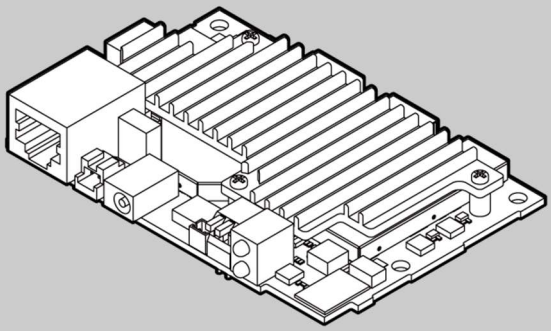
CONTEC

IEEE802.11ax/ac/n/a/b/g Wireless LAN
(Access Point / Station)

FXE5000-US



CONTENTS

CONTEC CO., LTD.

Table of Contents

Table of Contents

Table of Contents

Introduction

This section provides necessary information of the product such as the outline, bundled items and manuals before actual use.

1.Related Manuals

The manuals related to the product are listed below.

Read them as necessary along with this document.

◆ Must Read the Following Manuals.

Name	Purpose	Contents	How to get
Please Read the following	Must read this after opening the package.	This introduces related materials that are made available on the CONTEC website, such as those for the included items, manuals, and software.	Included in the package (Printed matter)
Reference Manual - Hardware (This document)	Read this when operating the product.	This describes the hardware aspects such as functions and settings.	Download from the Contec website (PDF)

◆ Download Manuals

Download the manuals accordingly from the following URL.

Download https://www.contec.com/download/

1.Features

Wi-Fi 6E (IEEE 802.11ax) compliant high-speed and low-latency communication

Effective throughput is greatly improved, and data transmission and reception is 2.8 times faster (2.4Gbps) than Wi-Fi 5 (800Mbps). New technologies such as OFDMA(Orthogonal Frequency Division Multiple Access) and MU-MIMO (Multi-User MIMO) have been implemented, greatly improving throughput degradation and delays that occur when many satellite stations are used simultaneously.

Mesh Wi-Fi network

The wireless mesh network function allows a single network group (ESSID) to be configured by multiple access points in a mesh pattern. Even if a failure occurs in any part of the communication path, the network can be built resistant to failures, such as automatically securing the best alternative path and maintaining communication connections. Wireless connections between access points make it easy to expand the communication area by simply increasing the number of access points.

Smart Roaming (Duplex)

Dual Station Mode is installed to extend communication from one wireless connection to two wireless connections. If one wireless connection is lost, data communication will not be lost while roaming because another wireless connection is available. Contec's unique tuning for "uninterruptible wireless LAN" enables high-dimensional roaming.

Supports a various power supply

AC adaptor (sold separately) and 5~30VDC DC power supply are supported.

- ## This product can be switched between access point, station (client), and repeater operation modes

By switching the operation mode, you can use this product as not only an access point but also as a station (client) and a repeater. You can use this product as a wireless LAN converter for a wired LAN device.
You can also use both 5 GHz / 6GHz and 2.4 GHz interfaces simultaneously in Dual Station Mode.

- ## The proprietary encryption technology "WSL" that is available along with WPA3/WPA2/WPA and WEP.

In addition to the certifications for advanced security standards WPA3/WPA2/WPA and IEEE802.1X, this product is also equipped with our proprietary encryption technology "WSL", which can be used at the same time as these certifications. MAC address filtering and ESSID hiding are also supported.

Features variety of functions, including VLAN and a virtual AP function

This product is equipped with a VLAN function for constructing virtual networks and a virtual AP function for operating one AP as multiple virtual APs with different security settings. Also, large capacity event logs can be saved.

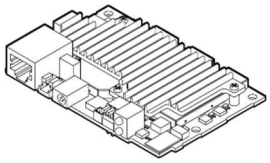
*VLAN function will be supported by firmware upgrade.

2.Included Items

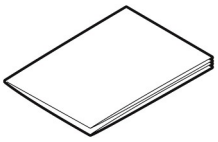
The product consists of the items listed below.

Check, with the following list, that your package is complete.

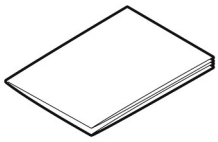
If you discover damaged or missing items, contact your retailer.



Main unit...1



Please read the following...1



Setup Guide...1

3.Check the firmware version

Before running the product, visit our website to check the firmware version and update to the latest one if necessary.

Updating firmware to the latest version will resolve troubles and stabilize the operation.

Download https://www.contec.com/download/

Safety Precautions

Understand the following definitions and precautions to use the product safely.
Never fail to read them before using the product.

1. Safety Information

This document provides safety information using the following symbols to prevent accidents resulting in injury or death and the destruction of equipment and resources.

Understand the meanings of these labels to operate the equipment safely.

⚠ **DANGER**	Signal word used to indicate an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ **WARNING**	Signal word used to indicate a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ **CAUTION**	Signal word used to indicate a potentially hazardous situation which, if not avoided, could result in minor or moderate injury.

2.Handling Precautions

⚠ DANGER

Do not use the product where it is exposed to flammable or corrosive gas. Doing so may result in an explosion, fire, electric shock, or failure.

⚠ CAUTION

- This product contains precision electronic elements and must not be used in locations subject to physical shock or strong vibration. Otherwise, the board may malfunction, overheat, or cause a failure.
- Do not use or store this device in high temperature or low temperature surroundings, or do not expose it to extreme temperature changes. Otherwise, the board may malfunction, overheat, or cause a failure.
- Do not use or store this device where it is exposed to direct sunlight or near stoves or other sources of heat. Otherwise, the board may malfunction, overheat, or cause a failure.
- Do not use or store this device near strong magnetic fields or devices emitting electromagnetic radiation. Otherwise, the board may malfunction, overheat, or cause a failure.
- If an unusual smell or overheat is noticed, unplug the power cable immediately.
- In the event of an abnormal condition or malfunction, please contact your retailer.
- This product may become hot. Do not touch this product directly during operation or immediately after the power is turned off. Also, do not place this product where you may touch this part.
- The specifications of this product are subject to change without notice for enhancement and quality improvement.
  Even when using the product continuously, be sure to read the manual on the website and understand the contents.
  For details about settings that have been added as a result of the specification changes, refer to Help of the browser settings screen. The Help of the latest firmware provides the latest information.
  For the latest version of the firmware, download the firmware from our company website and perform the version upgrade yourself.
- Do not modify the product. CONTEC will bear no responsibility for any problems, etc., resulting from modifying the product.
- Regardless of the foregoing statements, CONTEC is not liable for any damages whatsoever (Including damages for loss of business profits) arising out of the use or inability to use this CONTEC product or the information contained herein.
- Repair or replacement of this product is a sendback.

- Wireless LAN devices may not perform normal wireless communication due to factors such as the installation environment, the unit's settings, and the communication load of the network system.
- When replacing this product (FLEXLAN 5000 series) with another series of wireless LAN devices (FLEXLAN 4000/3000/2000/1000/DS540 series, etc.), it may be necessary to rebuild the network system due to differences in product specifications and functions. When using this product, we recommend that you thoroughly evaluate it using a our company lender in the actual environment.
- When using this product in a location that is affected by overcurrent or overvoltage (lightning surge, etc.), select and use an appropriate surge protective device (SPD) for all approach routes (Power line, ground, etc.). SPD selection, installation, and installation should be performed by a professional service provider.
- Communication quality may be degraded if this product is too close to metal/concrete walls (including steel beams).
- Radio equipment on the same channel (wireless frequency) as this product existing in the area where communication is possible may lead to reduced transfer speed or degraded communication quality and may even make normal communication impossible.
- This product is approved under U.S. radio laws and cannot be used in other countries.
- Because this product communicates wirelessly, the radio waves reach all locations within a certain range, passing through obstacles (such as walls). Consequently, it may be possible for a third party to intercept communication if the security settings are not configured.
- This product is equipped with security functions, so—to reduce security problems—be sure to configure the security settings before use.
- Do not touch the power connector when supplying power via the DC jack. Doing so creates the risk of electric shock and malfunction.
- Do not touch the DC jack when supplying power via the power connector. Doing so creates the risk of electric shock and malfunction.
- When disposing of the product, follow the disposal procedures stipulated under the relevant laws and municipal ordinances.
- Do not turn off the power to the product during startup, restart, or initialization.
- Doing so may cause the product to stop operating normally.
- This product is intended for installation by a trained person. Ensure that the product complies with local electrical and safety regulations.
- The power cord for this equipment must be connected to an electrical outlet with a ground connection.
- This product is intended to be supplied by a UL-certified power supply. Contact your retailer for more information.

1. Federal Communication Commission Interference Statement

This device complies with Part 15 of 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.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CAUTION

Any changes or modifications not expressly approved by the party responsible for compliance could avoid the electromagnetic compatibility (EMC) and wireless compliance and negate your authority to operate the product.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

FOR MOBILE DEVICE USAGE (>20cm/low power)

Radiation Exposure Statement

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

FOR COUNTRY CODE SELECTION USAGE (WLAN DEVICES)

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

KDB 996369 D03 OEM Manual v01 rule sections:

List of applicable FCC rules

This module has been tested for compliance to FCC Part 15.247, 15.407

Summarize the specific operational use conditions

The module is tested for standalone mobile RF exposure use condition. Any other usage conditions such as co-location with other transmitter(s) or being used in a portable condition will need a separate reassessment through a class II permissive change application or new certification.

For 6ID (Low-power indoor access points)

This module is authorized for use in a Low-power Indoor Access Point (6ID) device. The final host

product must comply with the following operational restrictions:

a) Must be limited to indoor locations, have an integrated antenna, and cannot use a weatherized enclosure.

b) Must be powered by a wired connection and not by battery power, except for battery backup only during power outages.

c) The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet in the 5.925-6.425GHz band.

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

For 6XD (Indoor Client)

This module is authorized for Indoor Client (6XD) device applications under the control of a low-power indoor access point or subordinate.

The final host product must comply with the following operational restrictions:

a) Must be limited to indoor locations only;

b) Cannot connect directly to any other client device;

c) Cannot source internet/network (obtained via wired connection or other means such as cellular) to other clients, access points and subordinate devices, or provide any direct peer to peer connections to other clients or subordinates;

d) Is prohibited for control of or communications with unmanned aircraft systems.

Limited module procedures

Not applicable.

Trace antenna designs

Not applicable.

RF exposure considerations

This equipment complies with FCC mobile radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator & your body. If the module is installed in a portable host, a separate SAR evaluation is required to confirm compliance with relevant FCC portable RF exposure rules.

Antennas

The following antennas have been certified for use with this module; antennas of the same type with equal or lower gain may also be used with this module, except as described below. The antenna must be installed such that 20 cm can be maintained between the antenna and users.

For 6ID, 6XD,:

Demonstration of compliance to Contention-Based Protocol requirements across U-NII-5/6/7/8 bands has been determined using a lowest antenna gain of 2.7 dBi. The use of antennas with gain lower than this will require a separate Class II permissive change re-evaluation or new certification.

Antenna model	Antenna Type	Antenna Gain (dBi)		
		2.4GHz	5GHz	6GHz
FXE5000-ANT	CHIP	2.0dBi	1.5dBi	2.7dBi
FX-ANT-A14	CHIP	3.80dBi	3.63dBi	3.97dBi

Label and compliance information

The final end product must be labeled in a visible area with the following: "Contains FCC ID: PQRFXE5000-US". The grantee's FCC ID can be used only when all FCC compliance requirements are met.

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module.

The end product user manual shall include all required regulatory information/warning as shown in this manual.

Information on test modes and additional testing requirements

This transmitter is tested in a standalone mobile RF exposure condition and any co-located or simultaneous transmission with other transmitter(s) or portable use will require a separate class II permissive change re-evaluation or new certification.

Additional testing, Part 15 Subpart B disclaimer

This transmitter module is tested as a subsystem and its certification does not cover the FCC Part 15 Subpart B (unintentional radiator) rule requirement applicable to the final host. The final host will still need to be reassessed for compliance to this portion of rule requirements if applicable.

OEM/Host manufacturers are ultimately responsible for the compliance of the Host and Module. The final product must be reassessed against all the essential requirements of the FCC rule such as FCC Part 15 Subpart B before it can be placed on the US market. This includes reassessing the transmitter module for compliance with the Radio and EMF essential requirements of the FCC rules. This module must not be incorporated into any other device or system without retesting for compliance as multi-radio and combined equipment.

As long as all conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed.

Note EMI Considerations

Please follow the guidance provided for host manufacturers in KDB publications 996369 D02 and D04.

How to make changes

Only Grantees are permitted to make permissive changes. Please contact us should the host integrator expect the module to be used differently than as granted:

CONTEC CO,. LTD. https:/www.contec.com

IMPORTANT NOTE: In the event that these conditions cannot be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID cannot be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

For 6ID (Low-power indoor access points)

a. FCC regulations restrict the operation of this device to indoor use only.

b. The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet in the 5.925-6.425 GHz band.

c. Transmitters in the 5.925-7.125 GHz band are prohibited from operating to control or communicate with unmanned aircraft systems.

For 6XD (Indoor Client)

Transmitters in the 5.925-7.125 GHz band are prohibited from operating to control or communicate with unmanned aircraft systems.

3.Precaution on use

It is prohibited to modify the inside of this product. The product cannot be used in any country other than those authorized for use.

If the 6 GHz band is used with a bandwidth of 20 MHz or 40 MHz, the transmission power will be low.

4. Usage limitation

This product has not been developed or manufactured to be used in systems including the equipment which is directly related to human lives *1 or the equipment which involves human safety and may significantly affect the maintenance of public functions *2. Therefore, do not use the product for such purposes.

*1: Medical devices such as life-support equipment and devices used in an operating theater.

*2: Main control systems at nuclear power stations, safety maintenance systems at nuclear facilities, other important safety-related systems, operation control systems within group transport systems, air-traffic control systems, etc.

5.Supported Wireless LAN Standards

This product conforms to IEEE802.11ax/ac/n/a (W52/W53/W56/W58)/b/g.

This product supports the following 5 GHz /6 GHz band channels.

W52(5.2GHz Band 36, 40, 44, 48ch)

W53(5.3GHz Band 52, 56, 60, 64ch)

W56(5.6GHz Band 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144ch)

W58(5.8GHz Band 149, 153, 157, 161, 165ch)

6 GHz band(1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93ch)

When using the W53 and W56, the access point is subject to the following restrictions by law.

- After starting, the channel is checked for radar waves for one minute, so at a minimum, one minute or longer is required.
- If radar waves are detected during startup or while started, the access point may start on another channel since it must use a channel different from the set channel.

⚠ CAUTION

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

6.Security Precautions

Wireless LAN uses radio waves instead of LAN cables to send and receive data between a computer and a wireless access point, making it possible to freely establish a LAN connection within a range of the radio waves. However, radio waves can be received through obstacles, such as walls, when within the range. Therefore, if security settings are not made, the following problems may occur.

Unauthorized viewing of data

An unauthorized third party can intercept the radio waves and view e-mail messages and personal information, such as user ID and password or your credit card information.

Unauthorized access

An unauthorized third party can access a personal or corporate network and cause the following damage:

Intercepting personal information and confidential information (information leak)

Using a false identity to communicate and disclose information illegally (identity theft)

Changing and transmitting intercepted data (tampering)

Damaging data and systems by spreading a computer virus (destruction)

The wireless LAN card and wireless access point have security features to counter these problems. Using the security settings of the wireless LAN equipment can help prevent these problems from occurring. The security settings of the wireless LAN equipment are not configured at the time of purchase.

To reduce security problems, configure all security settings of the wireless LAN equipment according to the manual before using the wireless LAN card and wireless access point. Please be aware that the security settings do not provide complete security protection due to wireless LAN specifications. If you are unable to configure the security settings yourself, please contact your local authorized dealer. The customer is responsible for configuring the security settings and understanding the risks inherent in using the product without the security settings configured.

7.Environment

Use this product in the following environment. If used in an unauthorized environment, the board may overheat, malfunction, or cause a failure.

Operating temperature

DC input (without wind) : -20 - +40°C

DC input (with air flow 0.6m/s) : -20 - +50°C

Humidity

10 - 90%RH (No condensation)

Corrosive gases

None

Floating dust particles

Not to be excessive

8. Inspection

Inspect the product periodically to use it safely.

9.Storage

When storing this product, keep it in its original packing form.

- Put this product in the storage bag.
- Wrap it in the packing material, and then put it in the box.
- Store the package at room temperature at a place free from direct sunlight, moisture, shock, vibration, magnetism, and static electricity.

10. Disposal

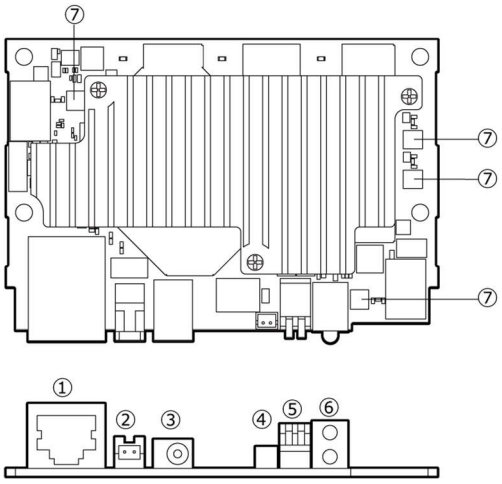
When disposing of the product, follow the disposal procedures stipulated under the relevant laws and municipal ordinances.

Product Nomenclature and Function

This section describes product component names and their functions, pin assignment of each connector.

1.Nomenclature of Product Components

Component names of the product are shown in the figure below.



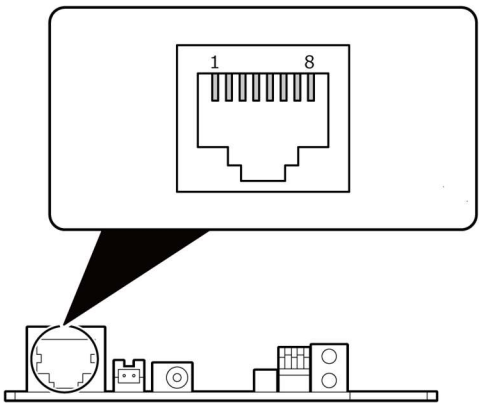
No.	Title	Function
1	LAN port	Connect the LAN cable to the PC.
2	Power connector	Connect this to the power connector when supplying power from an external source.
3	DC JACK	This is the jack for DC power.
4	INIT Connector	This connector is used to initialize the unit.
5	DIP Switch	This switch is used to initialize the unit.
6	LED display	This is an LED that indicates the status of the unit.
7	Antenna connector	This is a connector for an antenna. J2 is antenna 1, and J4 is antenna 2.

2.Description of Product Components

Components such as connectors, switches are described.

1. LAN port

This product has 1 Ethernet ports.

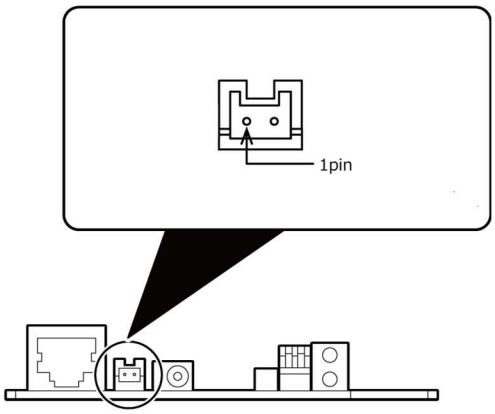


Pin assignment

No.	Sign	Contents
1	TRD+(0)	Positive side of data pair 0 / Alternative A type positive PoE supply
2	TRD-(0)	Negative side of data pair 0 / Alternative A type positive PoE supply
3	TRD+(1)	Positive side of data pair 1 / Alternative A type negative PoE supply
4	TRD+(2)	Positive side of data pair 2 / Alternative B type positive PoE supply
5	TRD-(2)	Negative side of data pair 2 / Alternative B type positive PoE supply
6	TRD-(1)	Negative side of data pair 1 / Alternative A type negative PoE supply
7	TRD+(3)	Positive side of data pair 3 / Alternative B type negative PoE supply
8	TRD-(3)	Negative side of data pair 3 / Alternative B type negative PoE supply

2. Power connector

Connect to an external power source using a 3-pin connector.

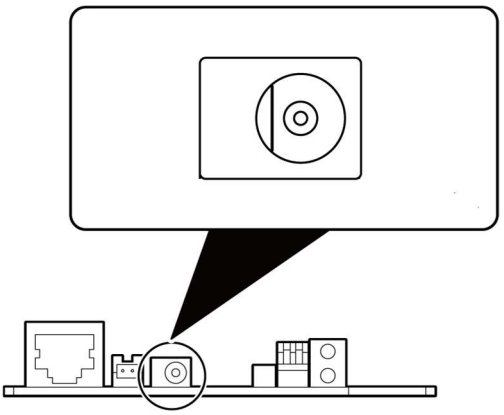


Pin assignment

Pin No.	Signal name	Operation / Function
1	Vi+	5-30VDC±5%
2	Vi-	GND

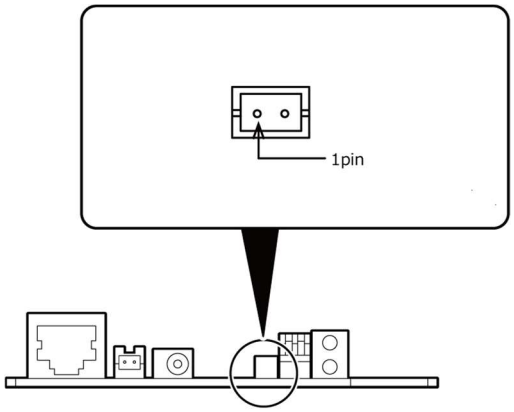
3. DC JACK

DC power jack. Use this jack with an optional AC adaptor.



Pin	Sign
Center	Input power
Periphery	GND

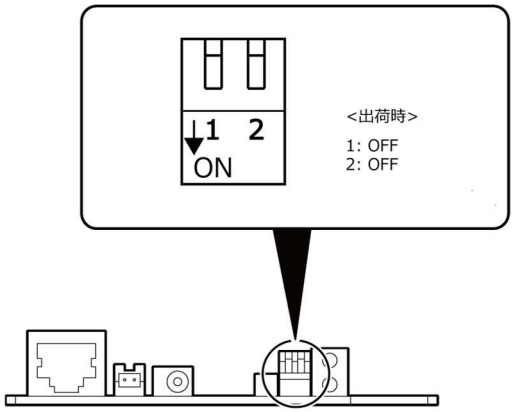
4. INIT Connector



No.	Item	Function
1	INIT	When the INIT signal is short-circuited with GND, the POWER, WLAN, and LAN LEDs will flash and light up (approximately 3 seconds), the INIT signal will be opened to return to the factory settings after the next startup.
2	GND	GND

- When initializing the product by turning the INIT signal on and off, the LEDs will continue flashing for a short time after the signal is turned off. This indicates the internal memory files are being deleted. If the power is turned off while the LEDs are flashing, the internal memory files may be damaged and the product may no longer be able to start properly. Always restart the product after the LEDs stop flashing.

5. DIP Switch

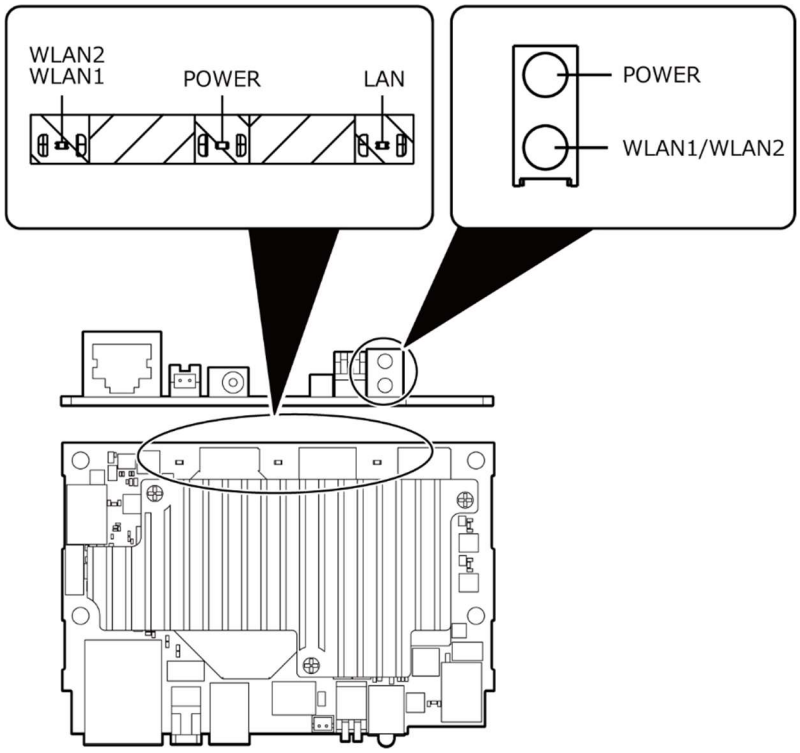


No.	Item	Function
1	INIT	Use this switch to initialize the unit (restore the factory settings). When the DIP switch is turned on, the POWER, WLAN, and LAN LEDs will start flashing. If you turn this switch off during the period from flashing to lighting (approximately three seconds), all settings of the unit will return to the factory settings the next time you start the unit.
2	-	Unused

- When initializing by turning the DIP switch ON or OFF, the flashing continues for a while after the switch is turned OFF. This indicates that a file in the internal memory is being deleted. If you turn off the power before the flashing stops, the file in the internal memory may be corrupted and the machine may not start normally. Be sure to restart after the flashing stops.
- Do not turn off the machine during startup, restart, or initialization. Doing so may cause the machine to stop operating normally.

6. LED Indicator

Status of the product is indicated by ON/OFF and flashing of LED.



Display colors and their meanings

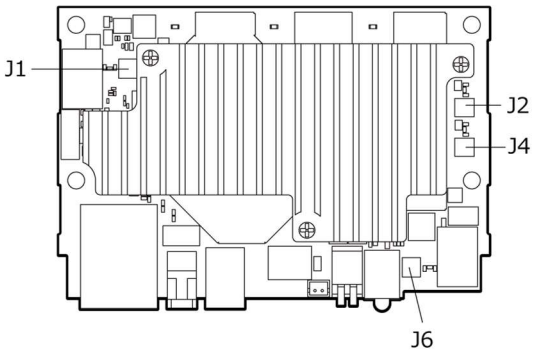
LED name		Color	Status	Indicator
POWER ※1		Blue	ON	Indicates that the device is operating.
			Flashing (Interval)	Indicates that the device is being started (This device turned on)
			OFF	Power has not been supplied.
LAN		Green	ON	Indicates that a wired LAN connection.
			Flashing	Indicates data is being transmitted and received over a wired LAN.
			OFF	Indicates that a wired LAN is not connected.
WLAN	WLAN1 (2.4GHz interface)	Blue	ON	Indicates that wireless LAN1 (2.4 GHz) is connected.
			Flashing	Indicates data is being transmitted to or received from the device connected through wireless LAN1 (2.4GHz).
			OFF	Indicates that wireless LAN1 (2.4 GHz) is not connected.
	WLAN2 (5GHz interface)	Green	ON	Indicates that wireless LAN2 (5 GHz/6 GHz) is connected.
			Flashing	Indicates data is being transmitted to or received from the device connected through wireless LAN2 (5GHz/6 GHz).
			Flashing (Interval)	Indicates that the radar wave is being checked. (When using W53, W56)
			OFF	Indicates that wireless LAN2 (5 GHz/6 GHz) is not connected.
POWER/ LAN/		Blue/Green/	Flashing	Indicates that a file is being written.

LED name	Color	Status	Indicator
WLAN1/WLAN2	Blue/Green	(simultaneously)	
POWER/LAN	Blue/Green	Blinking twice /On	DHCP error

※1 The POWER LED on the side of the unit lights and flashes green.

7. Antenna connector

Connector for antenna.



3.DFS function

When set to DFS-supported channels (5 GHz only), if radar waves are detected, the channel must be changed in order to avoid radio wave interference with weather radars and other radars, so note the following.

DFS-enabled channel (frequency: 5 GHz)

Channel	DFS capability
W52 : 36, 40, 44, 48	Disabled
W53 : 52, 56, 60, 64	Enabled
W56 : 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144	Enabled
W58 : 149, 153, 157, 161, 165	Disabled

* The DFS function applies to W53 and W56. The DFS function does not apply to W52 and W58 because the DFS function is not required.

⚠ CAUTION

- After starting, the channel is checked for radar waves for one minute, so at a minimum, one minute or longer is required.
- If radar waves are detected during startup or while started, the access point may start on another channel since it must use a channel different from the set channel.
- Even after starting with the set DFS-supported channel, the channel may change while running.
- If radar waves are detected, the radio waves must stop for 30 minutes, so the detected channel cannot be used for 30 minutes.

Setting Up

This section describes how to set up the product.

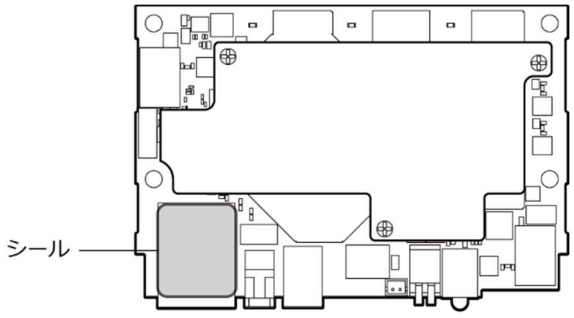
1.Checking the Network Addresses

This product requires a PC connected to the network for configuration via the network. Connect the PC to be configured to the network and configure the settings using a web browser.

The Ethernet (wired LAN), wireless LAN MAC address and IP address are defined on the housing sticker on the side of this product. Write down the MAC addresses for Ethernet and wireless LAN in the following table as they are device-individual values and may be required for future setup.

Network Address

Description on the housing sticker	Explanation	Address
IP:	Default IP Address	192.168.0.1
LAN MAC:	LAN MAC Address	
2.4GHz MAC:	2.4GHz Wireless LAN MAC Address	
5GHz MAC:	5GHz Wireless LAN MAC Address	



2.Power Supply

This product is powered by the following methods.

1. Using the DC JACK

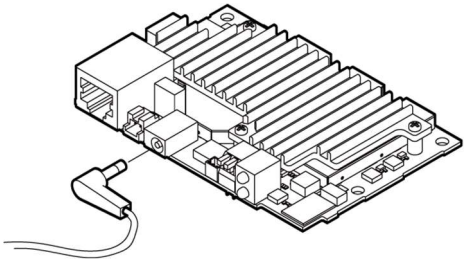
The power plug to be used must conform to EIAJ voltage classification 2.

⚠CAUTION

When supplying power through the DC jack, do not use it together with supplying power from the power connector.

2. When using the AC adapter (FX-AC053)

Connect the DC plug of the AC adaptor to the DC jack of the machine.



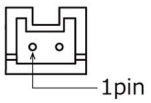
*Since FX-AC053 is a product for Japan, it may not be usable outside of Japan.

⚠CAUTION

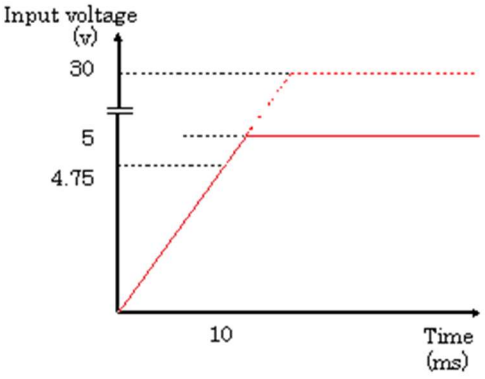
When supplying power through the AC adaptor, do not use it together with supplying power from the power connector.

3. Using the Power connector

Power can be externally supplied using the power connector. Use the components indicated to the followings for the power cable or use equivalent components.

Function			
Power connector: S02B-PASK-2(LF)(SN) [JST] Cable: AWG28-16(on the condition that the cable length satisfies the power specifications)			
Pin No.	**Signal name**	**Meaning**	
1	Vi+	Power supply (5 to 30 VDC ±5%)	
2	Vi-	Power supply (GND)	

Power Supply Time



⚠ CAUTION

- Carefully manufacture the power cable taking care not to mistake the wiring. In particular, if the power cable is used with mistaken housing pin numbers, there is a risk of malfunction or accidents.
- The input voltage range of this product is 5 - 30VDC±5%. Powering the product with anything other than that may cause equipment failure or accidents.
- Use a power supply that rises to an input voltage range of 4.75 VDC or higher within 10 ms. Power supply that does not meet those conditions may cause equipment failure or accidents.

3.Installation

Connection to Devices and Setup Methods

This product is set up via a network using a Web browser. Follow the setup procedure below once the product is set up.

1.Preparation before Setup

You must use a PC which can be connected to a network as the product is set up via the network.
The setup is performed by connecting a PC for setup purposes and then using a Web browser.

1. Connecting for the first time

1 Connect this product to PC on a wired LAN.

2 Select an IP address 192.168.0.XXX (e.g. 192.168.0.10) for the PC, which is not the same address as for this product. And then set the subnet mask to 255.255.255.0
*** The default setting IP address is 192.168.0.1.**

The following example settings are for Windows 11 or Windows 10 using Microsoft Edge.

◆ Windows 11 / Windows 10

1 Click [Start] (the Windows logo button), and then click [Control Panel], [Network and Internet], [Network and Sharing Center], then [Change adapter settings]. Then, right-click the Ethernet icon, and then click [Properties].

2 If a User Account Control window appears, click "Yes" or "Continue".

3 Select the "Internet Protocol Version 4 (TCP/IPv4)" check box, and click "Properties".

4 In the "Use the following IP address" field, type an IP address 192.168.0.XXX, which is not the same address as this product (e.g. 192.168.0.10), and then set the subnet mask to 255.255.255.0.

5 Click "OK", and then click "OK" or "Close" to enable the settings.

2. Changing the settings

1 Connect this product to PC on a wired LAN.

2 Set the network address of the PC to the same network address as for this product.

2.Setup Using a Web Browser

Start up a Web browser and enter the IP address of this product after “http://” in the address bar. If connecting for the first time, enter the default IP address. When the default setting IP address is 192.168.0.1, enter as follows.

http://192.168.0.1/

Enable the JavaScript function in the browser setting as it is used.

Recommended web browsers

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

1. Setting the Browser

You may have to change the browser settings as well as the IP address and subnet mask for the PC to be connected to this product via the network.

◆ Changing browser settings

(1) Proxy Settings

Networks at companies and schools may use browsers with proxy settings. Proxy is not required as a PC is used to set up the product, which is on a local network. Disable the proxy settings temporarily when setting up this product on a Web browser.
The following example settings are for Microsoft Edge, Google Chrome, or Mozilla Firefox.
Actual settings will depend upon the environment you are using. For details, see your web browser's help information or contact the software manufacturer.

Microsoft Edge or Google Chrome

1. Right-click [Start] (the Windows logo button), and then click [Network & Internet].
2. Click [Proxy], and then turn off "Use a proxy server".

Mozilla Firefox

1. Launch Mozilla Firefox.
2. From the menu bar, click [Tools] - [Options].
3. Click [Advanced], open the [Network] tab, and then click [Settings].
4. Select "No proxy", and then click "OK".
5. Click "OK" button.

(2) Enable JavaScript.

The following example settings are for Microsoft Edge, Google Chrome, or Mozilla Firefox.
Actual settings will depend upon the environment you are using. For details, see your web browser's help information or contact the software manufacturer.

Microsoft Edge

1. Launch Microsoft Edge.
2. Click [...] in the upper right corner of the screen to access the Menu tab, and then click [Settings].
3. Click [Site permissions], and then click [JavaScript].
4. Turn on "Allow (recommended)".

Google Chrome

1. Launch Google Chrome.
2. Click [...] in the upper right corner of the screen to access the Menu tab, and then click [Settings].
3. Click [Security and Privacy], and then click [Site settings].
4. Click [JavaScript], and then Turn on "Allow (recommended)".

Mozilla Firefox

1. Launch Mozilla Firefox.
2. From the menu bar, click [Tools] - [Options].
3. Click [Contents], and then select "Enable JavaScript" to turn on JavaScript.
4. Click [OK] to enable the settings.

⚠ CAUTION

When the Web browser settings have been changed, restore the original browser settings upon the completion of setup of this product.

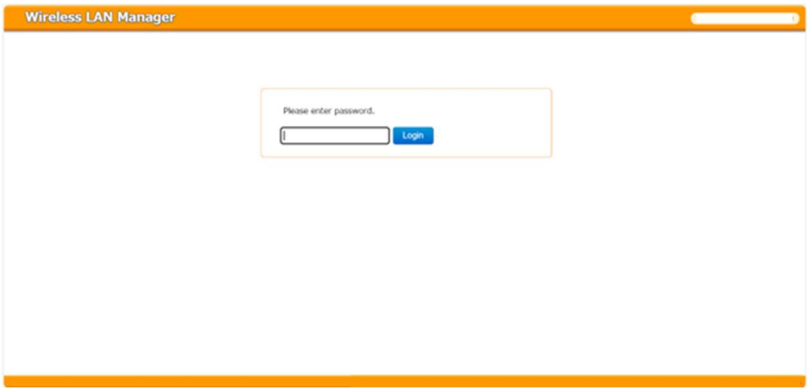
2. Connecting to This Product Using Web Browser

When you connect to this product using a web browser, the login screen will be displayed.

If it does not appear, one or more of the following may be incorrect: the PC's IP address settings, the browser settings, or the URL entered in the browser's address bar.

Enter your password on the login screen, then click the "Login" button to log in.

The password is set to "pass" by default.



⚠ CAUTION

Please change the password from the factory defaults to avoid possible security issues.

For details on how to change the password, please refer to " **Setup and Status Display** " > "**4. Maintenance** " > " **Password** ".

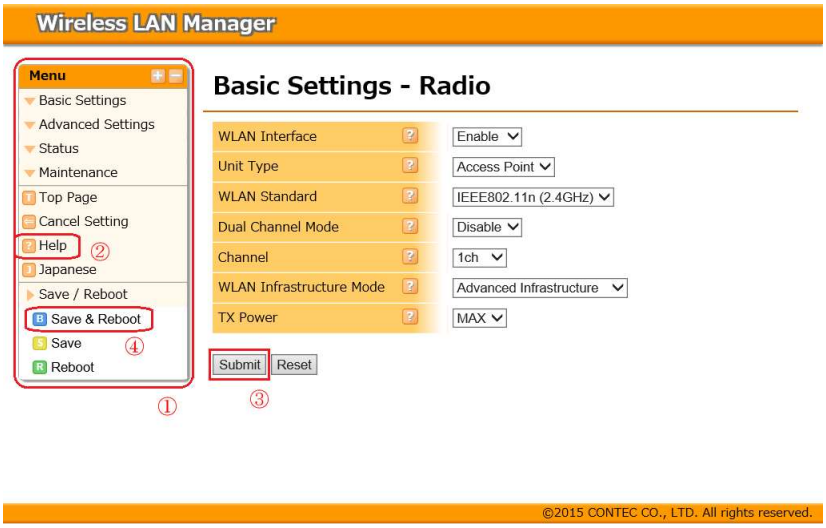
3. Configuring Settings from a Web Browser

Select [Basic Settings] on the menu on the left side of the screen ((1) in the following figure), and then select the setting item in the menu that opens.

For details on the setting items, refer to the [Help] ((2) in the following figure).

The settings must be temporarily recorded on this product, so, after changing the settings on each page, be sure to click [Submit] ((3) in the following figure).

After you have configured all the settings, save them and restart this product to enable the settings. Click [Save & Reboot] ((4) in the following figure) on the menu on the left side of the screen.



There will be no problem if you just save the settings now but reboot the product later when necessary. In this case, saving the settings does not actually change the settings of the product. Therefore, make sure to reboot the product later.

* For explanations of functions and setting instructions, see the manual available from the CONTEC website or see help information.

⚠ CAUTION

Saving the settings takes about 5 to 10 seconds. During this time, all LEDs flash. Do not restart or turn off the power until "Save complete" appears on the display. If you restart or turn off the power while the settings are being saved, the settings files and firmware may be corrupted, resulting in the inability to start up normally.

Do not turn off the power to the machine during startup, restart, or initialization. Doing so may cause the machine to stop operating normally.

Setup and Status Display

This chapter describes how to explains each setting item and status display, IEEE802.1X supplicant setting. Always read **"Setting U"** and **"Connection to Devices and Setup Method"** for preparation before performing setup or viewing the status.

1.Basic Settings

The "Basic Settings" are the minimal required settings for using this device as wireless networking equipment.

Other customized settings can be configured in "Advanced Settings".

In the setting to input a character string, a space cannot be used as the first character. Also, the following 4 types of symbols cannot be used.

' (single quote)

" (double quote)

` (backquote)

¥ (backslash)

1. System

DHCP Client

To set the IP address of the device using the DHCP client function, set to "Enable".

To specify the IP address of the device, set to "Disable".

When set to "Disable", the address configured by "IP Address" is the IP address for the device.

Default Setting : Disable

IP Address

Set the IP address for the device.

This setting is valid when "DHCP Client" is set to "Disable".

Default Setting : 192.168.0.1

Subnet Mask

Set the subnet mask for the device.

This setting is valid when "DHCP Client" is set to "Disable".

Default Setting : 255.255.255.0

Default Gateway

Set the IP address of the default gateway for the device.

This setting is valid when "DHCP Client" is set to "Disable".

Default Setting : 0.0.0.0

Language

Set the language to display the "Wireless LAN Manager" configuration web page.

You can select from "Auto", "Japanese" and "English".

This setting is reflected immediately when you press the "Change" button.

Default Setting : Auto

Time Zone

Set the time zone for the device.

Default Setting : North America: Eastern Standard Time (EST+5)

2. Radio

Operation Mode

Select the operation mode of this device. There are five modes of operation: "Access Point", "Repeater", "Single Station", "Dual Station" and "Mesh".

Default Setting : Single Station

Item	Description
Access Point	A master device to which wireless client devices connect. One or more VAPs operate as an access point.
Repeater	VAP1 operates as a station, and VAP2 and later operate as an access point. Multiple VAPs can be configured to operate as an access point.
Single Station	It operates as a station (client) with only one VAP using either the 5GHz interface or the 2.4GHz interface. A single station can only connect to either 5GHz or 2.4GHz wireless networks.
Dual Station	It operates as a station (client) using VAP1 as a 5GHz interface and VAP2 as a 2.4GHz interface. A dual station can connect to both 5GHz or 2.4GHz wireless networks simultaneously. VAP1 is fixed to 5GHz interface, VAP2 is fixed to 2.4GHz interface, VAP1 and VAP2 should be set to the same "WLAN Infrastructure Mode". Packets communicating between VAP1 and VAP2 are not bridged, so communication between the VAP1 network and the VAP2 network is not possible.
Mesh	It automatically builds and operates a mesh network consisting of one controller and multiple agents.

To build a mesh network

(1) First, configure the controller device to act as a mesh controller in the “Wireless Common” settings, then configure VAP3 and VAP4 as the fronthaul to which the stations will connect. After completing the settings, save and reboot.
(2) After rebooting, the backhaul for communication between the controller and agent is automatically created as VAP1 and VAP2.
(3) Connect to the device that will be the agent via a wired LAN connection. Configure it to operate as a mesh agent in the “wireless common” setting, and set VAP1 to wirelessly connect to the controller's front hall (VAP3 or VAP4). Save and reboot after configuration.
* If you want the agent to be a wired backhaul agent, wireless configuration is not required. Ensure that the agent can communicate over a wired LAN to the controller.
(4) After reboot, the agent connected wirelessly to the controller will automatically create fronthaul and backhaul VAPs and act as a mesh agent. It will take 3-5 minutes for all automatic settings to complete.
(5) When adding agents to the mesh network, perform step 3.

Mesh Type

When "Mesh" is selected for the operation mode, set the mesh device type to one of the items in the table below.

Default Setting : Agent

Item	Description
Controller	A device that controls agents as the core of the mesh network. Only one controller should be on the mesh network.
Agent	A device connected to a mesh network, whose settings are controlled by a controller. Agents connect to the controller or other agents via wireless or wired LAN.
Controller Backup	Select this if you want the device to be a backup for the controller for mesh network redundancy. When setting it as a backup, install only one device on the mesh network. Please also set his IP address and login password for the controller that will operate as the main machine. It automatically copies settings, monitors whether the controller is alive, and operates as a controller when it determines that it is not working. If you have changed the operation mode or mesh type settings when operating as a controller, the settings will be forced back to the startup settings.

Target Device IP Address

When the mesh type is set to "Controller Backup", set the IP address of the controller to be backed up.

Default Setting : (None)

Target Device Password

When the mesh type is set to "Controller Backup", set the login password for the controller to be backed up.

Default Setting : (None)

Link Down Detection for Mesh

When the mesh type is set to "Controller" or "Controller Backup", you can set whether to use "Link Down Detection".

Default Setting : Disable

Primary Interface

Set whether the station gives priority to the 2.4GHz interface or the 5GHz interface when "Dual Station" is selected in the operation mode.

Default Setting : 5GHz/6GHz

Repeater Independent

When you select "Repeater" for the operation mode, set whether VAPs that operate as an access point in wireless mode operate independently on the same wireless interface (2.4GHz, 5GHz).

When "Disabled", the VAP configured on the access point will work with a station (VAP1) and will operate when the station connects to the wireless LAN access point.

When "Enabled", the VAP configured on the access point will operate regardless of whether the station (VAP1) is connected to a wireless LAN or not. When the station is not connected to the

wireless LAN, the VAP configured on the access point will start on the configured channel, but please note that after the station establishes a wireless connection, the channel will change to that of the connected access point.

Default Setting : Disable

WLAN Interface

This device has a 2.4GHz interface and a 5GHz interface. Both are normally enabled, but it is also possible to disable each interface.

When set to "Disable", the wireless LAN interface cannot be used.

Default Setting : Enable

WLAN Standard

Select the wireless networking standard to use on the device.

Default Setting : IEEE802.11ax

Band Width

This setting can only be configured when the WLAN Standard is IEEE802.11n/ac/ax.

To set the wireless networking bandwidth to 20MHz or 40MHz.

Default Setting : 20MHz

Band

This setting can only be configured when the WLAN Standard is IEEE802.11a/ax.

When the operation mode is "Access Point", "Repeater", or "Mesh", it is fixed to "5GHz". (This model, which has replaceable antennas, cannot use 6GHz channels due to legal restrictions.)

When the operation mode is "Single Station" or "Dual Station", you can select from "5GHz", "6GHz", and "5+6GHz".

Default Setting5+6GHz

Channel

This setting is available when the unit type is "Access Point" or "Repeater", "Mesh" (Agent).

Select the channels to use for the 2.4GHz and 5GHz interfaces. The available channels vary depending on the wireless LAN standard and operation mode.

When the operation mode is "Mesh", If there is a possibility of radar detection, it is better not to set it as a DFS channel. This is because it interferes with wireless communication when radar is detected.

Default Setting : 1ch / 36ch

TX Power

Select the transmit power.

You can select either "MAX, "50%", "25%", or "12%".

Default Setting : MAX

Antenna Selection

This setting can only be configured when the wireless networking standard is IEEE802.11a/b/g.

Select the antenna mode as "Auto" or "Fixed".

This setting is not normally required. Select "Fixed" when using only one external antenna.

Default Setting : Auto

3. VAP

◆ VAP Settings

VAP Interface

By setting it to "Disable", VAP will be in a state of stopping without VAP operation.

Default Setting : Enable

WLAN Interface

Set whether to bind the VAP to the 5GHz interface or the 2.4GHz interface.

Default Setting : 2.4GHz

WLAN Mode

This is the setting for whether the VAP operates as an access point or a station. It cannot be changed because it is determined by "Operation Mode" in the Radio settings.

Default Setting : Single Station

WLAN Infrastructure Mode

Select the operation mode for the device. There are three types of operation modes: "Standard Infrastructure", "Compatible Infrastructure", and "Advanced Infrastructure".

When the unit type is station, "Advanced Infrastructure" cannot be selected.

Default Setting : Compatible Infrastructure

Item	Description
Standard Infrastructure	A configuration where a standard infrastructure access point is the core and stations (wireless networking cards, etc.) are located under it. (Infrastructure) With standard infrastructure, the device can use its own wireless networking feature.
Compatible Infrastructure	A configuration where a compatible infrastructure access point is the core and stations (wireless networking cards, etc.) are located under it. (Infrastructure) The device cannot use its own wireless networking feature.
Advanced Infrastructure	A mixed mode of both modes where the device can use an advanced infrastructure access point as standard infrastructure while also using compatible infrastructure at the same time.

WDS

Enabling the WDS setting allows wireless connection and wireless communication between WDS-enabled access points/stations. By using WDS, it becomes possible to connect and communicate with multiple devices under the wired LAN of the station.

Default Setting : Disable

ESSID

Set the ESSID for the device as alphanumeric characters between 2 and 32 characters in length. Spaces are not allowed.

The ESSID for VAP1 must be set.

When the unit type is "Access Point", by setting the ESSID of each VAP, the VAP (Virtual AP) is enabled. When setting the ESSIDs for multiple VAPs, ensure that the ESSID values are not already in use.

When the unit type is "Station", the VAP1 settings are required.

When the unit type is "Repeater", set the ESSID for VAP1 and VAP2. Due to the characteristics of the repeater, normally set the ESSID for VAP1 and VAP2 to the same setting.

Default Setting : LocalGroup

◆ Encryption Settings

Encryption

Select the encryption to use with wireless networking.

Further settings that must be configured are displayed depending on the selected setting, so configure the displayed settings.

Default Setting : Disable

⚠ CAUTION

WEP and TKIP cannot be used with IEEE802.11ax/ac/n due to the rules of the standard.

WEP or TKIP can be used only when the operation mode is "Access Point", but it operates with IEEE802.11a/b/g.

WSL

The setting that selects whether or not to encrypt wireless data with our proprietary encryption (WSL). Note that communication between a terminal with the WSL feature enabled and a terminal with the WSL feature disabled is not possible. This device can only use WSL (Type 2) that utilizes the new algorithm.

The WSL key setting is only valid when the WSL feature is enabled. Note that communication between terminals with different WSL keys is not possible.

Enter the WSL key as a 20 digits hexadecimal value (0 to 9, a to f or A to F).

Default Setting : Disable, (Blank)

◆ Fixed Key Settings

Default Key

This setting is only available when the encryption is set to either "WEP(Open)" or "WEP(SharedKey)".

Select the key to use as "Fixed Key 1" to "Fixed Key 4".

Default Setting : Fixed Key 1

Fixed Key

This setting is only available when the encryption is set to either "WEP(Open)" or "WEP(SharedKey)".

Set the fixed key.

The fixed keys are a common setting for the VAPs. The fixed keys are displayed in the settings for each VAP, but if the setting is changed, the change is reflected in the fixed keys for the other VAPs.

Default Setting : (Blank)

◆ WPA Settings

Group Key Updating Interval (sec)

When the encryption is set to "WPA", "WPA2", "WPA3", "WPA-PSK", "WPA2-PSK" or "WPA3-SAE", set the group key updating interval in seconds.

This setting can be configured as 0 (disabled) or between 120 (2 minutes) and 259200 (3 days).

When set to 0, the setting is disabled and group key renewal is not performed.

Default Setting : 3600

◆ PSK Settings

WPA Pre-Shared Key (PSK)

When the encryption is set to "WPA-PSK" or "WPA2-PSK", set the WPA encryption key (PSK: pre-shared key) to use for encryption.

Enter the value as alphanumeric characters between 8 and 63 characters or 64 hexadecimal digits.

Default Setting : (Blank)

◆ SAE Settings

SAE Password

When the encryption is set to "WPA3-SAE", set the SAE password to use for encryption.

Enter the value as alphanumeric characters between 8 and 63 characters or 64 hexadecimal digits.

Default Setting : (Blank)

◆ MAC Address Authentication

MAC Address Authentication

Please set to "Enable" if you want to use the MAC address authentication using external RADIUS server.

You will also need to set the RADIUS server.

Default Setting : Disable

◆ Authentication Settings (AP)

Reauth Period (sec)

Set the interval for reauthentication in seconds.

This setting can be configured as 0 (disabled) or between 120 (2 minutes) and 259200 (3 days).

When set to 0, the setting is disabled and reauthentication is not performed.

Default Setting0 : (Disabled)

Server IP Address

Set the IP address for the RADIUS server.

Default Setting : (Blank)

Server Port

Set the port number for the RADIUS server. Port 1812 is most commonly used.

Default Setting : (Blank)

Shared Secret

Set the shared secret for the RADIUS server as alphanumeric characters between 1 and 64 characters in length.

Default Setting : (Blank)

◆ Authentication Settings (Client)

Authentication Type

Set the RADIUS authentication type to either "PEAP" or "EAP-TLS".

When "PEAP", you must register a server certificate with "Certificate Registration".

When "EAP-TLS", you must register the server certificate, client certificate, and private key with "Certificate Registration".

Default Setting : PEAP

User Name

Set the authentication user name for RADIUS authentication as alphanumeric characters with a maximum length of 32 characters.

Default Setting : (Blank)

User Password

Set the authentication password for RADIUS authentication as alphanumeric characters with a maximum length of 32 characters.

Default Setting : (Blank)

Certificate Registration

Register (upload) the certificates required for RADIUS authentication.

When you click the button to register certificates, the certificate registration frame will open. Browse to a file in that frame and upload the certificate to the device with the "Upload" button.

Next to the button to open the certificate registration frame is a message that indicates whether or not that certificate has been registered. When the certificate is registered, "Registered" is displayed. When not registered, "Not Registered" is displayed.

Default Setting : (Not Registered)

2.Advanced Settings

1. System

Device Name

Set the address for the name of this device as alphanumeric characters with a maximum length of 31 characters.

It is okay to leave this value blank.

Default Setting : (Blank)

Roaming Notification Bridge

To bridge the roaming notification received by the wired LAN to wireless LAN, set to "Enable".

Default Setting : Enable

Turn off all LEDs

By enabling this setting, turn off all LEDs after the start of this equipment.
 However, When the firmware update and save settings, LEDs blink.

Default Setting : Disable

◆ Access Security

HTTP Server

To use the HTTP Server (Port 80/443), set to "Enable".

Default Setting : Enable

FTP Server

To use the FTP Server, set to "Enable".

Default Setting : Enable

Wireless Access

By setting to disable this feature, you can deny access to HTTP and FTP via wireless LAN, and allow access only via ethernet.

Default Setting : Enable

Allowed IP Address Function

If you want to use the function to specify the IP addresses that can access the HTTP or FTP, set to "Enable".

Default Setting : Disable

Allowed IP Address

When the "Enable" allowed IP address function, specify the IP addresses that are allowed to access.

You can specify the IP address to specify a range, or only one.

If you specify only one, enter the IP address only in the left form of the allowed IP address 1/2.

If you specify only one, enter the start IP address in the left form of the allowed IP address 1/2, and enter the end IP address in the right form.

Please note that because if you've set the IP address that is not intended, you may become not be able to access this equipment in a FTP or HTTP. If you've lost the IP address, you will need to be initialized with the initialization switch.

Default Setting : (Blank)

◆ Interception Settings

This setting is used when the operation mode is "Single Station" and the multi-client function is "Disabled."

When the device is connected to a PC via wired LAN, you can use the intercept function to access the device from the wireless LAN and perform maintenance via HTTP, etc.

In this case, the IP address to be accessed is the PC connected to the wired LAN.

Intercept Function

By enabling the intercept function, you can access the device from the wireless LAN and perform maintenance via HTTP, etc., even when the wireless connection mode is Compatible Infrastructure and the multi-client function is disabled.

Default Setting : Disabled

Intercept Target

When the intercept function is enabled, select the management communication to be intercepted. You can set HTTP (port 80), HTTPS (port 443), SNMP (port 161), SNMP Trap (port 162), SYSLOG (port 514), and NTP (port 123).

Default Setting : All Disabled

◆ DHCP Server

DHCP Server

Set to "Enable" if you want to use the DHCP server function.

Default Setting : Disable

Start IP Address

Set the start address of the range of IP addresses to be assigned to the client.

Default Setting : 192.168.0.221

End IP Address

Set the end address of the range of IP addresses to be assigned to the client.

Default Setting : 192.168.0.250

Subnet Mask

Set the subnet mask to be assigned to the client.

Default Setting : 255.255.255.0

Default Gateway

Set the IP address of the default gateway to be assigned to the client.

When set to 0.0.0.0, the default gateway is disabled.

Default Setting : 0.0.0.0 (Disable)

DNS

Set the IP address of the DNS to be assigned to the client.

When set to 0.0.0.0, the DNS is disabled.

Default Setting : 0.0.0.0 (Disable)

Lease Time (hour)

Set effective time (lease time) of the IP address assigned to the client.

This value can be set as 1 (hour) to 2400 (hours).

Default Setting : 24 (hours)

2. Ethernet

Port Speed

Select the Ethernet port speed.

You can select from "Auto (1Gbps)", "100Mbps (Full Duplex)", "100Mbps (Half Duplex)", "10Mbps (Full Duplex)", and "10Mbps (Half Duplex)". " (1Gbps)" is used normally.

If you want to use in other than "Auto (1Gbps)", you must set the same as this device connected device.

Default Setting : Auto (1Gbps)

Link Down Condition

When "Link Down Sense" is enabled in the "Advanced Settings" for each VAP, set the link down judgment condition.

The condition for "Link Status" is when the Ethernet link is disconnected. The condition for "Ping" is when a specific address can no longer be pinged, in addition to that for "Link Status".

When "Ping" is selected, the settings for "Ping Parameters" appear.

Default Setting : Link Status

Behavior After Link Down

When "ping" is selected in the "Link Down Sense" setting, set the behavior after link down.

When "Link Status" is selected, only "WLAN Interface Down" can be selected.

When "Ping" is selected, you can select “WLAN Interface Down” or Reboot.

Default Setting : WLAN Interface Down

◆ Ping Parameter

Ping IP Address

When the link down condition is set to "Ping", set the IP address for the device to ping.

Set the IP address for the device to ping to a device connected to this device by the wired network.

Be careful not to set the IP address for a device that cannot be pinged when this device starts, such as setting the IP address to a device on the wireless network.

Default Setting : (Blank)

Ping Interval (sec)

When the link down condition is set to "Ping", set the interval to ping the IP address between 1 and 65535 seconds.

Default Setting : 60

Ping Response Wait Time (sec)

When the link down condition is set to "Ping", set the wait time in seconds to wait for a response from the IP address to ping. A timeout is assumed if there is no response within the set time.

Set this value between 1 and 15 seconds.

Default Setting : 3

Ping Retry Count

Set the number of times to retry pinging the IP address from 0 to 15.

When a ping timeout occurs, the ping is retried within the number of times set here. If all the pings timeout, the ping is judged to have failed.

Default Setting : 3

3. VAP

TX Rate

Set the TX rate for wireless networking for the device.

This setting is normally set to "Auto".

Default Setting : Auto

Link Down Detection

This function monitors the wired networking port and stops the wireless function when the wired

networking port link is down (when disconnected). To use this function, set to "Enable".

If the unit type is set to "Station", use caution when using this function because the wireless network cannot be accessed when the wired networking port is down.

This setting is not available when the unit type is set to "Repeater". It is forcibly set to disabled.

Default Setting : Disable

Hide ESSID

This setting is available when the unit type is "Access Point" or "Repeater".

You can prohibit access by ANYID terminals (terminals with no ESSID set) by setting ESSID security to "Enable", and you can also hide the ESSID from being broadcast by the station.

In this manner, you can restrict unauthorized access using ANYID and prevent third parties from easily learning the ESSID.

Default Setting : Disable

Maximum Client Logins

This setting is available when the WLAN Mode is "Access Point".

Set the number of client logins to the station. The value can be set from 1 to 128 or 512 for each VAP.

Default Setting : 2.4GHz:128, 5GHz/6GHz : 512

Denial Response (Maximum Client Logins)

When the login number has reached to "Maximum Client Logins", is to ignore the connection request from the station, does not return a response. To use this function, set to "Enable".

This feature, you might want to use when there is the station to connect repeatedly.

Default Setting : Disabled

Beacon Interval (msec)

This setting is available when the unit type is "Access Point" or "Repeater".

Set the interval to send the beacon.

This value can be set between 100 ms and 1000 ms. It is not normally necessary to change the default value (100 ms).

This setting is a common setting for the VAPs.

Default Setting : 100

DTIM Period

This setting is available when the unit type is "Access Point" or "Repeater".

Set the DTIM (delivery traffic indication message) interval which is information added to the beacon for wireless terminals in a power-saving state to cancel that state.

This value can be set as 1 to 15.

Default Setting : 1

WLAN Bridge Between VAP

This setting is available when the unit type is "Access Point".

When set to "Disable", node on this VAP can not communicate (WLAN bridge) with nodes on other VAPs.

Default Setting : Enable

WLAN Bridge in This VAP

This setting is available when the unit type is "Access Point".

When set to "Disable", node on this VAP can not communicate (WLAN bridge) with other nodes on this VAP.

Default Setting : Enable

11g Only Mode

This setting is available when the unit type is "Access Point" or "Repeater".

When the wireless networking standard is IEEE 802.11n (2.4GHz) or IEEE 802.11g, this function prohibits logins by IEEE 802.11b wireless terminals. To use this function, set to "Enable".

Default Setting : Disable

11g Protect Mode

When the wireless networking standard is "IEEE802.11n (2.4GHz)" or "IEEE802.11g", protect mode is used for stable communication in an environment with a mix of IEEE 802.11b wireless terminals by setting "RTS-CTS" or "CTS only".

When "RTS-CTS", RTS and CTS are used. When "CTS only", only CTS is used.

11g protect mode is displayed for each VAP, but this setting is common to all VAPs.

Default Setting : Disable

Basic Rate

When the unit type is access point or repeater and the wireless networking standard is "IEEE802.11b", "IEEE802.11g", or "IEEE802.11n (2.4GHz)", you can set the basic rates.

You can select "802.11 (1,2Mbps)" or "802.11b (1,2,5.5,11Mbps)".

If 11g only mode is enabled, this setting is ignored.

Default Setting : 802.11b (1,2,5.5,11Mbps)

Link Monitoring

This setting is used when the operating mode is "Single Station", "Dual Station" or "Repeater" and the VAP wireless mode is "Station."

When enabled, after the VAP connects to the access point, it monitors the link status, and if the disconnection continues for the specified time or longer, it resets the wireless LAN function to attempt recovery.

Set the time in seconds, in the range of 10 to 3600.

Do not use this in conjunction with Link Down Detection (WLAN Interface Down).

Default Setting : Disable

Multi-Client

This setting is available when the unit type is "Station" and the wireless connection mode is "Compatible Infrastructure".

To connect multiple PCs under this device, set to "Enable".

When set to "Disable", only one PC can connect under this device.

When the operating mode is "Dual Station" or WDS is enabled, it is forcibly enabled.

Default Setting : Enable

Static Node Address

This setting is available when the operation mode is "Single Station", the wireless connection mode is "Compatible Infrastructure", and the multi-client function is "Disable".

Enter the MAC address for the PC that will connect to this device. Normally this setting is required when connecting to a device that will only receive communications, such as a POS terminal.

When not using this function, do not enter or enter the MAC address "00-00-00-00-00-00" which indicates it is disabled.

Enter the MAC address as two characters, a hyphen, two characters, and so on. (Ex: 00-80-4C-00-00-00)

Default Setting : (Blank)

Roaming Threshold

This setting is available when the unit type is "Station".

When the RSSI value for the connected access point falls below the set value, the station scans access points and searches for an access point that it can roam to.

This value can be set as 0 to 96. The larger the value, scans happen more often (roaming happens more easily). The smaller the value, scans happen less often (roaming happens less easily).

Default Setting : 24

Scan Channels

This setting is available when the unit type is "Station".

Select the channels to be scanned.

Note that communication between access point that is not set to the channel to be scanned is not possible.

Default Setting : (All)

Aging Time of the AP (sec)

This setting is available when the unit type is ¥"Station¥".

Specify how long to keep the information of access points in the wireless node information.

If you want to change from the default setting, please perform sufficient validation in the system to be used. You do not need to be changed in normal conditions of use.

Set this value between 10 and 120 seconds.

Default Setting : 120

Preferred AP

This setting is available when the unit type is "Station" or "Repeater".

This setting is for when there are multiple access points that can be connected to and you wish to apply a priority to the access points.

You can set the access point to preferentially connect to by specifying this setting. Enter the wireless MAC address for the access points in "Preferred AP1" to "Preferred AP5".

For the priority of access points to connect to, "Preferred AP1" has the highest priority, "Preferred AP5" has the lowest priority. This function is enabled by entering a valid wireless MAC address. When entering MAC addresses, specify them in order from "Preferred AP1".

When not using this function, do not enter or enter the MAC address "00-00-00-00-00-00" which indicates it is disabled.

Enter the MAC address as two characters, a hyphen, two characters, and so on. (Ex: 00-80-4C-00-00-00)

When the unit type is "Repeater", we recommend that you configure this setting and clearly specify the connection destination in the settings for VAP2 (station) on networks with two or more repeaters. If you do not specify the connection destination, when a chained repeater goes down, repeaters under it may connect to repeaters even further below themselves and form a loop.

By clicking the button to the right of the entry form, you can display a list of wireless MAC addresses for access points based on the "Wireless Node Information" in a drop-down list. By selecting an address from this list, it can be entered in the form.

Default Setting : (Blank)

Connections to Non-Preferred APs

This setting is available when the unit type is "Station" or "Repeater".

When using the preferred AP function and the device cannot connect to the access points specified in "Preferred AP1" to "Preferred AP5", set whether or not to allow connections to other access points. To allow a connection to access points other than the access points specified as preferred APs, set this setting to "Enable". To forbid connections, set this setting to "Disable".

When the unit type is "Repeater", we recommend that you set this setting to "Disable" and clearly specify the connection destination in the settings for VAP2 (station) on networks with two or more repeaters. If you do not specify the connection destination, when a chained repeater goes down, repeaters under it may connect to repeaters even further below themselves and form a loop.

Default Setting : Enable

4. MAC Address Filter

◆ MAC Address Filtering

MAC Address Filtering

This is the setting when the unit type is "Access point" or "Repeater".

The device can allow logins from stations (client terminals) with their wireless MAC addresses registered in advance and forbid logins from all other stations by enabling the MAC address filtering function.

Default Setting : Disable

◆ List Registration

Registered Address

Enter the addresses to register in "Registered Addresses". Enter the MAC address as two characters, a hyphen, two characters, and so on. (Ex: 00-80-4C-00-00-00)

To register only a single address, enter the address only in "Registered Address (Start)" and click the "Add" button. To set a range of addresses, enter the range in "Registered Address (Start)" and "Registered Address (End), and click the "Add" button. All the MAC addresses within that range are allowed.

Default Setting : (None)

VAP

The registered addresses are applied only to the VAP checked with "VAP". Typically there is no problem leaving all VAPs checked. When applicable VAPs are specified, select the VAPs to check.

Default Setting : (All)

◆ MAC Address List

MAC Address List

The registered MAC addresses are displayed in the "MAC Address Filtering List". When you wish to delete an entry, click the "DEL" button for the appropriate entry to delete it. Click the "ALL" button to delete all the entries.

A maximum of 1000 MAC addresses that allow login can be registered.

Default Setting : (None)

5. SNMP

◆ Common Settings

SNMP Agent

To enable the device's SNMP agent function, set to "Enable".

This device can be accessed by an external SNMP manager and its MIB can be acquired by enabling the SNMP agent function.

Default Setting : Disable

Community Name

Set the SNMP authentication string, called the community name, as alphanumeric characters between 1 and 32 characters in length.

The SNMP authentication string works like a password for accessing the device when using SNMP. The SNMP manager can access this device's MIB by using the community name.

Default Setting : public

sysContact

Set the address for the system contact as alphanumeric characters with a maximum length of 32 characters.

It is okay to leave this value blank.

Default Setting : Unknown

sysName

Set the SNMP name for the device as alphanumeric characters with a maximum length of 32 characters.

It is okay to leave this value blank.

Default Setting : Unknown

sysLocation

Set a description of the installation location for the device as alphanumeric characters with a maximum length of 32 characters.

It is okay to leave this value blank.

Default Setting : Unknown

◆ Trap Settings

Trap IP Address

Traps are a function to notify users that a change has occurred in the SNMP agent system.

The trap function can be enabled by specifying the trap destination IP address, and the trap is sent to the specified IP address.

When set to 0.0.0.0, the trap function is disabled.

Default Setting : (Blank)

Notification: Link Status (Ethernet)

Set whether or not to send a trap when the wired network link status has changed (link up/down).

When enabled, the device sends a trap regarding the wired network link status change.

Default Setting : Disable

Notification: Link Status (WLAN 1/2)

Set whether or not to send a trap when the wireless network link status has changed (link up/down).

When enabled, the device sends a trap regarding the wireless network link status change.

Default Setting : Disable

Notification: Channel Change (DFS)

Set whether or not to send a trap when a channel change occurs by DFS when "Unit Type" is access point and "Channel" is set to a channel subject to DFS.

When enabled, the device sends a trap regarding the DFS channel change.

Default Setting : Disable

Notification: Initialize (INIT-SW)

Set whether or not to send a trap when the device was initialized by pressing the initialization switch on the unit.

When enabled, the device sends a trap regarding initialization by the initialization switch.

Default Setting : Disable

6. NTP

NTP Client

The device can synchronize its time with network time by enabling the NTP client function and configuring the NTP server setting.

To use this function, select "Enable".

Default Setting : Disable

NTP Server

When enabling the network time function, specify the IP address for the NTP server.

Default Setting : (Blank)

NTP Interval (sec)

Set the interval time to send a request for NTP client function.

Set this value between 15 and 604800 sec.

Default Setting : 86400

7. Log

Log Function

To record the log for the device using the log function, set to "Enable".

You can prevent the log from being recorded by setting this setting to "Disable", but in normal operation this is unnecessary.

Default Setting : Enable

Save Log

To save the recorded log information as a file, set to "Enable". To only temporarily retain the recorded log information in memory, set to "Disable".

Temporary retention means the log information is retained only while the device is running. When "Disable", the log information is deleted when the device restarts or the power is disconnected.

Default Setting : Disable

Block Size (KB)

Set the size of one log file block between 1 and 1024 (KB).

Default Setting : 100

Number of Blocks

Set the number of blocks for the log file between 1 and 20.

If the block size is 100KB and the number of blocks is 10, the log file will be a maximum of 1MB.

Default Setting : 10

Save Interval (min)

Set the interval at which to save the log.

Set this value between 5 and 1440 minutes.

Default Setting : 20

SYSLOG Server

To send the acquired log information to a SYSLOG server as a SYSLOG, set the IP address for the SYSLOG server.

When not sending the log information to a SYSLOG server, set to 0.0.0.0 to disable.

You can specify up to two SYSLOG servers.

Default Setting : 0.0.0.0

Debug Log

Please set to "Enable" if you want to log for more detailed debugging.

"Enabled" has two levels, "Common" and "Verbose". Setting it to "Verbose" will output a lot of wireless-related debug logs.

Default Setting : Disable

Hostapd Debug Log

This setting is available when the debug log setting is "Enable (Verbose)".

When enabled, outputs verbose hostapd debug logs.

Default Setting : Enable

WPA Supplicant Debug Log

This setting is available when the debug log setting is "Enable (Verbose)".

When enabled, outputs verbose WPA supplicant debug logs.

Default Setting : Enable

3.Status

1. System

Loader Version

Shows the loader version.

Firmware Version

Shows the firmware version.

Board ID

Shows the board ID.

Product ID

Shows the product ID.

Machine ID

Shows the machine ID.

Product Name

Shows the product name.

Country ID

Shows the country ID.

Ethernet MAC Address

Shows the ethernet MAC address.

5GHz /6GHz Wireless MAC Address

Shows the wireless MAC address of 5GHz / 6GHz interface.

2.4GHz Wireless MAC Address

Shows the wireless MAC address of 2.4GHz interface.

IP Address

Shows the IP address.

Subnet Mask

Shows the subnet mask.

Default Gateway

Shows the default gateway. When not configured (00-00-00-00-00-00), nothing is shown.

Sensor Temperature

Shows the the surface temperature (degrees celsius) of the CPU and 5GHz /6GHz components.

CPU Information

Displays information such as the CPU usage rate of this device.

usr	User level application
nice	User level application with nice priority
sys	Kernel
iowait	Idle (disk I/O request)
irq	Hardware interrupts
soft	Software interrupts
steal	Hypervisor processing for virtual CPU
guest	Virtual CPU Processing
gnice	Virtual CPU Processing with nice priority
idle	Idle(excluding iowait)
intr/s	Number of interrupts per second

Memory Information

Displays information such as the device's memory usage in KB.

total	Total memory amount
used	Used memory
free	Unallocated unused memory
shared	Memory used by shared memory
buff/cache	Total memory for file buffers and cache memory
available	Available memory

ARP Table

Displays ARP table.

2. WLAN

◆ Common Settings

Operation Mode

Shows the configured operation mode.

Mesh Type

When working as a mesh, shows the configured mesh type.

Primary Interface

When working as a dual station, shows the configured primary interface.

◆ 5GHz / 6GHz, 2.4GHz Interface

WLAN Interface

Shows whether the interface is enabled or disabled.

WLAN LAN Standard

Shows the configured wireless infrastructure mode.

Band Width

Shows the configured bandwidth.

Band

Shows the band (5GH/6GHz) selected for the 5GHz/6GHz interface.

Channel

Shows the channel when operating as an AP.

◆ VAP

WLAN MAC Address

Shows the wireless MAC address of the VAP.

WLAN Interface

Shows whether the VAP is set to 5GHz/6GHz or 2.4GHz interface.

WLAN Standard

Shows the operating wireless LAN standard of the VAP. Unknown is displayed when the station is not associated to an access point.

WLAN Mode

Whether it is operating as an access point or a station is displayed.

WLAN Infrastructure Mode

Shows whether the WLAN infrastructure mode is a standard infrastructure, a compatible infrastructure, or an advanced infrastructure.

ESSID

Shows the ESSID of the VAP.

Channel

Shows the operating channel of the VAP.

Number of Assoc

Shows the number of stations associated into the VAP when the wireless mode of the VAP is access point.

Assigned AP

Shows the wireless MAC address of the associated access point when the wireless mode of the VAP is station.

RSSI

Shows the RSSI of the associated access point when the wireless mode of the VAP is station.

TX Rate

Shows the TX rate to the associated access point when the wireless mode of the VAP is station.

RX Rate

Shows the RX rate from the associated access point when the wireless mode of the VAP is station.

◆ Statistics

Shows the counter of WLAN interface and VAP.

◆ Certificate Information

Displayed when a certificate is installed.

Issued by

Shows the name of the certificate publisher (CA).

Issued to

Shows the name of the organization the certificate was issued to.

Valid from

Shows the date the certificate was issued.

Valid to

Shows the date the certificate expires.

◆ Station Lists

Shows a list of the stations logged in to the device.

◆ Surrounding AP

Shows a list of surrounding APs.

◆ Mesh Information

When the operation mode is mesh, the mesh network is displayed in a tree view.

By clicking on each node, you can retrieve and display the status of the VAP.

The table below shows what the icons and numbers displayed to the right of the icons indicate.

	Controller
	Wireless Backhaul Agent
	Ethernet Backhaul Agent
	Unknown Device
	2.4GHz RSSI (Wireless Backhaul Agent)
	5GHz/6GHz RSSI (Wireless Backhaul Agent)
	2.4GHz Number of Assoc (Fronthaul)
	5GHz/6GHz Number of Assoc (Fronthaul)

◆ RSSI Graph

An RSSI trend graph is displayed when the Operation Mode is Single Station or Dual Station, Mesh Agent (Ethernet Backhaul).

3. MAC Address Table

Shows a list of MAC address the device has learned of by communications over the wired and wireless networks.

MAC Address

Shows the MAC addresses for this device and those of other learned of devices.

Interface

Devices learned of via the wired network are shown as "LAN(1)", devices learned of via the wireless network are shown as "WLAN(2)".

Aging Time

Shows the aging time (expiration time) for the target device.

WLAN MAC Address

Shows the wireless MAC address of devices learned of via the wireless network.

4. Log

Shows the log recorded by the device.

If the number of log entries exceeds 500 entries, the most recent 500 entries are displayed. If you wish to check the entire log, open the link to the log file at the bottom of the page.

When the device's "Save Log" setting is enabled, the log in memory is regularly written to the unit's flash ROM. The number of times the log has been written to the flash ROM is displayed in "Number of Times Log Saved" at the top of the page.

To delete the entire device log, click "Clear All Logs", and then click "OK" on the confirmation dialog. Use caution as the log cannot be restored when cleared.

Category	Event	Description
SYSTEM	Start	Start (Firmware version)
	Manual reboot	Manual reboot
	Save logs	Saving logs
SWITCH	Init	Initializing using the initialization switch
LAN	Set LAN speed duplex = XXX	Port speed setting
	Link down	Link down
	Link up (1000/100/10Mbps full/half duplex)	Link up (link speed and communication mode)
WLAN	Login XX-XX-XX-XX-XX-XX,YYch,ZZ (VAPX)	Login (MAC address, Channel, RSSI, VAP)
	Roaming XX-XX-XX-XX-XX-XX,YYch,ZZ (VAPX)	Roaming (MAC address, Channel, RSSI, VAP)
	Logout XX-XX-XX-XX-XX-XX,YYch,ZZ (VAPX)	Logout (MAC address, Channel, RSSI, VAP)
	Switch bandwidth from 40MHz to 20MHz (2.4GHz)	Bandwidth (2.4GHz) changed from 40MHz to 20MHz
	DFS CAC started (Xch)	Start of CAC (channel availability check) period (channel)
	DFS CAC completed (Xch)	End of CAC period (channel)
	DFS radar detected (Xch)	Radar detection (channel)
	DFS Xch (XMHz) -> Xch (XMHz)	Dynamic frequency selection (channel &frequency)
	DFS NOL started (Xch)	Start of NOL (Non-Occupancy List) period (channel)
	DFS NOL finished (Xch)	End of NOL period (channel)
	DFS channel is not available (WLAN1)	No more available channels
	Standby as mesh controller backup device	This device stands by as a controller backup device
	Start as mesh controller (for backup)	For backup, this device will start working as a mesh controller
	Standby as mesh controller backup device (the target controller	Since the target controller has recovered, this device will stand by as a controller backup device

Category	Event	Description
	XXX.XXX.XXX.XXX has recovered)	
WEB	Login (X.X.X.X)	Login (IP address)
	Logout (X.X.X.X)	Logout (IP address)
	Firmware update(XXX -> XXX)	Updated firmware (old version -> new version)
	Setting clock (YYYY-MM-DD HH:MM:SS)	Setting time (old time)
	Change password	Change password
	Restore config	Restore configuration file
	Default setting	Default settings
	Save config and reboot	Save settings and reboot
	Save config	Save settings
	Clear logfile	Clear logfile
	Upload server certificate	Upload server certificate
	Server certificate upload failure	Server certificate upload failure
	Upload client certificate	Upload client certificate
	Client certificate upload failure	Client certificate upload failure
	Upload private key	Upload private key
	Private key upload failure	Private key upload failure
	Upload PKCS#12 certificate	Upload PKCS#12 certificate
	PKCS#12 certificate upload failure	PKCS#12 certificate upload failure
FTP	Login (X.X.X.X)	Login (IP Address)
	Logout (X.X.X.X)	Logout (IP Address)
	Login failed (X.X.X.X)	Login failed (IP Address)
	Firmware update (XXX -> XXX)	Updated firmware (old version -> new version)
	Firmware update error	Firmware update failed
	Config write	Writing configuration file
	Config write error	Writing configuration file failed
	Server certificate write	Writing server certificate
	Server certificate write error	Writing server certificate failed
	Client certificate write	Writing client server certificate
	Client certificate write error	Writing client certificate failed
	Private key write	Writing private key
	Private key write error	Writing private key failed
	PKCS#12 certificate write	Writing PKCS#12 certificate
	PKCS#12 certificate write error	Writing PKCS#12 certificate failed
	RST command	Reset command issued
NTP	Setting clock (YYYY-MM-DD HH:MM:SS)	Setting time (old time)
DHCP	Lease YYY.YYY.YYY.YYY to XX-XX-XX-XX-XX-XX	Leased IP address YYY.YYY.YYY.YYY to XX-XX-XX-XX-XX-XX
	No IP address to lease to XX-XX-XX-XX-XX-XX	No IP address to lease to XX-XX-XX-XX-XX-XX

Category	Event	Description
	Lease YYY.YYY.YYY.YYY(Zh)	IP address YYY.YYY.YYY.YYY leased for Z hour(s)
	No lease	IP address not leased

4.Maintenance

1. Flash Firmware

You can update the firmware on the device.
Click the "Browse" button, select the version update file system file, and then click the "Confirm" to upload the file to the device.
The checksum and file size of the uploaded file are displayed, so you can check if it is the same as the original file.
Click the "Proceed" button to update the firmware and switch the screen after completion. After that, the device starts up with the rewritten firmware by rebooting.
When the version update fails, check that the uploaded file is the correct file, and then try to update the version again.
Do not turn off the device's power under any circumstances during the updating task from when the "Update" button is clicked until the screen changes as this will result in malfunction.
The progress bar displayed during the update is a guide that indicates the progress status in terms of time, it does not indicate the actual progress of the work. The progress bar indicates the completion time when the gauge is full.

2. Time Setting

Set the date and the time for the device. Enter the year as four digits, the month, the day, the hour (24-hour time), the minute, and the seconds, and then click the update button. When the month and day are a single digit, a 0 is added and they are displayed as two digits. You can enter the values as either a single digit or as two digits. (Example: 2024/4/1 0:0:0)
Or click the "Set PC Time" button to set the time in the PC's internal clock where the browser is open in the entry form.

3. Password

You can change the login password to this device including the Wireless LAN Manager (this configuration web page).
Enter the password as alphanumeric characters with a maximum length of 31 characters.
The changed password is reflected immediately.
For security enhancement, change the password from the default.

⚠ CAUTION

Please change the password from the factory defaults to avoid possible security issues.

4. Backup

You can backup the device's current configuration file, MAC address filtering file and log file by clicking the link.

The name of backuped file has the extension .txt added to it.

The backup configuration file cannot be used for other series of wireless devices.

5. Restore

You can restore the device's configuration file / MAC address filtering file.

Press the “Browse...” button to select the file to be uploaded and press the “Update” button to upload the file to this device. After pressing the “Update” button, it takes a few seconds to a few dozen seconds for the file upload and update process to be completed, and the screen will change.

If the upload fails, check that the file to be uploaded is correct and try uploading again.

Never turn off the power to this equipment during the update process from the time you press the “Update” button until the screen changes over, as this may cause equipment failure.

Do not restore with configuration files backed up by other series of wireless devices. Some settings can be loaded, but operation after configuration is not guaranteed.

6. Default Settings

You can restore the device's settings to the default settings.

At this time, select with the radio button to also restore the IP addresses (including subnet mask) to the defaults or to leave them as they are. Then click the "Default" button.

Even when the default settings are restored, they are not saved to the device's configuration file, so you must save and restart to reflect the settings.

7. Ping

You can ping to the specified IP address.

Enter the IP address of the ping to "Target IP Address".

To "Count", select the number of times to send the ping packet.

Set the ping data size to "Data Size (bytes)". This value can be set between 4 and 65000 bytes.

By clicking the "Ping" button, then the results displayed below the button.

Wireless Link Mode and Wireless LAN Function

This chapter describes the major functions of the FLEXLAN series as a wireless LAN system and the wireless link modes of the product along with configuration examples of networks available in the wireless link modes.

1.Wireless Link Mode

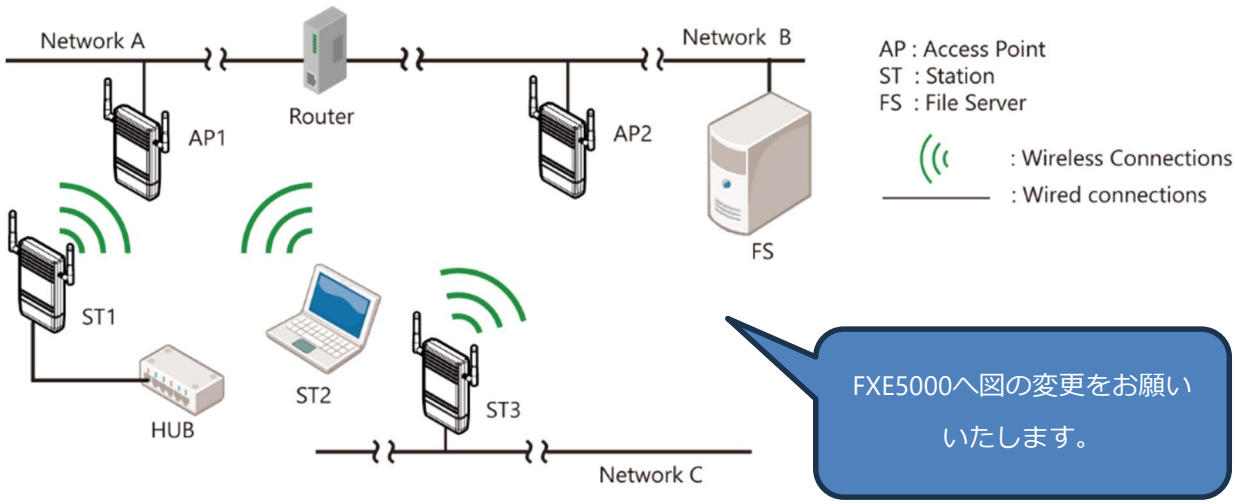
This product has three wireless link modes. The available functions and network configurations differ depending on the mode. Use the wireless link mode most suitable to the type of network you are constructing.

The factory default setting is “Advanced Infrastructure Mode”.

“Connection to Devices and Setup Methods (Page 39)“ and **“Setup and Status Display (Page 46)“** describe the software setting procedures for the wireless link modes and related items.

1. Standard Infrastructure Mode

In this mode, each access point (AP) can accommodate stations (ST) to make up a network.
This mode allows the use of multiple APs to configure a wide-area wireless LAN. All communication between wireless terminals must go through an AP.



In the Standard Infrastructure mode above, all wireless terminals communicate via AP. Roaming functions are supported, allowing login to any AP within range of radio waves.
For the IP tunneling function to work properly, one of the APs must be setup as a master AP.

Advantages

(1) Allows log-in restrictions (security function).

(2) Improves security using the WSL (Wireless Security Link).

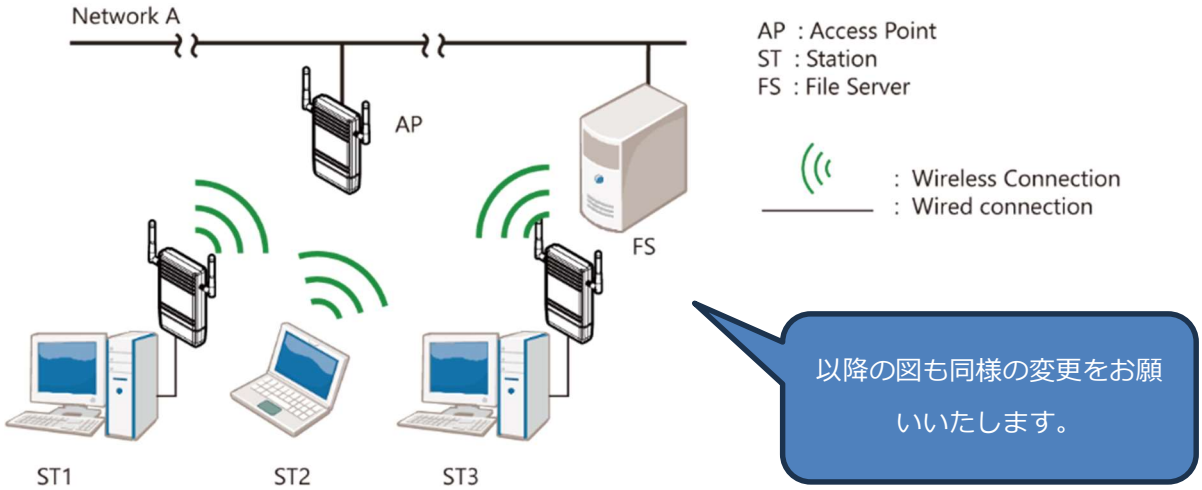
(3) When connecting a CONTEC station to this product using a wired connection, there is no limit to protocols and the number of devices that can be connected.

2. Compatible Infrastructure Mode

This mode allows the product to be networked with other manufacturers' Wi-Fi certified wireless terminals other than the FLEXLAN series. Communications between the wireless terminals are always made via the APs.

⚠ CAUTION

The Compatible Infrastructure mode does not guarantee interconnection with Wi-Fi compliant products of other manufacturers.

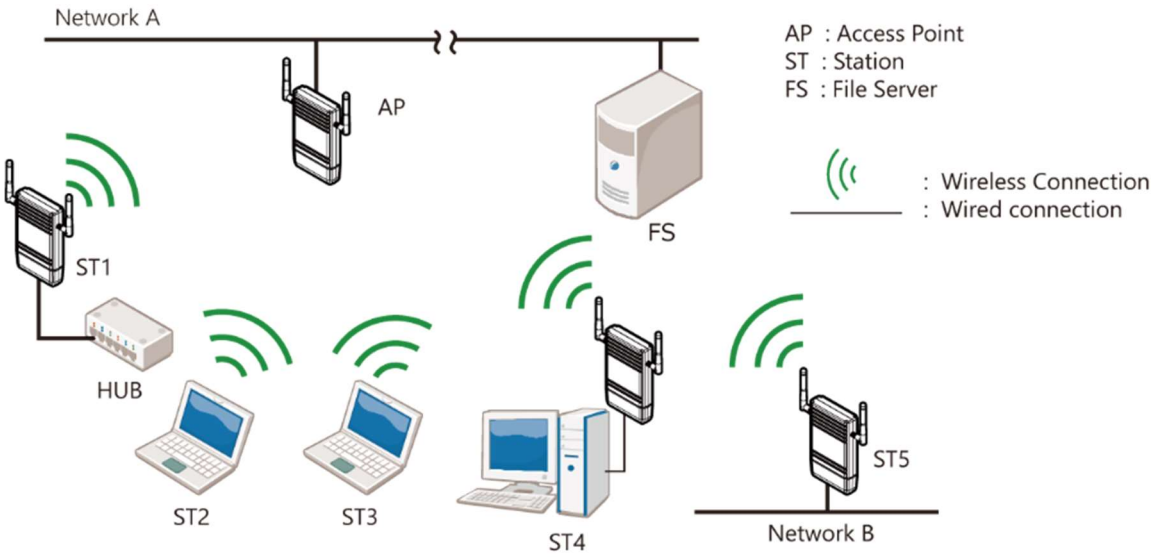


In the Compatible Infrastructure mode, each wireless terminal performs communication via the AP as in the Standard Infrastructure mode. Roaming functions are supported, allowing login to any AP within range of radio waves.

APs operate as simple bridges and cannot use the unique features of the FLEXLAN series.

3. Advanced Infrastructure Mode

The Advanced Infrastructure mode is a mixture of the Standard Infrastructure and Compatible Infrastructure modes. The Advanced Infrastructure mode can be used only when the product is configured as an access point.



On the terminal set to the Standard Infrastructure mode, the FLEXLAN series' unique functions can be used.

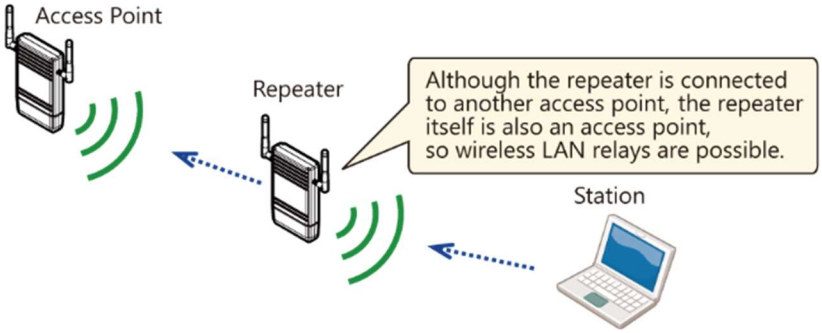
The terminal set to the Compatible Infrastructure mode serves as a simple bridge and thus the FLEXLAN series' unique functions cannot be used on this terminal.

2.Repeater

1. What's Repeater?

The repeater used with the wireless LAN is a function that operates the wireless LAN equipment as a pair of virtual wireless LAN devices (VAP). One of these devices is set as the access point and the other is set as the station.

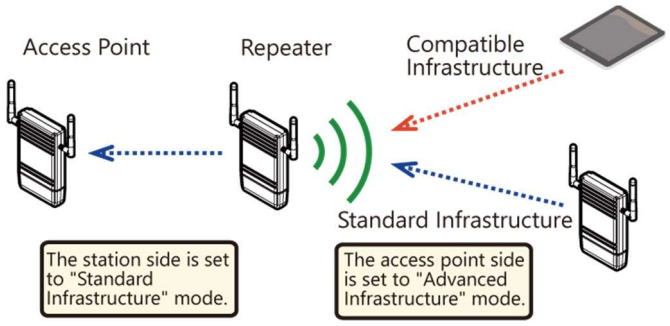
It is possible to connect to other access points from the station and to log in to the access point from other stations.



2. Specification for Repeater and Wireless Connection Mode

When a piece of equipment is set as a repeater, its VAP2 becomes an access point and its VAP1 becomes a station. In this situation, if you set "Wireless Connection Mode" to "Advanced Infrastructure", the repeater's access point side will operate in "Advanced Infrastructure" mode and the repeater's station side will operate in "Standard Infrastructure" mode.

If you set "Wireless Connection Mode" to "Compatible Infrastructure", both the access point and the station will operate in "Compatible Infrastructure" mode. In this situation, the multi-client function of VAP1 (the station) will be forcibly enabled.



Wireless connection mode of repeater	VAP2 of repeater (AP side)	VAP1 of repeater (ST side)
Standard Infrastructure	Standard Infrastructure	Standard Infrastructure
Compatible Infrastructure	Compatible Infrastructure	Compatible Infrastructure
Advanced Infrastructure	Advanced Infrastructure	Standard Infrastructure

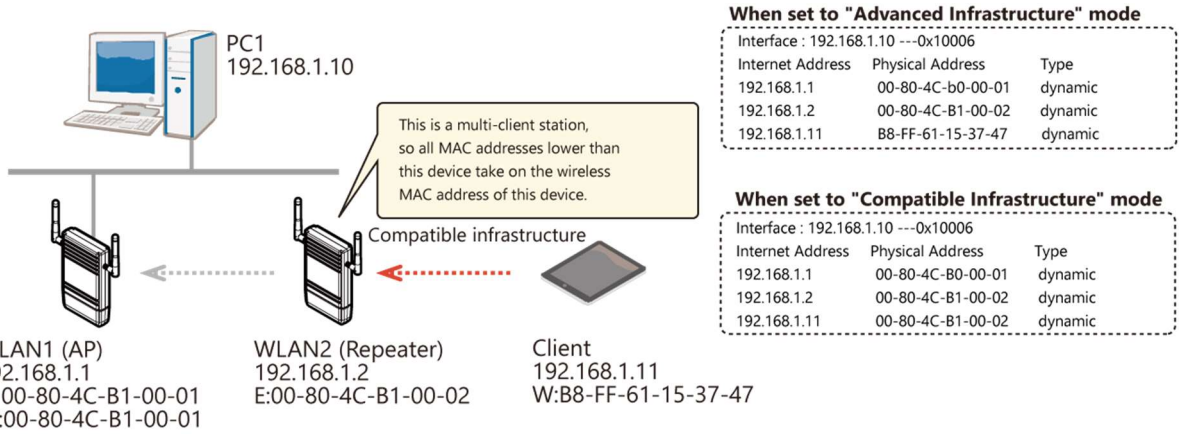
If you set "Wireless Connection Mode" to "Advanced Infrastructure", you will be able to connect to stations in "Standard Infrastructure" mode and to stations in "Compatible Infrastructure" mode.

3. Recommended Setting

When "Wireless Connection Mode" is set to "Compatible Infrastructure", the VAP2 (station side) of each repeater located under this device is also set to "Compatible Infrastructure" mode. As such, all terminals under the repeater have the same MAC address in the PC1 ARP table.

In this situation, clients roam from WLAN2 to WLAN1, and communication cannot be performed from PC1 to 192.168.1.11. The reason for this is that if a client connects to WLAN1, its MAC address will be changed.

To have PC1 perform communication, you have to delete the PC1 ARP table, and have PC1 learn the 192.168.1.11 MAC address again.



PC1 is linked to the client roaming, so the PC1 ARP table cannot be deleted. When you use repeaters to construct your system, we recommend that you operate the repeaters in "Advanced Infrastructure" mode.

⚠ CAUTION

If APs without "Standard Infrastructure" mode made by other companies exist within your system, you will not be able to use "Advanced Infrastructure" mode.

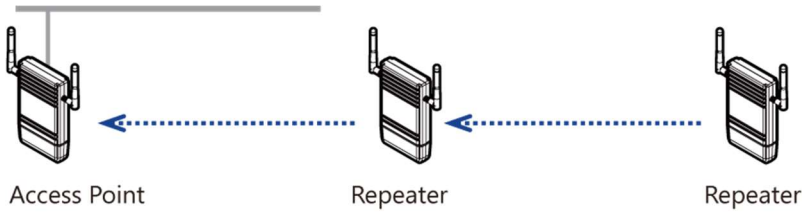
For example, if WLAN1 in the above figure is an access point made by another company and you set WLAN2 to "Advanced Infrastructure" mode, WLAN1 and WLAN2 will not be able to communicate with each other.

4. Notes

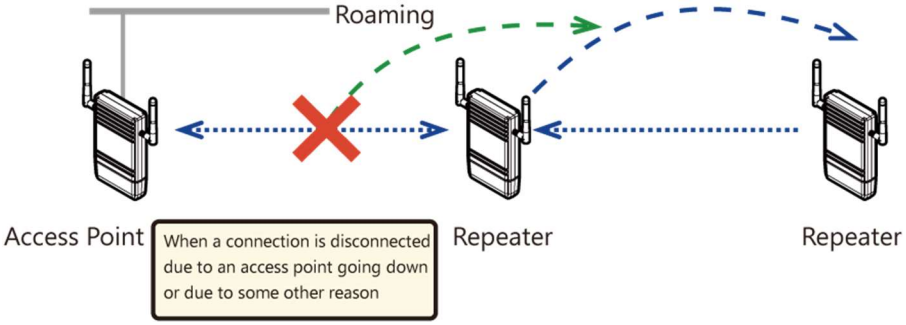
When you configure the device to operate as a repeater, regardless of whether the network configuration is chain or star, use the "Preferred AP" function to specify the connection destination access point.

Also, you have to set the "Connections to Non-Preferred APs" function to "Disable" in order to prevent loops between repeaters with unauthorized connections to unexpected access points.

(1) Use the preferred access points to specify the connection destinations to establish an arbitrary connection structure.

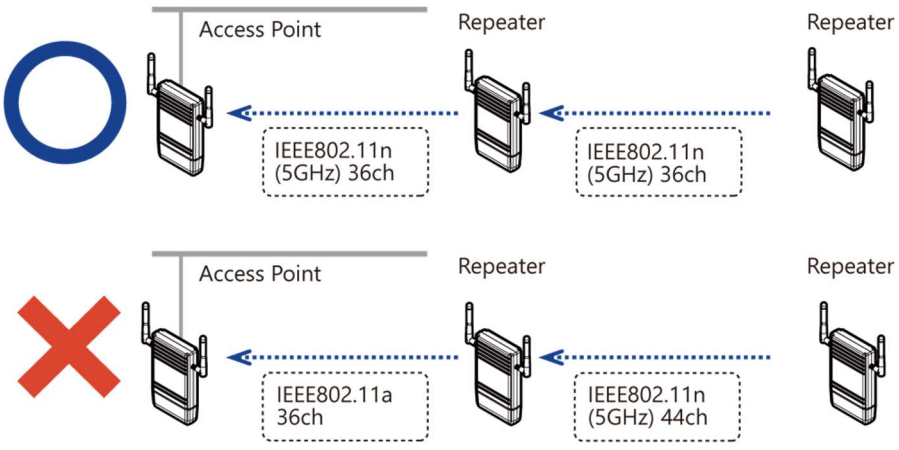


(2) If you do not fix the connection destinations, loops may occur between repeaters.



If you set a device as a repeater, set all parts of the wireless network to the same channels and the same wireless LAN standard.

For example, if you construct a network with one access point and two repeaters for a total of three pieces of wireless equipment, configure all the equipment so that the same wireless LAN standard and the same channels are used.



3.Installation in a Network

This section describes how to install this product to construct a network with improved performance and discusses the general features and radio characteristics of the wireless LAN as well as the guidelines for constructing the network.

1. Features of the Wireless Network

In general, the operation of a wireless network is the same as for most other types of LAN. The most prominent feature of the wireless network is that it uses radio waves as its medium, eliminating the need for cabling. The wireless network thus requires no cabling cost and has other advantages as listed below：

- Quick construction of a LAN
- Temporary installation of a LAN
- Higher flexibility in layout of connected PCs (terminals)
- Assured mobility of connected PCs (terminals)

On the other hand, the wireless network has the following drawbacks from the operational point of view due to the nature of radio waves：

- Signal attenuation
- Signal interference

Also, although this unit does not require a radio license, it is subject to radio regulations.

2. Operating Environment and Radio Waves

When using this product to construct a network, install and operate it considering the radio environment to optimize the performance.

◆ Is allowed to use radio equipment at the installation location?

In some medical institutions and laboratories, radio-sensitive precision instruments are used and it may be prohibited to use radio equipment.

◆ Radio waves are attenuated.

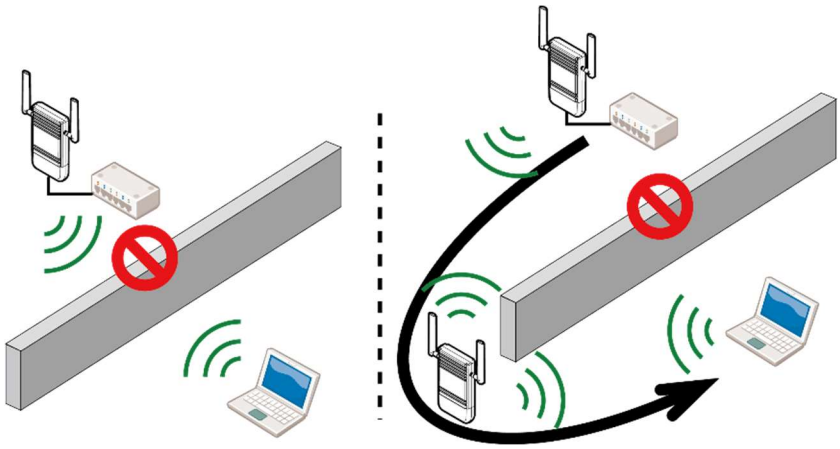
Although a radio wave is attenuated naturally as it travels from its transmission source, it may also be attenuated by an object existing in its way. Major obstacles that attenuate radio waves are as follows：

- Concrete wall
- Metal surfaces in the vicinity of the antenna

Obstacles blocking radio waves include metal walls and walls containing a metal firewall.

Strictly speaking, nearly all objects in the path of the radio waves (such as partitions or people) cause some attenuation but these do not have a significant impact on network performance.

RSSI (Receive Signal Strength Indication) utility is available as a means of knowing the signal strength of an incoming radio wave. Placing this product for a greater RSSI value makes the communication state more stable. If the RSSI value is small and slightly moving the position of the product does not increase the RSSI value, it indicates radio wave attenuation either to the distance or by an obstacle.



◆ Pay attention to radio interference.

Radio interference means the reception of radio waves in the frequency band used by this network that are generated by equipment that is not part of the network to which this product belongs. Listed below are major examples of sources of interfering radio waves generated in general environments excluding plants and factories：

- 5GHz (if using this product in the 11ax/ac/n/a 5 GHz band) or 2.4GHz (if using this product in the 11ax/n/b/g 2.4 GHz band) band wireless networks that do not comply with IEEE802.11.
- If using IEEE 802.11ax/n/b/g standard in the 2.4GHz band. Ex. microwave ovens, security gates (installed near the entrances of some department stores and rental shops), copiers which give off the 2.4GHz electric waves.

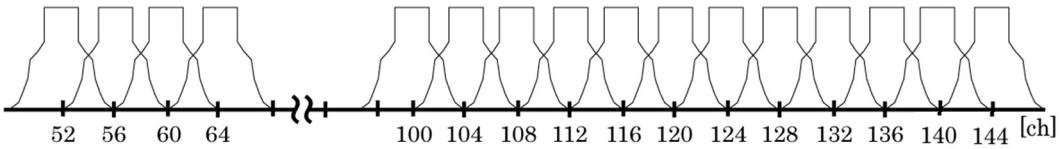
Where there is a large metal wall such as in a warehouse, the radio wave generated from the sender is reflected, resulting in those radio waves reaching the receiver which have taken different routes (thereby phase-shifted). This has the similar effect as the generation of interfering radio waves, possibly slowing down data transfer.

Most of the interfering radio wave sources other than wireless networks have local and/or temporary effects, not so affecting network performance. Rarely, however, the date rate is reduced and, in the worst case, communication is disabled temporarily. In such cases, change the location of this product and the channel used for communication. This may solve the problem.

◆ 5GHz band (W53/W56)

When using the 5 GHz band, you need to take into account that a function called DFS works when you set the channel to 52, 56, 60, 64ch (W53) or 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140c, or 144ch (W56).

The W53 and W56 channels use the same frequency band as weather radar and ship radar, and DFS is a function that changes the access point channel to avoid radio interference with these radar waves. W53 and W56 are DFS-compatible channels.



The following is an overview of DFS.

- When an access point is set to one of the DFS-enabled channels, the access point checks for radar waves in the channel for 1 minute before starting to transmit radio waves.
- If a radar wave is detected, the access point uses a different channel from the specified channel. If the channel is a DFS-enabled channel, the access point checks for radar waves again.
  If no radar wave is detected, the access point transmits radio waves on the specified channel. However, if the W56 channel is used, the access point moves only to the W56 channel.
- When a radar wave is detected, the access point does not transmit radio waves to the channel for 30 minutes after detection. In other words, when a radar wave is detected, the channel cannot be used for radio communication for at least 30 minutes.
- If the access point detects a radar wave during activation, it immediately stops transmitting radio waves (stops radio communication). At this time, the access point uses a different channel than the specified channel.

In other words, when building a wireless network on a W53 or W56 DFS-enabled channel, note the following points:

- The access point needs at least 1 minute to start up on the DFS-enabled channel.
- The access point might start up on a different channel than the DFS-enabled channel set.
- Even if the access point starts up on the DFS-enabled channel set, the channel might be changed during operation.

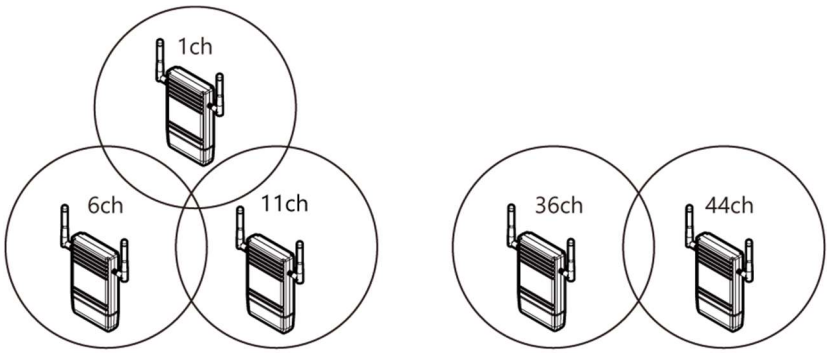
When configuring a network using DFS-enabled channels, consider whether there is no problem with DFS channel changes. Even if radar waves are not detected during network design, radar waves may be detected later.

In addition, the "WLAN2" LED of the product blinks during a one-minute check for radar waves immediately after startup.

◆ Constructing a Network

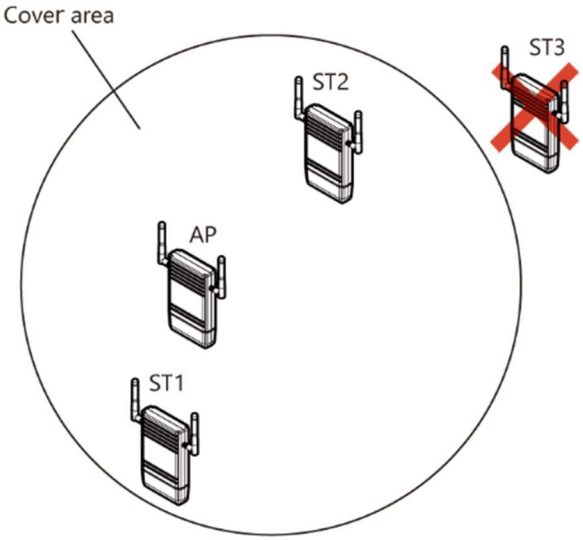
This section gives some pointers and cautions relating to constructing a network using the AP and station, and provides some practical examples.

- Wireless communication is possible with the station corresponding to the channel. Wireless communication is possible with stations that support the above channels. Using different channels for wireless networks adjacent to each other (In 5GHz band, set it to 36.44, 8ch or more apart and in 2.4GHz, 1, 6, 11 5ch or more apart) prevents radio interference and improves the throughput of either network.



When using it in 2.4GHz　　When using it in 5GHz

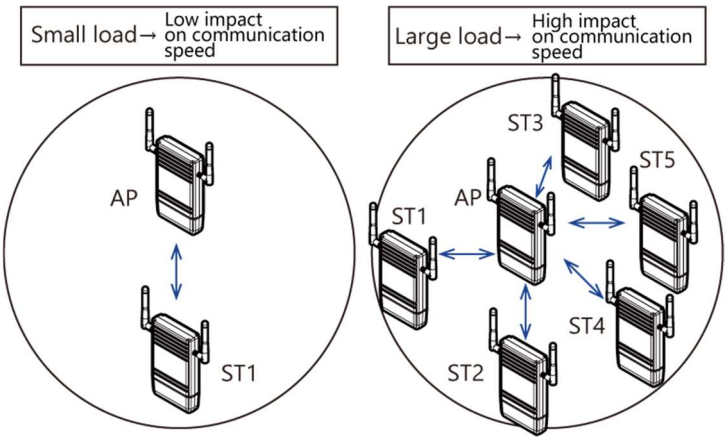
- Check the coverage (cover area) of the AP.　To use the AP with two or more station logged in AP, all the station must be installed within the cover area.　The AP's coverage varies with obstacles (concrete walls, iron doors, elevator halls, etc.).　Note also that the number of transmission/reception errors increases beyond a certain transmission distance.



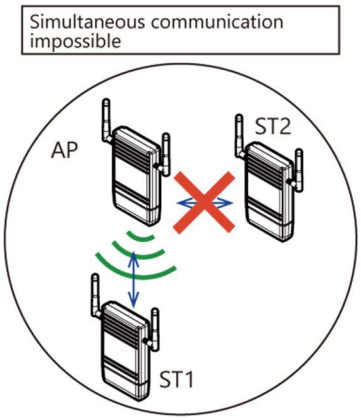
When setting up the network, check the RSSI level then confirm that communication works correctly with the application you plan to use. For a TCP/IP system, for example, you can use the Windows PING command. To use PING, start the command prompt (MS-DOS) and enter the following command. The example command is for an AP with an IP address of 192.168.0.2.

```
ping 192.168.0.2
```

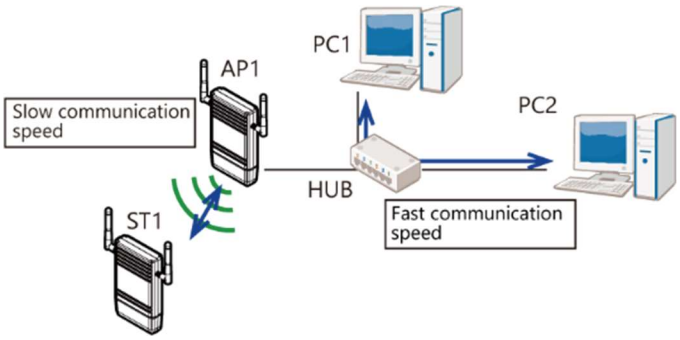
- Two or more stations can log in the AP at the same time However, remember that the communication speed slows due to the increased loading as the number of user units for a particular AP increases.



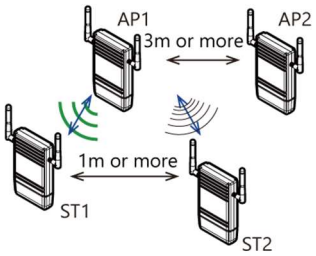
- If a pair of wireless terminals are communicating via a particular channel, no other communications can use that channel within the range of the radio signal (the exception is broadcasting which transmits to all terminals). As a result, communication speed tends to drop as the density of wireless terminals increases although this depends to a large extent on how frequently the network is used.



- If the AP is connected to an Ethernet hub or similar, an unexpectedly large load can occur on the AP if the Ethernet traffic is heavy and this may reduce the performance of the wireless network. This can be solved by changing the hub connected to the AP to a switching hub (bridge).



- Setup the software in accordance with how the network will be used.
- The communication speed may also drop due to interference if two wireless terminals are located close to each other. In general, maintain a gap of about 1m between station, 3m between APs and station, and 3m between APs.



- The best performance is achieved from antennas if they are located in an open space free from obstructions. Avoid locating antennas where they will be hidden. In particular, when communication distance is an important consideration, it is recommended that you install antennas in a high location with a clear view.
- Floors often contain steel beams or metal firewalls and therefore communication between floors is often not possible.

Maintenance

This chapter describes how to perform maintenance on the AP and explains the tools to be used. Here, “maintenance” means the following : log file collection, firmware upgrades, and saving and restoring the software settings.

1.Maintenance Tool

This maintenance tool is available for the FTP, Web browser and FLEX HELPER. This section describes how to use the tool by the FTP. or details about downloading using a Web browser, see the section titled **"Setup and Status Display (Page 46)"**.

For details and applications of FLEX HELPER, contact your dealer.

2.Log File Collection

To collect the log file, you collect it by using Web browser or FTP via the LAN.

The log file is in text format and can be displayed in the Notepad or WordPad programs that come with Windows.

The collected log file is stored the AP memory with the following file name.

File name : LOGFILE

⚠CAUTION

To collect the log file, log collection must be enabled. Note also that the contents of the log file differ depending on the operating mode and software settings.

1. Using FTP to Get the Log File

To collect log files using FTP, follow step 1 to 6.

1 Move to the folder in which you wish to save the file.

2 Run FTP to log in to the AP.

3 Run FTP to log in to the AP. (Enter FTP user's name)

4 Run FTP to log in to the AP. (Enter FTP password)

5 Transfer the log file.

6 Exit FTP.

The following is an example for the time when Windows Command Prompt (MS-DOS Prompt) is used.

In this example, the file will be moved to the saving folder D : ¥tmp and LOGFILE will be collected after connecting to this product via FTP. The example assumes the User as admin (blank is OK), Password as Pass (initial setting) and the IP address as 192.168.0.1.

```
C:¥>cd D:¥tmp                          ..... 1
D:¥tmp>ftp 192.168.0.1                 ..... 2
User (192.168.0.1:none):admin          ..... 3
Password:pass                          ..... 4
ftp>get LOGFILE                        ..... 5
ftp>bye                                ..... 6
```

* For details about downloading using a Web browser, see the section titled **"Setup and Status Display (Page 46)"** .

3.Saving the Settings File

Making a backup of the AP software settings file has the following benefits :

- If you have more than one AP and all APs have the same settings, you just need to setup one AP then use the resulting settings file for the other APs. (However, as this sets the same IP address for all APs, you need to change the IP address separately.)
- The old settings can be restored easily if a fault causes the settings file to be erased.

The settings file is stored the AP memory with the following file name.

File name … CONFIG

If the MAC address filtering is used, its setting file should also be saved. The setting file is stored in memory on the AP with the following file name：

MAC address filtering … MACFIL

The file is in the memory even when the MAC address filtering function is not in use it, however, does not have to be saved.

1. Using FTP to Backup the Settings File

To collect configuration files using FTP, follow step 1 to 6 below.

1. Move to the folder in which you wish to save the file.
2. Run FTP to log in to the AP.
3. Run FTP to log in to the AP. (Enter FTP user's name)
4. Run FTP to log in to the AP. (Enter FTP password)
5. Transfer the settings file (CONFIG). MACFIL is also transferred if necessary.
6. Exit FTP.

The following is an example for the time when Windows Command Prompt (MS-DOS Prompt) is used.

In this example, the file will be moved to the saving folder D : ¥tmp and CONFIG and MACFIL will be collected after connecting to the product via FTP. The example assumes the IP address as 192.168.0.1.

C:¥>cd D:¥tmp	.....	1
D:¥tmp>ftp 192.168.0.1	.....	2
User (192.168.0.1:none):admin	.....	3
Password:pass	.....	4
ftp>get CONFIG	.....	5
ftp>get MACFIL	.....	5
ftp>bye	.....	6

* For details about downloading using a Web browser, see the section titled **"Setup and Status Display (Page 46)".**

4.Restoring the Software Settings

The software settings of this product can be recovered by using the saved setup file.

1. Using FTP to Restore the Settings

Follow the procedure below to recover the software settings using FTP.

1. Move to the folder with file.
2. Run FTP to log in to the AP.
3. Run FTP to log in to the AP. (Enter FTP user's name)
4. Run FTP to log in to the AP. (Enter FTP password)
5. Transfer the settings file(config). MACFIL is also transferred if necessary.
6. Issue the reset request command(command：quote rst).
7. Exit FTP.

The following is an example for the time when Windows Command Prompt (MS-DOS Prompt) is used.

In this example, the file will be moved to the folder with file D : ¥tmp and CONFIG and MACFIL will be transferred after connecting to the product via FTP. The example assumes the IP address as 192.168.0.1.

C:¥>cd D:¥tmp	.....	1
D:¥tmp>ftp 192.168.0.1	.....	2
User (192.168.0.1:none):admin	.....	3
Password:pass	.....	4
ftp>put CONFIG	.....	5
ftp>put MACFIL	.....	5
ftp>quote rst	.....	6
ftp>bye	.....	7

The reset request command shown in (6) is a command used to reboot the product. There is no problem to skip (6), stop FTP in (7) and reboot the product later.

5.Upgrading the Firmware

The AP firmware may be upgraded to resolve any bugs found in the software or to add new functions. Contact CONTEC via our web site for details of the latest firmware.

There are two ways to upgrade the version of the firmware : FTP; and Access Point Manager with a Web setup screen.

1. Performing an Upgrade Using FTP

Follow the procedure below for the firmware version up settings using FTP.

1. Move to the folder with file.
2. Run FTP to log in to the AP.
3. Run FTP to log in to the AP. (Enter FTP user's name)
4. Run FTP to log in to the AP. (Enter FTP password)
5. Change the transfer mode to binary.
6. Transfer the firmware file FIRMWARE.BIN.
7. Issue the reset request command (quote rst).
8. Exit FTP.

The following is an example for the time when Windows Command Prompt (MS-DOS Prompt) is used.

In this example, the firmware file for version up will be moved to the folder with file D : ¥tmp and FIRMWARE.BIN will be transferred after connecting to the product via FTP. The example assumes the IP address as 192.168.0.1.

```
C:¥> cd D:¥tmp ..... 1
D:¥tmp>ftp 192.168.0.1 ..... 2
User (192.168.0.1:none):admin ..... 3
Password:pass ..... 4
ftp>bin ..... 5
ftp>put FIRMWARE.BIN ..... 6
ftp>quote rst .....7
ftp>bye .....8
```

* For details about downloading using a Web browser, see the section titled **"Setup and Status Display (Page 46)"**.

⚠ CAUTION

The setup file data and firmware data may be damaged and the product may not operate properly if it is rebooted or switched off while the firmware is still being updated (data being written).

6.Initialization

There are two ways to initialize this product (recovering the factory settings).

- Using a Web browser
- Using the INIT switch of the main unit

Each initialization method is described below.

1. Using a Web Browser

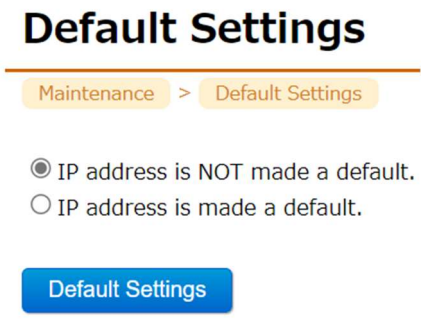
Follow the procedure below when using Web browser to initialize the product.

1 Log in to the machine using a web browser.

2 Select “Maintenance” - “Default setting” from the menu.

3 To leave the IP address of the product unchanged without initialization, tick “Do not set IP address to default”. To initialize the IP address, tick “Set IP address to default” and then click “Default Settings”.

4 Click “Save/Reboot” on the menu to save the default setting and reboot the product.



⚠CAUTION

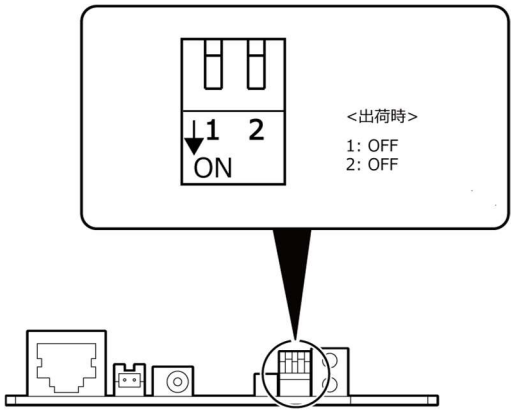
Even when the default settings are restored, they are not saved to the device's configuration file, so you must save and restart to reflect the settings.

Do not turn off the machine during startup, restart, or initialization. Doing so may cause the machine to stop operating normally.

2. Using the DIP Switch of the Main Unit

Follow the procedure below when using the DIP Switch of the Main Unit to initialize the product.

There is an DIP Switch on the side of the machine. Use a thin, non-conductive rod to initialize the settings as described below.



1 The LEDs of POWER, LAN and WLAN continue to blink for a little while after DIP switch 1 is turned off.

2 Release this button after the LED starts flashing but before it reverts to an ON state (an interval of approx. 3 seconds).

3 All the settings are restored to the default settings after the product is started next time.

⚠ CAUTION

The flashing continues for a little while after the product is switched off during initialization by switching on and off the INIT switch No.1. This indicates internal memory files are being deleted. The internal memory files may be damaged and the product may not start up properly if the power is switched off before the flashing stops. Always reboot the product after the flashing stops.

When you're in trouble

It explains the causes of faults and problems, how to handle them, and how to check them.

1.Troubleshooting

If any problem occurs during use, follow the procedure below.

1. When Communication Fails

◆ Check wired LAN communication

Check the wired LAN communication between this product and the connected PC.

- Check that the LAN cable is connected correctly.
- Check if the IP addresses and subnet masks of the product and PC are set correctly.
- The communication with this product is not possible unless the TCP/IP protocol is installed in the PC.

◆ Check wireless LAN communication

If no problem is detected in the wired LAN communication between the product and PC, check the wireless LAN communication between the product and access point.

- The FLEXLAN series is designed to handle a variety of operating formats, and requires software setting for each type of operation. Check that the settings are appropriate for the type of operation, and check the format in which communication is being attempted.
- The terminals that cannot communicate with each other may have the same ESSID. Two terminals with the same ESSID cannot communicate with each other.
- Check whether the wireless link mode has been set correctly. The wireless link mode of the station (slave station) must support the wireless link mode set on this product.
- Check whether communication is restricted by security functions such as the MAC address filtering.
- Check whether the data encryption setting is the same as that of the recipient.
- Communication cannot be performed while data encryption is being switched between ON (enabled) and OFF (disabled).

◆ Check the peripheral environment and place of installation

A nearby source of electromagnetic interference can prevent communication. In general locations (excluding factories) the following may be sources of electromagnetic emissions.

- Wireless network not conforming to wireless LAN.
- When using by 2.4GHz band, electric devices which give off 2.4GHz band electric wave - microwave oven, security gate (it is an antitheft gate in the shop), copy machine and so on.

Most electromagnetic sources other than wireless networks are local and not continuous, and therefore by moving the location of the unit and waiting briefly, communication may be possible.

Sometimes communication is hindered by attenuation of electric waves. Attenuation occurs naturally as distance from the source of transmission increases, but may also be caused by objects in the path of the transmission. The objects primarily responsible for attenuation are the following.

- Concrete walls
- Metallic surfaces around this product

2. Setup Screen Unavailable on Web Browser

Check if communication is possible between the product and PC.

If no problem is detected in the communication between the product and PC, it may be related to the browser settings. For the browser settings, see **"Connection to Devices and Setup Methods (Page 39)"**.

3. Does not start

◆ Check the LED

- Check whether the "POWER" LED is illuminated. If it is not illuminated, check the power cable and make sure that it is connected correctly to the power jack and the socket.
- Check whether the Power LED is flashing. If the power LED is still flashing more than 5 minutes after the power is switched on, the problem may be an AP firmware failure.
  In this case, the problem may be a startup error caused by corrupt data in the memory of this product.
  If you cannot restore it, contact your retailer.

◆ Check the power

- If using an AC adapter, check that the adapter is an optional accessory of a type specified by CONTEC. Only use AC adapters specified by CONTEC with this product.

- If supplying power from the power connector, check the power supply connection, supply voltage, etc., and make sure that there are no problems. For details about connecting the power supply, see **"Power Supply (Page 36)".**

Appendix

This section lists the specifications and the physical dimensions of the product, and the details of model name.

1.Hardware Specifications

1. Hardware Specifications

Function Specifications

Item			Description
Unit Type			Single Station/Access point/Repeater/ Dual Station/Mesh
Wired LAN			
	Ethernet standard		IEEE802.3 (10BASE-T), IEEE802.3u (100BASE-TX), IEEE802.3ab (1000BASE-T), IEEE802.3af
	Port Speed/Type/Port Number		10/100/1000Mbps / Half Duplex, Full Duplex / 1
Wireless LAN			
	5GHz/6GHz		
		Wireless Standard	IEEE802.11ax, IEEE802.11ac, IEEE802.11n, IEEE802.11a
		Band Width	20/40/80/160MHz
		The Number of Connectable Devices	512
		Channel	5GHz: 25ch(36, 40, 44, 48ch[W52], 52, 56, 60, 64ch [W53], 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144ch [W56] 149, 153, 157, 161, 165ch [W58]) 6GHz: 24ch(1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93ch)
		Data transmission speed *1 IEEE802.11ax	2402 - 0.9Mbps [MCS0 -11, 0.8us/1.6us/3.2us GI]
		Data transmission speed *1 IEEE802.11ac	866 - 7.2Mbps [MCS0 - 9, Short/Long GI]
		Data transmission speed *1 IEEE802.11n	300 - 6.5Mbps [MSC0 - 15, Short/Long GI]
		Data transmission speed *1 IEEE802.11a	54, 48, 36, 24, 18, 12, 9, 6Mbps
	2.4GHz		
		Wireless Standard	IEEE802.11ax, IEEE802.11n, IEEE802.11b, IEEE802.11g
		Band Width	20/40MHz
		The Number of Connectable Devices	128
		Channel	11ch (1 - 11)
		Data transmission speed *1 IEEE802.11ax	574 - 0.9Mbps [MCS0 -11, 0.8us/1.6us/3.2us GI]
		Data transmission speed *1 IEEE802.11n	300 - 6.5Mbps [MSC0 - 15, Short/Long GI]
		Data transmission speed *1 IEEE802.11g	54, 48, 36, 24, 18, 12, 9, 6Mbps
		Data transmission speed *1 IEEE802.11b	11, 5.5, 2, 1Mbps
	Security		
		IEEE802.11ax/ac/n	WPA(AES), WPA2(AES), WPA3, WPA3 192bit, WPA-PSK(AES), WPA2-PSK(AES), WPA3-SAE, WSL(combination mentioned above are possible)
		IEEE802.11a/b/g	WEP(Open/Shared Key) *2, WPA(AES, TKIP), WPA-PSK(AES,TKIP),

Item	Description
	WPA2(AES, TKIP), WPA2-PSK(AES,TKIP), WPA3, WPA3 192bit, WPA3-SAE, IEEE802.1X(EAP-TLS, PEAP), WSL(combination mentioned above are possible)
Antenna	Dipole Antenna x2 MIMO
External Dimensions (mm)	60.0(W) x 89.2(D) x 17.9(H)
Weight	100g

*1 These are theoretical values based on their respective wireless LAN standards; they do not indicate actual data transfer rates.

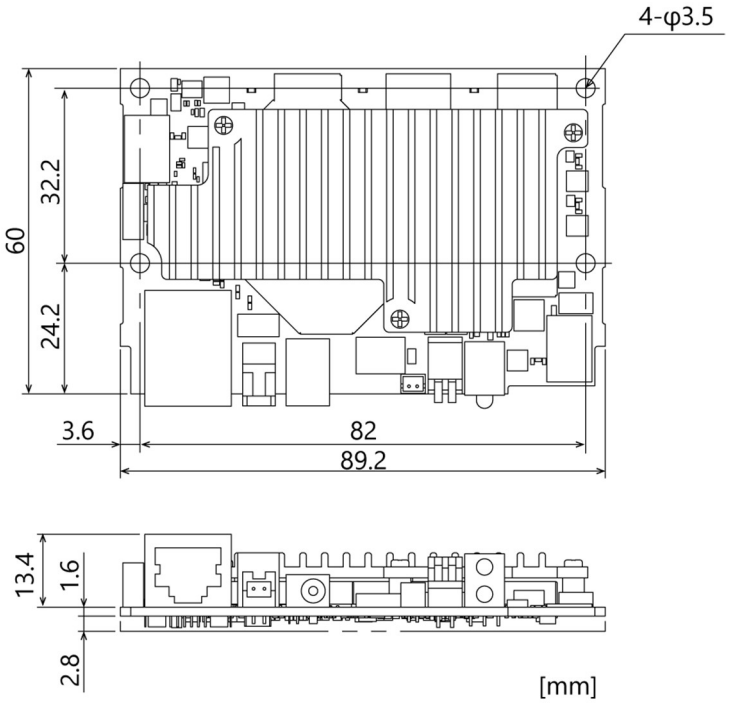
*2 WEP encryption for access points only.

Environment Requirements

Item		Description
Input voltage range		5VDC±5% (DC Jack), 5 - 30VDC±5% (Power Connector)
Rating input current		1.87A(5V DC input), 0.78A(12V DC input), 0.39A(24V DC input), 0.32A(30V DC input)
Operating ambient temperature	DC input	-20 - +40°C (without wind) -20 - +45°C (with air flow 0.6m/s)
Operating ambient humidity		10 - 90%RH (No condensation)
Floating dust particles		Not extreme
Corrosive gases		None
Line-noise resistance *1	Line noise	AC Power Line /±2kV (IEC61000-4-4 Level 3, EN61000-4-4 Level 3), Signal Line /±1kV (IEC61000-4-4 Level 3, EN61000-4-4 Level 3)
	Static electricity resistance	Touch /±4kV (IEC61000-4-2 Level 2, EN61000-4-2 Level 2), Air /±8kV (IEC61000-4-2 Level 3, EN61000-4-2 Level 3)
Vibration resistance	Sweep resistance	10 - 57Hz /semi-amplitude vibration 0.035mm, 57 - 150Hz/0.5G 40minutes each in X, Y, and Z directions (JIS C60068-2-6-compliant, IEC60068-2-6-compliant)
Shock resistance		10G half-sine shock for 11ms in X, Y, and Z directions (JIS C 60068-2-27 –compliant, IEC 60068-2-27 -compliant)
Permitted transient power failure		17ms or less (100VAC@25°C) An automatic reset is performed when low voltage is detected.
Standard		FCC Class A, UL

*1 Check with optional AC adapter FX-AC053.

2.Physical Dimensions



3.Differences from FXE3000-US

Title	FXE5000-US	FXA3000-US
Unit Type	Single Station/Access point/Repeater/ Dual Station/Mesh	Access point/ Station /Repeater
Wired LAN		
Ethernet standard	IEEE802.3(10BASE-T), IEEE802.3u(100BASE-TX), IEEE802.3ab(1000BASE-T), IEEE802.3af	IEEE802.3(10BASE-T), IEEE802.3u(100BASE-TX), IEEE802.3af
Port Speed/ Type/Port Number	10/100/1000Mbps/Half Duplex, Full Duplex/1	10/100Mbps/Half Duplex, Full Duplex/1
Wireless Standard	IEEE802.11ax, IEEE802.11ac, IEEE802.11n, IEEE802.11a, IEEE802.11b, IEEE802.11g	IEEE802.11n, IEEE802.11a, IEEE802.11b, IEEE802.11g
IEEE802.11ax		
Channel	2.4GHz : 11ch(1-11ch) 5GHz : 25ch(36, 40, 44, 48ch, 52, 56, 60, 64ch, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144ch, 149,153,157,161,165ch) 6GHz: 24ch(1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93ch)	-
Data transmission speed	2402 - 0.9Mbps[MCS0 -11, 0.8us/1.6us/3.2us GI]	-
IEEE802.11ac		
Channel	5GHz: 25ch(36, 40, 44, 48ch, 52, 56, 60, 64ch, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144ch, 149,153,157,161,165ch)	-
Data transmission speed	866 - 7.2Mbps[MCS0 - 9, Short/Long GI]	-
Security	IEEE802.11ax/ac/n : WPA(AES), WPA2(AES), WPA3, WPA3 192bit, WPA-PSK(AES), WPA2-PSK(AES), WPA3-SAE, WSL(combination mentioned above are possible)	IEEE802.11n : WPA(AES), WPA2(AES), WPA-PSK(AES), WPA2-PSK(AES), WSL(combination mentioned above are possible)
	IEEE802.11a/b/g : WEP(Open/ Shared Key /Auto), WPA(AES, TKIP), WPA-PSK(AES,TKIP), WPA2(AES, TKIP), WPA2-PSK(AES,TKIP), WPA3, WPA3 192bit, WPA3-SAE, IEEE802.1X(EAP-TLS, PEAP), WSL(combination mentioned above are possible)	IEEE802.11a/b/g : WEP(Open/ Shared Key /Auto), WPA(AES, TKIP), WPA-PSK(AES,TKIP), WPA2(AES, TKIP), WPA2-PSK(AES,TKIP), IEEE802.1X(EAP-TLS, PEAP), WSL(combination mentioned above are possible)

Title	FXE5000-US	FXA3000-US
Input voltage range	5VDC±5% (DC Jack), 5 - 30VDC±5% (Power Connector),	
Rating input current	1.87A (5VDC input), 0.78A (12VDC input), 0.39A (24VDC input), 0.32A (30VDC input),	0.83A (5VDC input), 0.15A (30VDC input) (Max.), 0.13A (PoE 48V)
Operating ambient temperature	-20 - +40℃ / 10 - 90%RH(without wind) -20 - +50℃ / 10 - 90%RH(with air flow 0.6m/s)	0 - 40°C

List of Optional Products

This section lists optional items that can be used along with the product.

1.Optional Products

Optional product items are as follows:

Acquire them as required.

Item	Model	Description
AC adapter *1	FX-AC053	AC adapter (5VDC, 3A)

* Since FX-AC053 is a product for Japan, it may not be usable outside of Japan.

Visit the CONTEC website for the latest optional products.

Website https://www.contec.com/

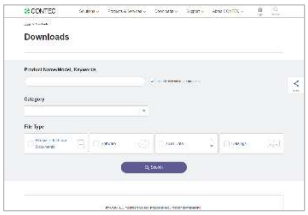
Customer Support and Inquiry

CONTEC provides the following support services for you to use CONTEC products more efficiently and comfortably.

1.Services

CONTEC offers the useful information including product manuals that can be downloaded through the CONTEC website.

Download



https://www.contec.com/download/

You can download updated device driver, firmware, and differential manuals in several languages. Membership registration (myCONTEC) is required to use the services.

Revision History

MONTH YEAR	Summary of Changes
January 2025	The First Edition

CONTEC CO., LTD. 3-9-31, Himesato, Nishiyodogawa-ku, Osaka 555-0025, Japan

https://www.contec.com/

FXE5000-US Reference Manual

NA10612 (LXEK171) [01262025] January 2025 Edition