

Wireless Presentation Box

Z-1

User's Manual (Configuration Method)



Index

1. Introduction	1
1-1. Introduction	2
About the Notation	2
Disclaimers.....	2
Trademarks	2
1-2. Safety Instructions	3
1-3. Product Information and Customer Services	7
Product Information.....	7
Customer Support Center	7
2. Product Specifications	9
2-1. Features.....	10
2-2. Parts and Functions	11
2-3. Specifications.....	16
2-3-1. Hardware Specifications	16
2-3-2. Software Specifications.....	22
2-3-3. Others.....	24
2-3-4. Restrictions	25
2-4. Radio Waves	27
2-5. DFS Function.....	29
3. Network Configuration	31
3-1. Configuration on Web Page.....	32
3-1-1. Necessary Items.....	32
3-1-2. Connecting Display to Z-1	33
3-1-3. Turning on Z-1	34
3-1-4. Connecting Windows PC	36
3-1-5. Z-1's Web Page	38
How to Access the Web Page.....	38
How to Log Out.....	40

3-1-6. Configuration on Web Page	41
Basic Network Configuration	41
Detailed Network Configuration	43
3-1-7. Initial Configuration Wizard.....	45
3-1-8. Chairperson Menu Page	46
3-2. Wireless Configuration Using Smart Wireless Setup (STA)	47
3-2-1. Before Setup.....	47
3-2-2. Push Button Method	47
Wireless Configuration Using Function Switch	48
Wireless Configuration Using PC	49
3-2-3. PIN Code Method.....	51
4. Projection to Connected Display	53
4-1. Projection Mode Setting.....	54
4-1-1. Projection Mode Type.....	54
Single Presenter mode	54
Multi-Presenter Mode.....	55
Distribution Master/Slave Mode.....	56
Pair Display Mode.....	58
4-1-2. Projection Mode Change	59
How to Change Projection Mode Using Function Switch	59
How to Change Projection Mode Using OSD Icon.....	60
How to Change Projection Mode Using Web Page.....	60
4-2. Projecting Screen to Display	62
4-2-1. Device Preparation	62
4-2-2. Starting Projection.....	62
5. Use of Wireless Access Point Function	63
5-1. Connecting Wireless Stations.....	64
5-1-1. Connecting Windows PC	64
5-1-2. Use of Function Switch to Connect	65
5-1-3. Use of Web Page to Connect.....	66

Use of Push Button Method	67
Use of PIN Code Method	68
5-2. MAC Address Filter on Wireless Stations	69
5-3. Communication Filter on Wireless Stations	71
5-4. How to Disable Smart Wireless Setup.....	73
5-5. AP Bridge Function	75
6. Other Functions	77
6-1. Status Monitor Using Web Browser	78
6-1-1. Checking System Status	78
6-1-2. Checking Wireless LAN Status	80
6-2. Use of DHCP Server Function.....	81
6-2-1. DHCP Server Function Setting	81
6-3. Use of VLAN Function	83
6-3-1. VLAN Function.....	83
6-3-2. VLAN Function Setting	83
Checking VLAN Information.....	84
VLAN Function Setting.....	84
Connecting Z-1 to Trunk Port of VLAN HUB.....	86
6-4. Time Sync with NTP Server	87
6-4-1. What is NTP Function?.....	87
6-4-2. NTP Function Setting.....	87
6-5. Projection Authentication (PIN Code) Function.....	89
6-5-1. What is Projection Authentication Function?	89
6-5-2. Projection Authentication Function Setting	89
6-6. Device Server Function	91
6-6-1. Downloading & Installing SX Virtual Link.....	92
What is SX Virtual Link?	92
How to Download SX Virtual Link	92
How to Install SX Virtual Link	93
6-6-2. Sharing USB Devices over the Network	97
How to Start SX Virtual Link.....	97

How to Connect/Disconnect to/from USB Devices	98
How to Open the SX Virtual Link's Online Help.....	99
6-6-3. Uninstalling SX Virtual Link.....	100
6-7. Security Function	102
6-7-1. Use of Security Function.....	102
How to Change Administrator Password	102
Access Control	103
6-7-2. How to Accept/Block Specific Wired LAN Devices	104
6-7-3. How to Control Push Switch Function.....	106
6-8. Administrative Function	108
6-8-1. Export/Import of Setting Data	108
Export Setting from Web Page	108
Import Setting from Web Page	109
Import Certificate from Web Page	110
6-9. Maintenance Function.....	112
6-9-1. Restart	112
Restart Using AC Cable.....	112
Restart Using Web Page	112
6-9-2. Factory Default Configuration.....	113
Factory Default Configuration Using Reset Switch.....	113
Factory Default Configuration Using Web Page	114
6-9-3. Firmware Update.....	116
How to Download Latest Firmware	116
How to Update Firmware	117

A. Setting Items 119

A-1. General Configuration.....	120
A-2. Detailed Configuration	121
A-2-1. Product Configuration	121
Product Configuration.....	121
A-2-2. Wireless LAN (AP).....	125
Basic Settings.....	125

Extended Settings.....	132
Security	135
Smart Wireless Setup	136
A-2-3. Wireless LAN (STA)	137
Basic Settings.....	137
Smart Wireless Setup	141
A-2-4. Wired LAN.....	142
Wired LAN Settings.....	142
Security Settings.....	142
A-2-5. VLAN	145
A-2-6. NTP	146
A-2-7. Display Setting.....	148
Display Configuration.....	148
Standby Screen Configuration	150
A-3. Security	151
A-3-1. Password.....	151
A-3-2. Access Control	151
A-4. Device Management	153
A-4-1. Import Configuration	153
A-4-2. Export Configuration.....	154
B. Appendix.....	155
B-1. Certificate Standard.....	156

(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, Inc.
- Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Mac, macOS, iPadOS, 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, Google Cast, Android, Chrome OS, Chromebook, Google Photos are trademarks or registered trademarks of Google LLC.
- HDMI, HDMI logo and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC.
- QR Code is a registered trademark of DENSO WAVE INCORPORATED.
- 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	
	<ul style="list-style-type: none"> 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	
	<ul style="list-style-type: none">• Do not use or store the product under the following conditions. It may cause malfunction.<ul style="list-style-type: none">- 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	
	<ul style="list-style-type: none">• 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	
	<ul style="list-style-type: none">• 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	
	<ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> - 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	
	<ul style="list-style-type: none"> • Do not cover up the vents on the product. The temperature inside may rise and cause fire or malfunction.

<Disassembly / Modification>



 Warning	
	<ul style="list-style-type: none"> • 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	
	<ul style="list-style-type: none"> • Use the correct power voltage. Improper voltage may cause fire or an electrical shock.

 Caution	
	<ul style="list-style-type: none"> • 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	
	<ul style="list-style-type: none">• 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	
	<ul style="list-style-type: none">• 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 cord may be broken, which could result in fire or an electrical shock.• Verify all cables 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's website. For details, please visit the Silex Technology's website.

Silex Technology's 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 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 our Customer Support Center.

Contact Information	
USA	support@silexamerica.com
Europe	support@silexeurope.com



Note

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

(Blank page)

2. Product Specifications

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, macOS, Chrome OS)

- The special projection utility "AMC Meeting" allows the user to mirror Windows and transmit audio. This utility 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 the screens can play videos, and it can be switched with a drag-drop action.)
- Distribution mode sends the projected 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 (keyboard, mouse, & touch panel)

- 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.
- If a USB touch panel is connected instead of a USB mouse, the same operation will be available.
- 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)

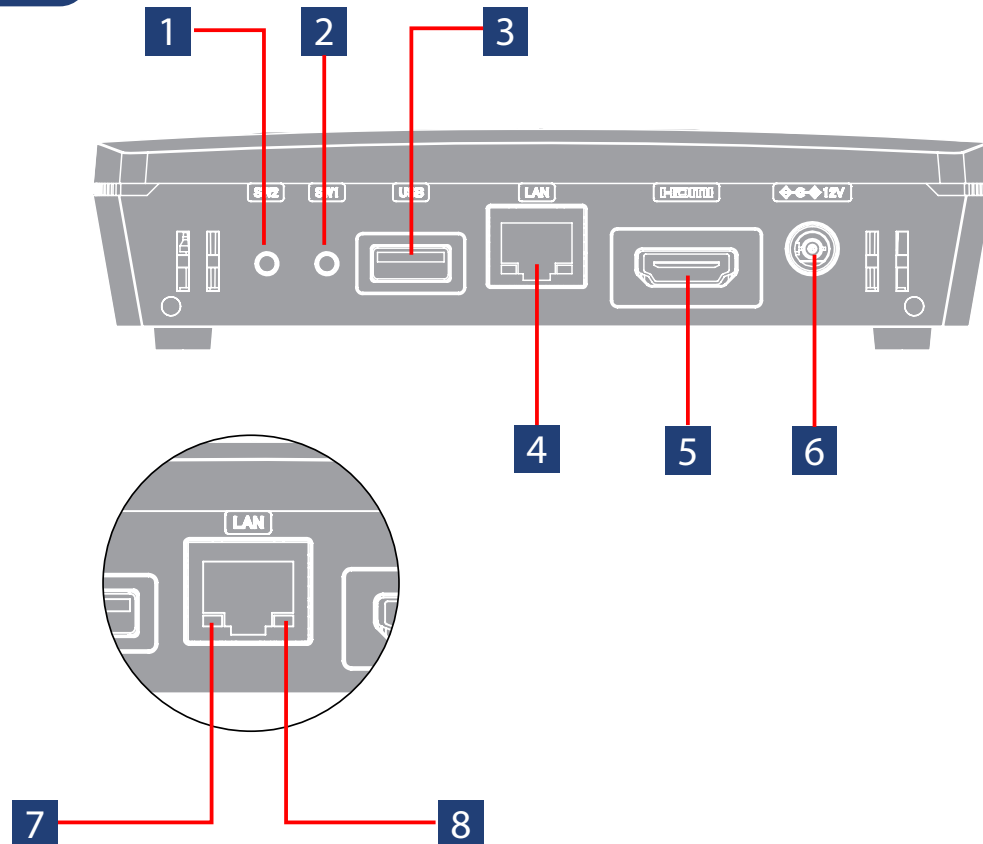
- AMC Manager® allows the user to remotely operate and monitor Z-1, change the settings, assign IP addresses, and upgrade the firmware for multiple Z-1 units at once.
- For details of AMC Manager®, see Silex Technology's website.

2-2. Parts and Functions



- When you are using 'Z-1 Rev. B', the LED light pattern will be different. To see if your Z-1 is 'Z-1 Rev. B', check the bottom label.

Front



- 1** Function switch (SW2)
Use this switch to:
 - Change the projection mode
 - Execute Smart Wireless Setup (push button method)
- 2** Reset switch (SW1)
Use this switch to reset Z-1 to the factory default setting.
- 3** USB port
Connect a USB mouse or a USB keyboard.
Use a USB HUB to connect both.
- 4** LAN port
Connect a LAN cable.
- 5** HDMI port
Connect an HDMI cable.

- 6** DC jack
Connect the AC adapter that comes with Z-1.

- 7** LINK LED
Shows the wired LAN connection status.

Color	Light	Description
Green	ON	The wired LAN is being connected.
	OFF	The wired LAN is not connected.

- 8** STATUS LED
Shows the packet reception state of the wired LAN

Color	Light	Description
Yellow	Blink	Turns on for 100 milliseconds when Z-1 receives a packet, and then turns off.

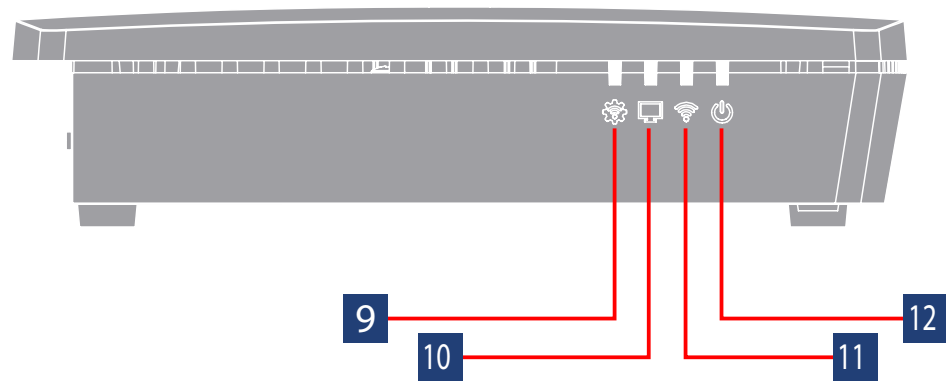


TIP

- When you are using 'Z-1 Rev.B', the light pattern of the LINK / STATUS LED is as follows.

LED	Light	Description
LINK LED	ON	A wired LAN is connected.
	Blink	Wired packets are sent or received. Turns on for 100 milliseconds and then turns off.
	OFF	A wired LAN is not connected.
STATUS LED	ON	The power is on.
	Blink	Wireless packets are sent or received. Turns off for 100 milliseconds and then turns on.
	Blink (2-second cycle)	DFS is working in Access Point mode.
LINK/STATUS LEDs	Blink alternately (2-second cycle)	Smart Wireless Setup is in progress.
	Blink alternately and fast (200-millisecond cycle)	Smart Wireless Setup has failed. (Turns off in 10 seconds)
	ON	Smart Wireless Setup has been successfully done. (Turns off in 10 seconds)
	Blink (2-second cycle)	The firmware update is in progress.

Side



• When you are using 'Z-1 Rev.B', these LEDs do not turn on.

TIP

- 9** STATUS LED
Shows the operating information of Z-1.

Color	Light	Description
None	OFF	Normal operating state
Blue	ON	Smart Wireless Setup has been successfully done. (Turns off in 3 minutes)
	Blink (2-second cycle)	Smart Wireless Setup is in progress.
Red	ON	Smart Wireless Setup has failed. Timeout / Overlap (Turns off in 3 minutes)
	Blink (100-millisecond cycle)	Smart Wireless Setup has failed. Other errors (Turns off in 1 minute)
	Blink (2-second cycle)	The firmware is being updated.

- 10** DISPLAY LED
Shows the video output state.

Color	Light	Description
-	OFF	A display (HDMI cable) is not connected.
Purple	ON	4K(3840x2160) video output is in progress.
Blue	ON	2K(1920x1080) video output is in progress.
Red	ON	720p(1280x720) video output is in progress while some functions are limited.

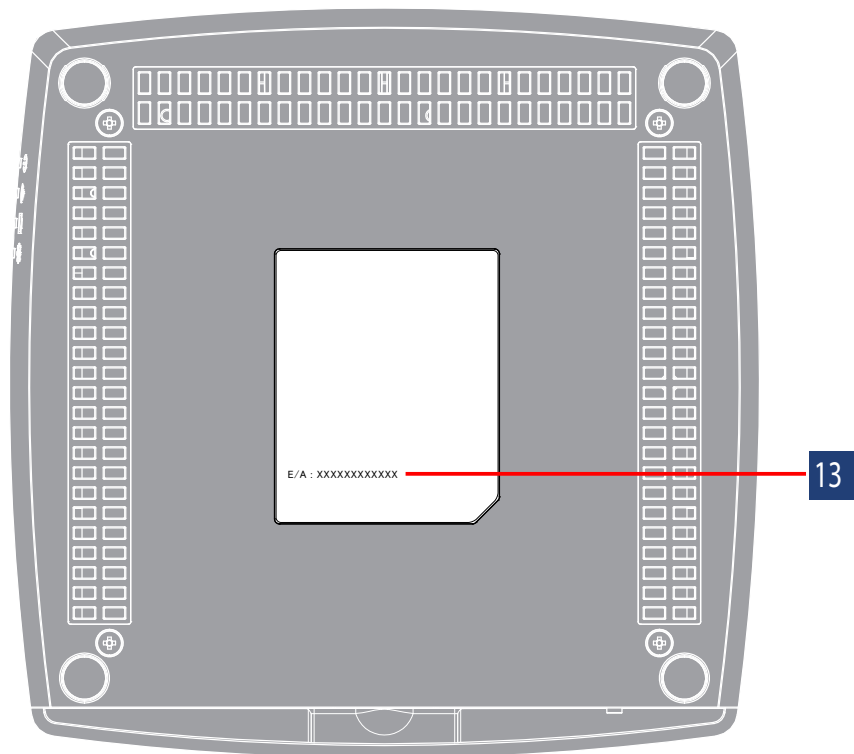
11 WLAN LED
Shows the wireless LAN state.

Color	Light	Description
-	OFF	Wired-only mode or Smart Wireless Setup is in progress.
Blue	ON	Access Point mode is on.
	Blink	Wireless packets are sent or received in Access Point mode. Turns off for 100 milliseconds and then turns on.
Purple	ON	Station mode is on and the wireless LAN has been connected.
	Blink	Wireless packets are sent or received in Station mode. Turns off for 100 milliseconds and then turns on.
	Blink (2-second cycle)	A specified Access Point is not connected in Station mode.
Red	Blink	DFS is working in Access Point mode.

12 POWER LED
Shows the power state.

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

Bottom

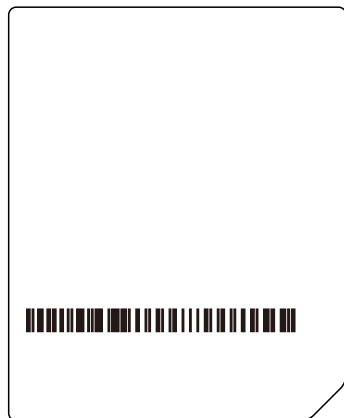


13 Product label
Shows MAC address (E/A) of the Z-1.

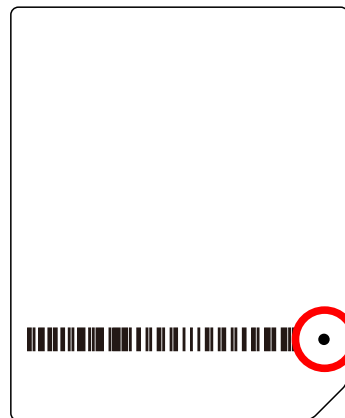


- When Z-1 is 'Z-1 Rev.B', a black circle is printed on the right side of the barcode.

- Z-1



- Z-1 Rev.B



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	LAN port	2 LEDs	Link (green)
			Status (yellow)
	Side	4 LEDs	POWER (blue/red)
			WLAN (blue/red)
DISPLAY (blue/red)			
STATUS (blue/red)			



TIP

- When you are using 'Z-1 Rev.B', these LEDs do not turn on.

Wired network interface	1000BASE-T / 100BASE-TX (auto-sensing): 1 port		
Wireless network interface	IEEE802.11a	Frequency	5 GHz band
		Transmission method	OFDM
		Transmission 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 method	DS-SS
		Transmission speed	1M, 2M, 5.5M, 11M
		Channel	[US] : 1-11Ch [EU] : 1-13Ch

Wireless network interface	IEEE802.11g	Frequency	2.4 GHz band
		Transmission method	OFDM
		Transmission speed	6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M
		Channel	[US] : 1-11Ch [EU] : 1-13Ch
	IEEE802.11ng HT20 / HT40	Frequency	2.4 GHz band
		Transmission method	DSSS-OFDM
		Transmission 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 method	OFDM
		Transmission 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 method	OFDM
		Transmission 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 supply	AC adapter	Operating voltage 12V +/-5%
		Rated current consumption 1500mA
Maximum power consumption	9.36W (DC12V 0.78A) * Excluding the USB bus power	
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

EMC	VCCI Class-A FCC Part 15 Subpart B Class-A ICES-003 Class-A EN 301 489-1/-17, EN 55032 Class-A	
Radio regulation	MIC FCC Part 15 Subpart C / Subpart E ISED RSS-247 EN 300 328, EN 301 893	

Notice to US Customers



Z-1

Contains FCC ID: N6C-PCEACDB

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

Silex Technology America, Inc.

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

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 Subpart B

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

FCC Rules Part 15 Subpart E

Data transmission is always initiated by software, which is 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 discontinues transmission in case of either absence of information to transmit or operational failure.

Frequency Tolerance: +/-20 ppm

Co-Location Rule

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

FCC Rules Part 15 Subpart C §15.247 and Subpart E

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment and meets the FCC radio frequency (RF) Exposure Guidelines. This equipment should be installed and operated keeping the radiator at least 20cm or more away from person's body.

Notice to Canadian Customers

CAN ICES-3 (A)/NMB-3 (A)

Contains ISED ID: 4908A-SXPCEACDB

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique 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;
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

for indoor use only (5150-5350 MHz)

Pour usage intérieur seulement (5150-5350 MHz)

Data transmission is always initiated by software, which is then 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 discontinues transmission in case of either absence of information to transmit or operational failure.

La transmission des données est toujours initiée par le logiciel, puis les données sont transmises par l'intermédiaire du MAC, par la bande de base numérique et analogique et, enfin, à la puce RF. Plusieurs paquets spéciaux sont initiés par le MAC. Ce sont les seuls moyens pour qu'une partie de la bande de base numérique active l'émetteur RF, puis désactive celui-ci à la fin du paquet. En conséquence, l'émetteur reste uniquement activé lors de la transmission d'un des paquets susmentionnés. En d'autres termes, ce dispositif interrompt automatiquement toute transmission en cas d'absence d'information à transmettre ou de défaillance.

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment and meets RSS-102 of the ISED 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 d'exposition aux fréquences radioélectriques (RF) CNR-102 de l'ISDE. Cet équipement doit être installé et utilisé en gardant une distance de 20 cm ou plus entre le radiateur et le corps humain.

Notice to European Customers



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

Notice to UK Customers



Restrictions or Requirements in the UK

2-3-2. Software Specifications

Wireless LAN	Mode	Access point Station	
	Wireless LAN	Access Point	Authentication method
Encryption mode			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 method	OPEN Shared WPA-PSK WPA2-PSK WPA/WPA2-PSK WPA-Enterprise WPA2-Enterprise WPA/WPA2-Enterprise
		Encryption mode	WEP(64/128-bit) TKIP/AES
		Smart Wireless Setup	Push switch PIN code

Basic protocol	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) HTTP (TCP #50000) 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)

H.264 License

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C.
SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com)

2-3-3. Others

Supported USB device	HID keyboard HID mouse HID touch panel
Supported OS	[Microsoft Windows] Windows 8.1 or later [Android] Android 6 or later [Chromebook] Chrome OS 90 or later [iOS] iOS 11 or later [MacOS] macOS 10.12 or later

**TIP**

- Windows RT is not supported.
- Windows 10 S mode is not supported.
- For the latest OS compatibility, see the Silex Technology's website.

2-3-4. Restrictions

This chapter describes the restrictions on use of Z-1.

Android (Google Cast)

- Z-1 can be used only in Single Presenter mode.
- Z-1 needs to get the correct time information. Enable the NTP client for time synchronization.
- When Z-1 is not connected to the Internet, the Android device may not be connected correctly. Try the followings in case the connection fails.
 - Restart the Android device.
 - Disable the mobile data communication on the Android device.
 - If these do not help, try to use Z-1 in an environment where the Internet connection is available.
- Z-1 does not support streaming playback mode (e.g. playback orders from Google Photos or YouTube application) which receives contents via the Internet.
- Z-1 disconnects from Android devices every day at 0:00 (local time) 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. playback orders from Google Photos or YouTube application) which receives contents via the Internet. Some applications use streaming playback mode for playing videos saved in the device, and which is also not supported by Z-1.

Chromebook (Google Cast)

- Z-1 can be used only in Single Presenter mode.
- Make sure that Z-1 has a correct time setting. Enable the NTP client to set the correct time. By connecting Z-1 from a Windows PC, the time of the Windows PC can be set to Z-1.
- It is not possible to receive & play the contents of the Internet (streaming playback from the Google Photos or YouTube applications).
- Due to a digital certificate renewal process to connect to Chromebook, a disconnection occurs every day at 0:00 (local time).
- The projection is usually enlarged to full screen, however, in the following cases, the full screen is not displayed and a black frame appears around the screen, since the size of image is too small when it is sent from the Chromebook.
 - When the CPU/GPU load is high on the Chromebook
 - When projecting a Chrome browser tab
- Z-1 does not support "Cast file".
- Although it is possible to project from Google Chrome (Web browser) on Windows or Linux, the operation is not officially supported.

Distribution Master mode/Slave mode

- Z-1 units of master/slave mode have to be in the same segment (broadcast domain). Make sure that only one of them is set to master mode in the segment.

Distribution mode for wireless communication

- Z-1 of master mode has to be Access Point mode and Z-1 of slave mode has to be Station mode. If Z-1 of master mode is set to Station mode, video distribution may become unstable since the transmission rate of multicast packets decrease.

Exclusive use of device server function

- The OSD function and device server function of Z-1 cannot be used together at a time. When the device server function is enabled, the OSD function is disabled.

Functional limitations on the display resolutions

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

Screen resize function

- Since the screen resize 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

Notes on Usage

Do not use Z-1 near the equipment below.

- Industrial, scientific, and medical equipment such as microwave ovens and pacemakers
- Short-range wireless base stations (wireless base stations that require a license) for mobile identification used in factory manufacturing lines and other applications
- Low-power wireless base stations (wireless base station that do not require a license)

The above equipment uses the same signal frequency band as wireless LANs. Signal interference can occur if Z-1 is used near the above equipment. This can result in a communication failure or slow communication speeds.

Avoid use of Z-1 near cellular telephones, PHS, televisions, and radios as much as possible.

Cellular phones, PHS, televisions, radios, and other devices use a different frequency band than the wireless LAN. Therefore, use of these devices near Z-1 will not affect communication by Z-1 or by these devices. However, if these devices are brought near a wireless LAN product, noise may occur in the audio or video due to the electromagnetic waves generated by Z-1 and other wireless LAN products.

Communication is not possible through reinforced steel, metal, or concrete barriers.

The signals used in Z-1 will pass through wood, glass, and other barriers used in a typical home, and so communication is possible even in rooms with walls made from wood or glass. However, the signals will not pass through barriers made of reinforced steel, metal, concrete, or similar materials.

Communication cannot be performed in rooms with walls made from these types of materials. In the same way, communication cannot be performed through floors using reinforced steel, metal, concrete, or similar materials.

Z-1 complies with the certification of conformance to technical standards.**Please pay attention to the following points:**

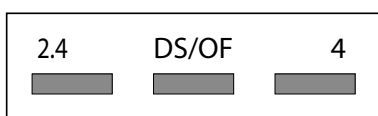
- Please do not disassemble or remodel the product. Such action is prohibited by law.
- Please do not remove the certificate label. Using the product without a label is prohibited.


Wireless Equipment Using 2.4 GHz Band

The operating frequency band of this equipment is used by microwave ovens, industrial, scientific, and medical equipment, and also by short-range wireless base stations (wireless base stations that require a license) and low-power wireless base stations (wireless base station that do not require a license) for mobile identification used in factory manufacturing lines and other applications.

- Before using this equipment, check that there are no short-range wireless base stations or low-power wireless base stations for mobile identification in the immediate area.
- If any cases of signal interference occur in short-range wireless base stations for mobile identification due to this equipment, either immediately change the operating frequency band, or stop the transmission of signals, and contact Silex Technology about possible corrective actions for preventing interference (such as installation of a partition).
- In addition, if any cases of signal interference occur in low-power wireless base stations for mobile identification due to this equipment, or if any other problems occur, contact Silex Technology.

*Meaning of the indicators written on the rear panel of the product



2.4	: Indicates wireless equipment using the 2.4 GHz frequency band.
DS/OF	: Indicates that DS-SS and OFDM are being used as the modulation scheme.
4	: Indicates that the estimated interference distance is "40 m maximum".
	Indicates that all bands are used and the band for mobile identification devices can be avoided.

Notes When Using 5 GHz Band

- Usage of the 5.2 GHz band (W52/W53) outdoors is prohibited under the Radio Law. For outdoor usage, use the W56 channel only, and do not use the W52/W53 channel.

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 (5GHz band)

Band	Channel bandwidth setting		Channel switching order
W53	HT20/VHT20		52>56>60>64>36
	HT40/ VHT40	+	52>60>36
		-	56>64>40
	VHT80		36
W56	HT20/VHT20		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 1 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 on a channel by the DFS function, the channel cannot be used for about 30 minutes.

(Blank page)

3. Network Configuration

3-1. Configuration on Web Page

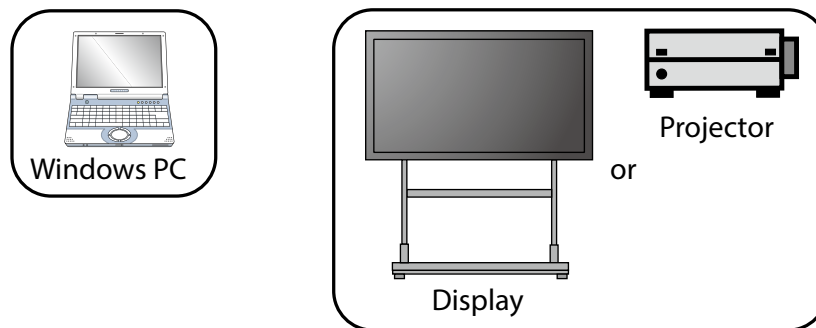
The user can change the Z-1's settings using a Web browser.



- The useful functions (remote restart, factory default configuration, etc.) can be used from the Web page. For more details, see **6-9 Maintenance Functions**.

Note

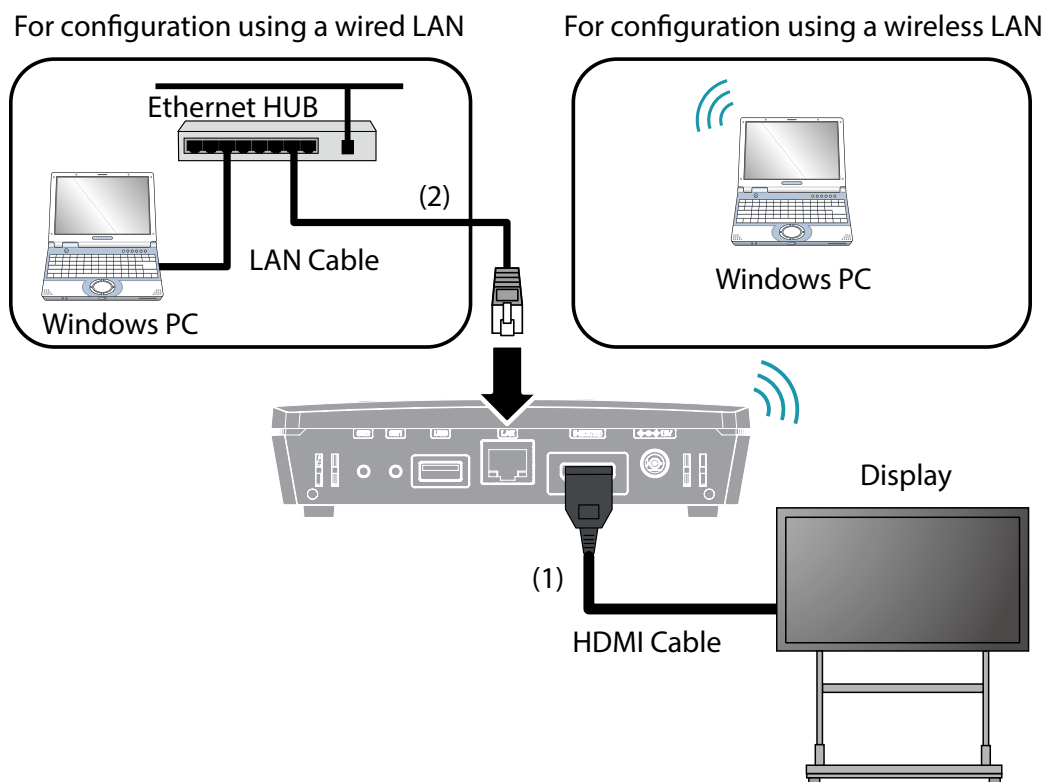
3-1-1. Necessary Items



- Windows 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

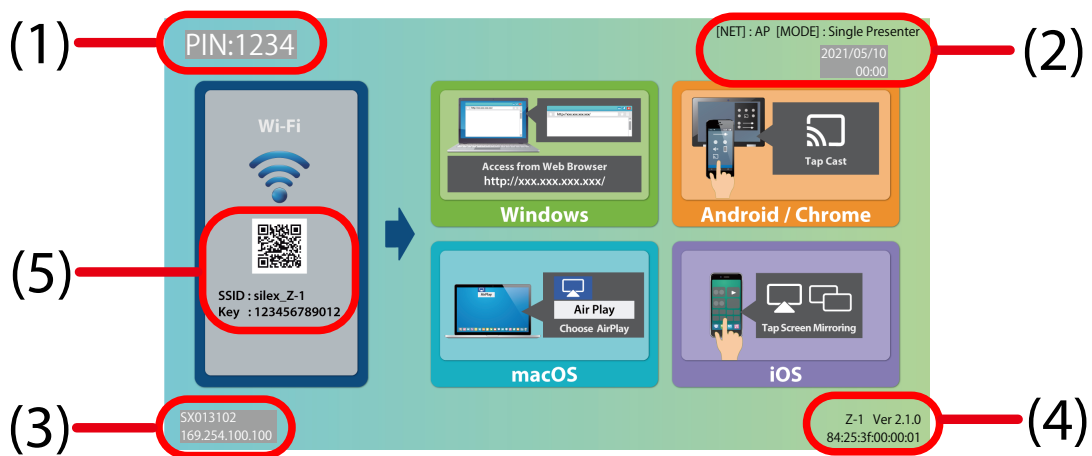
1. Connect the AC adaptor and power code. Then, connect the AC adaptor to the DC jack of Z-1 and the power plug to the outlet.



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

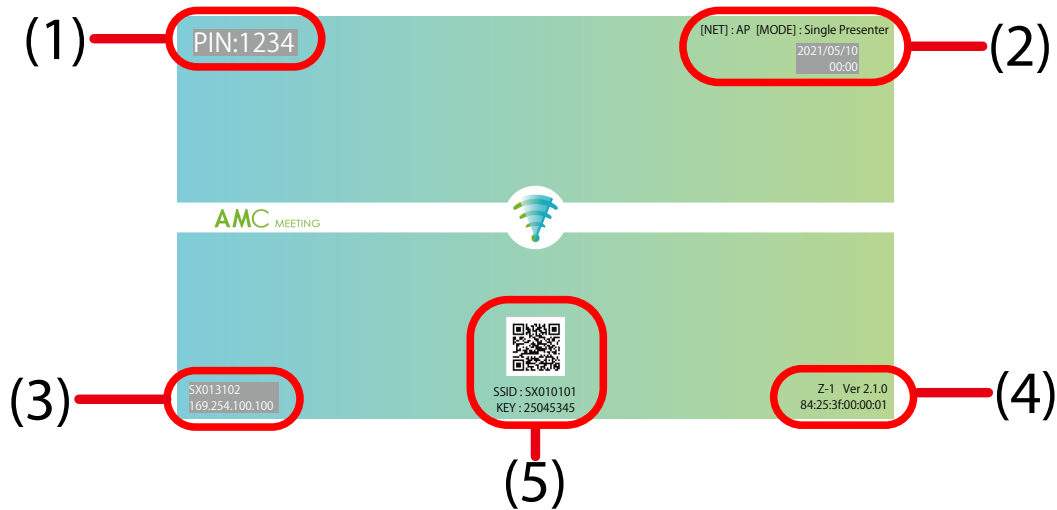
2. The standby screen is displayed on the display connected to Z-1. The standard screen, the instruction screen or the custom screen can be selected for the standby screen. When the animation in the middle of the screen stops, the power-on process is completed.

Instruction screen



- (1) PIN code of Z-1
- (2) System time, operating mode and network mode of Z-1
- (3) Host name and IP address of Z-1
- (4) Product name (Z-1) and firmware version
- (5) SSID and WPA key of Z-1, and QR Code for connection

Standard screen / Custom screen



- (1) PIN code of Z-1
- (2) System time, operating mode and network mode of Z-1
- (3) Host name and IP address of Z-1
- (4) Product name (Z-1) and firmware version
- (5) SSID and WPA key of Z-1, and QR Code for connection

**TIP**

- When **Custom** is set for the standby screen, a user-specified image can be displayed for the standby screen. The supported image size is 1920x1080 pixels.
- The operating mode and network mode of (2), and all information of (4) and SSID and WPA key of (5) have no background, and the font colors are black. If dark background colors are used, you may not be able to see them well.
- Each item of (1)-(5) is displayed at the following X and Y coordinate positions. Be careful of each position when creating an image for the standby screen. The coordinate of the upper left corner of the standby screen is (0, 0), and the coordinate of the lower right corner is (1919, 1079).

Coordinate position

No.	Item	Upper left (X coordinate, Y coordinate)	Upper right (X coordinate, Y coordinate)	Lower right (X coordinate, Y coordinate)	Lower left (X coordinate, Y coordinate)
(1)	PIN code	(96, 54)	(320, 54)	(320, 125)	(96, 125)
(2)	Operating mode and network mode	(1400, 15)	(1905, 15)	(1905, 65)	(1400, 65)
	System time	(1684, 54)	(1824, 54)	(1824, 128)	(1684, 128)
(3)	Host name and IP address	(96, 952)	(306, 952)	(306, 1026)	(96, 1026)
(4)	Product name (Z-1) and firmware version and MAC address	(1690, 1000)	(1905, 1000)	(1905, 1065)	(1690, 1065)
(5)	SSID and WPA key	(520, 1000)	(1400, 1000)	(1400, 1065)	(520, 1065)
	QR Code for connection	(885, 830)	(1035, 830)	(1035, 980)	(885, 980)

**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".
- When **PIN Code Type** is **DISABLE**, the PIN code is not displayed.

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. Z-1's Web Page.**

3-1-4. Connecting Windows PC

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



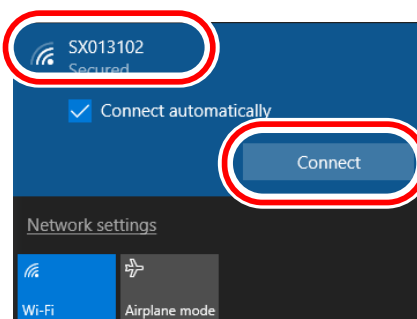
Note

- 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 started.

3. Press and hold the function switch of Z-1 (SW2). When the STATUS LED blinks blue at 2 sec interval, release the switch.



Note

- When you are using 'Z-1 Rev.B', release the switch when the LINK LED and STATUS LED of the LAN port blink alternately at every 2 sec.

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



- When you are using 'Z-1 Rev.B', the configuration is completed when the LINK LED and STATUS LED of the LAN port turn on.

Note

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**.

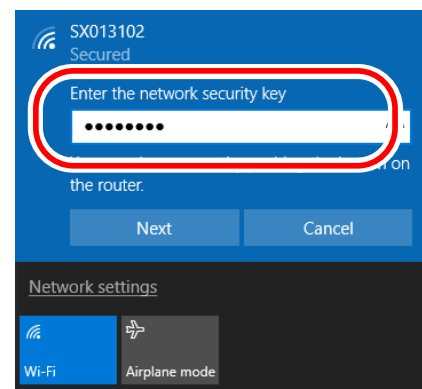
Now, the PC has connected to Z-1.



Note

- The PC can also be connected by entering the pre-shared key manually.

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



3-1-5. Z-1's Web Page

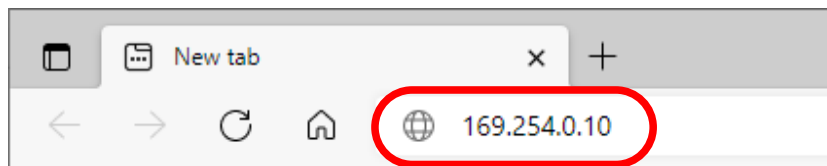
How to Access the Web Page

1. Start a Web browser on your PC. 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 "169.254.0.10", enter it to the address bar as below.



- The display of the Web page may differ depending on your environment and Web browser.

2. The login password configuration page will be displayed. Enter the password to configure for Z-1 and click **Submit**. The easy setup wizard page is displayed.

Please set a password for this unit.

Password

Confirm Password

1-8 Character String(Password)

Select Language

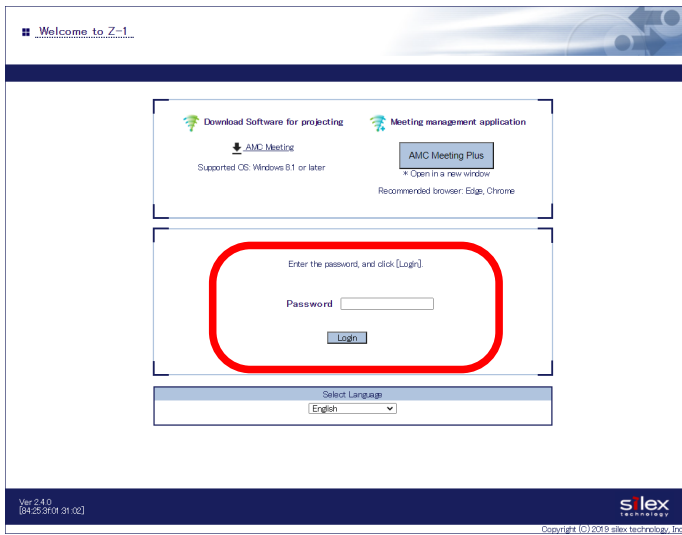
English



Note

- The login password configuration window is displayed only when Z-1 is configured for the first time.
- For details on the easy setup wizard page, refer to **3-1-7. Initial Configuration Wizard**.

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

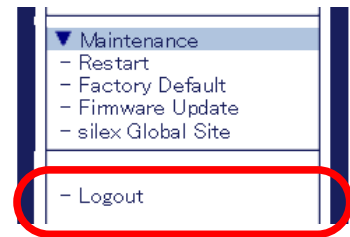


4. The Web page (System Status) appears.

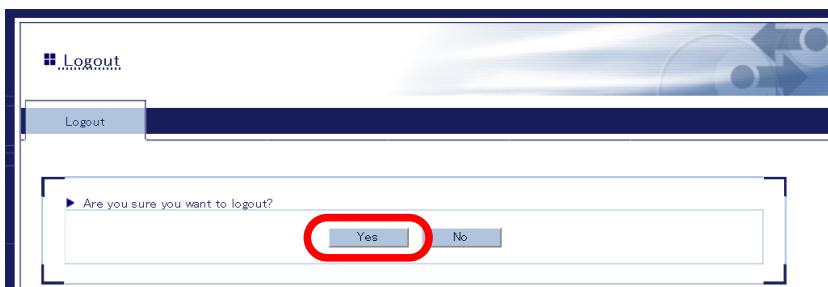


How to Log Out

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



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



3. The login page will appear.

3-1-6. Configuration on Web Page

The network settings can be changed from the basic/detailed configuration pages.

General configuration

The basic settings can be changed including settings for the TCP/IP, wireless LAN, and the DHCP server.

Detailed configuration

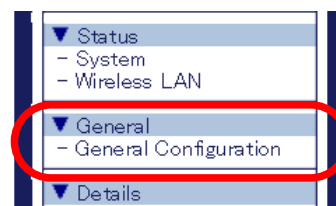
The detailed settings for the following items can be changed.

Item	Details
Product Configuration	TCP/IP communication setting
Wireless LAN Configuration(AP)	For use as AP on wireless LAN
Wireless LAN Configuration(STA)	For use as STA on wireless LAN
Wired LAN Configuration	Wired LAN interface setting
VLAN Configuration	VLAN ID setting for Wireless LAN SSID
NTP Configuration	Time synchronization setting
Display Configuration	Video function setting

Basic Network Configuration

Go to the basic configuration page to configure the network settings.

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



Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

- The general configuration page appears. Change the setting values if needed, and click **Submit** at the bottom right.

General Configuration

AP Bridge: ENABLE

Wireless Interface: Wireless LAN 1

Wireless LAN Basic Configuration

Name	Value
Interface	ENABLE
SSID	Sx013102
Stealth Mode	DISABLE
Network Authentication	WPA2-PSK

WPA/WPA2 Configuration

Name	Value
Encryption Mode	AES
Pre-Shared Key	●●●●●●●●
Group key renew interval	60

DHCP Server Configuration

Name	Value
DHCP Server Function	DISABLE
Start IP Address	192.168.0.11
End IP Address	192.168.0.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Lease Time	

Submit



TIP

- When the setting page is switched 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.

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

Setting is completed.
To take effect of this setting, please restart.

Restart



Note

- When you are to configure the settings on other pages, restart Z-1 when all other configuration is done.

- When the login page shows up, the basic configuration is now completed.

Detailed Network Configuration

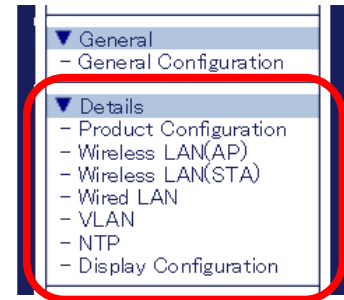
1. Access the Z-1's Web page.



- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page**.

Note

2. Click the setting you want to configure from the menu.



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

The screenshot shows the 'Product Configuration' page. It contains several configuration sections:

- DHCP Client:** ENABLE (dropdown), IP Address (0.0.0.0), Subnet Mask (0.0.0.0), Default Gateway (0.0.0.0).
- DNS Configuration:** DNS Server (Primary) (0.0.0.0), DNS Server (Secondary) (0.0.0.0).
- DHCP Server Configuration:** DHCP Server Function (DISABLE dropdown), Start IP Address (192.168.0.11), End IP Address (192.168.0.254), Subnet Mask (255.255.255.0), Default Gateway (0.0.0.0), Lease Time (0 Days, 0 Hours, 0 minutes).
- Push Switch Control Configuration:** Reset Switch (ENABLE dropdown), Function Switch (ENABLE dropdown).

The 'Submit' button is located at the bottom right of the page and is circled in red.



TIP

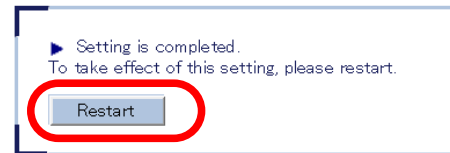
- When the setting page is switched to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. Before accessing other pages, click **Submit** to save the entered values.



Note

- See **A. Setting Items** for details on each item.

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



Note

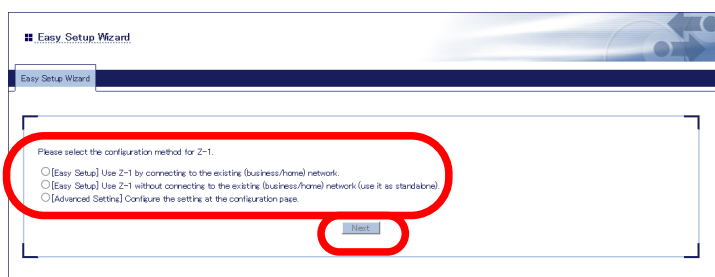
- To continue changing settings in other pages, go back to **2**. Restart Z-1 when all other configuration is done.

- 5.** When the login page shows up, the configuration is now completed.

3-1-7. Initial Configuration Wizard

The initial configuration wizard (hereinafter, "Easy Setup Wizard") appears when the password is set to the password configuration page which is displayed if the password configuration is not yet done.

On Easy Setup Wizard, the basic settings can be configured by selecting the appropriate images on the Web browser. Select how you like to configure Z-1 and click **Next**.



Configure the settings according to the instructions on the screen. Easy Setup Wizard will require Z-1 to be restarted upon completion of the configuration. The new settings will take effect after the restart is completed.

The following basic settings can be configured using Easy Setup Wizard.

	Name	Details
TCP/IP Configuration	DHCP Client	Set whether to use DHCP.
	IP Address	Set the IP address.
	Subnet Mask	Set the subnet mask.
	Default Gateway	Set the default gateway.
Wireless LAN Basic Configuration	Wireless Mode	Select the wireless LAN standard.
	SSID	Set the SSID for wireless LAN.
	Network Authentication	Set the network authentication mode.
WPA/WPA2 Configuration	Pre-Shared Key	Set the pre-shared key.
NTP Configuration	NTP	Set whether to use NTP.
	NTP Server	Set the NTP server address.
	Local Time Zone	Set the local time zone.

3-1-8. Chairperson Menu Page

This is the page for users who take a role of chairperson in the meeting.

For the detailed functions and menu options for this function, refer to **Z-1 User's Manual (Projection Method)**.

3-2. Wireless Configuration Using Smart Wireless Setup (STA)

This chapter explains the easy wireless configuration method (STA) of Smart Wireless Setup that can be used when your wireless LAN router supports WPS (Wi-Fi Protected Setup).

When the network mode is "Station", the following configuration methods are available.

Push button method

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

- Press the function switch of Z-1.
- Go to the Smart Wireless Setup page of the Z-1's Web page and click **Execute**.



- To use the function switch, the **Function Switch** setting needs to be **ENABLE**. For details, refer to **6-7-3. How to Control Push Switch Function**.

PIN code method

Go to the Z-1's Web page and enter the PIN code of the enrollee.

3-2-1. Before Setup

In order to use the Smart Wireless Setup function and configure the wireless LAN settings, a wireless LAN router supporting WPS is needed. Make sure that your wireless LAN router supports WPS and is operating in the network.

To check if your wireless LAN router supports WPS, see the operating manual or contact the manufacturer.



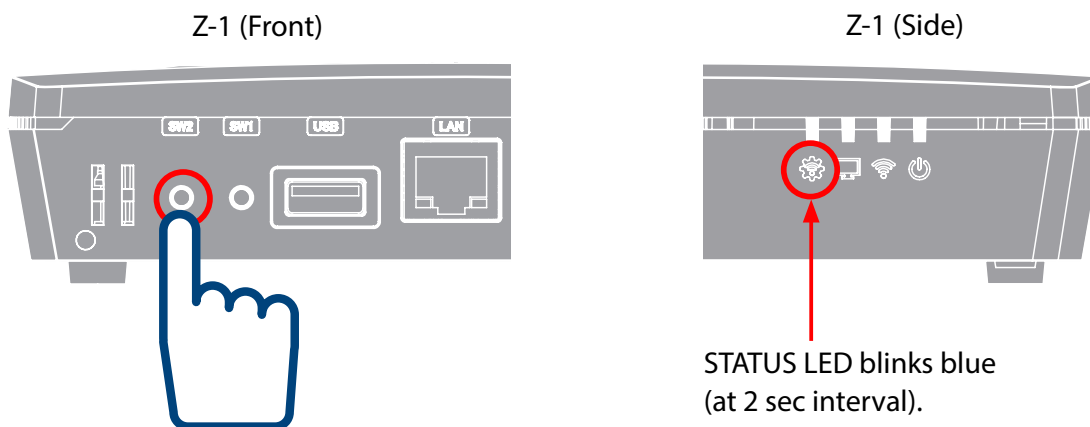
- Some wireless LAN routers need WPS function to be enabled manually. Check the operating manual for more details.
- When the security function (e.g. MAC address filter) is used on the wireless LAN router, make it allow an access from Z-1.

3-2-2. Push Button Method

The wireless LAN setting (STA) can be configured by using the function switch of Z-1 or by accessing the Smart Wireless Setup page of Z-1's Web page.

Wireless Configuration Using Function Switch

1. Press and hold the function switch until blue STATUS LED blinks every 2 seconds.



Keep pressing the function switch.



- When you are using 'Z-1 Rev.B', release the switch when the LINK LED and STATUS LED of the LAN port blink alternately at every 2 sec.

Note

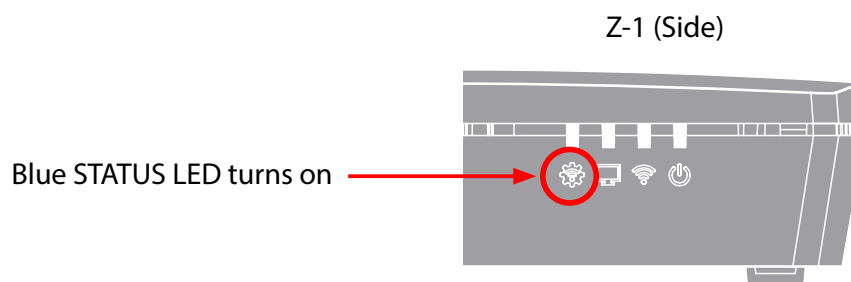
2. Push the WPS button of the wireless LAN router. Check that the wireless LAN router is waiting for a connection.



- The name, position and shape of WPS button vary with each wireless LAN router. For details, see the operating manual that comes with the router.
- Use only one wireless LAN router during this configuration. When multiple routers are waiting for connection, Z-1 cannot connect.

Note

3. When the configuration is successfully completed, the blue STATUS LED turns on.

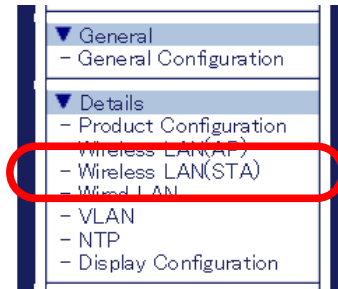


Note

- When 'Z-1 Rev.B' is used, the LINK LED and STATUS LED of the LAN port will turn on and then turn off in 10 seconds, when the configuration is successfully completed.
- The red STATUS LED turns on when the Smart Wireless Setup fails due to the followings:
 - No wireless LAN router was found in 120 seconds after the Smart Wireless Setup started (timeout error, WPS specification).
 - Two or more wireless LAN routers are handling WPS-PBC when the Smart Wireless Setup (push-button) is executed (overwrap error, WPS specification).
- When 'Z-1 Rev.B' is used, the LINK LED and STATUS LED of the LAN port will blink alternately at high speed and then turn off in 10 seconds, when Smart Wireless Setup has failed.
- The red STATUS LED turns on every 100 milliseconds when the Smart Wireless Setup fails due to the followings:
 - The Smart Wireless Setup is executed with the wireless LAN router, authentication of which only supports WPS 1.0 but does not support WPS 2.0.

Wireless Configuration Using PC

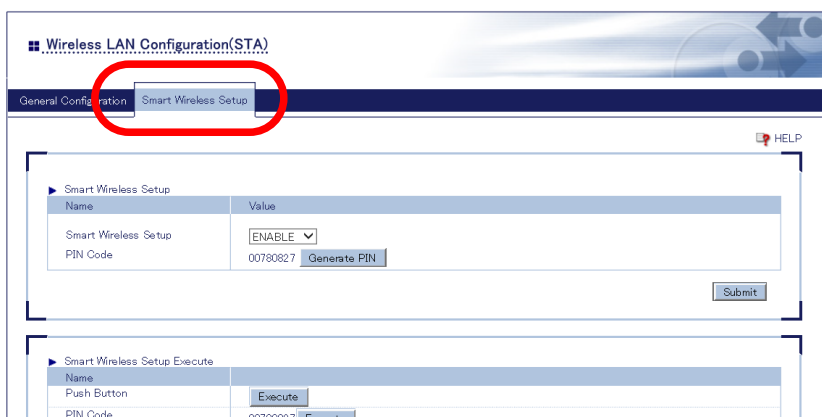
1. Click **Wireless LAN (STA)** on the page menu.



Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

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



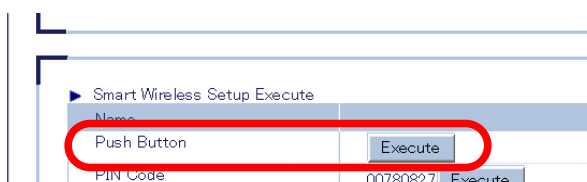
3. Push the WPS button of the wireless LAN router. Check that the wireless LAN router is waiting for a connection.



Note

- The name, position and shape of WPS button vary with each wireless LAN router. For details, see the operating manual that comes with the router.
- Use only one wireless LAN router during this configuration. When multiple routers are waiting for connection, Z-1 cannot connect.

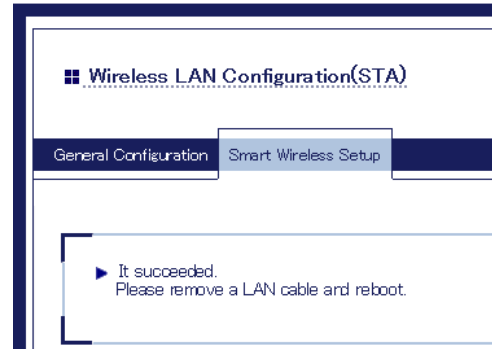
4. Click **Execute** button of the **Push Button** method to start the Smart Wireless Setup.



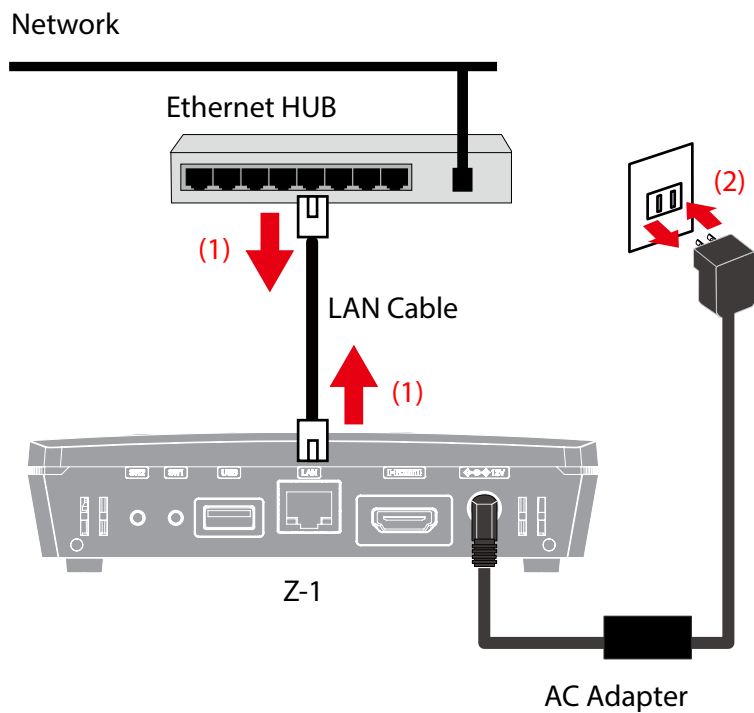
Note

- It may take a while to complete the wireless configuration in some environments (max 2 minutes).

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



6. Unplug a LAN cable from Z-1 and from the network or the Access Point (1), and restart Z-1 by unplugging and then plugging the AC adapter back into the outlet (2).



Now, the wireless LAN configuration (STA) is completed.

3-2-3. PIN Code Method

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



Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

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

 A screenshot of the 'Wireless LAN Configuration(STA)' web page. The 'Smart Wireless Setup' tab is highlighted with a red circle. The page contains two main sections: 'Smart Wireless Setup' and 'Smart Wireless Setup Execute'. The 'Smart Wireless Setup' section has a table with 'Name' and 'Value' columns. The 'Smart Wireless Setup Execute' section has a table with 'Name' and 'Value' columns.

Name	Value
Smart Wireless Setup	ENABLE
PIN Code	00780827

3. Check the PIN code on the page, and enter the PIN code to the Web page of the Access Point. Do not close this page as you will need it again during the configuration.

 A close-up screenshot of the 'Smart Wireless Setup' section. The 'PIN Code' field is highlighted with a red circle, showing the value '00780827' and a 'Generate PIN' button next to it.

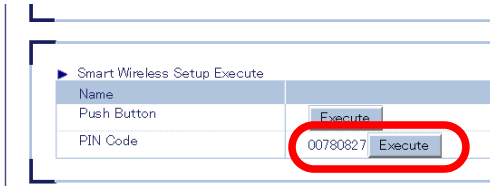
Name	Value
Smart Wireless Setup	ENABLE
PIN Code	00780827



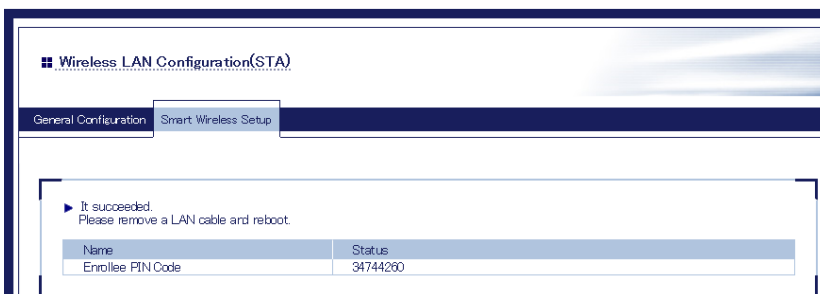
Note

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

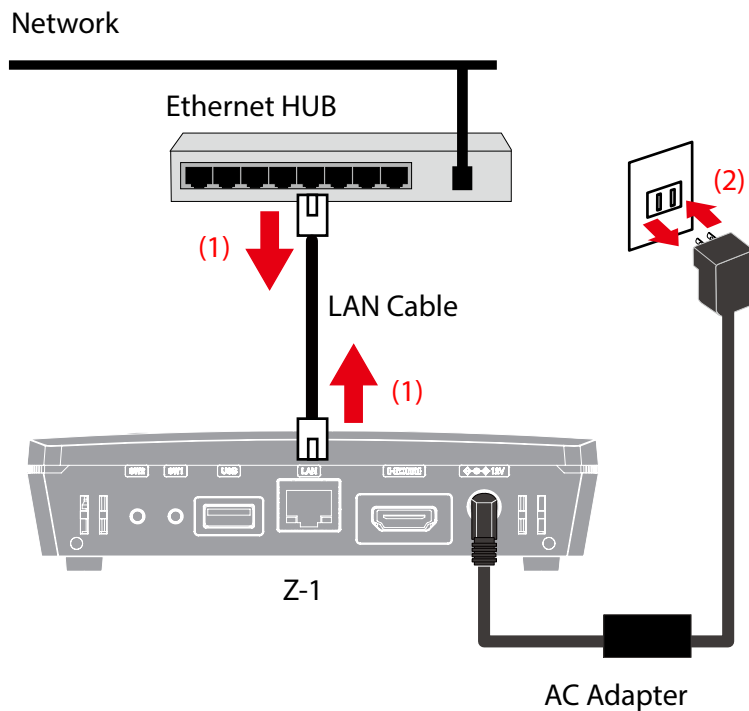
4. Open the Web page of wireless LAN router.
Enter Z-1's PIN code (see 3), and start the WPS connection from the router.
5. Go back to the Z-1's Web page and click **Execute** of **PIN-code**.



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



7. Unplug a LAN cable from Z-1 and from the network or the Access Point (1), and restart Z-1 by unplugging and then plugging the AC adapter back into the outlet (2).



Now, the wireless LAN configuration (STA) is completed.

4. Projection to Connected Display

4-1. Projection Mode Setting

4-1-1. Projection Mode Type

Z-1 has the following five projection modes. Choose one of them for video and audio output. When Z-1 is turned on for the first time, the Single Presenter mode is applied.

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



- Projection in Multi-Presenter mode, Distribution Master mode, Distribution Slave mode, and Pair Display mode is supported on Windows PC only.

TIP

Single Presenter mode

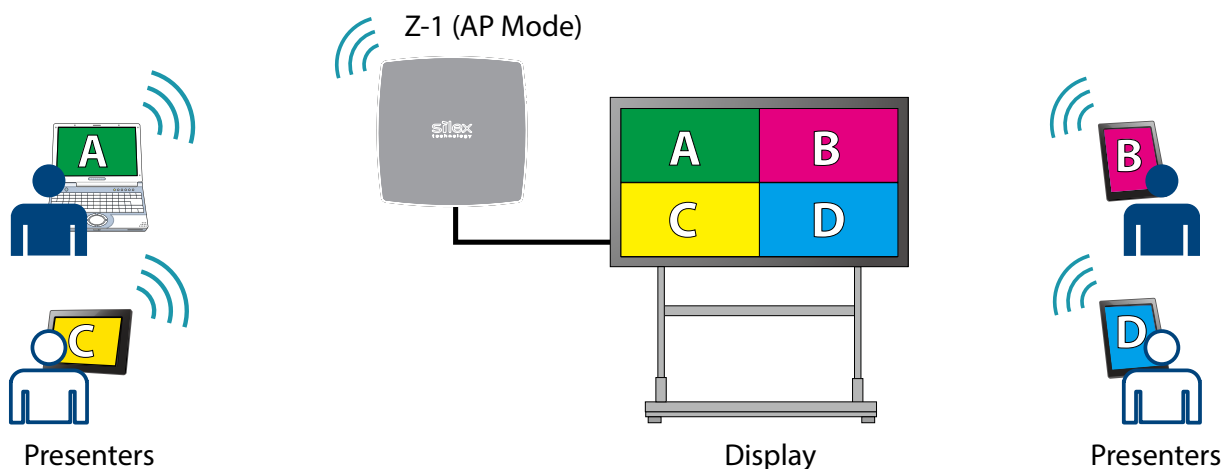
Single Presenter mode shows the video of one user in full screen.



- 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 (portrait screen resolution (1,080 x 1,920) is supported when iOS is connected).
- Video frame rate is up to 30 fps at 2K resolution and audio output is supported.
- For Windows devices, the dedicated tool is available. For Android, iOS, macOS and Chrome OS, the OS-standard function can be used for projection.
- When the size of distributed video does not meet the valid resolution, a black border will appear around the screen.

Multi-Presenter Mode

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



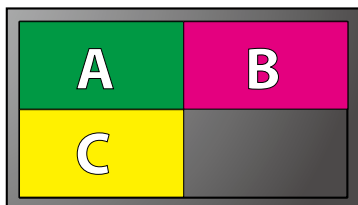
- One of presenters can become the primary session and Z-1 plays audio data of the primary device.
- The full-screen or split-screen display can be chosen on OSD menu.

Note

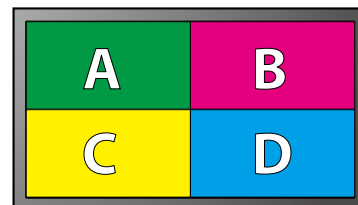
When 3 or 4 users are connecting:

Four-split screen

3 users



4 users

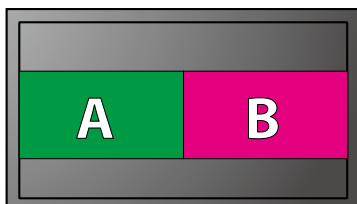


TIP

- 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.

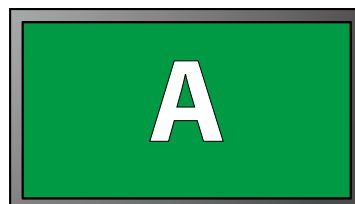
When 2 users are connecting:

Two-split screen



When only 1 user is connecting:

Full screen: same as Single Presenter mode

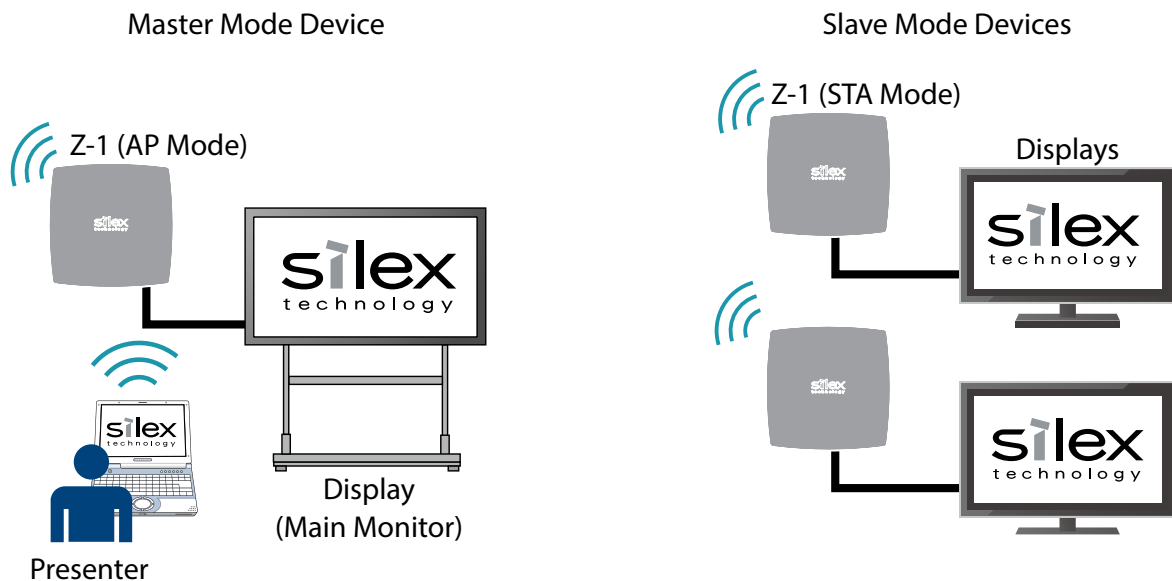


Distribution Master/Slave Mode

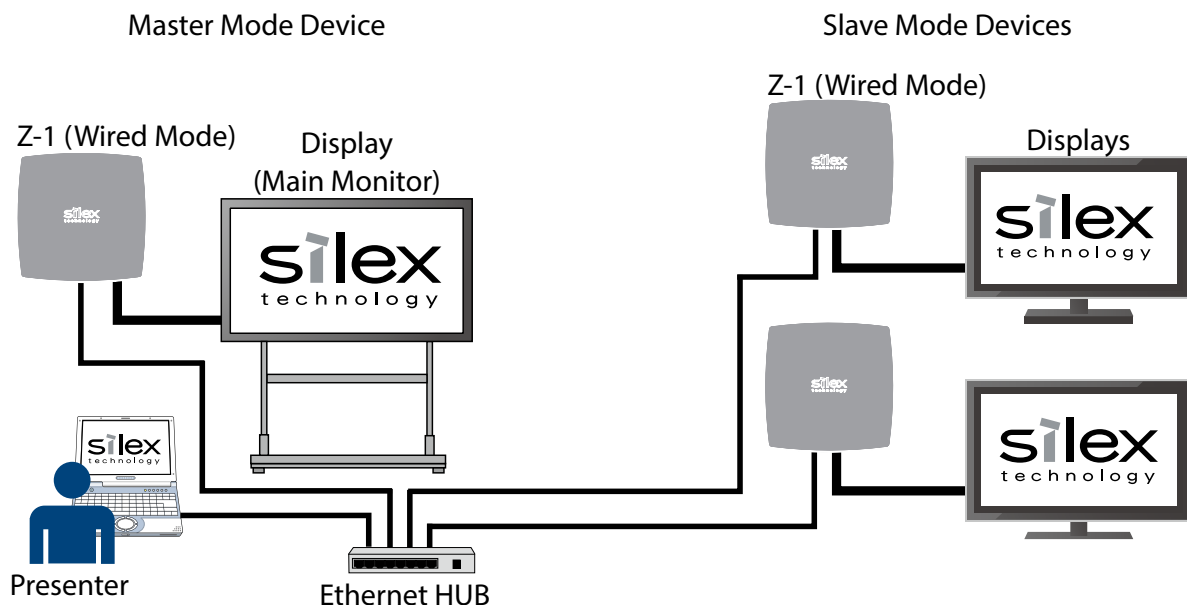
When the screen is projected to the main monitor connected to Master-mode Z-1, the same screen is also projected to the displays connected to Slave-mode Z-1. It is useful for large conference venues which have multiple displays and projectors in order to show the same screen on them at a time (up to 16 displays or projectors can be connected).

Distribution master / slave mode can be used on a wired LAN connection.

Projection using wireless LAN connection



Projection using wired LAN connection



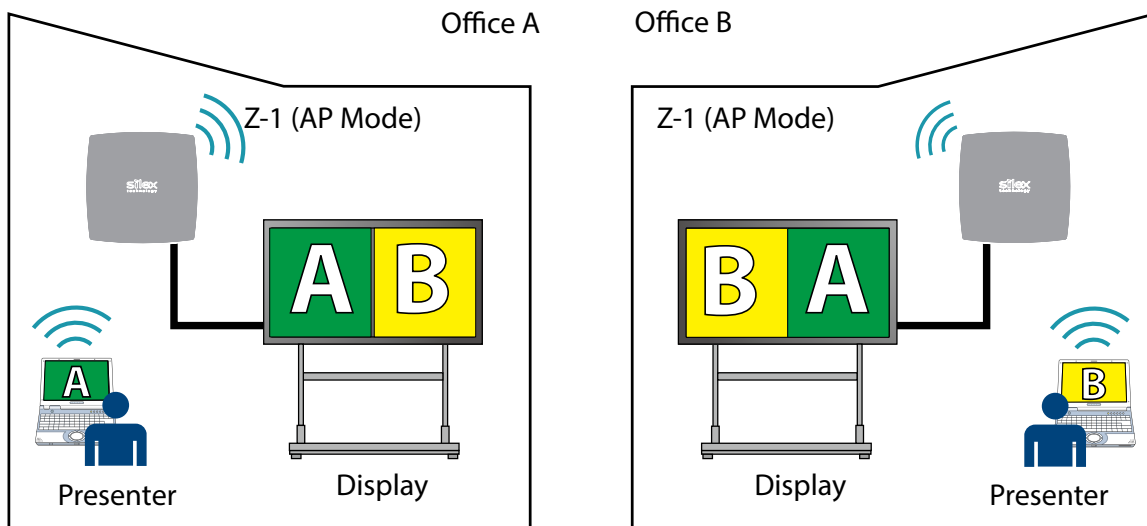


- For a network mode of the Master Z-1, select **AccessPoint** for wireless connection and **Wired** for wired connection.
- For a network mode of the Slave Z-1, select **Station** for wireless connection and **Wired** for wired connection.
- Both the Master and Slave Z-1 units have to be in the same segment (broadcast domain).
- Only one Master Z-1 can be used in the same segment (regardless of whether a wireless LAN connection or wired LAN connection is used).
- Up to 16 Slave Z-1 units can receive a video.

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.

- By registering the destination IP address to the address book of the toolbar, two Z-1 units can be connected when they are operating in Pair Display mode.
- The presenter's screen is shown on the left side of the screen (Local) while the same screen is transmitted to the other Z-1.
- The received screen image is 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

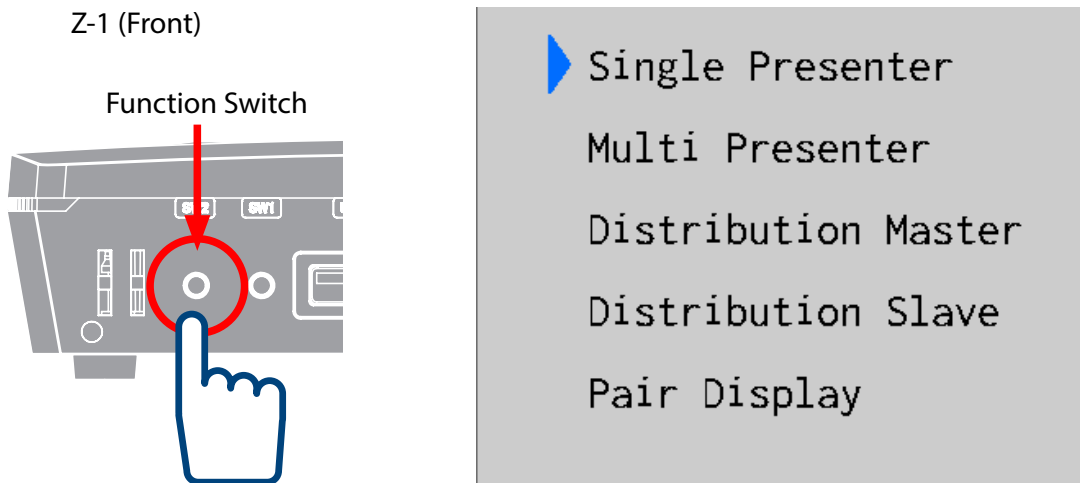
The projection mode can be changed using the function switch, OSD icon, or the Web interface.



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

How to Change Projection Mode Using 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.



- To use the function switch, the **Function Switch** setting needs to be **ENABLE**. For details, refer to **6-7-3. How to Control Push Switch Function**.

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 new mode and change the projection type.



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

How to Change Projection Mode Using OSD Icon

The projection mode can be changed using the projection-mode change icon on the toolbar. If this icon is clicked, the mode change menu will appear from which you can change the projection mode. For more details, see "Z-1 User's Manual (Projection Method)".

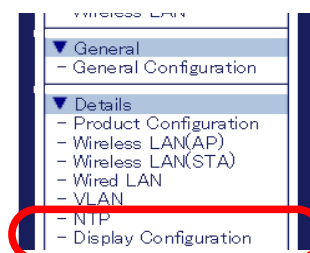


- USB mouse is required to click the icon on the toolbar.

TIP

How to Change Projection Mode Using Web Page

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



Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

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



TIP

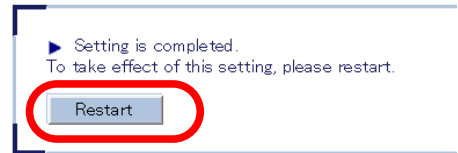
- When the setting page is switched to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. Before accessing other pages, click **Submit** to save the entered values.



Note

- If the destination IP address is registered at the pair display configuration, it will be displayed in the address book of the toolbar.

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

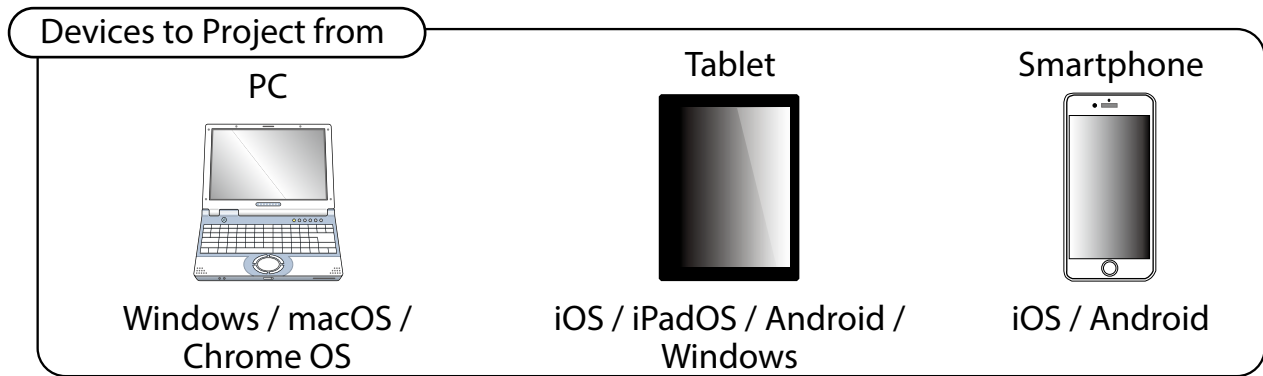


- 4.** After the restart, close the Web browser.

4-2. Projecting Screen to Display

4-2-1. Device Preparation

Prepare the device, screen of which is projected to the display of Z-1.



4-2-2. Starting Projection

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

5. Use of Wireless Access Point Function

5-1. Connecting Wireless Stations

5-1-1. Connecting Windows PC

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



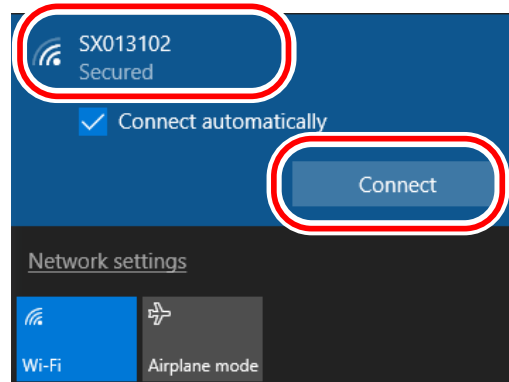
Note

- 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 a PC with the other OS, follow the appropriate procedure for that OS.

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



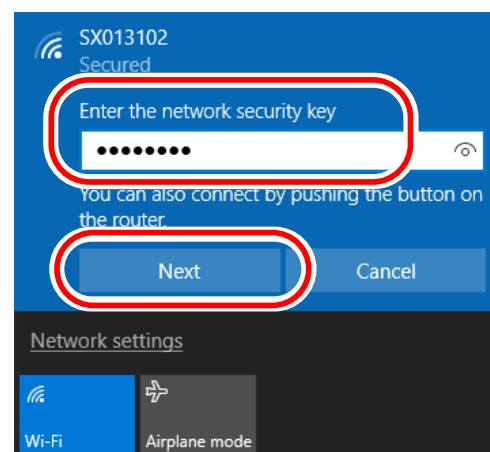
2. Select SSID of Z-1 and click **Connect**.



Note

- If **Connect automatically** is checked, 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 to Connect

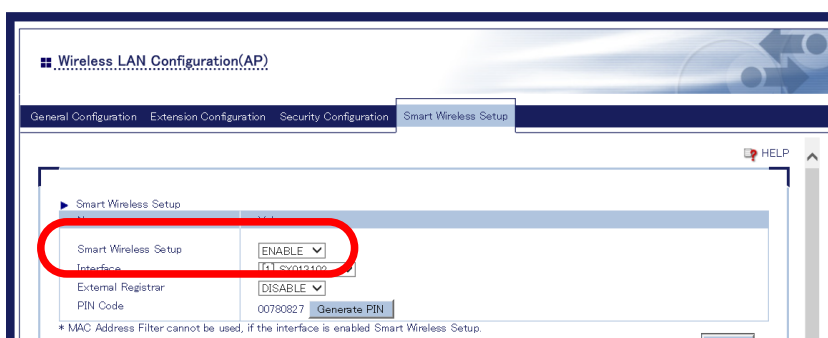
This chapter shows how to use the function switch to connect a Windows PC as a wireless station.



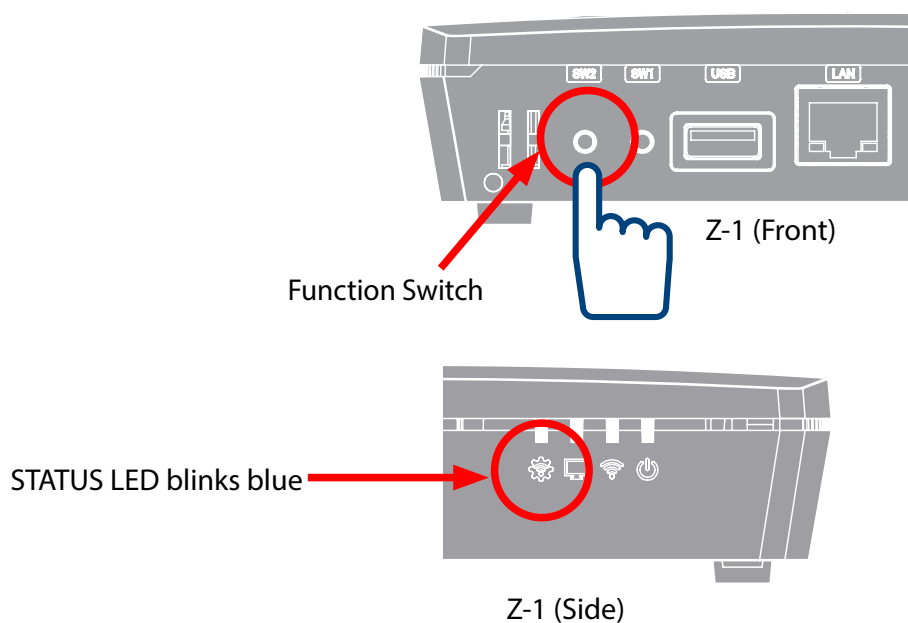
TIP

- Before going through the following procedure, make sure that the wireless LAN device supports Wi-Fi Protected Setup (WPS).
- To use the function switch, the **Function Switch** setting needs to be **ENABLE**. For details, refer to **6-7-3. How to Control Push Switch Function**.

1. Access the Z-1's Web page and check that **Smart Wireless Setup** is **ENABLE** at the wireless LAN configuration(AP) page.



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

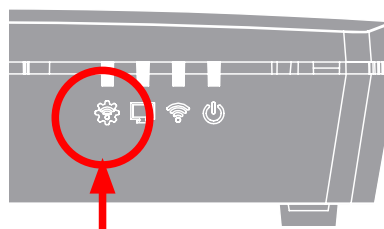


Note

- When you are using 'Z-1 Rev.B', release the switch when the LINK LED and STATUS LED of the LAN port blink alternately at every 2 seconds.

3. Press a wireless function switch on the wireless station device to connect.

4. Z-1 starts communicating and automatically provides the same setting values to the station. When the STATUS LED turns blue, the setting is completed.



STATUS LED turns blue Z-1 (Side)



Note

- When you are using 'Z-1 Rev.B', the configuration is completed when the LINK LED and STATUS LED of the LAN port turn on.

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

5-1-3. Use of Web Page to Connect

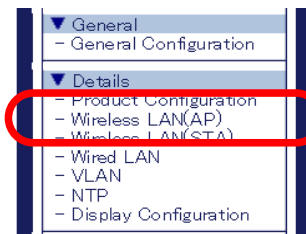
This chapter shows how to connect a wireless station device using the Web page of Z-1.



TIP

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

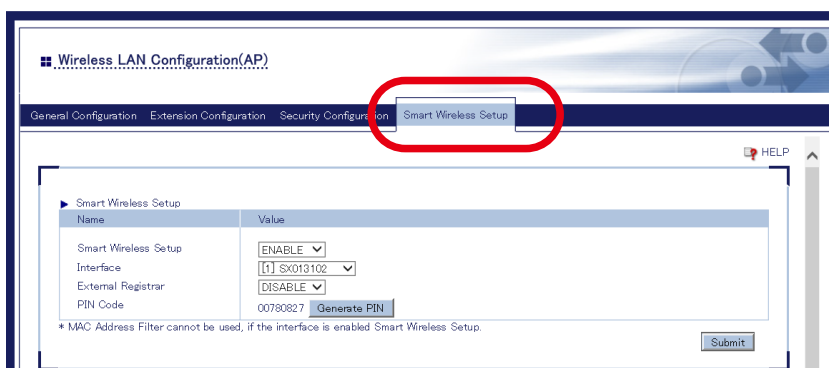
1. Access the Z-1's Web page and click **Wireless LAN (AP)** on the page menu.



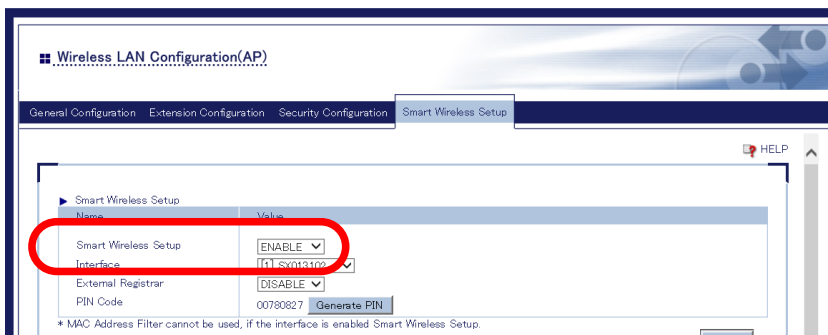
Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

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



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

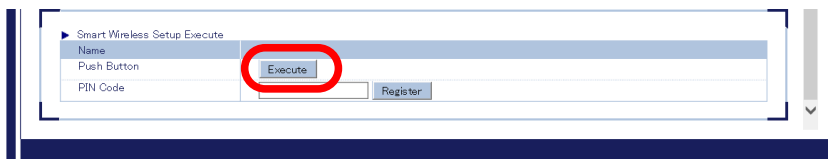


4. The Smart Wireless Setup page provides the following two methods to connect Z-1 and a wireless station.

- Push button method
- PIN code method

Use of Push Button Method

1. Click **Execute** of the **Push Button** at the Smart Wireless Setup page.



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

3. Z-1 starts communicating and automatically provides the same setting values to the station. When the STATUS LED turns blue, the setting is completed.



STATUS LED turns blue Z-1 (Side)



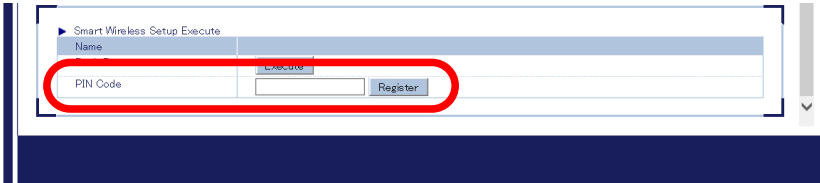
Note

- When you are using 'Z-1 Rev.B', the configuration is completed when the LINK LED and STATUS LED of the LAN port turn on.

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

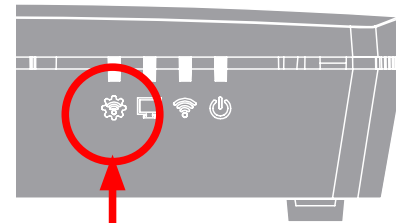
Use of PIN Code Method

1. Go to the Smart Wireless Setup page, enter the PIN code of the wireless station to **PIN Code** and click **Register**.



- The PIN code has to be the one assigned to the wireless station. For details, refer to the operating manual that comes with your wireless station device.

2. Z-1 starts communicating and automatically provides the same setting values to the station. When the STATUS LED turns blue, the setting is completed.



STATUS LED turns blue Z-1 (Side)



Note

- When you are using 'Z-1 Rev.B', the configuration is completed when the LINK LED and STATUS LED of the LAN port turn on.

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

5-2. MAC Address Filter on Wireless Stations

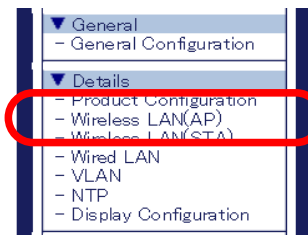
This chapter shows how to register the MAC addresses of wireless stations to accept or block connections to Z-1.



TIP

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

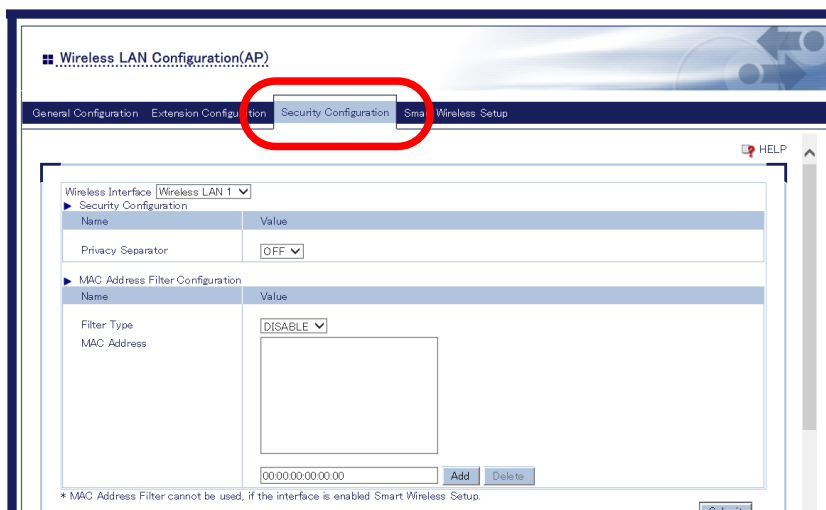
1. Access the Z-1's Web page and click **Wireless LAN (AP)** on the page menu.



Note

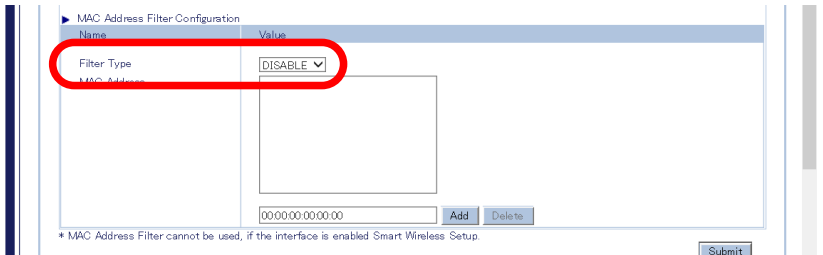
- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page**.

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

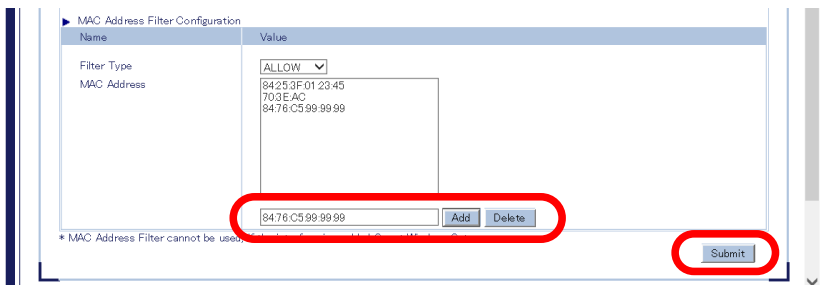


3. Select the filter type under MAC Address Filter Configuration.

- ALLOW: Accepts connection only from the registered wireless stations.
- DENY: Blocks the connection from the registered wireless stations.



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



TIP

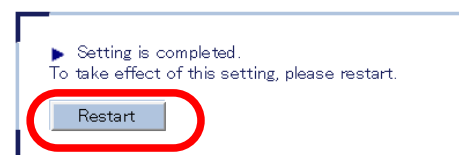
- When the page is switched to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. Before accessing other pages, click **Submit** to save the entered values.



Note

- MAC addresses must be the form of "XX:XX:XX:XX:XX:XX".
- It is possible to register the target device by vendor code (the first 6 characters of MAC address). 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

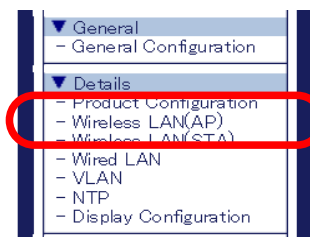
- When you are to configure the settings on other pages, restart Z-1 when all other configuration is done.

6. After the restart, close the Web browser.

5-3. Communication Filter on Wireless Stations

This chapter describes how to block communication among the connected wireless stations, and to allow only the communication of devices connected on a wired LAN.

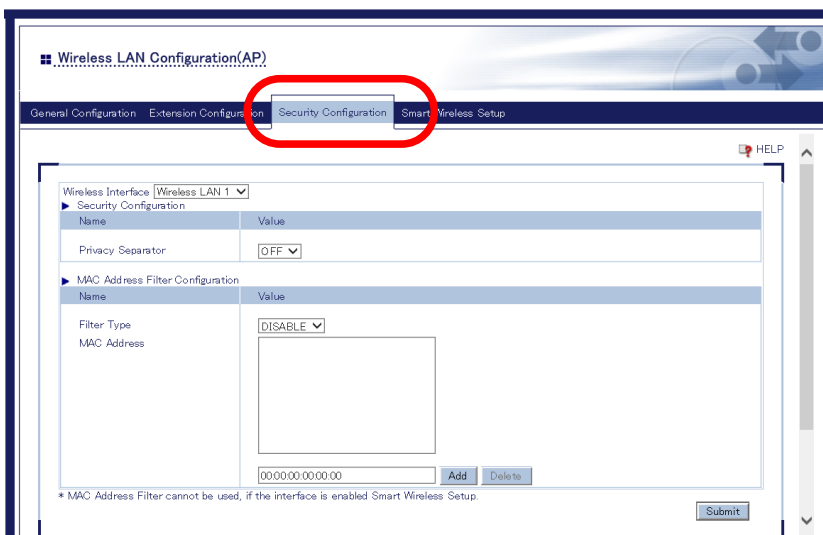
1. Access the Z-1's Web page and click **Wireless LAN (AP)** on the page menu.



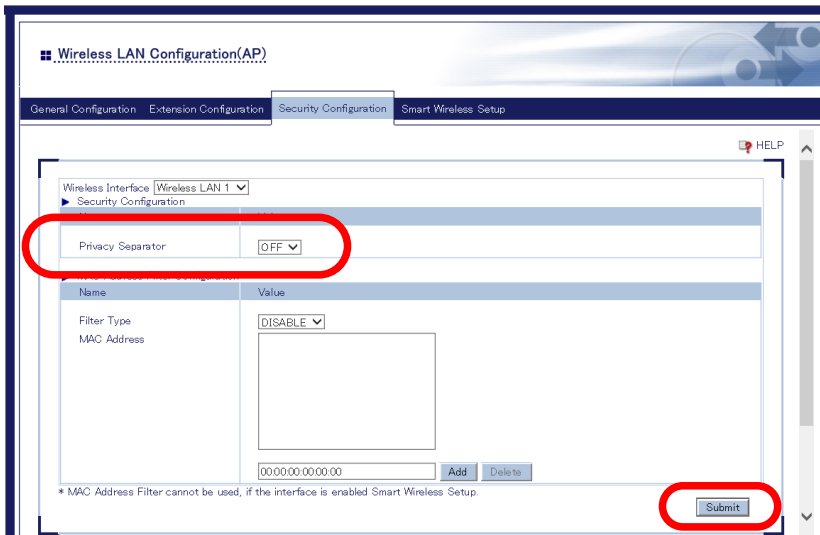
Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

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

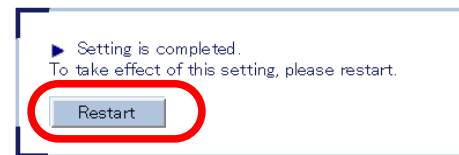


3. Choose **ON** for **Privacy Separator**, and click **Submit**.



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

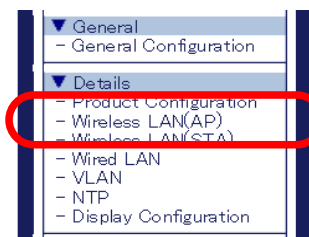
- When you are to configure the settings on other pages, restart Z-1 when all other configuration is done.

5. After the restart, close the Web browser.

5-4. How to Disable Smart Wireless Setup

This chapter shows how to disable the Smart Wireless Setup functions (e.g. Push switch method to connect to a wireless station).

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



Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

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

Wireless LAN Configuration(AP)

General Configuration Extension Configuration Security Configuration **Smart Wireless Setup**

Smart Wireless Setup

Name	Value
Smart Wireless Setup	ENABLE
Interface	[1] Sx013102
External Registrar	DISABLE
PIN Code	00780827 <input type="button" value="Generate PIN"/>

* MAC Address Filter cannot be used, if the interface is enabled Smart Wireless Setup.

Smart Wireless Setup Information

Name	Status
Smart Wireless Setup	ENABLE
Wireless LAN config status	Configured <input type="button" value="Unconfigures"/>

Wireless LAN Information

Name	Status
Interface	ENABLE

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

The screenshot shows a configuration page for 'Smart Wireless Setup'. It contains a table with the following data:

Name	Value
Smart Wireless Setup	ENABLE
Interface	[GigabitEthernet0/24]
External Registrar	DISABLE
PIN Code	00780827

Below the table, there is a 'Generate PIN' button and a note: '* MAC Address Filter cannot be used, if the interface is enabled Smart Wireless Setup.' A 'Submit' button is located at the bottom right of the form.



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

The screenshot shows a confirmation message: 'Setting is completed. To take effect of this setting, please restart.' Below the message is a 'Restart' button.



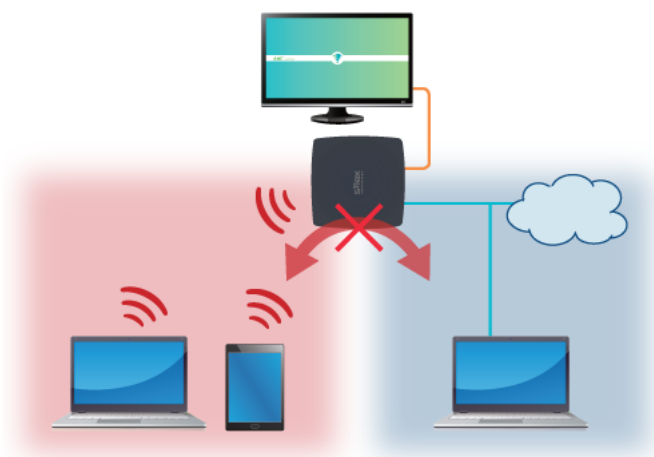
Note

- When you are to configure the settings on other pages, restart Z-1 when all other configuration is done.

5. After the restart, close the Web browser.

5-5. AP Bridge Function

If the AP bridge setting is configured, communication can be controlled for accesses between wired LAN network and wireless LAN network. By disabling the AP bridge function, the network can be divided into a corporate network and a guest network.

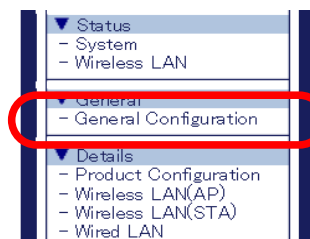


TIP

- This function provides a simple network separation function. For the advanced network separation, please use the VLAN feature. Remember that AP bridge function cannot be disabled while the VLAN function is used. When the VLAN is used, the AP bridge must be enabled.

The following explains how to configure the AP bridge function.

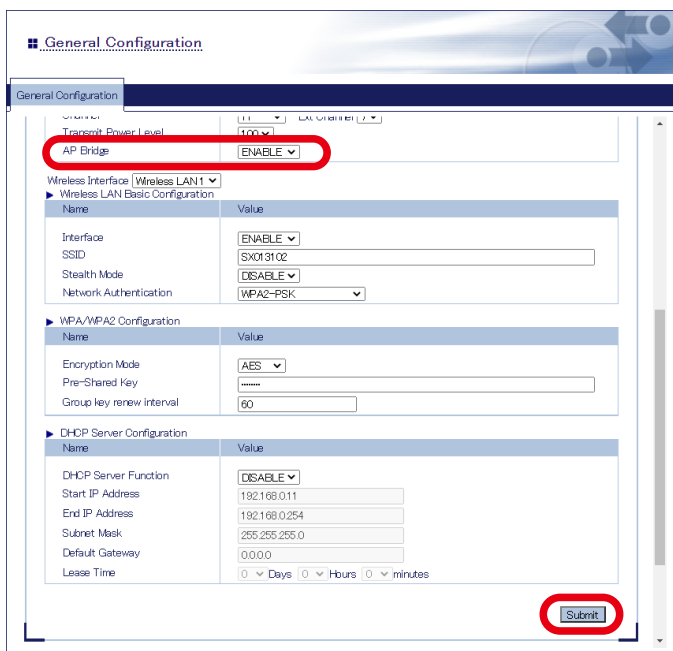
1. Access the Z-1's Web page and click **General Configuration** on the page menu.



Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page** at **3-1-5. Z-1's Web Page**.

2. In the general configuration page, select the desired setting at **AP Bridge** and click **Submit**.



TIP

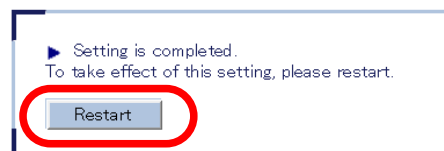
- When the setting page is switched to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. Before accessing other pages, click **Submit** to save the entered values.



Note

- If **AP Bridge** is set to **DISABLE**, the VLAN function is disabled and the DHCP server function is enabled.
- If **AP Bridge** is set to **DISABLE**, the IP address to use for each network interface will be determined as below.
 - IP address on a wired LAN : Follows to the TCP/IP setting of Z-1
 - IP address on a wireless LAN : Uses the start address registered to the DHCP server function setting.
 Do not use the IP address of the same segment for wired LAN and wireless LAN interfaces.

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



Note

- When you are to configure the settings on other pages, restart Z-1 when all other configuration is done.

4. After the restart, close the Web browser.

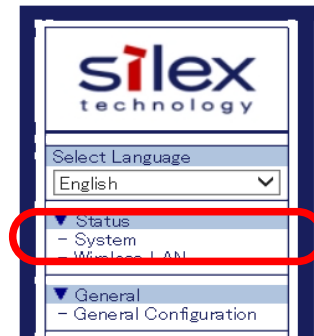
6. Other Functions

6-1. Status Monitor Using Web Browser

6-1-1. Checking System Status

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

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

2. The system status page appears.

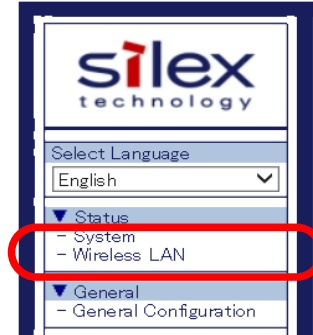


Item	Description
System status	
Product name	Name of the product, Z-1
Version	Firmware version of the product
MAC address	MAC address of the product
Host name	Host name in use
IP address	Currently assigned IP address
Subnet mask	Subnet mask in use
Default gateway	Gateway address in use
DHCP server	Address 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	Wireless connection status
Current channel	Channel in use

6-1-2. Checking Wireless LAN Status

The operating status of the connected wireless station can be checked on the Web page. 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

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

2. The wireless LAN status page appears.



Item	Description
MAC Address	Shows MAC addresses of wireless 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 Function

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

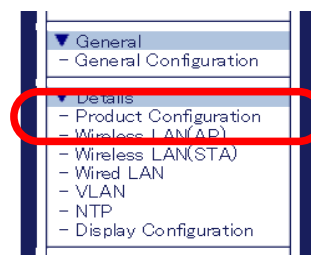


Note

- In order to assign an IP address to PC automatically using the DHCP server function, enable "**Obtain an IP address automatically**" on the PC.

6-2-1. DHCP Server Function Setting

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



Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

- The product configuration page appears. Select **ENABLE** for **DHCP Server Function**, enter the following settings and click **Submit**.

Name	Value
DHCP Server Function	ENABLE
Start IP Address	192.168.0.11
End IP Address	192.168.0.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Lease Time	0 Days 0 Hours 0 minutes

Name	Value
Reset Switch	ENABLE
Function Switch	ENABLE



TIP

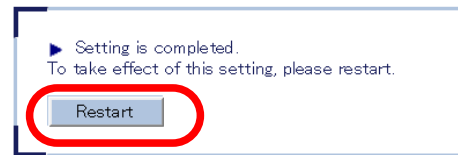
- To use the DHCP server function, disable the DHCP client function and set a static IP address.
- When the page is switched to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. Before accessing other pages, click **Submit** to save the entered values.



Note

- See "**A. Setting Items**" for details on each setting item.

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



Note

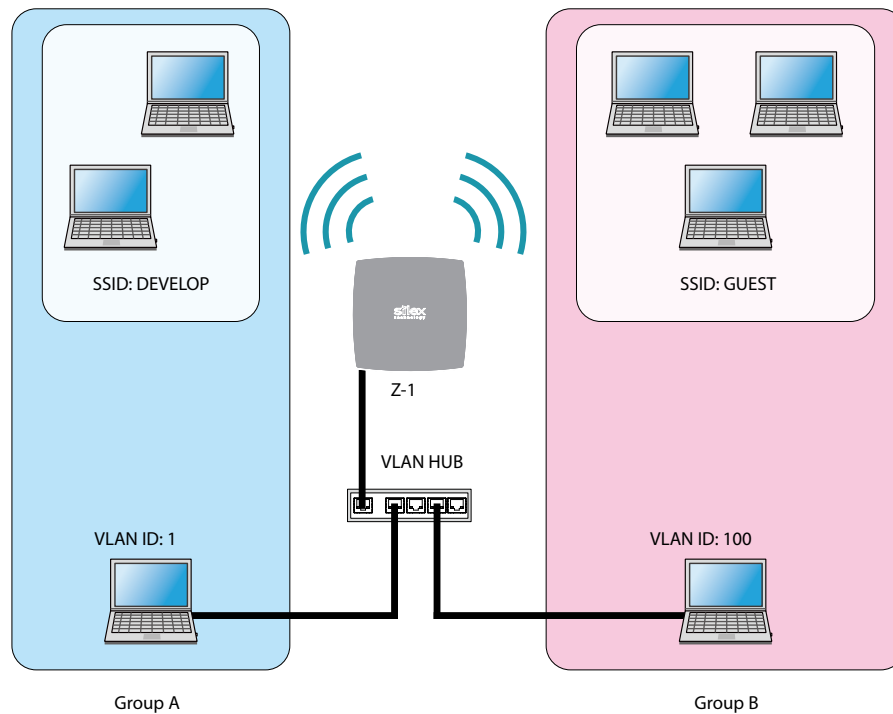
- When you are to configure the settings on other pages, restart Z-1 when all other configuration is done.

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 can give VLAN ID to each SSID, and can create up to four virtual network groups using a switching HUB that supports tagged VLAN (VLAN HUB).



Creating Virtual Network Groups



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

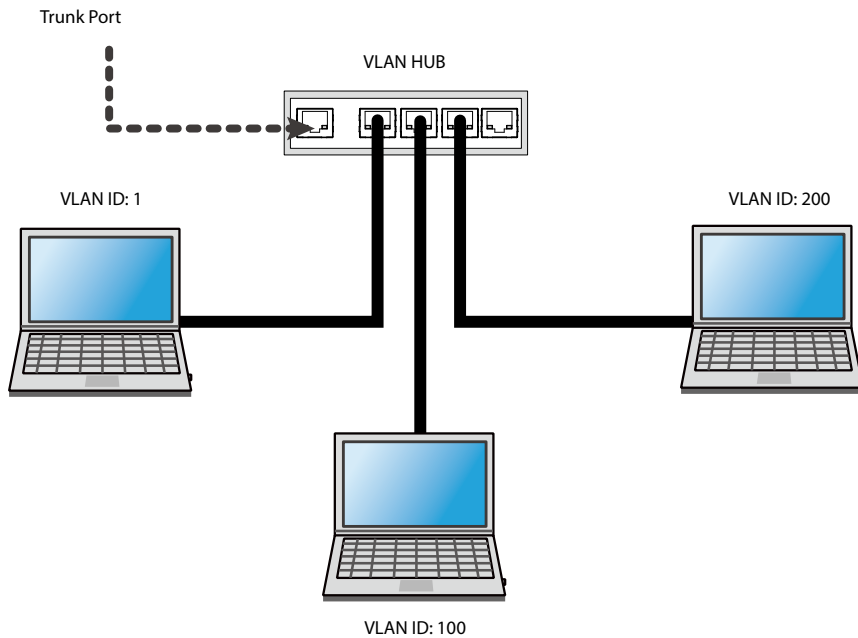
6-3-2. VLAN Function Setting

This chapter describes how to connect Z-1 to a network where network groups have already been established using a VLAN HUB.

Checking VLAN Information

Check the following information of the network:

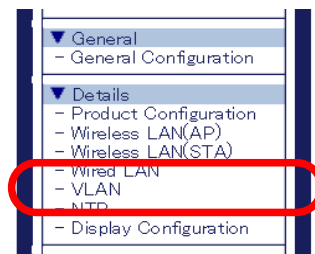
- Location of the trunk port on the VLAN HUB to connect Z-1
- VLAN ID of the native VLAN
- VLAN ID of devices connected to the VLAN HUB



- When there is no available trunk port on the VLAN HUB, create a trunk port.
- For details of the VLAN HUB, see the operating manual that comes with the VLAN HUB.

VLAN Function Setting

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



- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

2. The VLAN configuration page appears. Enter the settings and click **Submit**.



TIP

- When the page is switched to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. Before accessing 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 when the VLAN function is enabled, enter the same VLAN ID to **Management VLAN ID** as the network group where the RADIUS server is installed.



Note

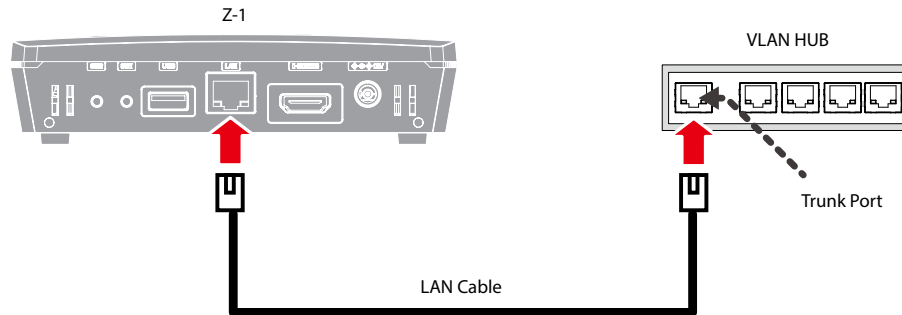
- See "**A. Setting Items**" for details on each item.
- For **Native VLAN ID**, enter the native VLAN ID of the VLAN HUB.
- For the VLAN ID under wireless LAN 1 to 4, enter the VLAN ID of devices connected to the HUB.
- After the VLAN function is enabled, Z-1 can be configured only from the network group that has the same VLAN ID as the Management VLAN ID.
- When the VLAN function is enabled, the VLAN ID can also be set from the wireless LAN general configuration page.
- When **Native VLAN ID** and **Management VLAN ID** have the same value and the VLAN function is enabled, access is allowed even from the HUB that does not support VLAN. For this reason, it is recommended to set the same value for **Native VLAN ID** and **Management VLAN ID**.

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

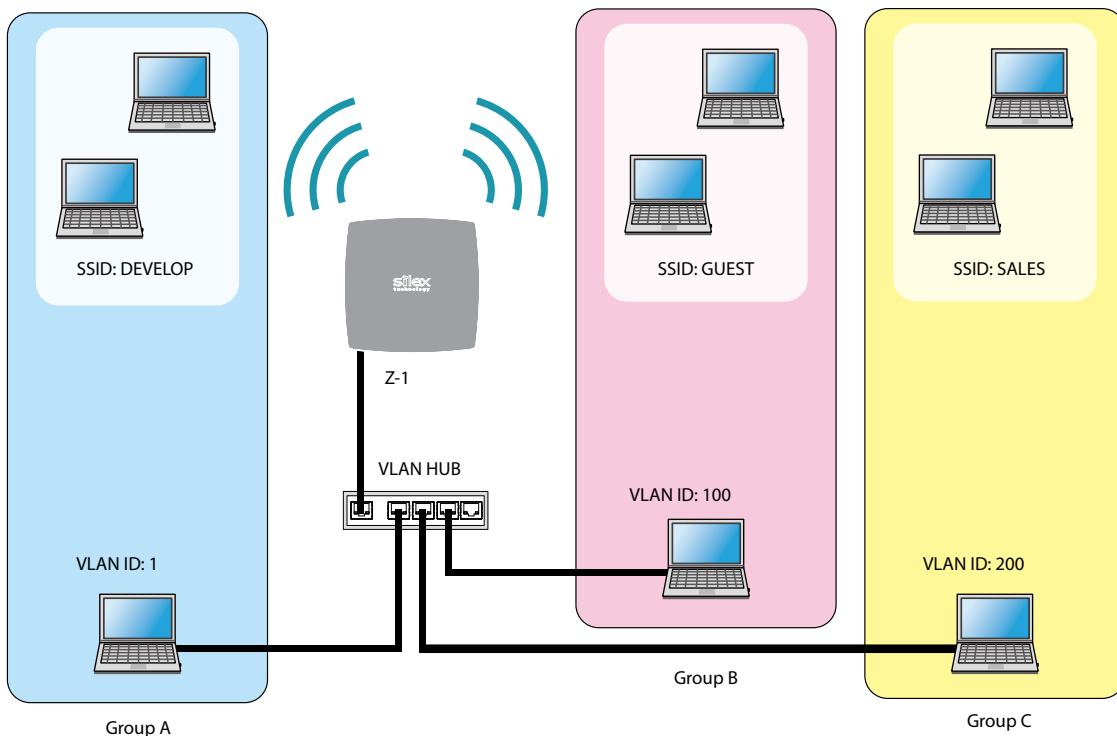
4. After the restart, close the Web browser.

Connecting Z-1 to Trunk Port of VLAN HUB

Connect one end of the LAN cable to a wired port of Z-1 and the other end to a trunk port of the VLAN HUB.



The VLAN function setting has been configured.
Z-1 will operate with virtual network groups based on the VLAN ID settings.



Creating Virtual Network Groups



- After the VLAN function is enabled, Z-1 can be configured only from the network group that has the same VLAN ID as the Management VLAN ID. If you are not sure of the VLAN ID of the Management VLAN ID, the configuration needs to be initialized.
- To configure from a PC that is connected to a wireless LAN on the VLAN-enabled environment, the VLAN ID of the wireless LAN (SSID) needs to be the same as the VLAN ID of the management VLAN ID.

6-4. Time Sync with NTP Server

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

6-4-1. What is NTP Function?

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



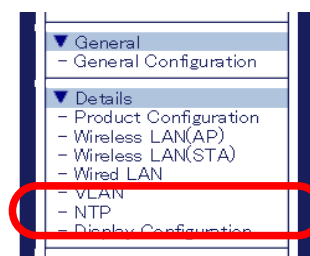
- When there is no NTP server in the network, the system time will start at "00:00:00 (hours: minutes: seconds) on January 1, 2001".

Note

- By connecting from Windows, the time of Windows PC can be set to Z-1.

6-4-2. NTP Function Setting

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



- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

Note

2. The NTP configuration page appears. Select **ENABLE** for **NTP**, enter the necessary settings and click **Submit**.

Name	Value
NTP	ENABLE
NTP Server	
Local Time Zone	+8:00
Scheduled Reboot	DISABLE
Reboot Time	00 : 00

Submit



TIP

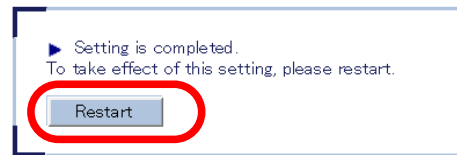
- When the setting page is switched to another page from the page menu before **Submit** is clicked, all the entered values will be cleared. Before accessing other pages, click **Submit** to save the entered values



Note

- See **A. Setting Items** for details on each item.

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



4. After the restart, close the Web browser.

6-5. Projection Authentication (PIN Code) Function

6-5-1. What is Projection Authentication Function?

The projection authentication function is a function to prevent an unintended projection using a PIN code.

The following options can be selected.

Item	Description
DISABLE	The projection authentication function is not used (default).
PRESET	Uses the PIN code that is pre-configured by the user (administrator). The default value is a last 4-digit number of the Z-1's serial number.
RANDOM	The random PIN code is set at 0:00 (*) every day and when Z-1 is started. It changes every time when Z-1 is restarted. The user will need to enter the PIN code shown on the screen.



Note

- The local time zone setting is used for this function.
- When the time setting is not configured on Z-1, the PIN code is reset in 24 hours. To use this function correctly, the NTP server setting is required.

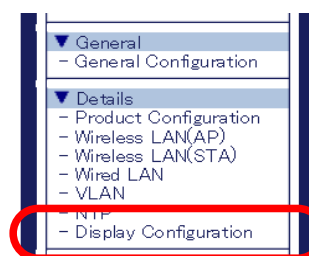


TIP

- If this function is enabled, the projection is accepted only when the PIN code matches on the terminal after the connection is requested from AirPlay or Windows.
- This function does not support Google Cast. Connection from Google Cast performs without authentication.

6-5-2. Projection Authentication Function Setting

1. Access the Z-1's Web page and click **Display Configuration** on the page menu.



Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

- In the display configuration page, select the desired setting at **PIN Code Type**. When **PRESET** is selected for **PIN Code Type**, enter a 4-digit number for **PIN Code** and click **Submit**.

The screenshot shows the 'Display Configuration' web page. The 'PIN Code Type' dropdown is set to 'PRESET' and the 'PIN Code' field contains '1234'. A red circle highlights the 'Submit' button at the bottom right.

Name	Value
Initial Presentation Mode	[Single Presenter ▼]
Allow presenter interrupt	[ENABLE ▼]
PIN Code Type	[PRESET ▼]
PIN Code	1234
Resolution of display (mm)	10
Display Resolution	[2K ▼]

Name	Name	IP Address
Pair 1	Pair1	0.0.0.0
Pair 2	Pair2	0.0.0.0
Pair 3	Pair3	0.0.0.0
Pair 4	Pair4	0.0.0.0
Pair 5	Pair5	0.0.0.0
Pair 6	Pair6	0.0.0.0
Pair 7	Pair7	0.0.0.0
Pair 8	Pair8	0.0.0.0
Pair 9	Pair9	0.0.0.0
Pair 10	Pair10	0.0.0.0



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

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

Setting is completed.
To take effect of this setting, please restart.



Note

- When you are to configure the settings on other pages, restart Z-1 when all other configuration is done.

- After the restart, close the Web browser.

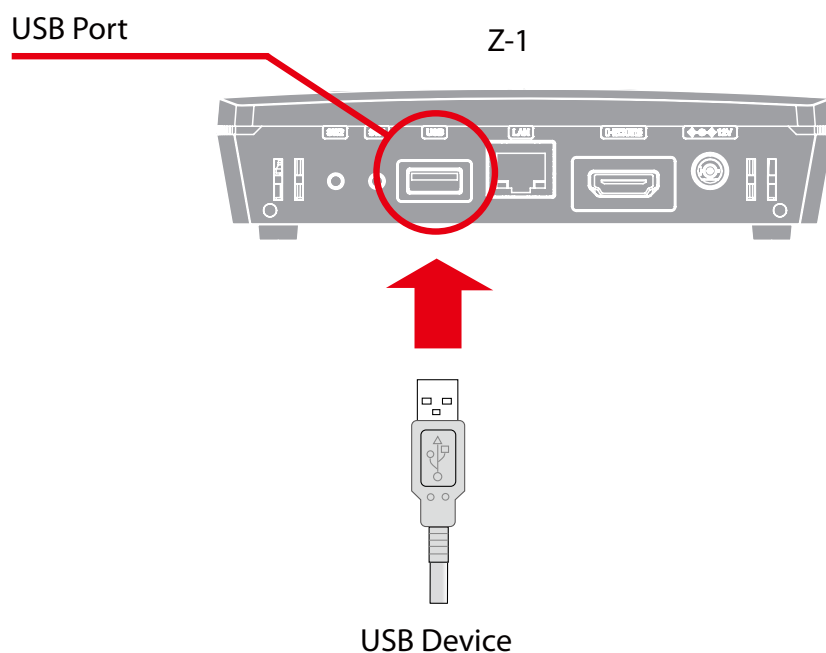
6-6. Device Server Function

The USB devices connected to Z-1 can be shared over the network.
To use the device server feature, the USB connection utility, "SX Virtual Link" is required.
How to install and use SX Virtual Link is as follows:



- To use the device server feature, the **Device Server** setting needs to be enabled on the access control page. For details, refer to **6-7-1. Use of Security Functions - Access Control**.
- The device server feature of Z-1 supports only HID (Human Interface Device) class devices such as mouse and keyboard. A touch panel can also be connected if it is a HID class device.
- To connect the USB device, it needs to be connected using SX Virtual Link.

Connect the USB device that you wish to share over the network to the USB port of Z-1.



6-6-1. Downloading & Installing SX Virtual Link

What is SX Virtual Link?

SX Virtual Link allows you to connect your PC to a USB device that is connected to Z-1. Use SX Virtual Link when you want to connect/disconnect to/from the USB device. The USB devices can be used as if they were directly connected to your PC.

How to Download SX Virtual Link

1. Access our website below.

URL: <https://www.silxtechnology.com/>

2. Go to the support section and download SX Virtual Link.

How to Install SX Virtual Link



TIP

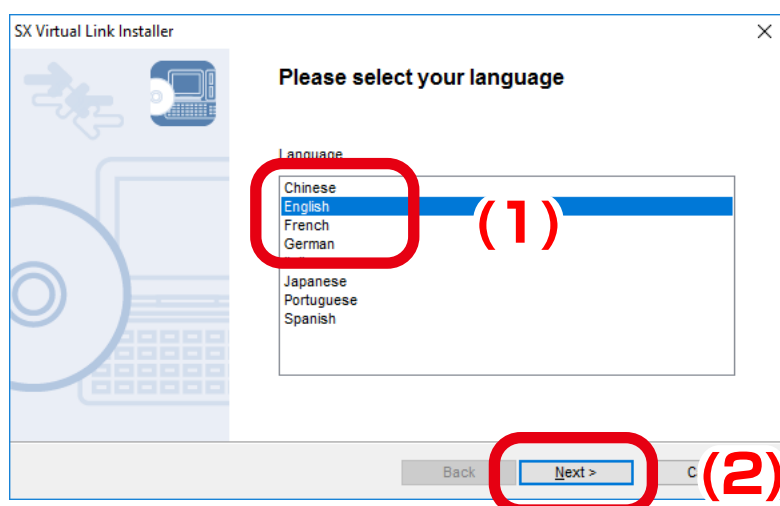
- Administrator privilege is required for installation.

1. Decompress the file you have downloaded and then double-click **Cosetup.exe**.

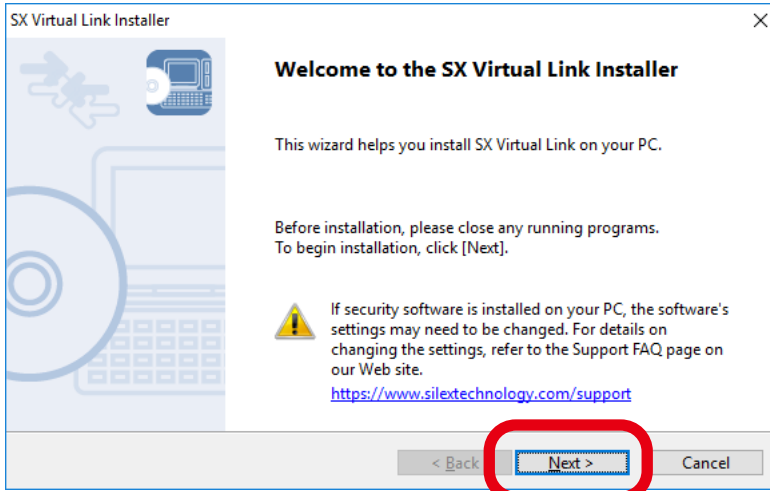


2. The User Account Control message is displayed. Click **Yes**.

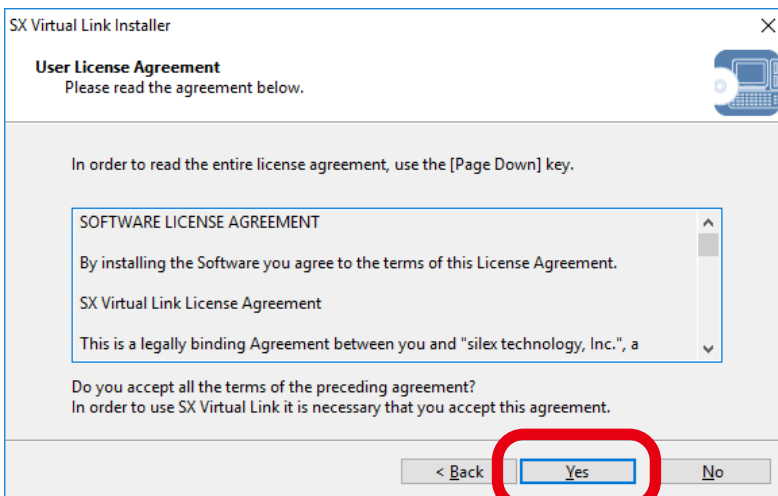
3. SX Virtual Link installer is started and the language selection menu is displayed. Select **English** and click **Next**.



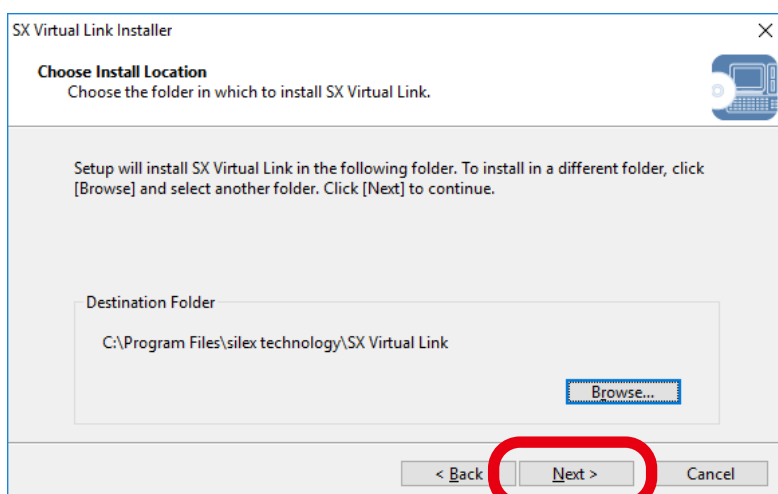
4. Click **Next**.



5. Read the **SOFTWARE LICENSE AGREEMENT** and click **Yes**.



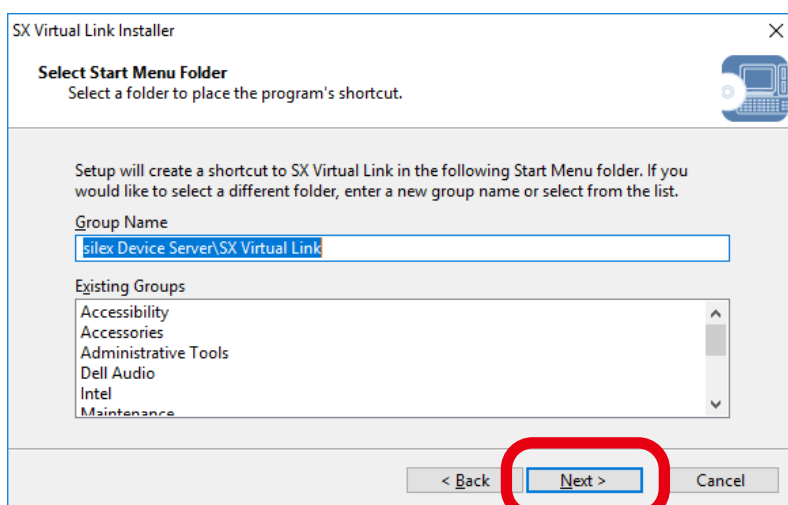
6. Select the folder to install SX Virtual Link into and click **Next**.



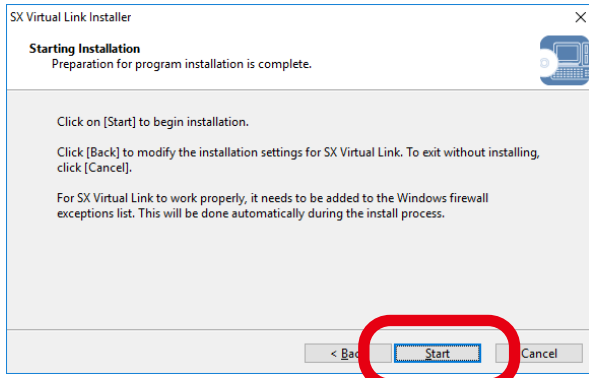
- By clicking **Browse**, the folder can be changed.

Note

7. Enter the group name to be displayed in the start menu and click **Next**.

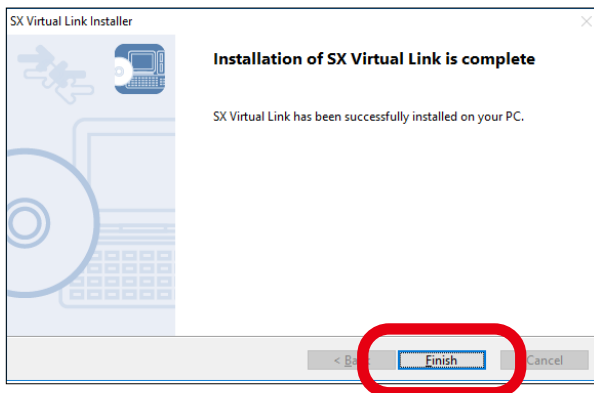


8. Click **Start** to begin the installation.



• When the **Windows Security** screen is displayed, click **Install**.


9. SX Virtual Link has been installed. Click **Finish**.



• If using a firewall function of commercial security software, please add SX Virtual Link to the exception list in your security software. Refer to the FAQ on our website (<https://www.silextechnology.com/>) for details on adding an application to the exception list.

6-6-2. Sharing USB Devices over the Network

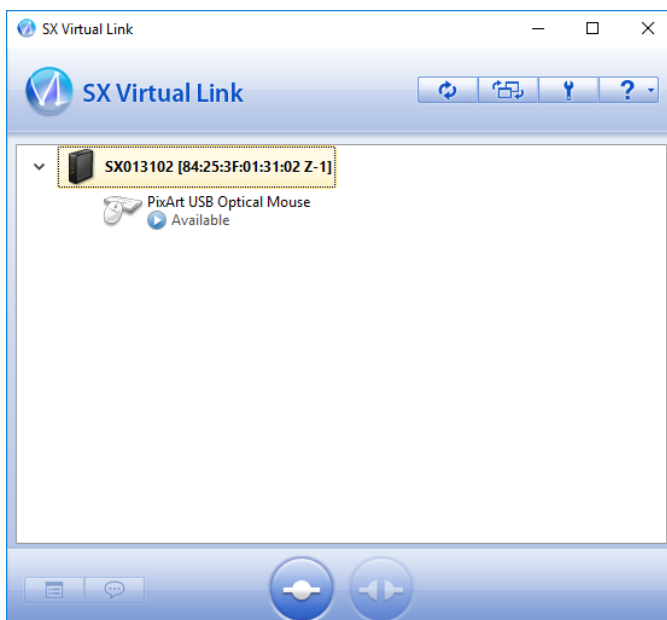
How to Start SX Virtual Link

1. Click the SX Virtual Link icon () in the task tray.

**Note**

- If SX Virtual Link is not running, click **Start - SX Virtual Link**.

2. The SX Virtual Link's main window appears. The USB devices running on a network are displayed in the device list.


**Note**

- SX Virtual Link can be set to automatically run at startup as a minimized application in the task tray by changing the optional settings. For details on optional settings, refer to the SX Virtual Link's online help.


How to Connect/Disconnect to/from USB Devices

1. Select the USB device in SX Virtual Link's main window and connect to it.
2. When successfully connected to the USB device, Windows Plug and Play will run and the USB device will become ready to use.
3. When finished using the USB device, disconnect it using SX Virtual Link.

How to connect:

Double-click	Double-click the USB device in SX Virtual Link's main window.
Use a button	Select the USB device and click the Connect button  in SX Virtual Link's main window. If you select two or more USB devices, you can connect to them at once.
Right-click	Right-click on the USB device in SX Virtual Link's main window and click Connect in the menu displayed. If you select two or more USB devices, you can connect to them at once.
Use a keyboard	Select the USB device using the up/down arrow keys and press Alt+C on your keyboard.

How to disconnect:

Double-click	Double-click the USB device in SX Virtual Link's main window.
Use a button	Select the USB device and click the Disconnect button  in SX Virtual Link's main window.
Right-click	Right-click on the USB device in SX Virtual Link's main window and click Disconnect in the menu displayed.
Use a keyboard	Select the USB device using the up/down arrow keys and press Alt+D on your keyboard.




- If a USB device is shared among several users, make sure that each user disconnects from the USB device after they have finished using it. Otherwise, other users will not be able to connect to the USB device.

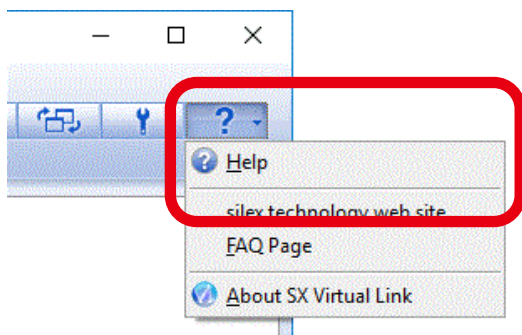


Note

- For details on how to use SX Virtual Link, refer to the SX Virtual Link's online help.

How to Open the SX Virtual Link's Online Help

1. Start SX Virtual Link.
2. In the SX Virtual Link's main window, click the Help button () and select **Help** from the menu displayed.



3. The online help will open.



6-6-3. Uninstalling SX Virtual Link

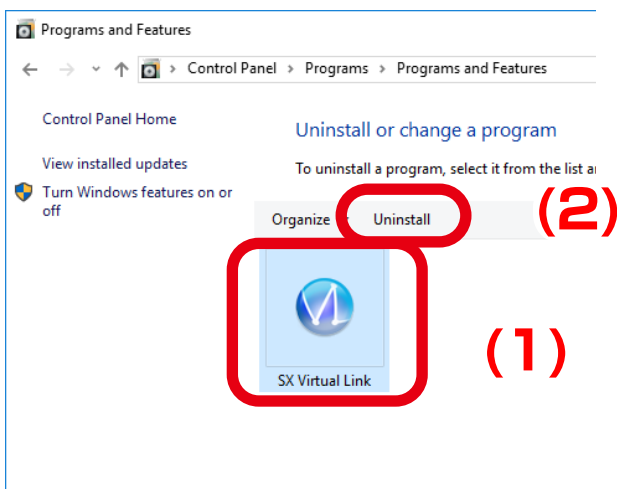
The following explains how to uninstall the USB device connection utility, SX Virtual Link.



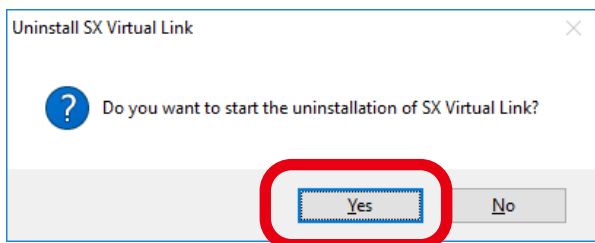
• To uninstall SX Virtual Link, administrator privilege is required.

1. Click **Control Panel - Uninstall a program.**

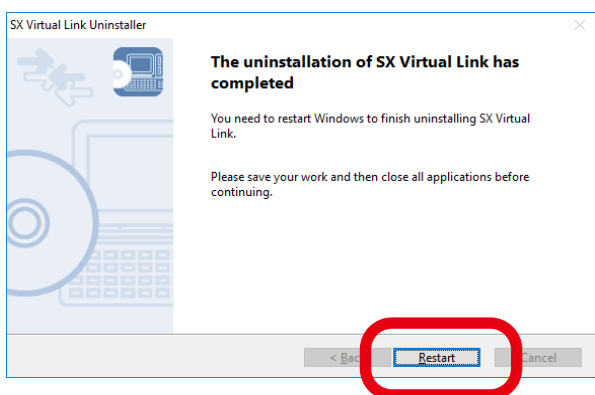
2. Select SX Virtual Link from the list and click **Uninstall.**



3. A confirmation message is displayed. Click **Yes** to start the uninstallation.



4. When the below window is displayed, click **Finish**.



6-7. Security Function

6-7-1. Use of Security Function

How to Change Administrator Password

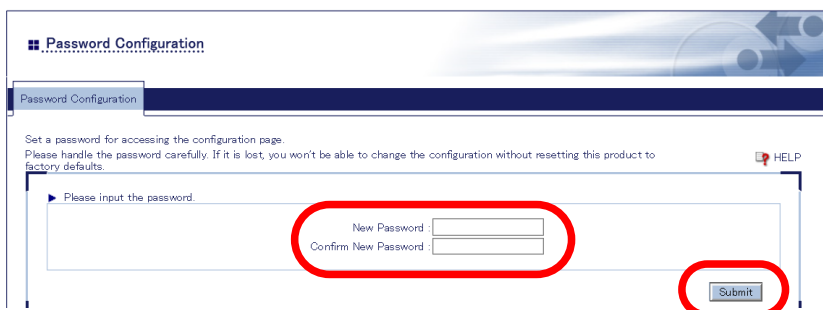
1. Access the Z-1's Web page and click **Password** on the page menu.



Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

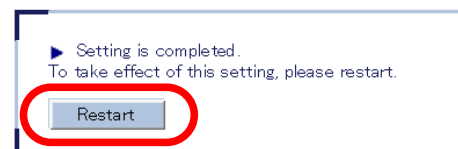
2. The password configuration page appears. Enter the new password in **New Password** and **Confirm New Password**, and then click **Submit**.



TIP

- Be careful not to forget the password. If the password is lost, you will not be able to change the configuration unless Z-1 is reset to the factory default setting.

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



Note

- When you are to configure the settings on other pages, restart Z-1 when all other configuration is done.

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

Access Control

If the access control function is used, the specified protocols can be disabled so that any accesses using those protocols can be blocked. The access control can be set respectively for wired LAN and wireless LAN.

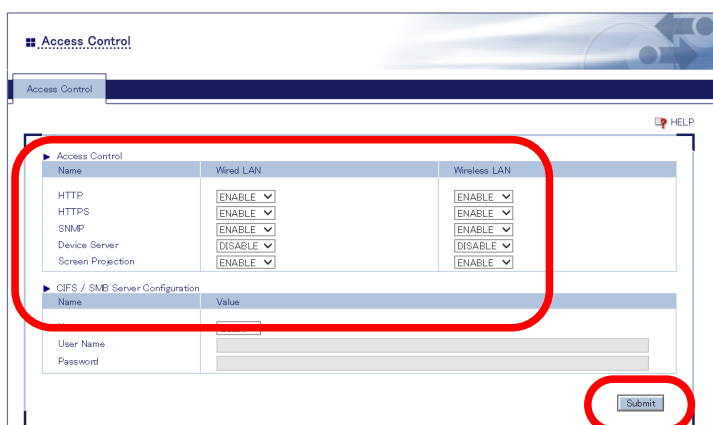
1. Access the Z-1's Web page and click **Access Control** on the page menu.



- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

Note

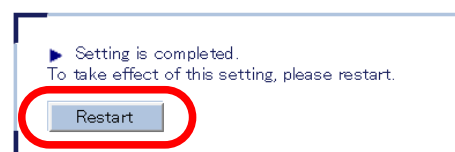
2. The access control page appears. Select **Enable** or **Disable** for each protocol and click **Submit**.



- When you are to configure the settings on other pages, restart Z-1 when all other configuration is done.

Note

3. The restart page shows up. The 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.

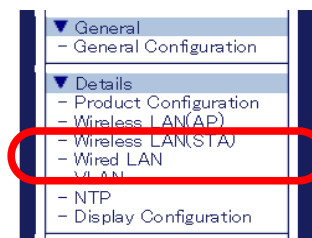
6-7-2. How to Accept/Block Specific Wired LAN Devices

This chapter explains how to register the MAC addresses of wired LAN devices to accept or block accesses to Z-1.



- Before you begin, check the MAC addresses of the target devices.

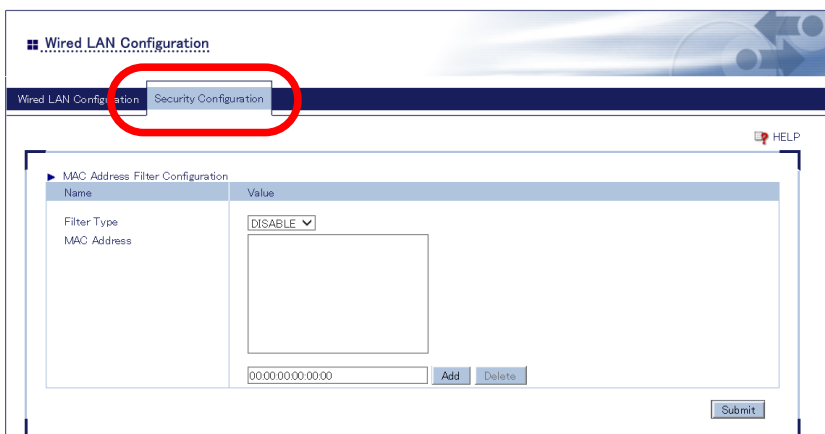
1. Access the Z-1's Web page and click **Wired LAN** on the page menu.



Note

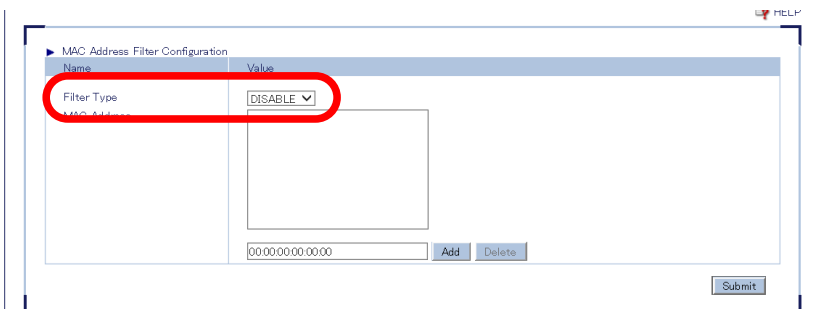
- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

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



3. Select the filter type at **MAC Address Filter Configuration**.

- **ALLOW:** Accepts connection only from the registered wired LAN devices.
- **DENY:** Blocks connection from the registered wired LAN devices.



4. Enter the MAC address of the wired LAN device to the address field, and click **Add**. Repeat this when there are multiple devices to register. Click **Submit** when all MAC addresses have been registered.

Name	Value
Filter Type	ALLOW
MAC Address	84253F012945 703EAD

8476C5999999 Add Delete

Submit



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



- MAC address must be entered in the form of "XX:XX:XX:XX:XX:XX".
- It is possible to register only with the vendor code (the first 6 characters of MAC address). In that case, wired devices having that vendor code will be accepted or blocked.
- To delete the registered MAC address, select it and click **Delete**.

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

▶ Setting is completed.
To take effect of this setting, please restart.

Restart



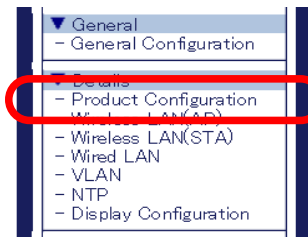
- When you are to configure the settings on other pages, restart Z-1 when all other configuration is done.

6. After the restart, close the Web browser.

6-7-3. How to Control Push Switch Function

This chapter describes how to control the push switch that you can find on bottom of the Z-1 unit.

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



Note

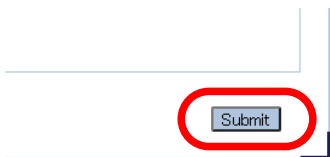
- For how to access the Z-1's Web page, refer to **How to Access the Web Page** at **3-1-5. Z-1's Web Page**.

2. Enable/Disable the use of **Reset Switch** and **Function Switch**.

A screenshot of the 'Product Configuration' web page. The page is divided into several sections: DHCP Client, DNS Configuration, DHCP Server Configuration, and Push Switch Control Configuration. The 'Push Switch Control Configuration' section is highlighted with a red circle. It contains two items: 'Reset Switch' and 'Function Switch', both with 'ENABLE' selected in a dropdown menu. A 'Submit' button is located at the bottom right of the section.

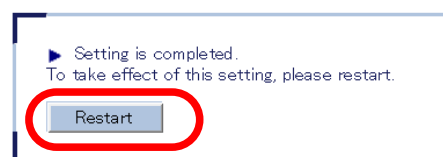
Items	Description
Reset Switch	Set whether to use Reset Switch (SW1). If DISABLE is selected, this switch cannot be used to initialize Z-1.
Function Switch	Set whether to use Function Switch (SW2). If DISABLE is selected, this switch cannot be used for Smart Wireless Setup and projection mode change.

3. Click **Submit** at the bottom right of the Web page.



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

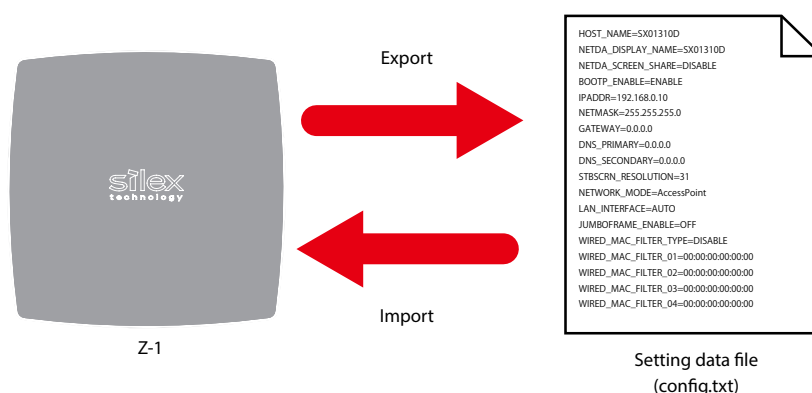


5. After the restart, close the Web browser.

6-8. Administrative Function

6-8-1. Export/Import of Setting Data

This chapter explains how to export/import the setting data. The export function can save the Z-1's setting as a file (config.txt) to external hardware. The import function can read and apply the saved setting back to Z-1. Use a Web browser for the setting export/import.

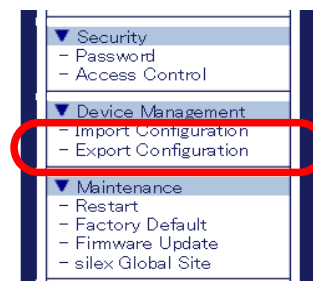


TIP

- For the setting file to import, be sure to specify the one that has been exported from Z-1.
- Do not change the file name or the content of the exported setting file, otherwise the file cannot be imported correctly.
- If the firmware version is different between the Z-1 unit from which the setting file is exported and the other Z-1 unit to which the setting file is imported, the import may not perform correctly.

Export Setting from Web Page

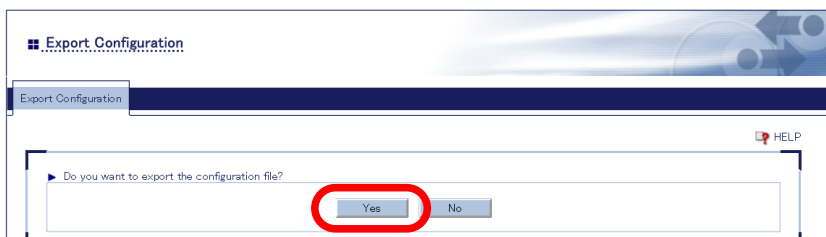
1. Access the Z-1's Web page and click **Export Configuration** on the page menu.



Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page**.

- The export configuration page appears. Click **Yes**.



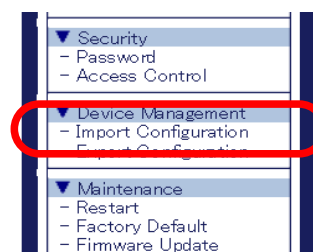
- When the download confirmation message appears, select the preferred option.

Import Setting from Web Page



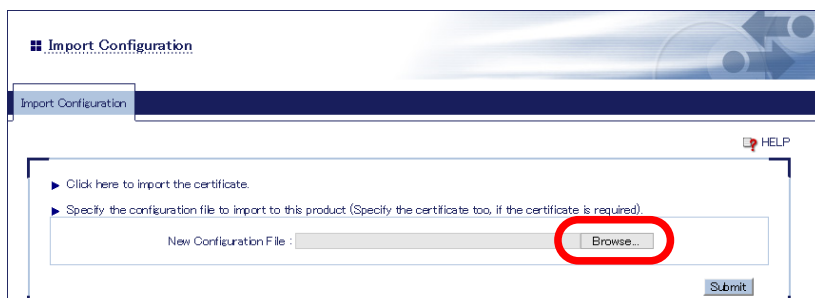
- When importing the setting that uses a certificate, the certificate needs to be imported beforehand.

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



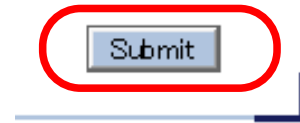
- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page**.

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



- For the setting file to import, be sure to specify the one that has been exported from Z-1.

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



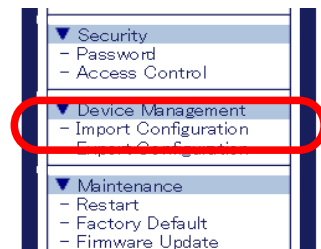
TIP

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

4. The import confirmation dialog appears. Click **OK** to start the file import.

Import Certificate from Web Page

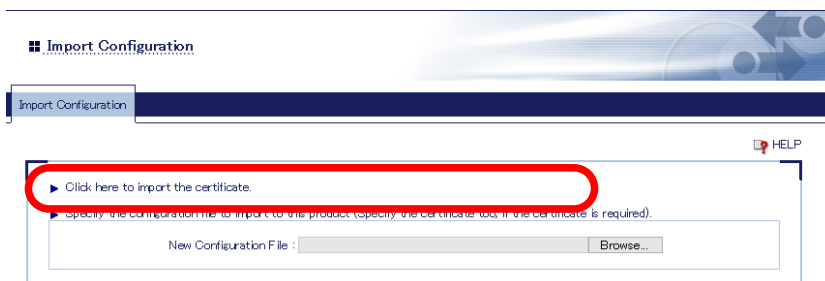
1. Access Z-1's Web page and click **Import Configuration** on the page menu.



Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page**.

2. The import configuration page appears. Click "**Click here to import the certificate**".



3. Register the certificate to use for the IEEE802.1X authentication. Make sure that it is registered for both wireless LAN and wired LAN.

The screenshot shows a web interface for certificate registration. It is divided into two main sections: 'Wireless LAN (STA)' and 'Wired LAN'. Each section contains a 'Certificate import' table and a 'Certificate Registration Status' table. The 'Certificate import' tables have columns for 'Name' and 'Value'. The 'Certificate Registration Status' tables have columns for 'Certificate Name' and 'Registration Status'. The 'Client Certificate Password' field is highlighted with a red circle in both sections. The 'Registration Status' for 'Client Certification' is 'Not Registered' in both sections. A 'Submit' button is located at the bottom right of the interface.

Certificate import [Wireless LAN(STA)]	
Name	Value
Client Certificate Password	<input type="text"/>
Client Certification	<input type="text"/> Browse...
CA Certification	<input type="text"/> Browse...
PAC File Distribution	<input type="text"/> Browse...

Certificate Registration Status [Wireless LAN(STA)]	
Certificate Name	Registration Status
Client Certification	Not Registered
CA Certification	Not Registered
PAC File Distribution	Not Registered

Certificate import [Wired LAN]	
Name	Value
Client Certificate Password	<input type="text"/>
Client Certification	<input type="text"/> Browse...
CA Certification	<input type="text"/> Browse...

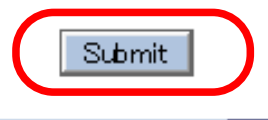
Certificate Registration Status [Wired LAN]	
Certificate Name	Registration Status
Client Certification	Not Registered
CA Certification	Not Registered

Specify the configuration file to import to this product. (Specify the certificate too, if the certificate is required).

New Configuration File : Browse...

Submit

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



TIP

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

6-9. Maintenance Function

6-9-1. Restart

Z-1 can be restarted by the following methods.

- Restart using an AC cable
- Restart using the Web page



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

Restart Using AC Cable

1. Unplug the AC plug from the outlet.
2. Plug the AC plug back into the outlet.
3. The standby screen appears on the display connected to Z-1. When the animation stops, the restart is completed.

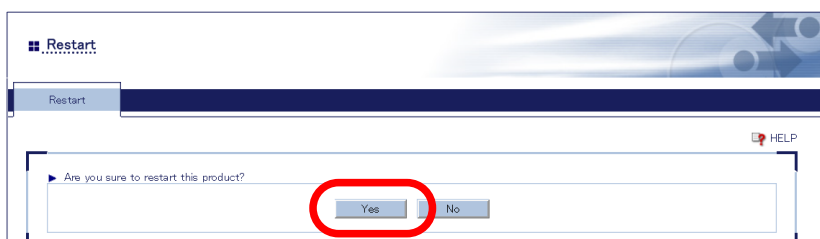
Restart Using Web Page

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



- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

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



3. When the restart is completed, the login page appears. Close the Web browser.

6-9-2. Factory Default Configuration

If Z-1 has a specific network setting to use for another network, or if the administrative password is lost and the Z-1's Web page cannot be accessed, you need to reset Z-1 to the factory default setting. There are two methods below for factory default configuration.

- Factory default configuration using the reset switch
- Factory default configuration using Web page



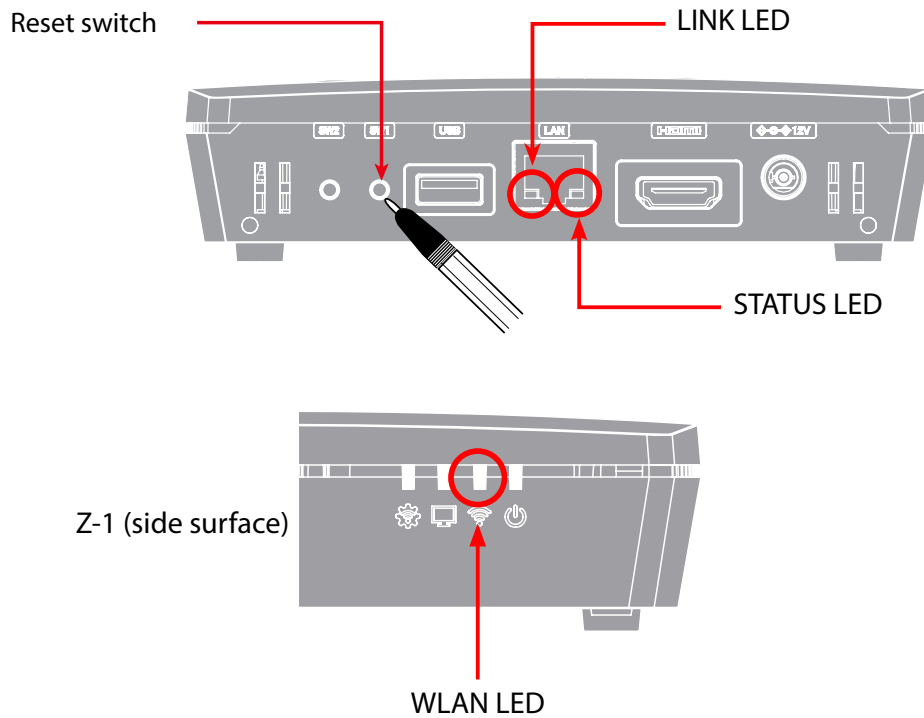
TIP

- It is recommended to take notes of the current settings. Once the factory default configuration is done, all the settings will be reset to the factory default settings.
- Make sure that there is no device connected to Z-1 during the factory default configuration.
- Do not unplug the AC plug during the factory default configuration.
- Do not push the reset switch when you turn on Z-1 after the factory default configuration is finished.
- To use the Reset Switch, the **Reset Switch** setting needs to be **ENABLE**. For details, refer to **6-7-3. How to Control Push Switch Function**.

Factory Default Configuration Using Reset Switch

1. Unplug the AC plug from the outlet.
2. Press and hold the reset switch with a fine tipped object such as a pen or pencil while plugging the AC plug back into the outlet. The LINK LED and STATUS LED of the LAN port will turn on. Keep holding the switch.

3. The factory default configuration will start when the STATUS LED of the LAN port turns off. Then, release the switch. When the WLAN LED turns on or blinks, the factory default configuration is completed.



Note

- When you are using 'Z-1 Rev.B', the factory default configuration is completed when the LINK LED and STATUS LED of the LAN port turn on.

Factory Default Configuration Using Web Page

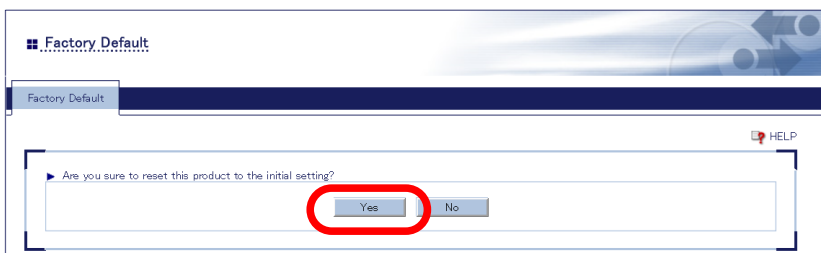
1. Access the Z-1's Web page and click **Factory Default** on the page menu.



Note

- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

- The factory default configuration page appears. Click **Yes**.



- The confirmation dialog appears. Click **OK** to start the factory default configuration.

- Z-1 is restarted when the factory default configuration is finished.

- The login page will appear. Close the Web browser.



- Since the IP address of Z-1 is also reset to the default one when the factory default configuration is finished, the login page may not be displayed correctly on the PC. In such a case, change the IP address of Z-1 or of the PC so that they can communicate each other.

6-9-3. Firmware Update

How to Download Latest Firmware

The latest firmware can be downloaded from the Silex Technology's website. Before updating the firmware, download the latest one.

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 on the PC.

Now, you have the latest firmware.

How to Update Firmware



- Make sure that there is no PC connected to Z-1 during the firmware update.
- Do not unplug the AC plug from the outlet during the firmware update.

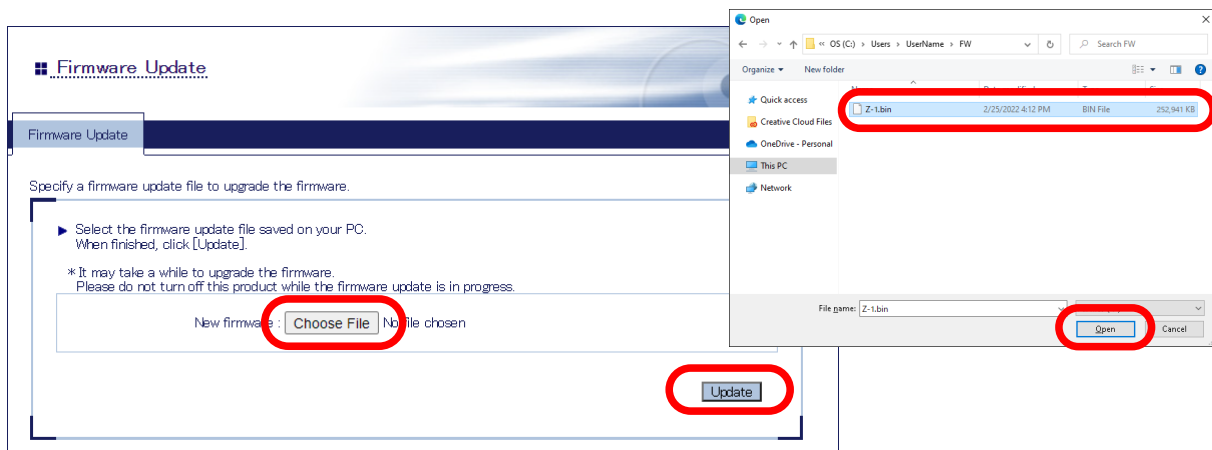
1. Access the Z-1's Web page and click **Firmware Update** on the page menu.



Note

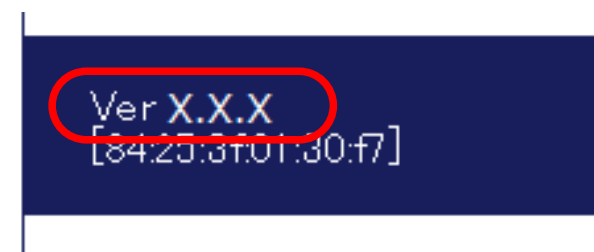
- For how to access the Z-1's Web page, refer to **How to Access the Web Page at 3-1-5. Z-1's Web Page.**

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



3. The update confirmation 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 restart Z-1 by unplugging/plugging the AC cable from/into the outlet.

A. Setting Items

A-1. General Configuration

The Z-1's general configuration items are explained at "**A-2. Detailed Configuration**".

A-2. Detailed Configuration

This chapter shows the Z-1's detailed configuration items.

A-2-1. Product Configuration

Product Configuration

General Configuration

Name	Host Name
Description	Set the host name. Be sure to set a unique name that is not used by other devices.
Value/Range	1 to 15 alphanumeric characters and symbols
Default value	SXxxxxxx (xxxxxx: last 3 bytes of the MAC address)

Name	Display name
Description	Set 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)

Name	Search Tag
Description	This is a character string used to search for devices from AMC Meeting. Two or more settings can be configured by separating them with a space.
Value/Range	Character string (50 characters or less)
Default value	NONE

Name	Default Touch Mode
Description	<p>Set the operation mode to apply when the touch panel display is connected to Z-1.</p> <p>Interactive :</p> <p>The interactive function is enabled when the touch panel display is connected. When the screen of a Windows PC is projected using AMC Meeting, it is possible to control that PC by touching the touch panel display.</p> <p>Draw :</p> <p>The drawing function is enabled when the touch panel display is connected. It is possible to draw on the touch panel display by touching or dragging.</p> <ul style="list-style-type: none"> - The operation mode can be changed from the toolbar. - If the Windows PC to project is switched after the operation mode is changed from the toolbar, the operation mode will be reset to the mode selected at this setting.
Value/Range	Interactive / Draw
Default value	Interactive

TCP/IP Configuration

Name	DHCP Client
Description	Enable/Disable the 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	Specify the IP address. When DHCP client is enabled, an IP address obtained from DHCP server will be assigned.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

Name	Subnet Mask
Description	Specify the subnet mask. When DHCP client is enabled, a subnet mask obtained by DHCP server will be 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	Specify the default gateway. If 0.0.0.0 (default value) is given, this setting is disabled. When DHCP client is enabled, a default gateway obtained from DHCP server will be 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	Specify the DNS primary server address. When DHCP client is enabled, DNS server address obtained from DHCP server will be assigned.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

Name	DNS Server (Secondary)
Description	Specify the DNS secondary server address. When DHCP client is enabled, DNS server address obtained from DHCP server will be 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	Enable/Disable the DHCP server. When Z-1 is used as DHCP server to automatically assign an IP address to PC, choose Enable . When DHCP server is operating in the same network, choose Disable . To enable this function, disable the DHCP client function and set a static IP address.
Value/Range	Enable/Disable
Default value	Disable

Name	Start IP Address
Description	Specify the start IP address to use 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	Specify the end IP address to use 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	Specify the subnet mask for the IP address to assign. If 0.0.0.0 is given, this setting is disabled and a subnet mask corresponding to the start IP address will automatically be used.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	255.255.255.0

Name	Default Gateway
Description	Specify the default gateway. If 0.0.0.0 (default value) is given, this setting is disabled.
Value/Range	0.0.0.0 to 255.255.255.255
Default value	0.0.0.0

Name	Lease Time
Description	Specify the lease time. When 0 days 0 hours 0 minutes are given, the lease time period will be 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

Push Switch Control Configuration

Name	Reset Switch
Description	Enable/Disable the control of Reset Switch.
Value/Range	Enable/Disable
Default value	Enable

Name	Function Switch
Description	Enable/Disable the control of Function Switch.
Value/Range	Enable/Disable
Default value	Enable

A-2-2. Wireless LAN (AP)

Basic Settings

Wireless LAN Common Configuration

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

Name	Wireless Mode
Description	Set the IEEE 802.11 wireless standard.
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	Specify the frequency bandwidth for 802.11n/b/g, 802.11n/a or 802.11ac. In wireless LAN, a frequency band is divided up so that more wireless devices can communicate at once. The segmented band is called channel. The frequency bandwidth is 20 MHz per channel. When the channel bandwidth is 40 MHz or 80 MHz, the data amount increases per traffic, and Z-1 can attain the high-speed communication. 80 MHz is only available for 802.11ac.
Value/Range	20 MHz/40 MHz/80 MHz
Default value	40 MHz

Z-1 User's Manual (Configuration Method)

Name	Channel
Description	Specify a channel to use in the wireless LAN. A channel is a divided frequency band. In wireless LAN, a frequency band is divided up so that more 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 with other wireless products, change the channel. * For W53 and W56 channels, communication is lost for 1 min when Z-1 is started or when a radar wave is detected.
Default value	36

Name	Ext Channel
Description	The extended channel is displayed. 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 channel.
Default value	40

Name	DFS Primary Channel
Description	Specify a channel to be switched if radar waves are detected when the communication channel is subject to DFS. When the alternative channel is not specified or when radar waves are detected even on the switched channel, Z-1 will switch the channel in the specific order. This setting is applied only when the communication channel is W53 or W56.
Value/Range	For the W53 channel, set the W53 band channels or NONE. For the W56 channel, set the W56 band channels or NONE.
Default value	NONE

Name	Transmit Power Level
Description	Specify the strength of radio transmission for 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

Name	AP Bridge
Description	By disabling this setting, communication between a wireless LAN and a wired LAN can be restricted.
Value/Range	Enable/Disable
Default value	Enable

Wireless LAN Basic Configuration

Name	Interface
Description	Enable/Disable the wireless interface 1-4.
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	Specify the SSID of wireless LAN that Z-1 is connected to. SSID is an ID for a group of devices to communicate over a wireless network. The wireless devices need to share the same SSID to communicate with each other.
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	Specify the VLAN ID for wireless interface.
Value/Range	1 to 4094
Default value	Wireless LAN1: 1 Wireless LAN2: 1 Wireless LAN3: 1 Wireless LAN4: 1

Name	Stealth Mode
Description	Enable/Disable the stealth mode function.
Value/Range	Enable/Disable
Default value	Wireless LAN1: Disable Wireless LAN2: Disable Wireless LAN3: Disable Wireless LAN4: Disable

Name	Network Authentication
Description	Specify the authentication method used for communicating with wireless devices. WPA/WPA2 is recommended for robust security. TKIP cannot be used for IEEE 802.11n/IEEE 802.11ac.
Value/Range	<p>Open (Open system): Accepts all access without performing authentication. WEP is used for encryption.</p> <p>Shared (Shared key): Uses the WEP key for encryption as the authentication key, and allows access of devices having the same key. WEP is used for encryption.</p> <p>WPA-PSK: Uses the PSK for network authentication. The communication encryption method is chosen from TKIP/AES/AUTO. The encryption key is generated by communicating with a wireless device based on the shared key. WEP key setting will not be used.</p> <p>WPA2-PSK: Uses the PSK for network authentication. The communication encryption method is chosen from AES/AUTO. The encryption key is generated by communicating with a wireless device based on the shared key. WEP key setting will not be used.</p> <p>WPA/WPA2-PSK: Both WPA-PSK and WPA2-PSK can be used.</p> <p>802.1X: Provides the IEEE 802.1X's user authentication and dynamic WEP encryption.</p> <p>WPA-Enterprise: Provides the IEEE 802.1X's user authentication and TKIP/AES/AUTO encryption.</p> <p>WPA2-Enterprise: Provides the IEEE 802.1X's user authentication and AES/AUTO encryption.</p> <p>WPA/WPA2-Enterprise: Provides the IEEE 802.1X's user authentication and AES/AUTO encryption.</p>
Default value	<p>Wireless LAN 1: WPA2-PSK</p> <p>Wireless LAN 2: Open</p> <p>Wireless LAN 3: Open</p> <p>Wireless LAN 4: Open</p>

WEP Configuration

Name	WEP
Description	Enable/Disable the WEP encryption when the network authentication is Open. When the WEP encryption is used, communication will be encrypted in wireless LAN using the WEP key (1 to 4) and Key index settings.
Value/Range	ON / OFF
Default value	Wireless LAN1: OFF Wireless LAN2: OFF Wireless LAN3: OFF Wireless LAN4: OFF

Name	Key Index
Description	Specify the WEP key number (1 to 4). The key index has to be the same as that of the device to communicate with.
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	Specify the WEP key.
Value/Range	5 or 10-digit alphanumeric characters 10 or 26 hexadecimal digits * In most cases, alphanumeric characters and numbers are used. * When the key size (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	Select the encryption mode when the network authentication method is set to one of the followings: 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	Specify the pre-shared key to use when the network authentication method is set to one of the followings and the encryption mode is TKIP/AES. WPA-PSK WPA2-PSK WPA/WPA2-PSK The pre-shared key is a key word to generate an encryption key. It is also known as 'network key' or 'password'.
Value/Range	8 to 63 alphanumeric characters 64 hexadecimal digits
Default value	Wireless LAN1: xxxxxxxx Wireless LAN2: xxxxxxxx_2 Wireless LAN3: xxxxxxxx_3 Wireless LAN4: xxxxxxxx_4 (xxxxxx: Generated from the MAC address)

Name	Group key renew interval
Description	Specify the refresh interval for the encryption key (mins). Zero (0) disables this setting.
Value/Range	0 to 1440
Default value	Wireless LAN1: 60 Wireless LAN2: 60 Wireless LAN3: 60 Wireless LAN4: 60

RADIUS Server Configuration (Primary Server)

Name	Server IP
Description	Specify the IP address of RADIUS server. This setting is valid only 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	Specify the port number used for communication with RADIUS server.
Value/Range	0 to 65535
Default value	1812

Name	Shared Secret
Description	Specify the secret key used for communication with RADIUS server.
Value/Range	0 to 255 alphanumeric characters
Default value	None

RADIUS Server Configuration (Secondary Server)

Name	Server IP
Description	Specify the IP address of RADIUS server. This setting is valid only 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	Specify the port number used for communication with RADIUS server.
Value/Range	0 to 65535
Default value	1812

Name	Shared Secret
Description	Specify the secret key used for communication with RADIUS server.
Value/Range	0 to 255 alphanumeric characters
Default value	None

Extended Settings

Extension Configuration

Name	Beacon Interval(msec)
Description	Set the interval to send beacons (millisecond).
Value/Range	20 to 1000
Default value	100

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

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

Name	A-MPDU
Description	Enable/Disable the A-MPDU setting. When ON is selected, the throughput may increase. This setting is valid 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	Enable/Disable the Short Guard Interval setting. When ON is selected, the throughput may increase. This setting is valid 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	Set the 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

**Abbreviations**

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

Note

Name	ECWmax
Description	Set the 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	Set the 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	Set the 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	Set the 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	Set the 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	Set the 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	Set the 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	Set the 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

Security Configuration

Name	Privacy Separator
Description	Allow/Deny the communication between wireless LAN stations connected to Z-1. A wireless interface with the enabled privacy separator forwards wireless frames only to the wired LAN interface but not to the other wireless interfaces.
Value/Range	ON/OFF
Default value	OFF

MAC Address Filter Configuration

Name	Filter Type
Description	Specify the security type of the MAC address filter.
Value/Range	<p>DISABLE: Allows access of all wireless stations.</p> <p>ALLOW: Allows access of the wireless stations registered to the MAC address filter list.</p> <p>DENY: Blocks access of the wireless stations registered to the MAC address filter list.</p>
Default value	DISABLE

Name	MAC Address
Description	MAC address or the vendor code of MAC address (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	Enable/Disable the smart wireless setup.
Value/Range	Enable/Disable
Default value	Enable

Name	Interface
Description	Select the wireless interface to execute the Smart Wireless Setup.
Value/Range	1 to 4
Default value	1

Name	External Registrar
Description	Enable/Disable the external registrar.
Value/Range	Enable/Disable
Default value	Disable

Name	PIN Code
Description	Specify 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)

Basic Settings

Wireless LAN Common Configuration

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

Wireless LAN Basic Configuration

Name	SSID
Description	Set the SSID of the wireless LAN that Z-1 is connected to. SSID is an ID for group of devices to communicate in a wireless LAN. Devices need to have the same SSID to communicate with each other.
Value/Range	1 to 32 alphanumeric character(s)
Default value	SXxxxxxx (xxxxxx: Last 3 bytes of the MAC address)

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

Value/Range	<p>WPA2-Enterprise: Provides the IEEE 802.1X's user authentication and AES/AUTO encryption.</p> <p>WPA/WPA2-Enterprise: Provides the IEEE 802.1X's user authentication and AES/AUTO encryption.</p> <p>* For 802.11n/802.11ac, the Shared authentication, 802.1X authentication, WEP encryption, and TKIP encryption cannot be used.</p>
Default value	Open

Name	Encryption Mode
Description	<p>Select the encryption mode (TKIP/AES/AUTO) for the following network authentication methods:</p> <ul style="list-style-type: none"> • WPA-PSK • WPA2-PSK • WPA/WPA2-PSK • WPA-Enterprise • WPA2-Enterprise • WPA/WPA2-Enterprise <p>* When the network authentication method is one of the following, TKIP cannot be selected:</p> <ul style="list-style-type: none"> • WPA2-PSK • WPA/WPA2-PSK • WPA2-Enterprise • WPA/WPA2-Enterprise
Value/Range	TKIP AES AUTO
Default value	AES

WEP Configuration

Name	WEP
Description	Enable/Disable the WEP encryption. This can be selected when the authentication method is Open.
Value/Range	ON / OFF
Default value	OFF

Name	Key Index
Description	<p>Set the key index of the WEP key to use (1-4).</p> <p>The key index has to be the same as that of the device to communicate with.</p>
Value/Range	1 to 4
Default value	1

Name	WEP Key (1 to 4)
Description	Set the 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	Specify this 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	Select 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	Specify 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

Z-1 User's Manual (Configuration Method)

Name	Client Certificate Password
Description	Set a password for the client certificate to use for client authentication of the IEEE 802.1X authentication. This 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	Select a client certificate to use for client authentication of the IEEE 802.1X authentication. This is used when the authentication method is set to EAP-TLS.
Value/Range	Select a file.
Default value	-

Name	EAP Password
Description	Specify 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 used 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	Set the inner authentication method (PAP/CHAP/MSCHAP/MSCHAPv2) that will be conducted during TLS tunneling of the IEEE 802.1X authentication. When the authentication method is PEAP, the inner authentication is fixed to MS-CHAPv2.
Value/Range	PAP CHAP MSCHAP MSCHAPv2
Default value	PAP

Name	Auto PAC Provisioning
Description	Enable/Disable the automatic distribution of PAC (Protected Access Credential) for EAP-FAST authentication. When the automatic distribution is disabled, a PAC file needs to be registered after it is generated by the server.
Value/Range	ON/OFF
Default value	OFF

Name	PAC File Distribution
Description	Register a PAC file that is generated by the server, and is used to manually distribute PAC (Protected Access Credential) for EAP-FAST authentication.
Value/Range	Select a file.
Default value	-

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

Name	Server authentication
Description	Set whether to verify the server credibility on the IEEE 802.1X authentication. When it is ON , CA certificate is needed for server authentication.
Value/Range	ON/OFF
Default value	OFF

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



- Please create the client certificate and the CA certificate separately. Z-1 does not support the certificate composed of multiple certificate files.

Smart Wireless Setup

Name	Smart Wireless Setup
Description	Enable/Disable the Smart Wireless Setup.
Value/Range	Enable/Disable
Default value	Enable

Name	PIN Code
Description	Specify a PIN code for Z-1.
Value/Range	8-digit number (decimal)
Default value	Unique to each Z-1.

A-2-4. Wired LAN

Wired LAN Settings

Name	Link Speed
Description	Specify the physical network type. Use AUTO for regular operation. When a LINK lamp of the connected HUB 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: Allows access of any devices. DENY: Blocks access of the devices registered to the MAC address filter. ALLOW: Allows access from the devices registered to the 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

IEEE 802.1X Configuration

Name	IEEE 802.1X
Description	Enable/Disable the IEEE 802.1X user authentication for wired LAN. When Enable is selected and Z-1 is operating in Access Point mode, a multi-host mode needs to be set for a port of the authentication-compatible switch. For details, refer to the operating manual that comes with the switch.
Value/Range	Enable/Disable
Default value	Disable



- Multi-host mode: This is a mode to allow communication of multiple hosts on a single port.

Note

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

Name	EAP User Name
Description	Specify the EAP user name used for the 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	EAP Password
Description	Specify 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 used when the authentication method is EAP-TTLS or PEAP.
Value/Range	Character string (32 characters or less)
Default value	None

Name	Client Certificate Password
Description	Set the password for client certificate to use for client authentication of the IEEE 802.1X authentication. This 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	Select a client certificate used for the IEEE 802.1X's client authentication. It is used when the authentication method is set to EAP-TLS.
Value/Range	Select a file.
Default value	-

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

Name	Server Authentication
Description	Set whether to verify the server credibility on the IEEE 802.1X authentication. When it is ON , CA certificate is needed for server authentication.
Value/Range	ON/OFF
Default value	OFF

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



TIP

- Please create the client certificate and the CA certificate separately. Z-1 does not support the certificate composed of multiple certificate files.

A-2-5. VLAN

IEEE802.1Q VLAN Configuration

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

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

Name	Management VLAN ID
Description	Set the management VLAN ID to access 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	Set the VLAN ID used for a wireless interface.
Value/Range	1 to 4094
Default value	1

Name	DHCP Client
Description	Enable/Disable the DHCP client function. To set the IP address using DHCP, the DHCP server has to be operating in the subnetwork.
Value/Range	Enable/Disable
Default value	Disable

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

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

A-2-6. NTP

NTP Configuration

Name	NTP
Description	Enable/Disable the NTP protocol.
Value/Range	Enable/Disable
Default value	Disable

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

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

Name	Scheduled Reboot
Description	Enable/Disable the periodic restart function.
Value/Range	Enable/Disable
Default value	Disable

Name	Reboot Time
Description	Specify the time to restart Z-1 when the scheduled reboot function is in use.
Value/Range	00:00 to 23:50 (set by 10 minutes)
Default value	00:00

Time Synchronization

Name	Browser Time
Description	Shows the system time of the PC in which the Web browser is opened.
Value/Range	* The value is not variable.
Default value	-

Name	NTP Server
Description	Shows the name of the NTP server to synchronize with. Synchronization runs for the server that is set at NTP Server of NTP Configuration .
Value/Range	* The value is not variable.
Default value	-

Synchronous State

Name	Synchronized Time
Description	Shows the time obtained from the NTP server.
Value/Range	* The value is not variable.
Default value	-

Name	Synchronized NTP Server
Description	Shows the name of the NTP server that was synchronized to get the time information.
Value/Range	* The value is not variable.
Default value	-

A-2-7. Display Setting

Display Configuration

Display Configuration

Name	Initial Presentation Mode
Description	Select the projection mode to apply when Z-1 is started.
Value/Range	Z-1 will operate in one of the following modes: <ul style="list-style-type: none"> • Single Presenter • Multi Presenter • Distribution Master • Distribution Slave • Pair Display
Default value	Single Presenter

Name	Allow presenter interrupt
Description	Allows an interrupt of new connection when the projection is in progress.
Value/Range	Enable/Disable
Default value	Enable

Name	PIN Code Type
Description	This is a function to prevent an unintended projection that may occur as a result of incorrect use.
Value/Range	DISABLE : Does not use the PIN code. PRESET : Uses the PIN code pre-configured by the user (administrator). RANDOM : A random PIN code is set at 0:00 every day and when Z-1 is started.
Default value	DISABLE

Name	PIN Code
Description	Set the PIN code to use when the PIN code type is Preset.
Value/Range	4 digit number (decimal number)
Default value	The initial value is generated from the Z-1's MAC Address.

Name	Time to stop signal output (minutes)
Description	Set the time until the HDMI signal stops when projection does not take place. If 0 is set, it will not stop.
Value/Range	0-60
Default value	0

Name	Display Resolution
Description	Set the HDMI resolution output from Z-1.
Value/Range	2K : HDMI output is executed at 2K(1920x1080). Even if a 4K compatible display is connected, output will be executed at 2K. 2K/4K : HDMI output is executed at 2K(1920x1080) or 4K(3849x2160). The appropriate resolution level is automatically selected according to the connected display.
Default value	2K

Pair Display Config

Name	Pair 1 to 10 (Name)
Description	Register the devices to use as a pair. Up to 10 pairs can be registered (Pair 1 to 10).
Value/Range	1 to 15 alphanumeric characters
Default value	"Pair1" to "Pair10"

Name	Pair 1 to 10 (IP Address)
Description	Register the devices to use as a pair. Up to 10 pairs 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	This deletes all records of the paired devices. Note that it clears everything.
Value/Range	None
Default value	None

Standby Screen Configuration

Standby Screen Configuration

Name	Standby Screen
Description	Select the standby screen from Instruction screen, Standard screen or Custom screen. The Instruction screen is displayed only in single presenter mode.
Value/Range	Instruction / Standard / Custom
Default value	Instruction

Name	Customized Standby Screen
Description	Select an image file to use for the custom screen, and upload it to Z-1. The file must be a PNG file (1,920 x 1,080 pixels). The maximum size is 1,048,560 bytes.
Value/Range	None
Default value	-

Display Information Configuration

Name	Show Connection Info
Description	Set whether to display the connection information (the host name, IP address, and SSID) on the OSD setting page.
Value/Range	Enable/Disable
Default value	Enable

Name	Show access point information
Description	This shows the access point information to display on the standard screen, instruction screen or custom screen.
Value/Range	None SSID Only SSID/QR Code SSID/Key SSID/Key/QR Code
Default value	SSID/Key/QR Code

Name	Target wireless interface
Description	Set a wireless interface used to display the access point information.
Value/Range	Wireless1 Wireless2 Wireless3 Wireless4
Default value	Wireless1

A-3. Security

A-3-1. Password

Please input the password.

Name	New Password
Description	Set 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	1 to 8 alphanumeric characters
Default value	None

A-3-2. Access Control

Access Control

Name	HTTP
Description	This can control an HTTP access from the wired/wireless LAN. Enable allows access and Disable denies access to Z-1.
Value/Range	Enable/Disable
Default value	Wired LAN: Enable Wireless LAN: Enable

Name	HTTPS
Description	This can control an HTTPS access from the wired/wireless LAN. Enable allows access and Disable denies access to Z-1.
Value/Range	Enable/Disable
Default value	Wired LAN: Enable Wireless LAN: Enable

Name	SNMP
Description	This can control an SNMP access from the wired/wireless LAN. Enable allows access and Disable denies access to Z-1.
Value/Range	Enable/Disable
Default value	Wired LAN: Enable Wireless LAN: Enable

Name	Device Server
Description	This can control an access from the wired/wireless LAN when Z-1's device server function is used. Enable allows access and Disable denies access to Z-1.
Value/Range	Enable/Disable
Default value	Wired LAN: Disable Wireless LAN: Disable

Name	Screen Projection
Description	This can control an access from the wired/wireless LAN when Z-1's display function is used. Enable allows access and 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	Set the user account. Guest allows an access from all users. User requires the user authentication.
Value/Range	Guest/User
Default value	Guest

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

A-4. Device Management

A-4-1. Import Configuration

Name	New Configuration File
Description	Import a setting file that can be used to change all settings at once.
Value/Range	Select a new setting file.
Default value	-

Certificate import

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

Name	Client Certification
Description	Select a client certificate to use for the IEEE 802.1X's client authentication. This 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 of the IEEE 802.1X authentication.
Value/Range	Select a file.
Default value	-

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

A-4-2. Export Configuration

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

B. **Appendix**

B-1. Certificate Standard

When using the authentication mode which uses a certificate, get the necessary certificate issued from the certificate authority and import it to the Z-1.

The Z-1 supports the following certificates:

Certificate Standard

The certificate supports the standards as follows:

Certificate	Item	Compatible standards
Client certificate	X509 certificate version	v3
	Public key algorithm	RSA
	Public key size	1024bit, 2048bit
	Signature algorithm	SHA1/SHA2(SHA-224,SHA-256,SHA-384,SHA-512) withRSA MD5withRSA
	X509v3 extended key usage	Client authentication (1.3.6.1.5.5.7.3.2)
CA certificate	Public key algorithm	RSA
	Public key size	1024bit, 2048bit
	Signature algorithm	SHA1/SHA2(SHA-224,SHA-256,SHA-384,SHA-512) withRSA MD5withRSA

Certificate Saving Format

The following saving formats are supported:

Certificate	Compatible standards
Client certificate	PKCS#12, pfx * This is the format which includes a secret key of the certificate.
CA certificate	DER (Binary encoded X509) PEM (A text form. DER is BASE64 encoded.)