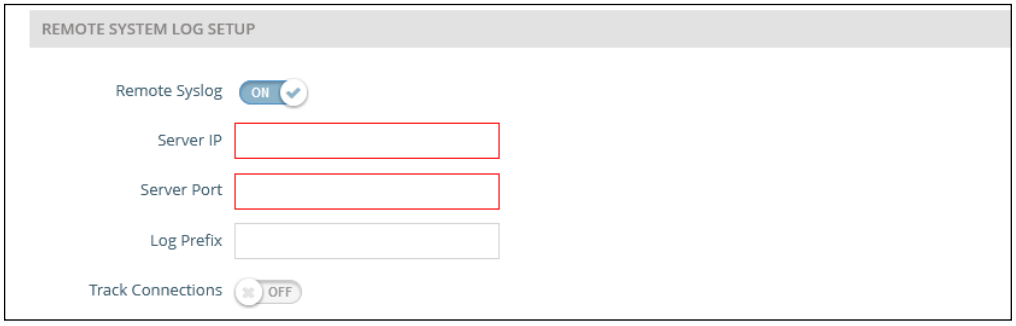
The following items are displayed on this page:

- **HTTP Port** — The TCP port to be used by the HTTP Web browser interface. (Range: 1-65535; Default: 80)
- **Allow HTTP from WAN** — Allows HTTP management access from the WAN.
- **HTTPS Port** — The TCP port to be used by the HTTPS Web browser interface. (Range: 1-65535; Default: 443)
- **Allow HTTPS from WAN** — Allows HTTPS management access from the WAN.

Remote System Log Setup

Use this feature to send log messages to a Syslog server.

Figure 63: Remote System Log Settings



The following items are displayed on this page:

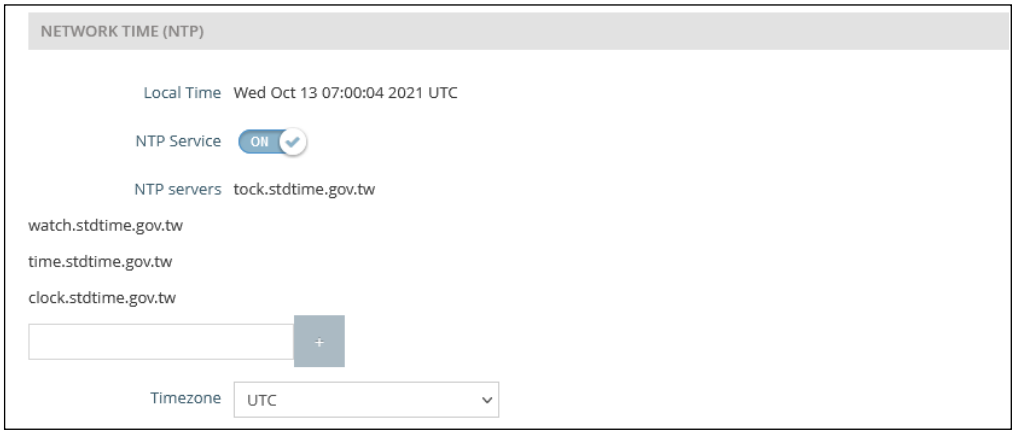
- **Remote Syslog** — Enables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Server IP** — Specifies the IP address of a remote Syslog server that will be sent log messages.
- **Server Port** — Specifies the UDP port number used by the remote Syslog server. (Range: 1-65535)
- **Log Prefix** — Sets a prefix string for log messages sent to the specified server. The prefix can help with sorting messages on the server.
- **Track Connections** — Enables the inclusion of connection information such as source IP and port, destination IP and port in log messages.

Network Time

Network Time Protocol (NTP) allows the access point to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the access point enables the system log to record meaningful dates and times for event entries. If the clock is not set, the access point will only record the time from the factory default set at the last bootup.

The access point acts as an NTP client, periodically sending time synchronization requests to specified time servers. The access point will attempt to poll each server in the configured sequence to receive a time update.

Figure 64: NTP Settings



The following items are displayed on this page:

- **Local Time** — Displays the local time as day of week, month, hour:minute:second, year, based on Universal Time Coordinates.
- **NTP Service** — Enables or disables sending of requests for time updates. (Default: Enabled)

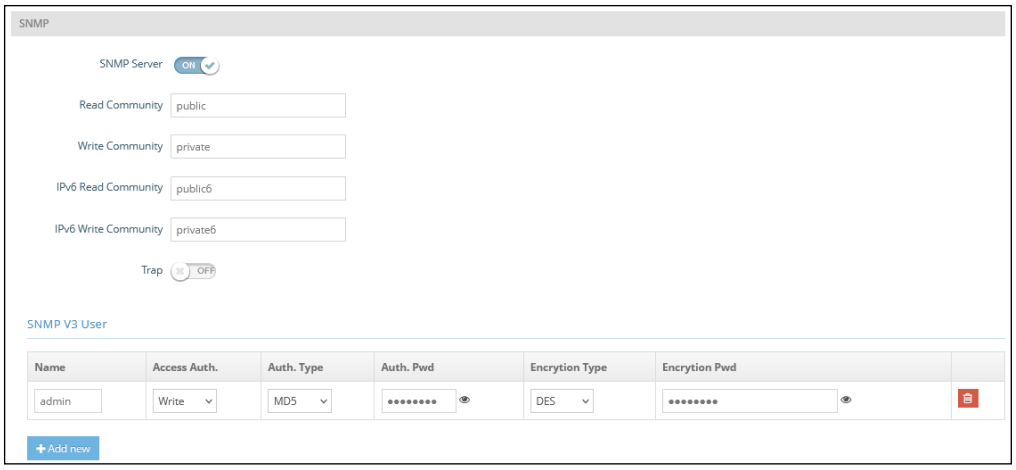
- **NTP Servers** — Sets the host names for time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence. To configure additional servers, click the "+" button to open a new edit field.

- **Timezone** — To display a time corresponding to your local time, choose one of the predefined time zones from the scroll-down list.

SNMP

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. It is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Figure 65: SNMP Settings



The following items are displayed on this page:

- **SNMP Server** — Enables or disables SNMP on the access point. (Default: Enabled)

- **Read Community** — A community string that acts like a password and permits read access to the access point's Management Information Base (MIB). (Range: 1-32 characters, case sensitive; Default: public)

- **Write Community** — A community string that acts like a password and permits write access to the access point's Management Information Base (MIB). (Range: 1-32 characters, case sensitive; Default: private)

- **IPv6 Read Community** — A community string for IPv6 read access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: public6)

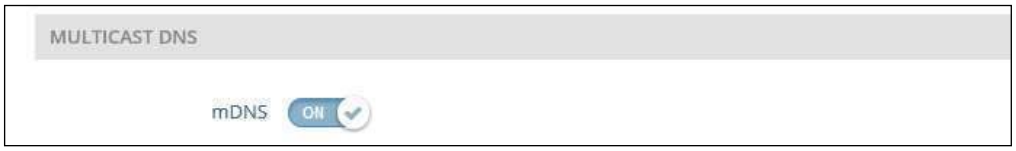
- **IPv6 Write Community** — A community string for IPv6 write access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: private6)

- **Trap** — Enables the sending of SNMP trap messages to a specified server. The access point sends the following trap messages: cold start, warm start, link up, and link down. (Default: Disabled)
  - **Server IP** — Specifies the IP address of the SNMP trap server that will be sent trap messages.
- **SNMPv3 User** — SNMP protocol version 3 provides secure access by account authentication and data encryption. An SNMP v3 user can be defined by clicking the "Add new" button.
  - **Name** — The user name used to access the SNMP service.
  - **Access Auth** — Select the access permission as "Read" or "Write."
  - **Auth Type** — Select the hash algorithm for authentication.
  - **Auth Pwd** — Configure the password for authentication.
  - **Encryption Type** — Select the encryption algorithm for data packets.
  - **Encryption Pwd** — Configure the password for data encryption.

Multicast DNS

The multicast DNS (mDNS) protocol is a zero-configuration service to facilitate connections within a local networks.

Figure 66: Multicast DNS Settings



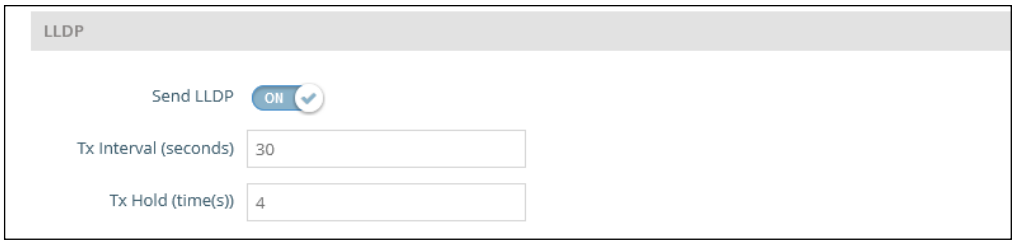
The following items are displayed on this page:

- **mDNS** — Enables or disables Multicast DNS on the access point. (Default: Enabled)

LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices in a network. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device.

Figure 67: LLDP Settings



The following items are displayed on this page:

- **Send LLDP** — Enables the sending of LLDP advertisements about the AP to neighboring devices in the network. (Default: Disabled)
- **Tx Interval (seconds)** — Sets the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)
- **Tx Hold (time(s))** — Configures a time-to-live (TTL) value sent in the LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

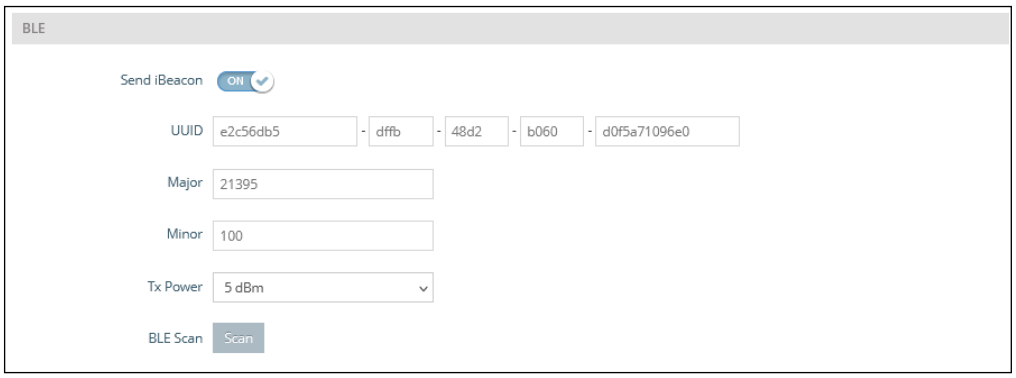
  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending device if it does not transmit updates in a timely manner.

  The TTL in seconds is based on the following rule:
  minimum value ((Tx Interval * Tx Hold), or 65535)
  Therefore, the default TTL is 4*30 = 120 seconds.

BLE

The AP supports the iBeacon standard based on Bluetooth Low Energy (BLE). Devices with BLE Beacons can provide location-based services to BLE clients, such as phones, that can recognize the beacon advertisements, extract the provided information, and then take actions based on the content.

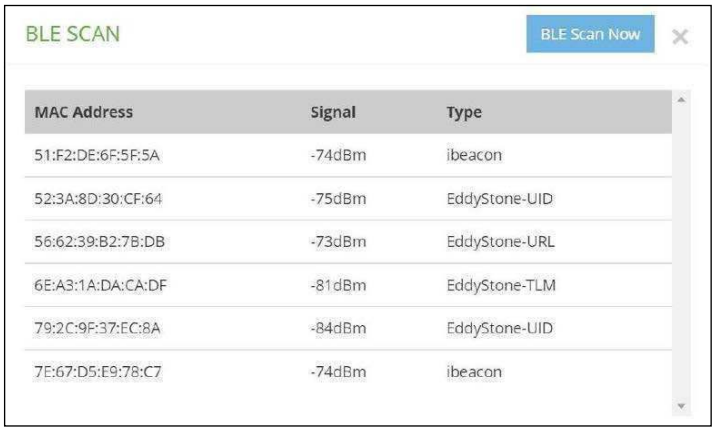
Figure 68: BLE Settings



The following items are displayed on this page:

- **Send iBeacon** — Enables iBeacon support on the AP. (Default: Enabled)
- **UUID** — The iBeacon Universally Unique Identifier that advertises the beacon service. The UUID contains 32 hexadecimal digits in five groups, separated by hyphens.
- **Major** — The iBeacon value that is used to identify a beacon group. (Range: 0-65535)
- **Minor** — The iBeacon value that is used to identify individual beacons within a group. (Range: 0-65535)
- **Tx Power** — Sets the BLE radio transmit power (supported only on EAP101 and EAP104). (Range: 5 dBm to -20 dBm; Default: 5 dBm)
- **BLE Scan** — (EAP101 and EAP104 only) Scans for all BLE devices, including these four types: EddyStone-UID, EddyStone-URL, EddyStone-TLM, and ibeacon.

Figure 69: BLE Scan



Diagnostics

The Diagnostics page provides Ping, Traceroute, Nslookup, and Speed Test tools for troubleshooting connectivity problems.

Ping Enter a hostname or IP address and click to run the ping tool.

Figure 70: Network Utilities - Ping

Traceroute Enter a hostname or IP address and click to run the traceroute tool.

Figure 71: Network Utilities - Traceroute

Nslookup Enter a hostname or IP address and click to run the Nslookup tool.

Figure 72: Network Utilities - Nslookup

Speed Test Enter a hostname or IP address of a Netperf server to test the speed between the AP and server.

Figure 73: Network Utilities - Speed Test

Device Discovery

The Device Discovery Tool provides a method for finding other Edgecore APs within the same Layer 2 network. To function, the Discovery Agent must be enabled (see "Edgecore Networks Discovery Tool" on page 91.

Click the Scan Network button to scan for devices.

Figure 74: Device Discovery Tool

Section III

Appendices

This section provides additional information and includes these items:

A Troubleshooting

Problems Accessing the Management Interface

Table 1: Troubleshooting Chart

Symptom	Action
Cannot connect using a web browser	■ Be sure the AP is powered up. ■ Check network cabling between the management station and the AP. ■ Check that you have a valid network connection to the AP and that intermediate switch ports have not been disabled. ■ Be sure you have configured the AP with a valid IP address, subnet mask and default gateway. ■ Be sure the management station has an IP address in the same subnet as the AP's IP. ■ If you are trying to connect to the AP using a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. ■ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent SSH sessions permitted. Try connecting again at a later time.
Forgot or lost the password	■ Reset the AP to factory defaults using its Reset button.

Using System Logs

If a fault does occur, refer to the *Quick Start Guide* to ensure that the problem you encountered is actually caused by the AP. If the problem appears to be caused by the AP, follow these steps:

1. Repeat the sequence of commands or other actions that lead up to the error.
2. Make a list of the commands or circumstances that led to the fault. Also, make a list of any error messages displayed.
3. Record all relevant system settings.
4. Display the log file through the System > Maintenance page, and copy the information from the log file.
5. Download the Diagnostics Log to a file from the System > Maintenance page.

6. Contact Edgecore and send a detailed description of the problem, along with all of the information mentioned in the above steps.

Wi-Fi 6 Access Point

Software Release 12.5.3

User Manual

www.edge-core.com

User Manual

Wi-Fi 6 Access Point

Cloud-Enabled Enterprise Access Points
EAP101
EAP102
EAP104
EAP104 (WL)
EAP111
EAP112
OAP101

E062024-CS-R15

How to Use This Guide

This guide includes detailed information on Edgecore access point (AP) software, including how to operate and use the management functions of APs. To deploy APs effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all software features.

Who Should Read This Guide?

This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks) and the Internet Protocol (IP).

How This Guide is Organized

The organization of this guide is based on the AP's web management interface. An introduction and initial configuration information is also provided.

The guide includes these sections:

- Section I "Getting Started" — Includes an introduction to AP management and initial configuration settings.
- Section II "Web Configuration" — Includes all management options available through the web interface.
- Section III "Appendices" — Includes information on troubleshooting AP management access.

Related Documentation

This guide focuses on AP software configuration, it does not cover hardware installation of an AP. For specific information on how to install an AP, see the following guide:

Quick Start Guide

For all safety information and regulatory statements, see the following documents:

Quick Start Guide

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Revision History

This section summarizes the changes in each revision of this guide.

June 2024 Revision

This is the 15th revision of this guide. It is valid for software release v12.5.3 and includes the following changes:

- Added support for EAP112
- Added HaLow and LTE support for EAP112
- Added 3G/LTE to Internet settings, see "Internet Settings" on page 43
- Added MQTT to BLE settings, see "BLE" on page 97

March 2024 Revision

This is the 14th revision of this guide. It is valid for software release v12.5.3 and includes the following changes:

- Minimum Signal Allowed setting for each SSID, see "Wireless Networks — General Settings" on page 69
- Added Device OS Blacklist, see "Wireless Networks — General Settings" on page 69

January 2024 Revision

This is the 13th revision of this guide. It is valid for software release v12.5.0 and includes the following changes:

- Added support for EAP111
- Added RADIUS NAS ID, see "Wireless Networks — Security Settings" on page 71
- Modified Minimum Signal Allowed default, see "Physical Radio Settings" on page 65

- Added OpenRoaming captive portal, see "OpenRoaming" on page 58
- Added OpenRoaming NAI Realm List Method/Authentication, see "OpenRoaming" on page 58
- Added Syslog Level, see "System Settings" on page 83

September 2023 Revision

This is the 12th revision of this guide. It is valid for software release v12.4.3 and includes the following changes:

- Added support for OAP101
- Added SSID isolation, see "Physical Radio Settings" on page 65
- Multiple PSK enhancement, see "Wireless Networks — Security Settings" on page 71

July 2023 Revision

This is the 11th revision of this guide. It is valid for software release v12.4.1 and includes the following changes:

- Added OpenRoaming, see "OpenRoaming" on page 58 and "Wireless Networks — OpenRoaming" on page 78
- Modified broadcast rate, see "Physical Radio Settings" on page 65
- Access Control List enhancement, see "Wireless Networks — Security Settings" on page 71
- Hostname enhancement, see "System Settings" on page 83
- Moved the language setting to the System page, see "System Settings" on page 83
- Firmware upgrade enhancement, see "Upgrading Firmware" on page 88
- Account username enhancement, see "User Accounts" on page 89

May 2023 Revision

This is the 10th revision of this guide. It is valid for software release v12.4.0 and includes the following changes:

- Added WAN port auto-detection to QR code Onboarding, see "QR Code Onboarding" on page 27
- Added automatic mesh AP configuration, see "Mesh AP Configuration" on page 30

- Removed Mark and Notrack from firewall rules, see “Firewall Rules” on page 51
- Modified Minimum Signal Allowed, see “Physical Radio Settings” on page 65
- Added RF Isolation, see “Physical Radio Settings” on page 65
- Modified Dynamic VLAN, see “Wireless Networks — Network Settings” on page 76
- Modified HotSpot 2.0 settings, see “Wireless Networks — Network Settings” on page 76
- Added Log Level, see “System Settings” on page 83
- Added SNMPv3 User, see “SNMP” on page 94
- Modified Diagnostics and added Speed Test, see “Diagnostics” on page 99

January 2023 Revision

This is the ninth revision of this guide. It is valid for software release v12.3.0 and includes the following changes:

- Updated QR code Onboarding, see “QR Code Onboarding” on page 27
- Updated wireless status, see “Wireless Status” on page 38
- Added support for dynamic PSK, see “Wireless Networks — Security Settings” on page 71
- Updated Hotspot 2.0 settings, see “Wireless Networks — Network Settings” on page 76
- Added CAPWAP Tunnel Interface to Ethernet Settings, see “Ethernet Settings” on page 46

November 2022 Revision

This is the eighth revision of this guide. It is valid for software release v12.2.0 and includes the following changes:

- Added Airtime Fairness, see “Physical Radio Settings” on page 65
- Modified the value range of BSS Coloring, see “Physical Radio Settings” on page 65
- Modified wireless security default, see “Wireless Networks — Security Settings” on page 71
- Added 802.11v, see “Wireless Networks — Security Settings” on page 71

- Added SNMP Trap, see "SNMP" on page 94
- Added BLE Scan, see "BLE" on page 97

November 2022 Revision

This is the seventh revision of this guide. It is valid for software release v12.1.0 and includes the following changes:

- Updated SNMP read/write community settings, see "SNMP" on page 94
- Added BLE radio Tx Power, see "BLE" on page 97
- Added Interference Detection, see "Physical Radio Settings" on page 65
- Added zero-touch provisioning information, see "Zero-Touch Provisioning" on page 20
- Modified the default value for Minimum Signal Allowed, see "Physical Radio Settings" on page 65
- Added 160MHz channel bandwidth option, see "Physical Radio Settings" on page 65
- Removed uCentral cloud option from the Setup Wizard.

July 2022 Revision

This is the sixth revision of this guide. It is valid for software release v12.0.0 and includes the following changes:

- Updated Setup Wizard for uCentral cloud, see "AP Setup Wizard" on page 22
- Added Proxy ARP, see "Wireless Networks — Network Settings" on page 76
- Added Multicast-to-Unicast Conversion, see "Wireless Networks — General Settings" on page 69
- Added Bandsteering, see "Physical Radio Settings" on page 65
- Added WPA3 Enterprise 192-bit and OWE security, see "Wireless Networks — Security Settings" on page 71
- Added multiple PSK keys, see "Wireless Networks — Security Settings" on page 71
- Added Short Guard Interval (SGI), see "Wireless Networks — Advanced Radio Settings" on page 79
- Added Multicast/Broadcast Rate, see "Physical Radio Settings" on page 65
- Added UPnP, see "LAN Settings" on page 49

- Added DHCP Snooping, see "DHCP Snooping" on page 61
- Added ARP Inspection, see "ARP Inspection" on page 62
- Added DHCP Relay, see "DHCP Relay" on page 63
- Added IPv6 for Internet access, see "IPv6 Settings" on page 46
- Added Hotspot 2.0, see "Wireless Networks — Network Settings" on page 76
- Added Device Discovery Tool, see "Device Discovery" on page 100
- Added Discovery Agent settings, see "Edgecore Networks Discovery Tool" on page 91
- Added Reset button and LED enable, see "System Settings" on page 83
- Added PoE Out setting, see "Ethernet Settings" on page 46
- Added caution on firmware upgrades in uCentral mode, see "Upgrading Firmware" on page 88

April 2022 Revision

This is the fifth revision of this guide. It is valid for software release v11.6.0 and includes the following changes:

- Added Client mode, see "Physical Radio Settings" on page 65
- Added Site Survey, see "Wireless Networks — General Settings" on page 69
- Added Custom LAN, see "LAN Settings" on page 49
- Added WME configuration, see "Physical Radio Settings" on page 65
- Added BSS Coloring, see "Physical Radio Settings" on page 65
- Added OFDMA, see "Physical Radio Settings" on page 65
- Added Target Wake Time, see "Physical Radio Settings" on page 65
- Added HTTPS captive portal, see "Captive Portal Settings" on page 56
- Added HTTPS certificate upload, see "Upload Certificate" on page 88

December 2021 Revision

This is the fourth revision of this guide. It is valid for software release v11.4.0 and includes the following changes:

- Updated QR code onboarding, see "QR Code Onboarding" on page 27

- Added mesh traffic graph to the dashboard, see "Traffic Graphs" on page 40
- Added MSP mode, see "System Settings" on page 83

November 2021 Revision

This is the third revision of this guide. It is valid for software release v11.3.1 and includes the following changes:

- Updated the Setup Wizard, see "AP Setup Wizard" on page 22
- Updated the Dashboard, see "Status Information" on page 33
- Added Smart Isolation, see "LAN Settings" on page 49
- Added Hotspot Settings, see "Hotspot Settings" on page 53
- Updated wireless network settings, see "Wireless Networks — Network Settings" on page 76
- Updated wireless open mesh settings, see "Wireless Networks — Open Mesh Settings" on page 78
- Added Telnet settings, see "Telnet" on page 91
- Added web server settings, see "Web Server" on page 91
- Added multicast DNS, see "Multicast DNS" on page 95
- Added firewall settings, see "Firewall Rules" on page 51
- Added a guest network, see "LAN Settings" on page 49

July 2021 Revision

This is the second revision of this guide. It is valid for software release v11.2.0 and includes the following changes:

- Added WPA3-Personal transition, WPA3-Enterprise, and WPA3-Enterprise transition. See "Wireless Networks — Security Settings" on page 71
- Support for IEEE 802.11 k/r, see "Wireless Networks — Security Settings" on page 71
- Added Minimum signal allowed (RSSI Threshold), see "Physical Radio Settings" on page 65
- Support for Open Mesh, see "Wireless Networks — Open Mesh Settings" on page 78
- SNMP v2 support, see "SNMP" on page 94

- Support for remote Syslog, see "Remote System Log Setup" on page 92
- Support for LLDP, see "LLDP" on page 96
- Support for management by an EWS-Series Controller, see "System Settings" on page 83

April 2021 Revision

This is the first revision of this guide. It is valid for software release v11.1.1.

Contents

Figures

Figures

Tables

Section I

Getting Started

This section provides an overview of the access point, and introduces some basic concepts about wireless networking. It also describes the basic settings required to access the management interface.

This section includes these chapters:

1 Introduction

The access point (AP) runs software that includes a network management agent. The agent offers a variety of management options, including a web-based interface. The AP can also be accessed through Secure Shell (SSH) for configuration using a command line interface (CLI).

Note: This manual describes the configuration interface for stand-alone mode. Refer to the Edgecore *ecCLOUD Controller User Manual* for information on configuring the AP through the cloud interface.

This chapter includes the following sections:

Configuration Options

The access point's web agent allows you to configure AP parameters, monitor wireless connections, and display statistics using a standard web browser. The AP's web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed remotely by a Secure Shell (SSH) connection over the network. The CLI is used primarily for technical support.

The AP's web interface allows you to perform management functions such as:

- Set management access user names and passwords
- Configure IP settings
- Configure 2.4 GHz and 5 GHz radio settings
- Configure HaLow radio settings (EAP112 only)
- Control access through wireless security settings
- Filter packets using Access Control Lists (ACLs)
- Download system firmware
- Download or upload configuration files
- Display system information

Zero-Touch Provisioning

APs can be automatically managed by the Edgecore ecCLOUD controller or an EWS-Series controller. If an AP is already registered with the ecCLOUD controller, it will be automatically managed when the WAN port of the AP is connected to the Internet.

When an AP is connected to a local LAN with an EWS-Series controller, the AP can be configured with the controller IP address through DHCP Option 138 and then automatically managed by the controller.

As an alternative to zero-touch provisioning, you can manually set the preferred management method from the web interface, see "System Settings" on page 83.

Connecting to the Web Interface

For first-time access to the AP's web management interface, you can connect a PC directly to one of the AP's LAN ports or use the quick-setup QR code (printed on a label next to the AP's ports). The first-time you access the web interface, it automatically runs the Setup Wizard for initial AP configuration.

For information on the Setup Wizard, see "AP Setup Wizard" on page 22.

For information on using the QR code, see "QR Code Onboarding" on page 27.

LAN Port Connection

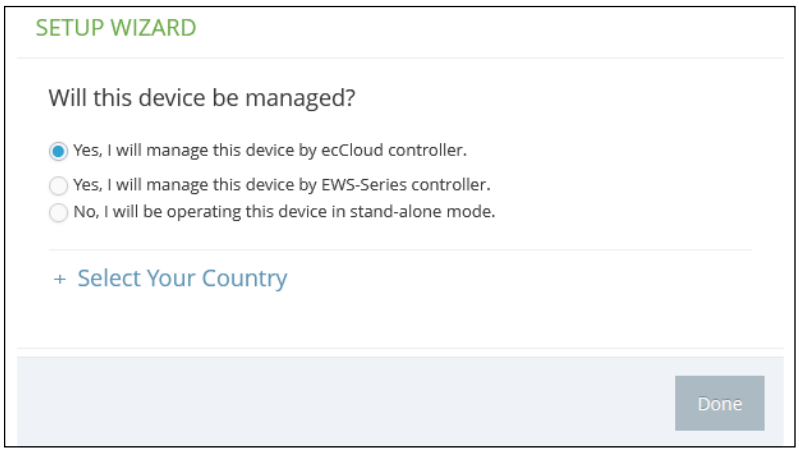
When connecting to the web management interface through one of the AP's LAN ports, the AP has a default management IP address of 192.168.2.1 and a subnet mask of 255.255.255.0. Therefore, you must set your PC IP address to be on the same subnet as the AP (that is, the PC and AP addresses must both start with192.168.2.x).

Note: To connect to the web interface using the Uplink(PoE) port, the IP address is automatically assigned through DHCP by default. If a DHCP server is unreachable, the Uplink(PoE) port reverts to a fallback IP address of 192.168.1.10.

To access the AP's web management interface, use your web browser to connect to the management interface by entering the default IP address of 192.168.2.1.

For first-time access, there is no user login and the Setup Wizard starts automatically. Follow the steps described in "AP Setup Wizard" on page 22.

Figure 1: Web Management Login



Note: To configure the AP with a different management IP address that is compatible with your network, see "LAN Settings" on page 49.

AP Setup Wizard

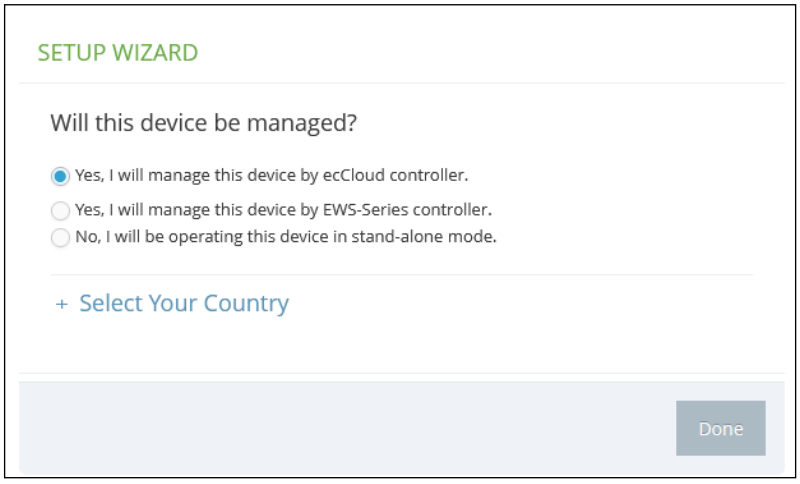
The Setup Wizard is designed to help you configure the basic settings required to get the AP up and running.

Step 1 Select How the AP will be Managed — To manage the AP using the Edgecore ecCLOUD controller, select "Yes, I will manage this device by ecCloud controller," and then continue to Step 6.

To manage the AP using the an Edgecore EWS-series controller, select "Yes, I will manage this device by EWS-Series controller," and then continue to Step 2.

Otherwise, select "No, I will be operating this device in stand-alone mode" and continue to Step 3.

Figure 2: Select ecCloud, EWS Controller, or Stand-Alone



If you select to manage the AP using the Edgecore ecCLOUD controller, go to cloud.ignitenet.com to register your AP. Log in and select Devices from the menu. Click Add Device and enter the AP serial number and MAC address to register the AP with your cloud network. The serial number and MAC address can be found on the product packaging or label.

Note: This manual describes the configuration interface for stand-alone mode. Refer to the Edgecore *ecCLOUD Controller User Manual* for information on configuring the AP through the cloud interface or the *EWS-Series Controller User Manual* for information on managing the AP through an EWS controller.

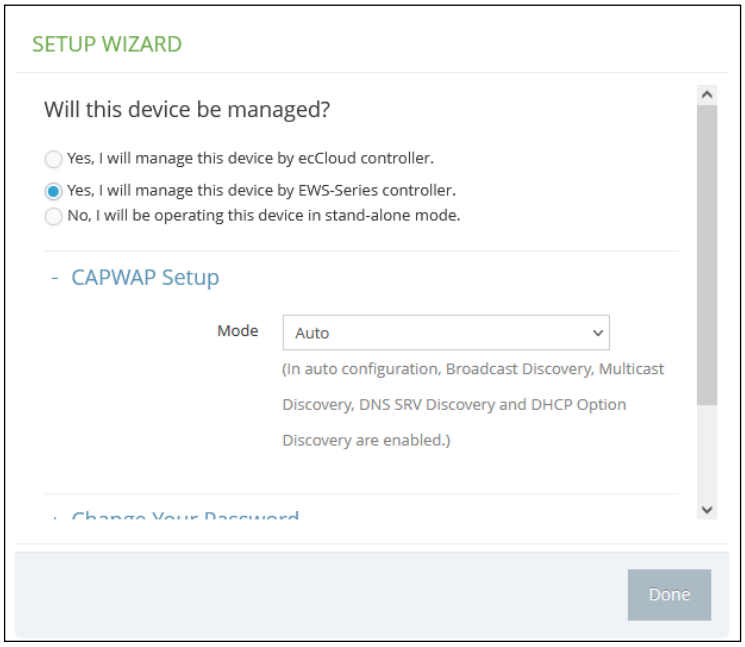
Step 2 CAPWAP Setup — When EWS-Series Controller management is selected, you can set the mode for discovering the controller. Once the AP has discovered the controller on the network it can then send a CAPWAP (Control And Provisioning of Wireless Access Points) join request.

In Auto mode, the AP uses four methods to discover the controller. These methods require no further configuration.

In manual mode, two options are available. Specify the Domain Name Suffix so that the AP can use DNS server records to discover the EWS controller. Or, just specify a static IP address for the controller.

For more information on CAPWAP setup, see "System Settings" on page 83.

Figure 3: CAPWAP Setup

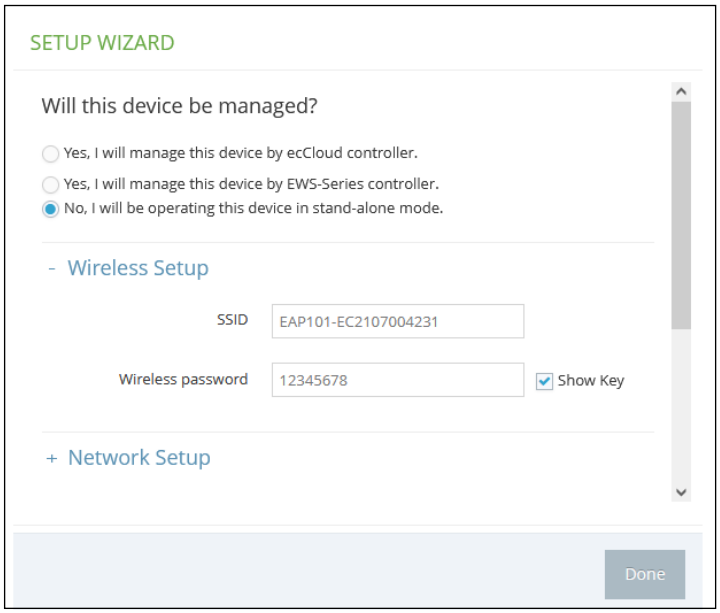


After completing the CAPWAP setup, continue with Step 5.

Step 3 Wireless Setup — If you select to manage the AP in stand-alone mode, you can configure the default wireless network.

The default wireless network name (SSID) consists of the AP model and its serial number, and there is a default wireless password. You have the option to modify the wireless network name and password to your preferred configuration. The wireless name must be 1-32 ASCII characters, and the password must be 8 to 63 ASCII characters (no special characters are allowed).

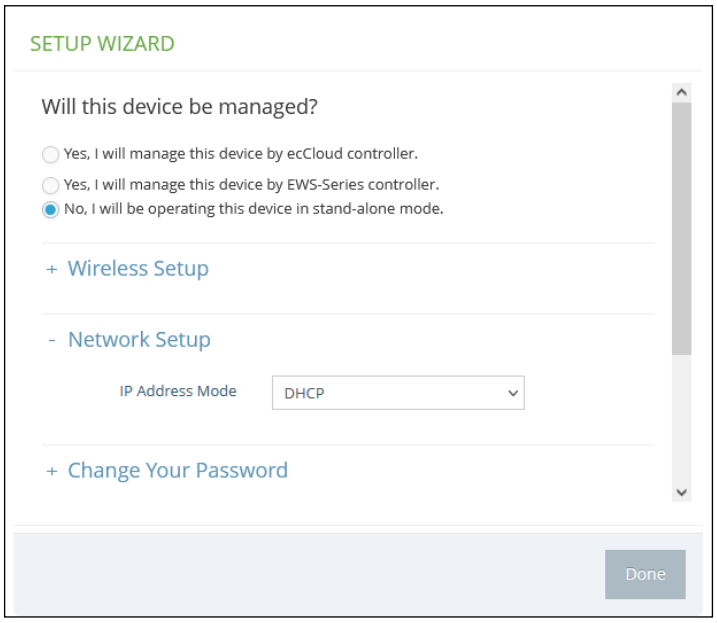
Figure 4: Wireless Setup



Step 4 Network Setup — For AP stand-alone mode, you also have the option to configure the IP address mode used to provide an IP address for the Internet access port.

The default IP Address Mode is DHCP and other options include Static IP and PPPoE. For more information, see "Internet Settings" on page 43.

Figure 5: Network Setup



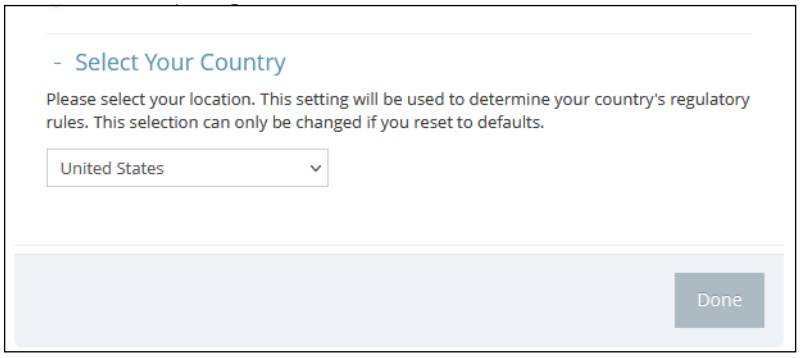
Step 5 Change Your Password — Set a new password for management access to the AP (the default user name is "admin" with password "admin"). The password must be 6-20 ASCII characters (case sensitive with no special characters).

Figure 6: Change Password

Note: For information on changing user names and passwords, see "User Accounts" on page 89.

Step 6 Select Your Country — Select the access point's country of operation from the drop-down menu. You must set the AP's country code to be sure that the radios operate according to permitted local regulations. That is, setting the country code restricts operation of the AP to the radio channels and transmit power levels permitted for wireless networks in the specified country.

Figure 7: Select Country



Caution: You must set the country code to the country of operation. Setting the country code ensures that the radios operate within the local regulations specified for wireless networks.

Note: The country code selection is for non-US models only and is not available to any US models. Per FCC regulation, all Wi-Fi products marketed in the US must be fixed to US operation channels only.

Step 7 After completing the Setup Wizard, click "Done."

QR Code Onboarding

For quick set up and registration of your AP with the ecCLOUD controller, you can scan the QR code on the AP using a phone.

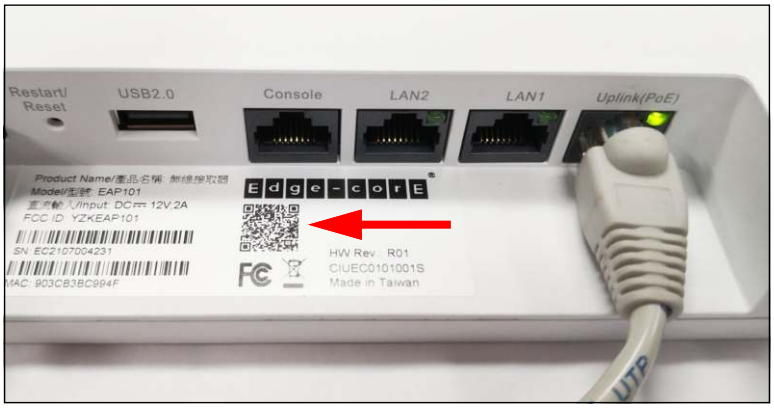
Follow these steps:

1. Power on the AP.

2. Connect the AP to the Internet. Connect your network or Internet access device to the AP's RJ-45 Uplink port.

3. Use the camera or a barcode app on your phone to scan the AP's QR code. The QR code is printed on a label next to the AP's ports.

Figure 8: Scanning the AP QR Code



4. When a message pops up, tap "yes" to join the Wi-Fi network. (iPhone requires you to go to Settings > Wi-Fi or open the browser for the message to pop up.)

   The web browser should open and redirect to the Setup Wizard page.

Note: If the phone cannot connect to the Wi-Fi network, type the SSID (network name) and password manually. The SSID name is the AP serial number (for example, EC0123456789), and the password is the AP MAC address (for example, 903CB3BC1234).

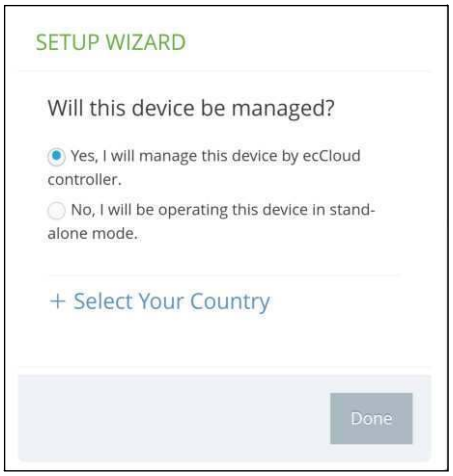
5. Wait for the auto-detection of the WAN port configuration (DHCP, Static IP, or PPPoE).

   When DHCP is detected, the AP automatically continues with the Setup Wizard.

Figure 9: Setup Wizard - Detect Network

6. Select to manage the AP using the ecCLOUD controller or to manage the AP in stand-alone mode.

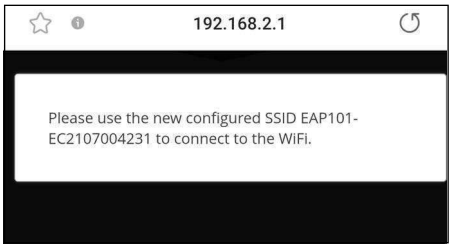
Figure 10: Setup Wizard - Device Management



a. Stand-Alone Mode: Use the default wireless network setting or customize the network name and password. Change the login password and set the country of operation. Tap “Done” to finish the setup wizard.

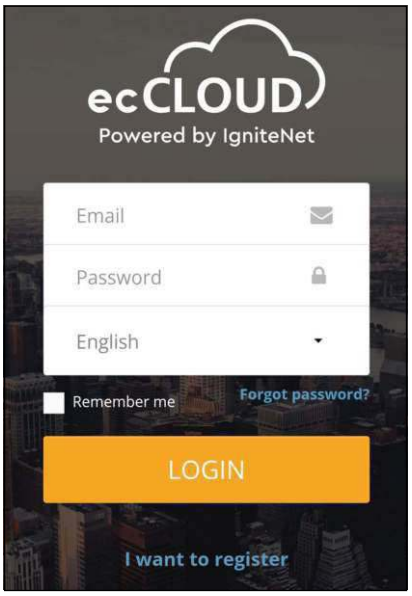
Wait about two minutes for the AP configuration to update, and then connect to the wireless network name configured in the Setup Wizard.

Figure 11: Connect to New SSID



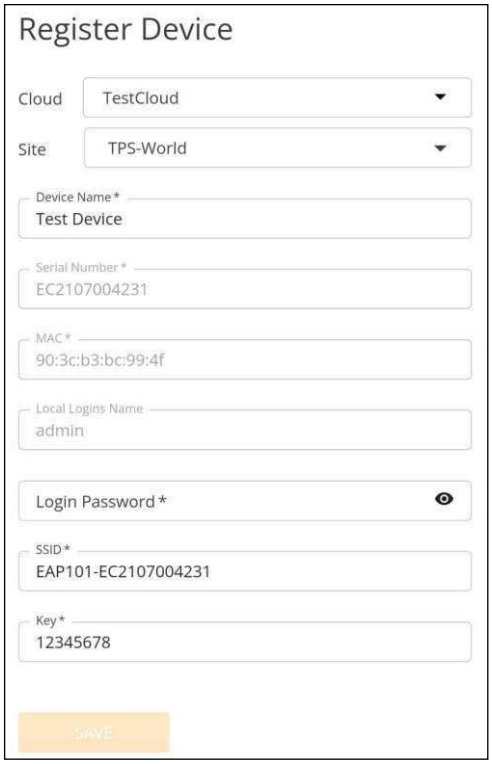
b. Cloud-Managed Mode: Set the country of operation and then tap “Done” to finish the Setup Wizard. The browser is redirected to the ecCLOUD login page.

Figure 12: ecCLOUD Login Page



If you already have an ecCLOUD account, log in and select a site for the AP. The AP is automatically registered for cloud management. Modify the device name, login password, SSID, and security key. After you tap "Save," wait about five minutes for the cloud controller to configure the AP.

Figure 13: ecCLOUD Device Registration



If you do not have an ecCLOUD account, tap "I want to register" and set up an account. Create a cloud and site before confirming the regulatory

country. After tapping “Next,” the AP is then automatically registered for cloud management.

After you tap “Save,” wait about five minutes for the cloud controller to configure the AP.

Note: Refer to the Edgecore *ecCLOUD Controller User Manual* for more information on setting up and configuring APs through ecCLOUD.

Mesh AP Configuration

The first AP can be managed either through ecCLOUD or in stand-alone mode. If a second AP needs to establish a mesh connection with the first AP, follow these steps:

1. Connect the LAN port of the first AP (Mesh Portal Point) to the LAN port of the second AP (Mesh Access Point), which then allows the second AP to synchronize its configuration with the first AP.

2. After unplugging the LAN port, the mesh connection will be established automatically.

Main Menu

The web interface Main Menu provides access to all the configuration settings available for the AP.

To configure settings, click the relevant Main Menu item. Each Main Menu item is summarized below with links to the relevant section in this guide where the configuration parameters are described in detail:

- **Dashboard** — The dashboard shows basic settings for the AP, including general status, local network settings, and wireless radio status. See “Status Information” on page 33.

- **Network** — Configures Internet, Ethernet, and LAN settings. See “Network Settings” on page 42.

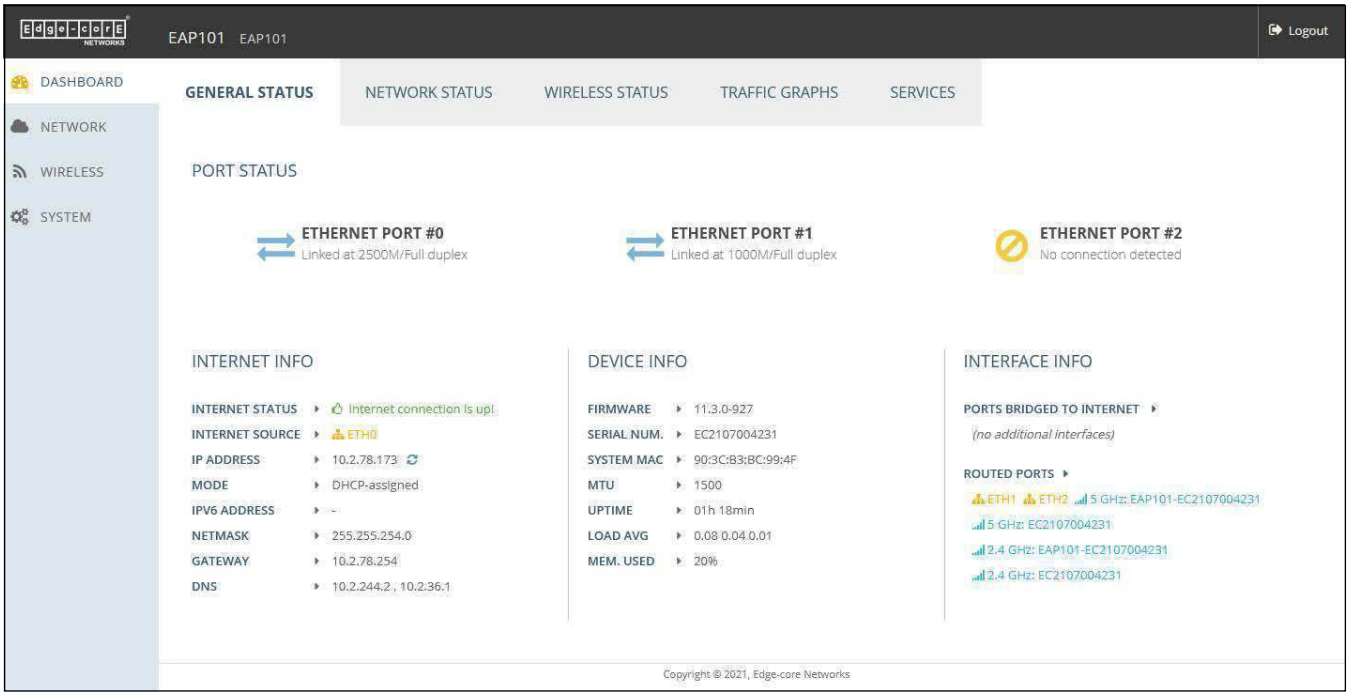
- **Wireless** — Configures 2.4 GHz Radio, 5 GHz Radio, HaLow and VLAN settings. See “Wireless Settings” on page 64

- **System** — Configures System (including cloud agent and various system settings), Maintenance (such as view log, reboot, reset defaults, backup defaults, restore defaults, and firmware upgrade), User Accounts, Services (network time), and Diagnostics (including ping, traceroute).

Dashboard

After logging in to the web interface, the dashboard displays. The dashboard shows basic settings for the AP, including Internet status, local network settings, and wireless radio status.

Figure 14: The Dashboard



Common Web Page Buttons

The list below describes the common buttons found on many of the web management pages:

- **Save** – Applies the new parameters and saves them to temporary RAM memory. Also displays a message at the top of the screen to inform you that the changes have not yet been saved to Flash memory. The running configuration will not be saved upon a reboot unless you click the "Save & Apply" button.

Figure 15: Saving Configuration Changes

- **Save & Apply** – Saves the changes made on a page and then applies them so that the configuration is retained after a restart.
- **Revert** – Cancels newly entered settings and restores the originals.
- **Logout** – Ends the web management session.

Section II

Web Configuration

This section provides details on configuring the access point using the web browser interface.

This section includes these chapters:

2 Status Information

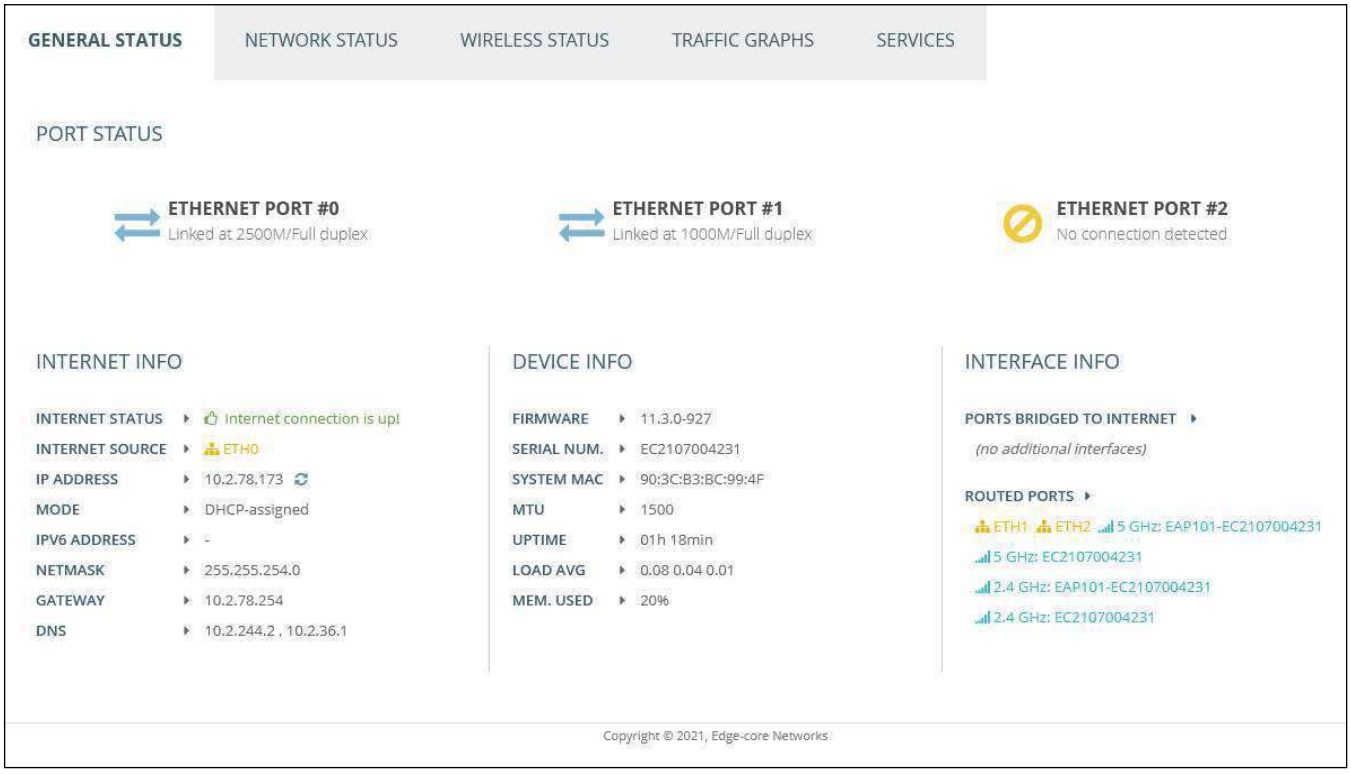
The Dashboard displays information on the current system configuration, including Internet status, local network settings, wireless radio status, traffic graphs, and services.

This chapter includes the following sections:

General Status

The General Status section shows descriptive information about the AP.

Figure 16: General Status Information



The following items are displayed in the “Port Status” section:

- **Ethernet Port #0** — Shows the status of the WAN Ethernet port, including link-up state, speed, and duplex mode.
- **Ethernet Port #1** — Shows the status of the LAN Ethernet port 1, including link-up state, speed, and duplex mode.
- **Ethernet Port #2** — Shows the status of the LAN Ethernet port 2, including link-up state, speed, and duplex mode.
- **3G/LTE** — Shows the status of the 3G/LTE connection (EAP112 only).

The following items are displayed in the “Internet Info” section:

- **Internet Status** — Shows whether or not the Internet connection is up.
- **Internet Source** — The Ethernet port connected to the Internet. By default, this is Ethernet Port 0.

- **IP Address** — IP address of the Internet connection.
- **Mode** — Shows if the IP address is a static setting or set by DHCP.
- **IPv6 Address** — The IPv6 address of the Internet connection.
- **Netmask** — The subnet mask of the IP address.
- **Gateway** — The IP address of the gateway router that is used when a destination address is not on the local subnet.
- **DNS** — The IP address of the Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

The following items are displayed in the "Device Info" section:

- **Firmware** — The software version number.
- **Serial Number** — The serial number of the physical access point.
- **System MAC** — The system MAC address of the access point.
- **MTU** — The maximum transmission unit for packets sent on the network.
- **Uptime** — Length of time the management agent has been up.
- **Load Average** — The last 1-minute, 5-minute and 15-minute CPU load average.
- **Memory Used** — The percentage of memory being used.

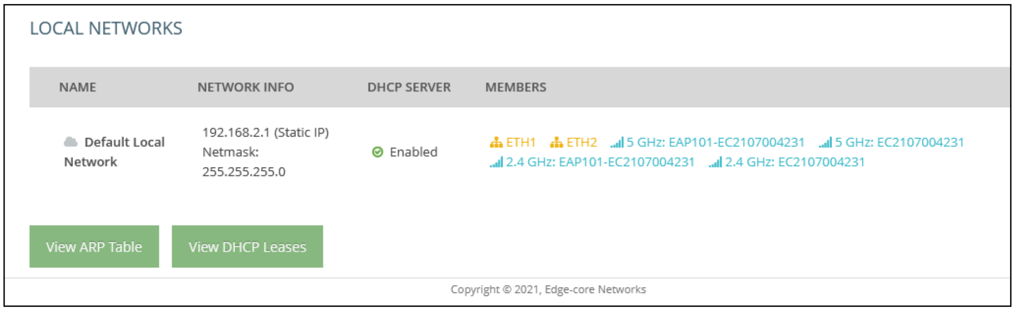
The following items are displayed in the "Interface Info" section:

- **Ports Bridged to Internet** — Additional interfaces attached directly to the Internet. Lists interfaces attached to the WAN (that is, the Internet).
- **Routed Ports** — By default, all interfaces are configured as a member of the LAN. Traffic from these interfaces is routed across the access point through Ethernet Port 0 to the Internet. (This is also called route to Internet.)

Network Status

The Network Status section shows information about local network connections.

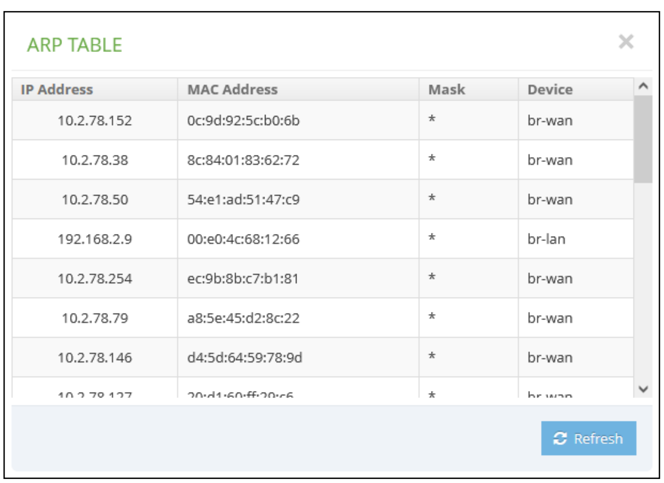
Figure 17: Local Networks



The following items are displayed in this section:

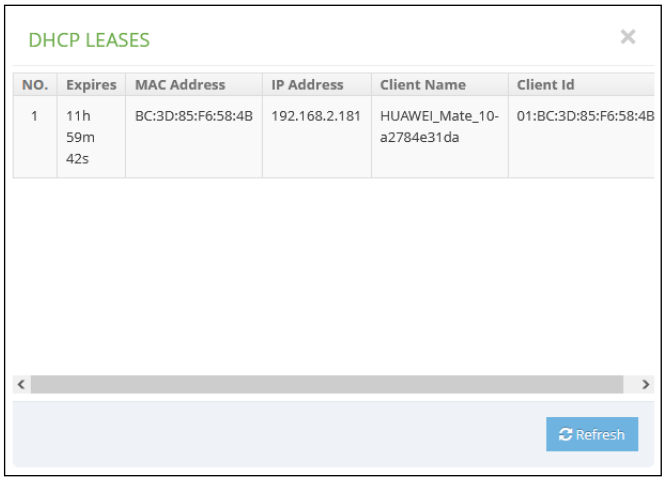
- **Name** — Shows information on the name of the local network.
- **Network Info** — Shows whether the local network uses static or dynamic configuration, and the network mask.
- **DHCP Server** — Shows if DHCP service is enabled on this network.
- **Members** — Shows the ports and wireless radios attached to this network. (Click on any of these interfaces to open the corresponding configuration page.)
- **View ARP Table** — Shows the ARP cache.

Figure 18: ARP Table



- **View DHCP Leases** — Shows DHCP leases.

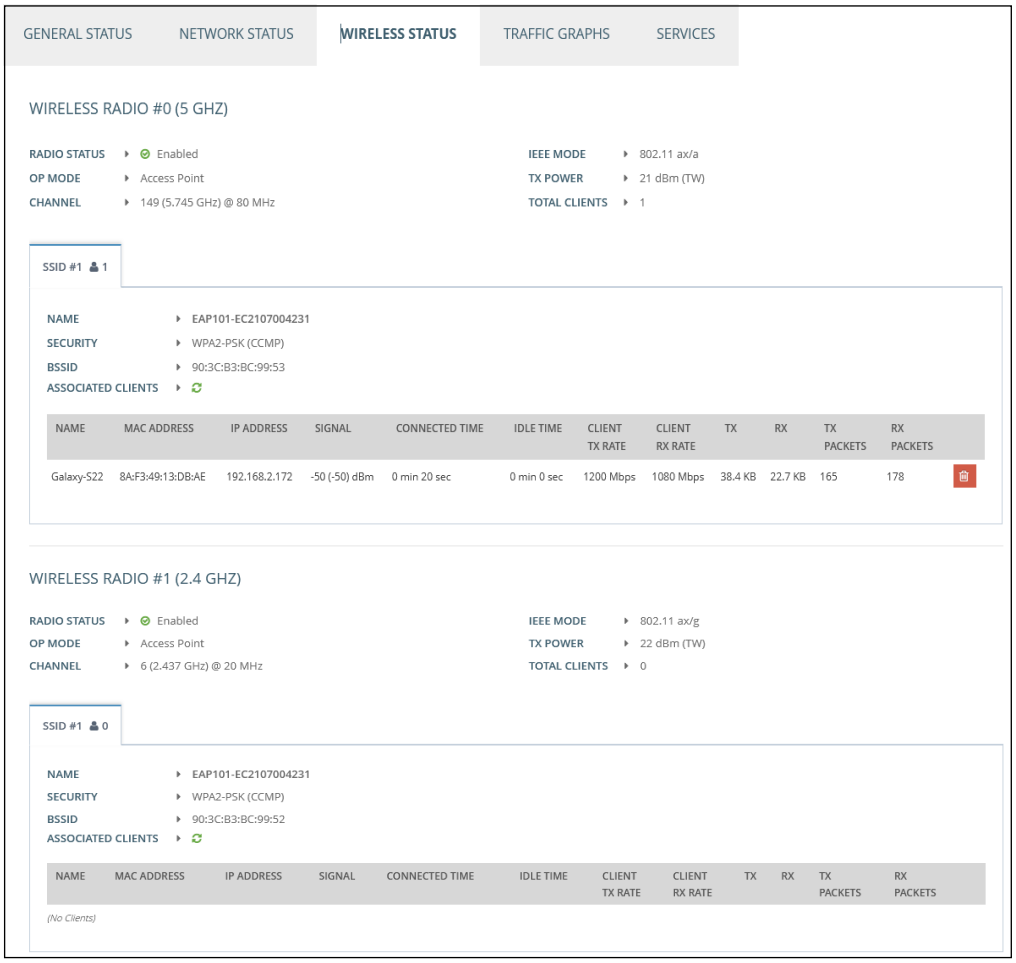
Figure 19: Active DHCP Leases



Wireless Status

The Wireless Status section shows information about the radio settings and associated clients.

Figure 20: Wireless Status



Note that you can click the red button next to an associated client to force disconnection.

The following items are displayed in this section:

- **Wireless Radio 5 GHz/2.4 GHz/HaLow** — Indicates the 2.4 GHz, 5 GHz, and HaLow (EAP112) wireless interface.
  - **Radio Status** — Shows if the wireless interface is enabled or disabled.
  - **IEEE Mode** — The 802.11 wireless LAN standards supported by the AP.
  - **Op Mode** — Shows if the wireless interface is configured to operate in an access point mode or client mode.

- **Tx Power** — The power of the radio signals transmitted from the AP.
- **Channel** — The radio channel the access point uses to communicate with wireless clients. The available channels depend on the 802.11 Mode, Channel Bandwidth, and Country Code settings.
- **Total Clients** — The total number of clients attached to this interface.

- **SSID #** — Service set identifier. Clients that want to connect to the wireless network through an access point must set their SSIDs to the same as that of the access point.
  - **Name** — A unique identifier for the local wireless network.
  - **Security** — Shows whether or not security has been enabled.
  - **BSSID** — The basic service set identifier. This is the MAC address of the AP generated by combining the 24 bit Organization Unique Identifier (OUI, the manufacturer's identity) and the manufacturer's assigned 24-bit identifier for the radio chipset in the AP.
  - **Associated Clients** — Shows detailed information about associated wireless clients.
    - **Name** — Client name.
    - **MAC Address** — The MAC address of the wireless client.
    - **IP Address** — The IP address assigned to the wireless client.
    - **Signal** — The signal strength (TX/RX) in dBm.
    - **Connected Time** — The time the wireless client has been associated.
    - **Idle Time** — The time the wireless client has been inactive.
    - **Client TX Rate** — The data transmit rate to the wireless client.
    - **Client RX Rate** — The data receive rate from the wireless client.
    - **TX** — The number of bytes transmitted to the wireless client.
    - **RX** — The number of bytes received from the wireless client.
    - **TX Packets** — The number of packets transmitted to the wireless client.
    - **RX Packets** — The number of packets received from the wireless client.

Traffic Graphs

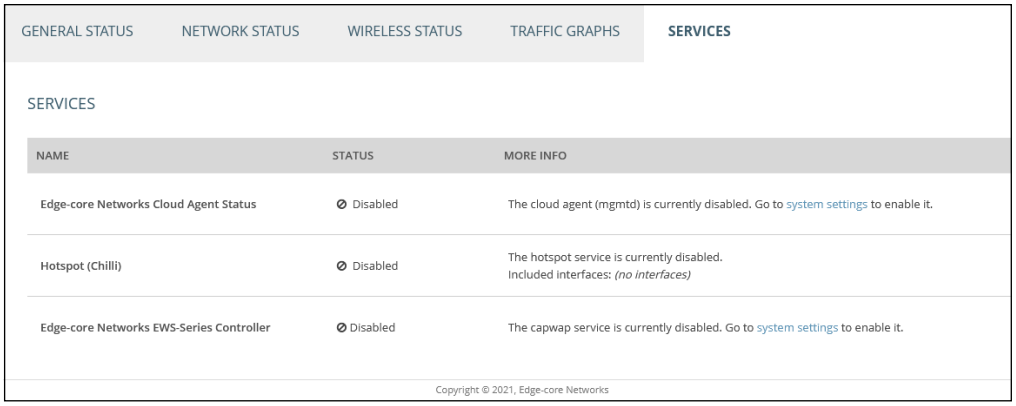
The Traffic Graphs section shows the data rate for the Ethernet ports, wireless interfaces, and mesh interface.

Figure 21: Traffic Graphs

Services

The Services section shows the status of the Edgecore cloud management agent.

Figure 22: Services



- **Edge-core Networks Cloud Agent Status** — Shows whether or not the agent for the cloud controller is enabled.

- **Hotspot (Chilli)** — Shows whether or not hotspot services are enabled. Click on this field to open the Hotspot Settings menu.

- **Edge-core Networks EWS-Series Controller** — Shows if the CAPWAP service is enabled for management of the AP through an EWS-Series controller.

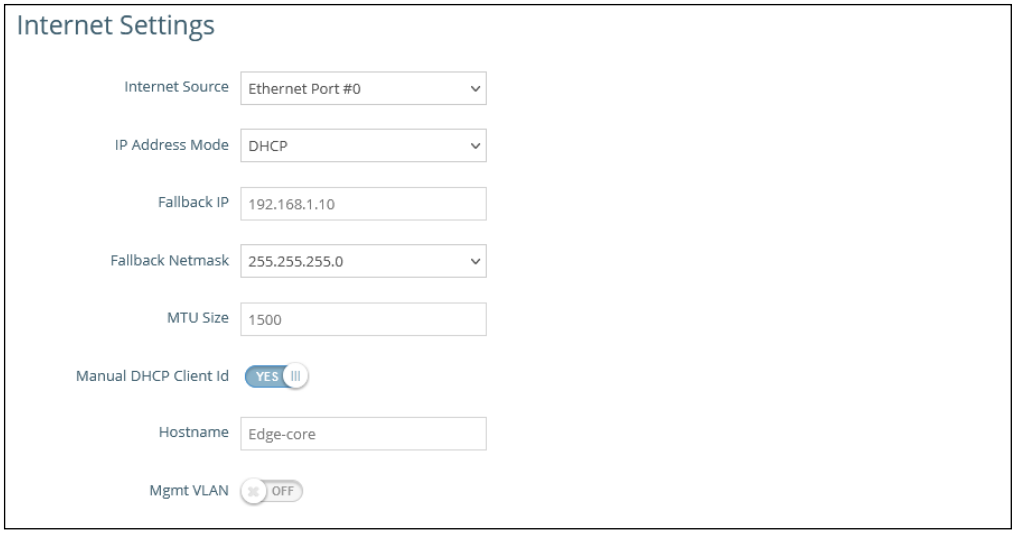
3 Network Settings

This chapter describes basic network settings on the access point. It includes the following sections:

Internet Settings

The Internet Settings page configures the basic Internet settings for the AP, such as the source port, IP aliases, as well as the host name and maximum MTU size.

Figure 23: Internet Settings

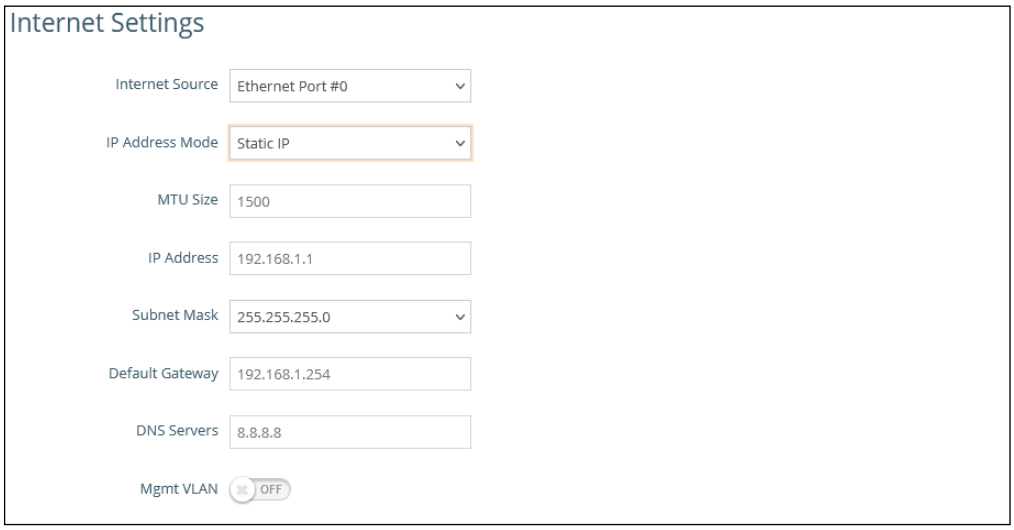


The following items are displayed on this page:

- **Internet Source** — The interface used to access the Internet.
  - **3G/LTE** — Selects the LTE interface as the Internet source. (EAP112 only.)
    - **Modem Device** — Selects the 3G/LTE modem device connected to the system.
    - **APN** — The Access Point Name (APN) used to identify this device when connected to an LTE network.
    - **PIN** — The personal identification number (PIN) of the SIM card installed in the device. The PIN authenticates use of the SIM card for access to an LTE network.
    - **Username** — The name used for LTE access.
    - **Password** — The password used for LTE access.
- **IP Address Mode** — The method used to provide an IP address for the Internet access port. (Default: DHCP; Options: DHCP, Static IP, PPPoE)
  - **DHCP** — Configuration options displayed for DHCP are shown in Figure 23.

- **Fallback IP** — This IP address is used if the DHCP service is unavailable or fails. (Default: 192.168.1.10)
- **Fallback Netmask** — The network mask associated with the fallback IP address. (Default: 255.255.255.0)
- **Manual DHCP Client Id** — An option to manually enter the hostname for the DHCP client.

Figure 24: IP Address Mode – Static IP



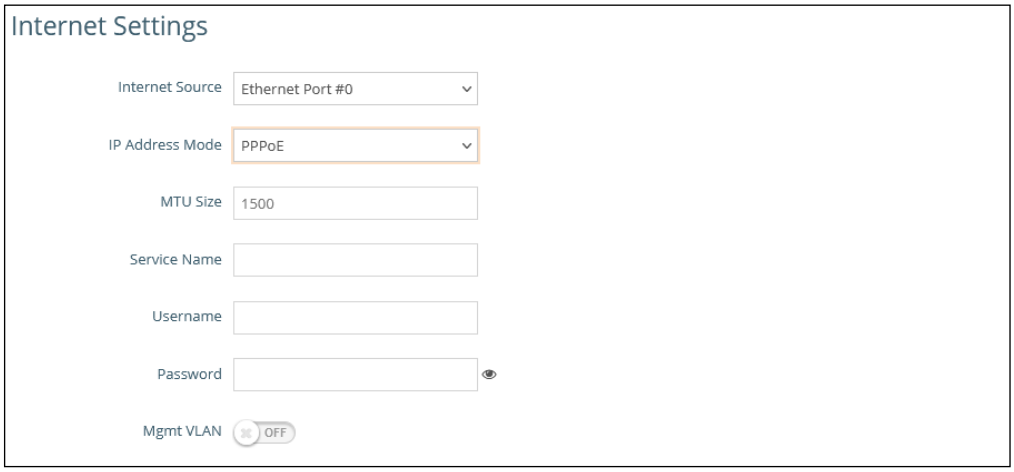
- **Static IP** — To configure a static IP address for the selected Ethernet interface, the following items must be specified.
  - **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this interface. (Range: 1400-1500 bytes; Default 1500 bytes)
  - **IP Address** — Specifies an IP address for the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.1.1)
  - **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
  - **Default Gateway** — The IP address of the default gateway, which is used if the requested destination address is not on the local subnet.

    If you have management stations, DNS, RADIUS, or other network servers located on another subnet, type the IP address of the default gateway router in the text field provided.
  - **DNS Servers** — The IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and

can be used to identify network hosts by familiar names instead of the IP addresses.

If you have a DNS servers located on the local network, type the IP address in the text fields provided.

Figure 25: IP Address Mode – PPPoE

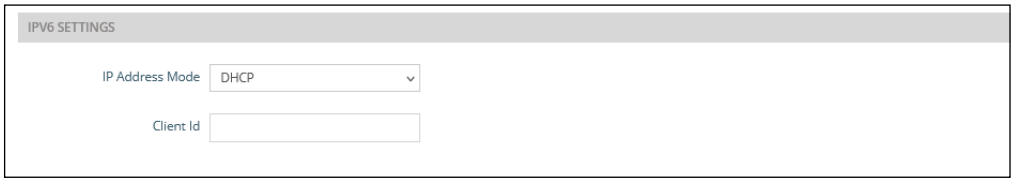


- **PPPoE** — To obtain an IP address for the selected Ethernet interface using PPPoE, the following items must be specified.
  - **Service Name** — The service name assigned for the PPPoE connection. The service name is normally optional, but may be required by some service providers. (Range: 1-32 alphanumeric characters)
  - **User Name** — The user name specified by the service provider. (Range: 1-32 characters)
  - **Password** — The password specified by the service provider. (Range: 1-32 characters)
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this interface. (Range: 1400-1500 bytes; Default 1500 bytes)
- **VLAN Tag** — Enable to activate tagging on this port and choose a tagging ID value between 2 and 4094, inclusive.
- **Mgmt VLAN** — Select this option to enable a management VLAN on this device. Once you enable this option, you will no longer be able to access this device on any of built-in the local networks (like 192.168.2.1 for example). You will only be able to access the device from the specified VLAN network. If this device's IP mode is set to DHCP, it will also request a new IP address in the subnet range assigned to the VLAN network.

IPv6 Settings

Enables you to configure the method used to provide an IPv6 address for the Internet access port.

Figure 26: IPv6 Settings



The following items are displayed on this section of the page:

- **IP Address Mode** — The method used to provide an IPv6 address for the Internet access port. (Default: DHCP; Options: DHCP, Static IP)
  - **DHCP** — If you configure DHCP, the Client Id must be specified.
    - **Client Id** — Manually enter the client ID for the DHCP client.
  - **Static IP** — To configure a static IPv6 address for the Internet access port, the following items must be specified.
    - **IP Address** — Specifies an IPv6 address for the access point. An IPv6 address must be configured according to RFC 2373 using 8 colon separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
    - **Default Gateway** — The IPv6 address of the default gateway, which is used if the requested destination address is not on the local subnet.
    - **DNS** — The IPv6 address of Domain Name Servers on the network. A DNS maps numerical IPv6 addresses to domain names and can be used to identify network hosts by familiar names instead of the IPv6 addresses. If you have a DNS server located on the local network, type the IPv6 address in the text field provided.

Ethernet Settings

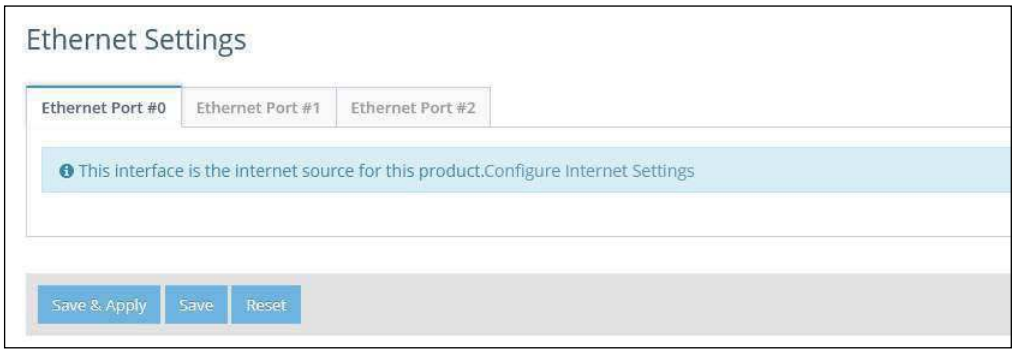
The Ethernet Settings page configures the network behavior of the Ethernet ports, indicating that a port provides an Internet connection for wireless clients attached to the local network (routed to the Internet), or is bridged directly to the Internet.

The following items are common for all pages under Ethernet Settings:

- **Ethernet Port #0** — Shows the status of the WAN Ethernet port.

- **Ethernet Port #1** — Shows the status of the LAN Ethernet port 1.
- **Ethernet Port #2** — Shows the status of the LAN Ethernet port 2.

Figure 27: Ethernet Settings – Internet Source

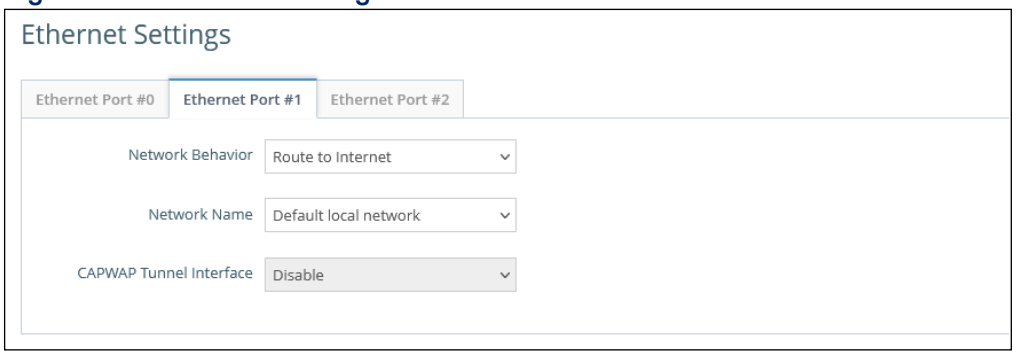


The following status message is displayed if an interface is set as the Internet source:

- "This interface is the internet source for this product. Configure Internet Settings"

  If more than one interface is connected to the Internet, only the last configured interface is used.

Figure 28: Ethernet Settings – Network Behavior



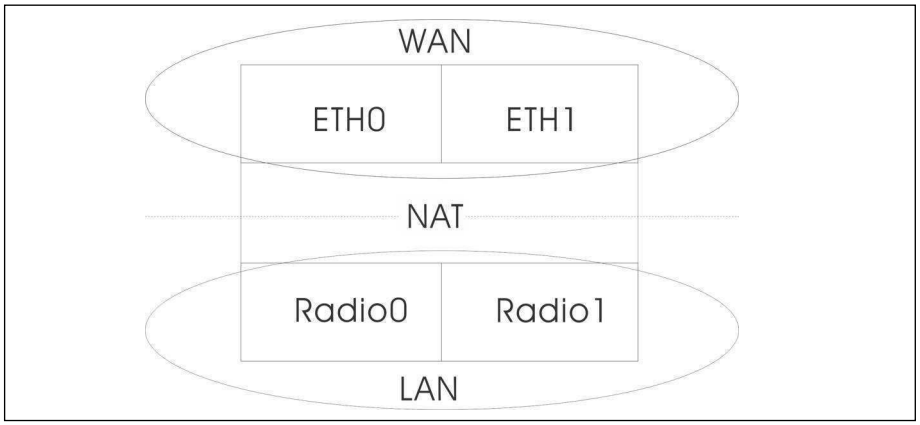
The following items are displayed on this page:

- **Network Behavior** — For the Ethernet port which is not providing Internet access, one of the following connection methods must be specified. (Default: Route to Internet)

  - **Bridge to Internet** — Configures an interface to be attached to the WAN. Traffic from this interface is directly bridged into the Internet. If an Ethernet port is bridged to the Internet, management access cannot be made by a direct connection to this port. However, if another Ethernet port or radio interface is within the LAN (routed to the Internet) the access point can be managed through this interface by a PC which is configured with an IP address in the same subnet.

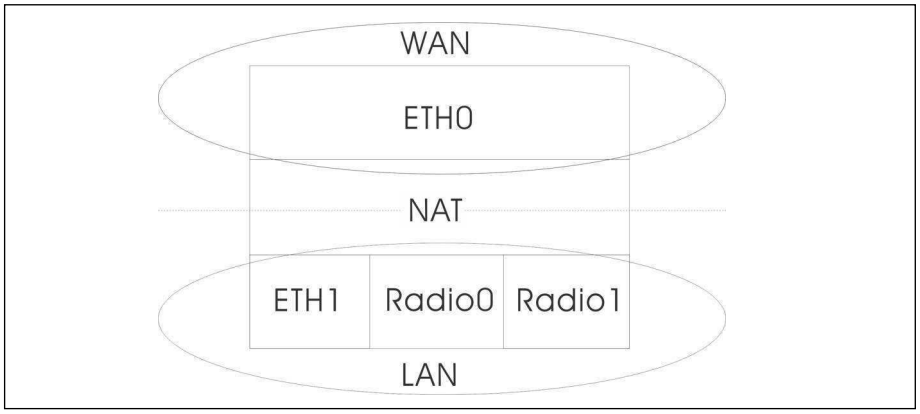
In the following figure, Ethernet Port 0 and Ethernet Port 1 are both attached to the WAN.

Figure 29: Bridge to Internet



- **Route to Internet** — Configures an interface to be a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged directly to the Internet. By default, Ethernet Port 1 is routed to Internet, allowing management access via a direct connection to a PC configured with an address in the same subnet.

Figure 30: Route to Internet



  - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Networks.

- **Add to Guest Network** — This port can only support the guest network.

- **Hotspot Controlled** — This port can only access hotspot services. Click the link to open the Hotspot Settings page. See "Hotspot Settings" on page 53.

- **VLAN Tag Traffic** — This port transmits tagged traffic from a specified VLAN. Select the VLAN ID from the configured list, or click the link to open

the Wireless VLAN Settings page and create a VLAN ID. See "VLAN Settings" on page 80.

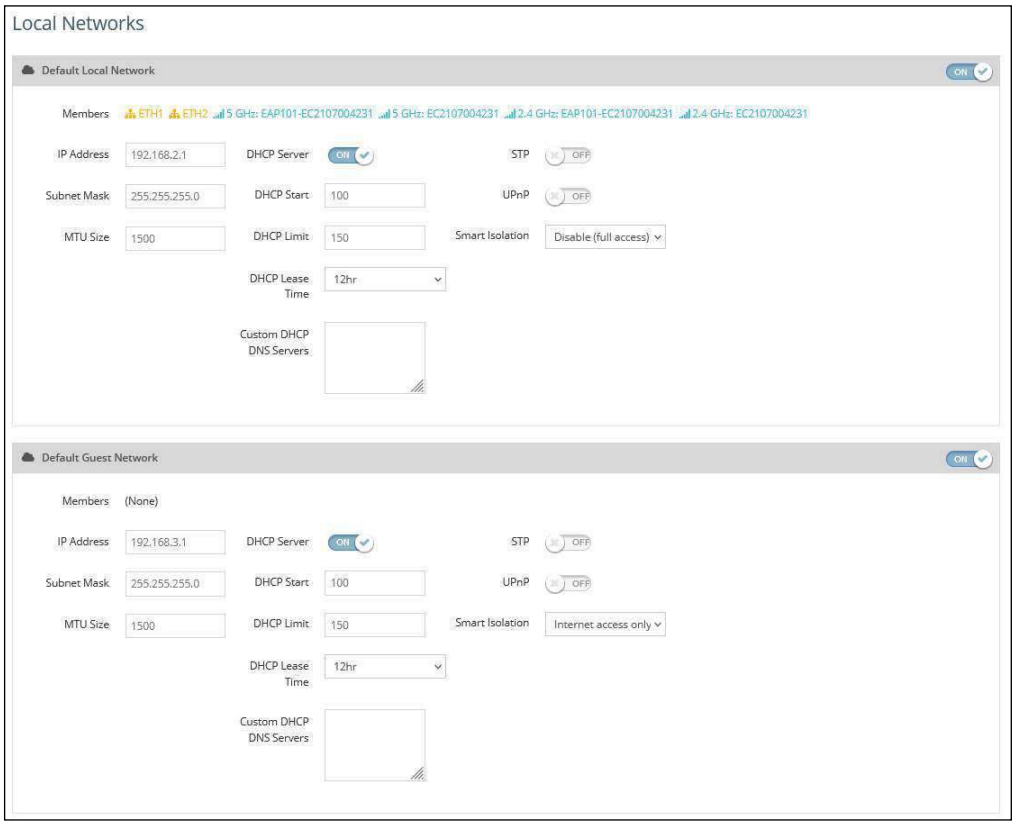
- **PoE Out** — (EAP104 only) Enables the PoE Out feature when the PoE source is detected as 802.3at, otherwise the PoE Out feature is disabled. When set to "Off," PoE Out is always disabled. (Default: On)

- **CAPWAP Tunnel Interface** — When the AP system management is set to EWS-Series Controller mode (see "System Settings" on page 83), the CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode can be configured for the Ethernet port from the controller template. The options are "Disable" or "Complete." A Complete tunnel sends all management, authentication, and data traffic from the AP back to the controller. (Default: Disable)

LAN Settings

The LAN Settings page configures the LAN settings for the local and guest networks, including IP interface setting, DHCP server settings, and STP administrative status.

Figure 31: Network – LAN Settings



The following items are displayed on this page:

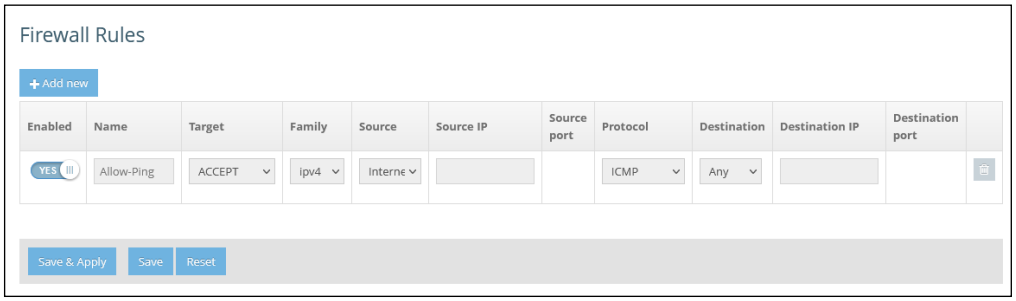
- **IP Address** — Specifies the IP address for the local network or guest network. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.2.1)
- **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this network. (Range: 1400-1500 bytes; Default 1500 bytes)
- **DHCP Server** — Enables/disables DHCP on this network. (Default: Enabled)
  - **DHCP Start** — First address in the address pool. (Range: 1-256; Default: x.x.x.100)
  - **DHCP Limit** — Maximum number of addresses in the address pool. (Range: 1-254; Default: 150)
  - **DHCP Lease Time** — The duration that an IP address is assigned to a DHCP client.
  - **Custom DHCP DNS Servers** — Specify the addresses or hostnames of custom DNS servers to be used.
- **STP** — Enables or disables processing of Spanning Tree Protocol messages. (Default: Disabled)
- **UPnP** — Enables or disables Universal Plug-and-Play broadcast messages. (Default: Disabled)
- **Smart Isolation** — Enables network traffic to be restricted to the specified network:
  - **Disable (full access)** — There is no traffic isolation. Clients can access the Internet and other devices on the local LAN.
  - **Internet access only** — Traffic from this network can only be routed to and from the Internet.
  - **LAN access only** — Traffic from this network is restricted to local LAN devices only.
  - **Internet access strict** — Traffic from this network can only be routed to and from the Internet, but with the additional restriction that users cannot access resources or devices on any private network (such as 192.168.0.0, 172.16.0.0, 10.0.0.0 etc.).
- **Add Custom LAN** — Click this button to create additional networks with their own custom settings. You can create up to 5 custom LANs.

Firewall Rules

Firewall filtering restricts connection parameters to limit the risk of intrusion. The firewall settings allow you to define a sequential list of rules that filter traffic based on source and destination IP addresses and ports. Ingress packets are tested against the filter rules one by one. As soon as a packet matches a rule, the configured target action is implemented.

One rule, "Allow-Ping," is pre-configured to allow Ping packets from the Internet. You can enable or disable this rule, but it cannot be modified or deleted. Click the "Add new" button to add a new firewall rule.

Figure 32: Firewall Rules



The following items are displayed on this page:

- **Enabled** — Enables or disables the rule.
- **Name** — A user-defined name for the filtering rule. (Range: 1-30 characters)
- **Target** — The action to take when a packet is matched. (Options: Accept, Reject, Drop; Default: Accept)
  - **Accept** — Accepts matching packets.
  - **Reject** — Drops matching packets and returns an error packet in response.
  - **Drop** — Drops matching packets.
- **Family** — The IP address family. (Options: Any, IPv4; Default: Any)
- **Source** — The source interface. (Options: Guest Network, Hotspot Network, Default Local Network, Internet, Any)
- **Source IP** — The source IPv4 address in CIDR notation. Includes an IPv4 address followed by a slash (/) and a decimal number to define the network mask.
- **Source port** — The source protocol port. (Range: 0-65535)

- **Protocol** — The protocol type. (Options: Any, TCP+UDP, TCP, UDP, ICMP; Default: TCP+UDP)
- **Destination** — The destination interface. (Options: Guest Network, Hotspot Network, Default Local Network, Internet, Any)
- **Destination IP** — The destination IP address.
- **Destination port** — The destination protocol port. (Range: 0-65535)

Port Forwarding

Port Forwarding can be used to map an inbound protocol type (TCP/UDP) and port to an "internal" IP address and port. The internal (local) IP addresses are the IP addresses assigned to local devices at the edge of a network, and the external IP address is the IP address assigned to the AP interface. This allows remote users to access different servers on your local network using your single public IP address.

Remote users accessing services such as web or FTP at your local site through your public IP address, are redirected (mapped) to other local server IP addresses and TCP/UDP port numbers. For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.3.9/80, then all HTTP requests from outside users are forwarded to 192.168.3.9 on port 80. Therefore, by just using your external IP address provided by your ISP, Internet users can access the services they need at the local addresses to which you redirect them.

Figure 33: Port Forwarding

The following items are displayed on this page:

- **Enabled** — Enables port forwarding.
- **Name** — User defined name. (Range: 1-30 characters)
- **Protocol** — Set the protocol to which port forwarding is applied. (Options: TCP, UDP, TCP+UDP)
- **External Port** — The TCP/UDP port number. (Range: 1-65535)

  The more common TCP service port numbers include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

- **Internal IP address** — The internal destination IP address.
- **Internal Port** — The internal destination protocol port. (Range: 1-65535)

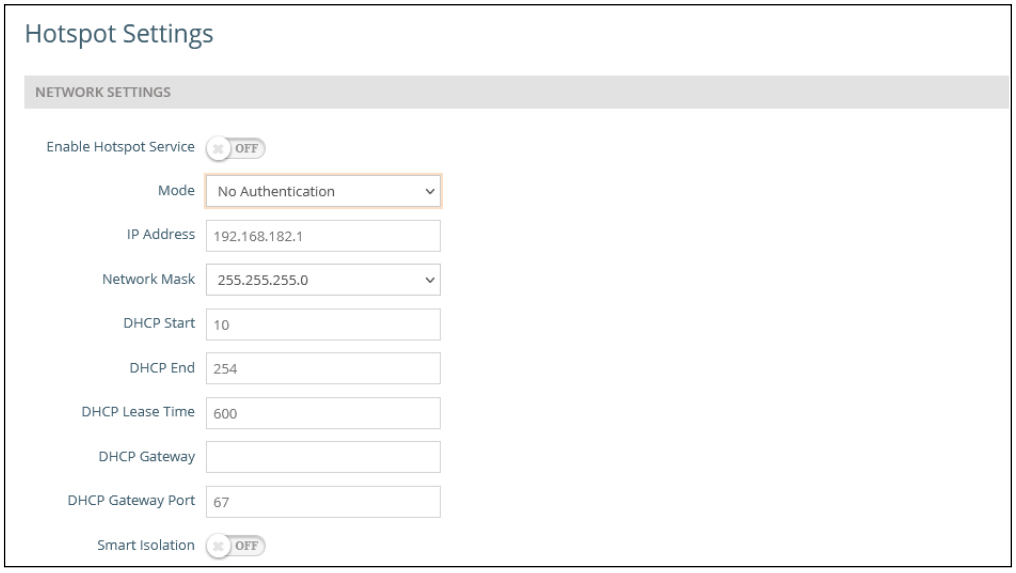
Hotspot Settings

The Hotspot Settings page can configure Internet access to the general public in places such as coffee houses, libraries and hospitals. Specific access rights may also be defined through a RADIUS server.

Network Settings

This section includes the option to enable or disable hotspot service, hotspot mode options, and network settings.

Figure 34: Hotspot Settings (Network Settings)



The following items are displayed on this page:

- **Enable Hotspot Service** — Enables or disables hotspot service. A hotspot is a physical location where people may obtain Internet access, typically using Wi-Fi technology, via a wireless local area network using a router connected to an Internet service provider.
- **Mode** — Hotspot service types include the following options:
  - **External Captive Portal Service** — This option will show the hotspot guest an externally hosted captive portal splash page and may prompt them to login, depending on how you've configured your service settings. Choose this option if you've signed up with a third-party captive portal service provider such as Cloud4Wi or HotSpotSystem.

- **No Authentication** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will not require the guest to login before accessing the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

- **Simple Password-Only Splash Page** — This option will show the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a simple password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

- **Local Spash Page with External RADIUS** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a valid RADIUS username and password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

- **Network IP** — Specifies the IP address for the hotspot. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.182.1)

  If your WAN subnet conflicts with any of the local networks (even the custom ones you create), the AP will automatically change the subnet of the local network.

- **Network Mask** — Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

- **DHCP Start** — Starting number of (last numeric field) in address pool. (Range: 1-254; Default: 10)

- **DHCP End** — Ending number of (last numeric field) in address pool. (Range: 1-254; Default: 254)

- **DHCP Lease Time** — The duration that an IP address is assigned to a DHCP client. (Range: 600-43200 seconds; Default: 600 seconds)

- **DHCP Gateway** — Configure the DHCP gate IP address if you want to use an external DHCP server instead of the internal one.

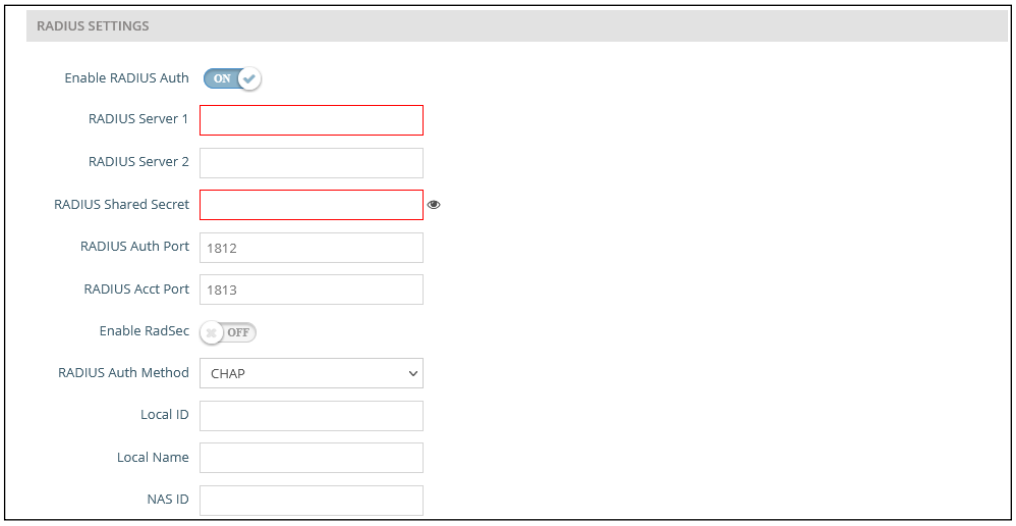
- **DHCP Gateway Port** — The listening port used by the DHCP gateway.

- **Smart Isolation** — Activate to prevent Hotspot users to possibly access WAN resources.

RADIUS Server

If you click set the mode to External Captive Portal Service or Local Splash page with External RADIUS, the following section is displayed.

Figure 35: Hotspot Settings (RADIUS Settings)



The following items are displayed on this page:

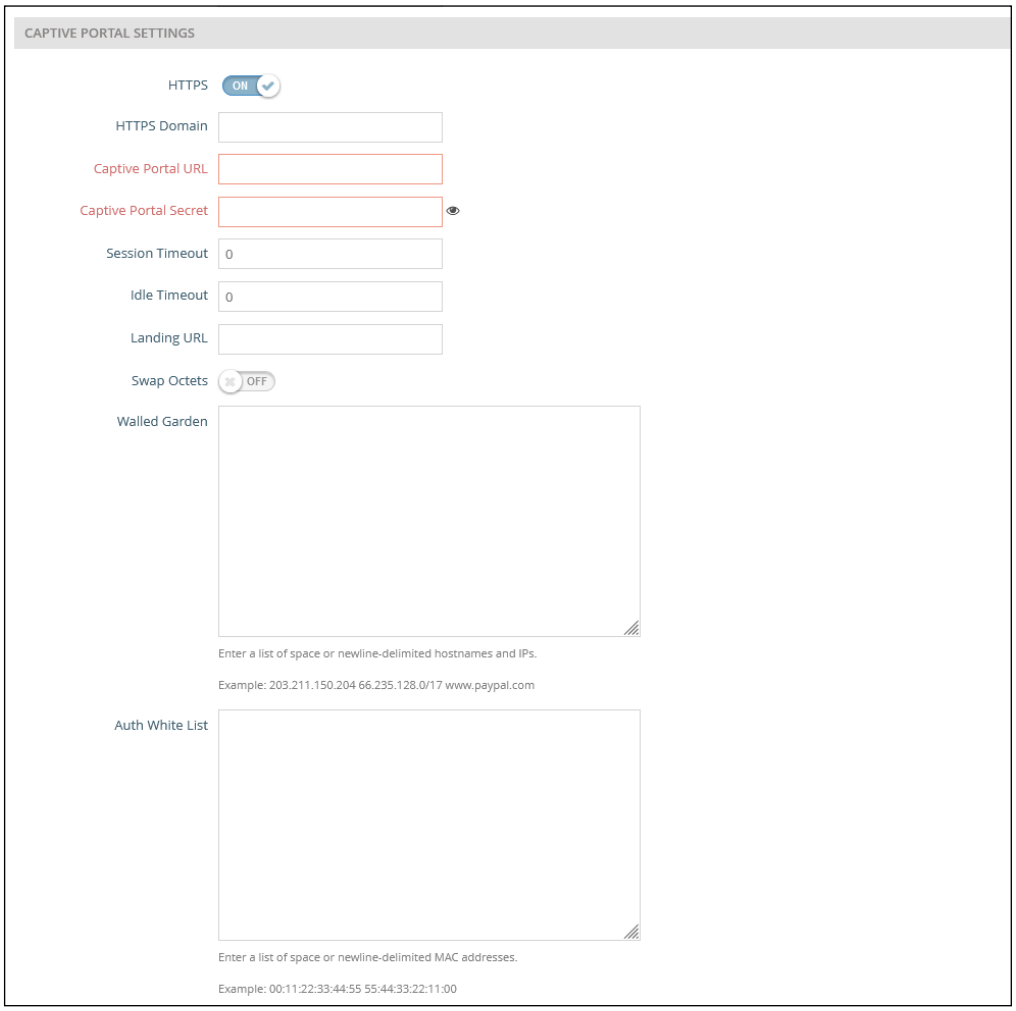
- **Enable RADIUS Auth** — Enables or disables client authentication via a RADIUS server.
- **RADIUS Server 1** — IP address or host name of the primary RADIUS server.
- **RADIUS Server 2** — IP address or host name of the secondary RADIUS server.
- **RADIUS Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Range: 1-255 characters).
- **RADIUS Auth Port** — RADIUS server UDP port used for authentication messages. (Range: 1-65535, Default: 1812)
- **RADIUS Acct Port** — RADIUS server UDP port used for accounting messages. (Range: 1-65535, Default: 1813)
- **Enable RadSec** — An authentication and authorization protocol for transporting RADIUS datagrams over TCP and TLS. RadSec replaces UDP used in the initial RADIUS design, providing a reliable transport protocol and more extensive security for the packet payload.
- **RADIUS Auth Method** — Selects the encryption method to use for messages between the AP and the RADIUS server; CHAP, PAP, or MSCHAPv2. The encryption method must match that used by the RADIUS server.

- **Local ID** — Local RADIUS server identifier.
- **Local Name** — Local RADIUS server name
- **NAS ID** — Local RADIUS server operation identifier.

Captive Portal Settings

The following section is displayed for all hotspot mode options.

Figure 36: Hotspot Settings (Captive Portal Settings)



The following items are displayed on this page:

- **HTTPS** — Enables HTTPS for the captive portal. (Default: Disabled)

Note: To upload a unique security certificate from a trusted certification authority for the HTTPS captive portal, see "Upload Certificate" on page 88.

- **HTTPS Domain** — The domain name of the HTTPS captive portal.
- **Captive Portal URL** — Host name of Internet service portal for the hotspot.

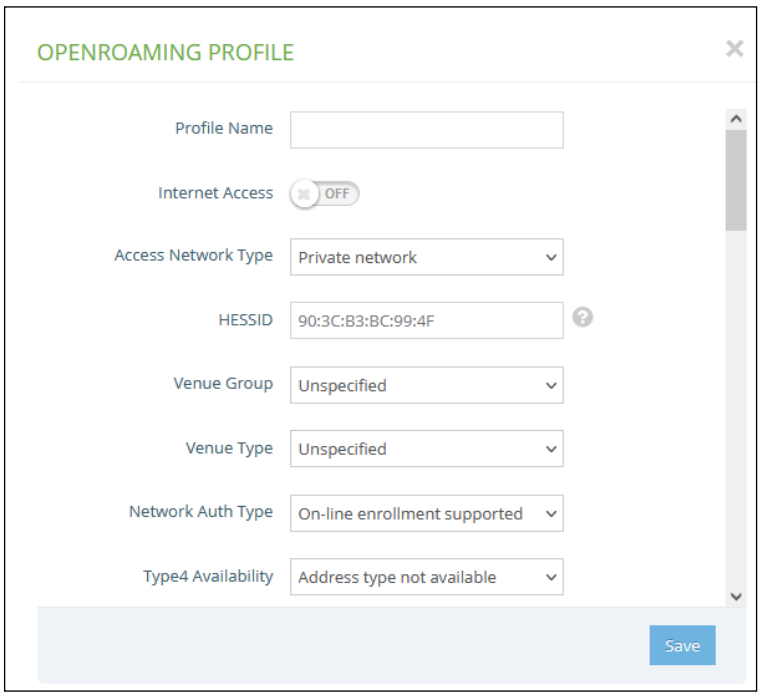
  The captive portal forces a hotspot client to access a welcome web page (normally used for authentication) before gaining further access to the Internet. The welcome page may require authentication and/or payment.
- **Captive Portal Secret** — The password used for logging into the hotspot.
- **Customize Splash Page** — This option is shown for all hotspot service options other than External Captive Portal Service. If enabled, fill in information for the title, background color, logo image file, and optional terms and conditions.
- **Session Timeout** — The maximum time a client can stay attached to the hotspot. (Range: 0-86400 seconds)
- **Idle Timeout** — The maximum a connection can remain inactive before it is closed. (Range: 0-86400 seconds)
- **Landing URL** — Indicates the URL to which the user is directed after logging in to the captive portal.
- **Swap Octets** — Swap the values of the reported “input octets” and “output octets.” This option only appears under External Captive Portal Service.
- **Walled Garden** — A list of web sites to which unauthenticated users are allowed to navigate.
- **Auth White List** — A list of MAC addresses that are allowed to bypass the captive portal to access the Internet.

OpenRoaming

OpenRoaming provides a standard for public-access Wi-Fi networks to support seamless roaming between wireless networks. An OpenRoaming network advertises its public Wi-Fi capabilities and services so that clients can decide if they want to connect to the network.

Up to 32 OpenRoaming profiles can be configured and applied to specific wireless networks (see "OpenRoaming" under "Wireless Networks — Network Settings" on page 76). Click "Add New" to configure a profile.

Figure 37: OpenRoaming Profile



The following items are displayed on this page:

- **Profile Name** — A name that identifies the profile.
- **Internet Access** — Enable if this network provides access to the Internet.
- **Access Network Type** — Select one from the predefined list.
  - **Private network** — Home and enterprise networks that unauthorized users cannot access.
  - **Private network with guest access** — A private network that provides for guest access. A typical example would be an enterprise network that offers guest access.

- **Chargeable public network** — A network that is available to all users, but requires a fee.
- **Free Public Network** — A network that is available to all users without any fees.
- **Personal device network** — A network for peripheral connectivity in an ad-hoc mode. For example, a camera that connects to a printer.
- **Emergency services only network** — A network that is dedicated for access to emergency services only.
- **Test or experimental** — A network for tests or experimental work.
- **Wildcard** — When selected, the AP will reply to clients regardless of the network type requested by the client query.

- **HESSID** — The Homogenous Extended Service Set Identifier (HESSID) for the OpenRoaming network. When configured, the HESSID (a MAC address) uniquely identifies all APs belonging to the same network.
- **Venue Group** — Identifies the general class of the venue. Select from the predefined list.
- **Venue Type** — Identifies the specific type of venue within each group.
- **Network Auth Type** — Specifies the authentication required for the network. Select an option from the predefined list. (Default: "Acceptance of terms and conditions")
- **Type4 Availability** — Specifies the IPv4 address type available from the network.
- **Type6 Availability** — Specifies the IPv6 address type available from the network
- **Operating Class** — A standard index (based on IEEE Std 802.11-2012 Annex E) that specifies the AP supported operating channels.
- **Captive Portal** — Enables the Captive Portal feature. (Default: Disabled)
  - **Captive Portal URL** — Host name of Internet service portal (HTTP or HTTPS).

    A captive portal forces a client to access a welcome web page (normally used for authentication) before gaining further access to the Internet. The welcome page may require authentication and/or payment.

- **Wall Garden** — A list of web sites to which unauthenticated users are allowed to navigate. Enter a list of space or newline-delimited host names and IP addresses.

- **Venue Name Information** — Configures a list of up to 10 venue names.
  - **Language Code** — Select a language from the list. (Default: English)
  - **Venue Name** — The name of the network venue. Multiple names can be added to the list.
  - **Venue URL** — Specifies a URL that provides additional venue information to users.

- **Cellular Network Information List (PLMN)** — (Optional) Identifies the 3GPP cellular networks available through the AP. Specifically, this field identifies the Public Land Mobile Network (PLMN) ID, comprised of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the mobile operator. Up to 10 PLMN IDs can be configured. Input the pair of MCC, MNC.
  For example: 400, 00
  MCC: Three decimal digits (000-999)
  MNC: Two (00-99) or three decimal digits (000-999)

- **Operator Friendly Name** — The name of the network operator and the specified language. Up to 10 names can be configured.

- **Roaming Consortium List** — (Optional) A roaming consortium is a group of service providers (SP) with which a user's credentials can be used for authentication. Each roaming consortium is identified by an organization identifier (OI) that is assigned by the IEEE. An OI is often 24 bits in length, but can also be 36 bits. Up to 10 identifiers can be configured.

- **Domain Name List** — Lists one or up to 10 domain names for the entity operating the AP. This is critical for OpenRoaming network selection policy, as it identifies the operator of the network. It indicates to the mobile device whether they are at a home hotspot or a visited hotspot.

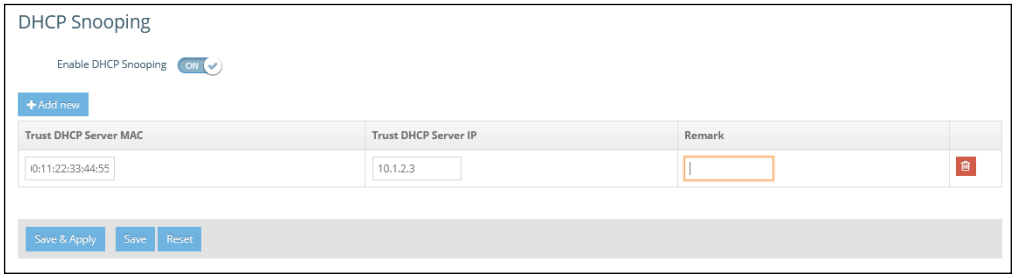
- **NAI Realm List** — (Optional) The network access identifier (NAI) realm list identifies those service provider or other networks that are accessible through the AP. By discovering which authentication realms are supported by a network, a mobile device can selectively authenticate to its preferred network. Up to 10 identifiers can be configured.
  - **Method/Authentication** — Specifies EAP methods and authentication for each service provider added to the NAI Realm List.

DHCP Snooping

DHCP snooping is used to validate and filter DHCP messages received by the AP. When DHCP snooping is enabled, DHCP messages received from a device not listed in the DHCP snooping table are dropped.

You can add known and trusted DHCP servers to the table by specifying their MAC and IP addresses.

Figure 38: DHCP Snooping



The following items are displayed on this page:

- **Enable DHCP Snooping** — Enables DHCP Snooping on the AP.
- **Trust DHCP Server MAC** — The MAC address of a known and trusted DHCP server.
- **Trust DHCP Server IP** — The IP address of a known and trusted DHCP server.
- **Remark** — A comment relating to the DHCP server configured.

ARP Inspection

ARP Inspection is a security feature that validates the MAC Address bindings for Address Resolution Protocol packets. It provides protection against ARP traffic with invalid MAC-to-IP address bindings, which forms the basis for certain "man-in-the middle" attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

Figure 39: ARP Inspection

The following items are displayed on this page:

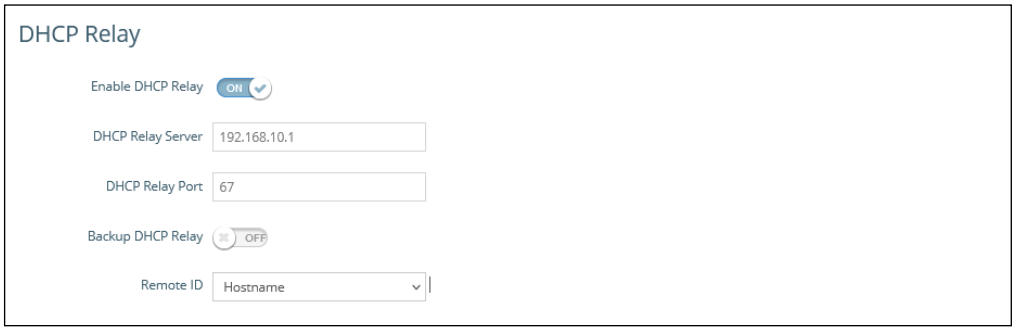
- **ARP Inspection** — When enabled, ARP packets are validated against ARP spoofing.
- **Force DHCP** — Allows the AP to only learn MAC/IP pair information through DHCP packets. Since devices configured with static IP address do not send DHCP traffic, any clients with static IP addresses will be blocked by the AP unless their MAC/IP pair is listed and enabled in the Static Trust List.
- **Trust List Broadcast** — Lets other APs learn the trusted MAC/IP pairs to issue ARP requests.
- **Static Trust List** — Adds the MAC or MAC/IP pairs of devices that are trusted to issue ARP requests. Other network nodes can still send their ARP requests, but if their IP appears in the static list with a different MAC, their ARP requests will be dropped.

DHCP Relay

When DHCP relay is enabled, the AP as an agent for all clients and sends all broadcast DHCP requests directly to a specified DHCP server. The DHCP server IP address and port must be configured, and optionally a backup server.

With DHCP relay enabled, the circuit ID can be set on the VLAN settings or LAN settings page. IP addresses of clients are then obtained by the DHCP relay server and the IP range is determined by the remote ID and circuit ID.

Figure 40: DHCP Relay



The following items are displayed on this page:

- **Enable DHCP Relay** — Enables the DHCP relay feature on the AP.
- **DHCP Relay Server** — Specifies the IP address of the DHCP server.
- **DHCP Relay Port** — Specifies the port of the DHCP server.
- **Backup DHCP Relay** — Optionally specifies a backup DHCP server IP address and port to use if there is no response from the primary server.
- **Remote ID** — Use the hostname as the remote ID, or manually configure a text string as the remote ID.

4 Wireless Settings

This chapter describes the wireless settings on the access point. It includes the following sections:

Radio Settings

The IEEE 802.11 wireless interfaces include configuration options for radio signal characteristics and wireless security features.

The access point can operate in several radio modes, 802.11b+g+n/ax (2.4 GHz) or 802.11a/a+n/ac+a+n/ax (5 GHz). Note that the dual-band access points can operate at 2.4 GHz and 5 GHz at the same time. The web interface identifies the radio configuration pages as:

- **Radio 2.4 GHz** — the 2.4 GHz 802.11b/g/n/ax radio interface
- **Radio 5 GHz** — the 5 GHz 802.11a/n/ac/ax radio interface
- **HaLow** — the HaLow (863-928 MHz) radio interface (EAP112 only)

Each radio supports 16 virtual access point (VAP) interfaces based on the SSIDs, referred to as SSID1 ~ SSID16. Each VAP functions as a separate access point, and can be configured with its own Service Set Identification (SSID) and security settings. However, most radio signal parameters apply to all VAP interfaces. Traffic to specific VAPs can be segregated based on user groups or application traffic. The clients associate with each VAP in the same way as they would with separate physical access points.

Physical Radio Settings

Figure 41: Physical Settings for Radio 5 GHz

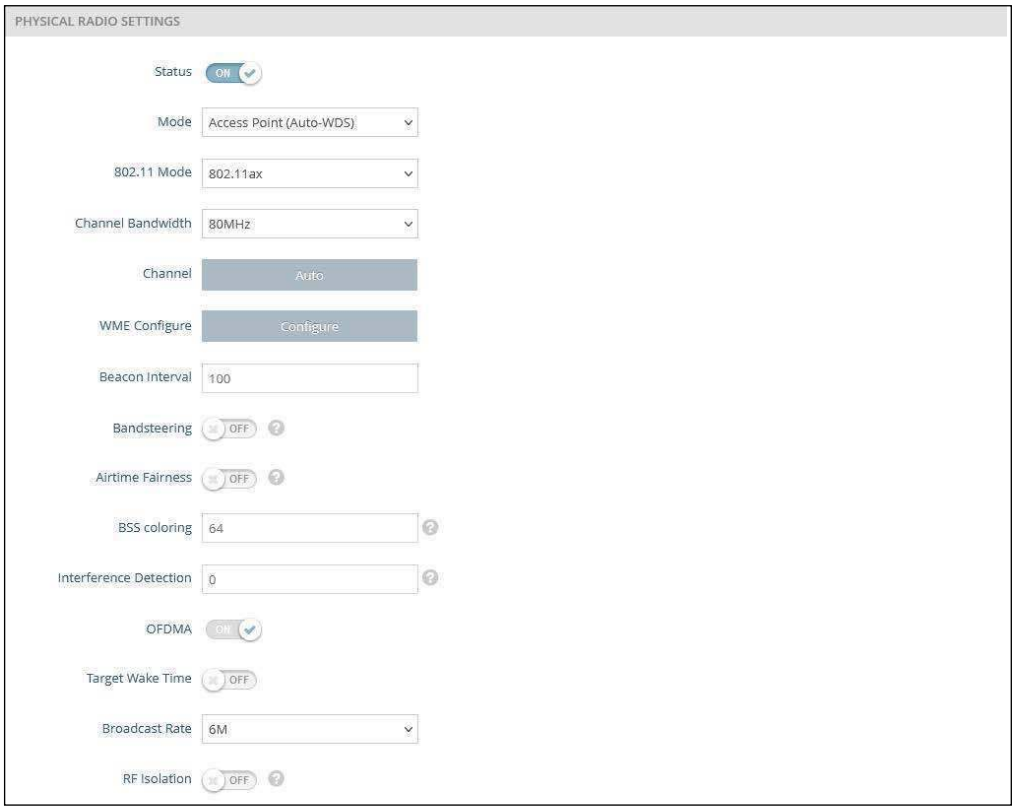


Figure 42: Physical Settings for Radio 2.4 GHz

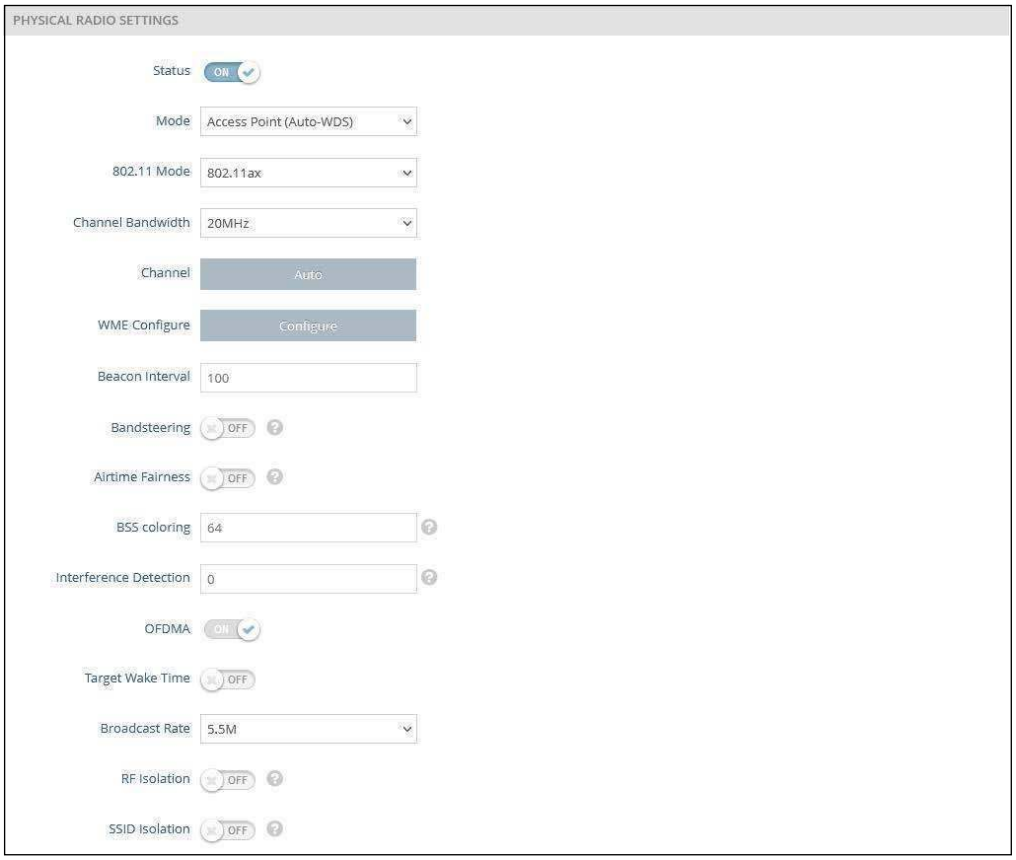
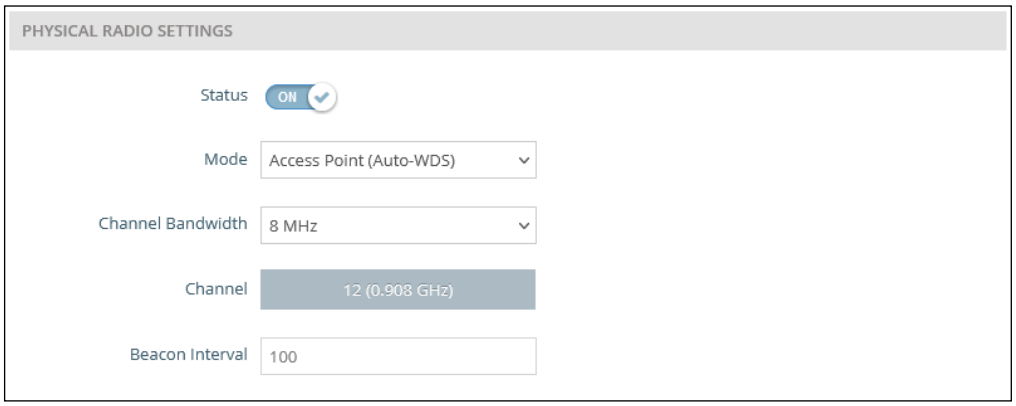


Figure 43: Physical Settings for HaLow (EAP112)



The following items are displayed on this page:

- **Status** — Enables or disables the wireless service on this interface.
- **Mode** — Selects the mode in which the AP will function.
  - **Access Point (Auto-WDS)** — The AP operates as an access point in WDS mode, which accepts connections from APs in Client WDS mode. (This is the default setting.)

In this mode, the AP provides services to clients as a normal access point. WDS is used to automatically search for and connect to other AP nodes using the same SSID and security settings.

- **Client** — The AP can provide a wireless connection to another AP, as well as pass information from or to locally wired hosts and wireless clients.

- **802.11 Mode** — Defines the radio operation mode.
  - **Radio 2.4 GHz** — Default: 11ax; Options: 11b+g+n/ax
  - **Radio 5 GHz** — Default: 11ax; Options: 11a, 11a+n, 11ac+a+n, 11ax

- **Channel Bandwidth** — The AP options for channel bandwidth include 20, 40 80, and 160 MHz. The available channel bandwidth is dependent on the 802.11 Mode. (Default: 20 MHz on 2.4 GHz Radio, 80 MHz on 5 GHz Radio; Options: 20 MHz, 40 MHz, 80MHz, 160MHz)
  - **1–8 MHz** — For 802.11ah HaLow (EAP112 only)
  - **20MHz** — For 802.11b+g+n and 802.11ax
  - **40MHz** — For 802.11b+g+n, 802.11a, 802.11a+n, 802.11ac+a+n and 802.11ax
  - **80MHz** — For 802.11ac+a+n and 802.11ax
  - **160MHz** — (Supported only on EAP104, EAP111, EAP112 and OAP101 5 GHz radio) For 802.11ac+a+n and 802.11ax

- **Channel** — The radio channel that the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, for 11g/n 20 MHz mode you can deploy up to three access points in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the access point to which it is linked. (The available channels are dependent on the 802.11 Mode, Channel Bandwidth, and Country Code settings.)

  Selecting Auto enables the access point to automatically select an unoccupied radio channel. (Default: Auto)

- **WME Configuration** — Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features for IEEE 802.11 networks. Access priority can be configured for four "Access Category"(AC) types using the following parameters:
  - **CW Min (Minimum Contention Window)** – The initial upper limit of the random backoff wait time before wireless medium access can be attempted. The initial wait time is a random value between zero and the

CWMin value. Specify the CWMin value in the range 0-15 microseconds. Note that the CWMin value must be equal or less than the CWMax value.

- **CW Max (Maximum Contention Window)** – The maximum upper limit of the random backoff wait time before wireless medium access can be attempted. The contention window is doubled after each detected collision up to the CWMax value. Specify the CWMax value in the range 0-15 microseconds. Note that the CWMax value must be greater or equal to the CWMin value.

- **AIFS (Arbitration Inter-Frame Space)** – The minimum amount of wait time before the next data transmission attempt. Specify the AIFS value in the range 0-15 microseconds.

- **TXOP Limit (Transmit Opportunity Limit)** – The maximum time an AC transmit queue has access to the wireless medium. When an AC queue is granted a transmit opportunity, it can transmit data for a time up to the TXOP Limit. This data bursting greatly improves the efficiency for high data-rate traffic. Specify a value in the range 0-8192 microseconds.

- **Beacon Interval** — The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They also carry power-management and other information. (Range: 100-1024 TUs; Default: 100 TUs)

- **Bandsteering** — When enabled, clients that support 2.4 GHz and 5 GHz are first connected to the 5 GHz radio. This feature helps balance the client load over the two radio bands. Note that both radios must have configured SSIDs and security settings that match for this feature to fully operate. (Default: Off)

- **Airtime Fairness** — Enabling this feature improves the overall performance of the wireless network. (Default: Disabled)

- **BSS coloring** — In 802.11ax (Wi-Fi 6) mode, BSS coloring allows nearby APs operating at the same frequency to identify traffic belonging to their own Basic Service Set (BSS). The BSS coloring enables Wi-Fi 6 networks to operate more efficiently in high-density environments where neighboring AP and client transmissions overlap. Assign a color value (a number from 1 to 63) to identify the radio BSS, or enter value 64 to allow the AP to randomly select a color value. (Range: 1-63, 64 random; Default: 64)

- **Interference Detection** — When the utilization in current channel reaches the configured threshold (as a percentage), the AP switches to a different channel. (Range: 0 - 100%; Default: 0, disabled)

- **OFDMA** — The 802.11ax (Wi-Fi 6) mode supports Orthogonal Frequency Division Multiple Access (OFDMA) and this cannot be disabled.

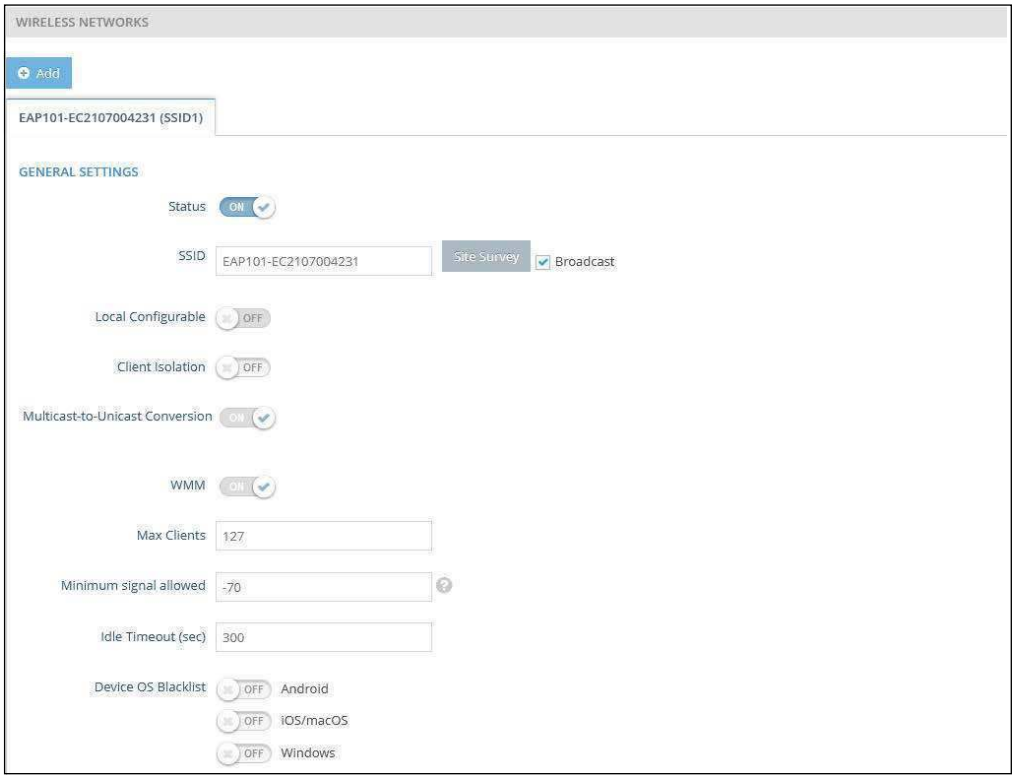
- **Target Wake Time** — In 802.11ax (Wi-Fi 6) mode, the AP can allow clients to request a specific Target-Wakeup Time (TWT) to transmit or receive frames,

rather than rely on periodic beacons. This feature enables client devices to have much longer sleep states and results in significant power savings. In addition, the AP can control and schedule client TWTs to both manage contention in the network and accommodate delay-sensitive traffic. (Default: Disabled)

- **Broadcast Rate** — Allows a limit to be placed on the wireless bandwidth consumed by broadcast packets.
  - **Radio 2.4 Ghz** — Options: 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 5.5M
  - **Radio 5 Ghz** — Options: 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 6M
- **RF Isolation** — When enabled, clients are isolated between different radio cards.
- **SSID Isolation** — When enabled, clients are isolated between different SSIDs on the same radio cards.

Wireless Networks — General Settings

Figure 44: Radio Settings (General Settings)



The following items are displayed in this section of the Wireless Settings page:

- **Status** — Enables or disables the wireless service on this VAP.

- **SSID** — The name of the basic service set provided by a Virtual Access Point (VAP) interface. Clients that want to connect to the network through the access point must set their SSID to the same as that of the access point's VAP interface. (Default: Edgecore5G-# (where # is 1-16) for 5 GHz, Edgecore2.4G-# (where # is 1-16) for 2.4 GHz; Range: 1-32 characters)

- **Site Survey** — Scans for all wireless networks that are broadcasting their SSID.

- **Broadcast** — The SSID can be broadcast at regular intervals so that wireless stations searching for a network connection can discover it. This allows wireless clients to dynamically discover and roam between WLANs. This feature also makes it easier for hackers to break into your home network. Because SSIDs are not encrypted, it is easy to grab one by snooping the WLAN looking for SSID broadcast messages coming from the AP. (Default: Enabled)

- **Local Configurable** — Enables the SSID to be user configurable when the system is operating in MSP mode (see "System Settings" on page 83). (Default: Disabled)

- **Client Isolation** — When enabled, wireless clients can talk to the LAN, and reach the Internet if such connection is available, but they cannot communicate with one another. (Default: Disabled)

- **Multicast-to-Unicast Conversion** — When enabled, the AP converts multicast traffic to unicast traffic and sends it to each associated client. This feature provides a network throughput enhancement, since the AP transmits multicast traffic at a low basic rate, whereas unicast traffic can be transmitted at HT, VHT, or HE rates.

- **Max Clients** — The maximum number of clients that can associate to this SSID at the same time. (Default: 127; Range: 1-256)

- **Minimum signal allowed** — Only allows clients to connect to the radio interface if their signal strength (RSSI) is equal or greater than the specified value. Setting the value to -100 disables this feature. Clients already connected are checked periodically. (Range: -1 to -100; Default: -100)

  This forces clients to associate with an AP that has a better signal strength (also called assisted roaming). Suggested value is -70 to -80 depending on access point density and coverage.

- **Idle Timeout (sec)** — The AP disconnects a client when there is no activity for the configured amount of time. (Default: 300 seconds; Range: 60-60000 seconds)

- **Device OS Blacklist** — Denies access to the SSID from client devices with either Android, iOS/macOS, or Windows operating systems. Set to ON to prevent a client OS from connecting to the SSID. Set to OFF to allow a client OS to connect to the SSID.

Wireless Networks — Security Settings

Figure 45: Wireless Security Settings

The following items are displayed in this section of the Wireless Settings page:

- **Method** — Sets the wireless security method for each VAP, including association mode, encryption, and authentication. (Default: WPA2-PSK)
  - **No Security** — The VAP broadcasts a beacon signal including the configured SSID. Wireless clients with an SSID setting of "any" can read the SSID from the beacon and automatically set their SSID to allow immediate connection.
  - **WPA-PSK** — For enterprise deployment, WPA requires a RADIUS authentication server to be configured on the wired network. However, for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access. The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the access point and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks.
    - **Encryption** — Data encryption uses one of the following methods:
      - **CCMP (AES)** — AES-CCMP is used as the multicast encryption cipher. AES-CCMP is the standard encryption cipher required for WPA2. (This is the default setting.)
      - **Auto: TKIP + CCMP (AES)** — The encryption method used by the client is discovered by the access point.
    - **Key Method** — Uses one of the following PSK methods:
      - **Single PSK** — Enables the entry of a single PSK key.
        - **Key** — WPA is used to encrypt data transmitted between wireless clients and the VAP. WPA uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

String length must be 8 to 63 ASCII characters (letters and numbers). No special characters are allowed.

- **Multiple PSK** —Enables the entry of multiple PSK keys. Up to 128 keys can be configured.

  - **Multiple Keys** — Enter multiple keys, one per line. Entering a key with a specific MAC address limits the key for use by a single client. Entering a key without a MAC address enables the key to be used by all clients.

    Multiple keys are supported for WPA-PSK, WPA2-PSK, and WPA3 Personal Transition security.

  - **Dynamic PSK** — Enables the use of dynamic PSK keys that are periodically generated and updated by a RADIUS authentication server. The RADIUS server IP address, UDP port, and secret text string must be specified. (See "RADIUS Settings" below for details.)

    Dynamic keys are supported only for WPA2-PSK security.

- **WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication.

  WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

  Refer to WPA-PSK for a description of encryption methods and the key.

- **WPA-EAP** — WPA employs a combination of several technologies to provide an enhanced security solution for 802.11 wireless networks. A RADIUS server is used for authentication, and can also be used for accounting.

  Refer to WPA-PSK for a description of encryption methods.

- **RADIUS Settings** — A RADIUS server must be specified for the access point to implement IEEE 802.1X network access control and Wi-Fi Protected Access (WPA) wireless security.

  In addition, you can configure a RADIUS Accounting server to receive user-session accounting information from the access point. RADIUS Accounting can be used to provide valuable information on user activity in the network.

Note: This guide assumes that you have already configured RADIUS server(s) to support the access point. Configuration of RADIUS server software is beyond the

scope of this guide, refer to the documentation provided with the RADIUS server software.

- **Radius Auth Server** — Specifies the IP address or host name of the RADIUS authentication server.
- **Radius Auth Port** — The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- **Radius Auth Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS authentication server. Do not use blank spaces in the string. (Maximum length: 255 characters)
- **NAS ID** — The RADIUS NAS identifier for the SSID interface This value must be between 1 and 48 characters long.
- **Backup Radius Auth** — Enables the support of a backup RADIUS authentication server.
  - **Radius Auth Server** — Specifies the IP address or host name of the backup RADIUS authentication server.
  - **Radius Auth Port** — The UDP port number used by the backup RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
  - **Radius Auth Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the backup RADIUS authentication server. Do not use blank spaces in the string. (Maximum length: 200 characters)
- **Use Radius Accounting** — Enables the support of a RADIUS accounting server.
  - **Acct Server** — Specifies the IP address or host name of the RADIUS accounting server.
  - **Acct Port** — The UDP port number used by the RADIUS server for accounting messages. (Range: 1024-65535; Default: 1813)
  - **Acct Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS accounting server. Do not use blank spaces in the string. (Maximum length: 200 characters)

- **Acct Interim Interval** — The time (in seconds) between each accounting update sent to the server. (Range: 60-600 seconds; Default: 60 seconds)

- **WPA2-EAP** — WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

  A RADIUS server is used for authentication, and can also be used to accounting.

  Refer to WPA-PSK for a description of encryption methods.

  Refer to WPA-EAP for a information on configuring the RADIUS server.

- **WPA3 Personal** — Clients using WPA3 with Simultaneous Authentication of Equals (SAE) are accepted for authentication.

  WPA3 provides more robust password-based authentication called Simultaneous Authentication of Equals (SAE), which replaces Pre-Share Key (PSK) in WPA2-Personal. This technology prevents offline dictionary attacks so that data traffic can be transmitted securely.

- **WPA3 Personal Transition** — Clients using WPA3 with SAE or clients using WPA2 with PSK are accepted for authentication. The AP negotiates the supported authentication and encryption with each client before allowing access to the network.

- **WPA3 Enterprise** — An enhanced version of WPA2-EAP security that uses more robust encryption. Clients must support one of the stronger WPA3 encryption options and use Protected Management Frames (PMF) to be able to access the network. The use of IEEE 802.1X network access control and a RADIUS server is required.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **WPA3 Enterprise Transition** — Allows WPA3 and WPA2 clients to access the network. Encryption options and the use of Protected Management Frames (PMF) are negotiated with each client before allowing access to the network.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **WPA3 Enterprise 192-bit** — WPA3 Enterprise security uses a standard 128-bit encryption. For a network handling more sensitive data, there is an option to use 192-bit encryption for additional protection.

Refer to RADIUS Settings above for information on RADIUS configuration.

- **OWE** — Opportunistic Wireless Encryption (OWE) is the WPA3 open network security that allows users of public Wi-Fi networks to gain secure access without using a password. OWE provides individual encryption of data communications between the AP and each client, but does not provide authentication of user identities.

- **PMF** — Protected Management Frames (PMF) provide WPA2/WPA3 security for unicast and multicast management frames between the AP and clients. The "Optional" setting allows clients that do not support PMF to access the network. The "Mandatory" setting allows only clients that support PMF to access the network. (Default: Optional)

- **802.11k** — Provides clients with information on neighbor APs when roaming. As a client is about to roam from an AP, it sends a request for a "Neighbor Report" that includes a list of available APs and associated information. The client can then quickly identify the best AP to which it can roam without having to scan all channels. (Default: Disabled)

- **802.11r** — Provides a method for fast transition roaming between APs. Before clients roam to a new AP, the initial handshake and encryption calculations are performed in advance, which results in a fast hand off without the need for re-authentication. (Default: Disabled)

- **802.11v** — Provides information to associated clients that facilitates the overall improvement of the wireless network. Also helps clients to improve battery life by setting the idle period. (Default: Disabled)

- **Radius MAC Auth** — The MAC address of the associating station is sent to a configured RADIUS server for authentication. (Default: Disabled)

- **Dynamic Authorization** — The Dynamic Authorization Extensions (DAE) to RADIUS enable a server to disconnect or change the authorization of clients that are already connected to the network. (Default: Disabled)

  - **DAE Port** — The UDP port number to use for DAE messages. (Default: 3799)

  - **DAE Client** — Specifies the IPv4 address of the RADIUS server.

  - **DAE Secret** — The shared text string used to encrypt DAE messages between the access point and the RADIUS server.

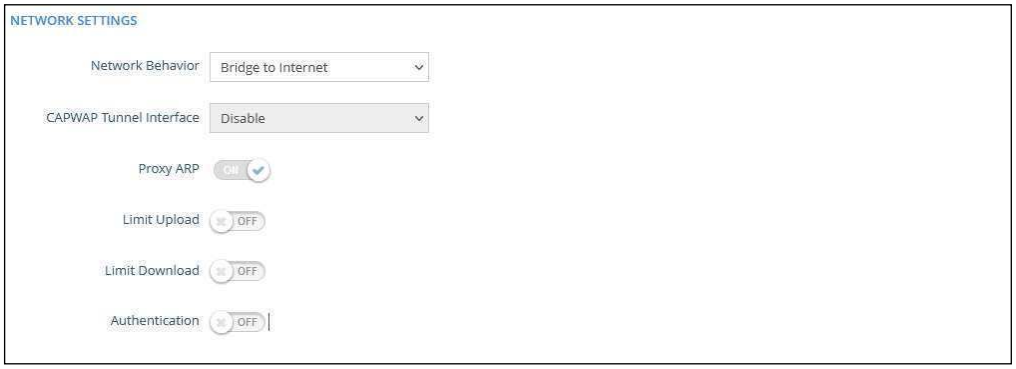
- **Access Control List** — Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point. (Default: OFF)

  - **Policy** — The MAC list can be configured to either allow or deny network access to specified clients. (Default: Allow all MACs on list)

- **Filtered MACs** — List of client MAC addresses. Up to 512 MAC addresses can be configured.

Wireless Networks — Network Settings

Figure 46: Wireless Network Settings



The following items are displayed in this section of the Wireless Settings page:

- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
  - **Bridge to Internet** — Configures an interface as attached to the WAN. Traffic from this interface is directly bridged into the Internet. (See Figure 29, "Bridge to Internet", on page 48.)
  - **Route to Internet** — Configures an interface as a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged to the Internet. (See Figure 30, "Route to Internet", on page 48.)
    - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.
  - **Add to Guest Network** — This interface can only support the guest network.
  - **Hotspot Controlled** — This interface can only support hotspot services.
    - **Configure Hotspot** — Opens Hotspot Settings page.
    - **Walled Garden** — Configures the Walled Garden list on the Hotspot Settings page.
  - **VLAN Tag Traffic** — Tags any packets passing from this VAP (virtual access point) to the associated Ethernet port with a VLAN ID configured under "VLAN Settings" on page 80.
    - **VLAN Id** — Selects the configured VLAN ID with which to tag the VAP traffic.

- **VLAN Settings** — Opens the VLAN Settings page.

- **Dynamic VLAN** — The RADIUS server provides the access point with the user VLAN information. The access point assigns the associated user to the related VLAN.

  - **Default VLAN Behavior** — Specifies the behavior (Accept or Reject) when a client's VLAN ID is not defined on the RADIUS server. The default setting is Reject.

    - **Reject** — A client cannot connect to the SSID when the client's VLAN ID is not defined on the RADIUS server.

    - **Accept** — A client can connect to the SSID with an assigned or untagged VLAN ID when the client's VLAN ID is not defined on the RADIUS server.

- **CAPWAP Tunnel Interface** — When the AP system management is set to EWS-Series Controller mode (see "System Settings" on page 83), the CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode can be configured. The options are "Disable," "Complete," or "Split." A Complete tunnel sends all management, authentication, and data traffic from the AP back to the controller. A Split tunnel only sends the management and authentication traffic to the controller. (Default: Disable)

- **Proxy ARP** — When Proxy ARP is enabled, the AP maintains its own ARP lookup table and replies to ARP requests on behalf of downstream stations, avoiding network inefficiencies. This feature is automatically enabled when client isolation is disabled, and disabled when client isolation is enabled. The feature cannot be configured manually. Proxy ARP is supported when the network behavior is "Bridge to Internet" or "VLAN Tag Traffic."

- **Limit Upload** — Enables rate limiting of traffic from the VAP interface as it is passed to the wired network. You can set a maximum rate in Kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

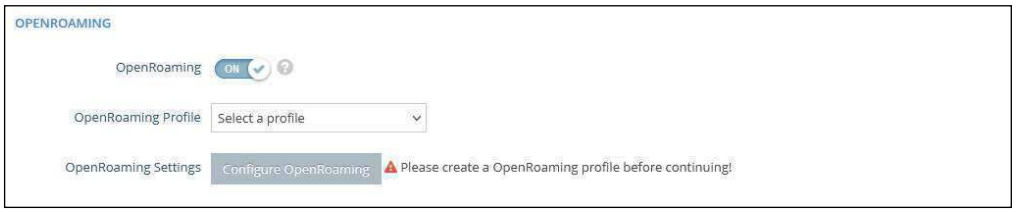
- **Limit Download** — Enables rate limiting of traffic from the wired network as it is passed to the VAP interface. You can set a maximum rate in kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

- **Authentication** — When the AP system management is set to ecCLOUD mode (see "System Settings" on page 83), this options authenticates the AP communications with the ecCLOUD controller. (Default: Disabled)

Wireless Networks — OpenRoaming

Available when WPA2-EAP security is selected, OpenRoaming (Hotspot 2.0) provides a standard for public-access Wi-Fi networks to support seamless roaming between wireless networks. A OpenRoaming AP advertises its public Wi-Fi capabilities and services so that clients can decide if they want to connect to the network.

Figure 47: OpenRoaming Settings



The following items are displayed in this section of the Wireless Settings page:

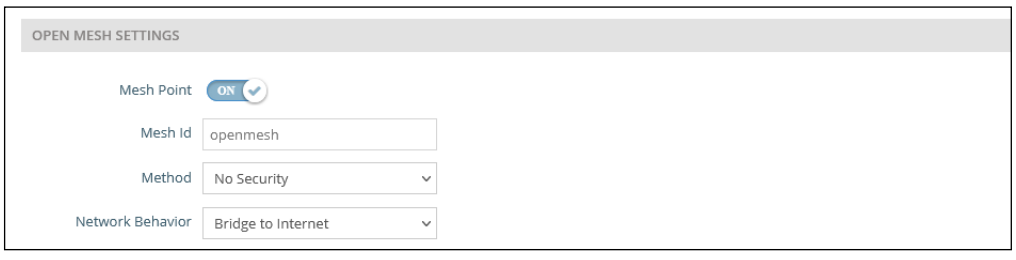
- **OpenRoaming** — Enables OpenRoaming when WPA2-EAP security is selected. (Default: Disabled)
- **OpenRoaming Profile** — Selects the profile to apply to the wireless network. See "OpenRoaming" on page 58 for profile configuration.
- **OpenRoaming Settings** — Click to access the OpenRoaming profile settings page. See "OpenRoaming" on page 58 for profile configuration.

Wireless Networks — Open Mesh Settings

Open Mesh is a network of interconnected node APs, of which only one has a wired connection to the network (and the Internet). The other AP nodes provide wireless links to each other and some support connections to wireless clients. The mesh network not only extends wireless connectivity over a greater distance, but also provides backup links should one node in the network fail.

When setting up an AP to be a node in a mesh network, select one radio interface (2.4 GHz or 5 GHz) and configure it to operate on a specific channel (do not select Auto).Set up other AP nodes to operate on the same radio interface, channel, and with the same SSID.

Figure 48: Open Mesh Settings



The following items are displayed in this section of the Wireless Settings page:

- **Mesh Point** — Enables Open Mesh support on the SSID interface.

- **Mesh ID** — Name of the mesh network.
- **Method** — Security applied on Open Mesh links.
  - **No Security** — None.
  - **WPA3-Personal** — Uses WPA3 with Simultaneous Authentication of Equals (SAE) on mesh links to other APs.
- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
  - **Bridge to Internet** — Configures an interface as attached to the WAN. Traffic from this interface is directly bridged into the Internet. (See Figure 29, "Bridge to Internet", on page 48.)
  - **Route to Internet** — Configures an interface as a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged to the Internet. (See Figure 30, "Route to Internet", on page 48.)
    - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.

Wireless Networks — Advanced Radio Settings

Figure 49: Advanced Radio Settings

The following items are displayed in this section of the Wireless Settings page:

- **Tx Power** — Adjusts the power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the AP model and the Country setting.)
- **SGI** — Enables the Short Guard Interval (SGI) in the following 802.11 modes:
  5 GHz radio; 802.11a, 802.11a+ n, 802.11ac+a+n.
  2.4 GHz radio; 802.11 b g+ n.

  The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns Short Guard Interval is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to

propagation delays, echoes, and reflections to which digital data is normally very sensitive. Enabling SGI sets it to 400ns. (Default: Disabled)

VLAN Settings

VLANs (virtual local area networks) are turned off by default. If turned on they will automatically tag any packets passed to the LAN port from the relevant VAP (virtual access point).

The access point can employ VLAN tagging to control access to network resources and increase security. VLANs separate traffic passing between the access point, associated clients, and the wired network. You can create up to 16 VLAN tagged networks.

Note the following points about the access point's VLAN support:

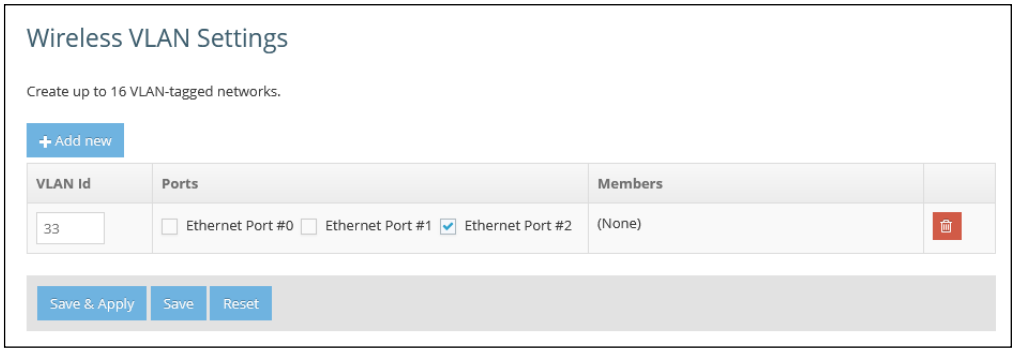
- If an Ethernet LAN port on the access point is assigned a VLAN ID, any traffic entering that port must be also tagged with the same VLAN ID.
- Wireless clients associated to the access point can be assigned to a VLAN. Wireless clients are assigned to the VLAN for the VAP interface with which they are associated. The access point only allows traffic tagged with correct VLAN IDs to be forwarded to associated clients on each VAP interface.
- When VLAN support is enabled on the access point, traffic passed to the wired network is tagged with the appropriate VLAN ID. When an Ethernet port on the access point is configured as a VLAN member, traffic received from the wired network must also be tagged with the same VLAN ID. Received traffic that has an unknown VLAN ID or no VLAN tag is dropped.
- When VLAN support is disabled, the access point does not tag traffic passed to the wired network and ignores the VLAN tags on any received frames.
- Network IP range conflict detection and resolution — The AP has two built-in local networks - one "main" network, and the more secure "guest" network. By default, the subnet ranges of these networks is set to 192.168.2.1 and 192.168.3.1, respectively.

  If your network is already configured to use one of these subnets, when you plug in your network cable to the WAN port of your AP, there would normally be an IP conflict in the local AP's network and your upstream network.

  However, if your WAN subnet conflicts with any of the local networks (even the custom ones you create), the AP will automatically change the subnet of the local network.

Note: Before enabling VLAN tagging on the access point, be sure to configure the attached network switch port to support tagged VLAN frames for the VLAN IDs configured on the access point. Otherwise, connectivity to the access point will be lost when you enable the VLAN feature.

Figure 50: Configuring VLANs



The following items are displayed on this page:

- **VLAN ID** — A VLAN identifier to be assigned. (Range: 2-4094) (VLANs 1 is reserved for internal use.)
- **Ports** — The Ethernet ports assigned to the specified VLAN.
- **Members** — The SSID of a VAP configured to be a member of the specified VLAN. This option is configured under Radio Settings (Network Settings – Network Behavior).

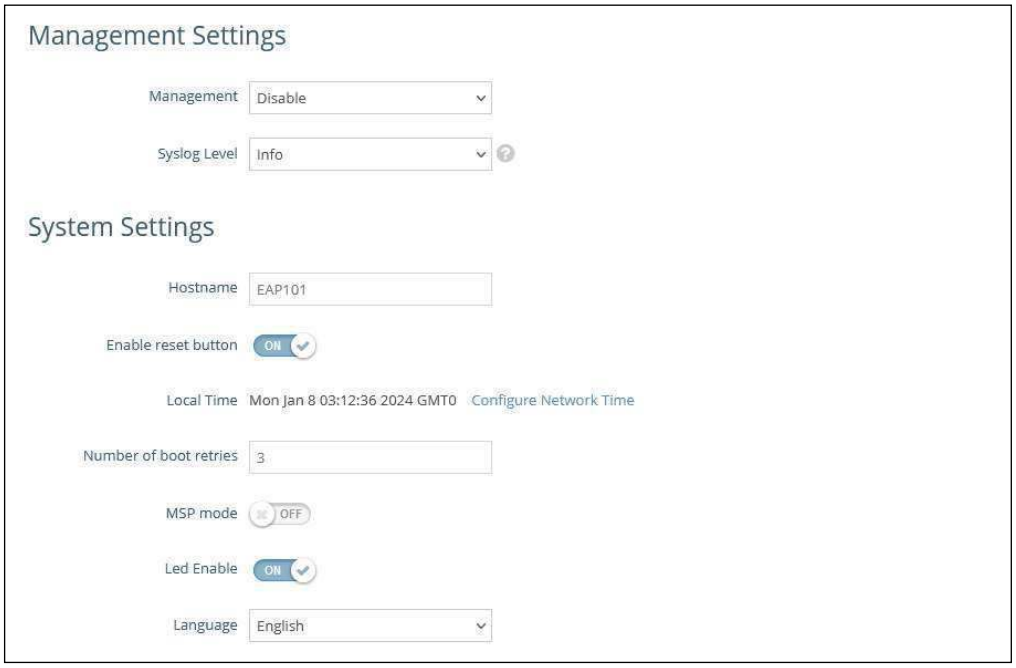
5 System Settings

This chapter describes maintenance settings on the access point. It includes the following sections:

System Settings

The System Settings page can be used to enable the AP to be managed from the Edgecore ecCLOUD controller or EWS-Series Controller, and configure general descriptive information about the AP.

Figure 51: System Settings



The following items are displayed on this page:

- **Management** — Set to "ecCLOUD" to manage this AP from the Edgecore ecCLOUD controller. Set to "EWS-Series Controller" to manage this AP from an Edgecore EWS-Series controller in the local network. Set to disable to manage the AP through the web interface in a stand-alone mode.
  - **ecCLOUD** — When selected, the following parameters are displayed:
    - **Controller URL** — Provides a URL link to the Edgecore ecCLOUD controller management site.
    - **Enable agent** — Enables the AP to be managed from the ecCLOUD controller.
      - **Registration URL** — Specifies the URL for device registration.
    - **Log Level** — Adjusts the system log level for the ecCLOUD daemon (mgmtd). The default value is Info. The standard ranking of log levels is as follows: Trace < Debug < Info < Warn < Error.

- **EWS-Series Controller** — When selected, the following parameters are displayed:
  - **CAPWAP** — Enables CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode.
  - **DNS SRV Discovery** — The AP uses DNS server records to discover the EWS controller to which it can send a CAPWAP join request.
    - **Domain Name Suffix** — Specifies the domain suffix of the controller.
  - **DHCP Option Discovery** — The AP uses the DHCP server to obtain an IP address in the same subnet as the EWS controller, which it can then discover and send a CAPWAP join request.
  - **Broadcast Discovery** — The AP sends broadcast requests to discover the EWS controller in the same subnet.
  - **Multicast Discovery** — The AP sends multicast discover packets across the network to find the EWS controller. This option requires routing paths to be properly configured in the network.
  - **Static Discovery** — Provides a manual method to reach an EWS controller by entering IP addresses that the AP uses to send a CAPWAP join request.

- **Syslog Level** — Limits system log messages based on severity. The standard ranking of log levels is as follows: Debug < Info < Notice < Warning < Error < Critical < Alert < Emergency. (Default: Info)
- **Hostname** — An alias for the AP, enabling the device to be uniquely identified on the network. (Default: EAP101; Range: 1-63 ASCII characters. Only accepts A-Z, a-z, 0-9, and dash "-".)
- **Enable Reset Button** — Enables the AP's hardware reset button. (Default: Enabled)
- **Local Time** — The local time, given as day of week, month, time, year.
- **Number of boot retries** — The maximum number of bootup retries before switching to the next boot bank. (Range: 1-254; Default: 3)
- **MSP Mode** — Enables the Managed Service Provider (MSP) mode that prevents end-users from accessing and modifying most device settings from user-defined user accounts. Management access from "root" and "admin" accounts still provide full access to all device settings. (Default: Disabled)

  With MSP mode enabled, service providers have the option of making specific wireless SSID settings available for user configuration by enabling the "Local

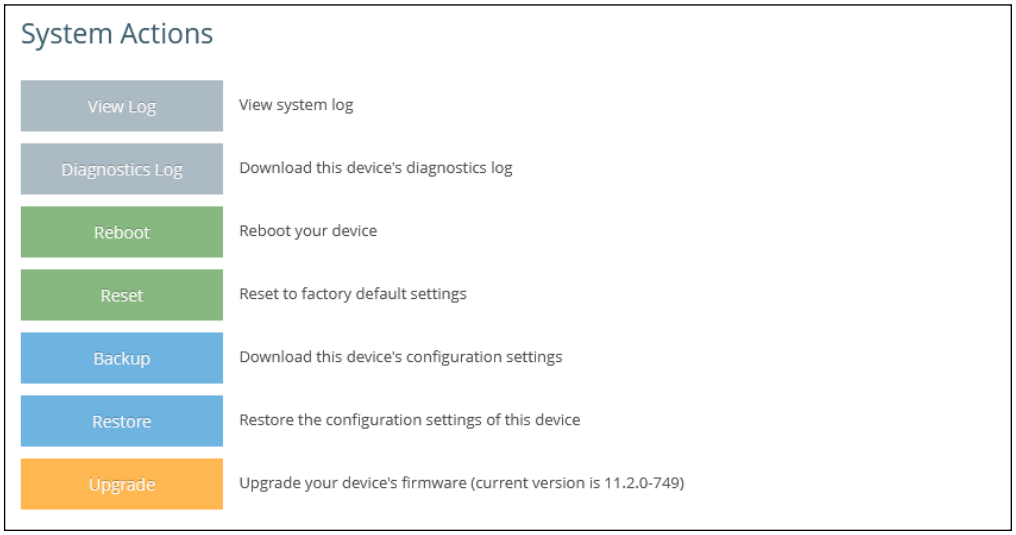
Configurable" setting. See "Wireless Networks — General Settings" on page 69.

- **LED Enable** — Enables the LED indicators on the AP. (Default: Enabled)
- **Language** — Selects the web interface language. (Options: English, Japanese; Default: English)

Maintenance

The Maintenance page supports general maintenance tasks including displaying the system log, downloading a diagnostics log, rebooting the device, restoring factory defaults, backing up or restoring configuration settings, and upgrading firmware.

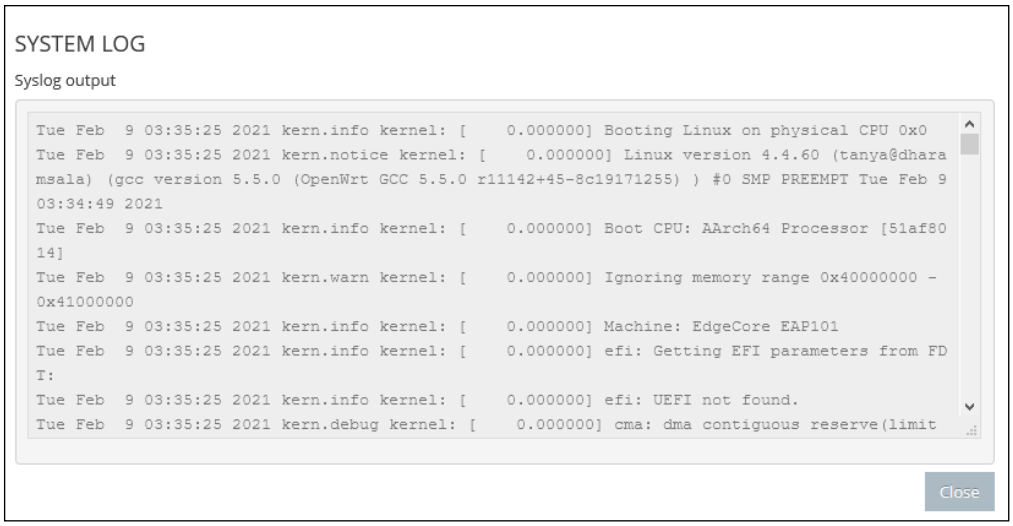
Figure 52: Maintenance



Displaying System Logs

The access point saves event and error messages to a local system log database. The log messages include the date and time, device name, message type, and message details.

Figure 53: System Log



Downloading the Diagnostics Log

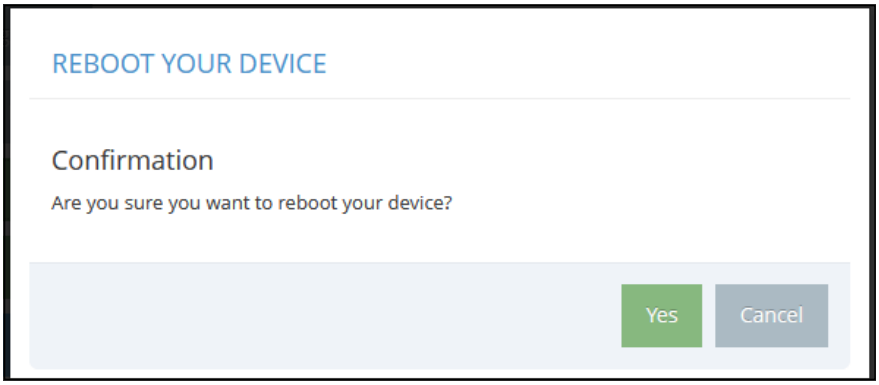
Click “Diagnostics Log” to download the log file to the management workstation. In Windows, a GNU Zip (*.tar.gz) file is stored in the Downloads folder.

The diagnostics log file contains information that can help Edgecore resolve technical issues with the AP.

Rebooting the Access Point

The Reboot page allows you to reboot the access point.

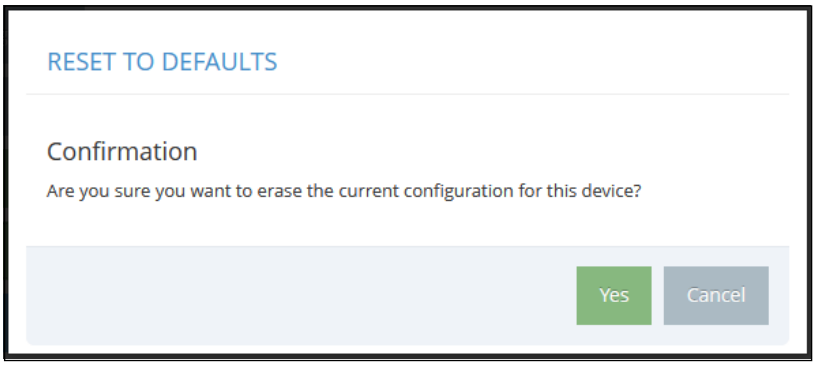
Figure 54: Rebooting the Access Point



Resetting the Access Point

The Reset page allows you to reset the access point to the factory defaults. Note that all user configured information will be lost. You will have to re-enter the default user name and password to re-gain management access to this device.

Figure 55: Resetting to Defaults



Note: It is also possible to reboot or reset the access point by inserting a pin in the pin hole labeled "Reset" on the connector panel of the access point and:

- give a quick press to reboot the access point;
- press and hold for 5 seconds to reset the access point to factory defaults.

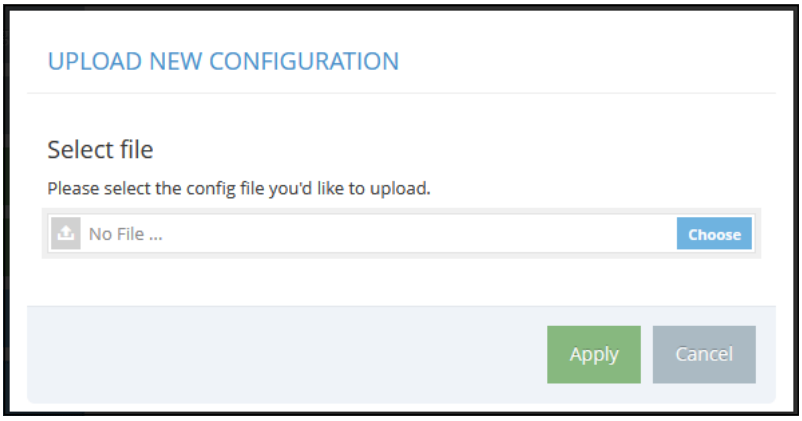
Backing Up Configuration Settings

The Backup function allows you to back up the access point's configuration to a management workstation. In Windows, a GNU Zip (*.tar.gz) file will be stored in the Downloads folder. This is a sample file name: backup-EAP101-2021-02-09.tar.gz

Restoring Configuration Settings

The Restore page allows you to upload configuration settings from a management workstation. The specified file must be one that was previously backed up from the access point.

Figure 56: Restoring Configuration Settings



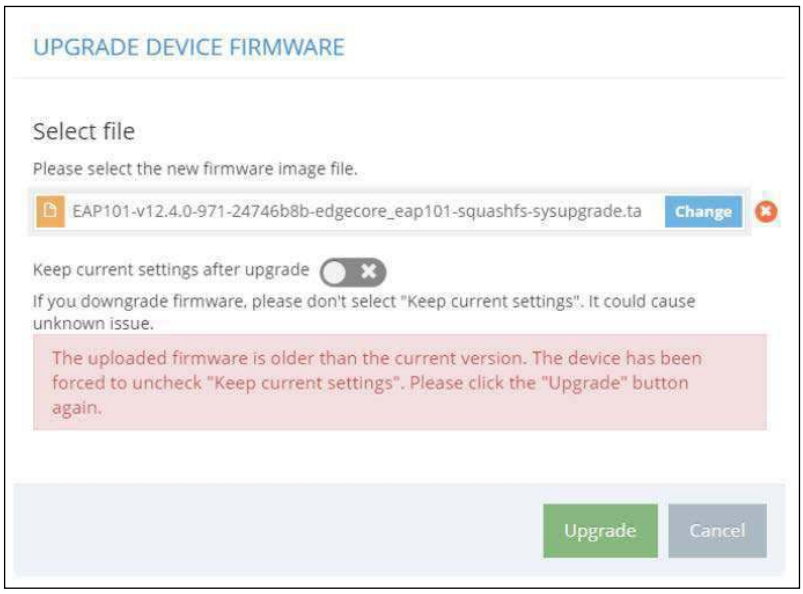
Upgrading Firmware

You can upgrade new access point software from a local file on the management workstation. New software may be provided periodically from Edgecore.

After upgrading new software, you must reboot the access point to implement the new code. Until a reboot occurs, the access point will continue to run the software it was using before the upgrade started. The access point supports dual software images, so if newly loaded software is corrupted, the alternate image will be used on the next reboot. Configuration settings are stored separately from the software, so the current settings will always be used for any new software. However, note that if the current configuration settings are corrupted, the system defaults will be used.

Note: If the uploaded firmware is older than the current version, the device forces the "Keep current settings after upgrade" option to unchecked.

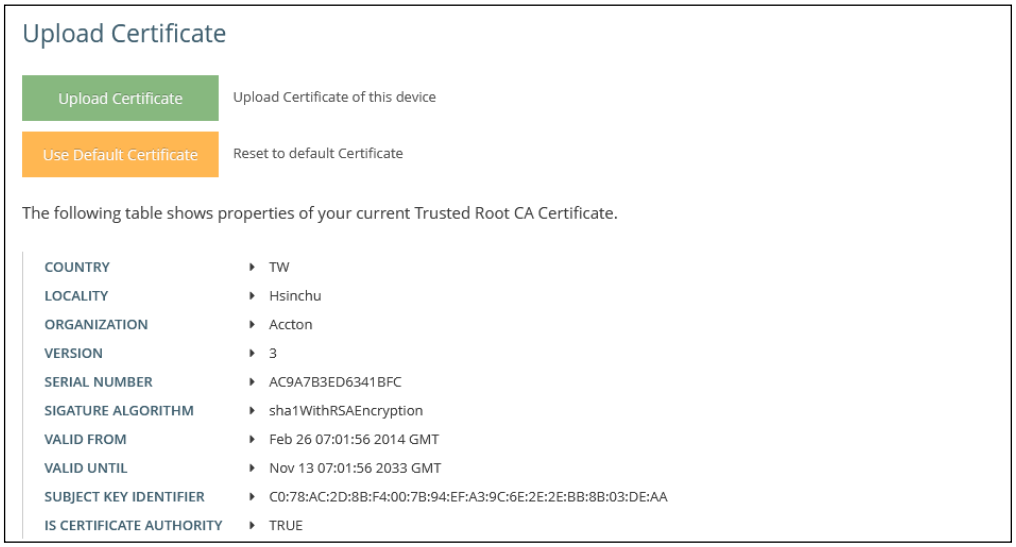
Figure 57: Upgrading Firmware



Upload Certificate

The Upload Certificate page allows you to upload a unique security certificate from a trusted certification authority for secure access (an encrypted connection) to a configured HTTPS captive portal. Alternatively, you can also reset to use the default certificate.

Figure 58: Upload Certificate



The following items are displayed on this page:

- **Upload Certificate** — Click to upload a security certificate and private key from a trusted certification authority.
- **Use Default Certificate** — Click to reset to use the AP's default certificate.

User Accounts

The User Accounts page allows you to control management access to the AP based on manually configured user names and passwords.

Figure 59: User Accounts

The following items are displayed on this page:

- **Enabled** — Click to enable or disable the user account.
- **Username** — The name of the user. (Range: 1-32 ASCII characters. Only accepts A-Z, a-z, 0-9, period ".", underscore "_", and hyphen "-". Usernames cannot begin with a hyphen "-" or period ".".)

- **Password** — The user password. (Range: 6-20 ASCII characters, case sensitive, no special characters)

Services

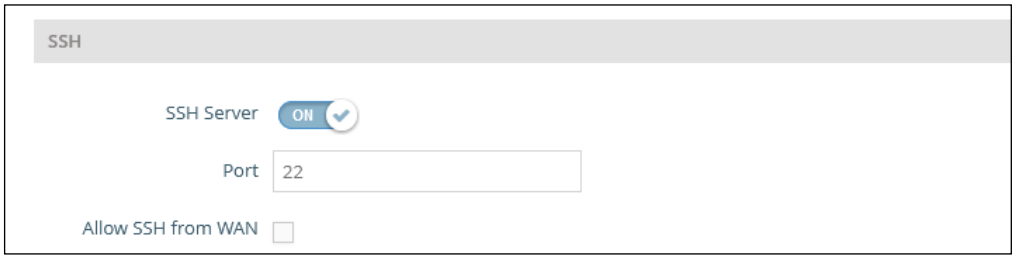
The Services page allows you to control SSH management access to the AP, configure NTP time servers, and configure iBeacon settings.

SSH

The Secure Shell (SSH) can act as a secure replacement for Telnet. The SSH protocol uses generated public keys to encrypt all data transfers passing between the access point and SSH-enabled management station clients and ensures that data traveling over the network arrives unaltered. Clients can then securely use the local user name and password for access authentication.

Note that SSH client software needs to be installed on the management station to access the access point for management via the SSH protocol.

Figure 60: SSH Settings



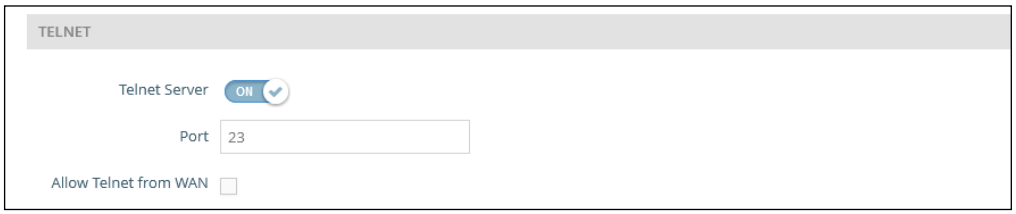
The following items are displayed on this page:

- **SSH Server** — Enables or disables SSH access to the access point. (Default: Enabled)
- **Port** — Sets the TCP port number for the SSH server on the access point. (Range: 1-65535; Default: 22)
- **Allow SSH from WAN** — Allows SSH management access from the WAN.

Telnet

Telnet is a remote management tool that can be used to configure the access point from anywhere in the network. However, note that Telnet is not secure from hostile attacks.

Figure 61: Telnet Server Settings



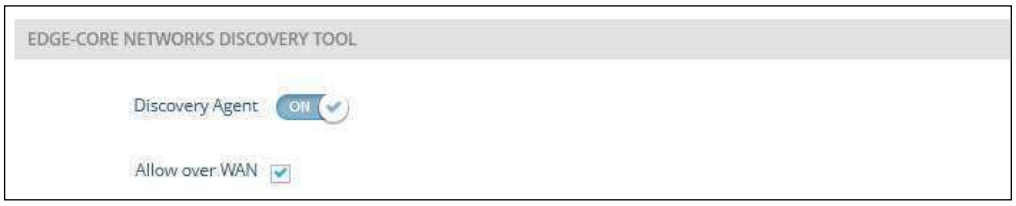
The following items are displayed on this page:

- **Telnet Server** — Enables or disables Telnet access to the access point. (Default: Enabled)
- **Port** — Sets the TCP port number for the Telnet server on the access point. (Range: 1-65535; Default: 23)
- **Allow Telnet from WAN** — Allows Telnet management access from the WAN.

Edgecore Networks Discovery Tool

The Discovery Tool agent enables the AP to find other Edgecore devices in the same Layer 2 network. See "Device Discovery" on page 100 to scan the network for devices.

Figure 62: Discovery Agent Settings



The following items are displayed on this page section:

- **Discovery Agent** — Enables the discovery agent. (Default: Enabled)
- **Allow over WAN** — Enables the discovery agent to operate over the port connected to the Internet source. (Default: Enabled)

Web Server

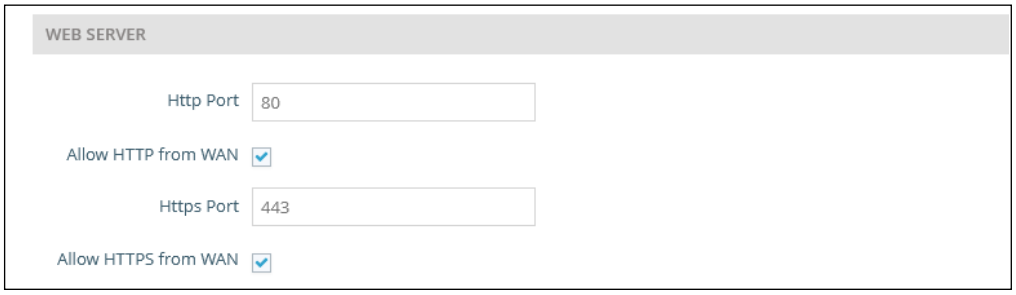
A Web browser provides the primary method of managing the access point. Both HTTP and HTTPS service can be accessed independently. If you enable HTTPS, you must indicate this in the URL: https://device:port_number]

When you start HTTPS, the connection is established in this way:

- The client authenticates the server using the server's digital certificate.

- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
- A padlock icon should appear in the status bar for most browsers.

Figure 63: Web Server Settings



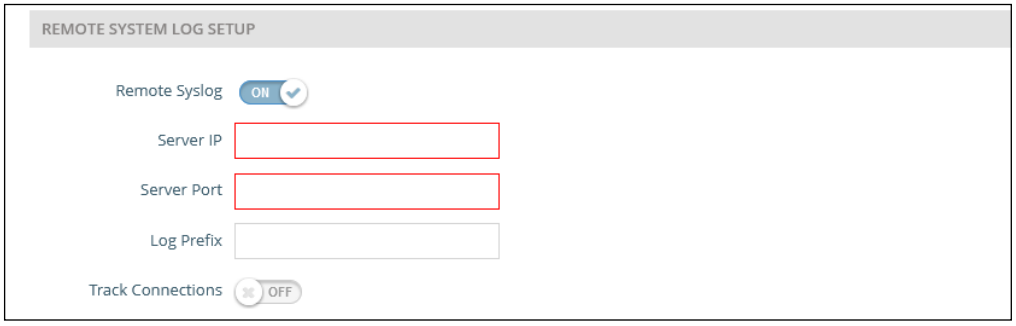
The following items are displayed on this page:

- **HTTP Port** — The TCP port to be used by the HTTP Web browser interface. (Range: 1-65535; Default: 80)
- **Allow HTTP from WAN** — Allows HTTP management access from the WAN.
- **HTTPS Port** — The TCP port to be used by the HTTPS Web browser interface. (Range: 1-65535; Default: 443)
- **Allow HTTPS from WAN** — Allows HTTPS management access from the WAN.

Remote System Log Setup

Use this feature to send log messages to a Syslog server.

Figure 64: Remote System Log Settings



The following items are displayed on this page:

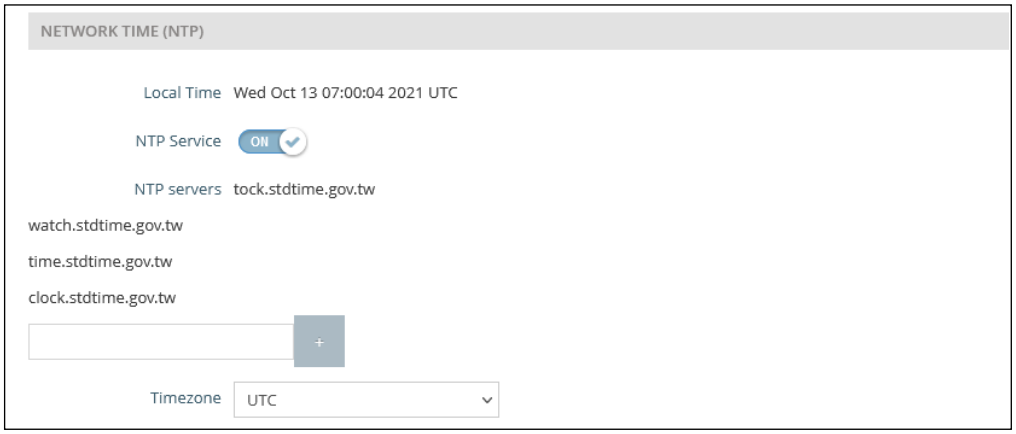
- **Remote Syslog** — Enables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Server IP** — Specifies the IP address of a remote Syslog server that will be sent log messages.
- **Server Port** — Specifies the UDP port number used by the remote Syslog server. (Range: 1-65535)
- **Log Prefix** — Sets a prefix string for log messages sent to the specified server. The prefix can help with sorting messages on the server.
- **Track Connections** — Enables the inclusion of connection information such as source IP and port, destination IP and port in log messages.

Network Time

Network Time Protocol (NTP) allows the access point to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the access point enables the system log to record meaningful dates and times for event entries. If the clock is not set, the access point will only record the time from the factory default set at the last bootup.

The access point acts as an NTP client, periodically sending time synchronization requests to specified time servers. The access point will attempt to poll each server in the configured sequence to receive a time update.

Figure 65: NTP Settings



The following items are displayed on this page:

- **Local Time** — Displays the local time as day of week, month, hour:minute:second, year, based on Universal Time Coordinates.
- **NTP Service** — Enables or disables sending of requests for time updates. (Default: Enabled)

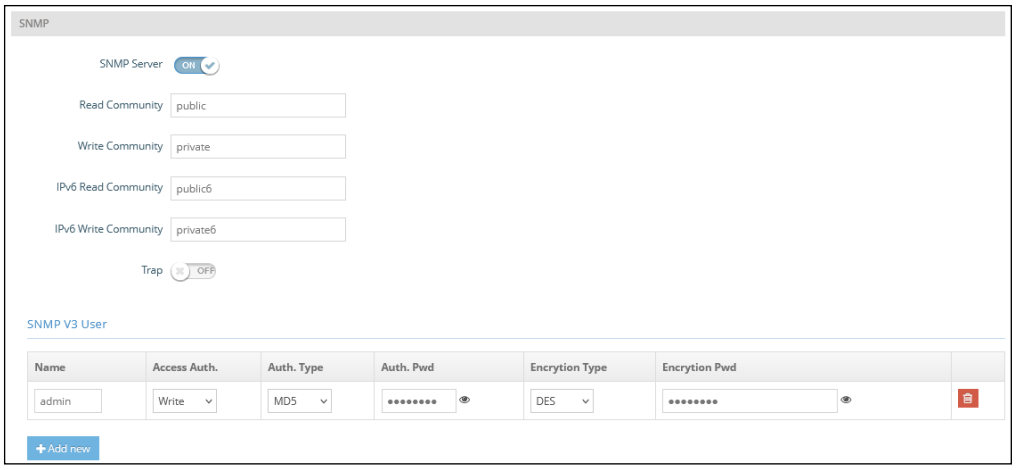
- **NTP Servers** — Sets the host names for time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence. To configure additional servers, click the "+" button to open a new edit field.

- **Timezone** — To display a time corresponding to your local time, choose one of the predefined time zones from the scroll-down list.

SNMP

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. It is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Figure 66: SNMP Settings



The following items are displayed on this page:

- **SNMP Server** — Enables or disables SNMP on the access point. (Default: Enabled)

- **Read Community** — A community string that acts like a password and permits read access to the access point's Management Information Base (MIB). (Range: 1-32 characters, case sensitive; Default: public)

- **Write Community** — A community string that acts like a password and permits write access to the access point's Management Information Base (MIB). (Range: 1-32 characters, case sensitive; Default: private)

- **IPv6 Read Community** — A community string for IPv6 read access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: public6)

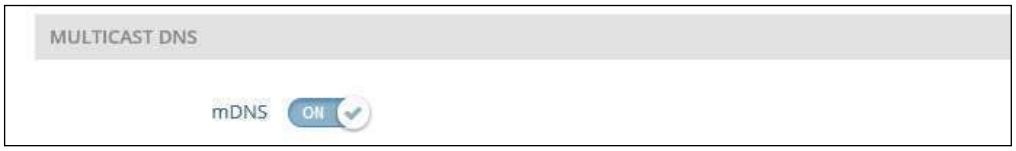
- **IPv6 Write Community** — A community string for IPv6 write access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: private6)

- **Trap** — Enables the sending of SNMP trap messages to a specified server. The access point sends the following trap messages: cold start, warm start, link up, and link down. (Default: Disabled)
  - **Server IP** — Specifies the IP address of the SNMP trap server that will be sent trap messages.
- **SNMPv3 User** — SNMP protocol version 3 provides secure access by account authentication and data encryption. An SNMP v3 user can be defined by clicking the "Add new" button.
  - **Name** — The user name used to access the SNMP service.
  - **Access Auth** — Select the access permission as "Read" or "Write."
  - **Auth Type** — Select the hash algorithm for authentication.
  - **Auth Pwd** — Configure the password for authentication.
  - **Encryption Type** — Select the encryption algorithm for data packets.
  - **Encryption Pwd** — Configure the password for data encryption.

Multicast DNS

The multicast DNS (mDNS) protocol is a zero-configuration service to facilitate connections within a local networks.

Figure 67: Multicast DNS Settings



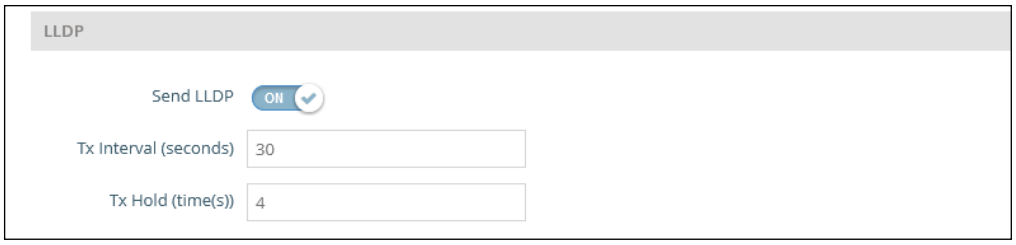
The following items are displayed on this page:

- **mDNS** — Enables or disables Multicast DNS on the access point. (Default: Enabled)

LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices in a network. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device.

Figure 68: LLDP Settings



The following items are displayed on this page:

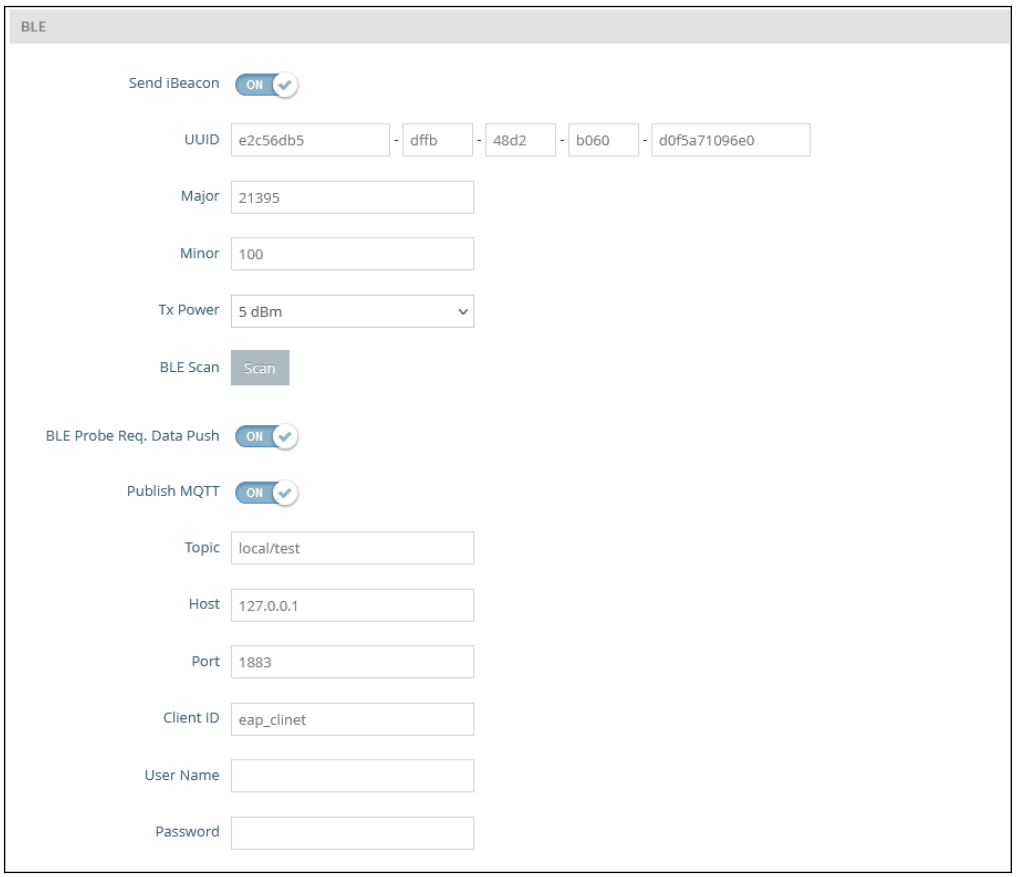
- **Send LLDP** — Enables the sending of LLDP advertisements about the AP to neighboring devices in the network. (Default: Disabled)
- **Tx Interval (seconds)** — Sets the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)
- **Tx Hold (time(s))** — Configures a time-to-live (TTL) value sent in the LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending device if it does not transmit updates in a timely manner.

  The TTL in seconds is based on the following rule:
  minimum value ((Tx Interval * Tx Hold), or 65535)
  Therefore, the default TTL is 4*30 = 120 seconds.

BLE The AP supports the iBeacon standard based on Bluetooth Low Energy (BLE). Devices with BLE Beacons can provide location-based services to BLE clients, such as phones, that can recognize the beacon advertisements, extract the provided information, and then take actions based on the content.

Figure 69: BLE Settings



The following items are displayed on this page:

- **Send iBeacon** — Enables iBeacon support on the AP. (Default: Enabled)
- **UUID** — The iBeacon Universally Unique Identifier that advertises the beacon service. The UUID contains 32 hexadecimal digits in five groups, separated by hyphens.
- **Major** — The iBeacon value that is used to identify a beacon group. (Range: 0-65535)
- **Minor** — The iBeacon value that is used to identify individual beacons within a group. (Range: 0-65535)
- **Tx Power** — Sets the BLE radio transmit power (supported only on EAP101 and EAP104). (Range: 5 dBm to -20 dBm; Default: 5 dBm)

- **BLE Scan** — (EAP101 and EAP104 only) Scans for all BLE devices, including these four types: EddyStone-UID, EddyStone-URL, EddyStone-TLM, and ibeacon.

Figure 70: BLE Scan

- **BLE Probe Req. Data Push** — Enables BLE Probe Request Data Push for the device. (EAP112 only.)
- **Publish MQTT** — Publishes pushed data as MQTT (Message Queuing Telemetry Transport) messages. (EAP112 only.)
  - **Topic** — The MQTT message topic name.
  - **Host** — The IP address of the MQTT server/broker.
  - **Port** — TCP port number.
  - **Client ID** — The identifier for this client device.
  - **User Name** — The client user name.
  - **Password** — The client password.

Diagnostics

The Diagnostics page provides Ping, Traceroute, Nslookup, and Speed Test tools for troubleshooting connectivity problems.

Ping

Enter a hostname or IP address and click to run the ping tool.

Figure 71: Network Utilities - Ping

Traceroute

Enter a hostname or IP address and click to run the traceroute tool.

Figure 72: Network Utilities - Traceroute

Nslookup

Enter a hostname or IP address and click to run the Nslookup tool.

Figure 73: Network Utilities - Nslookup

Speed Test

Enter a hostname or IP address of a Netperf server to test the speed between the AP and server.

Figure 74: Network Utilities - Speed Test

Device Discovery

The Device Discovery Tool provides a method for finding other Edgecore APs within the same Layer 2 network. To function, the Discovery Agent must be enabled (see "Edgecore Networks Discovery Tool" on page 91.

Click the Scan Network button to scan for devices.

Figure 75: Device Discovery Tool

Section III

Appendices

This section provides additional information and includes these items:

A Troubleshooting

Problems Accessing the Management Interface

Table 1: Troubleshooting Chart

Symptom	Action
Cannot connect using a web browser	■ Be sure the AP is powered up. ■ Check network cabling between the management station and the AP. ■ Check that you have a valid network connection to the AP and that intermediate switch ports have not been disabled. ■ Be sure you have configured the AP with a valid IP address, subnet mask and default gateway. ■ Be sure the management station has an IP address in the same subnet as the AP's IP. ■ If you are trying to connect to the AP using a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. ■ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent SSH sessions permitted. Try connecting again at a later time.
Forgot or lost the password	■ Reset the AP to factory defaults using its Reset button.

Using System Logs

If a fault does occur, refer to the *Quick Start Guide* to ensure that the problem you encountered is actually caused by the AP. If the problem appears to be caused by the AP, follow these steps:

1. Repeat the sequence of commands or other actions that lead up to the error.
2. Make a list of the commands or circumstances that led to the fault. Also, make a list of any error messages displayed.
3. Record all relevant system settings.
4. Display the log file through the System > Maintenance page, and copy the information from the log file.
5. Download the Diagnostics Log to a file from the System > Maintenance page.

6. Contact Edgecore and send a detailed description of the problem, along with all of the information mentioned in the above steps.

1,Creation Road 3,
Hsinchu Science Park,
Hsinchu 30077, Taiwan, R.O.C.

Statement of Environmental Directives Compliance

Edgecore's Statement

We hereby declare that, as the date of this declaration, the products listed in this declaration are fully in compliance with following environmental laws, directives and regulations for their intended markets and applications to the best of our knowledge and belief. We acknowledge that this statement may have based on the analysis of the components and materials used in the manufacture of our products and/or supported by suppliers' furnished material declarations and/or the 3rd party test results provided by the suppliers. This is to certify that adequate information provided by the suppliers is available and accurate to the best of our knowledge.

We accept no duty to notify users of updates or changes to this declarations. We shall not be liable for any damages, direct or indirect, consequential or otherwise, suffered by users or third parties as a result of the user's reliance on information in this declaration that has been updates or changed.

Our compliance statements do not extend to, or apply to any product subjected to unintended contamination, misuse, neglect, accident, improper installation, or to use in violation of instructions.

Product Environmental Compliance Status

Attachment	Regulation	Conclusion
1	EU RoHS Directive 2011/65/EU and the amended Directive (EU) 2015/863	Complied
2	EU REACH Regulation (EC) No. 1907/2006	Complied
3	China RoHS in accordance to SJ/T 11363-2014	Complied
4	Taiwan BSMI RoHS in accordance to CNS 15663	Complied
5	EU Directive 2006/122/EC regarding Perfluorooctane Sulfonates (PFOS)	Complied
6	U.S. EPA TSCA (Toxic Substances Control Act) Section 6(h)	Complied

Product Information

Item	Accton P/N	Description	Customer P/N
1	F0PWL4125001A	??SWITCH ECS4125-10T-0724-WL US , 1 O	ECS4125-10T US

1,Creation Road 3,
Hsinchu Science Park,
Hsinchu 30077, Taiwan, R.O.C.

Attachment 1 EU RoHS Directive 2011/65/EU and the amended Directive 2015/863/EU

Product meets EU RoHS requirements with exemption(s):

Banned Substance	Threshold Limit	RoHS Exemption*
Lead (Pb)	1,000 ppm (0.1 weight %)	6(c); 7(a); 7(c)-I
Cadmium (Cd)	100 ppm (0.01 weight %)	
Mercury (Hg)	1,000 ppm (0.1 weight %)	
Hexavalent Chromium (Cr^{6+})	1,000 ppm (0.1 weight %)	
Poly Brominated Biphenyls (PBB)	1,000 ppm (0.1 weight %)	
Poly Brominated Diphenyl Ethers (PBDE)	1,000 ppm (0.1 weight %)	
Bis(2-Ethylhexyl) phthalate (DEHP)	1,000 ppm (0.1 weight %)	
Benzyl butyl phthalate (BBP)	1,000 ppm (0.1 weight %)	
Dibutyl phthalate (DBP)	1,000 ppm (0.1 weight %)	
Diisobutyl phthalate (DIBP)	1,000 ppm (0.1 weight %)	

RoHS maximum limit (ppm) does not apply to applications for which exemptions have been granted by the RoHS Directive.

Applicable within the scope of categories and expiry dates as given in Annex III of Directive 2011/65/EU as listed below:

RoHS exemption	RoHS exemption description
6(c)	Copper alloy containing up to 4 % lead by weight.
7(a)	Lead in high melting temperature type solders (i.e. lead- based alloys containing 85% by weight or more lead).
7(c)-I	Electrical and electronic components containing lead in a glass or ceramic other than dielectric ceramic in capacitors, e.g. piezoelectronic devices, or in a glass or ceramic matrix compound.

1,Creation Road 3,
Hsinchu Science Park,
Hsinchu 30077, Taiwan, R.O.C.

Attachment 2 EU REACH Regulation (EC) No. 1907/2006

This statement reflects Products listed below that are in compliance to Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH). The Candidate List of SVHCs is continually updated at https://echa.europa.eu/candidate-list-table. (substance of very high concern, 242 SVHCs as amended on November 7th, 2024.

This product contains the following REACH Substances of Very High Concern above the limits (0.1% w/w) of component article within REACH:

CAS No.	SVHCs in a concentration above 0.1% weight by weight
1303-86-2	Diboron trioxide
1317-36-8	Lead monoxide (lead oxide)
25550-51-0	Hexahydromethylphthalic anhydride
7439-92-1	Lead
71868-10-5	2-methyl-1-(4-methylthiophenyl)-2-morpholinopropan-1-one
108-78-1	Melamine
115-86-6	Triphenyl phosphate

1,Creation Road 3,
Hsinchu Science Park,
Hsinchu 30077, Taiwan, R.O.C.

Attachment 3 China RoHS in accordance to SJ/T 11363-2014

Table of toxic and hazardous substances/elements and their content:

(As required by China's management methods for controlling pollution by electronic information products)

产品内含危害物质揭露表 Products contain hazardous substances exposing table						
零部件名称 Component Name	危害物质项目 Hazardous Substances Project					
	铅 (Pb)	镉 (Cd)	汞 (Hg)	六价铬 (Cr6+)	多溴联苯 (PBB)	多溴二苯乙醚 (PBDE)
电源供应器 Power Supply	X	○	○	○	○	○
风扇 FAN	X	○	○	○	○	○
散热片Heat Sink	X	○	○	○	○	○
网络连接器 RJ45+X'FMR	X	○	○	○	○	○
二极管 Diode	X	○	○	○	○	○
突波吸收器(静电保护) TVS Array	X	○	○	○	○	○
电阻 Resistor	X	○	○	○	○	○

本表格依据 SJ/T：11364-2014 的规定编制。

○：表示此部件使用的所有同类材料中此种有毒或有害物质的含量均低于 GB/T 26572-2011 规定的限制要求。

○：indicates the toxic or hazardous substance content of the part (at the homogenous material level) is lower than the threshold defined by Requirements for Concentration Limits for Toxic or hazardous Substances in Electronic Information Products(GB/T 26572-2011) issued by Chinese Ministry of Information Industry ("Not Contained" toxic or hazardous substances).

X:表示此部件使用的至少一种同类材料中，此种有毒或有害物质的含量高于 GB/T 26572-2011 规定的限制要求。

X: indicates the toxic or hazardous substance content of the part (at the homogenous material level) is over the threshold defined by standard of GB/T 26572-2011("Contained"toxic or hazardous substances). Suppliers can explain the technical cause of "X" according to actual situation.

1,Creation Road 3,
Hsinchu Science Park,
Hsinchu 30077, Taiwan, R.O.C.

Attachment 4 Taiwan BSMI RoHS in accordance to CNS 15663

The following tables are a declaration of the presence condition of restricted substances:

設備名稱：2.5G L2 網管型交換器 Equipment name				型號（型式）：ECS4125-10T Type designation (Type)		
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 Lead(Pb)	汞 Mercury(Hg)	鎘 Cadmium(Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
電路板組件 PCBA	-	O	O	O	O	O
電源供應器 Power Supply	-	O	O	O	O	O
風扇 FAN	-	O	O	O	O	O
機殼 Chassis	O	O	O	O	O	O
組合線 Cable ass'y	O	O	O	O	O	O

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note 1：“Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note 2：“○” indicates that the percentage content of the restricted substance does not exceed the percentage of referenc value of presence.

備考3. 〝－〞係指該項限用物質為排除項目。

Note 3：The “–” indicates that the restricted substance corresponds to the exemption.

1,Creation Road 3,
Hsinchu Science Park,
Hsinchu 30077, Taiwan, R.O.C.

Attachment 5 EU Directive 2006/122/EC regarding Perfluorooctane Sulfonates (PFOS)

The permissible maximum concentration values of hazardous substances present in electrical and electronic equipment, general requirements are as follows:

Specifications	Threshold Limit
Substance or constituent of preparations	< 0.001 weight % (10ppm)
Semi-finished products & articles & parts	< 0.1 weight % (1000ppm)
Textiles & other coated materials	< 1ug/m2

Attachment 6 Section 6(h) of US Toxic Substances Control Act (TSCA)

We hereby confirmed that the declared products do not contain the Persistent, Bioaccumulative, and Toxic (PBT) Chemicals under TSCA Section 6(h) listed below:

Substance	CAS No.
Decabromodiphenyl ether (DecaBDE)	1163-19-5
Phenol, isopropylated, phosphate (3:1) (PIP (3:1))	68937-41-7
2,4,6-Tris (tert-butyl) phenol (2,4,6-TTBP)	732-26-3
Pentachlorothiophenol (PCTP)	133-49-3
Hexachlorobutadiene (HCBD)	87-68-3

Signature:

Responsible person in charge (printed): Allen Chao
Date: December 05th,2024

De: Igor O. - SMA-CPL

Para: SMA-CPL - Comissão Permanente de Licitação

Data: 28/07/2025 às 11:22:22

Em anexo, documentos apresentados pela empresa na diligência efetuada na plataforma compras.gov.br, bem como documendos de solicitação da diligência por parte do pregoeiro.

–

Igor de Souza Oliveira
Pregoeiro Oficial

Anexos:

COMPROVANTE.pdf
DILIGENCIA.pdf
DILIGENCIA2_ass.pdf
DILIGENCIA_assinado.pdf
NF15.pdf
NF16.pdf
NF17.pdf
NF_27_FEV25_SDWAN.pdf
NF_29_MAR25_SDWAN.pdf
NF_31_ABR25_SDWAN.pdf
NF_33_MAI25_SDWAN.pdf
NF_35_MAI25_SDWAN.pdf
OFICIO_100_DILIGENCIA_PE900152025_PREFEITURA_CACERES_MT.pdf
OFICIO_101_DILIGENCIA_PE900152025_PREFEITURA_CACERES_MT.pdf
sicredi_1751573983751.pdf
sicredi_1751577319213.pdf

Comprovante de transferência

09 MAI 2025 - 13:56:57

Valor	R$ 35.000,00
Tipo de transferência	Pix

Destino

Nome	SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA
Agência	0001
Conta	160626821-5

Origem

Nome	REDE EXS TELECOMUNICACOES LTDA
Agência	0001
Conta	959722940-1

Dados gerais do pagamento

Identificador	LtHhYIxLkO

Nu Pagamentos S.A. - Instituição de Pagamento
CNPJ 18.236.120/0001-58

ID da transação:
E18236120202505091656s10a4f89c0e

Estamos aqui para ajudar se você tiver alguma dúvida.

Me ajuda →

Ouvidoria: 0800 887 0463 |
ouvidoria@nubank.com.br (Atendimento das 8h

Seleção de fornecedores - Habilitação

Online

Pregão Eletrônico N° 90015/2025 (SRP) (Lei 14.133/2021)

UASG 989047 - PREFEITURA MUNICIPAL DE CACERES - MT

Critério julgamento: **Menor Preço / Maior Desconto** Modo disputa: **Aberto**

Disputa | Julgamento | **Habilitação** | Fase Recursal | Adjudicação/ Homologação

GRUPO 1 | 8 itens
Julgado e habilitado (aguardando decisão de recursos)

Valor estimado (total) R$ 3.281.876,4200

44.122.701/0001-79
ME/EPP
Aceita e habilitada

Valor ofertado (total) R$ 2.735.200,0000
Valor negociado (total) **R$ 2.563.643,8900**

SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA
DF

Negociação: **Encerrada**
Envio de anexos: **Encerrado**
Diligência: **Encerrada**

PROPOSTAS DOS ITENS | ANEXOS | CHAT | **DILIGÊNCIAS**

Informo que, de forma equivocada, foi determinada diligência para apresentação de notas fiscais emitidas pela empresa Rede EXS Telecomunicações Ltda., quando o correto seria a solicitação de notas fiscais emitidas pela própria empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA.

Data início: 25/07/2025 16:22:45 Data encerramento: 28/07/2025 10:28:19
Situação: Encerrada

Informamos que será realizada diligência com a empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, com a finalidade de solicitar a apresentação das notas fiscais referentes aos serviços prestados à empresa Rede EXS Telecomunicações Ltda, conforme atestado técnico apresentado no certame

Data início: 24/07/2025 15:27:28 Data encerramento: 25/07/2025 15:16:22
Situação: Encerrada

Voltar | Cadastrar nova diligência

ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CÁCERES
SECRETARIA DE ADMINISTRAÇÃO
COMISSÃO PERMANENTE DE CONTRATAÇÃO

PROCESSO ADMINISTRATIVO Nº	PREGÃO ELETRONICO
29/2025	N.º 15/2025

PROCESSO ADMINISTRATIVO Nº 029/2025
PREGÃO ELETRÔNICO Nº 015/2025

ASSUNTO: Solicitação de Diligência – Apresentação de Notas Fiscais – SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA

Considerando o recurso interposto pela empresa **F.V.B.N. CONSTRUÇÕES E TECNOLOGIA LTDA**, que questiona a validade do atestado técnico apresentado pela empresa **SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA**, emitido pela empresa **Rede EXS Telecomunicações Ltda**, alegando vínculo societário entre as partes;

Considerando o **Parecer Jurídico nº 214/2025-PGM**, que recomenda a realização de diligência para verificar a veracidade e a fidedignidade do referido atestado, especialmente no que tange à comprovação da efetiva prestação dos serviços;

Considerando que, até o momento, a documentação apresentada pela empresa SH7 inclui **comprovantes de pagamento e contrato**, mas **não contempla as respectivas notas fiscais**, documento necessário para que o atestado possa ser validado como prova de capacidade técnico-operacional;

Considerando, ainda, o parecer técnico da unidade demandante (CTI), que informou que, **na ausência da validação do atestado da Rede EXS por meio de notas fiscais**, a empresa SH7 **não alcança o percentual mínimo de 30% do item de maior relevância técnica**, conforme item 9.17.13 do edital;

Com fundamento no **art. 67, §3º, da Lei nº 14.133/2021**, e com o objetivo de garantir o devido processo legal, a transparência e o julgamento objetivo das propostas, esta Comissão **solicita a realização de diligência junto à empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA**, para que apresente:

Notas fiscais emitidas pela empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, que comprovem a efetiva prestação dos serviços descritos no atestado técnico apresentado para fins de habilitação no certame.

O prazo para apresentação será de **24 (vinte e quatro) horas**, contadas do recebimento da notificação, para a apresentação da referida documentação.

Local e data: Prefeitura de Cáceres-MT, 25 de julho de 2025

Igor de Souza Oliveira
Agente de contratação/Pregoeiro
Portaria 251-2025

Igor de Souza Oliveira:04806954152
Assinado de forma digital por Igor de Souza Oliveira:04806954152
Dados: 2025.07.25 14:57:39 -04'00'

ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CÁCERES
SECRETARIA DE ADMINISTRAÇÃO
COMISSÃO PERMANENTE DE CONTRATAÇÃO

PROCESSO ADMINISTRATIVO Nº	PREGÃO ELETRONICO
29/2025	N.º 15/2025

PROCESSO ADMINISTRATIVO Nº 029/2025
PREGÃO ELETRÔNICO Nº 015/2025

ASSUNTO: Solicitação de Diligência – Apresentação de Notas Fiscais – SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA

Considerando o recurso interposto pela empresa **F.V.B.N. CONSTRUÇÕES E TECNOLOGIA LTDA**, que questiona a validade do atestado técnico apresentado pela empresa **SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA**, emitido pela empresa **Rede EXS Telecomunicações Ltda**, alegando vínculo societário entre as partes;

Considerando o **Parecer Jurídico nº 214/2025-PGM**, que recomenda a realização de diligência para verificar a veracidade e a fidedignidade do referido atestado, especialmente no que tange à comprovação da efetiva prestação dos serviços;

Considerando que, até o momento, a documentação apresentada pela empresa SH7 inclui **comprovantes de pagamento e contrato**, mas **não contempla as respectivas notas fiscais**, documento necessário para que o atestado possa ser validado como prova de capacidade técnico-operacional;

Considerando, ainda, o parecer técnico da unidade demandante (CTI), que informou que, **na ausência da validação do atestado da Rede EXS por meio de notas fiscais**, a empresa SH7 **não alcança o percentual mínimo de 30% do item de maior relevância técnica**, conforme item 9.17.13 do edital;

Com fundamento no **art. 67, §3º, da Lei nº 14.133/2021**, e com o objetivo de garantir o devido processo legal, a transparência e o julgamento objetivo das propostas, esta Comissão **solicita a realização de diligência junto à empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA**, para que apresente:

Notas fiscais emitidas pela empresa Rede EXS Telecomunicações Ltda, que comprovem a efetiva prestação dos serviços descritos no atestado técnico apresentado para fins de habilitação no certame.

O prazo para apresentação será de **24 (vinte e quatro) horas**, contadas do recebimento da notificação, para a apresentação da referida documentação.

Local e data: Prefeitura de Cáceres-MT, 24 de julho de 2025

Igor de Souza Oliveira
Agente de contratação/Pregoeiro
Portaria 251-2025

Igor de Souza Oliveira:04806954152
Assinado de forma digital por Igor de Souza Oliveira:04806954152
Dados: 2025.07.24 14:41:29 -04'00'

Governo do Distrito Federal
Secretaria de Estado de Economia do Distrito Federal
Fone: () - 156 - Opção 3 - www.sefaz.df.gov.br

Nota Fiscal Eletrônica

Série do Documento: Nota Fiscal de Serviço Eletrônica - NFS-e
Número da Nota Fiscal: 15

Dados do Prestador de Serviço

SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA
GONZALEZ CONSULTORIA
SRTVS QD 701 BLOCO O SALA 122 NOVO CENTRO MULTIEMP, - ASA SUL
CEP 70340-000 - Fone: (61)3242-5631 - Brasília/ DF
clientes@consulthec.com.br
Inscrição Municipal 0809456400111 - CPF/CNPJ 44.122.701/0001-79

Data de Geração da NFS-e: **24/07/2025 16:53:48**
Data de Competência: **30/06/2025**
Cód. de Autenticidade: **2381987EC**
Responsável pela Retenção:

Identificação da Nota Fiscal Eletrônica

Natureza da Operação	Número do RPS	Série do RPS	Data de Emissão do RPS
Exigível			

Local dos Serviços	Município Incidência
Brasília - Distrito Federal	Brasília - Distrito Federal

Dados do Tomador de Serviços

CNPJ/CPF :	23.935.457/0001-93	**IM :**	0795667300199
Razão Social :	REDE EXS TELECOMUNICACOES LTDA		
Endereço :	SIG QUADRA 1 LOTE 324 -SALA 324 ED PLATINUM OFFICE S/N	**Número :**	
Complemento :		**Bairro :**	ZONA INDUSTRIAL
CEP :	70610-410	**Cidade/UF :**	Brasília/ DF
Telefone :	(61)3242-5631	**E-mail :**	clientes@consulthec.com.br

Dados do Intermediário de Serviços

CNPJ/CPF	Inscrição Municipal	Razão Social

Descrição dos Serviços

Suporte 24x7, SIEM, NOC, SOC, SDWAN, NGFW

Detalhamento dos Tributos

Atividade do Município				Alíquota	Item da LC116/2003	Cód. NBS	Cód. CNAE
103 - (2%) 1.03 - Serviços de projeto, planejamento, implanta…				**2,00**	103		6209100
Vl. Total dos Serviços	Desconto Incondicionado	Deduções Base Cálculo	Base de Cálculo		Total do ISSQN	ISSQN Retido	Desconto Condicionado
R$ 7.460,00	R$ 0,00	R$ 0,00	R$ 7.460,00		R$ 149,20	Não	R$ 0,00
PIS	COFINS	INSS	IRRF	CSLL	Outras Retenções	Vl. ISSQN Retido	**Vl. Líquido da Nota Fiscal**
R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ **7.460,00**

Construção Civil	**Cód. Obra :**	**Art. :**

Informações Adicionais

Ref.: Jun25

PROCON: TEL 151- SETOR COMERCIAL SUL, QUADRA 8, BLOCO B-60, SALA 240- BRASILIA - DF

Chave de acesso no Ambiente de Dados Nacional: 53001081244122701000179000000000001525071753376020.

Consulte a autenticidade deste documento acessando o site: https://iss.fazenda.df.gov.br/online/Login/Login.aspx
ISS.NET - Sistema Nota Control® • www.notacontrol.com.br

Governo do Distrito Federal
Secretaria de Estado de Economia do Distrito Federal
Fone: () - 156 - Opção 3 - www.sefaz.df.gov.br

Nota Fiscal Eletrônica

Série do Documento: Nota Fiscal de Serviço Eletrônica - NFS-e
Número da Nota Fiscal: 16

Dados do Prestador de Serviço

SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA
GONZALEZ CONSULTORIA
SRTVS QD 701 BLOCO O SALA 122 NOVO CENTRO MULTIEMP, - ASA SUL
CEP 70340-000 - Fone: (61)3242-5631 - Brasília/ DF
clientes@consulthec.com.br
Inscrição Municipal 0809456400111 - CPF/CNPJ 44.122.701/0001-79

Data de Geração da NFS-e: **24/07/2025 18:57:22**
Data de Competência: **24/07/2025**
Cód. de Autenticidade: **F77ED924F**
Responsável pela Retenção:

Identificação da Nota Fiscal Eletrônica

Natureza da Operação	Número do RPS	Série do RPS	Data de Emissão do RPS
Exigível			

Local dos Serviços	Município Incidência
Brasília - Distrito Federal	Brasília - Distrito Federal

Dados do Tomador de Serviços

CNPJ/CPF :	23.935.457/0001-93	**IM :**	0795667300199
Razão Social :	REDE EXS TELECOMUNICACOES LTDA		
Endereço :	SIG QUADRA 1 LOTE 324 -SALA 324 ED PLATINUM OFFICE S/N	**Número :**	
Complemento :		**Bairro :**	ZONA INDUSTRIAL
CEP :	70610-410	**Cidade/UF :**	Brasília/ DF
Telefone :	(61)3242-5631	**E-mail :**	clientes@consulthec.com.br

Dados do Intermediário de Serviços

CNPJ/CPF	Inscrição Municipal	Razão Social

Descrição dos Serviços

Serviços Gerenciados de segurança com licenciamento de FortiAnalyzer 50 Gigas de Log/Dia com módulo Indicador de Compromissos (IoC), atualização de Firmware e Assinaturas para o Cliente TRT23-Cuiabá

Detalhamento dos Tributos

Atividade do Município	Alíquota	Item da LC116/2003	Cód. NBS	Cód. CNAE
103 - (2%) 1.03 - Serviços de projeto, planejamento, implanta…	**2,00**	103		6209100

Vl. Total dos Serviços	Desconto Incondicionado	Deduções Base Cálculo	Base de Cálculo	Total do ISSQN	ISSQN Retido	Desconto Condicionado
R$ 35.000,00	R$ 0,00	R$ 0,00	R$ 35.000,00	R$ 700,00	Não	R$ 0,00

PIS	COFINS	INSS	IRRF	CSLL	Outras Retenções	Vl. ISSQN Retido	**Vl. Líquido da Nota Fiscal**
R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ **35.000,00**

Construção Civil	**Cód. Obra :**	**Art. :**

Informações Adicionais

Ref.: Fev25 - Licenciamento TRT23 - MT

PROCON: TEL 151- SETOR COMERCIAL SUL, QUADRA 8, BLOCO B-60, SALA 240- BRASILIA - DF

Chave de acesso no Ambiente de Dados Nacional: 53001081244122701000179000000000001625071753383446.

Consulte a autenticidade deste documento acessando o site: https://iss.fazenda.df.gov.br/online/Login/Login.aspx
ISS.NET - Sistema Nota Control® • www.notacontrol.com.br

Governo do Distrito Federal
Secretaria de Estado de Economia do Distrito Federal
Fone: () - 156 - Opção 3 - www.sefaz.df.gov.br

Nota Fiscal Eletrônica

Série do Documento: Nota Fiscal de Serviço Eletrônica - NFS-e
Número da Nota Fiscal: 17

Dados do Prestador de Serviço

SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA
GONZALEZ CONSULTORIA
SRTVS QD 701 BLOCO O SALA 122 NOVO CENTRO MULTIEMP, - ASA SUL
CEP 70340-000 - Fone: (61)3242-5631 - Brasília/ DF
clientes@consulthec.com.br
Inscrição Municipal 0809456400111 - CPF/CNPJ 44.122.701/0001-79

Data de Geração da NFS-e: **24/07/2025 19:04:10**
Data de Competência: **24/07/2025**
Cód. de Autenticidade: **5FA271785**
Responsável pela Retenção:

Identificação da Nota Fiscal Eletrônica

Natureza da Operação	Número do RPS	Série do RPS	Data de Emissão do RPS
Exigível			

Local dos Serviços	Município Incidência
Brasília - Distrito Federal	Brasília - Distrito Federal

Dados do Tomador de Serviços

CNPJ/CPF :	23.935.457/0001-93	**IM :**	0795667300199
Razão Social :	REDE EXS TELECOMUNICACOES LTDA		
Endereço :	SIG QUADRA 1 LOTE 324 -SALA 324 ED PLATINUM OFFICE S/N	**Número :**	
Complemento :		**Bairro :**	ZONA INDUSTRIAL
CEP :	70610-410	**Cidade/UF :**	Brasília/ DF
Telefone :	(61)3242-5631	**E-mail :**	clientes@consulthec.com.br

Dados do Intermediário de Serviços

CNPJ/CPF	Inscrição Municipal	Razão Social

Descrição dos Serviços

Suporte 24x7, SIEM, NOC, SOC, SDWAN, NGFW (Atualização de Firmware - F40)

Detalhamento dos Tributos

Atividade do Município	Alíquota	Item da LC116/2003	Cód. NBS	Cód. CNAE
103 - (2%) 1.03 - Serviços de projeto, planejamento, implanta…	**2,00**	103		6209100

Vl. Total dos Serviços	Desconto Incondicionado	Deduções Base Cálculo	Base de Cálculo	Total do ISSQN	ISSQN Retido	Desconto Condicionado
R$ 20.000,00	R$ 0,00	R$ 0,00	R$ 20.000,00	R$ 400,00	Não	R$ 0,00

PIS	COFINS	INSS	IRRF	CSLL	Outras Retenções	Vl. ISSQN Retido	Vl. Líquido da Nota Fiscal
R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ **20.000,00**

Construção Civil	Cód. Obra :	Art. :

Informações Adicionais

Ref.: Jan25 (pro rata); mar25; abr25

PROCON: TEL 151- SETOR COMERCIAL SUL, QUADRA 8, BLOCO B-60, SALA 240- BRASILIA - DF

Chave de acesso no Ambiente de Dados Nacional: 53001081244122701000179000000000001725071753383857.

Consulte a autenticidade deste documento acessando o site: https://iss.fazenda.df.gov.br/online/Login/Login.aspx
ISS.NET - Sistema Nota Control® • www.notacontrol.com.br

Governo do Distrito Federal
Secretaria de Estado de Economia do Distrito Federal
Fone: () - 156 - Opção 3 - www.sefaz.df.gov.br

Nota Fiscal Eletrônica

Série do Documento: Nota Fiscal de Serviço Eletrônica - NFS-e
Número da Nota Fiscal: 27

Dados do Prestador de Serviço

REDE EXS TELECOMUNICACOES LTDA
EXS
SIG QUADRA 1 LOTE 324 -SALA 324 ED PLATINUM OFFICE S/N , - ZONA INDUSTRIAL
CEP 70610-410 - Fone: (61)3242-5631 - Brasília/ DF
clientes@consulthec.com.br
Inscrição Municipal 0795667300199 - CPF/CNPJ 23.935.457/0001-93

Data de Geração da NFS-e: **06/02/2025 11:20:30**
Data de Competência: **06/02/2025**
Cód. de Autenticidade: **67FE961AA**
Responsável pela Retenção:

Identificação da Nota Fiscal Eletrônica

Natureza da Operação	Número do RPS	Série do RPS	Data de Emissão do RPS
Exigível			

Local dos Serviços	Município Incidência
Brasília - Distrito Federal	Brasília - Distrito Federal

Dados do Tomador de Serviços

CNPJ/CPF : 37.115.425/0001-56
IM :
Razão Social : TRIBUNAL REGIONAL DO TRABALHO DA 23 REGIAO
Endereço : Avenida Historiador Rubens de Mendonça, 3355 (Tribunal Regional do Trabalho 23ª Região)
Número : 3355
Complemento :
Bairro : Centro Político Administrativo
CEP : 78049-935
Cidade/UF : Cuiabá/ MT
Telefone :
E-mail :

Dados do Intermediário de Serviços

CNPJ/CPF	Inscrição Municipal	Razão Social

Descrição dos Serviços

Solução SDWAN alta disponibilidade capital e sites remotos (item 1.4 CT 033/2022)

Detalhamento dos Tributos

Atividade do Município	Alíquota	Item da LC116/2003	Cód. NBS	Cód. CNAE
1011 - (5%) 1.01 - Análise e desenvolvimento de sistemas. -		101		6190699

Vl. Total dos Serviços	Desconto Incondicionado	Deduções Base Cálculo	Base de Cálculo	Total do ISSQN	ISSQN Retido	Desconto Condicionado
R$ 31.532,51	R$ 0,00	R$ 0,00	R$ 31.532,51	R$ 0,00	Não	R$ 0,00

PIS	COFINS	INSS	IRRF	CSLL	Outras Retenções	Vl. ISSQN Retido	Vl. Líquido da Nota Fiscal
R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ **31.532,51**

Construção Civil | **Cód. Obra :** | **Art. :**

Informações Adicionais

I - "DOCUMENTO EMITIDO POR ME OU EPP OPTANTE PELO SIMPLES NACIONAL"; e II - "NÃO GERA DIREITO A CRÉDITO FIS CAL DE IPI."
PROCON: TEL 151- SETOR COMERCIAL SUL, QUADRA 8, BLOCO B-60, SALA 240- BRASILIA - DF

Consulte a autenticidade deste documento acessando o site: https://iss.fazenda.df.gov.br/online/Login/Login.aspx
ISS.NET - Sistema Nota Control® • www.notacontrol.com.br

Governo do Distrito Federal
Secretaria de Estado de Economia do Distrito Federal
Fone: () - 156 - Opção 3 - www.sefaz.df.gov.br

Nota Fiscal Eletrônica

Série do Documento: Nota Fiscal de Serviço Eletrônica - NFS-e
Número da Nota Fiscal: 29

Dados do Prestador de Serviço

REDE EXS TELECOMUNICACOES LTDA
EXS
SIG QUADRA 1 LOTE 324 -SALA 324 ED PLATINUM OFFICE S/N , - ZONA INDUSTRIAL
CEP 70610-410 - Fone: (61)3242-5631 - Brasília/ DF
clientes@consulthec.com.br
Inscrição Municipal 0795667300199 - CPF/CNPJ 23.935.457/0001-93

Data de Geração da NFS-e: **11/03/2025 21:01:32**
Data de Competência: **11/03/2025**
Cód. de Autenticidade: **6DBA666FB**
Responsável pela Retenção:

Identificação da Nota Fiscal Eletrônica

Natureza da Operação	Número do RPS	Série do RPS	Data de Emissão do RPS
Exigível			

Local dos Serviços	Município Incidência
Brasília - Distrito Federal	Brasília - Distrito Federal

Dados do Tomador de Serviços

CNPJ/CPF : 37.115.425/0001-56
IM :
Razão Social : TRIBUNAL REGIONAL DO TRABALHO DA 23 REGIAO
Endereço : Avenida Historiador Rubens de Mendonça, 3355 (Tribunal Regional do Trabalho 23ª Região)
Número : 3355
Complemento :
Bairro : Centro Político Administrativo
CEP : 78049-935
Cidade/UF : Cuiabá/ MT
Telefone :
E-mail :

Dados do Intermediário de Serviços

CNPJ/CPF	Inscrição Municipal	Razão Social

Descrição dos Serviços

Solução SDWAN alta disponibilidade capital e sites remotos (item 1.4 CT 033/2022)

Detalhamento dos Tributos

Atividade do Município	Alíquota	Item da LC116/2003	Cód. NBS	Cód. CNAE
1011 - (5%) 1.01 - Análise e desenvolvimento de sistemas. -		101		6190699

Vl. Total dos Serviços	Desconto Incondicionado	Deduções Base Cálculo	Base de Cálculo	Total do ISSQN	ISSQN Retido	Desconto Condicionado
R$ 31.532,51	R$ 0,00	R$ 0,00	R$ 31.532,51	R$ 0,00	Não	R$ 0,00

PIS	COFINS	INSS	IRRF	CSLL	Outras Retenções	Vl. ISSQN Retido	Vl. Líquido da Nota Fiscal
R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ **31.532,51**

Construção Civil	Cód. Obra :	Art. :

Informações Adicionais

I - "DOCUMENTO EMITIDO POR ME OU EPP OPTANTE PELO SIMPLES NACIONAL"; e II - "NÃO GERA DIREITO A CRÉDITO FISCAL DE IPI."
PROCON: TEL 151- SETOR COMERCIAL SUL, QUADRA 8, BLOCO B-60, SALA 240- BRASILIA - DF

Consulte a autenticidade deste documento acessando o site: https://iss.fazenda.df.gov.br/online/Login/Login.aspx
ISS.NET - Sistema Nota Control® • www.notacontrol.com.br

Governo do Distrito Federal
Secretaria de Estado de Economia do Distrito Federal
Fone: () - 156 - Opção 3 - www.sefaz.df.gov.br

Nota Fiscal Eletrônica

Série do Documento: Nota Fiscal de Serviço Eletrônica - NFS-e
Número da Nota Fiscal: 31

Dados do Prestador de Serviço

REDE EXS TELECOMUNICACOES LTDA
EXS
SIG QUADRA 1 LOTE 324 -SALA 324 ED PLATINUM OFFICE S/N , - ZONA INDUSTRIAL
CEP 70610-410 - Fone: (61)3242-5631 - Brasília/ DF
clientes@consulthec.com.br
Inscrição Municipal 0795667300199 - CPF/CNPJ 23.935.457/0001-93

Data de Geração da NFS-e: **07/04/2025 23:02:59**
Data de Competência: **07/04/2025**
Cód. de Autenticidade: **E0B70AB27**
Responsável pela Retenção:

Identificação da Nota Fiscal Eletrônica

Natureza da Operação	Número do RPS	Série do RPS	Data de Emissão do RPS
Exigível			

Local dos Serviços	Município Incidência
Brasília - Distrito Federal	Brasília - Distrito Federal

Dados do Tomador de Serviços

CNPJ/CPF : 37.115.425/0001-56
IM :
Razão Social : TRIBUNAL REGIONAL DO TRABALHO DA 23 REGIAO
Endereço : Avenida Historiador Rubens de Mendonça, 3355 (Tribunal Regional do Trabalho 23ª Região)
Número : 3355
Complemento :
Bairro : Centro Político Administrativo
CEP : 78049-935
Cidade/UF : Cuiabá/ MT
Telefone :
E-mail :

Dados do Intermediário de Serviços

CNPJ/CPF	Inscrição Municipal	Razão Social

Descrição dos Serviços

Solução SDWAN alta disponibilidade capital e sites remotos (item 1.4 CT 033/2022)

Detalhamento dos Tributos

Atividade do Município	Alíquota	Item da LC116/2003	Cód. NBS	Cód. CNAE
1011 - (5%) 1.01 - Análise e desenvolvimento de sistemas. -		101		6190699

Vl. Total dos Serviços	Desconto Incondicionado	Deduções Base Cálculo	Base de Cálculo	Total do ISSQN	ISSQN Retido	Desconto Condicionado
R$ 31.532,51	R$ 0,00	R$ 0,00	R$ 31.532,51	R$ 0,00	Não	R$ 0,00

PIS	COFINS	INSS	IRRF	CSLL	Outras Retenções	Vl. ISSQN Retido	Vl. Líquido da Nota Fiscal
R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ **31.532,51**

Construção Civil	Cód. Obra :	Art. :

Informações Adicionais

I - "DOCUMENTO EMITIDO POR ME OU EPP OPTANTE PELO SIMPLES NACIONAL"; e II - "NÃO GERA DIREITO A CRÉDITO FISCAL DE IPI."
PROCON: TEL 151- SETOR COMERCIAL SUL, QUADRA 8, BLOCO B-60, SALA 240- BRASILIA - DF

Consulte a autenticidade deste documento acessando o site: https://iss.fazenda.df.gov.br/online/Login/Login.aspx
ISS.NET - Sistema Nota Control® • www.notacontrol.com.br

Governo do Distrito Federal
Secretaria de Estado de Economia do Distrito Federal
Fone: () - 156 - Opção 3 - www.sefaz.df.gov.br

Nota Fiscal Eletrônica

Série do Documento: Nota Fiscal de Serviço Eletrônica - NFS-e
Número da Nota Fiscal: 33

Dados do Prestador de Serviço

REDE EXS TELECOMUNICACOES LTDA
EXS
SIG QUADRA 1 LOTE 324 -SALA 324 ED PLATINUM OFFICE S/N , - ZONA INDUSTRIAL
CEP 70610-410 - Fone: (61)3242-5631 - Brasília/ DF
clientes@consulthec.com.br
Inscrição Municipal 0795667300199 - CPF/CNPJ 23.935.457/0001-93

Data de Geração da NFS-e: **12/05/2025 21:13:19**
Data de Competência: **12/05/2025**
Cód. de Autenticidade: **6A35823CE**
Responsável pela Retenção:

Identificação da Nota Fiscal Eletrônica

Natureza da Operação	Número do RPS	Série do RPS	Data de Emissão do RPS
Exigível			

Local dos Serviços	Município Incidência
Brasília - Distrito Federal	Brasília - Distrito Federal

Dados do Tomador de Serviços

CNPJ/CPF :	37.115.425/0001-56	**IM :**	
Razão Social :	TRIBUNAL REGIONAL DO TRABALHO DA 23 REGIAO		
Endereço :	Avenida Historiador Rubens de Mendonça, 3355 (Tribunal Regional do Trabalho 23ª Região)	**Número :**	3355
Complemento :		**Bairro :**	Centro Político Administrativo
CEP :	78049-935	**Cidade/UF :**	Cuiabá/ MT
Telefone :		**E-mail :**	

Dados do Intermediário de Serviços

CNPJ/CPF	Inscrição Municipal	Razão Social

Descrição dos Serviços

Solução SDWAN alta disponibilidade capital e sites remotos (item 1.4 CT 033/2022)

Detalhamento dos Tributos

Atividade do Município	Alíquota	Item da LC116/2003	Cód. NBS	Cód. CNAE
1011 - (5%) 1.01 - Análise e desenvolvimento de sistemas. -		101		6190699

Vl. Total dos Serviços	Desconto Incondicionado	Deduções Base Cálculo	Base de Cálculo	Total do ISSQN	ISSQN Retido	Desconto Condicionado
R$ 31.532,51	R$ 0,00	R$ 0,00	R$ 31.532,51	R$ 0,00	Não	R$ 0,00

PIS	COFINS	INSS	IRRF	CSLL	Outras Retenções	Vl. ISSQN Retido	Vl. Líquido da Nota Fiscal
R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ **31.532,51**

Construção Civil	Cód. Obra :	Art. :

Informações Adicionais

I - "DOCUMENTO EMITIDO POR ME OU EPP OPTANTE PELO SIMPLES NACIONAL"; e II - "NÃO GERA DIREITO A CRÉDITO FISCAL DE IPI."
PROCON: TEL 151- SETOR COMERCIAL SUL, QUADRA 8, BLOCO B-60, SALA 240- BRASILIA - DF

Consulte a autenticidade deste documento acessando o site: https://iss.fazenda.df.gov.br/online/Login/Login.aspx
ISS.NET - Sistema Nota Control® • www.notacontrol.com.br

Governo do Distrito Federal
Secretaria de Estado de Economia do Distrito Federal
Fone: () - 156 - Opção 3 - www.sefaz.df.gov.br

Nota Fiscal Eletrônica

Série do Documento: Nota Fiscal de Serviço Eletrônica - NFS-e
Número da Nota Fiscal: 35

Dados do Prestador de Serviço

REDE EXS TELECOMUNICACOES LTDA
EXS
SIG QUADRA 1 LOTE 324 -SALA 324 ED PLATINUM OFFICE S/N , - ZONA INDUSTRIAL
CEP 70610-410 - Fone: (61)3242-5631 - Brasília/ DF
clientes@consulthec.com.br
Inscrição Municipal 0795667300199 - CPF/CNPJ 23.935.457/0001-93

Data de Geração da NFS-e: **15/06/2025 14:33:30**
Data de Competência: **15/06/2025**
Cód. de Autenticidade: **390FAF18D**
Responsável pela Retenção:

Identificação da Nota Fiscal Eletrônica

Natureza da Operação	Número do RPS	Série do RPS	Data de Emissão do RPS
Exigível			

Local dos Serviços	Município Incidência
Brasília - Distrito Federal	Brasília - Distrito Federal

Dados do Tomador de Serviços

CNPJ/CPF : 37.115.425/0001-56
IM :
Razão Social : TRIBUNAL REGIONAL DO TRABALHO DA 23 REGIAO
Endereço : Avenida Historiador Rubens de Mendonça, 3355 (Tribunal Regional do Trabalho 23ª Região)
Número : 3355
Complemento :
Bairro : Centro Político Administrativo
CEP : 78049-935
Cidade/UF : Cuiabá/ MT
Telefone :
E-mail :

Dados do Intermediário de Serviços

CNPJ/CPF	Inscrição Municipal	Razão Social

Descrição dos Serviços

Solução SDWAN alta disponibilidade capital e sites remotos (item 1.4 CT 033/2022)

Detalhamento dos Tributos

Atividade do Município	Alíquota	Item da LC116/2003	Cód. NBS	Cód. CNAE
1011 - (5%) 1.01 - Análise e desenvolvimento de sistemas. -		101		6190699

Vl. Total dos Serviços	Desconto Incondicionado	Deduções Base Cálculo	Base de Cálculo	Total do ISSQN	ISSQN Retido	Desconto Condicionado
R$ 31.532,51	R$ 0,00	R$ 0,00	R$ 31.532,51	R$ 0,00	Não	R$ 0,00

PIS	COFINS	INSS	IRRF	CSLL	Outras Retenções	Vl. ISSQN Retido	Vl. Líquido da Nota Fiscal
R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ **31.532,51**

Construção Civil | **Cód. Obra :** | **Art. :**

Informações Adicionais

I - "DOCUMENTO EMITIDO POR ME OU EPP OPTANTE PELO SIMPLES NACIONAL"; e II - "NÃO GERA DIREITO A CRÉDITO FISCAL DE IPI."
PROCON: TEL 151- SETOR COMERCIAL SUL, QUADRA 8, BLOCO B-60, SALA 240- BRASILIA - DF

Consulte a autenticidade deste documento acessando o site: https://iss.fazenda.df.gov.br/online/Login/Login.aspx
ISS.NET - Sistema Nota Control® • www.notacontrol.com.br

Ofício nº 100/2025

Brasília-DF, 25 de julho de 2025

Da Área Administrativo Financeira

Sh7 Proteção e Inteligência Cibernpetica Ltda

Para a Comissão Permanente de Contratação da Prefeitura de Cáceres MT

Pregoeiro

Assunto: Solicitação de Diligência – Apresentação de Notas Fiscais – SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA

Referência: Processo Administrativo nº 29/2025; Pregão Eletrônico nº 15/2025

Senhor Pregoeiro,

Após cumprimentá-lo cordialmente, passo a tratar da diligência considerando o recurso interposto pela empresa F.V.B.N. CONSTRUÇÕES E TECNOLOGIA LTDA, que questiona a validade do atestado técnico apresentado pela empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, emitido pela empresa Rede EXS Telecomunicações.

Ressalte-se que este pedido está fundamentada no Parecer Jurídico nº 214/2025-PGM, que recomenda a realização de diligência para verificar a veracidade e a fidedignidade do referido atestado, especialmente no que tange à comprovação da efetiva prestação dos serviços.

Destaque-se que a Sh7 apresentou documentação que inclui comprovantes de pagamento e contrato, mas não contempla as respectivas notas fiscais (emitido da Sh7 para a EXS), documentos necessários para que o atestado possa ser validado como prova de capacidade técnico operacional.

Ademais, conforme o parecer técnico da unidade demandante (CTI), que informou que, na ausência da validação do atestado da Rede EXS por meio de notas fiscais, a empresa SH7 não alcança o percentual mínimo de 30% do item de maior relevância técnica, conforme item 9.17.13 do edital.

Neste sentido, uma vez que as informações não foram suficientes para convalidação da documentação acostada ao processo, e, com fulcro no art. 67, §3º, da Lei nº 14.133/2021, e com o objetivo de garantir o devido processo legal, a transparência e o julgamento objetivo das propostas, essa Comissão Permanente de Contratação solicitou, no prazo de 24 horas, a realização de diligência junto à empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, para que apresente Notas fiscais emitidas pela empresa Rede EXS Telecomunicações Ltda, que comprovem a efetiva prestação dos serviços descritos no atestado técnico apresentado para fins de comprovação da

prestação do serviço objeto do contrato de parceria para subsequente habilitação no certame.

Do exposto, foi solicitado junto a Rede EXS as Notas Fiscais condizentes com o acordo de cooperação técnica entre as empresas Sh7 e EXS, uma vez que a primeira é uma empresa de cibersegurança focada em serviços e projetos de alta complexidade e, a segunda, empresa de Tecnologia da Informação e Comunicações, em que abas são autônomas e independentes, mas que uma contrata serviços da outra em modelo de parceria.

Por fim, para que não pairem dúvidas acerca da veracidade documental, encaminho-vos as Notas Fiscais solicitadas, a fim de comporem este processo com o objetivo de garantir o devido processo legal, a transparência e o julgamento objetivo das propostas, de acordo com o que essa Comissão Permanente de Contratação solicitou, dentro do prazo determinado de 24 horas.

Atenciosamente,

PAOLA DERRIAUX CHASTAGNIER:09387055710

Assinado de forma digital por PAOLA DERRIAUX CHASTAGNIER:09387055710
Dados: 2025.07.25 12:18:09 -03'00'

Paola Derriaux Chastagnier
Diretora de Licitações - CPF: 093.870.557-10

Ofício nº 101/2025

Brasília-DF, 28 de julho de 2025

Da Área Administrativo Financeira

Sh7 Proteção e Inteligência Cibernpetica Ltda

Para a Comissão Permanente de Contratação da Prefeitura de Cáceres MT

Pregoeiro

Assunto: Solicitação de Diligência – Apresentação de Notas Fiscais – SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA

Referência: Processo Administrativo nº 29/2025; Pregão Eletrônico nº 15/2025

Senhor Pregoeiro,

Após cumprimentá-lo cordialmente, passo a tratar da diligência complementar considerando o recurso interposto pela empresa F.V.B.N. CONSTRUÇÕES E TECNOLOGIA LTDA, que questiona a validade do atestado técnico apresentado pela empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, emitido pela empresa Rede EXS Telecomunicações.

Em face da diligência complementar, encaminho-vos as Notas Fiscais referentes aos comprovantes de repasses da EXS para a Sh7 em razão do acordo de parceria técnica operacional entre as empresas, em atenção ao Parecer Jurídico nº 214/2025-PGM, que recomenda a realização de diligência para verificar a veracidade e a fidedignidade do referido atestado, especialmente no que tange à comprovação da efetiva prestação dos serviços.

Isso posto, a referida documentação cumpre o estabelecido no referido parecer e nas regras editalícias bem como atende o prazo para o envio estipulado pela Comissão Permanente de Contratação solicitou.

Atenciosamente,

PAOLA DERRIAUX CHASTAGNIER:09387055710

Assinado de forma digital por PAOLA DERRIAUX CHASTAGNIER:09387055710
Dados: 2025.07.28 09:06:48 -03'00'

Sh7 Proteção e Inteligência Cibernética LTDA

Comprovante de Pagamento Pix

Valor: R$ 7.460,00

Realizado em: 11/06/2025 - 14:05:17

Solicitante: ROSELANE GONZALEZ DO NASCIMENT

Cooperativa e conta origem: 3953/36087-6

Nome do destinatário: G2Z

CNPJ do destinatário: 44.122.701/0001-79

Instituição do destinatário: NU PAGAMENTOS - IP

Agência e conta do destinatário: 1 / 160626821-5

Nome do pagador: Rede Exs Telecomunicacoes Ltda

CNPJ do pagador: 23.935.457/0001-93

Instituição do pagador: BANCO COOPERATIVO SICREDI S.A.

ID da transação: E10736214202506111705O1kTrODMo1k

Autenticação Eletrônica: E107.3621.4202.5061.1170.501k.TrOD.Mo1k

Número de Controle: 12532167101

Emitido em: 03/07/2025 - 17:19:43

* A transação acima foi realizada no nosso Aplicativo Sicredi conforme as condições especificadas neste comprovante.
* Os dados digitados são de responsabilidade do usuário.
Serviços por telefone 3003 4770 (Capitais e Regiões Metropolitanas) / 0800 724 4770 (Demais Regiões)
SAC 0800 724 7220 / Ouvidoria 0800 646 25 19

Comprovante de Pagamento Pix

Valor: R$ 20.000,00

Realizado em: 03/07/2025 - 18:15:16

Solicitante: ROSELANE GONZALEZ DO NASCIMENT

Cooperativa e conta origem: 3953/36087-6

Nome do destinatário: G2Z

CNPJ do destinatário: 44.122.701/0001-79

Instituição do destinatário: NU PAGAMENTOS - IP

Agência e conta do destinatário: 1 / 160626821-5

Nome do pagador: Rede Exs Telecomunicacoes Ltda

CNPJ do pagador: 23.935.457/0001-93

Instituição do pagador: BANCO COOPERATIVO SICREDI S.A.

ID da transação: E10736214202507032114 32J8CBvC6q3

Autenticação Eletrônica: E107.3621.4202.5070.3211.432J.8CBv.C6q3

Número de Controle: 12731695532

Emitido em: 03/07/2025 - 18:15:19

* A transação acima foi realizada no nosso Aplicativo Sicredi conforme as condições especificadas neste comprovante.
* Os dados digitados são de responsabilidade do usuário.
Serviços por telefone 3003 4770 (Capitais e Regiões Metropolitanas) / 0800 724 4770 (Demais Regiões)
SAC 0800 724 7220 / Ouvidoria 0800 646 25 19

De: Igor O. - SMA-CPL

Para: SMA-CPL - Comissão Permanente de Licitação

Data: 28/07/2025 às 11:27:17

Segue em anexo termo de julgamento e relatório de diligência

–

Igor de Souza Oliveira
Pregoeiro Oficial

Anexos:

relatorios_diligencia_98904705900152025_grupo_1.pdf
relatorio_julg_hab_98904705900152025_s1_grupo1.pdf

GOVERNO DO ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CACERES

RELATÓRIO DE DILIGÊNCIAS

UASG 989047 - PREFEITURA MUNICIPAL DE CACERES - MT

PREGÃO 90015/2025

Grupo 1

Diligência

Data início	Data encerramento	Situação	Solicitante
25/07/2025 às 16:22:45	28/07/2025 às 10:28:19	Encerrada	***.069.***-*2 - IGOR DE SOUZA OLIVEIRA

Fornecedor

44.122.701/0001-79 - SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA

Motivo

Informo que, de forma equivocada, foi determinada diligência para apresentação de notas fiscais emitidas pela empresa Rede EXS Telecomunicações Ltda., quando o correto seria a solicitação de notas fiscais emitidas pela própria empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA.

Análise

Em atendimento à diligência determinada no âmbito do julgamento do recurso administrativo interposto pela empresa F.V.B.N. CONSTRUÇÕES E TECNOLOGIA LTDA, foi solicitado à empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, conforme disposto no §3ª do art. 67 da Lei nª 14.133/2021, que apresentasse notas fiscais que comprovassem a efetiva prestação dos serviços descritos no atestado técnico emitido pela empresa.

No prazo concedido, a empresa apresentou as seguintes documentações:

Notas fiscais emitidas pela empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, correspondentes ao atestado apresentado para fins de habilitação;

Documentos que corroboram a efetiva execução dos serviços prestados, com detalhamento compatível com o objeto do certame, conforme exigido no item 9.17.13 do edital.

Conclusão

Diante da documentação apresentada dentro do prazo estabelecido, especialmente as notas fiscais emitidas pela empresa, que comprovam de forma idônea a efetiva prestação dos serviços descritos no atestado técnico, considera-se cumprida a diligência determinada.

Assim, declara-se encerrada a fase de diligência.

Anexos da diligência

Data/Hora	Anexos
25/07/2025 às 16:23:13	DILIGENCIA.docx

Anexos do fornecedor

Data/Hora	Anexos
28/07/2025 às 09:08:04	sicredi_1751577319213.pdf
28/07/2025 às 09:08:04	sicredi_1751573983751.pdf
28/07/2025 às 09:08:04	NF15.pdf
28/07/2025 às 09:08:28	NF17.pdf

Data/Hora	Anexos
28/07/2025 às 09:08:28	NF16.pdf
28/07/2025 às 09:09:03	OFICIO 101 - DILIGENCIA PE900152025 - PREFEITURA CACERES MT.pdf
28/07/2025 às 09:10:05	COMPROVANTE.pdf

Mensagens

Responsável	Data/Hora	Mensagem
Sistema para o participante 44.122.701/0001-79	25/07/2025 às 16:22:45	Sr. Fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79, uma nova diligência foi aberta para o item G1.
Sistema para o participante 44.122.701/0001-79	25/07/2025 às 16:23:13	Sr. Fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79, o arquivo DILIGENCIA.docx foi anexado à diligência aberta para o item G1.
Sistema para o participante 44.122.701/0001-79	25/07/2025 às 16:25:12	Sr. Fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79, você foi convocado para enviar anexos para o item G1, em sede de diligência. Prazo para encerrar o envio: 15:00:00 do dia 28/07/2025. Justificativa: Informo que, de forma equivocada, foi determinada diligência para apresentação de notas fiscais emitidas pela empresa Rede EXS Telecomunicações Ltda., quando o correto seria a solicitação de notas fiscais emitidas pela própria empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA. .
Sistema para o participante 44.122.701/0001-79	25/07/2025 às 16:25:30	Informo que, de forma equivocada, foi determinada diligência para apresentação de notas fiscais emitidas pela empresa Rede EXS Telecomunicações Ltda., quando o correto seria a solicitação de notas fiscais emitidas pela própria empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA.
Sistema para o participante 44.122.701/0001-79	25/07/2025 às 16:25:39	Considerando o equívoco por parte da Administração e o fato de que a empresa SH7 encaminhou os documentos exatamente conforme solicitado, informa-se que será instaurada nova diligência, com a finalidade de solicitar a apresentação das notas fiscais emitidas pela própria empresa SH7, como meio de comprovação idônea da execução dos serviços descritos no atestado técnico apresentado.
Pelo participante 44.122.701/0001-79	25/07/2025 às 16:43:32	Boa tarde. Cientes. Enviaremos a documentação dentro do prazo estipulado.
Pelo participante 44.122.701/0001-79	28/07/2025 às 09:59:54	Prezado Sr. Pregoeiro, bom dia. Documentação complementar enviada, conforme solicitação. Seguimos à disposição.
Pelo participante 44.122.701/0001-79	28/07/2025 às 10:00:00	O item G1 teve a convocação para envio de anexos, em sede de diligência, encerrada às 10:00:00 de 28/07/2025. 7 anexos foram enviados pelo fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79.
Sistema para o participante 44.122.701/0001-79	28/07/2025 às 10:28:19	O item G1 teve a diligência do fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79, analisada e concluída às 10:28:19 de 28/07/2025.

Eventos

Data/Hora	Descrição
25/07/2025 às 16:22:45	Diligência cadastrada.
25/07/2025 às 16:23:13	Anexo da diligência incluído "DILIGENCIA.docx".
25/07/2025 às 16:25:12	Fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79 convocado para envio de anexo(s), em sede de diligência. Prazo para encerrar o envio: 15:00:00 do dia 28/07/2025. Justificativa: Informo que, de forma equivocada, foi determinada diligência para apresentação de notas fiscais emitidas pela empresa Rede EXS Telecomunicações Ltda., quando o correto seria a solicitação de notas fiscais emitidas pela própria empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA.

Data/Hora	Descrição
28/07/2025 às 10:00:00	Convocação do fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79 para envio de anexo(s), em sede de diligência, finalizada pelo fornecedor.
28/07/2025 às 10:28:19	Fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79 teve a diligência para o item analisada e concluída às 10:28:19 de 28/07/2025.

Diligência

Data início	Data encerramento	Situação	Solicitante
24/07/2025 às 15:27:28	25/07/2025 às 15:16:22	Encerrada	***.069.***-*2 - IGOR DE SOUZA OLIVEIRA

Fornecedor

44.122.701/0001-79 - SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA

Motivo

Informamos que será realizada diligência com a empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, com a finalidade de solicitar a apresentação das notas fiscais referentes aos serviços prestados à empresa Rede EXS Telecomunicações Ltda, conforme atestado técnico apresentado no certame

Análise

Em atendimento à diligência determinada no âmbito do julgamento do recurso administrativo interposto pela empresa F.V.B.N. CONSTRUÇÕES E TECNOLOGIA LTDA, foi solicitado à empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, conforme disposto no §3ª do art. 67 da Lei nª 14.133/2021, que apresentasse notas fiscais que comprovassem a efetiva prestação dos serviços descritos no atestado técnico emitido pela empresa Rede EXS Telecomunicações Ltda.

No prazo concedido, a empresa apresentou as seguintes documentações:

Notas fiscais emitidas pela empresa Rede EXS Telecomunicações Ltda, correspondentes ao período e escopo descrito no atestado apresentado para fins de habilitação;

Documentos que corroboram a efetiva execução dos serviços prestados, com detalhamento compatível com o objeto do certame, conforme exigido no item 9.17.13 do edital.

Conclusão

Diante da documentação apresentada dentro do prazo estabelecido, especialmente as notas fiscais emitidas pela empresa Rede EXS Telecomunicações Ltda, que comprovam de forma idônea a efetiva prestação dos serviços descritos no atestado técnico, considera-se cumprida a diligência determinada.

Assim, declara-se encerrada a fase de diligência, com a validação do referido atestado técnico.

Anexos da diligência

Data/Hora	Anexos
24/07/2025 às 15:42:37	DILIGENCIA.pdf

Anexos do fornecedor

Data/Hora	Anexos
25/07/2025 às 12:23:37	NF 33 - MAI25 - SDWAN.pdf
25/07/2025 às 12:23:37	NF 35 - MAI25 - SDWAN.pdf
25/07/2025 às 12:23:37	NF 31 - ABR25- SDWAN.pdf
25/07/2025 às 12:23:37	NF 29 - MAR25 - SDWAN.pdf
25/07/2025 às 12:23:37	NF 27 - FEV25 - SDWAN.pdf
25/07/2025 às 12:24:57	OFICIO 100 - DILIGENCIA PE900152025 - PREFEITURA CACERES MT.pdf

Mensagens

Responsável	Data/Hora	Mensagem
Sistema para o participante 44.122.701/0001-79	24/07/2025 às 15:27:28	Sr. Fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79, uma nova diligência foi aberta para o item G1.
Pelo participante 44.122.701/0001-79	24/07/2025 às 15:35:06	Boa tarde, Sr. Pregoeiro. Qual

Responsável	Data/Hora	Mensagem
Pelo participante 44.122.701/0001-79	24/07/2025 às 15:35:19	Qual o prazo para envio dos documentos complementares solicitados?
Sistema para o participante 44.122.701/0001-79	24/07/2025 às 15:42:37	Sr. Fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79, o arquivo DILIGENCIA.pdf foi anexado à diligência aberta para o item G1.
Sistema para o participante 44.122.701/0001-79	24/07/2025 às 15:45:22	Sr. Fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79, você foi convocado para enviar anexos para o item G1, em sede de diligência. Prazo para encerrar o envio: 16:00:00 do dia 25/07/2025. Justificativa: Informamos que será realizada diligência com a empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, com a finalidade de solicitar a apresentação das notas fiscais referentes aos serviços prestados à empresa Rede EXS Telecomunicações Ltda, conforme atestado técnico apresentado no certame.
Pelo participante 44.122.701/0001-79	24/07/2025 às 15:45:51	Ciente. Obrigada
Sistema para o participante 44.122.701/0001-79	24/07/2025 às 15:46:01	Informamos que será realizada diligência com a empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, com a finalidade de solicitar a apresentação das notas fiscais referentes aos serviços prestados à empresa Rede EXS Telecomunicações Ltda, conforme atestado técnico apresentado no certame
Pelo participante 44.122.701/0001-79	25/07/2025 às 12:27:34	O item G1 teve a convocação para envio de anexos, em sede de diligência, encerrada às 12:27:34 de 25/07/2025. 6 anexos foram enviados pelo fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79.
Pelo participante 44.122.701/0001-79	25/07/2025 às 12:28:08	Prezado Sr. Pregoeiro. Documentação complementar anexada, conforme solicitação
Sistema para o participante 44.122.701/0001-79	25/07/2025 às 15:09:33	Recebemos os documentos, estamos análisando.
Sistema para o participante 44.122.701/0001-79	25/07/2025 às 15:16:22	O item G1 teve a diligência do fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79, analisada e concluída às 15:16:22 de 25/07/2025.

Eventos

Data/Hora	Descrição
24/07/2025 às 15:27:28	Diligência cadastrada.
24/07/2025 às 15:42:37	Anexo da diligência incluído "DILIGENCIA.pdf".
24/07/2025 às 15:45:22	Fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79 convocado para envio de anexo(s), em sede de diligência. Prazo para encerrar o envio: 16:00:00 do dia 25/07/2025. Justificativa: Informamos que será realizada diligência com a empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, com a finalidade de solicitar a apresentação das notas fiscais referentes aos serviços prestados à empresa Rede EXS Telecomunicações Ltda, conforme atestado técnico apresentado no certame
25/07/2025 às 12:27:34	Convocação do fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79 para envio de anexo(s), em sede de diligência, finalizada pelo fornecedor.
25/07/2025 às 15:16:22	Fornecedor SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, CNPJ 44.122.701/0001-79 teve a diligência para o item analisada e concluída às 15:16:22 de 25/07/2025.