Wireless Presentation Box

Z-1

User's Manual

(Configuration Method)

silex technology

WA105980XX

Index

(Blank page)

1. Introduction

Thank you for purchasing the Wireless Presentation Box "Z-1". This manual provides information on how to configure and use Z-1. Please read the **1-2. Safety Instructions** carefully before using Z-1.

1-1. Introduction

About the notation

This manual uses the following symbols to indicate specific information for operating Z-1. Be sure to carefully review before using Z-1.


TIP : This symbol indicates important information that needs to be observed when operating Z-1. Make sure to read this information for safe and proper use.


Note : This symbol indicates information that is useful when using Z-1. If you experience difficulties operating Z-1, please refer to this information first.

Disclaimers

- The unauthorized transfer or copying of the content of this manual, in whole or in part, without prior written consent is expressly prohibited by law.
- The content of this manual is subject to change without notice.
- This manual was prepared to accurately match the content of each OS, but the actual information shown on the computer monitor may differ from the content of this manual due to future OS version upgrades, modifications, and other changes.
- Although every effort was made to prepare this manual with the utmost accuracy, Silex Technology will not be held liable for any damages as a result of errors, setting examples, or other content.

Trademarks

- AMC Manager® is a registered trademark of Silex Technology.
- Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Mac, Mac OS, AirPlay are registered trademarks of Apple Inc. in the United States and/or other countries.
- iOS is a trademark or registered trademark of Cisco in the United States and other countries.
- Google, Google logo, Google Chrome, Android, Chromecast are trademarks or registered trademarks of Google Inc.
- HDMI, HDMI logo and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing,LLC.
- Ethernet is a registered trademark of Xerox Corporation.
- Wi-Fi is a registered trademark of Wi-Fi Alliance.
- WPA and WPA2 are trademarks or registered trademarks of Wi-Fi Alliance.
- Other company names and product names contained in this manual are trademarks or registered trademarks of their respective companies.

1-2. Safety Instructions

This page provides the safety instructions for safe use of Z-1.
To ensure safe and proper use, please read the following information carefully before using Z-1.

<Indication of the warning>

	Warning	"Warning" indicates the existence of a hazard that could result in death or serious injury if the safety instruction is not observed.
	Caution	"Caution" indicates the existence of a hazard that could result in serious injury or material damage if the safety instruction is not observed.

<Meaning of the symbols>

	This symbol indicates the warning and caution. (Example:  "Danger of the electric shock")
	This symbol indicates the prohibited actions. (Example:  "Disassembly is prohibited")
	This symbol indicates the actions users are required to observe. (Example:  "Remove the AC plug from an outlet")

<Installation>

Warning	
	• Do not place anything on top of the product. Also, do not place the product on top of the other product. Failure to do so may cause fire, electrical shock, malfunction or performance degradation. • Do not cover up the product with a cloth such as blanket or table cloth. The heat remains inside and it may cause fire or malfunction.

Caution	
	• Do not use or store the product under the following conditions. It may cause malfunction. - Locations subject to vibration or shock - Shaky, uneven or tilted surfaces - Locations exposed to direct sunlight - Humid or dusty places - Wet places (kitchen, bathroom, etc.) - Near a heater or stove - Locations subject to extreme changes in temperature - Near strong electromagnetic sources (magnet, radio, wireless device, etc.) • When installing the product to a high position, make sure that the product is firmly fixed so it does not drop for weight of the cables.

<Safe handling>

Warning	
	• Do not move the product when the AC adaptor is connected to it. The cable of AC adaptor may be damaged, and which may result in fire or electric shock. • For use of the devices connected to the product, please follow all warnings, cautions and notices given by that manufacturer and carefully use them in a proper manner. Failure to follow these instructions may cause fire, electrical shock or malfunction. • If a ground wire is supplied with your device to use with, connect it to the ground terminal in order to prevent an electrical shock. Do not connect the ground wire to gas pipe, water pipe, lighting rod or telephone ground wire. It may cause malfunction.

Caution	
	• The product may become hot when it is in use. Be careful of the heat when moving or removing the product.

<Handling of malfunctioned units>

Warning	
	• In the following cases, turn off the connected devices and unplug the AC plug of the product from a power outlet. Failure to follow these instructions may cause fire or an electrical shock. - When the product emits a strange smell, smoke or sound or becomes too hot to touch. - When foreign objects (metal, liquid, etc.) gets into the product. - When the product is dropped or the case is broken or cracked.

<Ventilation>

Warning	
	• Do not cover up the vents on the product. The temperature inside may rise and cause fire or malfunction.

<Disassembly / Modification>

Warning	
	• Do not disassemble or modify the product. It may cause fire, electrical shock or malfunction. • Do not disassemble or modify the AC adaptor that comes with the product. It may cause fire, electrical shock or malfunction.

<Power supply>

Warning	
	• Use the correct power voltage. Improper voltage may cause fire or an electrical shock.

Caution	
	• Always use the AC adaptor supplied with the product. Other AC adaptors may cause malfunction. • When the product will not be used for a long period of time, unplug the power cables of the product and other devices.

<Use of AC adaptor and AC cord>

Warning	
	• Do not place any objects on top of AC adaptor, and do not cover it up with anything. Also, do not use the AC adaptor on top of the heat/moisture retaining materials (carpet, sponge, cardboard, styrofoam, etc.). The accumulated heat may result in fire or malfunction. • Do not roll up or wrap the AC cord. It may cause fire or an electrical shock. • Do not plug or unplug the AC adaptor or any other cables with wet hands. It may cause an electrical shock or malfunction. • Keep the cords and cables away from children. It may cause an electrical shock or serious injury.

Caution	
	• Do not place anything on top of the cables, and do not bend, twist and stretch the cables by force. • Do not use the cables or AC cords at a place where someone may trip over them. It may cause serious injury. • Do not pull on the cord to disconnect the plug from the power supply. The code may be broken, which could result in fire or an electrical shock. • Verify all codes or cables are plugged correctly before using the product. • When removing the product, disconnect the AC plugs of both the product and the other device you are using with.

1-3. Product Information and Customer Services

Product Information

The services below are available from the Silex Technology website. For details, please visit the Silex Technology website.

Silex Technology website
(URL) **https://www.silextechnology.com/**

- Latest firmware download
- Latest software download
- Latest manual download
- Support information (FAQ)

Customer Support Center

Customer Support is available by e-mail or telephone for any problems that you may encounter. If you cannot find the relevant problem in this manual or on our website, or if the corrective procedure does not resolve the problem, please contact Silex Technology Customer Support.

Contact Information		
USA	+1-657-218-5199	support@silexamerica.com
Europe	+49-2154-88967-0	support@silexeurope.com

Note

- Refer to the Silex Technology website (**https://www.silextechnology.com/**) for the latest FAQ and product information.

(Blank page)

2. Product Specification

2-1. Features

Z-1 is specialized for small to medium sized conference rooms, and shares presentations from not only PC but also tablets and smartphones over a wireless LAN.

Wireless LAN standards IEEE802.11n/a/b/g/ac

- The wireless features support Access Point (AP) mode and Station (STA) mode.
- 802.1X authentication is supported for office networks.

Multiple OS (Windows, Android, iOS, Mac OS)

- The designated projection tool "AMC Meeting" allows the user to mirror Windows and transmit audio. The tool does not require installation or the administrator authority.
- AirPlay, one of iOS and MacOS standard functions, is supported for mirroring and audio transmission.
- Google Cast is supported for standard mirroring and audio transmission from Android OS.

Various projection modes

- Single Presenter mode shows a presentation sent by one user in full screen.
- Multi-Presenter mode can split the screen up to 4. (Only one of windows can play videos, and the window can be changed with a drag-drop action.)
- Distribution mode sends a Z-1 main screen to up to 16 devices.
- Pair Display mode enables two units of Z-1 to send their screens each other to display them together.

Device server function exclusive to HID (keyboards & mice)

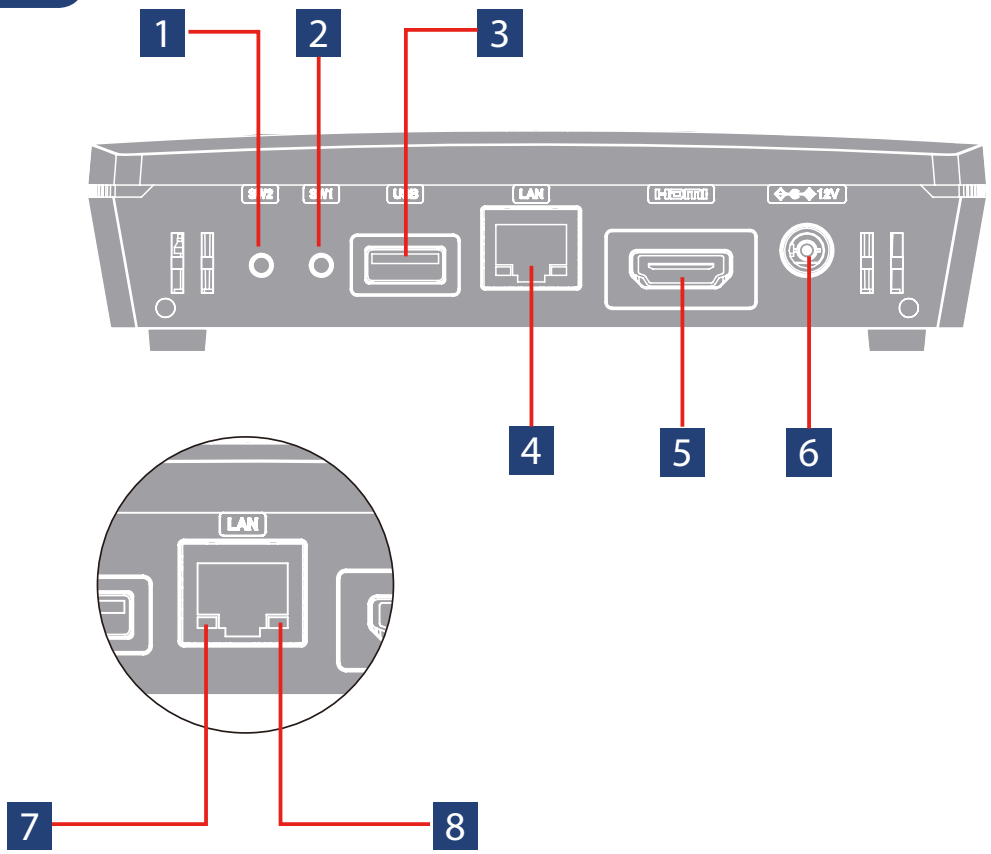
- The user can draw images on the projected screen with a USB mouse connected to Z-1. Since Z-1 enables drawing when the image is not projected, Z-1 can be used as an interactive whiteboard.
- When a USB mouse and a USB keyboard are connected to Z-1 via a USB hub, Z-1's basic settings can be updated on the OSD.

Comprehensive management software: AMC Manager® Free (free license) & AMC Manager® (non-free license)

- AMC Manager® allows the user to remotely operate and monitor Z-1, change the settings, assign IP addresses, and upgrade the firmware for multiple Z-1 at once.
- For details of AMC Manager®, see silex technology's website.

2-2. Parts and Functions

Front



1 Function switch (SW2)
Push to:
- Change the projection modes
- Apply Smart wireless setup (push button control)

2 Reset switch (SW1)
Push to reset Z-1 to the factory default settings.

3 USB port
Connect a USB mouse or a USB keyboard.
Use a USB hub to connect them both.

4 LAN port
Connect a LAN cable.

5 HDMI port
Connect an HDMI cable.

6 DC jack
Connect the included AC adapter.

7 LINK LED

Shows the wired LAN connection status.

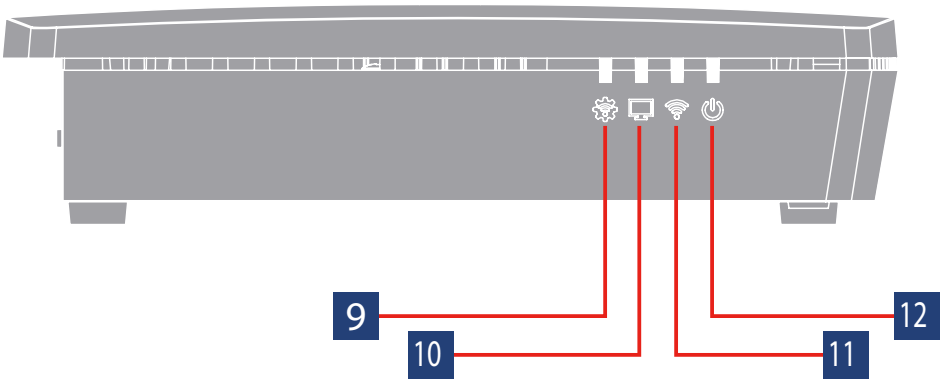
Color	Light	Description
Green	Solid on	The wired LAN is being connected.
	Blinking	The wired LAN is not connected.

8 STATUS LED

Shows the packet reception state of the LAN cable.

Color	Light	Description
Yellow	Blinking	It turns on when Z-1 receives a packet. It turns off in 100 milliseconds.

Side



9 STATUS LED

Gives the operation information of Z-1.

Color	Light	Description
None	Off	Regular state
Blue	Solid on	Smart wireless setup has been successfully done. (Turns off in three minutes)
	Blinking (2-second cycle)	Smart wireless setup is being applied.
Red	Solid on	Smart wireless setup has failed. Timeout / Overlapping (Turns off in three minutes)
	Blinking (100-millisecond cycle)	Smart wireless setup has failed. Other errors (Turns off in one minute)
	Blinking (2-second cycle)	The firmware is being updated.

10 DISPLAY LED

Shows the output state of videos.

Color	Light	Description
None	Off	A display (HDMI cable) is not connected.
Purple	Solid on	A 4K monitor (3840 x 2160) is connected and the video data is being sent.
Blue	Solid on	A 2K monitor (1920 x 1080) is connected and the video data is being sent.
Red	Solid on	A 720p monitor (less than 2K) is connected and some functions are limited.

11 WLAN LED

Shows the wireless LAN state.

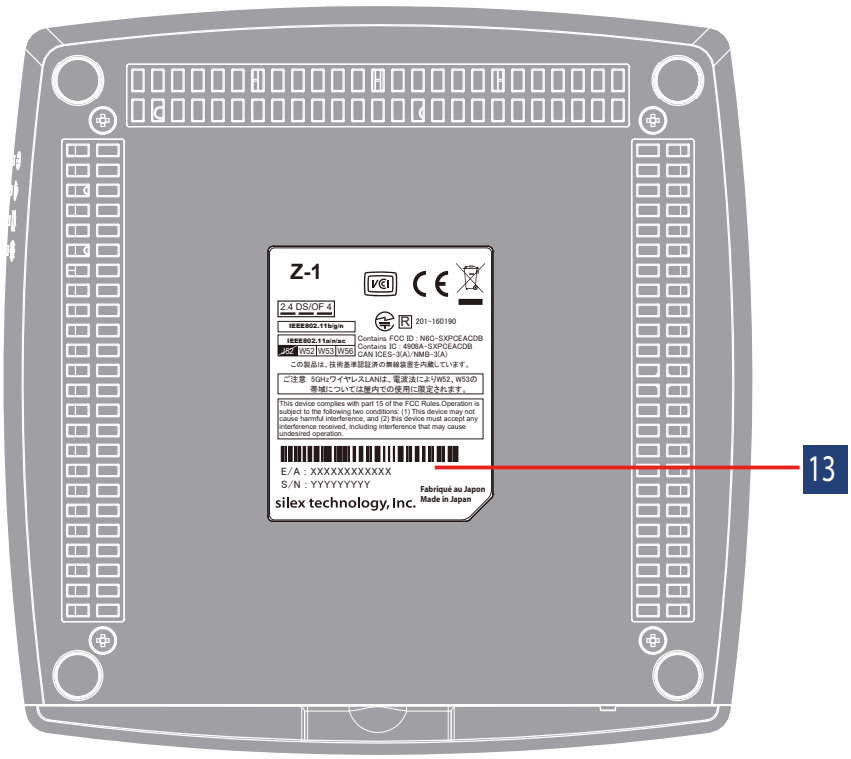
Color	Light	Description
None	Off	Wired-only mode or Smart wireless setup is being applied.
Blue	Solid on	Access point mode is operating.
	Blinking	Wireless packets are sent or received in Access point mode. Turns off in 100 milliseconds.
Purple	Solid on	Station mode is on and the wireless LAN has been connected.
	Blinking	Wireless packets are sent or received in Station mode. Turns off in 100 milliseconds.
	Blinking (2-second cycle)	A specified access point is not connected in Station mode.
Red	Blinking	DFS is working in Access point mode.

12 POWER LED

Shows the power state.

Color	Light	Description
Blue	Solid on	The power is on.
Red	Blinking	Power feeding has been suspended because of USB overcurrent detected.

Bottom



13 Product label
Shows Ethernet address (E/A) of the Z-1.

2-3. Specifications

2-3-1. Hardware Specifications

Memory	SDRAM	1 GByte	
	FlashROM	128 MBytes	
USB interface	USB2.0 Hi-Speed port (type A): 1 port Full-Speed mode, Low-Speed mode USB bus power: max. 500 mA		
Display interface	HDMI terminal: 1 port		
Display interface	Reset switch	1 (front)	
	Function switch	1 (front)	
LED lamp	LAN port	2 lights	Link (green)
			Status (yellow)
	Side	4 lights	POWER (blue/red)
			WLAN (blue/red)
			DISPLAY (blue/red)
			STATUS (blue/red)

Wired network interface	1000BASE-T / 100BASE-TX (auto-negotiation): 1 port		
Wireless network interface	IEEE802.11a	Frequency	5 GHz band
		Transmission	OFDM
		Tx speed	6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M
		Channel	[US] W52 : 36, 40, 44, 48 W53 : 52, 56, 60, 64 W56 : 100, 104, 108, 112, 116, 132, 136, 140 W58 : 149, 153, 157, 161, 165 [EU] W52 : 36, 40, 44, 48 W53 : 52, 56, 60, 64 W56 : 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
	IEEE802.11b	Frequency	2.4 GHz band
		Transmission	DS-SS
		Tx speed	1M, 2M, 5.5M, 11M
		Channel	[US] : 1-11Ch [EU] : 1-13Ch

Wireless network interface	IEEE802.11g	Frequency	2.4 GHz band
		Transmission	OFDM
		Tx speed	6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M
		Channel	[US] : 1-11Ch [EU] : 1-13Ch
	IEEE802.11ng HT20	Frequency	2.4 GHz band
		Transmission	DSSS-OFDM
		Tx speed	MCS0, 1, 2, 3, 4, 5, 6, 7
		Channel	[US] : 1-11Ch [EU] : 1-13Ch
	IEEE802.11na HT20 / HT40	Frequency	5 GHz band
		Transmission	OFDM
		Tx speed	MCS0, 1, 2, 3, 4, 5, 6, 7
		Channel	[US] W52 : 36, 40, 44, 48 W53 : 52, 56, 60, 64 W56 : 100, 104, 108, 112, 116, 132, 136, 140 W58 : 149, 153, 157, 161, 165 [EU] W52 : 36, 40, 44, 48 W53 : 52, 56, 60, 64 W56 : 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
	IEEE802.11ac VHT20 / VHT40 / VHT80	Frequency	5 GHz band
		Transmission	OFDM
		Tx speed	MCS0, 1, 2, 3, 4, 5, 6, 7, 8, 9
		Channel	[US] W52 : 36, 40, 44, 48 W53 : 52, 56, 60, 64 W56 : 100, 104, 108, 112, 116, 132, 136, 140 W58 : 149, 153, 157, 161, 165 [EU] W52 : 36, 40, 44, 48 W53 : 52, 56, 60, 64 W56 : 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Antenna	Built-in antenna		

Power feeding	AC adapter	AC adapter 12V +/-5%
		Rated current consumption 1500mA
Operation condition	Temperature	0°C to 35°C
	Humidity	20% to 80%RH (No condensation)
Storage condition	Temperature	-10°C to 50°C
	Humidity	20% to 90%RH (No condensation)

HDMI standard	Version	1.4b
HDMI video output	Resolutions	1280 x 720 @ 60 Hz 1920 x 1080 @ 60 Hz 3840 x 2160 @ 30 Hz

Regulatory compliance	VCCI Class A / FCC Class A / ICES Class A / CE

FCC / IC Notice

FCCID : **N6C-PCEACDB**
IC : 4908A-SXPCEACDB

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

Fcc Rules Part 15
FCC CAUTION
Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Rules, Part 15 §15.19(a)(3) / IC RSS Gen §8.4
Below sentences must be indicated on the final product which contains this module inside.
This device complies with Part 15 of FCC Rules and Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of this device.

Le présent appareil est conforme à la partie 15 des règles de la FCC et CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'appareil doit accepter tout brouillage subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

FCC Rules Part 15 Subpart C §15.247 and Subpart E / IC RSS-102 §2.6
This equipment complies with FCC/IC radiation exposure limits set forth for an uncontrolled

environment and meets the FCC radio frequency (RF) Exposure Guidelines and RSS-102 of the IC radio frequency (RF) Exposure rules. This equipment should be installed and operated keeping the radiator at least 20cm or more away from person's body.

Cet équipement est conforme aux limites d'exposition aux rayonnements énoncées pour un environnement non contrôlé et respecte les règles les radioélectriques (RF) de la FCC lignes directrices d'exposition et d'exposition aux fréquences radioélectriques (RF) CNR-102 de l'IC. Cet équipement doit être installé et utilisé en gardant une distance de 20 cm ou plus entre le radiateur et le corps humain.

FCC Rules Part 15 Subpart E §15.407(c)
Compliance with FCC requirement 15.407(c)
Data transmission is always initiated by software, which is the passed down through the MAC, through the digital and analog baseband, and finally to the RF chip. Several special packets are initiated by the MAC. These are the only ways the digital baseband portion will turn on the RF transmitter, which it then turns off at the end of the packet. Therefore, the transmitter will be on only while one of the aforementioned packets is being transmitted.
In other words, this device automatically discontinue transmission in case of either absence of information to transmit or operational failure.

FCC Rules Part 15 Subpart E §15.407(g)
Frequency Tolerance: +/-20 ppm

FCC Rules Part 15 Subpart C §15.247(g) / Subpart Etly prohibited for use with this device.

Le numéro IC du présent émetteur radio 4908A-PCEACDB a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué pour ce type, sont strictement interdits pour l'exploitation avec cet appareil.

- Antenna type
  Embedded Flex Antenna

- Model
  AS-146153

- Antenna Gain
  2.4GHz : +3.075dBi (Peak)
  5GHz : +4.75 dBi (Peak)

RSS-210
5150-5250 MHz and 5250-5350 MHz bands are restricted to indoor operations only.
High-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

La bandes 5150-5250 MHz et 5250-5350 MHz ont restreinte à une utilisation à l'intérieur seulement.
Les radars de haute puissance sont désignés comme utilisateurs principaux (c'est-à dire utilisateurs prioritaires) pour les bandes 5250-5350 MHz et 5650-5850 MHz, et que ces radars peuvent provoquer du brouillage et/ou des dommages aux dispositifs LAN-EL.

WARNING

The FCC / The Industry Canadaregulations provide that changes or modifications not expressly approved by the party responsible for compliance could void the user'sauthority to operate the equipment.

CE Notice

CE

2-3-2. Software Specifications

Wireless LAN	Mode	Access point Station	
	Access point	Authentication	OPEN Shared WPA-PSK WPA2-PSK WPA/WPA2-PSK 802.1X WPA-Enterprise WPA2-Enterprise WPA/WPA2-Enterprise
		Encryption	WEP(64/128-bit) TKIP/AES/AUTO
		Multi SSID	4
		Max number of connectable clients	100 units
		Smart wireless setup	Push switch PIN code External registrar
	Station	Authentication	OPEN Shared WPA-PSK WPA2-PSK WPA/WPA2-PSK WPA-Enterprise WPA2-Enterprise WPA/WPA2-Enterprise
		Encryption	WEP(64/128-bit) TKIP/AES
		Smart wireless setup	Push switch PIN code

Standard protocols	Network layer	ARP IP ICMP
	Transport layer	TCP UDP
	Application layer	SSH (TCP #22) BOOTP (UDP #67-68) DHCP (Client/Server) (UDP #67-68) DNS (UDP #53) / mDNS (UDP #5353) HTTP (TCP #80) / HTTPS (TCP #443) NTP (UDP #123) SMB (UDP #137 #138, TCP #139 #445) SNMP (UDP #161) Google Cast legacy discovery (UDP #1900) AirPlay (TCP #7000) AirPlay Video (TCP #7100) Google Cast (TCP #8009) DCNASP (UDP #19539) Pair Display Session (TCP #19539) SXUPTP (TCP/UDP #19540) JCP (UDP #19541) SXSMP (TCP/UDP #60000) SXSMP (TCP/UDP #60001)

2-3-3. Others

Supported USB device	HID keyboard HID mouse
Supported OS (as of Jan. 2020)	[Microsoft Windows] • Windows 8.1 (32-bit/64-bit) • Windows 10 (32-bit/64-bit) [Android] Android 6 or later [iOS] iOS 11 or later [MacOS] macOS 10.12 or later

TIP

- The software works as a desktop application on Windows 8 or later versions.
- Windows RT is not supported.
- Windows 10 S mode is not supported.
- For the latest OS support, see silex technology's web site.

2-3-4. Restrictions

This chapter describes restrictions on Z-1.

Android (Googlecast)

- Z-1 can be used only in Single Presenter mode.
- Z-1 needs to get the correct time information. Enable NTP client for synchronizing Z-1's clock.
- When Z-1 is not connected to the Internet, the client device may not able to connect correctly. Try the followings in case the connection fails.
  - Restart the client device.
  - Disable the mobile data communication on the client device.
  - If these do not help, please try to use Z-1 in an environment where the Internet connection is available.
- Z-1 does not support Streaming Playback mode (e.g. internal playback orders from Google Photo or YouTube application) which receives content from the Internet.
- Since the size of images from Android is fixed to 1,280 x 720, a black border will appear around projected images.
- Z-1 disconnects from Android devices every day at 0:00 UTC (9:00 JST) because of the update process of electronic certificates used for the connection.

AirPlay (iOS)

- Z-1 can be used only in Single Presenter mode.
- Z-1 does not support Streaming Playback mode (e.g. internal playback orders from Google Photo or YouTube application) which receives content from the Internet. Some applications use Streaming Playback mode for playing videos saved in the device but the mode is not supported by Z-1 either.

Distribution Master mode/Slave mode

- Both Master-mode and Slave-mode Z-1 have to be in the same segment (broadcast domain). Multiple Z-1 cannot be configured in Master mode in one segment.

Distribution mode for wireless communication

- Master-mode Z-1 has to be Access Point mode and Slave-mode Z-1 has to be Station mode. If Master-mode Z-1 is set to Station mode, the transmission rate of multicast packets will decrease and the video distribution will be unstable.

Exclusion from Device server function

- The OSD function or device server function of Z-1 is exclusively used. When the device server function is enabled, the OSD function is disabled and cannot be used.

Display resolutions with limited functions

- When Z-1 is connected to a display device that has a resolution of 1,920 x 1,080 or less, Z-1 is limited to Single Presenter mode for projection and cannot use the following functions:
  - OSD function (disabled)
  - Function switch (cannot switch the projection mode)

Resize screen function

- Since the resize screen function has fixed levels of magnification, a space appears in between the screen and the transmitted images depending on the size.

2-4. Radio Waves

Usage Notes

Do not use Z-1 around the following devices:

- industrial, scientific, and medical equipment such as microwave ovens and pacemakers
- Premises radio stations (radio stations requiring licenses) for RFID used for factory production lines
- Specified low-power radio stations (radio stations not requiring licenses)

The above devices share a radio frequency band with the wireless LAN. If Z-1 is used around those devices, it may create radio interference. Therefore, Z-1 may stop communicating or make slow communication.

Refrain from using mobile phones, PHS, TV, and radio players around Z-1.

Mobile phones, PHS, TV, and radio players use radio frequency bands different from the wireless LAN's radio. So, Z-1's and these devices' communications will not be interfered when these devices are used in the immediate area. When these devices, however, get near to a wireless LAN device, radio waves emitted by wireless LAN devices including Z-1 may generate noise on audio and movies.

Reinforcing bars, metal or concrete walls interrupt communications.

Z-1 can establish a communication through walls of wood and glass windows for ordinary houses. When reinforcing bars, metal and concrete materials are used on the walls or floors, radio waves do not pass through and Z-1 communication cannot be established through walls or floors.

Z-1 obtained the technical standard compliance certificate. Keep the following points in mind.

- Do not disassemble or remodel Z-1 since they are prohibited by law.
- Do not remove the technical standard compliance label. The use of unlabeled Z-1 is prohibited.

Wireless Devices in 2.4 GHz Bands

Z-1 shares a frequency band with microwave ovens, industrial, scientific, and medical equipment, premises radio stations (radio stations requiring licenses) and specified low-power radio stations (radio stations not requiring licenses) for RFID used for factory production lines.

- Make sure that premise radio stations and specified low-power radio stations for RFID do not operate nearby before Z-1 starts up.
- In the event that Z-1 causes harmful interference to any premises radio station for RFID, immediately change the frequency or halt radio wave emission, and contact silex technology, Inc. for consultation on interference avoidance measures (e.g. partition installation).
- Contact silex technology, Inc. if Z-1 causes harmful interference to any specified low-power radio stations for RFID or if other problems arise.

*Indication of the following symbols on the back of Z-1:

2.4	Represents radio equipment using the 2.4 GHz band.
DS/OF	Means the use of DS-SS and OFDM as the modulation scheme.
4	Means that the estimated distance with interference is "40m or less".
	Indicates that the equipment can use the entire band and is capable of avoiding the band used by RFID systems.

Use of 5GHz Band

- Outside use of W52 and W53 is prohibited by Radio Act. To use Z-1 outside, use only W56 channels and do not use W52/W53 channels.

2-5.DFS Function

Z-1 supports DFS (Dynamic Frequency Selection) function. When the configured channel is subject to DFS and Z-1 detects radar waves, Z-1 switches the channel to avoid radio interference with weather or other radar systems.

The user can set one alternate channel each in W53 and W56 for Z-1 to move the channel when it detects radar waves. In case no alternate channel is set or Z-1 detects radar waves again on the alternate channel, the next alternate channel will be decided with the following orders.

DFS channels (5 GHz bands)

Band	Channel bandwidth setting		Channel switching order
W53	HT20/VH20		52>56>60>64>36
	HT40/ VHT40	+	52>60>36
		-	56>64>40
	VHT80		36
W56	HT20/VH20		100>104>108>112>116>120>124>128>132>136>140
	HT40/ VHT40	+	100>108>116>124>132
		-	104>112>120>128>136
	VHT80		100>116, 104>120, 108>124>112>128, 116>100, 120>104, 124>108>128>112

TIP

- Radar waves are monitored for about one minute when Z-1 starts up or the channel is switched, and the wireless communication cannot be made while radar waves are being monitored.
  (*) The monitoring duration varies by country.
- When radar waves are detected by the DFS function on a channel, the channel cannot be used for about 30 minutes.

(Blank page)

3. Network Settings

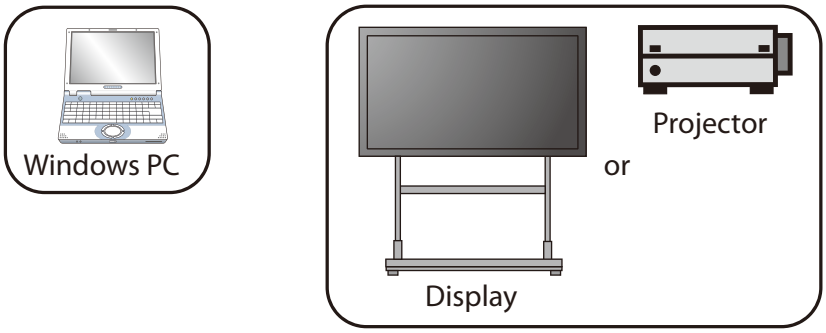
3-1. Settings from Web Page

The user can update and change Z-1's full settings using a web browser.

Note

- The web pages enable useful functions such as remote restart and factory reset. For more details, see "6-7 Maintenance Function".

3-1-1. Necessary Items

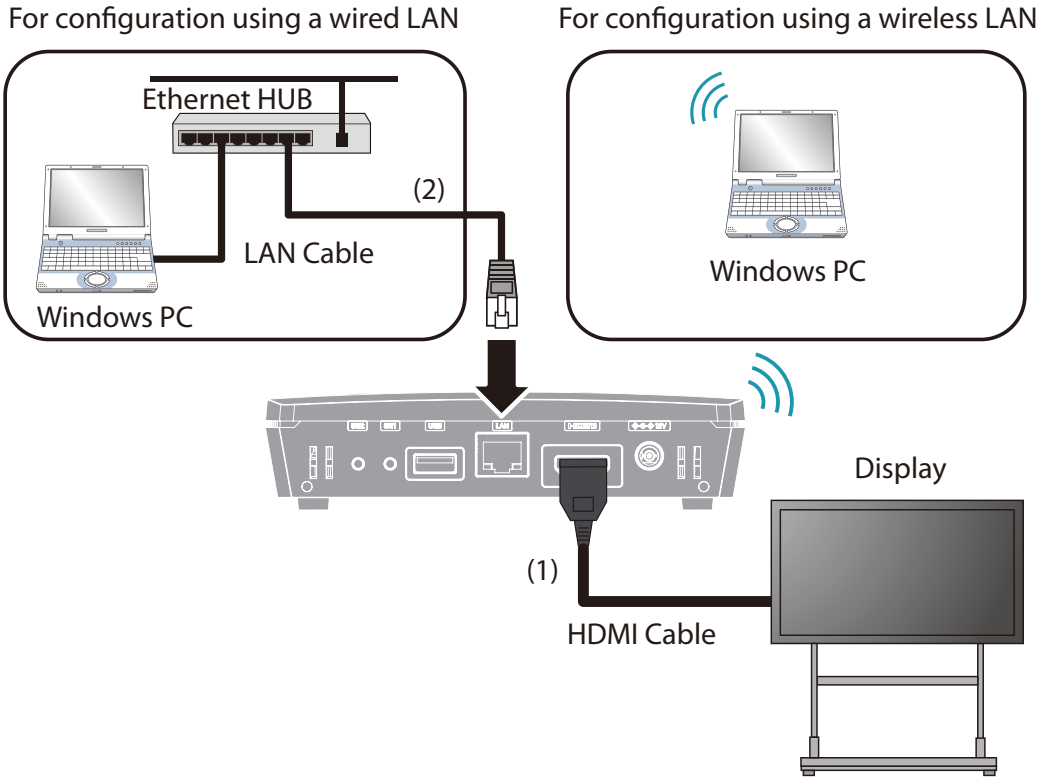


- Windows PC (Wireless PC)
- HDMI compatible display or projector
- HDMI cable
- To use a wired connection or the Access Point feature of Z-1, a LAN cable is required.

3-1-2. Connecting Display to Z-1

1. Connect the display to Z-1 using an HDMI cable and turn on the display.

2. Connect Z-1 to the PC via a wired LAN or wireless LAN.



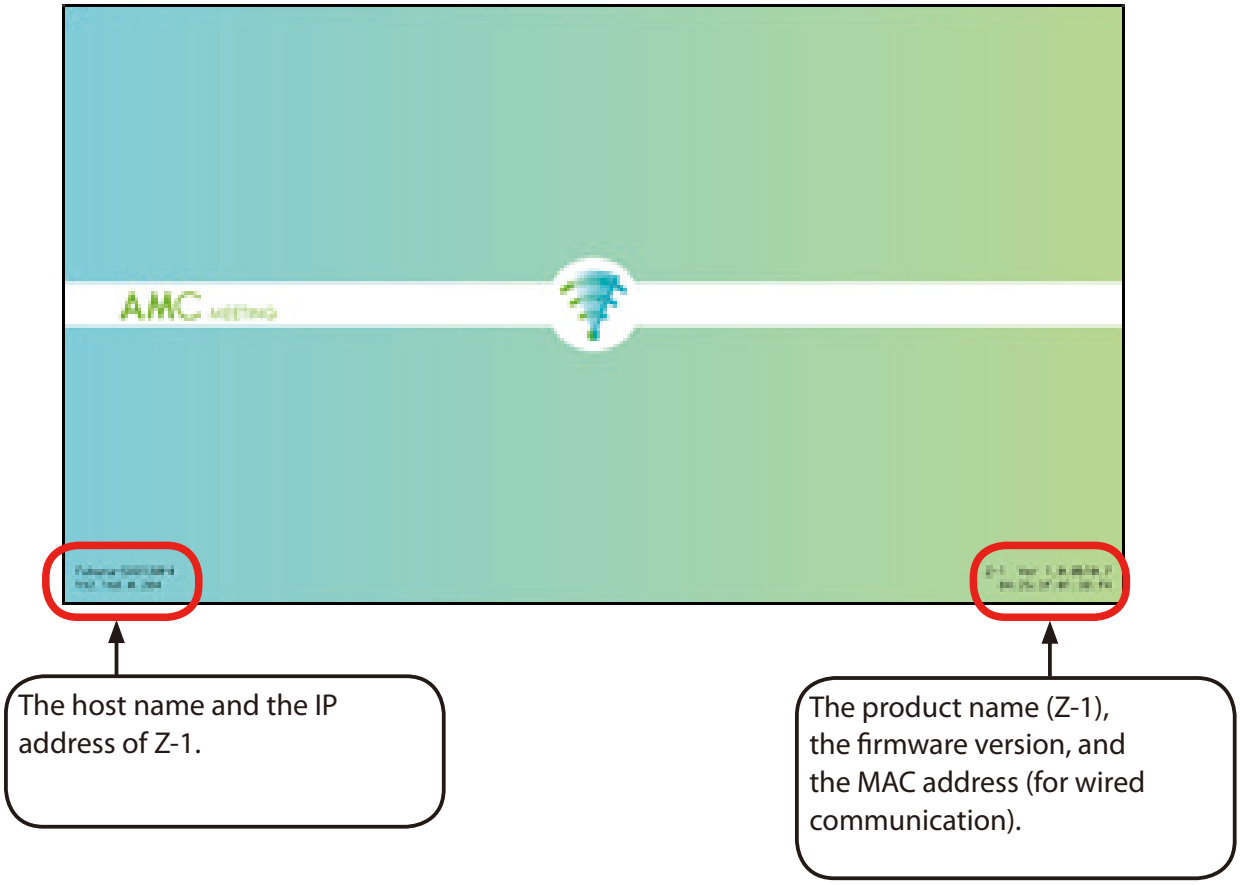
3-1-3. Turning on Z-1

1. Connect the AC adaptor and power code. Then, connect the AC adaptor to the DC jack of Z-1 and the power plug to the outlet.

TIP

- Be sure to always use the AC adaptor that comes with Z-1.

2. The standby screen is displayed on the display connected to Z-1.
When the animation in the middle of the screen stops, the power-on process is completed.



Note

- By default, Z-1 obtains an IP address using the DHCP client function. When there is no DHCP server in your environment, Z-1 will automatically use the IP address "169.254.xxx.xxx".

For configuration using a wireless LAN
Go to "3-1-4. Connecting Windows PC".

For configuration using a wired LAN
Go to "3-1-5. Web Pages".

3-1-4. Connect Windows PC

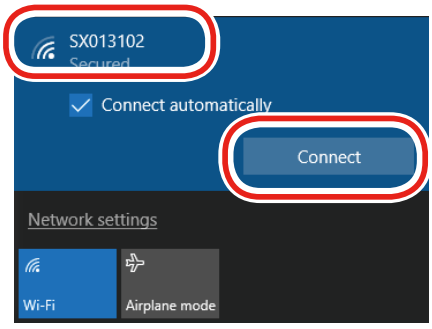
This chapter explains how to connect a Windows PC to Z-1 as a wireless client.

Note

- In the following explanation, Windows 10 is used as an example. If you are using an operating system other than Windows 10, follow the appropriate procedure for that operating system.

1. Click the network icon on the notification area (system tray) to show the wireless connection screen.

2. Select the SSID of Z-1(SXxxxxxx) from a list and click **Connect**.



Note

- "**xxxxxx**" of the SSID(SXxxxxxx) is the lower 3 bytes of the Z-1's MAC Address.
- If **Connect automatically** is checked, the PC will automatically connect to Z-1 every time it is restarted.

3. Press and hold the function switch of Z-1. When the STATUS LED blinks blue at 2 sec interval, release the switch.

4. Z-1 starts to communicate with the Windows PC, and configures the same setting to the PC. When the SETTING LED of Z-1 turns blue, the configuration is completed.

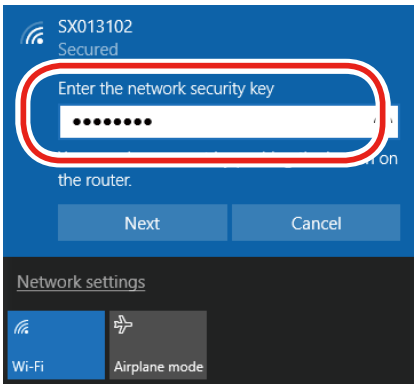
5. When a message "**Do you want to allow your PC to be discoverable by other PCs and devices on this network?**" appears, click **Yes**.

Now, the PC has connected to Z-1.

Note

- If you know the pre-shared key, it can also be used for wireless connection setup.

  Enter the pre-shared key of Z-1 in the **Enter the network security key** box and click **Next**.



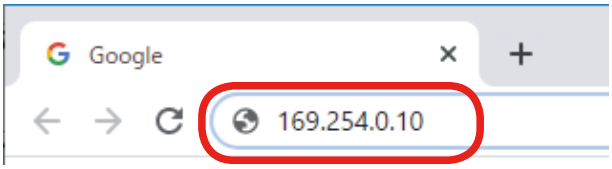
3-1-5. Web Pages

How to Access the Web Page

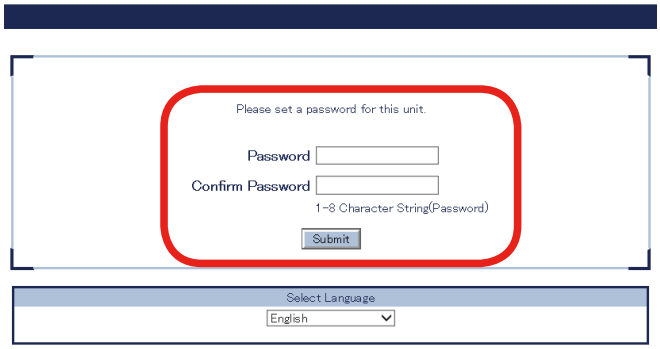
1. Start a Web browser on a computer. To the address bar of the Web browser, enter the IP address of Z-1 (the one shown on the bottom left of the standby screen) and press the Enter key.

Note

- Example) When the IP address of Z-1 is "192.254.0.10", enter it to the address bar as below.



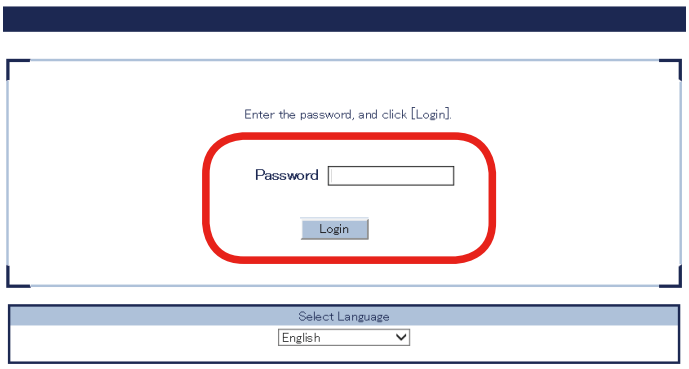
2. The Web browser will run and the login password configuration page will be displayed. Enter the password to configure for Z-1 and click **Submit**.



Note

- The login password configuration window is displayed only when Z-1 is configured for the first time.

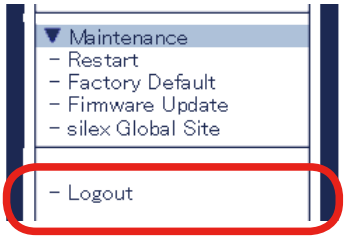
3. When the login page is displayed, enter the login password you have configured and click **Login**.



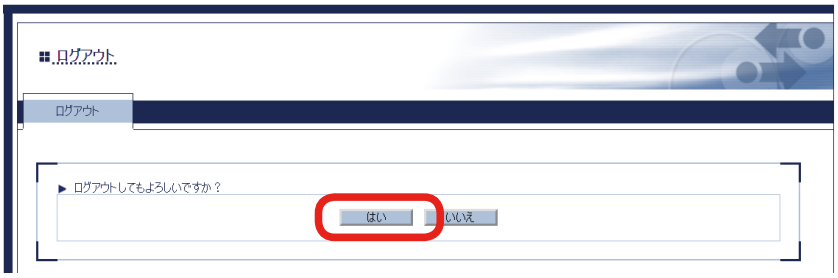
4. The web page (System Status) appears.

How to Log Out

1. Click **Logout** on the page menu.



2. The logout confirmation dialogue appears. Click **Yes**.



3. The login page will appear.

3-1-6. How to Update Settings from Web

The network settings can be updated from the basic or other settings page.

General Configuration

s can be updated including settings for the TCP/IP, wireless LAN, and the DHCP server.

Detailed settings

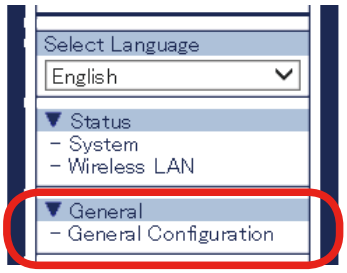
The following items can be updated in detail from corresponding setting pages.

Item	Detail
Product Configuration	TCP/IP communication settings
Wireless LAN Configuration(AP)	For AP use in wireless LAN
Wireless LAN Configuration(STA)	For STA use in wireless LAN
Wired LAN Configuration	Wired LAN interface settings
VLAN Configuration	VLAN ID setting for Wireless LAN SSID
NTP Configuration	Settings to get the current time through a network.
Display Configuration	For video functions

Network Basic Settings

Go to the basic setting page and update the network settings.

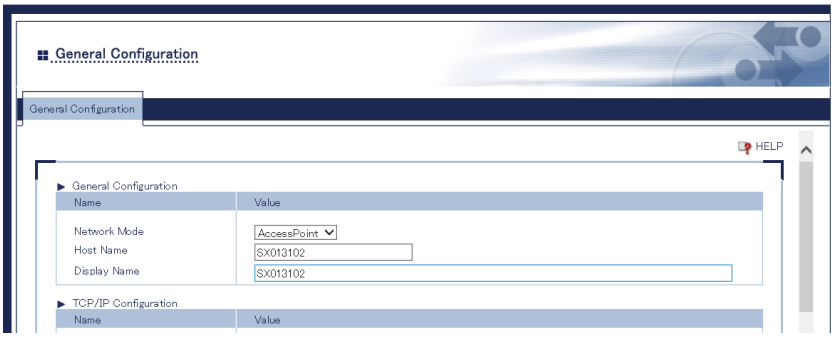
1. Click **General Configuration** on the page menu.



Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The basic setting page appears. Change the setting values if needed, and click **Submit** at the bottom right.



TIP

- When the setting page is switch to another page from the page menu before **Submit** is clicked, all the entered values will be cleared.

Note

- See "**A. Setting Items**" for item details.
- Click **Help** at the top right and go to the help page to see the explanation for setting items.

3. The restart page shows up. The update settings will be applied after Z-1 restarts. Click **Restart**.

Note

- To continue updating settings in other pages, wait restarting Z-1 until all updates are done.

4. When the login page shows up, the basing settings are now updated.

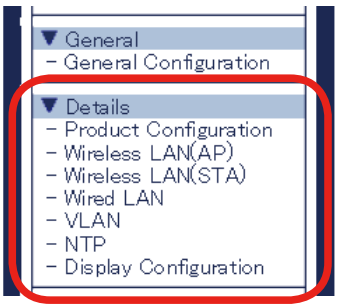
Detailed Network Settings

1. Access the web page.

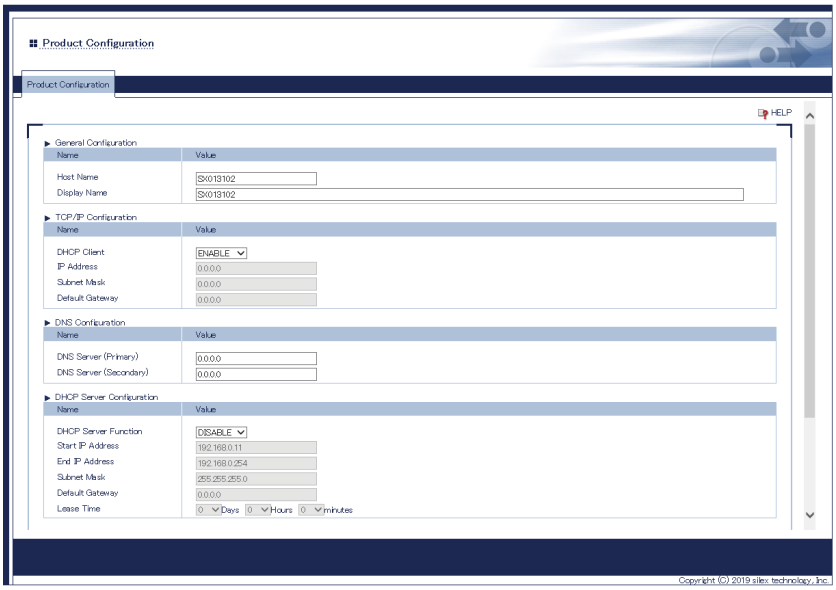
Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. Click the page link on the page menu to update settings.



3. When the setting page appears, change setting values if necessary, and click **Submit** at the bottom right.



TIP

- When the setting page is switch to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. To access other pages, click **Submit** to save the entered values.

Note

- See "**A. Setting Items**" for item details.

4. The restart page shows up. The update settings will be applied after Z-1 restarts. Click **Restart**.

Note

- To continue changing settings in other pages, go to Step 2 and wait restarting Z-1 until all updates are done.

5. When the login page shows up, the settings are now updated.

3-2. How to Change Wireless LAN (STA) Settings with Smart Wireless Setup

This chapter shows how easily wireless LAN (STA) settings can be changed using the smart wireless setup in a network with a wired LAN router supporting WPS (Wi-Fi Protected Setup). When the network mode is "Station", Z-1 works with the following methods under the smart wireless setup.

Push-button method

The wireless LAN settings can be updated with one of the following methods:

- Press the function switch of Z-1.
- Go to the smart wireless setup page and click [Start].

PIN-code method

Go to the web page and enter the PIN code of the enrollee to change the wireless LAN settings.

3-2-1. Before Setup

In order to use the smart wireless setup function and change the wireless LAN settings, a wireless LAN router supporting WPS is needed. Make sure that the WPS wireless LAN router is operating in the user's network.

To check if the wireless LAN router supports WPS, see its instruction manual or contact the maker.

- Some wireless LAN routers need WPS function enabled. Check the instruction manual for more details.
- When the wireless LAN router is used for security functions including Mac address filtering, change the setting for Z-1 to be able to connect with the router.

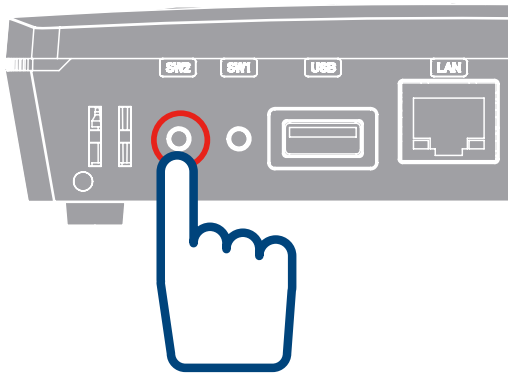
3-2-2. Settings with Push-Button Method

Use the function switch or the web page to initiate the smart wireless setup for the wireless LAN (STA) settings.

Function Switch

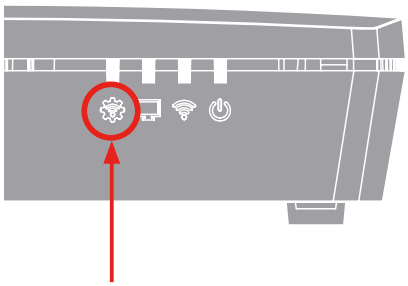
1. Keep and hold the function switch until blue STATUS LED blinks every two seconds.

Z-1 (Front)



Keep pressing the function switch.

Z-1 (Side)



STATUS LED blinks in blue.
(Two-second interval)

2. Push the WPS button of the wireless LAN router. Check that the wireless LAN router is in the standby mode for a connection.

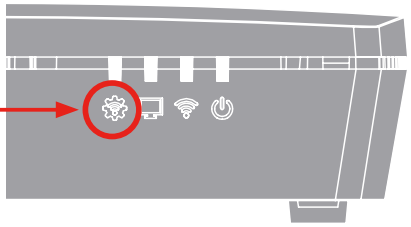
Note

- WPS button's name, position, and form vary with a wireless LAN router in use. For details, see the router's instruction manual.
- Use only one wireless LAN router in this step. When multiple routers are on standby at once, Z-1 cannot connect with a router.

3. When the settings is completely done, the steady blue STATUS LED turns on.

Z-1 (Side)

Steady blue STATUS LED

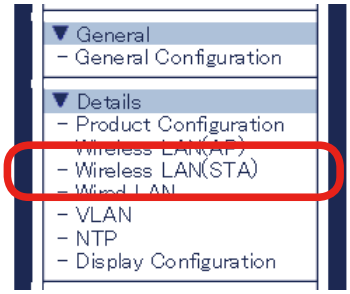


Note

- Red STATUS LED turns on when the smart wireless setup fails due to the following events:
  - No wireless LAN router was found in 120 seconds after the smart wireless setup started (time-out, WPS specification).
  - Two or more wireless LAN routers under WPS-PBC were found during the smart wireless (push-button) setup (overwrapped, WPS specification)
- Red STATUS LED turns on every 100 milliseconds when the smart wireless setup fails (other failure) due to the following event:
  - The smart wireless setup was initiated with a wireless LAN router (WPS 1.0 AP) that did not support WPS 2.0.

Wireless Settings from PC

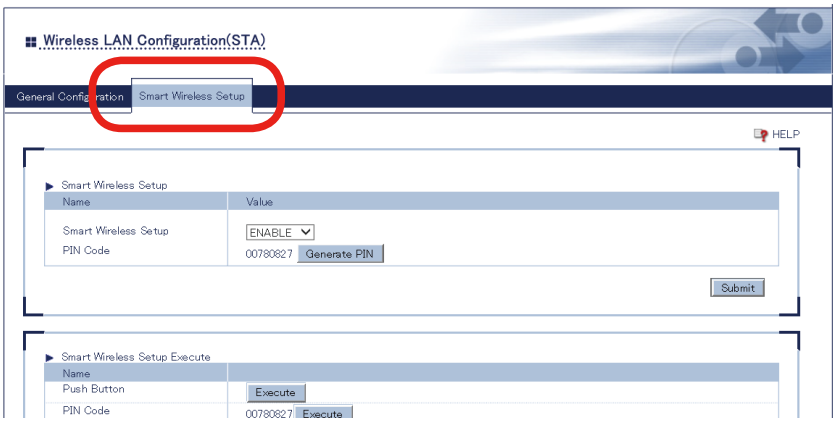
1. Click **Wireless LAN (STA)** on the page menu.



Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The wireless LAN (STA) setting page appears. Click **Smart Wireless Setup** tab.

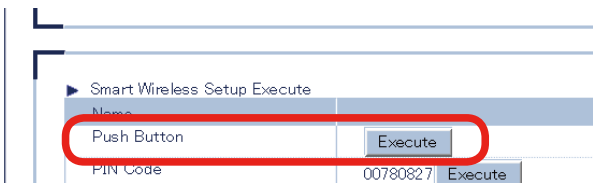


3. Push the WPS button of the wireless LAN router. Check that the wireless LAN router is in the standby mode for a connection.

Note

- WPS button's name, position, and form vary with a wireless LAN router in use. For details, see the router's instruction manual.
- Use only one wireless LAN router in this step. When multiple routers are on standby at once, Z-1 cannot connect with a router.

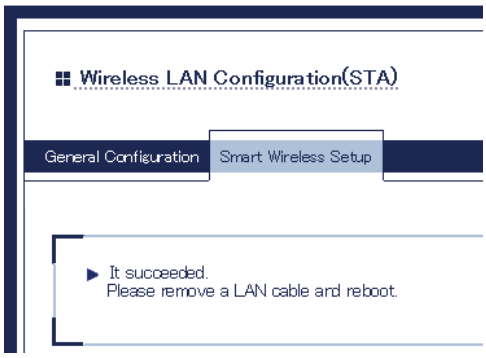
4. Click **Execute** button of the **Push Button** method to initiate the smart wireless setup.



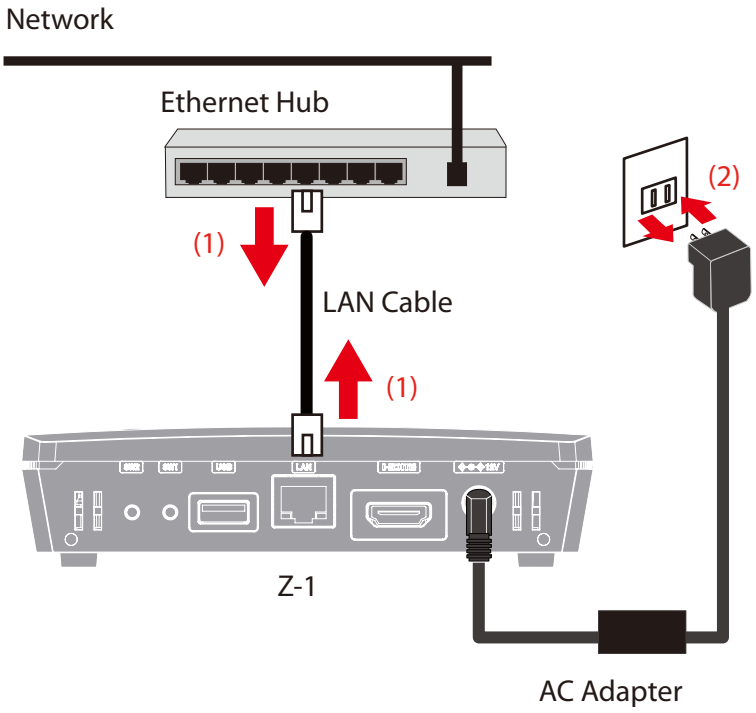
Note

- It may take some time to complete the setup in some environments (max two minutes).

5. Z-1 will get the same setting values of the wireless LAN router after the setup.



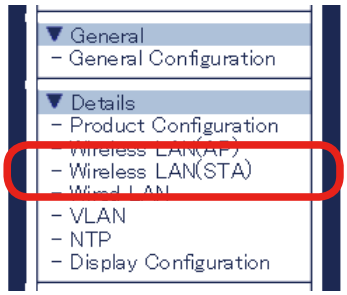
6. Unplug the LAN cable from Z-1 and from the network or the access point (1). Unplug and then plug the power to the outlet (2), and restart Z-1.



Now, the wireless LAN (STA) settings are completed.

3-2-3. Settings with PIN-code Method

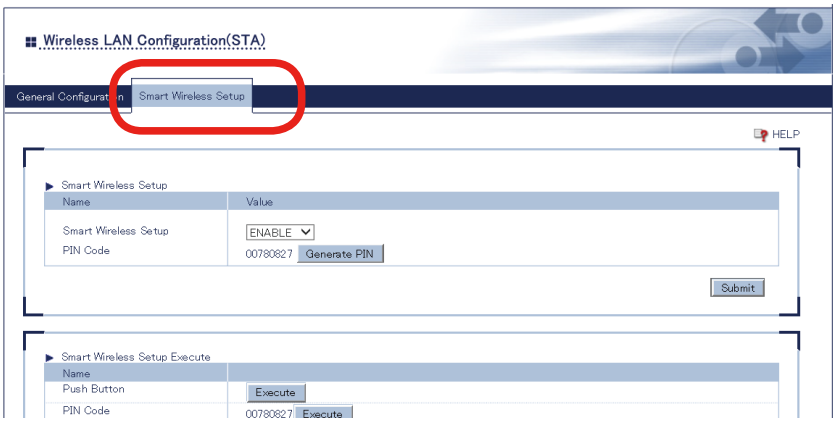
1. Click **Wireless LAN (STA)** on the page menu.



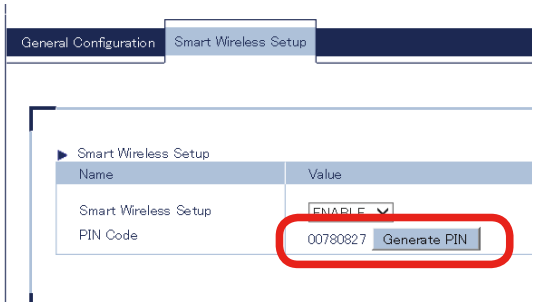
Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The wireless LAN (STA) setting page appears. Click **Smart Wireless Setup** tab.



3. Check the PIN code on the page, and provide the access point with the PIN code. Do not close this page for Step 5.

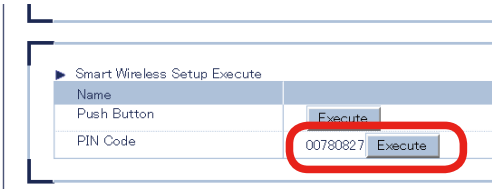


Note

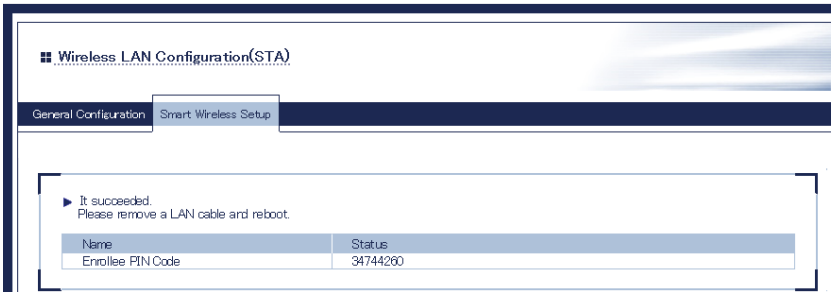
- To change the PIN code, click **Generate PIN** to issue new PIN code.

4. Open another page to access the wireless LAN router's webpage. Enter Z-1's PIN code (see Step 3), and start WPS connection from the router.

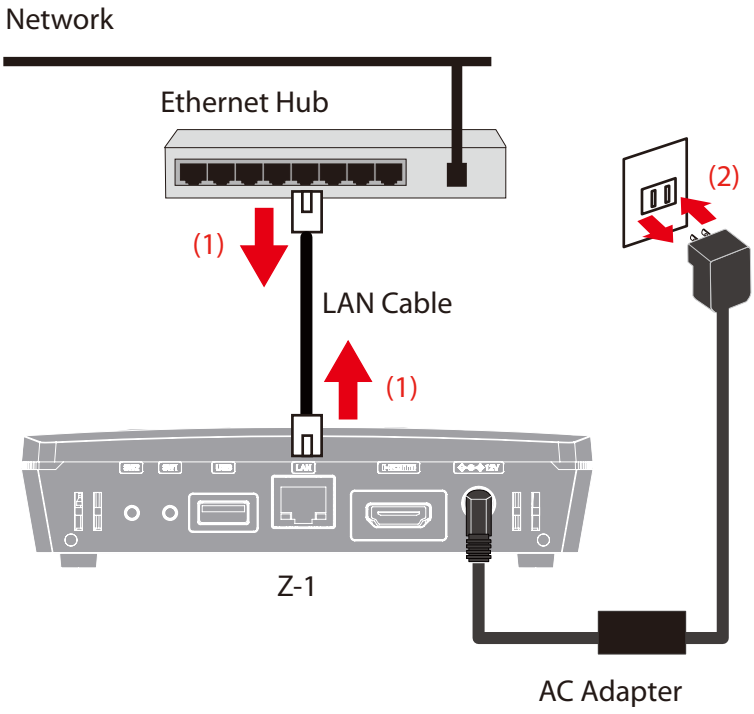
5. Go back to the Z-1's webpage and click **Excute** of **PIN-code**.



6. Z-1 will get the same setting values of the wireless LAN router after the setup.



7. Unplug the LAN cable from Z-1 and from the network or the access point (1). Unplug and then plug the power to the outlet (2), and restart Z-1.



Now, the wireless LAN (STA) settings are completed.

4. Projection on Display Devices

4-1. How to Change Projection Mode

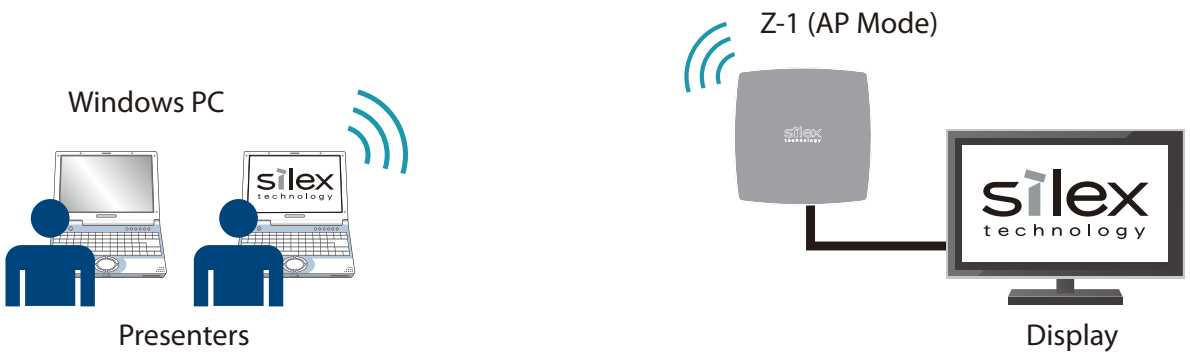
4-1-1. Projection Mode Type

Z-1 has the following five projection modes. Choose one of them, and then send videos and audio data. Z-1 initially starts in Single Presenter mode (factory default).

- Single Presenter mode
- Multi-Presenter mode
- Distribution Master mode
- Distribution Slave mode
- Pair Display mode

Single Presenter mode

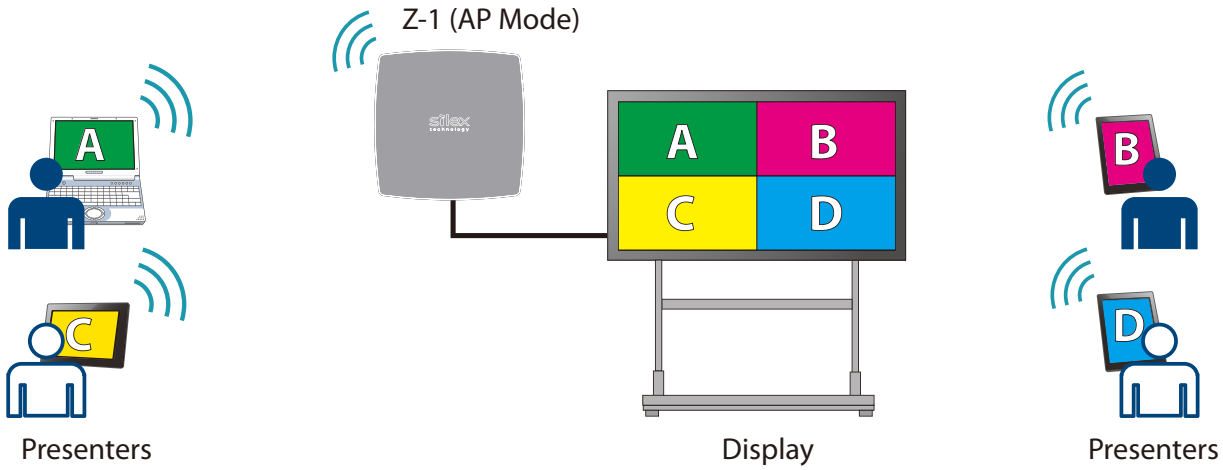
Single Presenter mode shows videos and images of one user in full screen.



- When a user connects to Z-1 during the other user's presentation, the current session will be disconnected and the presenter will be switched to the newly-connected user.
- Display resolutions are up to 1,920 x 1,080 (iOS connection enables a resolution of 1,080 x 1,920: portrait monitor). The screen will be enlarged when a 4K monitor is connected.
- The video frame rate is max 30 fps. The audio output is supported.
- For Windows devices, the dedicated tool is available. For Android, iOS and Mac OS, the OS-standard function can be used for projection.
- When the size of sent images does not meet Z-1's resolutions, a black border will appear around the images.

Multi-Presenter Mode

Multi-Presenter mode splits the screen and shows images sent by two to four presenters.



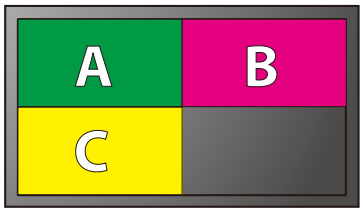
Note

- One of presenters can become the primary session and Z-1 plays audio data of the primary device.
- The full-screen or split-screen display can be chosen on OSD menu.

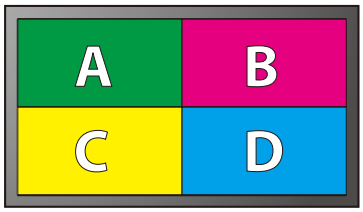
When three or four users are connecting:

Four-split screen

3 users



4 users

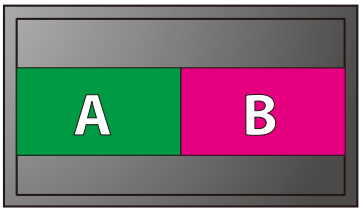


TIP

- When four users are connecting and another user tries to connect to Z-1, the oldest session (the first connection) will be disconnected and the new session will be established.

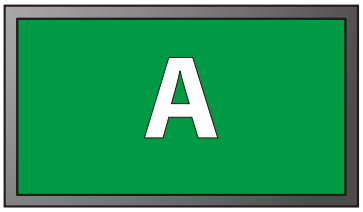
When two users are connecting:

Two-split screen



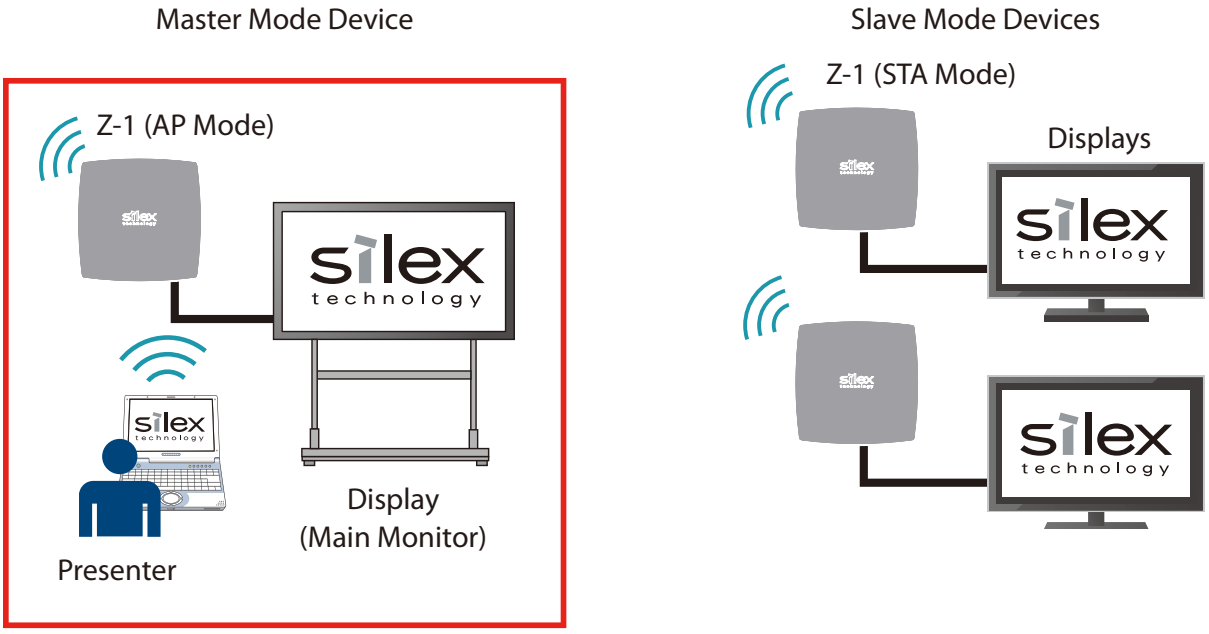
When only one user is connecting:

Full screen: same as Single Presenter mode



Distribution Master Mode

Distribution Master mode works the same way as Single Presenter mode does.
Z-1 can transmit the received images to slave-mode Z-1 (up to 16 units) while it is showing the images on the main monitor. It is useful for large conference venues which have multiple displays and projectors in order to show the main-monitor images on them at the same time.

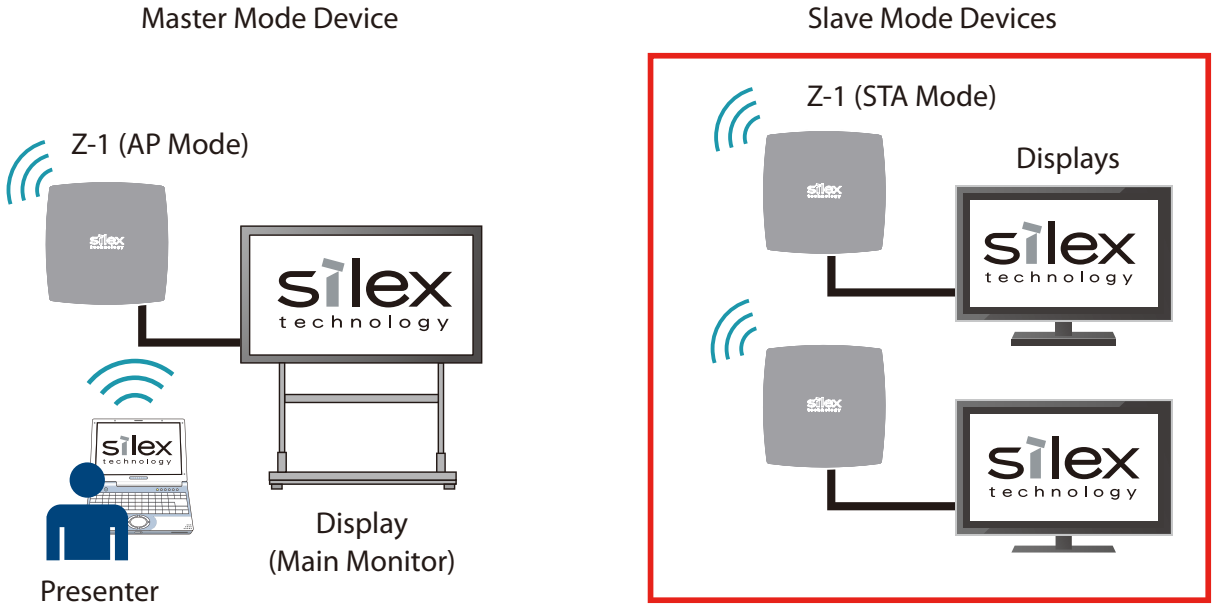


TIP

- Make sure that the network mode for Master Z-1 has to be Access Point mode.
- Both the Master and Slave Z-1 units have to be in the same segment (broadcast domain).
- Do not set more than one Z-1 unit to Master mode in one segment.

Distribution Slave Mode

Slave-mode devices are used together with the Master-mode device. These devices receive data from the Master-mode device and show the same images as those on the main monitor.



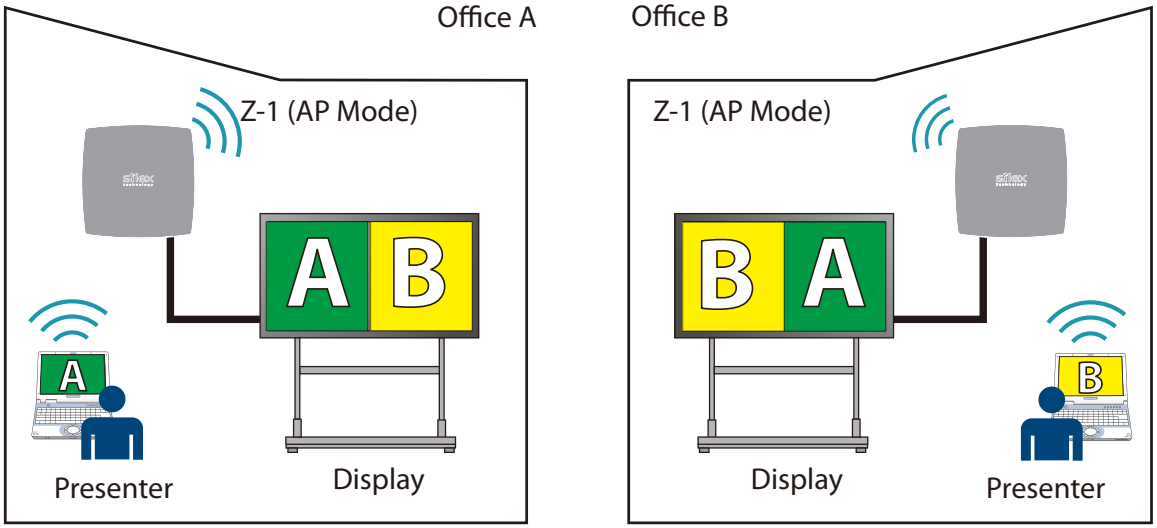
TIP

- Make sure that the network mode for Slave Z-1 has to be Station (STA) mode.
- Up to 16 units of Slave Z-1 can receive images at once.

Pair Display Mode

Two units of Z-1 can connect each other in Pair Display mode and show presenters' screens (Local and Remote screens) on a two-split-layout display.

- Use OSD interface to connect two Z-1 units in Pair Display mode.
- One presenter's screen is shown on the left side of the screen (Local) while it is being sent to the other Z-1.
- The received screen images are shown on the right side of the screen (Remote).
- The frame rate of Remote screen is max 1 fps, and the audio data is not transmitted.



4-1-2. Projection Mode Change

The projection mode can be changed with the function switch, OSD icon, or the web interface.

TIP

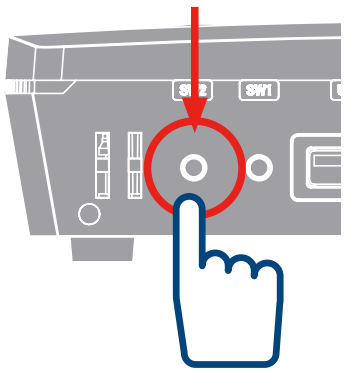
- When the projection mode is changed, the presenters and devices will be disconnected.

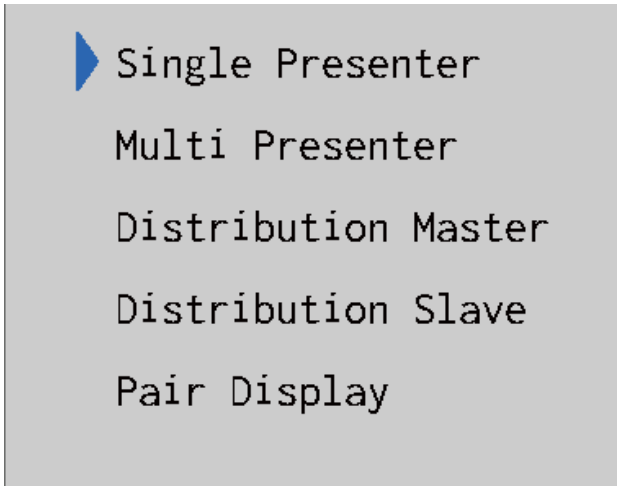
Function Switch

1. Push the function switch once on the front side of Z-1. The display will show the mode-change OSD menu and an arrow cursor appears next to the current projection mode.

Z-1 (Front)

Function Switch





2. Every time the function switch is pressed, the arrow cursor moves one menu down.

Move the arrow cursor to the new projection mode. Three seconds later, Z-1 will recognize the mode and change the projection type.

TIP

- The connection sessions will be disconnected when the mode is changed.
- Z-1 shows an OSD message and does not accept the control during the mode change.

Note

- The current projection mode is shown in bold.

OSD Icon

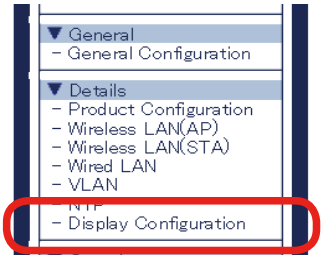
Click the projection-mode change icon on the tool bar, and the mode change menu will appear.
For more details, see "Z-1 User's Manual (Projection Control)".

TIP

- Need a USB mouse to click the icon on the tool bar.

Web Page

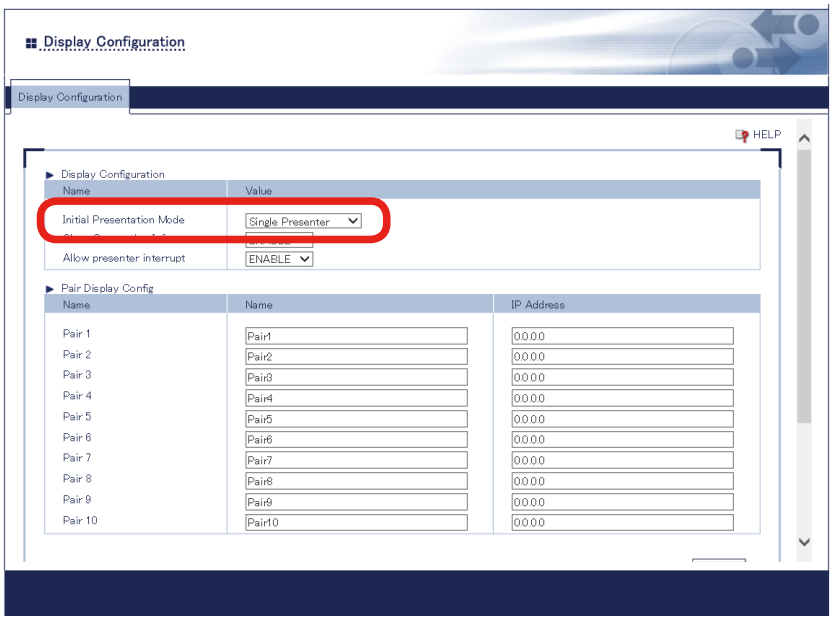
1. Access the web page and click **Display Configuration** on the page menu.



Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The display setting page appears. Change **Initial Presentation Mode** and click **Submit**.



TIP

- When the setting page is switch to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. To access other pages, click **Submit** to save the entered values.

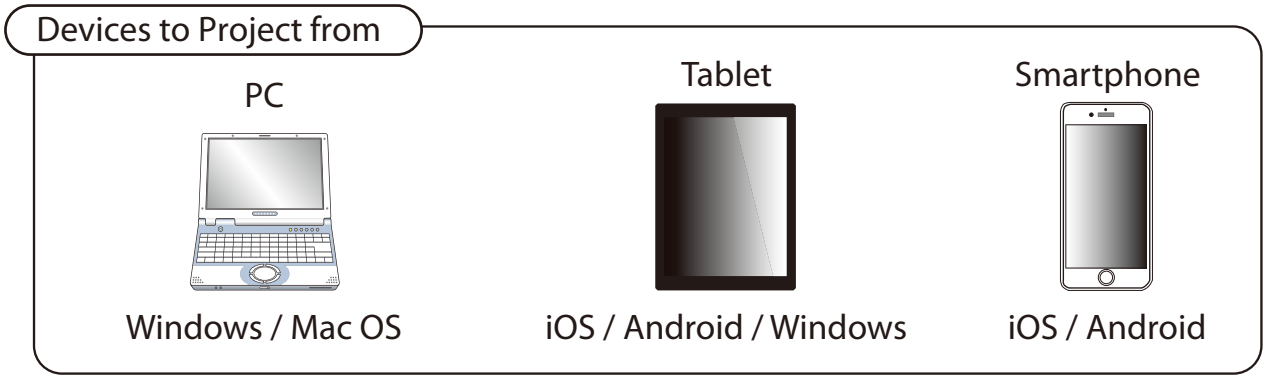
3. The restart page shows up. The update settings will be applied after Z-1 restarts. Click **Restart**.

4. After the restart, close the web browser.

4-2. How to Show Screens on Display

4-2-1. Device Preparation

Prepare devices to send data to the display of Z-1.



4-2-2. Projection

Send the device's screen to the Z-1 display.
For more details, see "Z-1 User's Manual (Projection Method)".

(Blank page)

5. Use of Wireless LAN Access Point Function

5-1. How to Connect Wireless LAN Stations

5-1-1. Connecting Windows PC

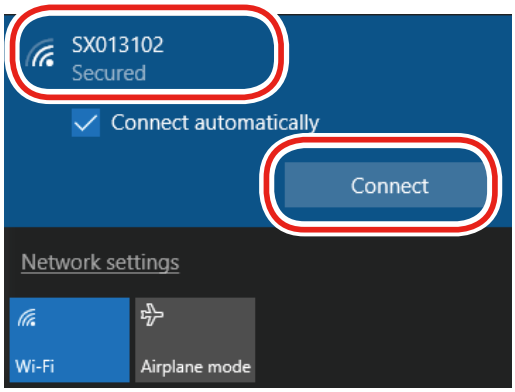
This chapter shows how to connect Z-1 with Windows PC as a wireless LAN station.

Note

- Check SSID and the security key (pre-shared key or WEP key) of Z-1 beforehand.
- Windows 10 is used for the following procedure. To connect PC with the other OS, follow the appropriate procedure of the OS.

1. Click the network icon on the notification area (system tray) to view wireless networks.

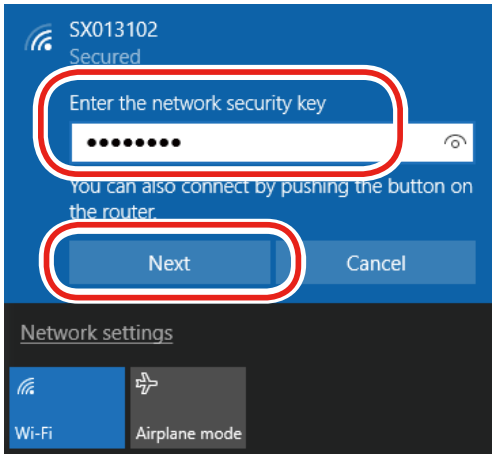
2. Select SSID of Z-1 and click **Connect**.



Note

- Tick **Connect automatically** and your PC will automatically connect to Z-1 every time it restarts.

3. Enter the pre-shared key or WEP key of Z-1 in the **Enter the network security key** box and click **Next**.



4. When a message **Do you want to allow your PC to be discoverable by other PCs and devices on this network?** appears, click **Yes**.

Now, the PC has connected to Z-1.

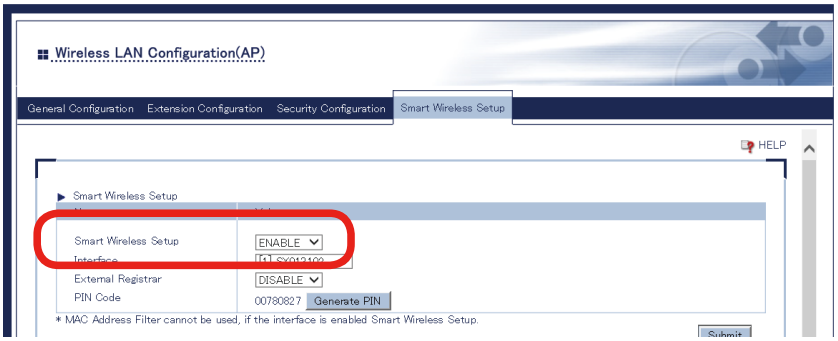
5-1-2. Use of Function Switch

This chapter shows how to use the function switch to connect Windows PC as a wireless LAN station.

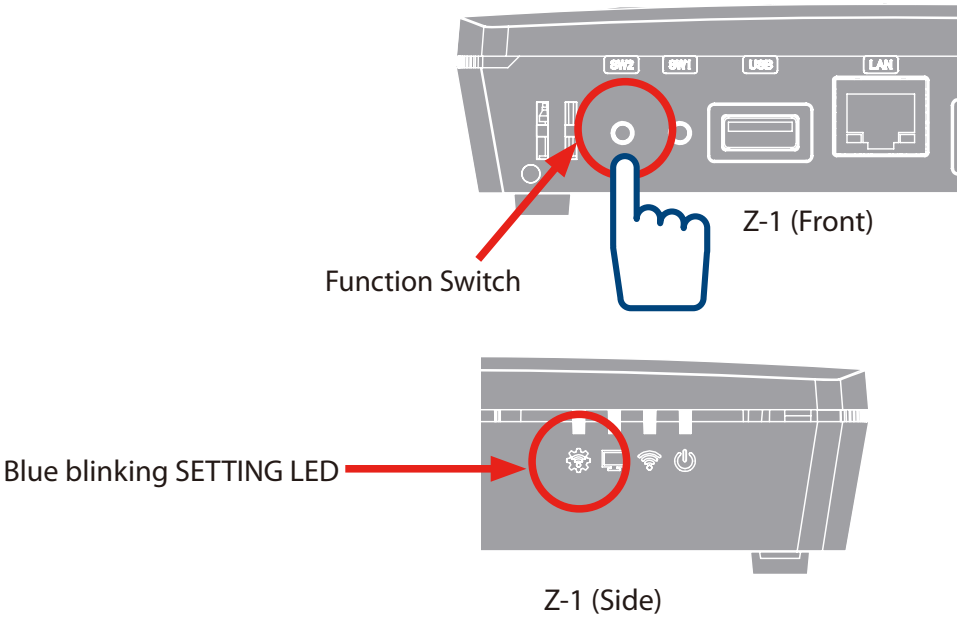
TIP

- before going through the following procedure, make sure that the wireless LAN device supports Wi-Fi Protected Setup (WPS).

1. Go to the web page of **Smart Wireless Setup** under the wireless LAN (AP) settings before the following steps, and make sure that **Smart Wireless Setup** is **ENABLE**.

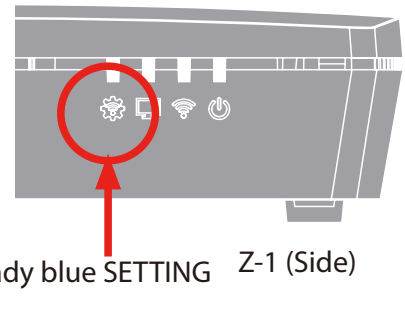


2. Press and hold the function switch until SETTING LED blinks in blue.



3. Press the wireless function switch on the wireless LAN station to connect.

4. Z-1 starts communicating and automatically provides the same setting values to the station. When SETTING LED turns steady blue, the setting has been done.



Now, the wireless LAN station has connected to Z-1.

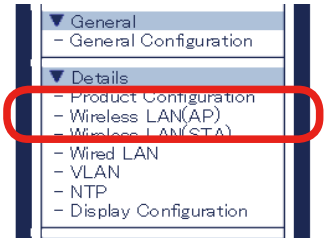
5-1-3. Use of Web Pages

This chapter shows how to connect a wireless LAN device by using web pages of Z-1.

TIP

- For the following procedure, make sure that the wireless LAN device supports Wi-Fi Protected Setup (WPS).

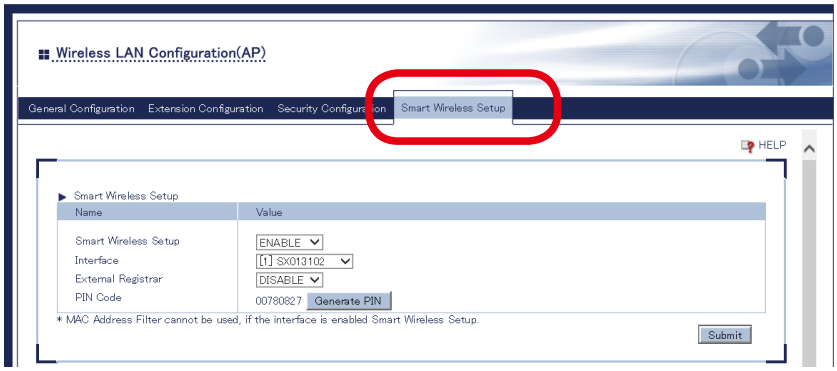
1. Access Z-1's web page and click **Wireless LAN (AP)** on the page menu.



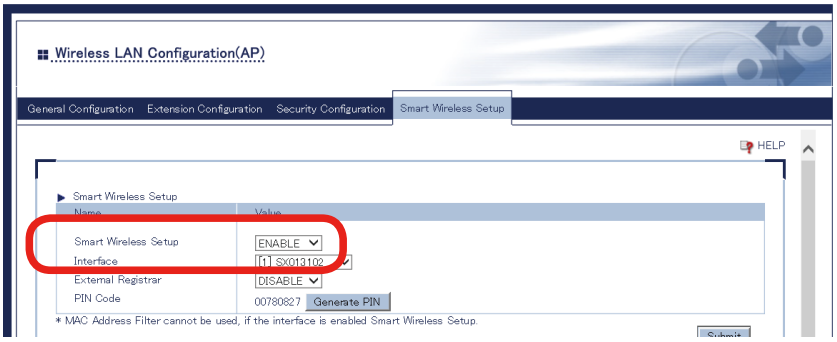
Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The wireless LAN (AP) setting page appears. Click the tab of **Smart Wireless Setup**.



3. Check that the **Smart Wireless Setup** is **ENABLE**.

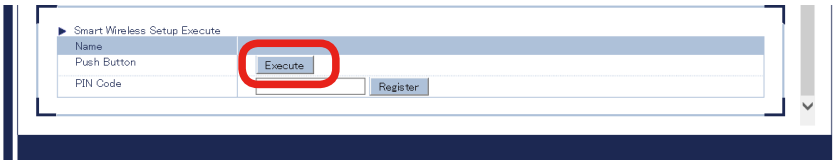


4. The smart wireless setup page allows the following two methods to connect Z-1 and a wireless LAN station.

- Push-button method
- PIN-code method

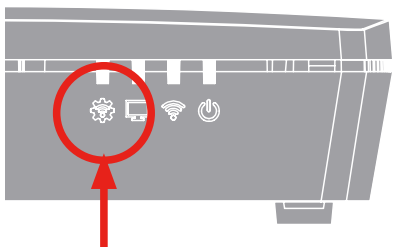
Use of Push-Button Method

1. Click **Execute** of the **Push Button** on the smart wireless setup page.



2. Press the wireless function switch on the wireless LAN station to connect.

3. Z-1 starts communicating and automatically provides the same setting values to the station. When SETTING LED turns steady blue, the setting has been done.



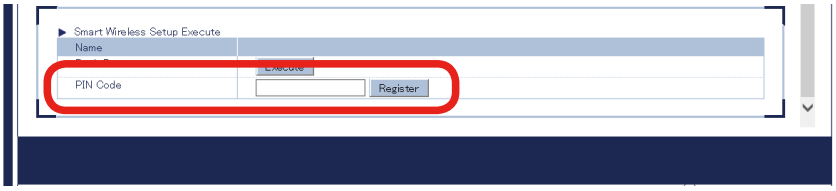
Steady blue SETTING LED

Z-1 (Side)

Now, the wireless LAN station has connected to Z-1.

Use of PIN Code

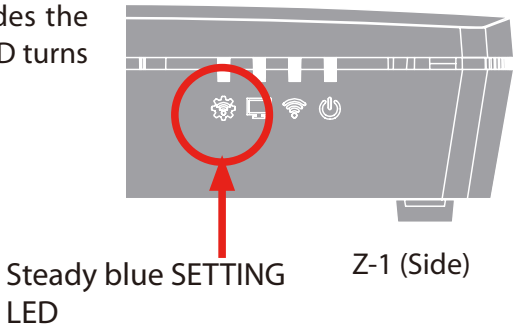
1. Go to the smart wireless setup page, and enter PIN code of the wireless LAN station in the **PIN Code**. Click **Register**.



TIP

- The PIN code has to be the one assigned to the wireless LAN station. See the device's instruction manual for details.

2. Z-1 starts communicating and automatically provides the same setting values to the station. When SETTING LED turns steady blue, the setting has been done.



Now, the wireless LAN station has connected to Z-1.

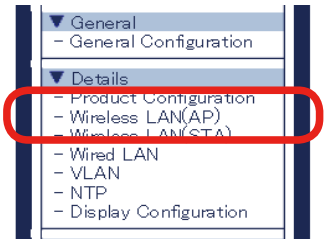
5-2. How to Accept/Block Specific Wireless LAN Station Devices

This chapter shows how to register MAC addresses of wireless LAN stations to accept or block connections to Z-1.

TIP

- Before going to the step below, check MAC addresses of the target devices.

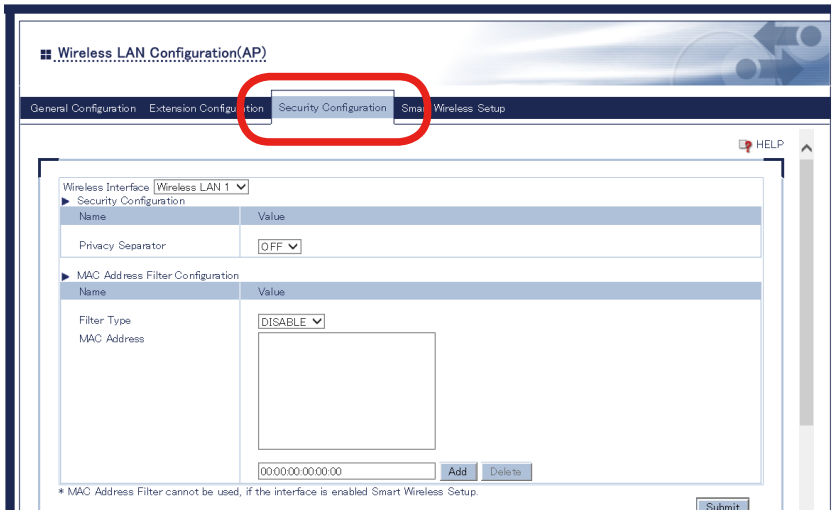
1. Access the web page and click **Wireless LAN (AP)** on the page menu.



Note

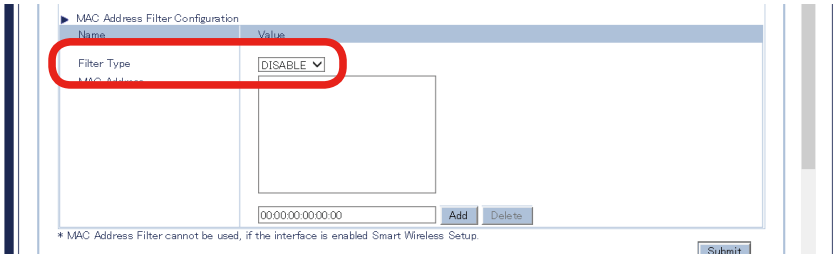
- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The wireless LAN (AP) setting page appears. Click the tab of **Security Configuration**.

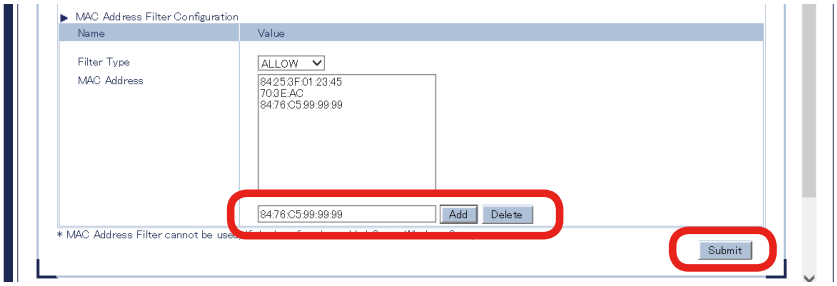


3. Select the filter type under MAC Address Filter Settings.

- ALLOW: Accepts only the registered wireless LAN stations to connect to Z-1.
- DENY: Blocks the registered wireless LAN stations to connect to Z-1.



4. Enter the MAC address of the wireless LAN station in the MAC address input box, and click **Add**. Repeat the step to register multiple devices. Click **Submit** after all MAC addresses have been registered.



TIP

- When the page is switch to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. To access other pages, click **Submit** to save the entered values.

Note

- MAC addresses must be the form of "XX:XX:XX:XX:XX:XX".
- The vender code (the first 6 characters of MAC address) alone can be registered. In that case, wireless devices having the vendor code will be accepted or blocked.
- To delete the registered MAC addresses, select them and click **Delete**.

5. The restart page shows up. The new settings will be applied after Z-1 restarts. Click **Restart**.

Note

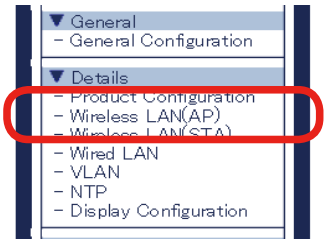
- To continue updating settings in other pages, wait restarting Z-1 until all updates are done.

6. After the restart, close the web browser.

5-3. Ban on Wireless LAN Station Communications

This chapter describes a way to prohibit wireless LAN stations from establish communication each other, and to allow communication of a device wired to Z-1.

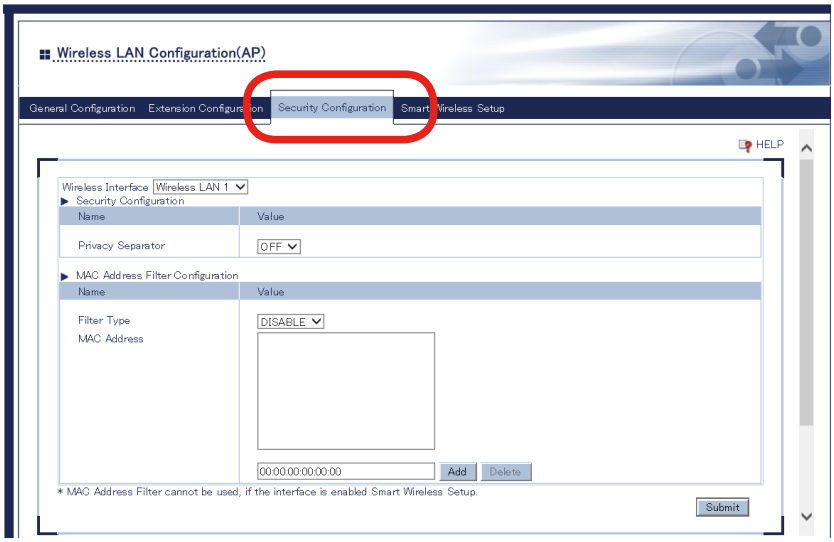
1. Access the web page and click **Wireless LAN (AP)** on the page menu.



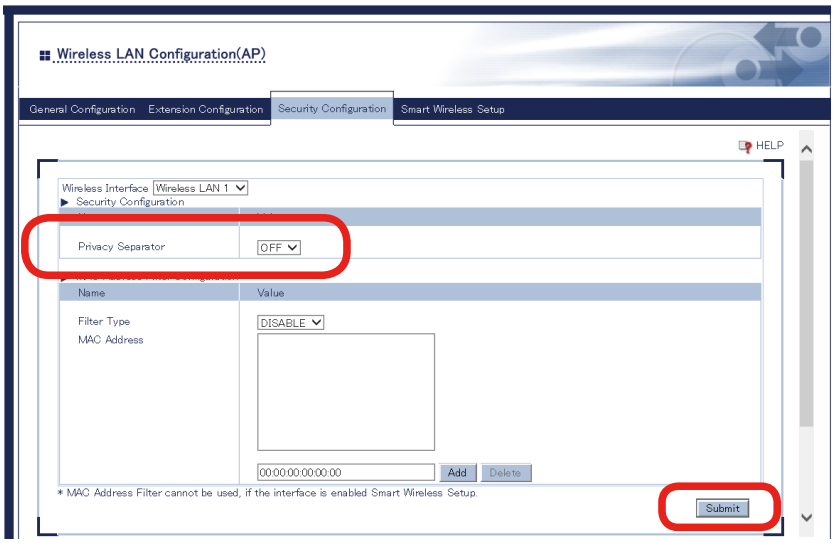
Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The wireless LAN (AP) setting page appears. Click the tab of **Security Configuration**.



3. Choose **ON** for **Privacy Separator**, and click **Submit**.



TIP

- When the page is switch to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. To access other pages, click **Submit** to save the entered values.

4. The restart page shows up. The new settings will be applied after Z-1 restarts. Click **Restart**.

Note

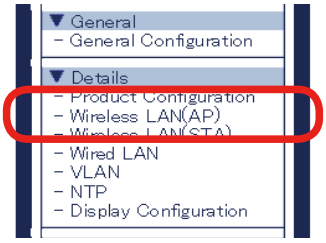
- To continue updating settings in other pages, wait restarting Z-1 until all updates are done.

5. After the restart, close the web browser.

5-4. Disabling Smart Wireless Setup

This chapter shows how to disable the smart wireless setup functions (e.g. Push-switch method to connect to a wireless LAN station).

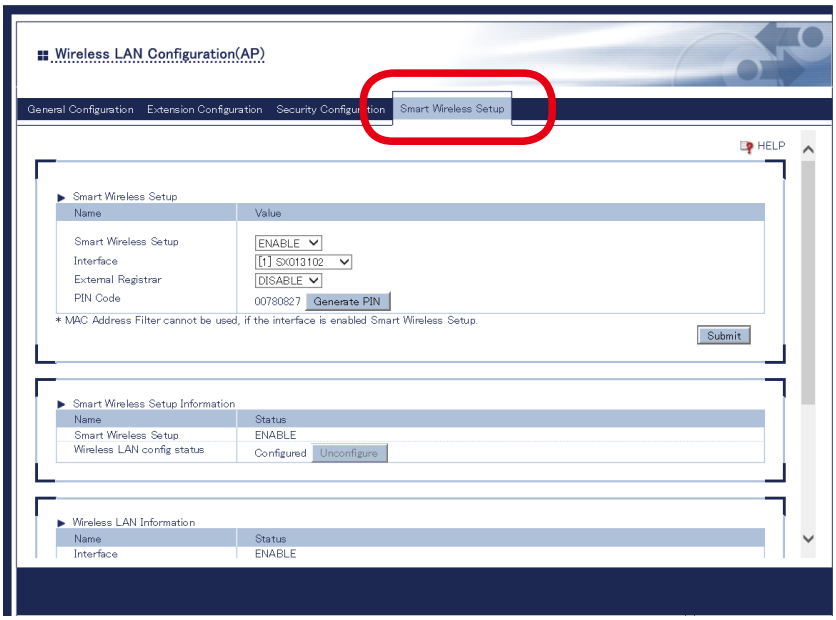
1. Access the web page and click **Wireless LAN (AP)** on the page menu.



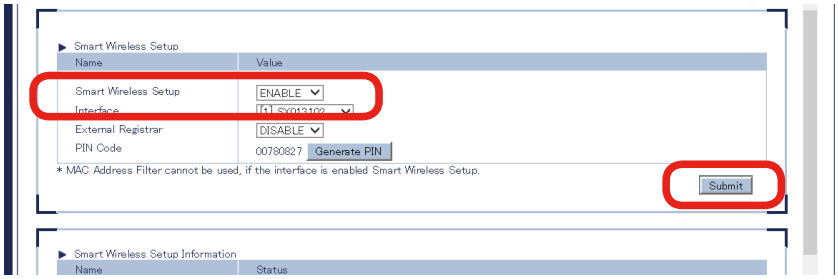
Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The wireless LAN (AP) setting page appears. Click the tab of **Smart Wireless Setup**.



3. Select **DISABLE** for **Smart Wireless Setup**, and click **Submit**.



TIP

- When the setting page is switch to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. To access other pages, click **Submit** to save the entered values.

4. The restart page shows up. The new settings will be applied after Z-1 restarts. Click **Restart**.

Note

- To continue updating settings in other pages, wait restarting Z-1 until all updates are done.

5. After the restart, close the web browser.

6. Other Functions

6-1. Status Monitoring Function on Web Browser

6-1-1. System Status Check

The network status of Z-1 including TCP/IP can be checked on the web page.

1. Access Z-1's web page and click **System** on the page menu.

Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

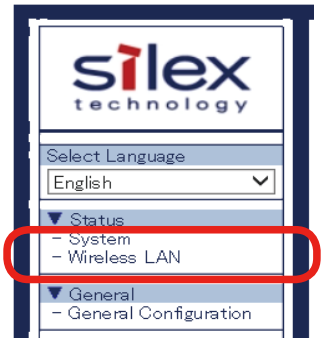
2. The system status page appears.

Item	Description
System status	
Product name	Name of the product, Z-1
Version	Firmware version of the product
MAC address	MAC address of the product
Host name	Host name in use
IP address	Currently assigned IP address
Subnet mask	Subnet mask in use
Default gateway	Gateway address in use
DHCP server	Address of the DHCP server that provided the IP address (This is shown only when the address is obtained from DHCP.)
Wireless LAN (AP) common settings	
Wireless mode	Wireless mode in use
Channel bandwidth	Channel bandwidth in use
Channel	Communication channel in use
Tx power	Radio transmission strength of the wireless LAN
Wireless LAN settings 1 to 4	
Interface	Status of the wireless interface in use
SSID	SSID in use
Network authentication	Configured network authentication
Encryption mode	Configured encryption method
Wireless LAN (STA) common settings	
Current SSID	SSID in use
Wireless LAN status	Connection status of the radio
Current channel	Channel in use

6-1-2. How to Check Wireless LAN Status

The web page provides the status of wireless LAN stations connected to Z-1. The status includes MAC address of devices and the radio strength.

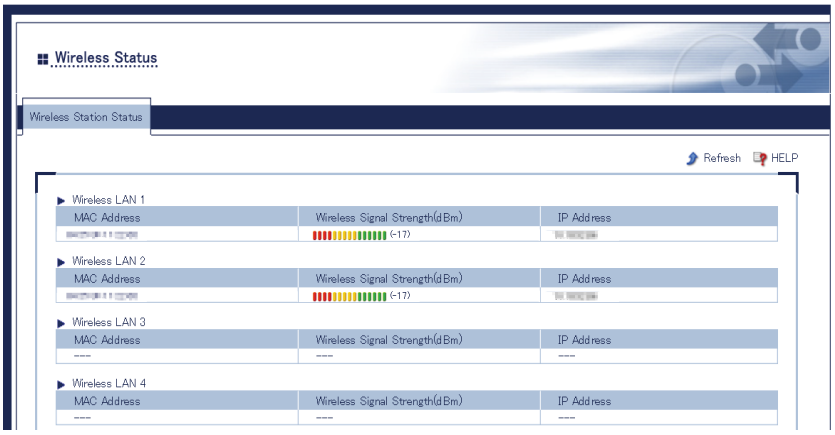
1. Access Z-1's web page and click **Wireless LAN** on the page menu.



Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The wireless LAN status page appears.



Item	Description
MAC Address	Shows MAC addresses of wireless LAN station devices connected to Z-1.
Wireless Signal Strength (dBm)	Shows the radio strength of the devices.
IP Address	Shows the IP addresses of the devices.

6-2. Use of DHCP Server Functions

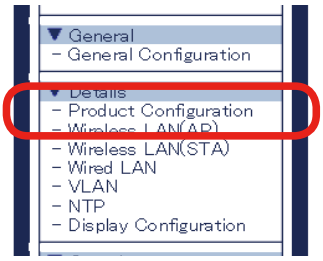
This chapter describes the DHCP server functions of Z-1. When there is no network device with DHCP server functions in the user's environment, Z-1 can automatically assign IP addresses to PC and network devices in the network.

Note

- In order to allocate an IP address to PC automatically with the DHCP server functions, enable "**Obtain an IP address automatically**" for the PC.

6-2-1. Setup for DHCP Server Functions

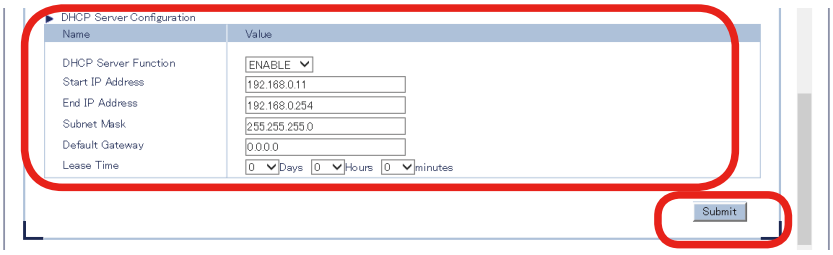
1. Access Z-1's web page and click **Product Configuration** on the page menu.



Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The product setting page appears. Enable the DHCP server functions under **DHCP Server Configuration**, change the following items, and click **Submit** at the right bottom of the page.



TIP

- When the page is switch to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. To access other pages, click **Submit** to save the entered values.

Note

- See "**A. Setting Items**" for item details.

3. The restart page shows up. The new settings will be applied after Z-1 restarts.

Note

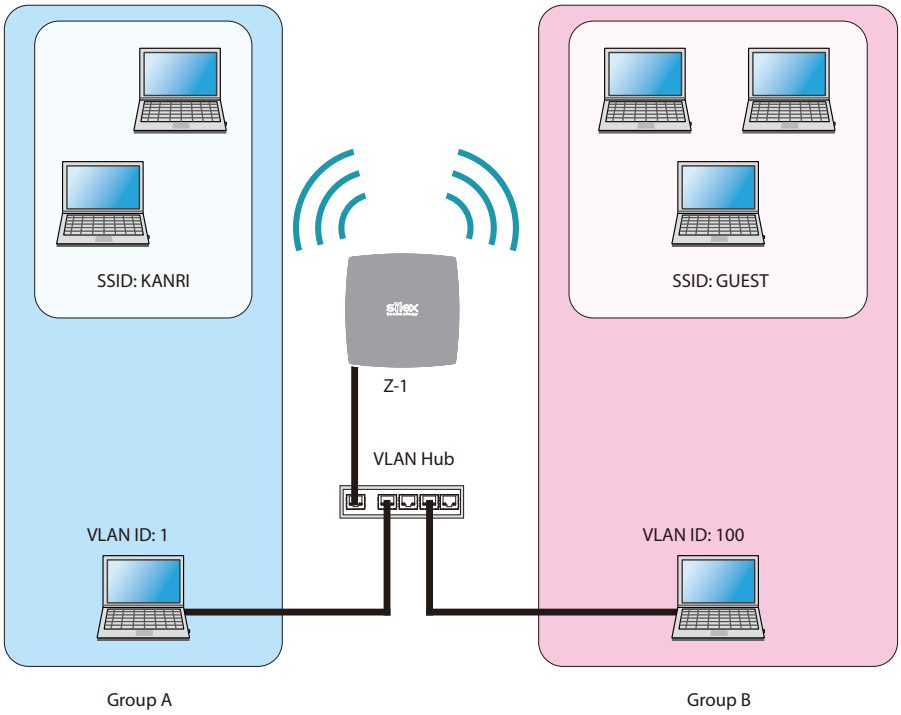
- To continue updating settings in other pages, wait restarting Z-1 until all updates are done.

4. After the restart, close the web browser.

6-3. Use of VLAN Function

6-3-1. VLAN Function

Z-1's access point mode supports multiple SSIDs. Z-1 (one unit) can give VLAN ID to each SSID, and can create up to four virtual network groups together with a switching hub supporting tagged VLAN (VLAN Hub).



Creating Virtual Network Groups

TIP

- Tagged VLAN must be compliant with IEEE802.1Q.
- Dynamic VLAN is not included.

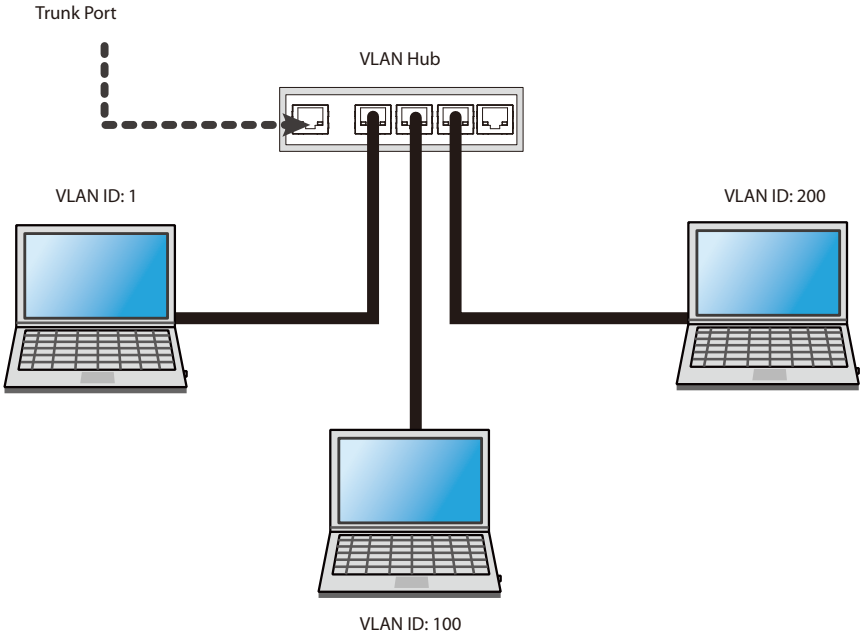
6-3-2. VLAN Function Setup

This chapter describes how to connect Z-1 to a network where network groups have been established with a VLAN hub.

Getting Information on Network VLAN

Check the following information of the network:

- Location of the trunk port on the VLAN hub.
- VLAN ID of the native VLAN
- VLAN ID of devices connected to the VLAN hub

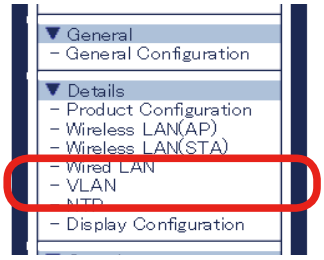


TIP

- When there is no available trunk port, create a trunk port for the VLAN hub.
- For details of the VLAN hub, check the instruction manual.

Updating VLAN Function on Z-1

1. Access Z-1's web page and click **VLAN** on the page menu.



Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The VLAN setting page appears. Enter the setting values and click **Submit** at the bottom right.

TIP

- When the page is switch to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. To access other pages, click **Submit** to save the entered values.
- To change the network authentication to 802.1X, WPA-Enterprise, WPA2-Enterprise, or WPA/WPA2-Enterprise in a network where VLAN function is enabled, provide the input box **Management VLAN ID** with VLAN ID of the network group that includes RADIUS server.

Note

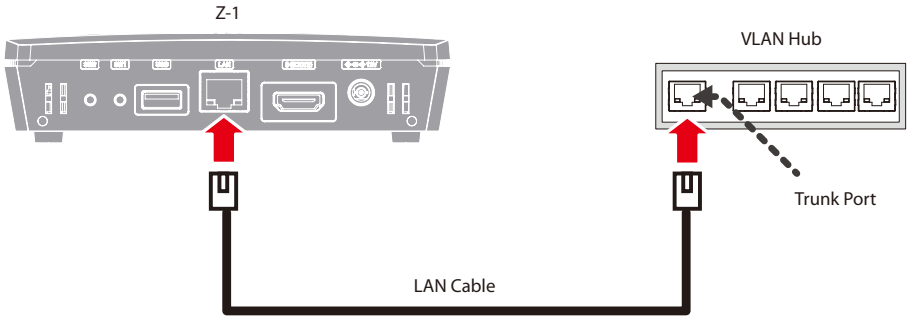
- See "**A. Setting Items**" for item details.
- The **Native VLAN ID** input box should get the native VLAN ID of the VLAN hub.
- The **VLAN ID** input boxes under wireless LAN 1 to 4 should get VLAN ID of devices connected to the hub.
- After the VLAN function is enabled, settings of Z-1 can be updated from the network group only when its VLAN ID is same as the management one.
- When the VLAN function is enabled, VLAN ID can be updated on the basic wireless LAN setting page as well.
- When **Native VLAN ID** and **Management VLAN ID** have the same value and the VLAN function is enabled, any hub can access Z-1 although the hub does not support VLAN. It is recommended that **Native VLAN ID** and **Management VLAN ID** have the same value.

3. The restart page shows up. The new settings will be applied after Z-1 restarts. Click **Restart**.

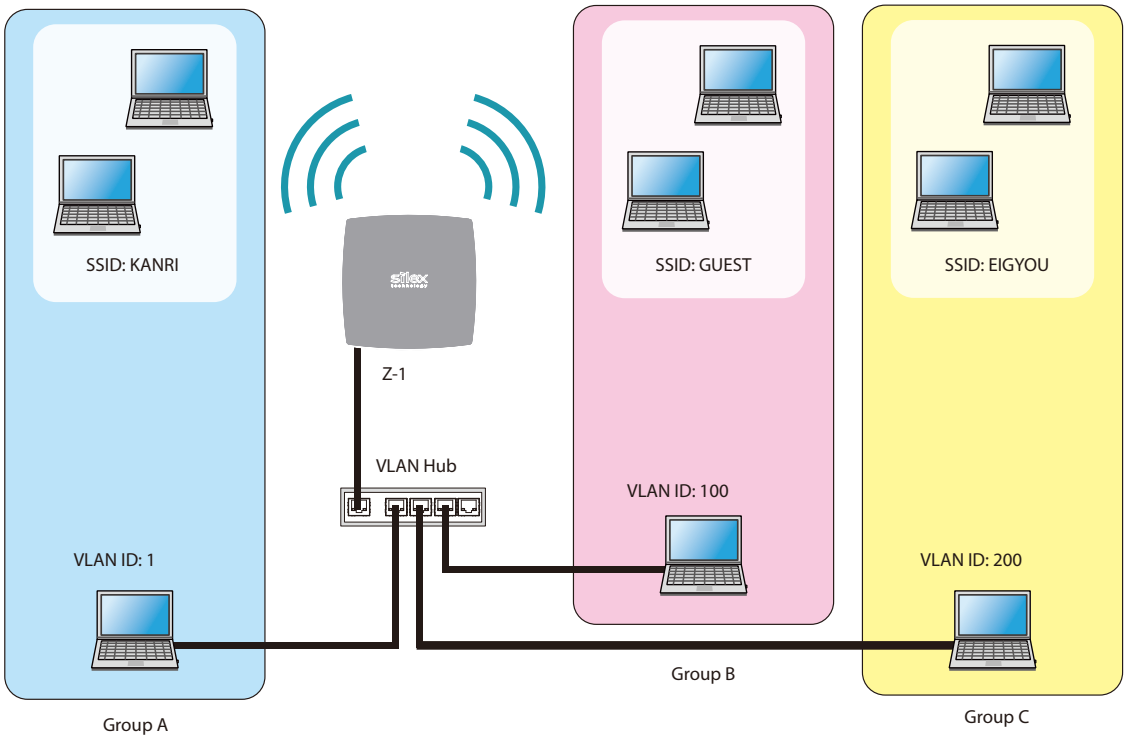
4. After the restart, close the web browser.

Connecting Z-1 to Trunk Port of VLAN Hub

Connect the wired port of Z-1 with the trunk port of the VLAN hub.



Now, the VLAN function setup is done, and Z-1 will operate with virtual network groups based on the VLAN ID settings.



Creating Virtual Network Groups

TIP

- After the VLAN function is enabled, settings of Z-1 can be updated from the network group only when its VLAN ID is same as the management one. If the management VLAN ID cannot be given to a group, reset Z-1 to the factory default settings and go through the VLAN function setting procedure again.
- To use PC in a wireless LAN with VLAN function to update the settings, VLAN ID for the wireless LAN's SSID needs to be same as management VLAN ID.

6-4. Clock Sync with NTP Server

This chapter describes how to get the time from the NTP server.

6-4-1. NTP Function Overview

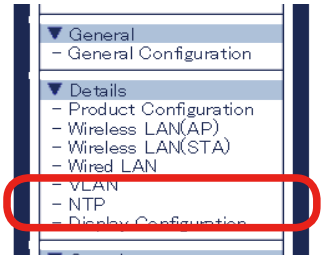
Z-1 can get the time information from the NTP server in the wired LAN network.

Note

- When there is no NTP server in the network, the system time will start at "00:00:00 (hours: minutes: seconds) on January 1, 1970".
- Z-1 clock can sync up with the time of Windows PC as well.

6-4-2. NTP Function Settings

1. Access the web page and click **NTP** on the page menu.



Note

- Check **How to Access Web Page** in **3-1-2 Web Pages**.

2. The NTP setting page appears. Enable **NTP**, update the following items, and click **Submit**.

TIP

- When the setting page is switch to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. To access other pages, click **Submit** to save the entered values

Note

- See "**A. Setting Items**" for item details.

3. The restart page shows up. The update settings will be applied after Z-1 restarts. Click **Restart**.

4. After the restart, close the web browser.

6-5. Security Functions

6-5-1. Use of Security Functions

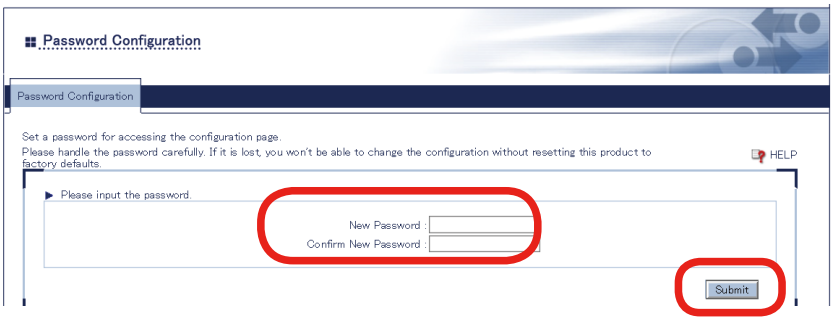
How to Change Administrator Password

1. Access Z-1's web page and click **Password** on the page menu.

Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The password setting page appears. Enter the new password in **New Password** and **Confirm New Password**, and then click **Submit**.



TIP

- You must memorize the password. If you forget it, you will not be able to change the settings unless Z-1 is restored to the factory default settings.

3. The restart page shows up. The update settings will be applied after Z-1 restarts. Click **Restart**.

Note

- To continue updating settings in other pages, wait restarting Z-1 until all updates are done.

4. After the restart, the login page appears. The new administrator password is now working.

Access Control

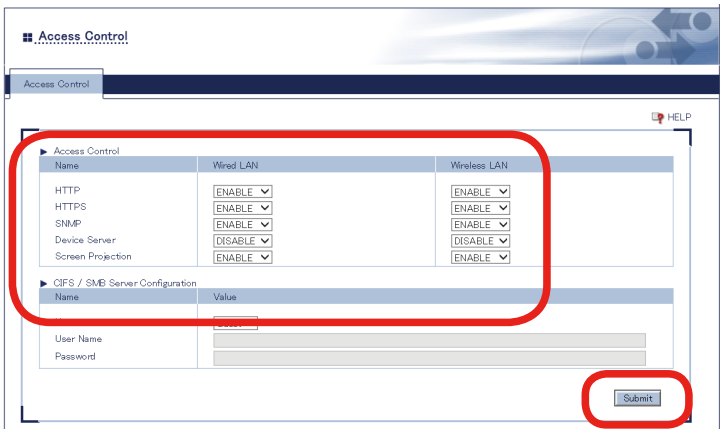
The access control function limits specific protocols to access Z-1. The wired LAN and the wireless LAN can have a separate access control setting.

1. Access Z-1's web page and click **Access Control** on the page menu.

Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The access control page appears. Set **Enable**/**Disable** to the following items and click **Submit**.



Note

- To continue updating settings in other pages, wait restarting Z-1 until all updates are done.

3. The restart page shows up. The update settings will be applied after Z-1 restarts. Click **Restart**.

4. After the restart, the login page appears. Now, the access control setting has been completed.

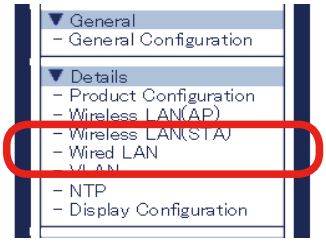
6-5-2. How to Accept/Block Specific Wired LAN Devices

This chapter shows how to register MAC addresses of wired LAN devices to accept or block connections to Z-1.

TIP

- Before going to the step below, check MAC addresses of the target devices.

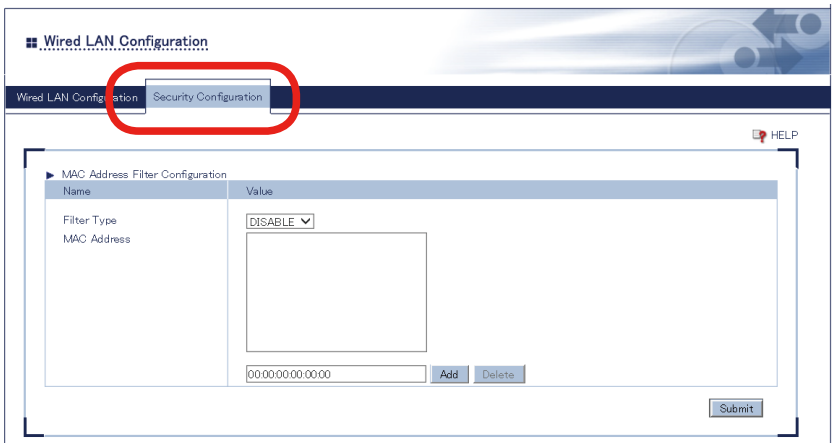
1. Access the web page and click **Wired LAN** on the page menu.



Note

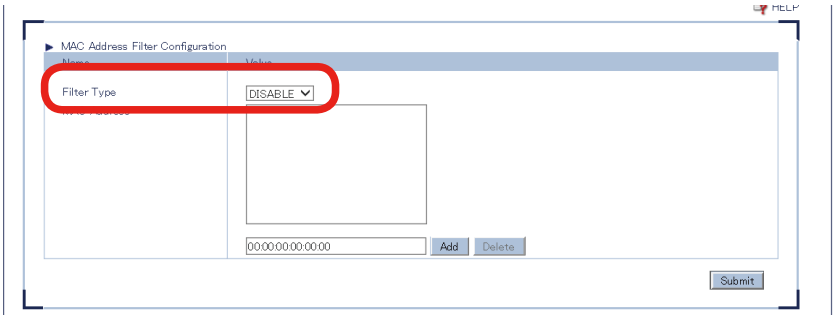
- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The wired LAN setting page appears. Click the tab of **Security Configuration**.

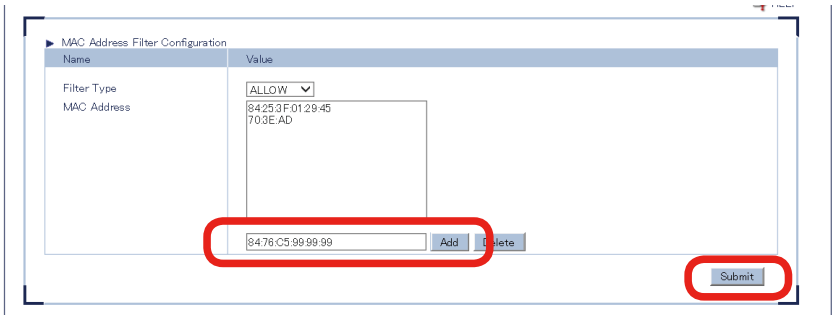


3. Select the filter type under MAC Address Filter Settings.

- ALLOW: Accepts only the registered wired LAN devices to connect to Z-1.
- DENY: Blocks the registered wired LAN devices to connect to Z-1.



4. Enter the MAC address of the wired LAN device in the MAC address input box, and click **Add**. Repeat adding MAC addresses to register multiple devices. Click **Submit** after all MAC addresses have been registered.



TIP

- When the page is switch to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. To access other pages, click **Submit** to save the entered values.

Note

- MAC addresses must be the form of "XX:XX:XX:XX:XX:XX".
- The vender code (the first 6 characters of MAC address) can be registered alone. In that case, wired devices having the vendor code will be accepted or blocked.
- To delete the registered MAC addresses, select them and click **Delete**.

5. The restart page shows up. The new settings will be applied after Z-1 restarts. Click **Restart**.

Note

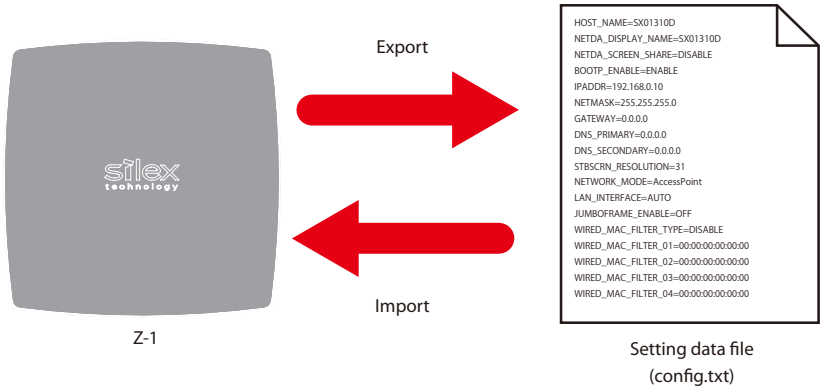
- To continue updating settings in other pages, wait restarting Z-1 until all updates are done.

6. After the restart, close the web browser.

6-6. Administrative Functions

6-6-1. Export/Import of Setting Data

This chapter explains how to export/import the setting data. The export function saves Z-1's setting information as a file (config.txt) in external hardware. The import function reads and applies the saved setting data to Z-1. Since the import and export can be done from the web page, use a web browser for the operation.



TIP

- Only the exported setting data file should be imported.
- Do not change the file name or the content of the exported setting data file, otherwise the file may not be imported.
- If the firmware version is different from when Z-1 exported the setting data file, Z-1 may not be able to import the file.

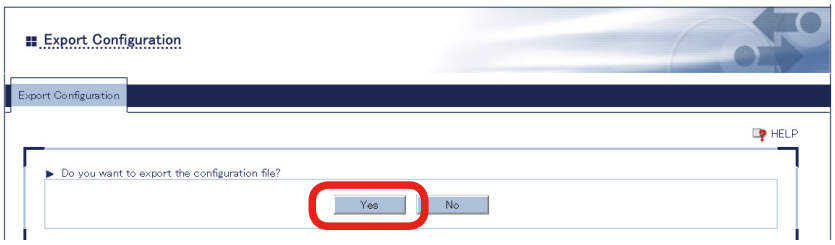
Export Setting from Web Page

1. Access Z-1's web page and click **Export Configuration** on the page menu.

Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The export setting page appears. Click **Yes**.



3. The confirmation dialog appears and asks where to save the setting data file (config.txt). Click **Save**.

Note

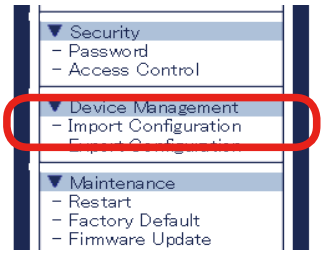
- Click [▼] and "**Save as**" function will appear.

Import Setting from Web Page

TIP

- When importing the setting that uses a certificate, the certificate needs to be imported beforehand.

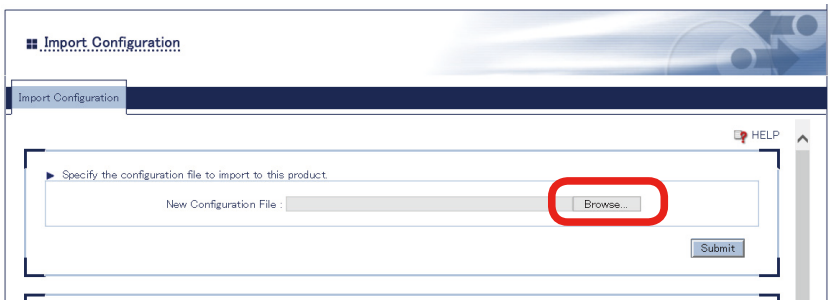
1. Access Z-1's web page and click **Import Configuration** on the page menu.



Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

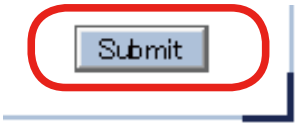
2. The import setting page appears. Click **Browse**, select the setting data file (config.txt) to import from the file dialog, and click **Open**.



Note

- The importing setting data file has to be the one exported from Z-1.

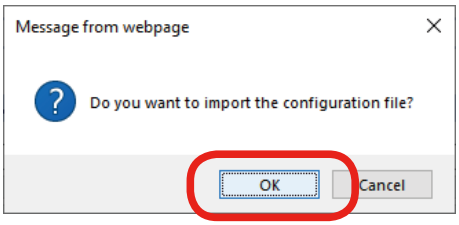
3. Check the specified file is shown at **New Configuration File**, and click **Submit**.



TIP

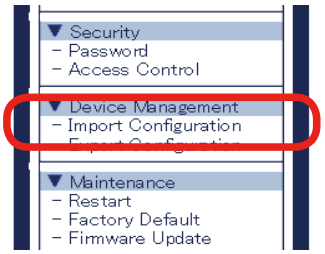
- When the page is switch to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. To access other pages, click **Submit** to save the entered values.

4. The check dialog for file import appears. Click **OK** and the file import begins.



Import Certificate from Web Page

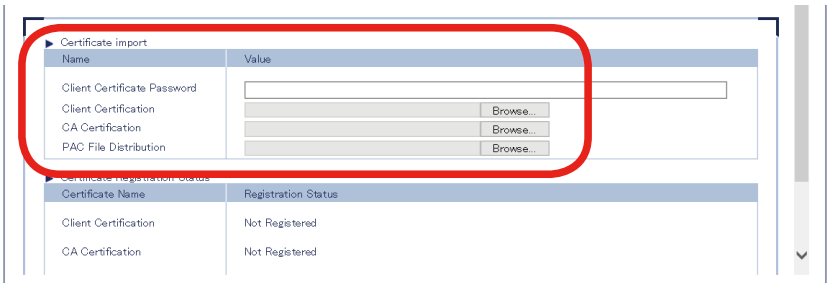
1. Access Z-1's web page and click **Import Configuration** on the page menu.



Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The import setting page appears. Register the certificate to use for the IEEE802.1X authentication.



3. Click **Submit**.
When the restart is completed, the login page appears.

TIP

- When the page is switch to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. To access other pages, click **Submit** to save the entered values.

6-7. Maintenance Functions

6-7-1. Restart

The following options can restart Z-1.

- Hard reboot
- Web page

TIP

- Before restarting Z-1, make sure that there is no device connected to Z-1.

Hardware Reboot

1. Unplug the power code from the outlet.

2. Plug the power code into the outlet.

3. The standby screen appears on the display connected to Z-1. When the animation stops, Z-1 is ready to operate.

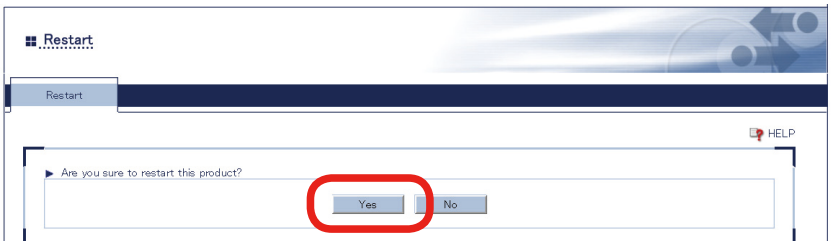
Restart from Web Page

1. Access the web page and click **Restart** on the page menu.

Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The restart page appears. Click **Yes** to restart Z-1.



3. After the restart, the login page appears . Close the web browser.

6-7-2. Factory Reset

Here are some examples why the user should restore the factory default settings to Z-1:
- Will change the settings because the Z-1 was used for the other network.
- Cannot access the web page because the administration password is lost.

There are two ways for a factory reset:
- Factory reset switch
- Web page

TIP

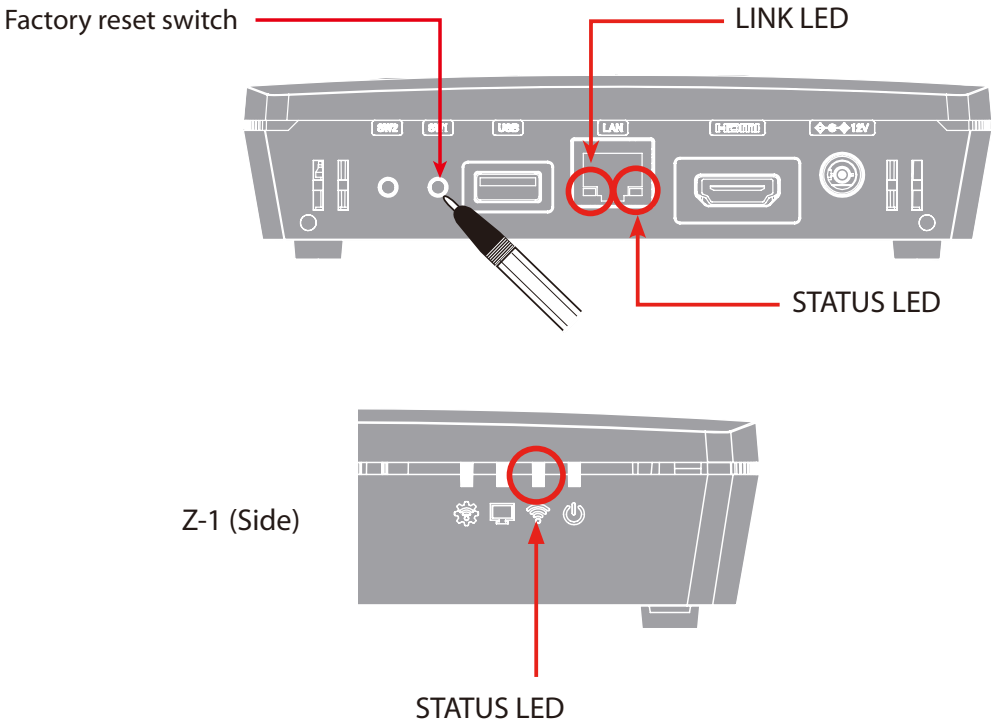
- After a factory reset, all the settings will be replaced with the factory default settings. Creating a backup of the current settings is recommended.
- Make sure that there is no device connected to Z-1 for a factory reset.
- Do not unplug the power code during a factory reset.
- Do not push the factory reset switch when Z-1 boots up after a factory reset.

How to Use Factory Reset Switch

1. Unplug the power code from the outlet.

2. Using a pen or something sharp, press and hold the factory reset switch and plug the power into the outlet. The LINK LED and STATUS LED of the LAN port will turn on. Keep holding the switch.

3. The factory reset procedure will start when the STATUS LED of the LAN port turns off. Then, release the switch. When the WLAN LED on the side turns on or blinks, Z-1 has been restored to the factory default settings.



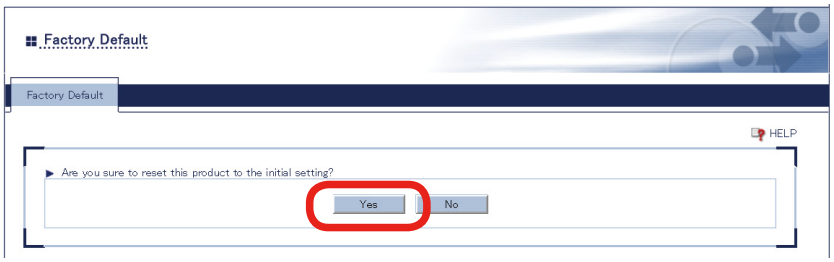
How to Factory Reset from Web Page

1. Access the web page and click **Factory Default** on the page menu.

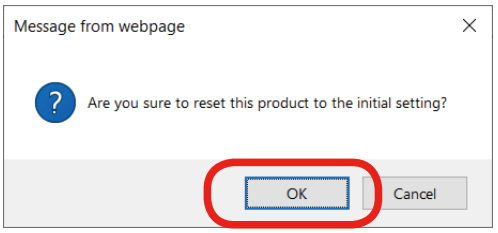
Note

- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. The factory reset page appears. Click **Yes**.



3. The confirm dialog appears. Click **OK** to initiate the factory reset.



4. Z-1 restarts after the factory reset.

5. When the factory reset is done, the login page will appear. Close the web browser.

TIP

- Since the IP address of Z-1 returns to the factory default setting, the PC will not be able to access the Z-1 and cannot show the login page. If it happens, change the IP address of Z-1 or of the PC.

6-7-3. Firmware Update

How to Download Latest Firmware

The latest firmware is published on silex technology's website. Before updating the firmware, download the latest one from the website.

1. Access our website below.

URL: https://www.silextechnology.com/

2. Go to the support page and select the product model.

3. Download the latest firmware (Z-1.bin) on the PC.

Now, you have the latest firmware.

How to Update Firmware

TIP

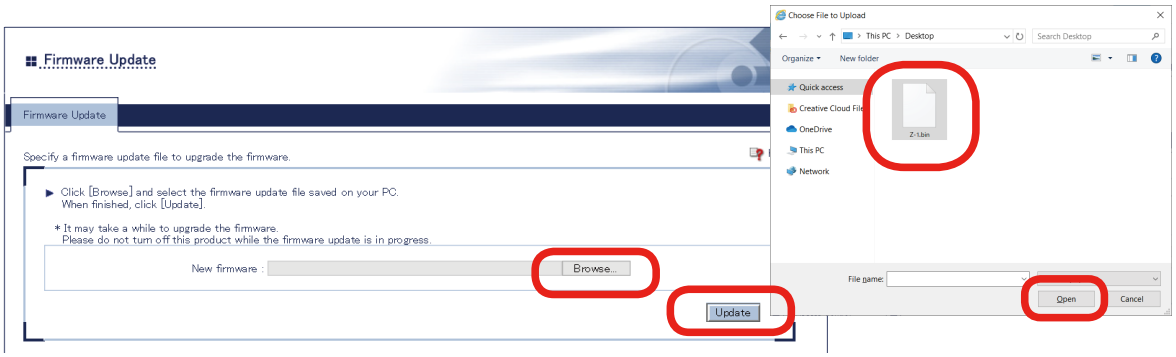
- Make sure that there is no PC connected to Z-1 before updating the firmware.
- Do not unplug the power code from the outlet while the firmware is being updated.

1. Access the web page and click **Firmware Update** on the page menu.

Note

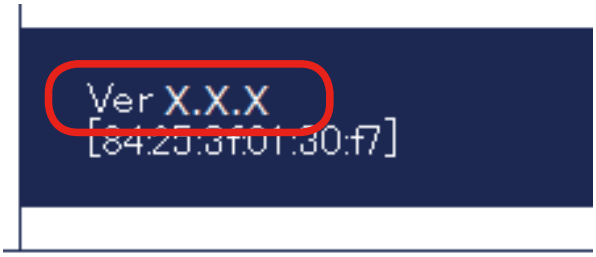
- Check "**How to Access Web Page**" in "**3-1-5 Web Pages**".

2. Click **Browse**, select the latest firmware (Z-1.bin) on the PC, and click **Update**.



3. The update confirm dialog appears. Click **OK** to update the firmware.

4. When the login page appears, check the latest version is displayed in the bottom left corner.



5. Now, the firmware has been updated. Close the web browser and unplug the power code from the outlet. Then, plug the power code again and reboot Z-1.

(Blank page)

A. Setting Items

A-1. Basic Setting Items

To change setting items from a web browser, see "**A-2. Detailed Setting Items**".

A-2. Detailed Setting Items

This chapter shows detailed setting items to be set from a web browser.

A-2-1. Z-1 Settings

Z-1 Settings

Product Configuration

Name	Host Name
Description	It sets the host name. Make sure the name is different from that of other devices.
Value/Range	1 to 15 alphanumeric characters and some symbols
Default value	SXxxxxxx (xxxxxx: Last 3 bytes of the MAC address)

Name	Display name
Description	It sets the name of Z-1 to be displayed on the dedicated application.
Value/Range	Character string (15 characters or less)
Default value	SXxxxxxx (xxxxxx: Last 3 bytes of the MAC address)

TCP/IP Configuration

Name	DHCP Client
Description	It enables or disables DHCP protocol. For Z-1 to get IP addresses automatically from the DHCP server, they should be operating in the same network.
Value/Range	Enable/Disable
Default value	Enable

Name	IP Address
Description	It specifies the IP address. When DHCP client is enabled, an IP address obtained from DHCP server will be preferentially assigned.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

Name	Subnet Mask
Description	It specifies the subnet mask. When DHCP client is enabled, a subnet mask sent by DHCP server will be preferentially assigned. When 0.0.0.0 is given, a subnet mask corresponding to the IP address's class will be automatically applied.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

Name	Default Gateway
Description	It specifies the default gateway. 0.0.0.0 (default value) disables the setting. When DHCP client is enabled, a default gateway obtained from DHCP server will be preferentially assigned.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

DNS Configuration

Name	DNS Server (Primary)
Description	It specifies DNS primary server address. When DHCP client is enabled, DNS server obtained from DHCP server will be preferentially assigned.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

Name	DNS Server (Secondary)
Description	It specifies DNS secondary server address. When DHCP client is enabled, DNS server obtained from DHCP server will be preferentially assigned.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

DHCP Server Configuration

Name	DHCP Server Function
Description	It enables or disables DHCP server. When Z-1 is used as DHCP server and automatically assigns an IP address to PC, choose **Enable**. When DHCP server is operating in the same network, choose **Disable**.
Value/Range	Enable/Disable
Default value	Disable

Name	Start IP Address
Description	It specifies the start IP address when DHCP server function is enabled.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	192.168.0.11

Name	End IP Address
Description	It specifies the end IP address when DHCP server function is enabled.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	192.168.0.254

Name	Subnet Mask
Description	It specifies the subnet mask for the assigned IP address. When 0.0.0.0 is given, a subnet mask corresponding to the assigned start IP address will be automatically used.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	255.255.255.0

Name	Default Gateway
Description	It specifies the default gateway. "0.0.0.0 (default value)" disables the setting.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

Name	Lease Time
Description	It specifies the lease time. When 0 days 0 hours 0 minutes are given, the lease time period is 10 days.
Value/Range	0 days 0 hours 0 minutes to 44 days 23 hours 59 minutes
Default value	0 days 0 hours 0 minutes

A-2-2. Wireless LAN (AP) Setting Items

Basic Settings

Wireless LAN Common Configuration

Name	Network Mode
Description	It sets the network operation mode.
Value/Range	AccessPoint Station Wired
Default value	AccessPoint

Name	Wireless Mode
Description	It sets the type of IEEE 802.11 wireless standards for Z-1.
Value/Range	[2.4 GHz] 802.11b: Communication in IEEE 802.11b 802.11b/g: Communication in IEEE 802.11b and IEEE 802.11g 802.11n/b/g: Communication in IEEE 802.11n, IEEE 802.11b, and IEEE 802.11g [5GHz] 802.11a: Communication in IEEE 802.11a 802.11n/a: Communication in IEEE 802.11n and IEEE 802.11a 802.11ac: Communication in IEEE 802.11ac
Default value	802.11ac

Name	Channel Bandwidth
Description	It specifies the frequency bandwidth when the wireless mode is **802.11n/b/g**, **802.11n/a** or **802.11ac**. Frequency bands are divided in a wireless LAN so that multiple wireless devices can communicate at once. Segmented bands are called channels. The frequency bandwidth is 20 MHz per channel in the wireless LAN. When the channel bandwidth is 40 MHz or 80 MHz, the data amount per traffic increases and Z-1 can attain the high-speed communication. 80 MHz is only available when the wireless mode is 802.11ac.
Value/Range	20 MHz/40 MHz/80 MHz
Default value	40 MHz

Name	Channel
Description	It specifies a channel used in the wireless LAN. Channels are divided frequency bands. Frequency bands are divided in a wireless LAN so that multiple wireless devices can communicate at once.
Value/Range	[2.4 GHz] 1 to 13 [5 GHz] W52: 36 / 40 / 44 / 48 W53: 52 / 56 / 60 / 64 W56: 100 / 104 / 108/ 112 / 116 / 120 / 124 / 128 / 132 / 136 / 140 W58: 149 / 153 / 157/ 161 / 165 [AUTO] AUTO * When Z-1's communication becomes unstable due to radio interference from other wireless products, change the channel. * Channels for W53 and W56 cannot make communication in one minute after Z-1 starts up or when Z-1 detects radar wave.
Default value	36

Name	Ext Channel
Description	It shows an extended channel to use. This setting can be applied only when the channel bandwidth is set to 40 MHz.
Value/Range	The extended channel setting depends on the communication channels.
Default value	40

Name	DFS Primary Channel
Description	It specifies a channel to be switched when the communication channel is subject to DFS and radar waves are detected. When the alternative channel is not specified or when radar waves are detected on the switched channel, Z-1 will switch the channel in the certain order. This setting is applied only when the communication channel is in W53 or W56 band.
Value/Range	When the communication channel is in: W53: A channel in W53 band or NONE. W56: A channel in W56 band or NONE.
Default value	NONE

Name	Transmit Power Level
Description	It specifies the strength of radio transmission in the wireless LAN. When the strength is reduced, Z-1's radio communication range will be shortened and the area where Z-1 can be searched will be narrowed. Narrowing down the search area may avoid causing interference to other wireless networks.
Value/Range	5 / 10 / 15 / 20 / 25 / 30 / 35 / 40 / 45 / 50 / 55 / 60 / 65 / 70 / 75 / 80 / 85 / 90 / 95 / 100
Default value	100

Wireless LAN Basic Configuration

Name	Interface
Description	It enables or disables wireless interface settings (#1 to #4).
Value/Range	Enable/Disable
Default value	Wireless LAN 1: Enable Wireless LAN 2: Disable Wireless LAN 3: Disable Wireless LAN 4: Disable

Name	SSID
Description	It specifies SSID of wireless LAN to connect to Z-1. SSID is an identification for groups to communicate in a wireless LAN. Devices need to have the same SSID to communicate in the same wireless LAN.
Value/Range	1 to 32 alphanumeric character(s)

Default value	Wireless LAN1: SXxxxxxx Wireless LAN2: SXxxxxxx_2 Wireless LAN3: SXxxxxxx_3 Wireless LAN4: SXxxxxxx_4 (xxxxxx: Last 3 bytes of the MAC address)

Name	WirelessLAN VLAN ID 1 to 4
Description	It specifies VLAN ID for wireless interfaces.
Value/Range	1 to 4094
Default value	Wireless LAN1: 1 Wireless LAN2: 1 Wireless LAN3: 1 Wireless LAN4: 1

Name	Stealth Mode
Description	It enables or disables the stealth mode functions.
Value/Range	Enable/Disable
Default value	Wireless LAN1: Disable Wireless LAN2: Disable Wireless LAN3: Disable Wireless LAN4: Disable

Name	Network Authentication
Description	It specifies the authentication method used for communicating with wireless devices. WPA/WPA2 is recommended for robust security. AES is only accepted for IEEE 802.11n.
Value/Range	Open (Open system): Accepts all access without performing authentication. WEP is used for encryption of the communication. Shared (Shared key): Uses WEP key for encryption as the authentication key, and allows access of devices having the same key. WEP is used for encryption of the communication. WPA-PSK: Uses PSK for network authentication. The communication encryption method is chosen from TKIP/AES/AUTO. The encryption key is generated with a wireless device based on the shared key. WEP key setting will not be used. WPA2-PSK: Uses PSK for network authentication. The communication encryption method is chosen from AES/AUTO. The encryption key is generated with a wireless device based on the shared key. WEP key setting will not be used. WPA/WPA2-PSK: Both WPA-PSK and WPA2-PSK can be used. 802.1X: Provides IEEE 802.1X's user authentication and makes encrypted communications using dynamic WEP.

Value/Range	WPA-Enterprise: Provides IEEE 802.1X's user authentication and makes encrypted communications using TKIP/AES/AUTO. WPA2-Enterprise: Provides IEEE 802.1X's user authentication and makes encrypted communications using AES/AUTO. WPA/WPA2-Enterprise: Provides IEEE 802.1X's user authentication and makes encrypted communications using AES/AUTO.
Default value	Wireless LAN 1: WPA2-PSK Wireless LAN 2: Open Wireless LAN 3: Open Wireless LAN 4: Open

WEP Configuration

Name	WEP
Description	It enables (**ON**) or disables (**OFF**) the WEP encryption functions when the network authentication is Open. When WEP encryption is used, transmit data will be encrypted in the wireless LAN based on the settings of WEP keys (1 to 4) and Key index.
Value/Range	ON / OFF
Default value	Wireless LAN1: OFF Wireless LAN2: OFF Wireless LAN3: OFF Wireless LAN4: OFF

Name	Key Index
Description	It specifies the WEP key numbers from 1 to 4. The key index has to be the same as that of communicating devices.
Value/Range	1 to 4
Default value	Wireless LAN1: 1 Wireless LAN2: 1 Wireless LAN3: 1 Wireless LAN4: 1

Name	WEP Key (1 to 4)
Description	It specifies the WEP key.
Value/Range	5 or 10-digit alphanumeric characters 10 or 26 hexadecimal digits * Alphanumeric characters usually mean single-byte alphabets and numbers. * When the size of key (key length) is 64 bits, enter 5 characters. When it is 128 bits, enter 13 characters. * Hexadecimal digits should be a combination of numbers (0 to 9) and alphabets (A to F). * When the key length is 64 bits, enter 10 hexadecimal digits. When it is 128 bits, enter 26 hexadecimal digits.

Default value	Wireless LAN1: None Wireless LAN2: None Wireless LAN3: None Wireless LAN4: None

WPA/WPA2 Configuration

Name	Encryption Mode
Description	The encryption algorithm has to be selected when the network authentication method is set to one of the following: WPA-PSK WPA2-PSK WPA/WPA2-PSK WPA-Enterprise WPA2-Enterprise WPA/WPA 2-Enterprise
Value/Range	TKIP / AES / AUTO
Default value	Wireless LAN1: AES Wireless LAN2: AES Wireless LAN3: AES Wireless LAN4: AES

Name	Pre-Shared Key
Description	The pre-shared key should be specified when the encryption algorithm is TKIP or AES because the network authentication method is set to one of the following: WPA-PSK WPA2-PSK WPA/WPA2-PSK The pre-shared key is a key word to generate an encryption key. It is called a network key or password for some wireless LAN devices.
Value/Range	8 to 63 alphanumeric characters 64 hexadecimal digits
Default value	Wireless LAN1: SXxxxxxx Wireless LAN2: SXxxxxxx_2 Wireless LAN3: SXxxxxxx_3 Wireless LAN4: SXxxxxxx_4 (xxxxxx: Generated from the MAC address)

Name	Group key renew interval
Description	It specifies the update interval for the encryption key in minutes. Zero (0) disables the setting.
Value/Range	0 to 1440
Default value	Wireless LAN1: 60 Wireless LAN2: 60 Wireless LAN3: 60 Wireless LAN4: 60

RADIUS Server Configuration

Name	Server IP
Description	It specifies the IP address of RADIUS server. It is only applied when the network authentication method is 802.1X, WPA-Enterprise, WPA2-Enterprise, or WPA/WPA2-Enterprise.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

Name	Port Number
Description	It specifies the port number used for communication with RADIUS server.
Value/Range	0 to 65535
Default value	1812

Name	Shared Secret
Description	It specifies the secret key used for communication with RADIUS server.
Value/Range	0 to 32 alphanumeric characters
Default value	None

Extended Settings

Extension Configuration

Name	Beacon Interval(msec)
Description	It sets the interval to send beacons in milliseconds.
Value/Range	20 to 1000
Default value	100

Name	DTIM
Description	It sets the DTIM interval for the wireless LAN.
Value/Range	1 to 255
Default value	1

Name	RTS Threshold
Description	It sets the threshold value for RTS transmission.
Value/Range	1 to 2346
Default value	2346

Name	A-MPDU
Description	It enables (**ON**) or disables (**OFF**) the A-MPDU setting. When **ON** is selected, the throughput may increase. This setting is applied only when the wireless mode is **802.11n/b/g**, **802.11n/a** or **802.11ac**.
Value/Range	ON/OFF
Default value	ON

Name	Short Guard Interval
Description	It enables (**ON**) or disables (**OFF**) the Short Guard Interval setting. When **ON** is selected, the throughput may increase. This setting is applied only when the wireless mode is **802.11n/b/g**, **802.11n/a** or **802.11ac**.
Value/Range	ON/OFF
Default value	ON

QoS(WMM) Configuration(for AP)

Name	ECWmin
Description	It changes WMM-EDCA setting items of Z-1 (QoS settings for each access category).
Value/Range	1 to 15
Default value	BE: 4 BK: 4 VI: 3 VO: 2

Note

Abbreviations

- BE: Best Effort
- BK: Back Ground
- VI: Video
- VO: Voice

Name	ECWmax
Description	It changes WMM-EDCA setting items of Z-1 (QoS settings for each access category).
Value/Range	1 to 15
Default value	BE: 6 BK: 10 VI: 4 VO: 3

Name	AIFSN
Description	It changes WMM-EDCA setting items of Z-1 (QoS settings for each access category).
Value/Range	1 to 15
Default value	BE: 3 BK: 7 VI: 1 VO: 1

Name	TxOPLimit
Description	It changes WMM-EDCA setting items of Z-1 (QoS settings for each access category).
Value/Range	0 to 8192
Default value	BE: 0 BK: 0 VI: 3008 VO: 1504

QoS(WMM) Configuration(for Station)

Name	ECWmin
Description	It changes WMM-EDCA setting items of stations (QoS settings for each access category).
Value/Range	1 to 15
Default value	BE: 4 BK: 4 VI: 3 VO: 2

Name	ECWmax
Description	It changes WMM-EDCA setting items of stations (QoS settings for each access category).
Value/Range	1 to 15
Default value	BE: 10 BK: 10 VI: 4 VO: 3

Name	AIFSN
Description	It changes WMM-EDCA setting items of stations (QoS settings for each access category).
Value/Range	1 to 15
Default value	BE: 3 BK: 7 VI: 2 VO: 2

Name	TxOPLimit
Description	It changes WMM-EDCA setting items of stations (QoS settings for each access category).
Value/Range	0 to 8192
Default value	BE: 0 BK: 0 VI: 3008 VO: 1504

Name	ACM
Description	It changes WMM-EDCA setting items of Z-1 and stations (QoS settings for each access category).
Value/Range	ON/OFF
Default value	BE: OFF BK: OFF VI: OFF VO: OFF

Security Settings

Security Configuration

Name	Privacy Separator
Description	It allows (**ON**) or denies (**OFF**) communication between wireless LAN stations connected to Z-1. A wireless interface with the enabled privacy separator forwards wireless frames not to the other wireless interface but only to the wired LAN interface.
Value/Range	ON/OFF
Default value	OFF

MAC Address Filter Configuration

Name	Filter Type
Description	It specifies the security type of the MAC address filter.
Value/Range	DISABLE: Enables all wireless stations to communicate with Z-1. ALLOW: Accepts only the registered wireless LAN stations to connect to Z-1. DENY: Blocks the registered wireless LAN stations to connect to Z-1.
Default value	DISABLE

Name	MAC Address
Description	MAC address or the vendor code of MAC addresses (1 to 50)
Value/Range	00:00:00:00:00:01 to FF:FF:FE:FF:FF:FF or 00:00:00 to FF:FF:FE
Default value	00:00:00:00:00:00

Smart Wireless Setup

Smart Wireless Setup

Name	Smart Wireless Setup
Description	It enables or disables the smart wireless setup.
Value/Range	Enable/Disable
Default value	Enable

Name	Interface
Description	It selects the wireless interface to execute the smart wireless setup.
Value/Range	8 to 63 alphanumeric characters 64 hexadecimal digits
Default value	Wireless LAN1: [1] SXxxxxxx Wireless LAN2: [2] SXxxxxxx_2 Wireless LAN3: [3] SXxxxxxx_3 Wireless LAN4: [4] SXxxxxxx_4 (xxxxxx: Generated from the MAC address)

Name	External Registrar
Description	It enables or disables the external registrar.
Value/Range	Enable/Disable
Default value	Disable

Name	PIN Code
Description	It specifies the PIN code of Z-1.
Value/Range	8-digit number (decimal)
Default value	Unique to each Z-1.

A-2-3. Wireless LAN (STA) Setting Items

Basic Settings

Wireless LAN Common Configuration

Name	Network Mode
Description	It sets the operation mode for the network.
Value/Range	AccessPoint Station Wired
Default value	AccessPoint

Wireless LAN Basic Configuration

Name	SSID
Description	It sets SSID of the wireless LAN to connect to Z-1. SSID is an identification for groups to communicate in a wireless LAN. Devices need to have the same SSID to communicate in the same wireless LAN.
Value/Range	1 to 32 alphanumeric character(s)
Default value	SXxxxxxx (xxxxxx: Last 3 bytes of the MAC address)

Name	Network Authentication
Description	It specifies the network authentication method for the wireless LAN.
Value/Range	Open (Open system): Accepts all access without performing authentication. WEP is used for encryption of the communication. Shared (Shared key): Uses WEP key for encryption as the authentication key, and allows access of devices having the same key. WEP is used for encryption of the communication. WPA-PSK: Uses PSK for network authentication. The communication encryption method is chosen from TKIP/AES/AUTO. The encryption key is generated with a wireless device based on the pre-shared key. WEP key setting will not be used. WPA2-PSK: Uses PSK for network authentication. The communication encryption method is chosen from AES/AUTO. The encryption key is generated with a wireless device based on the shared key. WEP key setting will not be used. WPA/WPA2-PSK: Both WPA-PSK and WPA2-PSK can be used. WPA-Enterprise: Provides IEEE 802.1X's user authentication and makes encrypted communications using TKIP/AES/AUTO.

Value/Range	WPA2-Enterprise: Provides IEEE 802.1X's user authentication and makes encrypted communications using AES/AUTO. WPA/WPA2-Enterprise: Provides IEEE 802.1X's user authentication and makes encrypted communications using AES/AUTO. * The following authentication methods and encryption communications are not available for 802.11n/802.11ac: Shared, 802.1X, WEP, and TKIP.
Default value	Open

Name	Encryption Mode
Description	It selects the encryption algorithm (TKIP/AES/AUTO) for the following network authentication methods: • WPA-PSK • WPA2-PSK • WPA/WPA2-PSK • WPA-Enterprise • WPA2-Enterprise • WPA/WPA2-Enterprise *When the network authentication method is one of the following, TKIP cannot be selected: • WPA2-PSK • WPA/WPA2-PSK • WPA2-Enterprise • WPA/WPA2-Enterprise
Value/Range	TKIP AES AUTO
Default value	AES

WEP Configuration

Name	WEP
Description	It enables (**ON**) or disables (**OFF**) the WEP encryption communication function. It is only applied when the authentication method is Open.
Value/Range	ON / OFF
Default value	OFF

Name	Key Index
Description	It sets the number (1 to 4) of WEP key to use. The key index has to be the same as that of communicating device.
Value/Range	1 to 4
Default value	1

Name	WEP Key (1 to 4)
Description	It sets WEP key. For hexadecimal key input: When the key size is 64 bits, enter 10 hexadecimal digits. When it is 128 bits, enter 26 hexadecimal digits. For alphanumeric key input: When the key size is 64 bits, enter 5 alphanumeric characters. When it is 128 bits, enter 13 characters.
Value/Range	5 or 10-digit alphanumeric characters 10 or 26 hexadecimal digits
Default value	None

WPA/WPA2 PSK Configuration

Name	Pre-Shared Key
Description	It needs to be specified when the authentication method is one of the following: WPA-PSK WPA2-PSK WPA/WPA2-PSK
Value/Range	8 to 63 alphanumeric characters 64 hexadecimal digits
Default value	xxxxxxxx xxxxxx: Generated from the MAC address

WPA/WPA2 EAP Configuration

Name	Authentication Method
Description	It selects the authentication method (EAP-TLS/EAP-TTLS/PEAP/EAP-FAST/LEAP) for IEEE 802.1X authentication.
Value/Range	EAP-TLS EAP-TTLS PEAP EAP-FAST LEAP
Default value	EAP-TLS

Name	EAP User Name
Description	It specifies the EAP user name used for IEEE 802.1X authentication. The server uses the EAP user name to identify the client.
Value/Range	Character string (64 characters or less)
Default value	None

Name	Client Certificate Password
Description	It sets the password of client certificate used for IEEE 802.1X's client authentication. It is needed when the client certificate has a password setting.
Value/Range	Character string (32 characters or less)
Default value	None

Name	Client Certification
Description	It selects a client certificate used for IEEE 802.1X's client authentication. It is applied when the authentication method is set to EAP-TLS.
Value/Range	Select a file.
Default value	-

Name	EAP Password
Description	It specifies an EAP password used for IEEE 802.1X authentication. The EAP password is used to check the credibility of the client device. This setting is applied when the authentication method is EAP-TTLS, PEAP, EAP-FAST or LEAP.
Value/Range	Character string (32 characters or less)
Default value	None

Name	Inner Authentication Method
Description	It sets the internal authentication method (PAP/CHAP/MSCHAP/MSCHAPv2) that will be conducted during TLS tunneling for IEEE 802.1X authentication. When the authentication method is PEAP, the internal authentication is fixed to MS-CHAPv2.
Value/Range	PAP CHAP MSCHAP MSCHAPv2
Default value	PAP

Name	Auto PAC Provisioning
Description	It enables (**ON**) or disables (**OFF**) automatic distribution of PAC (Protected Access Credential) for EAP-FAST authentication method. When the setting is disabled, a PAC file generated by the server needs to be registered.
Value/Range	ON/OFF
Default value	OFF

Name	PAC File Distribution
Description	It registers a PAC (Protected Access Credential) file generated by the server. The PAC file will be manually distributed for EAP-FAST authentication method.
Value/Range	Select a file.
Default value	-

Name	PAC File Password
Description	It is a password sets to the PAC file.
Value/Range	Character string (63 characters or less)
Default value	None

Name	Server authentication
Description	It accepts or denies the credibility check of the server under IEEE 802.1X authentication. When it is **ON**, CA certificate for server authentication will be needed.
Value/Range	ON/OFF
Default value	OFF

Smart Wireless Setup

Name	Smart Wireless Setup
Description	It enables or disables the smart wireless setup.
Value/Range	Enable/Disable
Default value	Enable

Name	PIN Code
Description	It specifies Z-1's PIN code.
Value/Range	8-digit number (decimal)
Default value	Unique to each Z-1.

A-2-4. Wired LAN Setting Items

Wired LAN Settings

Name	Link Speed
Description	It specifies the physical network type. Use AUTO for regular operation. When the connected hub's LINK lamp does not turn on while Z-1 is booting up, change the setting to that of the connected hub.
Value/Range	AUTO 100BASE-TX-Half 100BASE-TX-Full 1000BASE-T-Full
Default value	AUTO

Security Settings

MAC Address Filter Configuration

Name	Filter Type
Description	DISABLE: Enables communications from all the devices. DENY: Blocks communications from devices registered in the list of MAC address filter. ALLOW: Accepts communications from devices registered in the list of MAC address filter.
Value/Range	DISABLE ALLOW DENY
Default value	DISABLE

Name	MAC Address
Description	MAC address or the vendor code of MAC addresses (1 to 10)
Value/Range	00:00:00:00:00:01 to FF:FF:FE:FF:FF:FF or 00:00:00 to FF:FF:FE
Default value	00:00:00:00:00:00

A-2-5. VLAN Setting Items

IEEE802.1Q VLAN Configuration

Name	VLAN
Description	It enables or disables the VLAN tagging function complaint with IEEE802.1Q. When it is set to **Enable**, the wired LAN port will be the trunk port and the wireless LAN will be the access port to build VLAN. To relay packets to the wired LAN from the wireless LAN, IEEE802.1Q tags will be added to the packet frames. Meanwhile, packets from the wired LAN can be received only in the wireless LAN which has the same VLAN ID as the frame tag.
Value/Range	Enable/Disable
Default value	Disable

Name	Native VLAN ID
Description	It sets the native VLAN ID of the wired LAN port. When a packet without VLAN tag is received from the wired LAN, it will be handled as a packet of the specified VLAN ID.
Value/Range	1 to 4094
Default value	1

Name	Management VLAN ID
Description	It sets the management VLAN ID to enable access to Z-1. When the VLAN function is enabled, network groups without the management VLAN ID cannot access Z-1.
Value/Range	1 to 4094
Default value	1

TCP/IP Configuration

Name	WirelessLAN VLAN ID 1 to 4
Description	It sets VLAN ID used for wireless interfaces.
Value/Range	1 to 4094
Default value	1

Name	DHCP Client
Description	It enables or disables the DHCP client function. To set the IP address with DHCP, the DHCP server has to be in the subnetwork.
Value/Range	Enable/Disable
Default value	Disable

Name	IP Address
Description	It specifies the IP address. When DHCP client is enabled, an IP address obtained from DHCP server will be preferentially assigned.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

Name	Subnet Mask
Description	It specifies the subnet mask. When 0.0.0.0 is given (default setting), a subnet mask corresponding to the IP address will be automatically applied. When DHCP client is enabled, a subnet mask sent by DHCP server will be preferentially assigned.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

A-2-6. NTP Setting Items

NTP Configuration

Name	NTP
Description	It enables or disables NTP protocol.
Value/Range	Enable/Disable
Default value	Disable

Name	NTP Server
Description	It specifies the host name or the IP address of the NTP server.
Value/Range	0 to 128 alphanumeric characters
Default value	None

Name	Local Time Zone
Description	It specifies the Local time zone.
Value/Range	-12:00 to 12:00
Default value	[US] +9:00 [EU] +01:00

A-2-7. Display Setting Items

Display Configuration

Name	Initial Presentation Mode
Description	It selects the projection mode used at startup.
Value/Range	Z-1 will operate in one of the following modes: • Single Presenter • Multi Presenter • Distribution Master • Distribution Slave • Pair Display
Default value	Single Presenter

Name	Show Connection Info
Description	It enables or disables the connection information (the host name, IP address, and SSID) to be displayed on the OSD setting page.
Value/Range	Enable/Disable
Default value	Enable

Name	Allow presenter interrupt
Description	It allows switching to a new connection when the projection is being handled.
Value/Range	Enable/Disable
Default value	Enable

Pair Display Config

Name	Pair 1 to 10 (Name)
Description	It registers communicating devices to be in pairs. 10 devices can be registered (Pair 1 to 10).
Value/Range	1 to 15 alphanumeric characters
Default value	None

Name	Pair 1 to 10 (IP Address)
Description	It registers communicating devices to be in pairs. 10 devices can be registered (Pair 1 to 10).
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

Recent Pairing

Name	Clear Recent Pairing
Description	It deletes all the records of pair devices. Note that it clears everything.
Value/Range	None
Default value	None

A-3. Security Setting Items

A-3-1. Password Setting Items

Please input the password.

Name	New Password
Description	It sets the administrator password with an ASCII character string (8 characters or less). The password is used for authentication when the user tries to update settings from a web browser or to use the total management software AMC Manager® (non-free license).
Value/Range	0 to 8 alphanumeric characters
Default value	None

A-3-2. Access Control Setting Items

Access Control

Name	HTTP
Description	It controls access from the wired/wireless LAN via HTTP. **Enable** allows access whereas **Disable** denies access to Z-1.
Value/Range	Enable/Disable
Default value	Wired LAN: Enable Wireless LAN: Enable

Name	HTTPS
Description	It controls access from the wired/wireless LAN via HTTPS. **Enable** allows access whereas **Disable** denies access to Z-1.
Value/Range	Enable/Disable
Default value	Wired LAN: Enable Wireless LAN: Enable

Name	SNMP
Description	It controls access from the wired/wireless LAN via SNMP. **Enable** allows access whereas **Disable** denies access to Z-1.
Value/Range	Enable/Disable
Default value	Wired LAN: Enable Wireless LAN: Enable

Name	Device Server
Description	It controls access from the wired/wireless LAN when Z-1's device server function is used. **Enable** allows access whereas **Disable** denies access to Z-1.
Value/Range	Enable/Disable
Default value	Wired LAN: Disable Wireless LAN: Disable

Name	Screen Projection
Description	It controls access from the wired/wireless LAN when Z-1's display function is used. **Enable** allows access whereas **Disable** denies access to Z-1.
Value/Range	Enable/Disable
Default value	Wired LAN: Enable Wireless LAN: Enable

CIFS / SMB Server Configuration

Name	User
Description	It sets the user account. **Guest** allows all users' access. **User** requires the user authentication.
Value/Range	Guest/User
Default value	Guest

Name	User Name
Description	It is a user name used for the file sharing function, and needed when the user setting is **User**. The user name is used to access the shared folder of Z-1. When no name is given, the operation will be similar to when the user setting is **Guest**.
Value/Range	Character string (20 characters or less)
Default value	None

Name	Password
Description	It is for user authentication when the user setting is **User**.
Value/Range	Character string (31 characters or less, password)
Default value	None

A-4. Administrative Function Setting Items

A-4-1. Import Setting Information

Name	New Configuration File
Description	It imports a setting file to change settings of Z-1 at once.
Value/Range	Select a new setting file.
Default value	-

Certificate import

Name	Client Certificate Password
Description	It sets the password of client certificate used for IEEE 802.1X's client authentication. It is needed when the client certificate has a password setting.
Value/Range	Character string (32 characters or less)
Default value	-

Name	Client Certification
Description	It selects a client certificate used for IEEE 802.1X's client authentication. It is applied when the authentication method is set to EAP-TLS.
Value/Range	Select a file.
Default value	-

Name	CA Certification
Description	Select a CA certificate to use for server authentication on the IEEE 802.1X authentication.
Value/Range	Select a file.
Default value	-

Name	PAC File Distribution
Description	It registers a PAC (Protected Access Credential) file generated by the server. The PAC file will be manually distributed for EAP-FAST authentication method.
Value/Range	Select a file.
Default value	-

A-4-2. Export Setting Information

Name	Setting file
Description	It saves the setting information as a file.
Value/Range	Yes/No
Default value	-