IGAP-840D

Industrial WIFI5 Access Point with 4x10/100/1000Base-T(X)

User Manual

Version 1.0

November 2024

www.oringnet.com

COPYRIGHT NOTICE

Copyright © 2024 ORing Industrial Networking Corp.
All rights reserved.
No part of this publication may be reproduced in any form without the prior written consent of ORing Industrial Networking Corp.

TRADEMARKS

ORing is a registered trademark of ORing Industrial Networking Corp.
All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

WARRANTY

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.
Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. ORing shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ORing reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

ORing Industrial Networking Corp.
3F., NO.542-2, Jhongjheng Rd., Sindian District, New Taipei City 231, Taiwan, R.O.C.
Tel: + 886 2 2218 1066 // Fax: + 886 2 2218 1014
Website: www.oringnet.com

Technical Support
E-mail: support@oringnet.com

Sales Contact
E-mail: sales@oringnet.com (Headquarters)
info@oring-china.com (China)

Tables of Content

Getting Started

1.1 About the IGAP-840D

IGAP-840D is a reliable WLAN Access Point with 4 Ethernet Gigabit ports and WIFI5 wireless module. It can be configured to operate in AP/Client/Repeater mode. You are able to configure IGAP-840D by WEB interface via LAN port or WLAN interface. IGAP-840D provides Ethernet ports in switch mode to reduce the usage of Ethernet switch ports. Therefore, IGAP-840D series is one of the best communication solutions for wireless applications on the industrial network.

1.2 Software Features

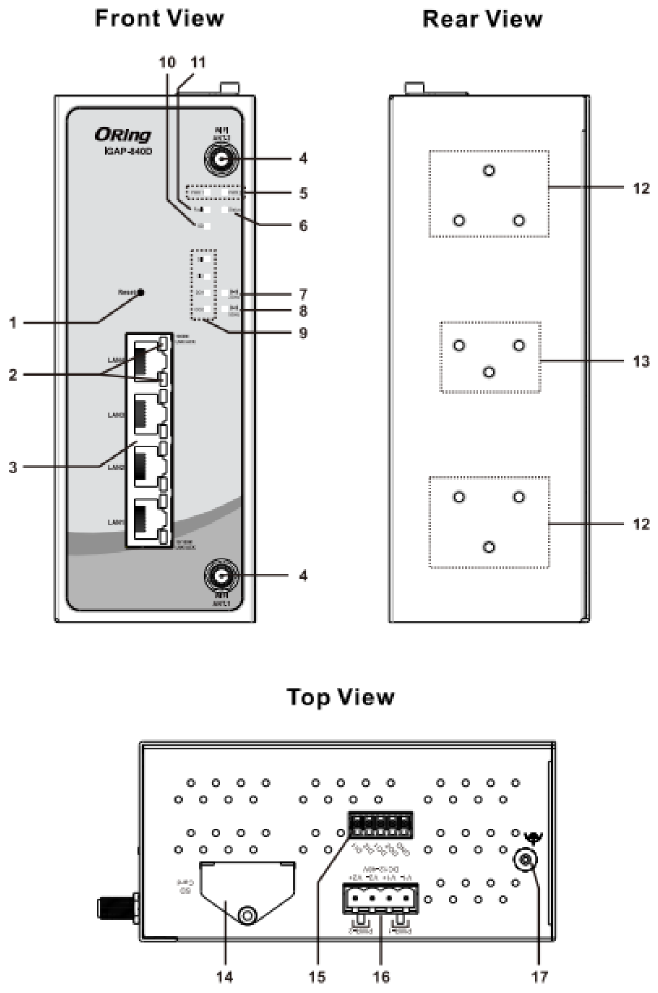
- Secure management by HTTPS
- Versatile modes & event alarm by e-mail
- Event warning by Syslog, e-mail, SNMP trap

1.3 Hardware Features

- 4 x 10/100/1000 Base-T(X) Ethernet ports.
- Dual band WIFI5 up to 867Mbps link speed
- Dual DC inputs
- Operating temperature: -30 to 70°C
- Storage temperature: -40 to 85°C
- Operating humidity: 5% to 95%, non-condensing
- DIN-Rail and Wall-mount.
- Casing: IP-30
- Dimensions: 60(W) x 125(D) x 158(H) mm

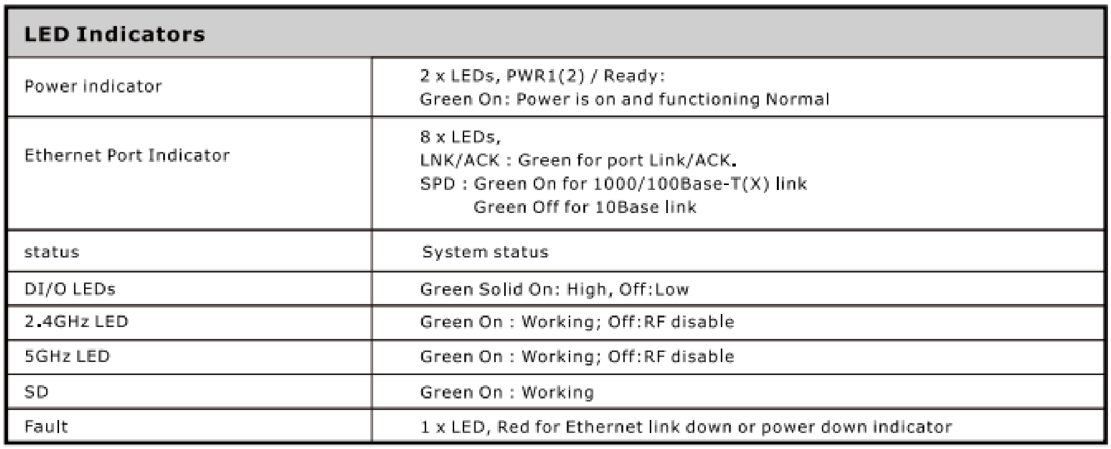
Hardware Overview

2.1 Panel Layouts



1. Reset button
2. Ethernet LED
3. Ethernet Port
4. WIFI antenna connector
5. LED for Power
6. LED for Status
7. WIFI 2.4GHz On
8. WIFI 5GHz On
9. Digital High/Low
10. SD card status
11. Fault LED
12. Wall-mount screw holes
13. Din-rail screw holes
14. SD card slot
15. Digital Input/Output
16. Power Input
17. Grounding screw

2.2 Front Panel LEDs

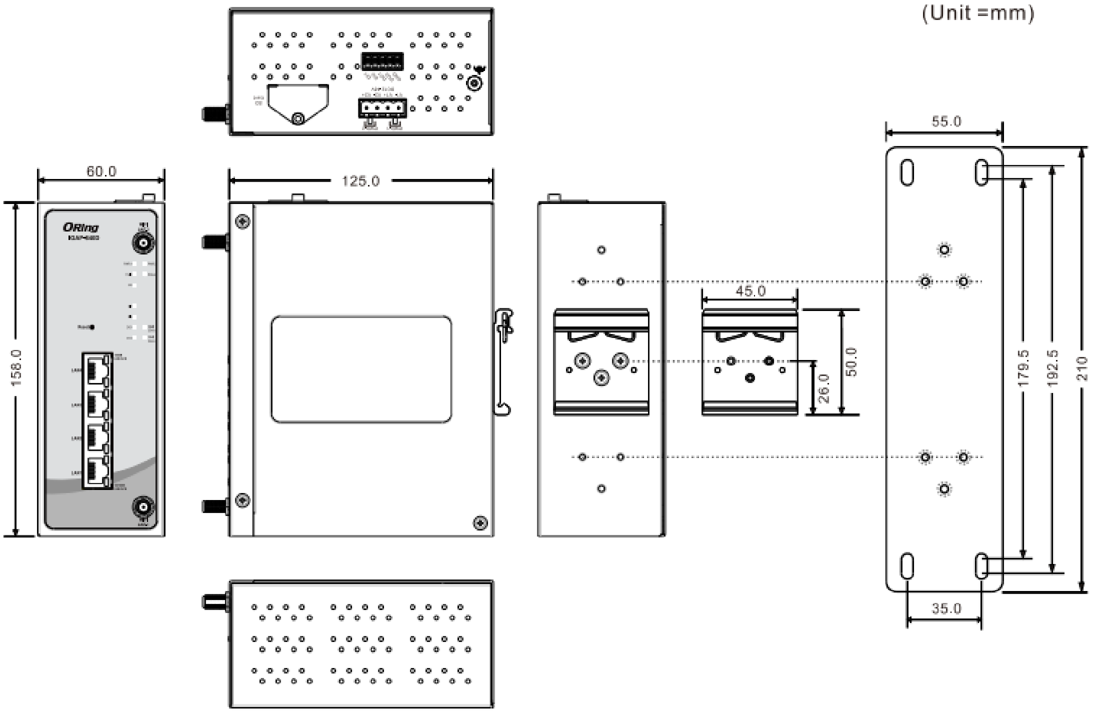


LED Indicators	
Power indicator	2 x LEDs, PWR1(2) / Ready: Green On: Power is on and functioning Normal
Ethernet Port Indicator	8 x LEDs, LNK/ACK : Green for port Link/ACK. SPD : Green On for 1000/100Base-T(X) link Green Off for 10Base link
status	System status
DI/O LEDs	Green Solid On: High, Off:Low
2.4GHz LED	Green On : Working; Off:RF disable
5GHz LED	Green On : Working; Off:RF disable
SD	Green On : Working
Fault	1 x LED, Red for Ethernet link down or power down indicator

Hardware Installation

3.1 Wall Mounting

Besides Din-rail, the Access Point can be fixed to the wall via a wall mount panel, which can be found in the package.



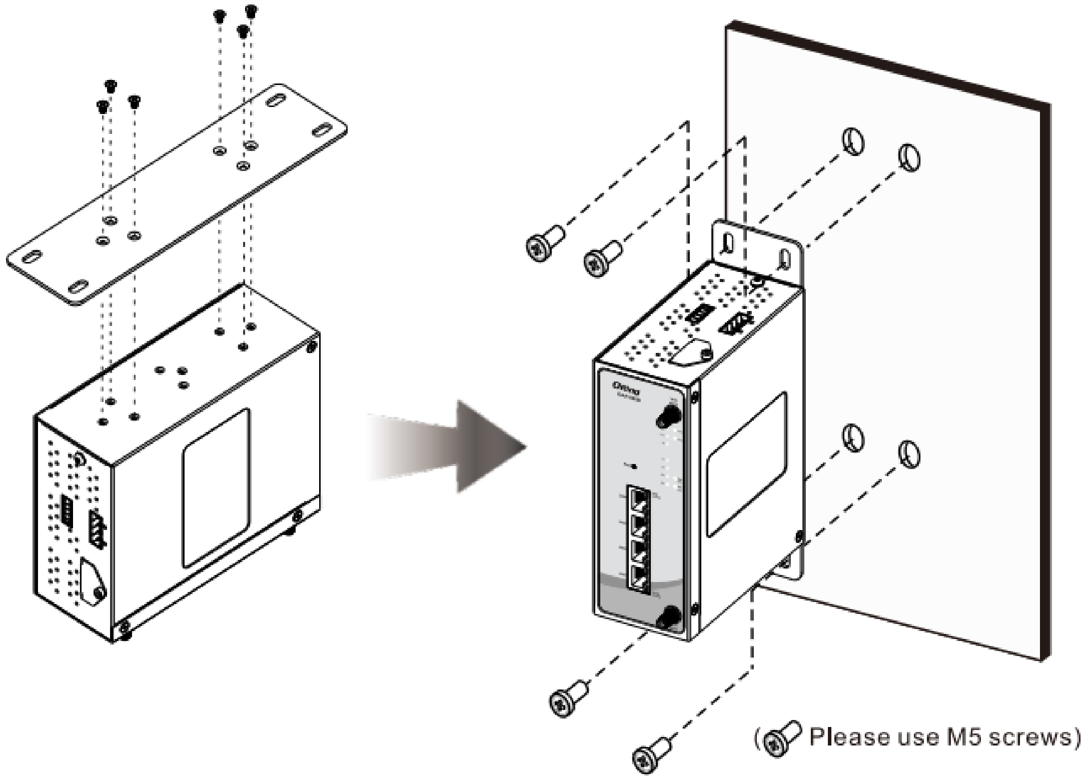
Wall-Mount Kit Measurement (Unit = mm)

To mount the Access Point onto the wall, follow the steps:

Step 1: Screw the two pieces of wall-mount kits onto both ends of the rear panel of the Access Point. A total of six screws are required, as shown below.

Step 2: Use the Access Point, with wall mount plates attached, as a guide to mark the correct locations of the four screws.

Step 3: Insert a screw head through the large part of the keyhole-shaped aperture on the plate, and then slide the Access Point downwards. Tighten the four screws for added stability.



The screws should be 6mm diameter head x 3mm diameter thread, as shown below. Note that the screws should not be larger than the size used in the series to prevent damaging the Access Point.

3.3 Wiring

WARNING
Be sure to switch off the power and make sure the area is not hazardous before disconnecting modules or wires. The devices may only be connected to the supply voltage shown on the type of plate.

3.3.1 Grounding

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices.

3.3.2 Dual Power Inputs

IGAP-840D has two sets of power inputs, power input 1 and power input 2, on a 4-pin terminal block on the Access Point's top panel. Follow the steps below to wire redundant power inputs.

Step 1: insert the negative/positive DC wires into the V-/V+ terminals, respectively.

Step 2: to keep the DC wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.

ATTENTION

1. Be sure to disconnect the power cord before installing and/or wiring your Access Points.
2. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.
3. If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.
4. Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
5. Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
6. You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring sharing similar electrical characteristics can be bundled together
7. You should separate input wiring from output wiring
8. It is advised to label the wiring to all devices in the system

Cables and Antenna

4.1 Ethernet Cables

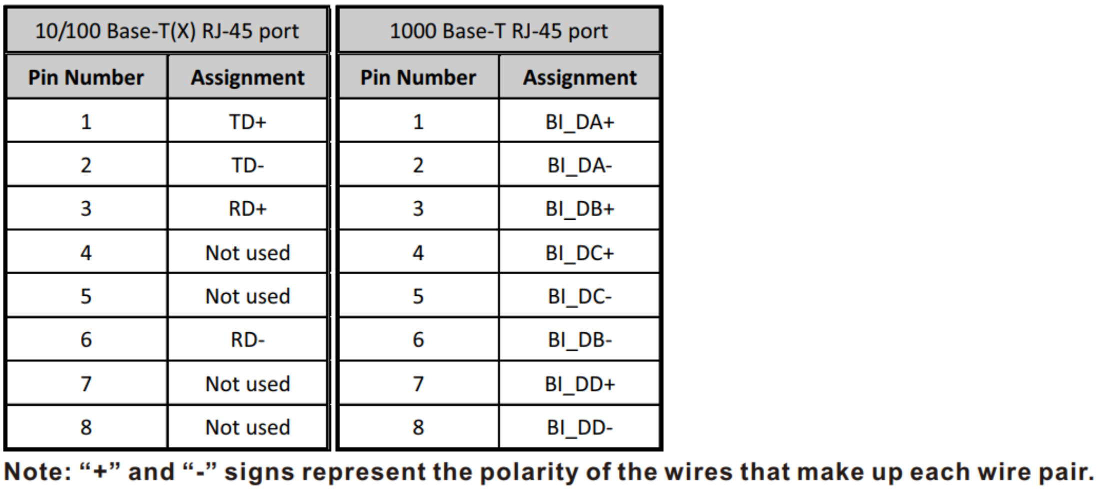
IGMG-8224D-D5G has four 10/100/1000Base-T(X) Ethernet ports. According to the link type, the device uses CAT 3, 4, 5, 5e, 6 UTP cables to connect to any other network device (PCs, servers, switches, Access Points, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft.)	RJ45
100BASE-T(X)	Cat. 5 100-ohm UTP	UTP 100 m (328 ft.)	RJ45
1000BASE-T(X)	Cat. 5e 100-ohm UTP	UTP 100 m (328 ft.)	RJ45

4.2 RJ-45 Pin Assignment

10/100/1000 Base-T(X) RJ-45 Pin Assignements :



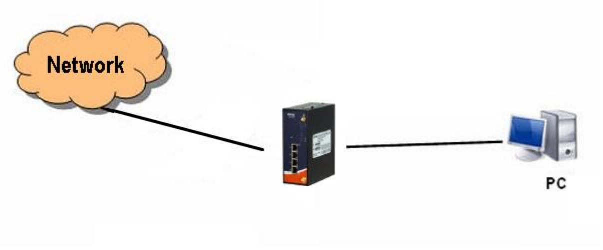
10/100 Base-T(X) RJ-45 port		1000 Base-T RJ-45 port	
Pin Number	Assignment	Pin Number	Assignment
1	TD+	1	BI_DA+
2	TD-	2	BI_DA-
3	RD+	3	BI_DB+
4	Not used	4	BI_DC+
5	Not used	5	BI_DC-
6	RD-	6	BI_DB-
7	Not used	7	BI_DD+
8	Not used	8	BI_DD-

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

Management Interface

5.1 Installation

Before installing the Access Point, you need to be able to access the Access Point via a computer equipped with an Ethernet card. To simplify the connection, it is recommended to use an Ethernet card to connect to a LAN.



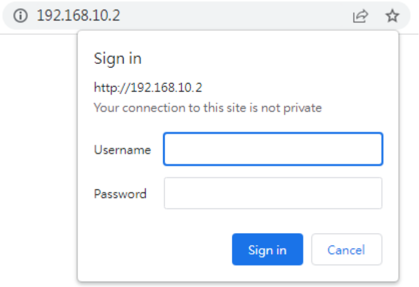
Follow the steps below to install and connect the Access Point to PC:

Step 1: Select power source. The Access Point can be powered by +12~48V DC power input.

Step 2: Computer set a static IP address 192.168.10.3 Subnet Mask 255.255.255.0 to Ethernet Card

Step 3: Connect a computer to the Access Point. Use either a straight-through Ethernet cable or cross-over cable to connect the LAN port to a computer. Once the LED of the LAN port lights up, which indicates the connection is established.

Step 4: Configure the Access point on a web-based management utility. Open a web browser on your computer and type http://192.168.10.2 (default gateway IP of the Access Point) in the address box to access the webpage. A login window will pop up where you can enter the default login name admin and password admin. For security reasons, we strongly recommend you go to change the password. Click on **Administration** > **System Settings** after logging in to change the password.

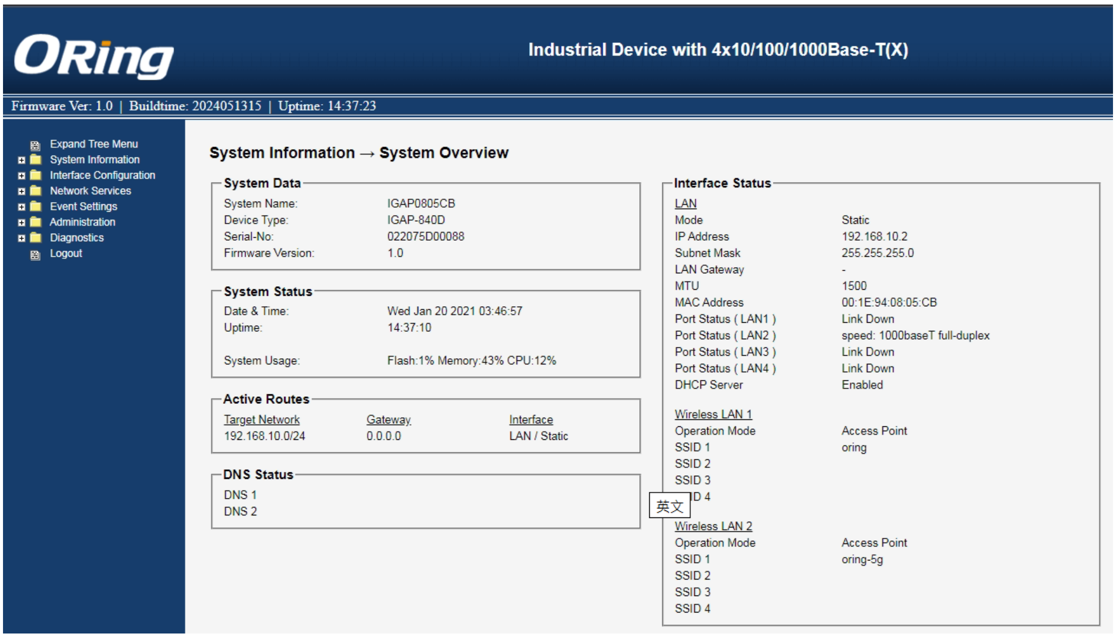


http://192.168.10.2
Your connection to this site is not private

Username

Password

After you log in successfully, a Web interface will appear, as shown below. On the left-hand side of the interface is a list of functions where you can configure the settings. The details of the configurations will be shown on the right screen.



Firmware Ver: 1.0 | Buildtime: 2024051315 | Uptime: 14:37:23

System Information → System Overview

System Data

System Name:	IGAP0805CB
Device Type:	IGAP-840D
Serial-No:	022075D00088
Firmware Version:	1.0

System Status

Date & Time:	Wed Jan 20 2021 03:46:57
Uptime:	14:37:10
System Usage:	Flash:1% Memory:43% CPU:12%

Active Routes

Target Network	Gateway	Interface
192.168.10.0/24	0.0.0.0	LAN / Static

DNS Status

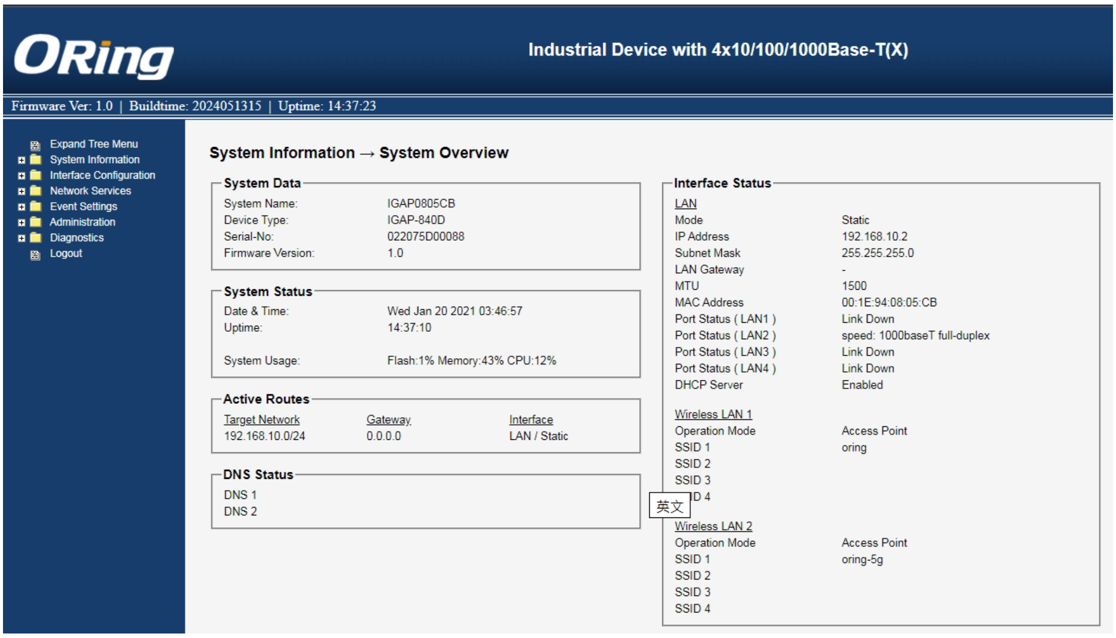
DNS 1
DNS 2

Interface Status

LAN	
Mode	Static
IP Address	192.168.10.2
Subnet Mask	255.255.255.0
LAN Gateway	-
MTU	1500
MAC Address	00:1E:94:08:05:CB
Port Status (LAN1)	Link Down
Port Status (LAN2)	speed: 1000baseT full-duplex
Port Status (LAN3)	Link Down
Port Status (LAN4)	Link Down
DHCP Server	Enabled
Wireless LAN 1	
Operation Mode	Access Point
SSID 1	oring
SSID 2	
SSID 3	
D 4	
Wireless LAN 2	
Operation Mode	Access Point
SSID 1	oring-5g
SSID 2	
SSID 3	
SSID 4	

5.2 Configuration

On top of the screen shows information about the firmware version and uptime.



```
Firmware Ver: 1.0 | Buildtime: 2024051315 | Uptime: 14:37:23

System Information → System Overview

System Data
System Name:          IGAP0805CB
Device Type:          IGAP-840D
Serial-No:            022075D00088
Firmware Version:     1.0

System Status
Date & Time:          Wed Jan 20 2021 03:46:57
Uptime:               14:37:10

System Usage:         Flash:1% Memory:43% CPU:12%

Active Routes
Target Network        Gateway        Interface
192.168.10.0/24       0.0.0.0        LAN / Static

DNS Status
DNS 1
DNS 2

Interface Status
LAN
Mode                  Static
IP Address            192.168.10.2
Subnet Mask           255.255.255.0
LAN Gateway           -
MTU                   1500
MAC Address           00:1E:94:08:05:CB
Port Status ( LAN1 )  Link Down
Port Status ( LAN2 )  speed: 1000baseT full-duplex
Port Status ( LAN3 )  Link Down
Port Status ( LAN4 )  Link Down
DHCP Server           Enabled

Wireless LAN 1
Operation Mode        Access Point
SSID 1                oring
SSID 2
SSID 3
D 4

Wireless LAN 2
Operation Mode        Access Point
SSID 1                oring-5g
SSID 2
SSID 3
SSID 4
```

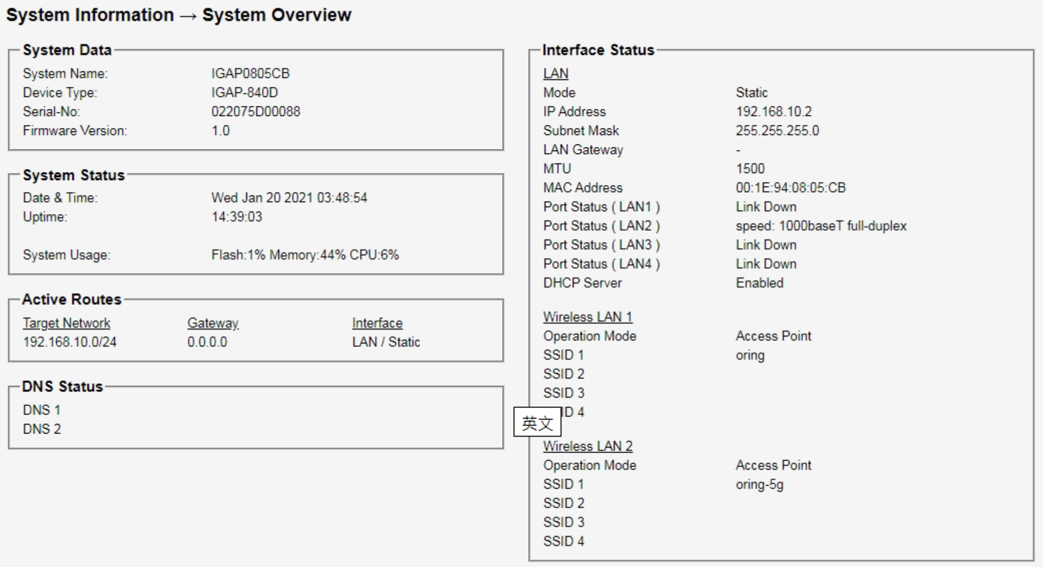
Label	Description
Firmware	Shows the current firmware version
Uptime	Shows the elapsed time since the Access Point is started

5.2.1 System Information

System information shows up all system information and Wired/Wireless LAN traffic statistics.

System Overview

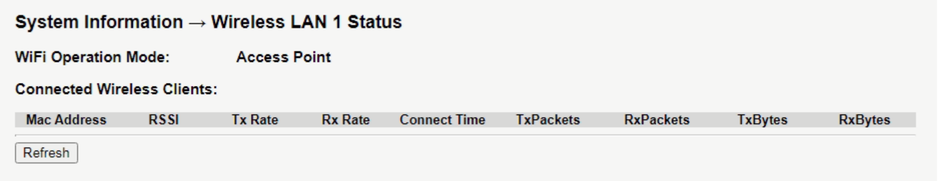
System basic information



```
System Information → System Overview

System Data
System Name:          IGAP0805CB
Device Type:          IGAP-840D
Serial-No:            022075D00088
Firmware Version:     1.0

System Status
Date & Time:          Wed Jan 20 2021 03:48:54
Uptime:               14:39:03

System Usage:         Flash:1% Memory:44% CPU:6%

Active Routes
Target Network        Gateway        Interface
192.168.10.0/24       0.0.0.0        LAN / Static

DNS Status
DNS 1
DNS 2

Interface Status
LAN
Mode                  Static
IP Address            192.168.10.2
Subnet Mask           255.255.255.0
LAN Gateway           -
MTU                   1500
MAC Address           00:1E:94:08:05:CB
Port Status ( LAN1 )  Link Down
Port Status ( LAN2 )  speed: 1000baseT full-duplex
Port Status ( LAN3 )  Link Down
Port Status ( LAN4 )  Link Down
DHCP Server           Enabled

Wireless LAN 1
Operation Mode        Access Point
SSID 1                oring
SSID 2
SSID 3
D 4

Wireless LAN 2
Operation Mode        Access Point
SSID 1                oring-5g
SSID 2
SSID 3
SSID 4
```

Wireless LAN 1&2 Status

Include Wireless Operation mode and connected client status.



System Information → Wireless LAN 1 Status

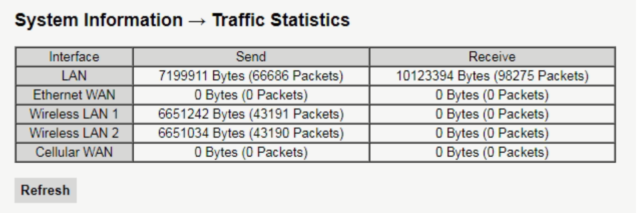
WiFi Operation Mode: Access Point

Connected Wireless Clients:

Mac Address	RSSI	Tx Rate	Rx Rate	Connect Time	TxPackets	RxPackets	TxBytes	RxBytes

Traffic Statistics

Wire LAN/WAN traffic statistics.



System Information → Traffic Statistics

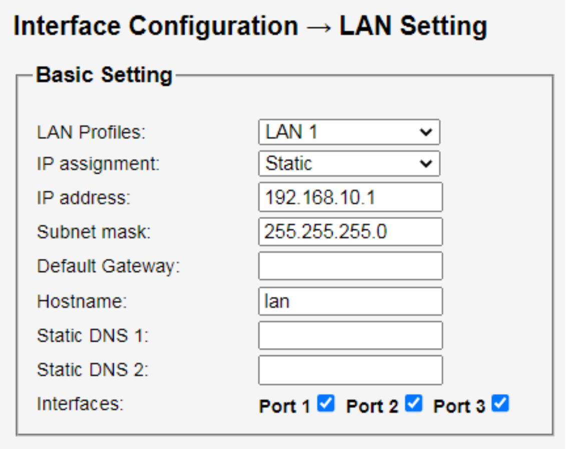
Interface	Send	Receive
LAN	7199911 Bytes (66686 Packets)	10123394 Bytes (98275 Packets)
Ethernet WAN	0 Bytes (0 Packets)	0 Bytes (0 Packets)
Wireless LAN 1	6651242 Bytes (43191 Packets)	0 Bytes (0 Packets)
Wireless LAN 2	6651034 Bytes (43190 Packets)	0 Bytes (0 Packets)
Cellular WAN	0 Bytes (0 Packets)	0 Bytes (0 Packets)

5.2.2 Interface Configuration

This section will guide you through the general settings for the Access Point.

LAN Setting

This page allows you to configure the IP settings of the LAN for the Access Point. The LAN IP address is private to your internal network and is not visible to Internet.



Interface Configuration → LAN Setting

Basic Setting

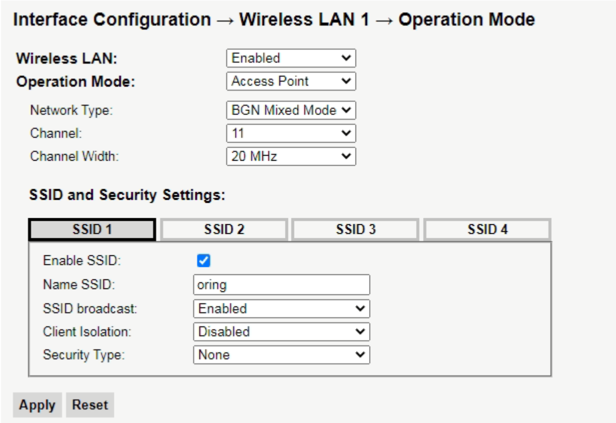
LAN Profiles:	LAN 1
IP assignment:	Static
IP address:	192.168.10.1
Subnet mask:	255.255.255.0
Default Gateway:	
Hostname:	lan
Static DNS 1:	
Static DNS 2:	
Interfaces:	Port 1 ☑ Port 2 ☑ Port 3 ☑

Label	Description
LAN Profiles	Assign profile (LAN1, LAN2 and LAN3) for group configuration
IP assignment	Assign IP address by static or DHCP
IP Address	The IP address of the LAN. The default value is **192.168.10.1**

Subnet Mask	The subnet mask of the LAN. The default value is **255.255.255.0**
Default Gateway	Assign default gateway address for Access Point
Hostname	Assign hostname for Access Point
Static DNS 1/2	Assign DNS address for Access Point
Interfaces	Assign interface (Port 1, Port 2 and Port 3) for above configuration

Wireless LAN 1&2

Operation Mode-Access Point



Interface Configuration → Wireless LAN 1 → Operation Mode

Wireless LAN: Enabled
Operation Mode: Access Point
Network Type: BGN Mixed Mode
Channel: 11
Channel Width: 20 MHz

SSID and Security Settings:

Enable SSID: ☑
Name SSID: oring
SSID broadcast: Enabled
Client Isolation: Disabled
Security Type: None

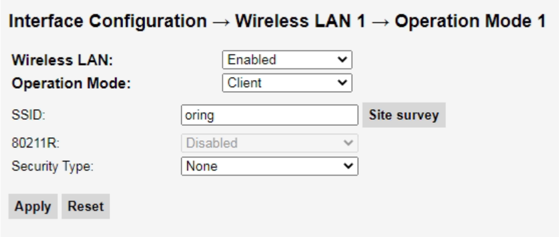
Label	Description
Wireless LAN	Enable/Disable interface
Operation Mode	Device provides 3 Wi-Fi connection mode and support Access Point/Client/Repeater mode
Network Type	Wireless support WIFI 2.4G BG/BGN mode and Wireless 2 support WIFI 5G A/AN/AC mode
Channel	WIFI Channel setting
Channel Width	Wireless support 20/40Mhz, Wireless 2 support 20/40/80MHz

SSID & Security Setting

Each Wireless interface supports up to 4 individual SSID and Security setting

Label	Description
Enable SSID	Enable/Disable SSID.
SSID Name	SSID naming.
SSID Broadcast	Enable/Disable SSID broadcast function.
Client Isolation	Client Isolation can be enabled on a WLAN where we do not want users communicating with each other within the local network and the goal is to only allow them access to the internet.
Security Type	Wireless support WPA/WPA2 Personal, AES/TKIP encryption.

Operation Mode-Client

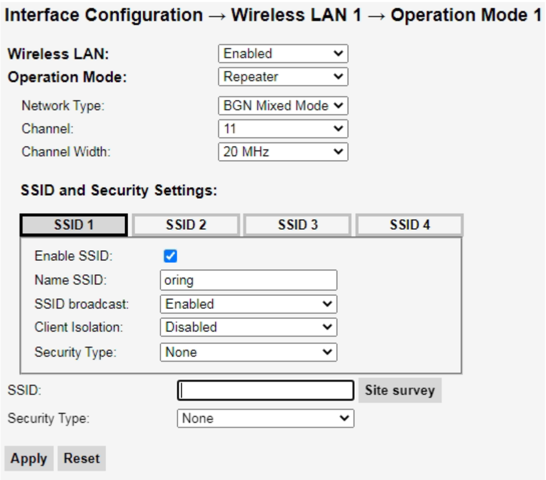


Interface Configuration → Wireless LAN 1 → Operation Mode 1

Wireless LAN: Enabled
Operation Mode: Client
SSID: oring
80211R: Disabled
Security Type: None

Label	Description
SSID Site survey	Site survey client SSID
802.11R	Enable/Disable 802.11R support
Security type	Wireless support WPA/WPA2 Personal, AES/TKIP encryption

Operation Mode-Repeater



Interface Configuration → Wireless LAN 1 → Operation Mode 1

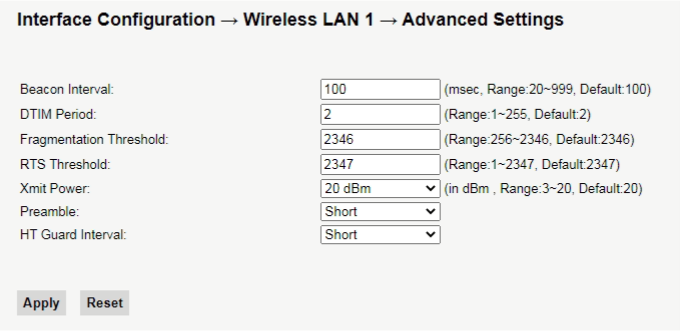
Wireless LAN: Enabled
Operation Mode: Repeater
Network Type: BGN Mixed Mode
Channel: 11
Channel Width: 20 MHz

SSID and Security Settings:

Enable SSID: ☑
Name SSID: oring
SSID broadcast: Enabled
Client Isolation: Disabled
Security Type: None
SSID:
Security Type: None

Label	Description
SSID Site survey	Site survey Repeater SSID
Security type	Wireless support WPA/WPA2 Personal, AES/TKIP encryption

Advanced Settings



Interface Configuration → Wireless LAN 1 → Advanced Settings

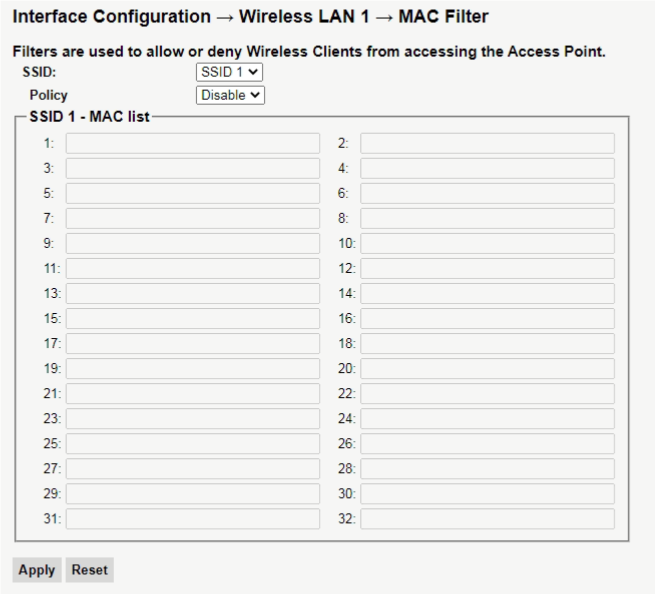
Beacon Interval:	100	(msec, Range:20~999, Default:100)
DTIM Period:	2	(Range:1~255, Default:2)
Fragmentation Threshold:	2346	(Range:256~2346, Default:2346)
RTS Threshold:	2347	(Range:1~2347, Default:2347)
Xmit Power:	20 dBm	(in dBm , Range:3~20, Default:20)
Preamble:	Short	
HT Guard Interval:	Short	

Label	Description
Beacon Interval	A beacon is a packet sent by a wireless access point to synchronize wireless devices. The beacon interval value indicates the frequency interval of the beacon. Increasing the beacon interval reduces the number of beacons and the overhead associated with them. The default value is 100, but 50 is recommended when reception is poor
DTIM Period	The value is an integer that ranges from 1 to 255, in Beacons. The DTIM interval specifies how many Beacon frames are sent before the Beacon frame that contains the DITM. A long DTIM interval lengthens the dormancy time of the STA and saves power, but degrades the transmission capability of the STA. A short interval helps transmitting data in a timely manner, but the STA is wakened up frequently, causing high power consumption
Fragmentation Threshold	Specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or “off”. Setting the Fragmentation Threshold too low may result in poor network performance. The use of fragmentation can increase the reliability of frame transmissions. Because smaller frames are sent, collisions are much less likely to occur. However lower values of the Fragmentation Threshold will result lower throughput as well. Little or no modification of the Fragmentation Threshold value is recommended as the default setting of 2346 is optimum for most wireless networks.
RTS Threshold	Determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes, or "off". The default value is 2347, which means that

	RTS is disabled. RTS/CTS (Request to Send / Clear to Send) is the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden AP25N01 User Manual 85terminal problem. RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately. System uses Request to Send/Clear to Send frames for the handshake which provide collision reduction for access point with hidden stations. The stations are sending an RTS frame first while data is sent only after handshake with an AP is completed. Stations respond with the CTS frame to the RTS, which provides clear media for the requesting station to send the data. CTS collision control management has time interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.
Xmit Power	Transmit power of the radio. This is the total power supplied to the antennas of the radio
Preamble	Available values include **Long** and **Short**, with **Long** as the default value. If all clients and access points in your wireless network support short preamble, then enabling it can boost overall throughput. However, if any wireless device does not support short preamble, then it will not be able to communicate with your network. If you are not sure whether your radio supports the short RF preamble, you must disable this feature

MAC Filter

Filters are used to allow or deny Wireless Clients from accessing the Access Point.



Interface Configuration → Wireless LAN 1 → MAC Filter

Filters are used to allow or deny Wireless Clients from accessing the Access Point.

SSID: SSID 1

Policy: Disable

SSID 1 - MAC list

Label	Description
SSID	Choose to apply SSID
Policy	Deny/Allow Policy
MAC list	Add Client MAC address to list table

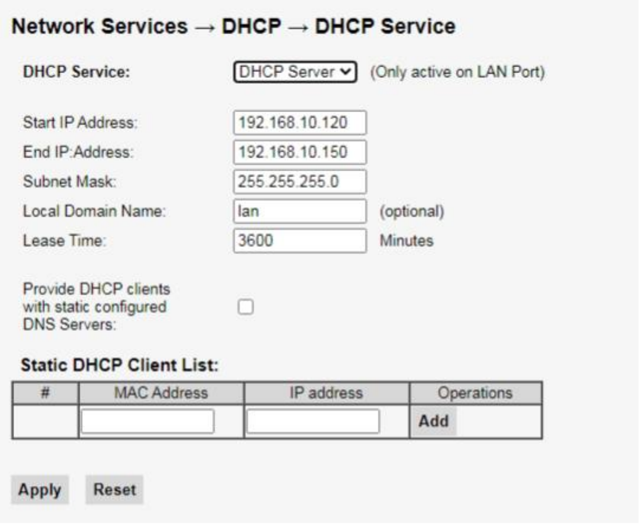
5.2.3 Networking Services

DHCP

DHCP is a network protocol designed to allow devices connected to a network to communicate with each other using an IP address. The connection works in a client-server model, in which DHCP clients request an IP address from a DHCP server. The Access Point comes with a built-in DHCP (Dynamic Host Control Protocol) server which assigns an IP address to a computer (DHCP client) on the LAN automatically. The Access Point can also serve as a relay agent which will forward DHCP requests from DHCP clients to a DHCP server on the Internet.

The IP allocation provides one-to-one mapping of MAC address to IP address. When a computer with a MAC address requesting an IP address from the Access Point, it will be assigned with the IP address according to the mapping. You can choose one from the client list and add it to the mapping list.

DHCP Service



Network Services → DHCP → DHCP Service

DHCP Service: DHCP Server (Only active on LAN Port)

Start IP Address: 192.168.10.120

End IP:Address: 192.168.10.150

Subnet Mask: 255.255.255.0

Local Domain Name: lan (optional)

Lease Time: 3600 Minutes

Provide DHCP clients with static configured DNS Servers: □

Static DHCP Client List:

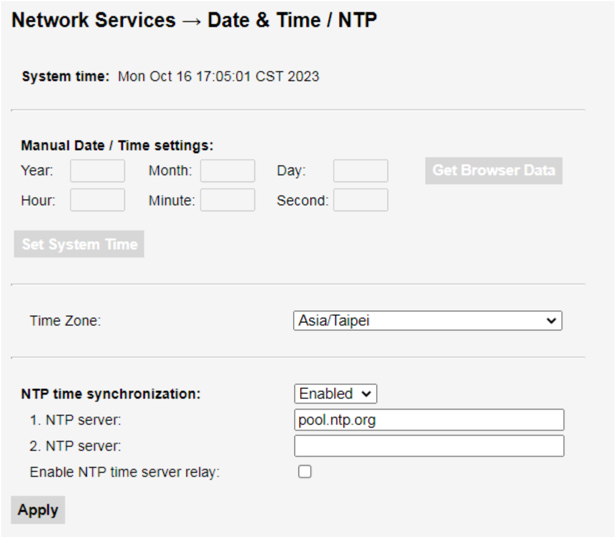
#	MAC Address	IP address	Operations
			Add

Label	Description
DHCP Server	Enable or disable the DHCP server function. The default setting is **Enabled**.
Starting IP	The starting IP address of the IP range assigned by the DHCP server
Ending IP	The ending IP address of the IP range assigned by the DHCP server
Lease Time	The period of time for the IP address to be leased. During the lease time, the DHCP server cannot assign that IP address to

	any other clients. Enter a number in the field. The default setting is 48 hours.
Local Domain Name	Enter the local domain name of a private network (optional)
Provide DHCP clients with static configured DNS Servers	Provide static configured DNS server address (LAN Setting) to DHCP clients.
Static DHCP Client List	Add the one-to-one relationship of the MAC address and IP address.

Date & Time / NTP

In this page, you can set the date & time of the device. A correct date and time will help the system log events. You can set up a NTP (Network Time Protocol) client to synchronize date & time with a NTP server on the Internet.



Network Services → Date & Time / NTP

System time: Mon Oct 16 17:05:01 CST 2023

Manual Date / Time settings:

Year: Month: Day:

Hour: Minute: Second:

Time Zone: Asia/Taipei

NTP time synchronization: Enabled

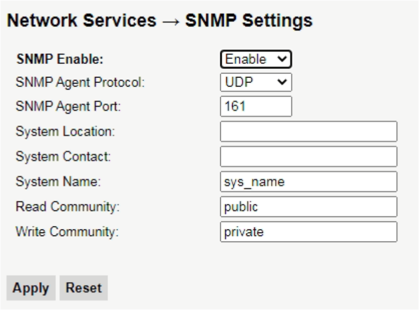
1. NTP server: pool.ntp.org

2. NTP server:

Enable NTP time server relay: □

Label	Description
Get Browser Date	Get Date and Time from Browser
Set System Time	Set the setting value to system
Time Zone	Assign Time Zone for system
NTP time synchronization	Enable or disable NTP function
Time Zone	Select the time zone you are located in
NTP Server	Set NTP server address for synchronization
Enable NTP time server relay	Check for NTP time server relay

SNMP Setting



Network Services → SNMP Settings

SNMP Enable: Enable

SNMP Agent Protocol: UDP

SNMP Agent Port: 161

System Location:

System Contact:

System Name: sys_name

Read Community: public

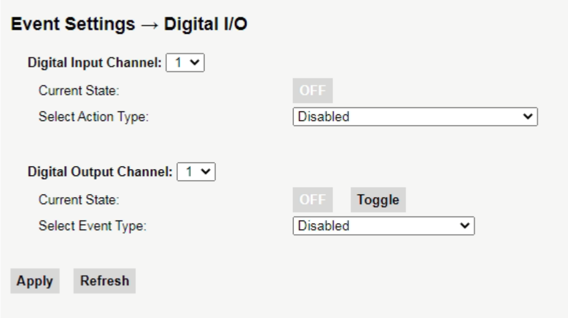
Write Community: private

Label	Description
SNMP Enable	SNMP (Simple Network Management Protocol) Agent is a service program that runs on the Access Point. The agent provides management information to the NMS by keeping track of various operational aspects of the system. Turn on to open this service and off to shutdown it.
SNMP Agent Protocol	Select packet type for SNMP protocol
SNMP Agent Port	Specify SNMP listening port
System Location	Specify System Location of SNMP Agent
System Contact	Specify System Contact of SNMP Agent
System Name	Specify System Name of SNMP Agent
Read Community	Community is essentially password to establish trust between managers and agents. Normally "public" is used for read-only community.
Write Community	Community is essentially password to establish trust between managers and agents. Normally "public" is used for read-write community.

5.2.4 Event Setting

When an error occurs, the device will notify you through system log, and SNMP messages. You can configure the system to issue a notification when specific events occur by checking the box next to the event.

Digital I/O



Event Settings → Digital I/O

Digital Input Channel: 1

Current State: OFF

Select Action Type: Disabled

Digital Output Channel: 1

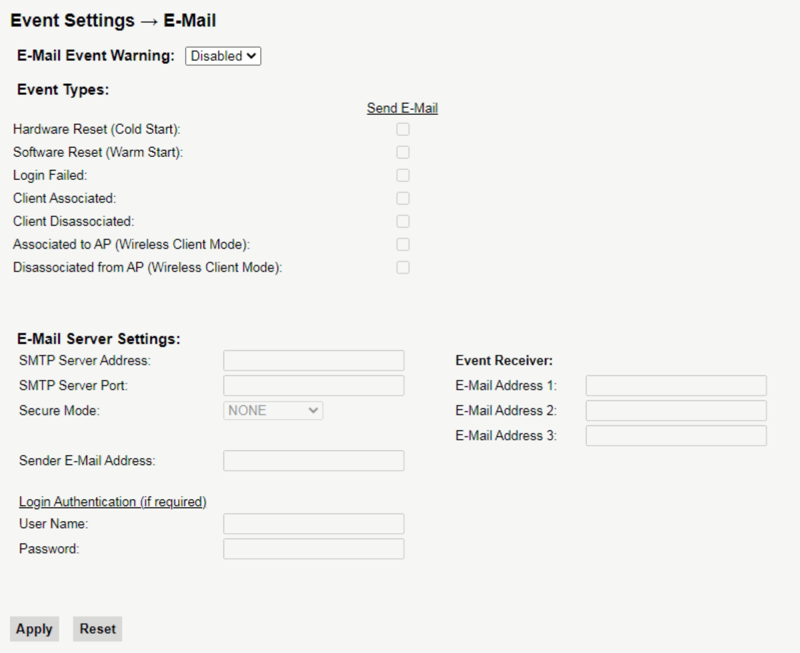
Current State: OFF

Select Event Type: Disabled

Label	Description
Digital Input	When Channel 1 and 2 State changed will action one of below **Start/Stop OpenVPN Server** or **Connect/Disconnect OpenVPN Client.**
Digital Output	manually or one of events below occur **OpenVPN Server status** or **OpenVPN Client status** will toggle channel 1 and 2 state

E-Mail

Send the event alert via email.



Event Settings → E-Mail

E-Mail Event Warning: Disabled

Event Types:

	Send E-Mail
Hardware Reset (Cold Start):	□
Software Reset (Warm Start):	□
Login Failed:	□
Client Associated:	□
Client Disassociated:	□
Associated to AP (Wireless Client Mode):	□
Disassociated from AP (Wireless Client Mode):	□

E-Mail Server Settings:

SMTP Server Address:

SMTP Server Port:

Secure Mode: NONE

Sender E-Mail Address:

Login Authentication (if required)

User Name:

Password:

Event Receiver:

E-Mail Address 1:

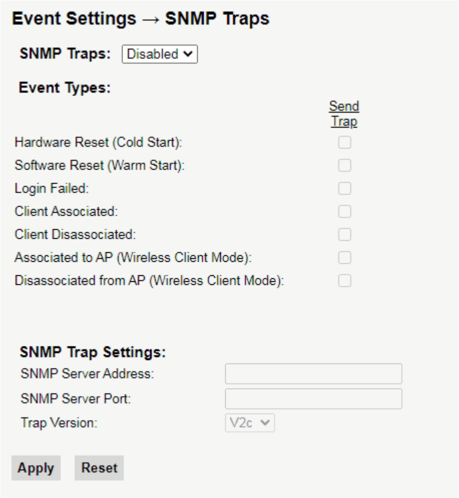
E-Mail Address 2:

E-Mail Address 3:

Label	Description
SMTP Server	Enter a backup host to be used when the primary host is unavailable.
Server Port	Specifies the port where MTA can be contacted via SMTP server
E-mail Address 1-3	Enter the mail address that will receive notifications

SNMP Traps

Send event alert via SNMP trap protocol.



Event Settings → SNMP Traps

SNMP Traps: Disabled

Event Types:

	Send Trap
Hardware Reset (Cold Start):	□
Software Reset (Warm Start):	□
Login Failed:	□
Client Associated:	□
Client Disassociated:	□
Associated to AP (Wireless Client Mode):	□
Disassociated from AP (Wireless Client Mode):	□

SNMP Trap Settings:

SNMP Server Address:

SNMP Server Port:

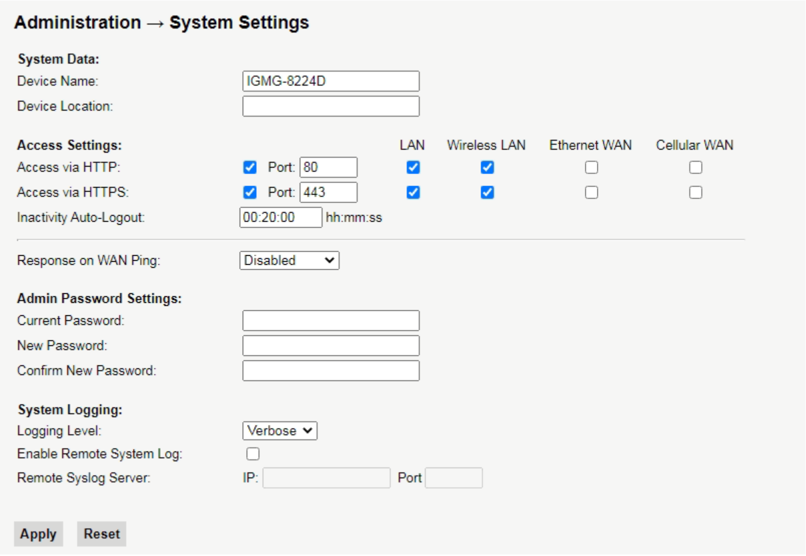
Trap Version: V2c

Label	Description
SNMP Server Address	Enter the IP address of the SNMP server which will send out traps generated by the AP.
SNMP Server Port	Enter Trap server using port
Trap Version	Support V2c

5.2.5 Administration

System Setting

System setting include web access setting, Web login name and password in page; default login name and password are both **admin** and system log server setting.



Administration → System Settings

System Data:
Device Name: IGMG-8224D
Device Location:

Access Settings:		LAN	Wireless LAN	Ethernet WAN	Cellular WAN
Access via HTTP:	☑ Port: 80	☑	☑	□	□
Access via HTTPS:	☑ Port: 443	☑	☑	□	□
Inactivity Auto-Logout:	00:20:00 hh:mm:ss				

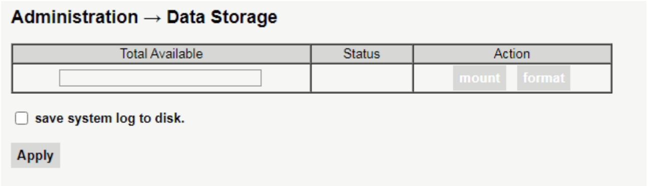
Response on WAN Ping: Disabled

Admin Password Settings:
Current Password:
New Password:
Confirm New Password:

System Logging:
Logging Level: Verbose
Enable Remote System Log: □
Remote Syslog Server: IP: Port

Label	Description
Device Name	Assign name for device
Device Location	Type in device location
Confirm New Password	Retype the new password to confirm it.
Access setting	Choose a web management page protocol from **HTTP** and **HTTPS**. HTTPS (HTTP over SSL) encrypts data sent and received over the Web. Choose HTTPS if you want a secure connection.
Port	Choose a web management page port number. For HTTP, default port is 80. For HTTPS, default port is 443.
Response on WAN Ping	Click Enable to allow system administrator to ping the Access Point from WAN interface
Remote Syslog IP	Enter the IP address of a remote server if you want the logs to be stored remotely. Leave it blank will disable remote syslog.
Remote Syslog Port	Specifies the port to be logged remotely. Default port is 514.

Data Storage



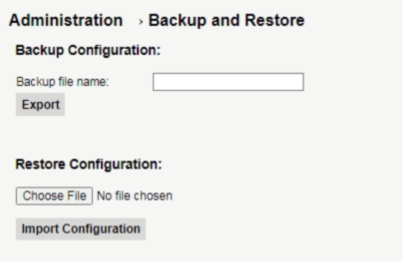
Administration → Data Storage

Total Available	Status	Action
		mount format

□ save system log to disk.

Backup and Restore Configurations

This page allows you to save configurations or return settings to previous status. You can download the configuration file from the Web. Note: users using old versions of Internet Explorer may have to click on the warning on top of the browser and choose Download File.



Administration › Backup and Restore

Backup Configuration:

Backup file name:

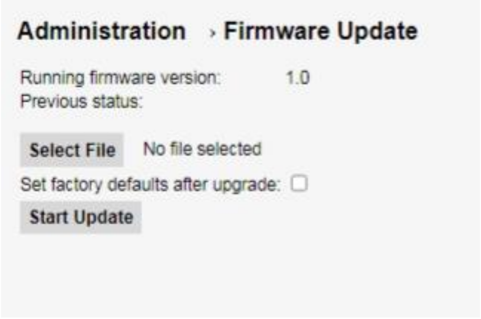
Restore Configuration:

Choose File No file chosen

Label	Description
Export	Click to Save existing configurations as a file for future usage.
Import	You can restore configurations to previous status by installing a previous configuration file.
Restore Factory Default Setting	Click to reset the Access Point to the factory settings. The Access Point will reboot to validate the default settings.

Firmware Upgrade

ORing launches new firmware constantly to enhance Access Point performance and functions. To upgrade firmware, download new firmware from ORing's website to your PC and install it via Web upgrade. Make sure the firmware file matches the model of your Access Point. It will take several minutes to upload and update the firmware. After upgrade completes successfully, reboot the Access Point.



Administration › Firmware Update

Running firmware version: 1.0

Previous status:

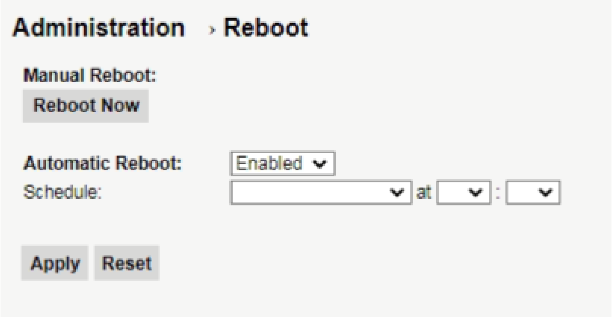
Select File No file selected

Set factory defaults after upgrade: □

⚠ During firmware upgrading, do not turn off the power of the Access Point or press the reset button.

Reboot

This page allows you to configure restart settings for the Access Point.

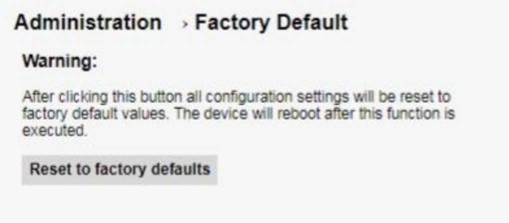


Automatic Reboot: Enabled

Label	Description
Reboot Now	Click to restart the Access Point via warm reset
Automatic Reboot	**Enable**: check to activate the setting Reboot at: specify the time for resetting the Access Point. You can configure the action to be performed periodically.

Factory Default

Click to reset the Access Point to the factory settings. The Access Point will reboot to validate the default settings.

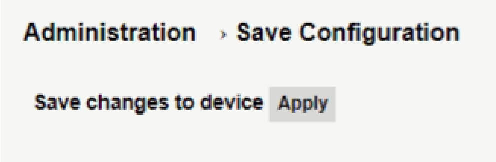


Warning:

After clicking this button all configuration settings will be reset to factory default values. The device will reboot after this function is executed.

Save device configuration.

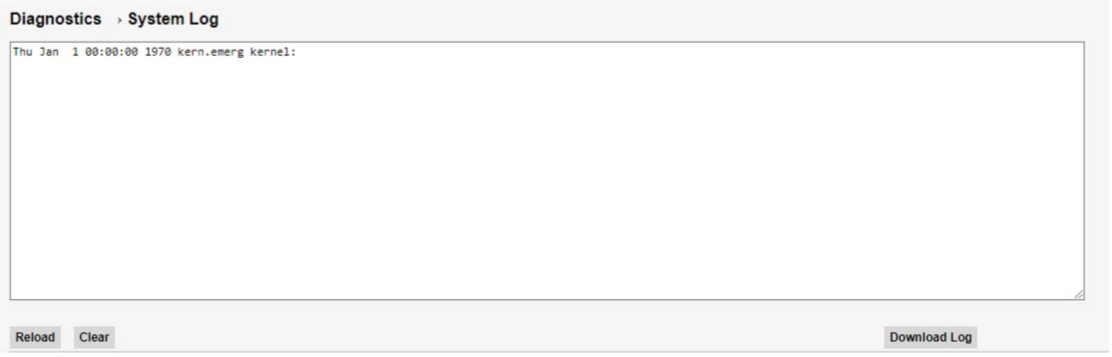
Click Apply to save all Changes to device.



5.2.6 Diagnostics

System Log

The Access Point will constantly log the events and provide the files for you to review. You can click **Reload** to renew the page, **Clear** to clear all or certain log entries and **Download** to save all logs to file.

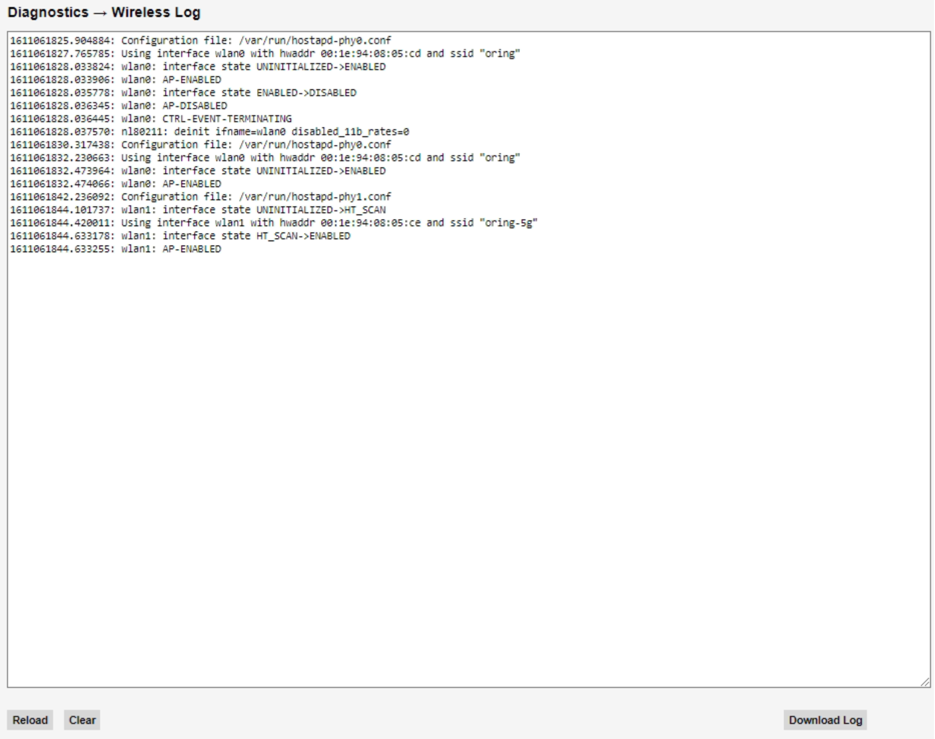


Diagnostics › System Log

```
Thu Jan  1 00:00:00 1970 kern.emerg kernel:
```

Wireless Log

The Access Point will constantly log the Wireless events and provide the files for you to review. You can click **Reload** to renew the page, **Clear** to clear all or certain log entries and **Download** to save all logs to file.

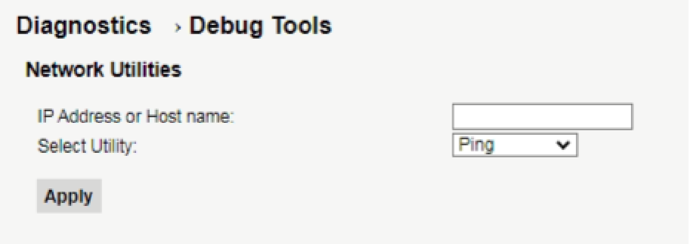


Diagnostics → Wireless Log

```
1611061825.904884: Configuration file: /var/run/hostapd-phy0.conf
1611061827.765785: Using interface wlan0 with hwaddr 00:1e:94:08:05:cd and ssid "oring"
1611061828.033824: wlan0: interface state UNINITIALIZED->ENABLED
1611061828.033906: wlan0: AP-ENABLED
1611061828.035778: wlan0: interface state ENABLED->DISABLED
1611061828.036345: wlan0: AP-DISABLED
1611061828.036445: wlan0: CTRL-EVENT-TERMINATING
1611061828.037570: nl80211: deinit ifname=wlan0 disabled_11b_rates=0
1611061830.317438: Configuration file: /var/run/hostapd-phy0.conf
1611061832.230663: Using interface wlan0 with hwaddr 00:1e:94:08:05:cd and ssid "oring"
1611061832.473964: wlan0: interface state UNINITIALIZED->ENABLED
1611061832.474066: wlan0: AP-ENABLED
1611061842.236092: Configuration file: /var/run/hostapd-phy1.conf
1611061844.101737: wlan1: interface state UNINITIALIZED->HT_SCAN
1611061844.420011: Using interface wlan1 with hwaddr 00:1e:94:08:05:ce and ssid "oring-5g"
1611061844.633178: wlan1: interface state HT_SCAN->ENABLED
1611061844.633255: wlan1: AP-ENABLED
```

Debug Tools

Use utility Tool Ping, Trace Route and NSLookup to check any IP or Host.



Diagnostics › Debug Tools

Network Utilities

IP Address or Host name:

Select Utility: Ping

Technical Specifications

ORing AP Model	IGAP-840D
Physical Ports	
10/100/1000 Base-T(X) Ports in RJ45 Auto MDI/MDIX	**4 LAN**
5-Pin Terminal Block	**DI x 2** and **DO x 2 :** Dry Contact: On: short to GND, Off: open Wet Contact (DI to COM/GND): On: 0 to 3VDC, Off: 10 to 30VDC
WLAN interface	
Antenna Connector	2 x Reverse SMA Female
Modulation	802.11a: OFDM 802.11b: CCK, DQPSK, DBPSK 802.11g: OFDM 802.11n: BPSK, QPSK, 16-QAM, 64-QAM 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
Frequency Band	America / FCC: 2.412~2.462 GHz (11 channels) 5.180~5.240 GHz & 5.745~5.825 GHz (9 channels) Europe CE / ETSI: 2.412~2.472 GHz (13 channels) 5.180~5.240 GHz (4 channels)
Transmission Rate	802.11b: 1/2/5.5/11 Mbps 802.11a/g: 6/9/12/18/24/36/48/54 Mbps 802.11n: UP to 300 Mbps 802.11ac: up to 867Mbps
Transmit Power	IEEE 802.11a: 21dBm ± 2dBm@54Mbps IEEE 802.11b: 23dBm ± 2dBm@11Mbps IEEE 802.11g: 20dBm ± 2dBm@54Mbps IEEE 802.11gn HT20: 18dBm ± 2dBm @MCS7 IEEE 802.11gn HT40: 18dBm ± 2dBm @MCS7 IEEE 802.11an HT20: 20dBm ± 2dBm @MCS7 IEEE 802.11an HT40: 20dBm ± 2dBm @MCS7 IEEE 802.11ac VHT80: 20dBm ± 2dBm @MCS9
Receiver Sensitivity	IEEE 802.11a : -75dBm ± 2dBm@54Mbps IEEE 802.11b : -90dBm ± 2dBm@11Mbps IEEE 802.11g : -75dBm ± 2dBm@54Mbps IEEE 802.11gn HT20:-72dBm ± 2dBm@MCS7 IEEE 802.11gn HT40:-70dBm ± 2dBm@MCS7 IEEE 802.11an HT20:-72dBm ± 2dBm@MCS7 IEEE 802.11an HT40:-69dBm ± 2dBm@MCS7 IEEE 802.11ac VHT80:-60dBm ± 2dBm@MCS9
Encryption Security	WEP: (64-bit ,128-bit key supported) WPA/WPA2 :802.11i(WEP and AES encryption) WPA-PSK (256-bit key pre-shared key supported) 802.1X Authentication supported TKIP encryption
Wireless Security	SSID broadcast disable
LED indicators	
Power indicator	2 x LEDs, PWR1(2) / Ready: Green On : Power is on and functioning Normal
Fault	Green On : When fault event occurs
Status	Green On: System Ready
SD	Green On: Working

DI/O LEDs	4 x LEDs Green Solid On: High, Off:Low
2.4GHz LED	Green On : Working; Off:RF disable
5GHz LED	Green On : Working; Off:RF disable
Power	
Redundant Input power	Dual DC inputs. 12-48VDC on 4-pin terminal block
Power consumption	13w
Overload current protection	Present
Reverse polarity protection	Present
Physical Characteristic	
Enclosure	IP-30
Dimension (W x D x H)	60(W) x 125(D) x 158(H) mm
Weight (g)	1000g
Environmental	
Storage Temperature	-40 to 85oC (-40 to 185°F)
Operating Temperature	-10 to 70°C (14 to 158°F)
Operating Humidity	5% to 95% Non-condensing
Regulatory approvals	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC60068-2-31
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	5 years