

Compact / Low-power Wireless Bridge

BR-110AX

User's Manual



Index

1. Introduction	1
1-1. Introduction.....	2
1-1-1. About the Notation	2
1-1-2. Disclaimers	2
1-1-3. Trademarks	2
1-1-4. Glossary	3
1-2. Safety Instructions.....	5
1-3. Notes on Use	9
1-3-1. Precautions.....	9
1-3-2. Use of Radio Waves.....	10
1-3-3. Notes on Security	12
1-3-4. Standards Compliance	13
2. About BR-110AX	16
2-1. Application Image.....	17
2-2. Key Features	18
2-3. Dimensions.....	20
2-4. Parts and Functions	21
2-4-1. LED Indications	22
2-5. Power Supply	23
3. How to Configure	24
3-1. Configuration Procedure	25
3-2. Initial Password Configuration.....	26
3-2-1. Displaying the BR-110AX's Web Page	26
Connecting BR-110AX to a PC	26
Displaying the Web Page Using Configuration Mode	28
Displaying the Web Page by Entering an IP Address	30
Password Configuration	31
Logging In.....	32
3-3. Downloading a Configuration File	33
3-3-1. Downloading from the BR-110AX's Web Page	33
3-3-2. Downloading from AMC Manager.....	34
3-4. Editing a Configuration File	36
3-5. Uploading a Configuration File	38
3-5-1. Uploading from the BR-110AX's Web Page	38
3-5-2. Uploading from AMC Manager.....	40
3-6. Checking the Connection.....	42
3-6-1. Checking the Connection When Operating in Station Mode	42

3-6-2. Checking the Connection When Operating in Access Point Mode.....	43
4. Product Installation.....	44
4-1. Notes on Installation	45
4-2. Installation Image.....	46
4-3. Installation on a Flat Surface	47
4-4. Installation Using Hook-and-Loop Fastener	48
5. Security Enhancement	50
5-1. Enhancing Security with IEEE 802.1X	51
5-1-1. Network Configuration	51
5-1-2. Using IEEE 802.1X in Station Mode.....	52
5-2. Access Control Using the Filter Function	54
5-3. Hiding the Access Point SSID	55
5-4. Changing the Login Password	56
5-4-1. Changing the Password Using the Configuration File.....	56
5-4-2. Changing the Password from the Web Page.....	57
6. Communication Performance Settings.....	58
6-1. Optimizing Roaming	59
6-2. Giving Priority to Voice and Video Traffic	60
6-3. Communicating with an Access Point That Supports the Proxy ARP Function	61
7. Network Functions	62
7-1. DHCP Server Function	63
7-2. Time Synchronization.....	64
8. Operating Status Check	65
8-1. Checking the Operating Status Using LEDs.....	66
8-2. Downloading the Logs	67
8-2-1. Downloading the Logs.....	67
8-2-2. Deleting the Logs.....	69
9. Maintenance	70
9-1. Cleaning BR-110AX	71
9-2. Restarting BR-110AX	72
9-2-1. How to Restart by Disconnecting a USB Cable.....	72
9-2-2. How to Restart from the Web Page	73
Restarting BR-110AX Immediately.....	73
Restarting BR-110AX at Fixed Intervals.....	74
Restarting BR-110AX at a Specified Date and Time.....	75
9-3. Updating Firmware	76
9-3-1. Downloading the Firmware	76
9-4. Factory Default Configuration	77

9-4-1. Initialization Using the Push Switch	77
9-4-2. Initialization from the Web Page	79
10. Troubleshooting	80
10-1. Problems During the Setup	81
10-2. Troubles When Operating in Station Mode	83
10-3. Troubles When Operating in Access Point Mode.....	84
A. List of All Settings	85
A-1. Product Configuration.....	86
A-1-1. Sample Settings for Scheduled Reboot.....	88
A-2. Wireless LAN Configuration.....	89
A-2-1. Sample Wireless Settings	93
A-3. Application Configuration	94
A-3-1. Sample SNTP Settings.....	95
B. Specifications.....	96
B-1. Hardware Specifications	97
B-2. Software Specifications.....	100
B-3. Security Information	101
B-3-1. Access Control Mechanism.....	101
B-3-2. Key Information	101
B-3-3. Known Vulnerabilities.....	102
C. Configuration Utility	103
C-1. AMC Manager	104
C-1-1. What is AMC Manager?	104
How to Download AMC Manager	105
D. Product Information and Customer Services.....	106
D-1. Product Information	106
D-2. Customer Support Center.....	106

1. Introduction

Thank you for purchasing the compact, low-power wireless bridge BR-110AX.
This manual provides information on how to configure and use BR-110AX.
Please read the **1-2. Safety Instructions** carefully before using BR-110AX.

1-1. Introduction

1-1-1. About the Notation

This manual uses the following symbols to indicate specific information for operating BR-110AX.

Be sure to carefully read before using BR-110AX.



: This symbol indicates important information that needs to be observed when operating BR-110AX. Make sure to read this information for safe and proper use.



: This symbol indicates information that is useful when using BR-110AX. If you experience difficulties operating BR-110AX, please refer to this information first.

1-1-2. 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.
- The screen display may vary depending on the BR-110AX firmware version, or the operating system, Web browser and its version of the PC. Some instructions may not be applicable.
- 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.

1-1-3. Trademarks

- AMC Manager® is a registered trademark of Silex Technology, Inc.
- Microsoft and Microsoft Edge are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Wi-Fi, WPA (Wi-Fi Protected Access), WPA2, WPA3, WMM (Wi-Fi Multimedia) are trademarks or registered trademarks of Wi-Fi Alliance.
- USB Type-C is a registered trademark of USB Implementers Forum.
- Other company names and product names contained in this document are trademarks or registered trademarks of their respective companies.
- Trademark symbols such as ™ and ® are omitted from this document except where necessary.

1-1-4. Glossary

The following explains the technical terms used in this manual.

Please refer to this as you read this manual.

Terms	Explanation
Wired LAN Device	In this manual, this refers to a device that is connected to BR-110AX via a LAN cable and communicates over a wired LAN.
Web Page	BR-110AX's Web interface to use for configuration.
IP Address	A value used to identify devices on network such as the Internet. Unlike the MAC address, this value can be changed by users.
MAC Address	This is a unique value assigned to network devices. Also called as 'Ethernet Address' for some devices or software programs. Some devices have multiple MAC addresses. MAC address cannot be changed and thus it can be used for device identification.
DHCP	A communication protocol for allocating and acquiring information which is needed for devices to connect to network. BR-110AX has a DHCP server function that distributes information to communicate, and a DHCP client function that obtains necessary communication information from another DHCP server.
DNS	A system that manages the mapping between IP addresses and domain names (names used to identify computers). It translates domain names into the corresponding IP addresses and IP addresses into the corresponding domain names.
SNTP	A communication protocol used to receive current time information. SNTP is a simplified version of NTP. It synchronizes the internal clock of a device with a dedicated time server, allowing devices on the network to maintain a consistent time.
Wi-Fi	One kind of wireless communication technology. If devices are compatible with this technology, they can communicate wirelessly with each other even if they are made from different manufacturers.
Access Point	A device or function that serves as a host unit when performing wireless communication. By connecting a wireless client device, PC, tablet, etc. to the Access Point on wireless LAN, users can communicate with them on the same network.
Wireless Client Device	In this document, it means all devices that connect to an Access Point via wireless LAN, such as client devices, PCs, and tablets.
SSID	A name to use for grouping on wireless LAN. It must be set for both Access Point and wireless client device to perform wireless communication. Devices with a different SSID cannot communicate with each other.

Terms	Explanation
Channel	A frequency band divided to allow multiple wireless devices to communicate simultaneously. A channel needs to be selected for wireless LAN communication. For a wireless client device, the same channel will automatically be used as the Access Point.
Authentication Method	A general term of authentication method to use for wireless LAN. Together with the encryption method, it ensures security of the wireless LAN. The same authentication method must be set to the Access Point and wireless client device.
Encryption Mode	A general term of communication encryption method. In this document, it refers to the encryption method to use for wireless LAN. The supported encryption methods will differ depending on each product. It ensures wireless LAN security in combination with the authentication method. The same encryption method must be set to the Access Point and wireless client device.
IEEE 802.1X	One of the authentication methods. Authentication is performed through an authentication server, such as a RADIUS server, using a user name, password, or certificate. Because authentication can be performed for each device, it provides a high level of security and is suitable for enterprise networks. To use IEEE 802.1X, select one of the following authentication methods: WPA-Enterprise, WPA2-Enterprise, WPA3-Enterprise, WPA/WPA2-Enterprise, WPA2/WPA3-Enterprise, WPA3-Enterprise 192-bit security
RSSI	The strength of a received wireless signal. The higher the value, the more stable the wireless communication.
WMM	A technology designed to enable efficient transmission of multimedia data over a wireless LAN. It prioritizes streaming traffic such as voice and video data to improve communication quality. WMM is suitable for communications that require real-time performance, such as VoIP and video streaming.

1-2. Safety Instructions

This page provides the safety instructions for safe use of BR-110AX.

To ensure safe and proper use, please read the following information carefully before using BR-110AX. The safety instructions include important information on safe handling of BR-110AX and on general safety issues.

< Indication of the warning >

	Danger	"Danger" indicates the existence of an imminent hazard that could result in death or serious injury if the safety instruction is not observed.
	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.

< Indication of the symbol >

	This symbol indicates the danger, warning and caution. (Example:  "Danger of the electric shock")
	This symbol indicates the prohibited actions. (Example:  "Disassembly is prohibited")
	This symbol indicates the necessary actions. (Example:  "Remove the AC plug from an outlet")

Product installation **Danger**

- * Do not use BR-110AX in areas where flammable or corrosive gases are generated. Doing so may cause fire, electric shock, or malfunction.

 Warning

- * Do not place any objects on top of BR-110AX. It may cause fire, electrical shock or malfunction.
- * Do not cover or wrap BR-110AX with cloth such as blankets or tablecloths. Accumulated heat may cause fire, accident, or malfunction.

 Caution

- * When installing BR-110AX on a wall or in a high location, make sure that it is securely fastened to prevent it from falling due to the weight of the cables.



- * Do not use or store BR-110AX under the following conditions. It may cause malfunction.
 - Locations subject to vibration or shock
 - Shaky, uneven or tilted surfaces
 - Locations exposed to direct sunlight
 - Humid or dusty places
 - Wet places (kitchen, bathroom, etc.)
 - Near a heater or stove
 - Locations subject to extreme changes in temperature
 - Near strong electromagnetic sources (magnet, radio, wireless device, etc.)

Safe handling

 Danger	
	* When using the device connected to BR-110AX, strictly observe the warnings and cautions indicated by the manufacturer of that device, and use it in the correct procedure. Failure to do so may result in fire, electric shock, accident or malfunction. * If your network device has a ground wire, it must be used to prevent electrocution and power surges. Do not connect it to a gas pipe, water pipe, telephone line ground, lightning rod, etc. Doing so may cause malfunction or accident.
	* Do not use BR-110AX in systems that include equipment directly related to human life, such as life-support systems and operating room equipment, or equipment that is critical to public safety and the maintenance of public functions, such as nuclear facilities and aerospace facilities.

Measures for abnormal operations

 Warning	
	* In the following cases, turn off the connected device and remove the power supply cable or plug. Failure to follow these instructions may cause fire, electrical shock, accident or malfunction. - When BR-110AX emits a strange smell, smoke or sound or becomes too hot to touch. - When foreign objects (metal, liquid, etc.) gets into BR-110AX. - When BR-110AX is dropped or the case is broken or cracked.

Disassembly and modification are prohibited

 Danger	
	* Do not disassemble or modify the product. It may cause fire, electrical shock or malfunction.

Notes on using the power supply

 Danger	
	* Be sure to use the specified power supply voltage. Using the power supply voltage other than the specified one may cause fire or electric shock.
 Warning	
	* Keep the cords and cables away from children. It may cause an electrical shock or serious injury.
	* Do not move BR-110AX while the power supply cable is connected. Doing so may damage the cable and which may result in fire or electric shock. * Do not put anything on the AC adapter or power supply cable, and do not cover it. Also, do not use the AC adapter on a heat-retaining or moisture-retaining object (carpet, sponge, cardboard, styrofoam, etc.). There is a risk of overheating, which may cause fire, accident 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 adapter, power supply cable or any other cables with wet hands. It may cause an electrical shock or malfunction.
 Caution	
	* Verify all cables are connected properly and safely before using BR-110AX.
	* When BR-110AX will not be used for an extended time, remove the power supply cable and power plug from the connected device and BR-110AX. * When removing BR-110AX, be sure to unplug the power supply cable and power plug of both BR-110AX and the connected device beforehand.
	* Do not place any objects on the cable, and do not bend, twist, or pull it excessively. * Keep cables and power cords away from the place where people walk by. It may cause injury if they trip over it. * When unplugging BR-110AX or the connected device, do not pull on the cord. The cord may break resulting in fire and/or electric shock. Pull only on the plug.

1-3. Notes on Use

This section describes important precautions to observe when using BR-110AX.

Be sure to read this section before using BR-110AX.

1-3-1. Precautions

- BR-110AX is designed for the region specified by Silex Technology. Silex Technology shall not be liable for any use of BR-110AX outside the designated region. In addition, Silex Technology does not provide maintenance services or technical support for BR-110AX outside the designated region. Please be aware of this before use.
- BR-110AX is not intended for incorporation into or use in the control of equipment or systems that are directly related to human life or require a high degree of reliability, including medical devices, nuclear facilities and equipment, aerospace equipment, and transportation facilities and equipment. Silex Technology assumes no liability for any personal injury, fire, property damage, or other damages resulting from the use of BR-110AX in such equipment, systems, or control applications.
- BR-110AX may be subject to the export control regulations of the Foreign Exchange and Foreign Trade Act of Japan and to the export control laws and regulations of other countries. Before exporting or re-exporting BR-110AX, confirm the applicable laws and regulations and obtain any licenses or approvals that are required.
- Silex Technology shall not be liable for any malfunction of devices connected to BR-110AX, or for any loss, corruption, alteration, or disclosure of data on such devices. This also applies when such problems result from unauthorized access to BR-110AX.
- When you dispose of BR-110AX, follow the regulations and ordinances of your local government.
- BR-110AX and its accessories are subject to change without notice.

1-3-2. Use of Radio Waves

When using BR-110AX near the medical devices

The radio wave interference may adversely affect the operation of medical devices such as pacemakers. When using BR-110AX near the medical devices that require a high level of safety and reliability, check with the manufacturer or distributor of each medical device about the effects of radio waves.

When using BR-110AX near the following devices

- Microwave oven, industrial/scientific equipment, etc.

The above devices use the same radio frequency band as the wireless LAN. Using BR-110AX near the above devices may cause radio wave interference. As the result, communication may be lost, the speed may slow down, or the operation of the above devices may be adversely affected.

Before using BR-110AX, make sure that no radio wave interference occurs. For example, if there is a microwave oven near BR-110AX, check the proper communication beforehand while actually using the microwave oven.

Do not use BR-110AX near a cellular phone, TV or Radio

A cellular phone, TV and radio use a different radio band than our products. Generally, if they are used near BR-110AX, it will not cause any problems. However, when they approximate BR-110AX, sound or image noise may occur.

If there is reinforced concrete/metal between wireless devices, they may not connect

BR-110AX can connect through wood or glass, but may have troubles connecting through reinforced concrete/metal.

BR-110AX complies with the certification of conformance to technical standards. Please pay attention to the following points:

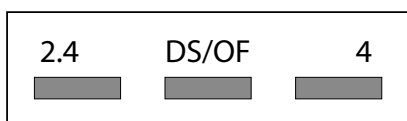
- Please do not disassemble or remodel the product. Such action is prohibited by law.
- Please do not remove the certificate label. Using the product without a label is prohibited.

Wireless devices using 2.4GHz band

The same frequency band of BR-110AX is used for a microwave, industry, science, medical equipment and licensed in room or low power (non-licensed) radio stations.

- Before you use BR-110AX, check that it does not interfere with other devices.
- If interference occurs, stop using BR-110AX or change the wireless band. Please consider to create a wall between these devices to avoid interference. Contact us for possible solution.

* The meaning of the symbols in the bottom of the unit:



2.4	: Wireless devices using 2.4GHz frequency band
DS/OF	: DS-SS or OFDM is used as modulation.
4	: The range of interference is equal to or lower than 40m.
  	: All bands can be used to avoid interference.

Notes on using 5GHz band

- Use of 5.2GHz band (W52) and 5.3GHz band (W53) outdoors is prohibited by the radio regulations.

1-3-3. Notes on Security

Because a wireless LAN uses electromagnetic signals instead of a LAN cable to establish communication with network devices, it has the advantage of allowing devices to connect to the network easily. However, a disadvantage of this is that within a certain range, the electromagnetic signals can pass through barriers such as walls, and if security countermeasures are not implemented in some way, problems such as the following may occur.

- Communication is intercepted by a third party
- Unauthorized access to the network
- Leakage of personal information (ID and Card information)
- Spoofing and the falsification of intercepted data
- System crashes and data corruption

Nowadays, wireless LAN cards or access points are equipped with security measures that address such security problems, so that you can enable security-related settings for wireless LAN products in order to reduce the likelihood of problems occurring.

We recommend that you make yourself fully acquainted with the possible implications of what might happen if you use a wireless product without enabling security features, and that you configure security-related settings and use wireless products at your own responsibility.

1-3-4. Standards Compliance

Notice to US Customers



Contains FCC ID : N6C-IM100

FCC Rules, Part 15 §15.19(a)(3)

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.

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

FCC Rules Part 15

FCC CAUTION

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Rules Part 15 Subpart B

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

RF Exposure Compliance

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

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 must be installed and operated keeping the radiator at least 20cm or more away from person's body.

Notice to Canadian Customers

Contains IC : 4908A-IM100

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

HMN BR-110AX

RSS-Gen Issue 5 §8.4

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.

RSS-247 Issue 4 §7.3

For indoor use only(5150-5350 MHz)

Pour usage intérieur seulement(5150-5350 MHz)

RSS-102 Issue 5 §2.6

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



UK

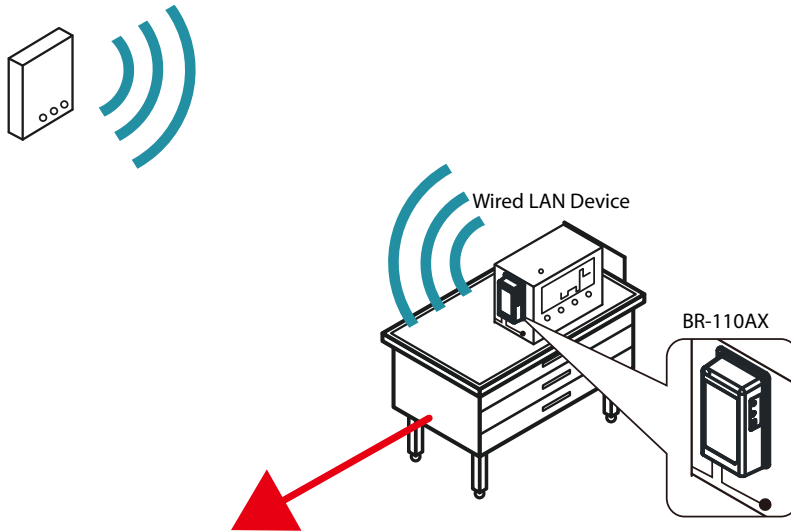
Restrictions or Requirements in the UK

2. About BR-110AX

2-1. Application Image

BR-110AX is a wireless bridge that enables wired LAN devices to be easily connected to a wireless network. It is designed for environments where installation space or power availability is limited, such as medical facilities and retail stores, as well as for moving devices that require wireless network connectivity.

Access Point



Devices that have traditionally been difficult to connect to a wireless network due to size or power constraints, such as monitors, dialysis machines, label printers, and POS systems, can be connected to a wireless network as power is supplied to BR-110AX through a USB cable.



- Only one device can be connected to the LAN port of BR-110AX. It is impossible to connect multiple devices using an Ethernet Hub.

2-2. Key Features

The following explains the features of BR-110AX.

Compact Design

BR-110AX features a compact enclosure measuring 48 × 77 × 22 mm (excluding protrusions), allowing installation even in limited spaces. Using the supplied hook-and-loop fastener, it can be easily attached to mobile carts or equipment.

Environmental Resistance

BR-110AX provides IP21 dust and drip protection and is resistant to disinfectants commonly used in medical environments. The enclosure is made of UL94 V-0 flame-retardant material.



- To maintain the IP21 dust and drip protection performance, install BR-110AX with the connector side facing downward (toward the floor). Refer to **4-1. Notes on Installation** for details.



Note

- For information on disinfectants that can be used for BR-110AX, refer to **9-1. Cleaning BR-110AX**.

Access Point Function

BR-110AX has an Access Point function and supports connection of up to 8 wireless client devices, including BR-110AX units operating in Station mode.

Security

The following authentication and encryption methods are supported.

For Station Mode

Authentication Method	Encryption Method
Open	None
WPA-Personal	AES
WPA2-Personal	
WPA3-Personal	
WPA/WPA2-Personal	
WPA3-Personal SAE Transition	
WPA-Enterprise	
WPA2-Enterprise	
WPA3-Enterprise	
WPA/WPA2-Enterprise	
WPA2/WPA3-Enterprise	
WPA3-Enterprise 192-bit security	

For Access Point Mode

Authentication Method	Encryption Mode
Open	None
WPA-Personal	AES
WPA2-Personal	
WPA3-Personal	

Fast Roaming

BR-110AX supports IEEE 802.11r (Fast Transition), enabling stable communication even for devices used while in motion, such as medical carts.

Low Power Consumption

With its low-power design, BR-110AX receives power through its USB Type-C connector. Power can be supplied from a connected device or a PC.

Support for AMC Manager, the unified device management software

The following functions are available when using AMC Manager:

- Remote control and monitoring
- Bulk configuration change

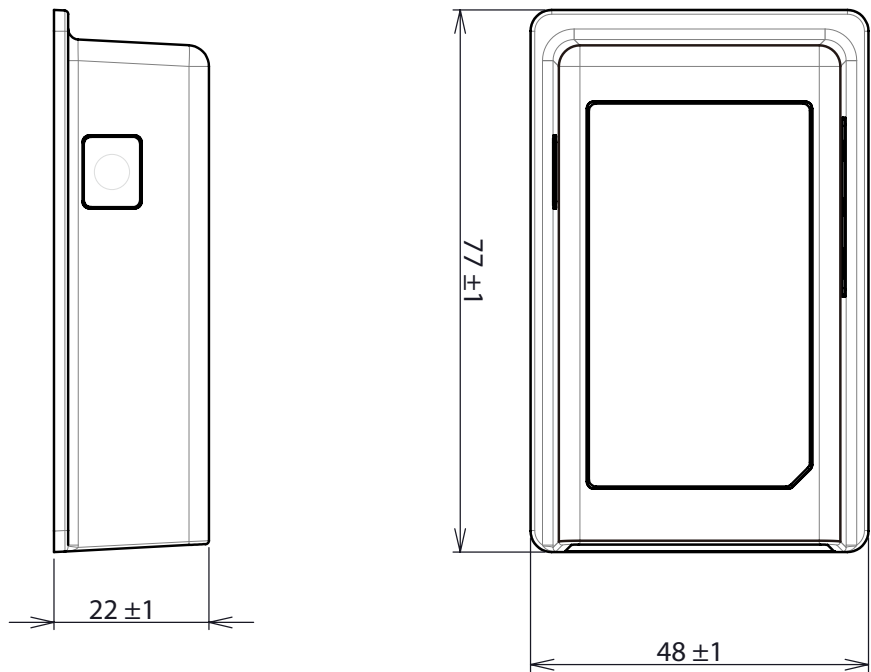


Note

- For details on AMC Manager, refer to **C. Configuration Utility** in this User's Manual or visit our website.

2-3. Dimensions

The external dimensions of BR-110AX are shown below.

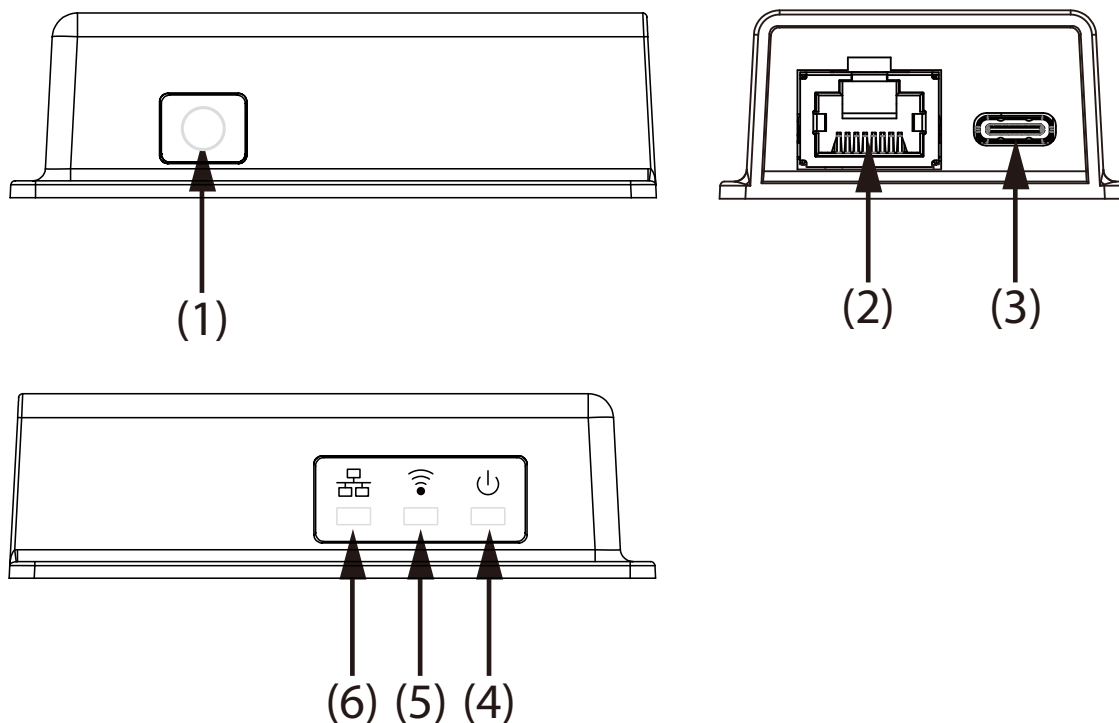


Unit : mm

Item	Specification
Dimensions	48 x 77 x 22 mm (W x D x H, excluding protrusions)
Weight	36g (excluding accessories)

2-4. Parts and Functions

The part names and functions of BR-110AX are shown below.



No.	Name	Function
(1)	Push Switch	Switches the operating mode to Configuration mode. For details, refer to 3-2-1. Displaying the BR-110AX's Web Page - Displaying the Web Page Using Configuration Mode. Initializes BR-110AX. For details, refer to 9-4-1. Initialization Using the Push Switch.
(2)	Wired LAN Port	Connect the wired LAN device that you want to use wirelessly. 10BASE-T and 100BASE-TX are supported.
(3)	USB Type-C Connector	Supplies power. This connector is used only for power input and does not support USB functions.
(4)	POWER LED	Indicates the power status. Refer to 2-4-1. LED Indications for details.
(5)	WLAN LED	Indicates the wireless connection status. Refer to 2-4-1. LED Indications for details.
(6)	LINK LED	Indicates the wired connection status. Refer to 2-4-1. LED Indications for details.

2-4-1. LED Indications

The operating status of BR-110AX can be checked using the LED indications.

The following tables show the LED patterns and their meanings.

POWER

Color	Light	Explanation
Green	ON	Power is on.
-	OFF	Power is off.

WLAN

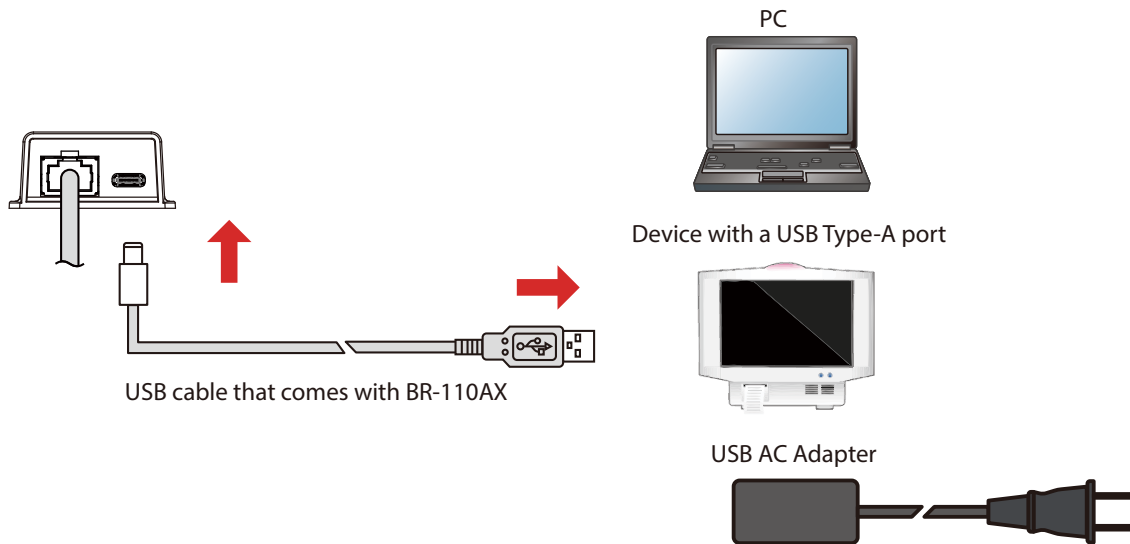
Color	Light	Explanation
Green	ON	Operating in Station mode
	Blinking (100ms)	Transmitting or receiving data in Station mode
	Blinking (1sec)	Operating in Station mode with weak signal strength
	Blinking (2sec)	Operating in Configuration mode
Orange	ON	Operating in Access Point mode
	Blinking (100ms)	Transmitting or receiving data in Access Point mode
Green/ Orange	Blinking alternately (500ms)	Operating in Station mode and attempting to connect to an Access Point
Red	Blinking (200ms)	Initialization error for wireless LAN function
		Detecting a change of wired LAN device while operating in Configuration mode
	Blinking (1sec)	Firmware update in progress
		Factory default configuration in progress
-	OFF	Wireless LAN is OFF

LINK

Color	Light	Explanation
Green	ON	Connected at 100BASE-TX
	Blinking (100ms)	Transmitting or receiving data at 100BASE-TX
Orange	ON	Connected at 10BASE-T
	Blinking (100ms)	Transmitting or receiving data at 10BASE-T
Red	Blinking (200ms)	Initialization error for wired LAN function
		Detecting a change of wired LAN device
-	OFF	Wired LAN devices are not connected.

2-5. Power Supply

BR-110AX receives power through its USB Type-C connector. The input voltage is DC5.0 V $\pm$ 5%. Power can be supplied from a USB port on a connected device, a PC, or a USB AC adapter.



- The USB Type-C connector is used only for power input. USB data communication (USB functions) is not supported.
- BR-110AX may not operate properly if the power supply is unstable. Connect it to a power source capable of supplying at least DC5.0V / 0.7A.
- Since BR-110AX temporarily consumes more than 500 mA when it is powered on, connecting it to a USB 2.0 compliant port (approximately 500 mA) may momentarily exceed the rated current. Make sure that the connected device (power source) can supply sufficient current.



- Be sure to use the USB cable that comes with BR-110AX. Using a cable other than the specified one may prevent proper operation.

3. How to Configure

3-1. Configuration Procedure

Configure the product in the following order.



- If BR-110AX has the factory default settings, a password must be configured first. For details, refer to **3-2. Initial Password Configuration**.

- 1.** Download the configuration file from the product. For details, refer to **3-3. Downloading a Configuration File**.
- 2.** Edit the downloaded configuration file. For details, refer to **3-4. Editing a Configuration File**.
- 3.** Upload the edited configuration file to BR-110AX. For details, refer to **3-5. Uploading a Configuration File**.

There are two methods for downloading and uploading a configuration file; one is to use the BR-110AX's Web page, and other one is to use AMC Manager. Select the method that best suits your operating environment.



- The configuration is performed properly if the wired LAN device has been connected to a wireless network successfully.
- A LAN cable is necessary to configure BR-110AX. Prepare one separately.

3-2. Initial Password Configuration

3-2-1. Displaying the BR-110AX's Web Page

There are two methods for displaying the Web page.

Displaying the Web Page Using Configuration Mode

Display the Web page by connecting BR-110AX directly to the PC using a LAN cable.

The Web page can be accessed even if you are not sure of the IP address of BR-110AX.

Refer to **Displaying the Web Page Using Configuration Mode**.

Displaying the Web Page by Entering an IP Address

Display the Web page by connecting the PC to a wired LAN, or a wireless LAN through an Access Point, and entering the BR-110AX's IP address to the address bar of the Web browser.

Refer to **Displaying the Web Page by Entering an IP Address**.



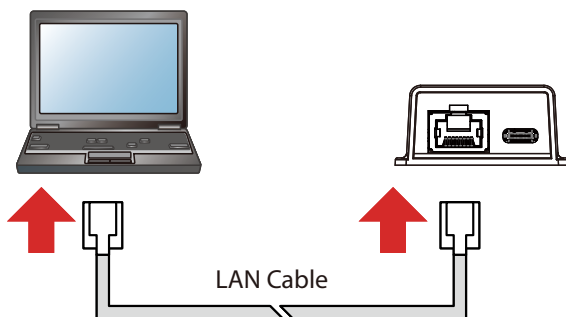
- The BR-110AX's Web page can be accessed only via HTTPS and cannot be accessed via HTTP.

TIP

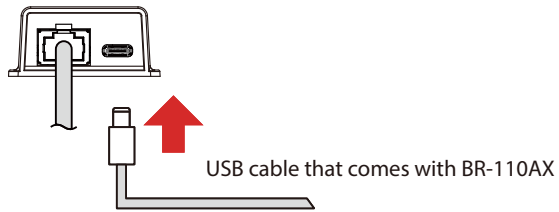
Connecting BR-110AX to a PC

1. Connect one end of LAN cable to the PC and the other end to BR-110AX.

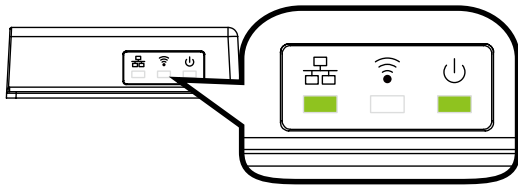
PC to use for configuration



- 2.** Connect BR-110AX to a power source using the USB cable that comes with the product.



- 3.** Check the connection status using the LEDs.
When BR-110AX has successfully connected to the PC, the LINK LED lights green or orange.



Displaying the Web Page Using Configuration Mode



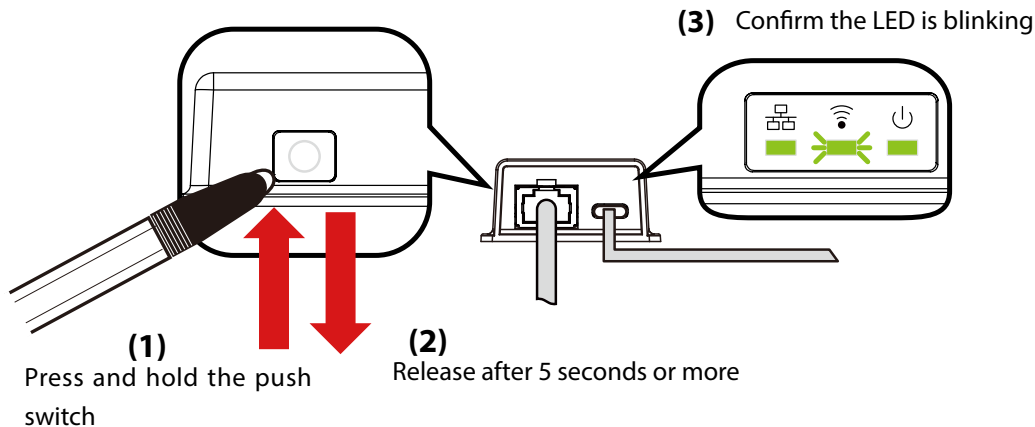
- When Configuration mode is on, the wireless LAN function of BR-110AX is disabled.
- Do not replace the connected wired LAN device while Configuration mode is on. Doing so causes an error and requires BR-110AX to be restarted.



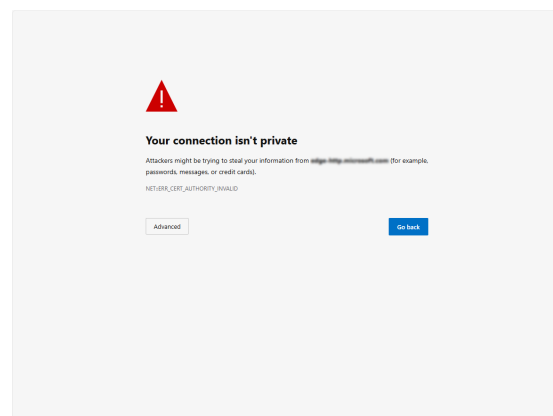
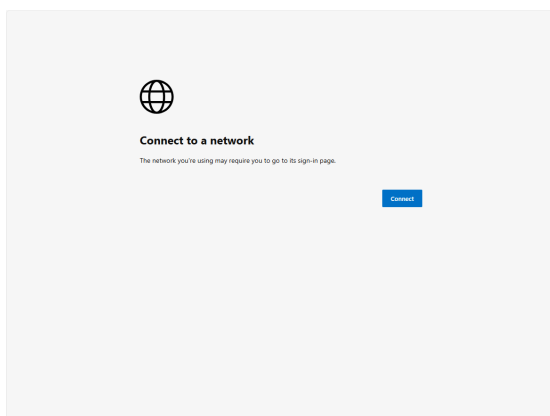
Note

- To exit Configuration mode and return to normal operation, restart BR-110AX.

1. Connect BR-110AX and the PC by following the instructions at **Connecting BR-110AX to a PC**.
2. When BR-110AX is turned on, press and hold the push switch using a pointed object, then release it after at least 5 seconds. Confirm that the WLAN LED is blinking green.
BR-110AX will start running in the Configuration mode and be ready to configure from the PC that has been connected to BR-110AX via a LAN cable.



3. Start the Web browser on the PC. The BR-110AX's Web page is displayed, then.
If the Web page is not displayed, enter "**https://silex**" in the address bar of the Web browser and press the Enter key.
If the **Connect to a network** screen appears, click **Connect**.
If a warning screen appears then, click **Advanced** and click **Continue to xxxxxx(unsafe)**.



**Note**

- The display of warning screen may differ depending on the Web browser and its version.

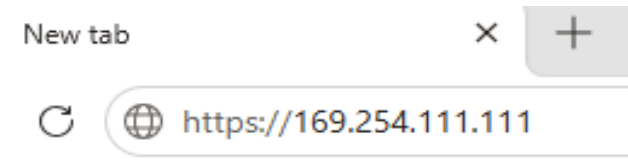
If BR-110AX has the factory default settings, the password configuration page appears. Proceed to **Password Configuration**.

Otherwise, the login dialog appears. Proceed to **Logging In**.

Displaying the Web Page by Entering an IP Address

1. Connect BR-110AX and the PC according to the instructions at **Connecting BR-110AX to a PC**.

2. Start a Web browser and enter the IP address of BR-110AX in the address bar.



TIP

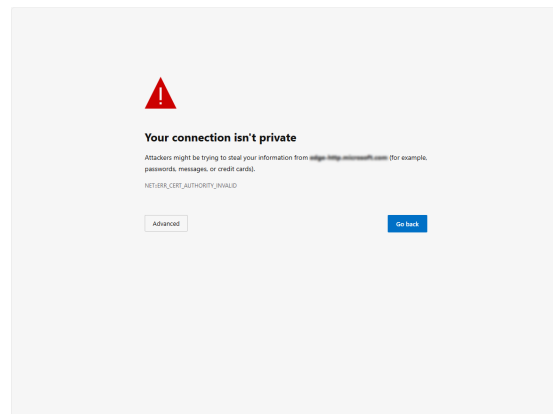
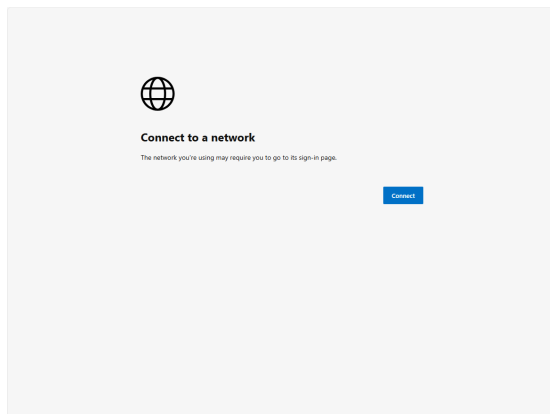
- If BR-110AX and the wired LAN device use the same IP address (for example, when the IP Intercept function is enabled and the wired LAN device obtains its IP address from a DHCP server), this method cannot be used to access the BR-110AX's Web page via the wired LAN. Refer to **Displaying the Web Page Using Configuration Mode** to display the Web page, then.



Note

- The default IP address of BR-110AX is 169.254.111.111.

3. If the **Connect to a network** screen appears, click **Connect**. If a warning screen appears then, click **Advanced** and click **Continue to xxxxxx(unsafe)**.



Note

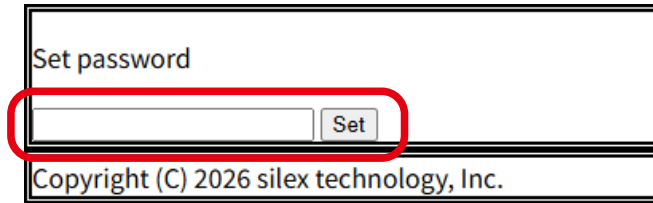
- The display of warning screen may differ depending on the Web browser and its version.

If BR-110AX has the factory default settings, the password configuration page appears. Proceed to **Password Configuration**.

Otherwise, the login dialog appears. Proceed to **Logging In**.

Password Configuration

1. The password configuration page of BR-110AX appears. Enter the password to configure for BR-110AX, and click **Set**.

**Note**

- The password needs to be set only for the initial configuration. This page is not displayed after a password has been set.
- The password must be a string of 1 to 15 characters.

2. The password is registered to BR-110AX, and BR-110AX restarts.
The restart is complete when the LINK LED turns off and then turns green again.

After BR-110AX restarts, access the BR-110AX's Web page again by referring to **Displaying the Web Page Using Configuration Mode** or **Displaying the Web Page by Entering an IP Address**.

Logging In

1. When the following dialog appears, enter "**admin**" for the **Username** and the configured password for **Password**, then click **Sign in**.

Sign in to access this site

Authorization required by <https://169.254.111.111>

Username

Password

The login procedure is now complete.

3-3. Downloading a Configuration File

The current settings of BR-110AX can be downloaded as a configuration file.

3-3-1. Downloading from the BR-110AX's Web Page

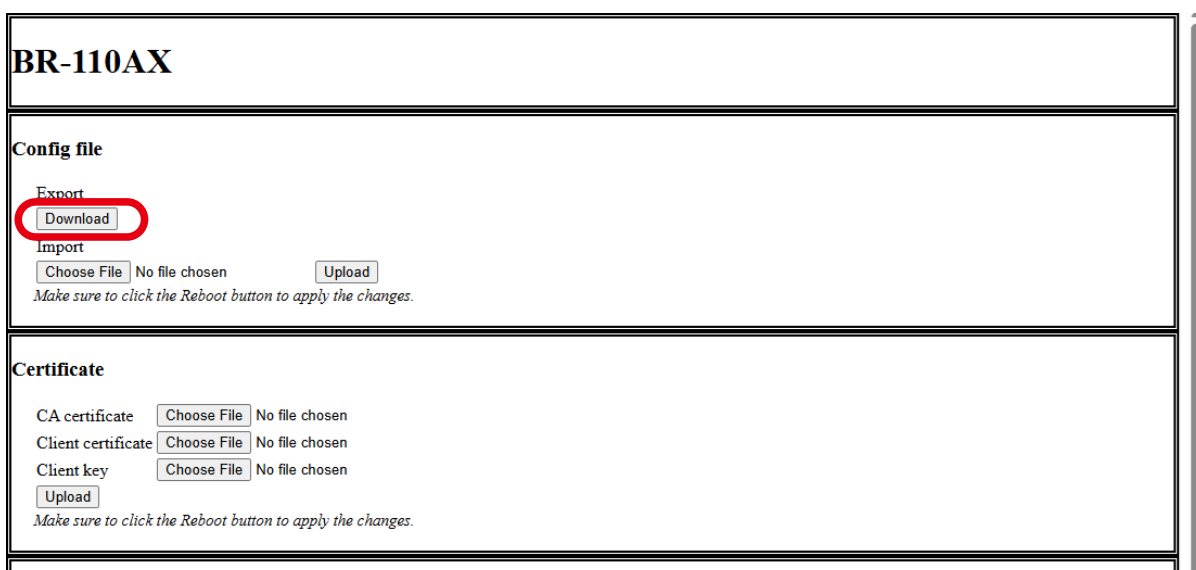
Download a configuration file from the BR-110AX's Web page.

The BR-110AX Web page can be accessed using HTTPS.



- For the default IP address of BR-110AX, refer to **A. List of All Settings**.

1. Connect BR-110AX and the PC according to the instructions at **Connecting BR-110AX to a PC**.
2. Display the BR-110AX's Web page. For details, refer to **3-2-1. Displaying the BR-110AX's Web Page**.
3. Click **Download** under **Export**.
The message for the config file (config.txt) appears.
Follow the instructions in the message.



BR-110AX

Config file

Export
Download

Import
Choose File No file chosen Upload

Make sure to click the Reboot button to apply the changes.

Certificate

CA certificate Choose File No file chosen
Client certificate Choose File No file chosen
Client key Choose File No file chosen
Upload

Make sure to click the Reboot button to apply the changes.

The download of the configuration file is now complete.

3-3-2. Downloading from AMC Manager

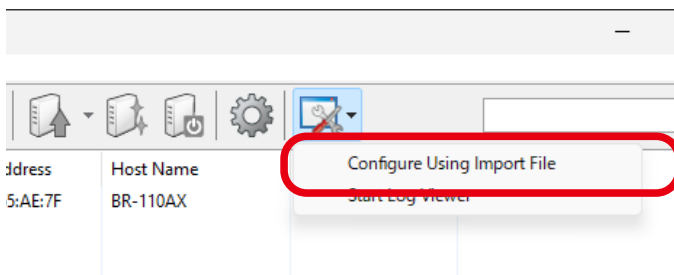
The following describes how to download a configuration file from BR-110AX using AMC Manager.



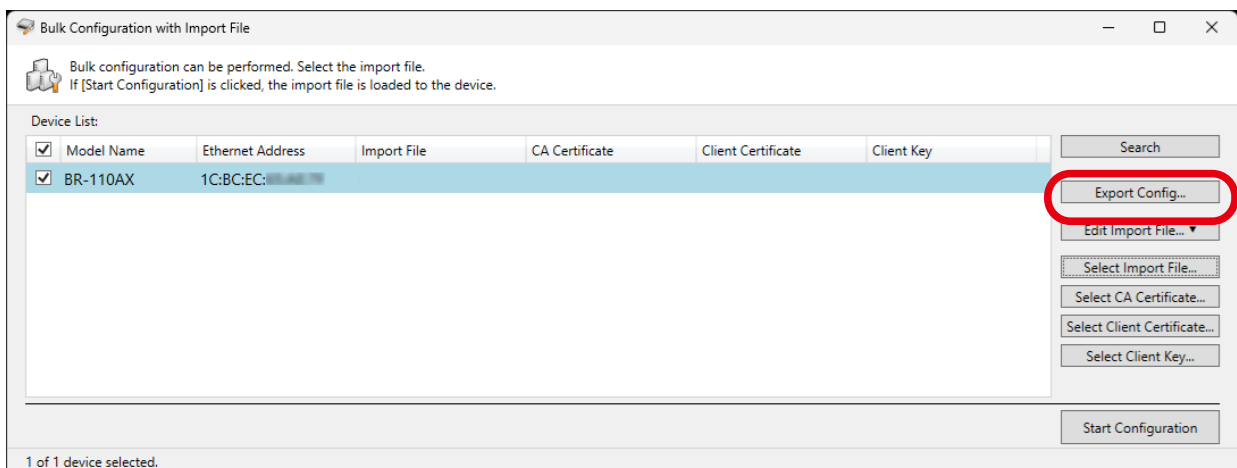
Note

- For information on how to download AMC Manager, refer to **C-1. AMC Manager**.
- The settings of BR-110AX can also be edited using AMC Manager. For details, refer to the AMC Manager® User's Manual.

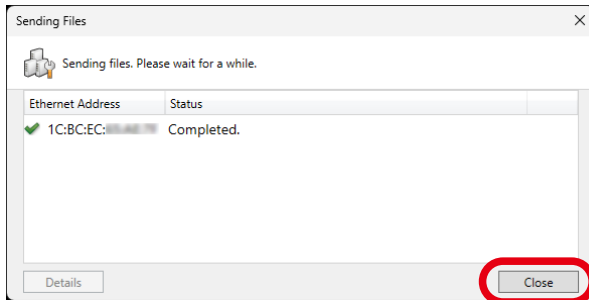
1. Start AMC Manager, click the **Start the plug-in tools** icon and select **Configure Using Import File** from the displayed menu.



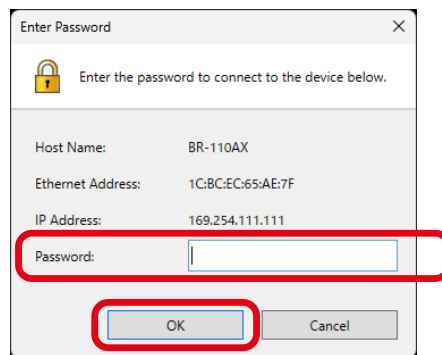
2. When the screen below appears, select the target BR-110AX unit and click **Export Config**.



- 3.** Select the destination folder to export the configuration file.
When the export is complete, click **Close**.

**Note**

- When a password is set to the device, the screen below is displayed. Enter the password of the device and click **OK**.

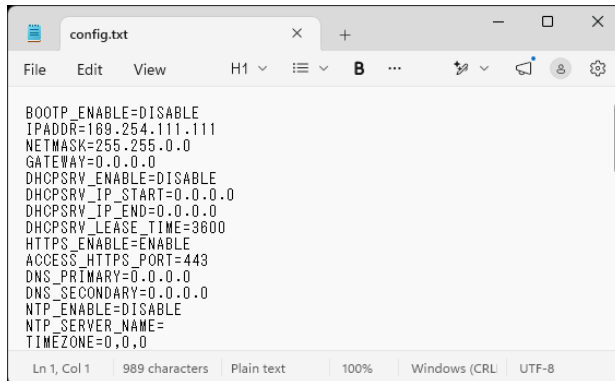


3-4. Editing a Configuration File

Edit the downloaded configuration file with a text editor.

The configuration file is a text file that consists of configuration items (keys) and setting values.

1. Open the configuration file with a text editor.



2. Edit the values of the configuration items that you want to change. The configuration items will differ depending on whether BR-110AX is used in Station mode or Access Point mode.

For Station mode

Item Name	Description	Sample Setting
SX_SREG_SX_CONNECT_STARTUP	Specify the wireless LAN operation mode to apply when BR-110AX is turned on (Station mode or Access Point mode). 2: Access Point mode / 4: Station mode * It is impossible to use 0, 1 and 3 as they are reserved.	4
WL_STA_SSID	Specify the SSID of the Access Point to connect (alphanumeric string of up to 32 characters).	Network_01
WL_STA_NETWORK_AUTH	Specify the authentication method of the Access Point to connect. 0: OPEN / 1: WPA / 2: WPA2 / 3: WPA3 / 4: WPA3 EAP 192-bit Mode / 6: WPA/WPA2 / 7: WPA2/WPA3 * It is impossible to use 5 as it is reserved.	3
WL_STA_WPA_PSK	Specify the pre-shared key (PSK) to use for Station mode.	pass_key

For Access Point Mode

Item Name	Description	Sample Setting
SX_SREG_SX_CONNECT_STARTUP	Specify the wireless LAN operation mode to apply when BR-110AX is turned on (Station mode or Access Point mode). 2: Access Point mode / 4: Station mode * It is impossible to use 0, 1 and 3 as they are reserved.	2
WL_SSID_0_0	Specify the SSID of the wireless LAN to connect (alphanumeric string of up to 32 characters).	Network_02
WL_CHANNEL_0	Specify the wireless channel to use for Access Point mode. Following values can be used: 2.4GHz: 1-13 5GHz: 36,40,44,48 W53 and W56 channels cannot be used for Access Point mode.	36
WL_AP_NETWORK_AUTH_0_0	Specify the authentication method for wireless client devices connecting to BR-110AX. 0: OPEN / 1: WPA / 2: WPA2 / 3: WPA3	3
WL_WPA_PSK_0_0	Specify the pre-shared key (PSK) to use for Access Point mode.	pass_key

**TIP**

- For security reasons, authentication information such as pre-shared keys is output with blank values.
- To upload a configuration file to BR-110AX using AMC Manager when BR-110AX has the factory default settings, the login password must be set in the configuration file.

Item Name	Description	Sample Setting
ROOT_PASSWORD	Specify the login password for BR-110AX.	passbr110

- If the IP Intercept function is enabled (**WB_IP_INTERCEPT = 1**) while BR-110AX is operating in Station Mode, the following settings are also required.
When the wired LAN device uses a static IP address, set **BOOTP_ENABLE** to **DISABLE** and configure the same IP address settings on BR-110AX as those configured on the wired LAN device. For details, refer to **6-3. Communicating with an Access Point That Supports the Proxy ARP Function**.

**Note**

- To use IEEE 802.1X for Station mode, refer to **5-1-2. Using IEEE 802.1X in Station Mode**.
- For other configuration items, refer to **A. List of All Settings**.

3. Save the edited configuration file.

**TIP**

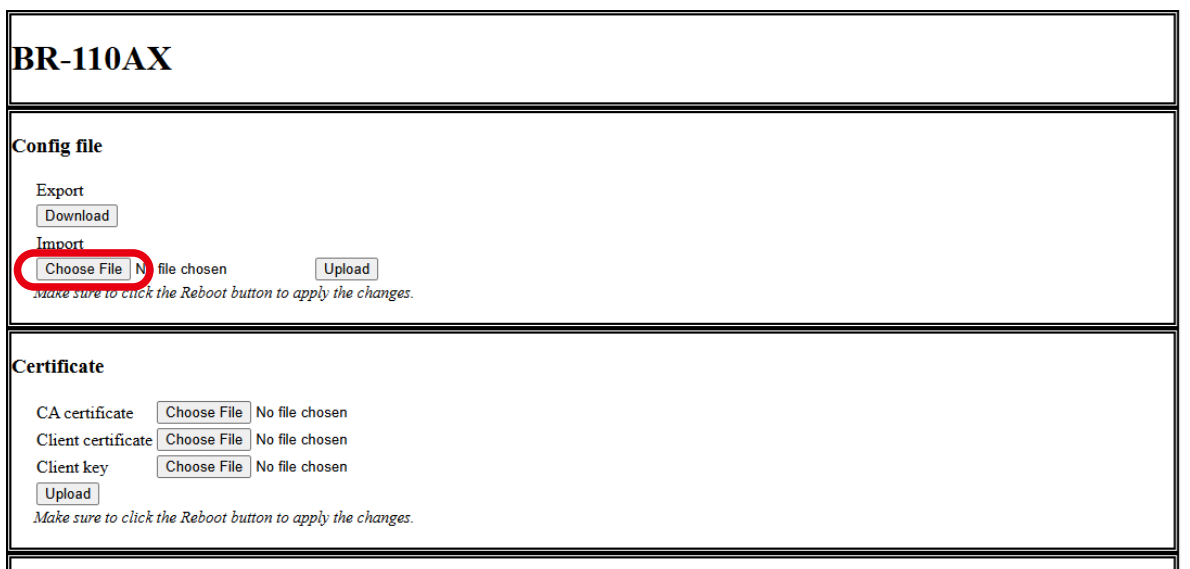
- The configuration file is not encrypted. Please handle the configuration file carefully.

3-5. Uploading a Configuration File

Upload the edited configuration file to BR-110AX. After the upload is completed, BR-110AX automatically restarts to apply the settings.

3-5-1. Uploading from the BR-110AX's Web Page

1. Display the BR-110AX's Web page. For details, refer to **3-2-1. Displaying the BR-110AX's Web Page**.
2. Click the button under **Import** in the BR-110AX's Web page.
When the file selection dialog appears, select the config file you have edited, and click **Open**.



The screenshot shows the BR-110AX web interface. The title is "BR-110AX". Below it is the "Config file" section. In this section, there are two main options: "Export" and "Import". Under "Export", there is a "Download" button. Under "Import", there is a "Choose File" button, which is circled in red, and an "Upload" button. To the right of the "Choose File" button, it says "No file chosen". Below these buttons, there is a note: "Make sure to click the Reboot button to apply the changes." Below the "Config file" section is the "Certificate" section. It contains three rows: "CA certificate", "Client certificate", and "Client key". Each row has a "Choose File" button and "No file chosen" text. There is also an "Upload" button at the bottom of the certificate section. A note at the bottom of the certificate section says: "Make sure to click the Reboot button to apply the changes."

3. Check that the specified config file is displayed and click **Upload**.

4. When the following message appears, click **Return to top pages**.

Update config success.
[Return to top pages.](#)

5. Click **Reboot** under **Reboot System**.
When the confirmation dialog appears, click **OK**.

Client certificate	Choose File	No file chosen
Client key	Choose File	No file chosen
Upload		
<i>Make sure to click the Reboot button to apply the changes.</i>		
Reboot System		
Reboot		
Log files		
System Log file	Export	Delete
Event Log file	Export	Delete
Update firmware image		
Application	Choose File	No file chosen
Upload		
Reset factory default		
Factory Reset & Reboot		

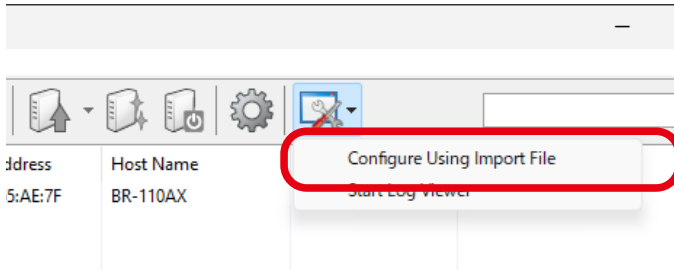
6. BR-110AX will restart.
When the following message appears, close the Web browser.

Rebooting...

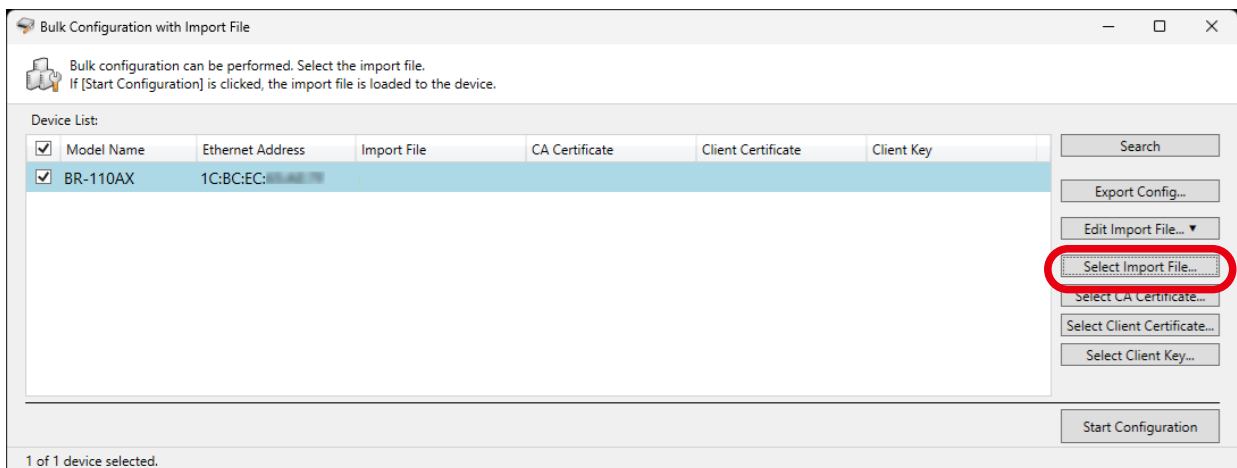
The upload of the configuration file is now complete.

3-5-2. Uploading from AMC Manager

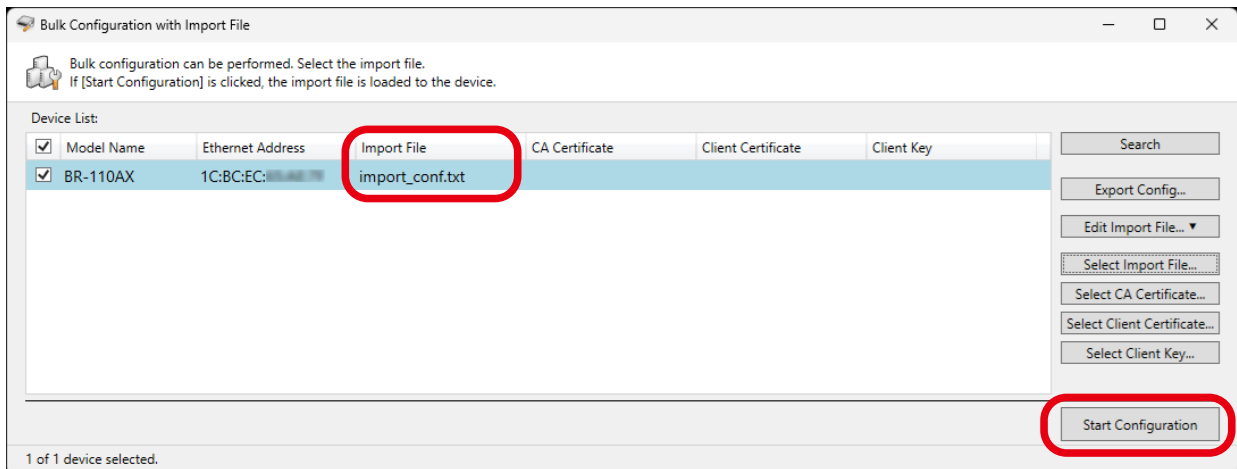
1. Start AMC Manager, click the **Start the plug-in tools** icon and select **Configure Using Import File** from the displayed menu.



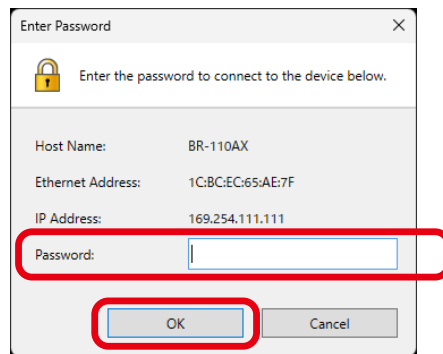
2. Select the BR-110AX unit to import the configuration to.
Click **Select Import File** and select the configuration file you have edited.



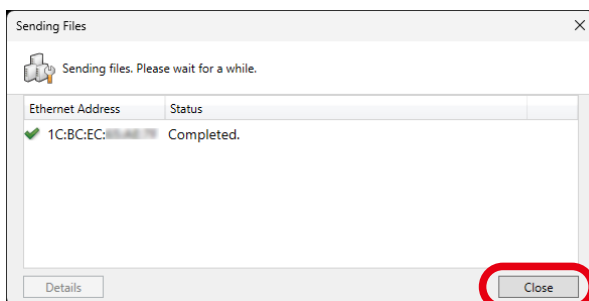
- 3.** Confirm that the name of the selected configuration file is displayed under **Import File**, and then click **Start Configuration**.



- When a password is set to the device, the screen below is displayed. Enter the password of the device and click **OK**.



- 4.** The execution results are displayed. BR-110AX automatically restarts and operates with the new settings.
Click **Close**.



The upload of the configuration file is now complete.

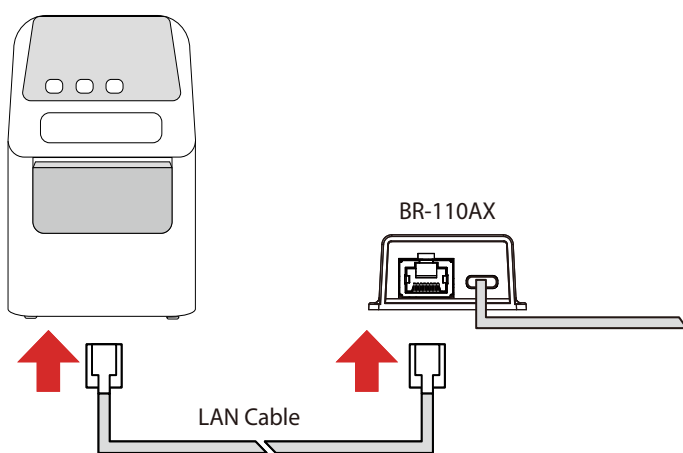
3-6. Checking the Connection

3-6-1. Checking the Connection When Operating in Station Mode

1. Connect the wired LAN device that you want to use wirelessly to BR-110AX using a LAN cable, and then turn on the device.

Also, turn on the Access Point.

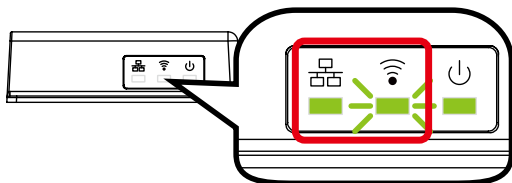
Wired LAN Device



2. Confirm that the LEDs are in the following states.

WLAN LED: ON or Blinking (Green)

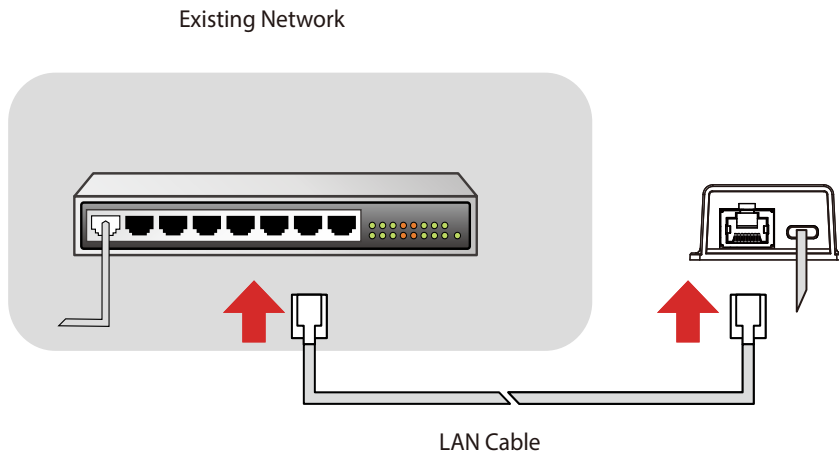
LINK LED: ON (Green or Orange)



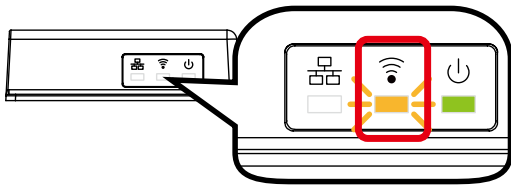
If the wired LAN device can communicate with other devices over the wireless LAN, the configuration is complete. If communication cannot be established, refer to **10-2. Troubles When Operating in Station Mode**.

3-6-2. Checking the Connection When Operating in Access Point Mode

1. Connect BR-110AX to the existing network using a LAN cable, and turn on BR-110AX and the wireless client device.



2. Confirm that the LEDs are in the following states.
WLAN LED: ON or Blinking (Orange)



If the wireless client device can communicate with other devices through BR-110AX, the configuration is complete. If communication cannot be established, refer to **10-3. Troubles When Operating in Access Point Mode**.

4. Product Installation

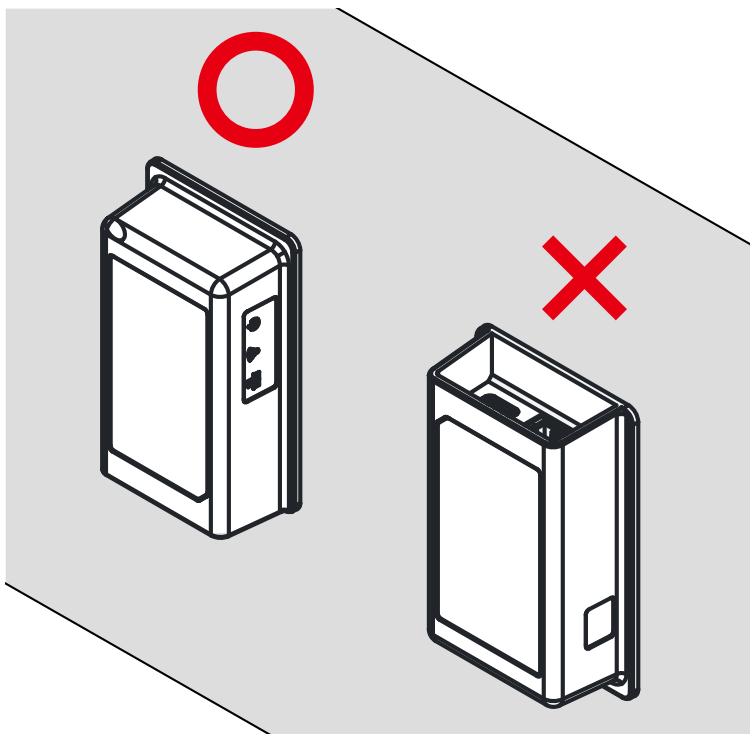
4-1. Notes on Installation

To ensure stable operation of BR-110AX, check the following points before installation.

- Install BR-110AX in a way that keeps the LEDs visible so that the LED status can be checked.
- Do not install BR-110AX near metal objects, concrete walls, or reinforced concrete structures that may block wireless signals.
- Do not install BR-110AX near devices that use the same frequency band, such as microwave ovens.



- Install BR-110AX with the connector side facing downward to maintain the IP21 dust and drip protection rating.



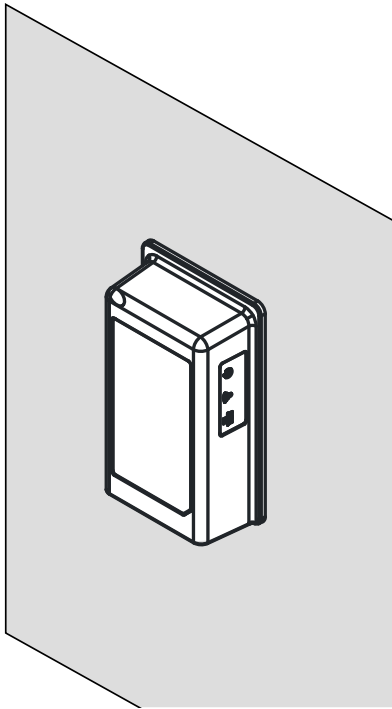
4-2. Installation Image

BR-110AX is designed to be used with a mobile cart or device by attaching them using the hook-and-loop fastener that comes with the product. Once BR-110AX is attached to a medical cart or other mobile medical equipment, they can be connected to a wireless network.

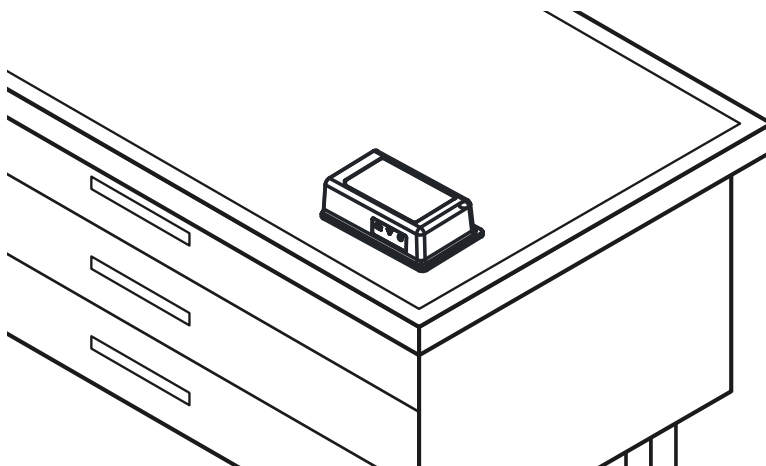


- BR-110AX can also be installed on a flat surface, however, the IP21 dust and drip protection rating cannot be maintained, then.

Attaching to a cart or device



Installing on a flat surface

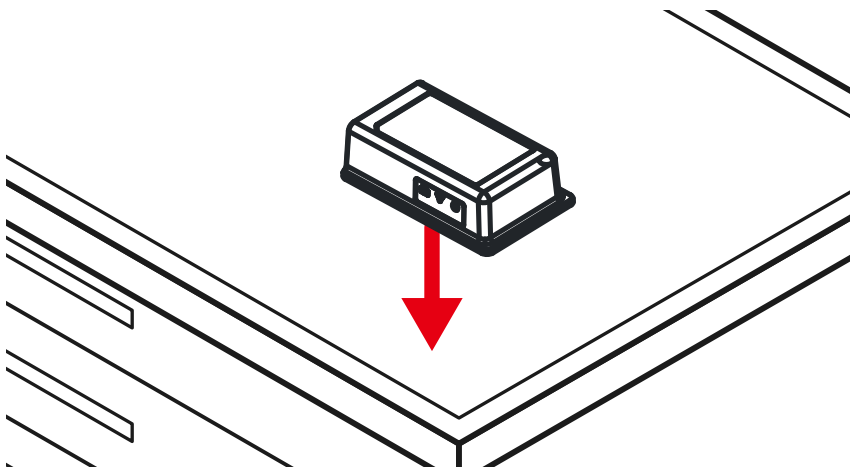


4-3. Installation on a Flat Surface

When using BR-110AX on a flat surface, place it on a desk or other location with a clear line of sight. Be sure to install BR-110AX with the side of the product label facing upward.



- When BR-110AX is installed on a flat surface, the IP21 dust and drip protection rating cannot be maintained. Do not use BR-110AX in environments exposed to dust or water droplets.
- Install BR-110AX so that the LEDs are visible.
- Secure BR-110AX to the surface of a target object using the hook-and-loop fastener that comes with BR-110AX to prevent it from falling due to cable tension. For details, refer to **4-4. Installation Using Hook-and-Loop Fastener.**



4-4. Installation Using Hook-and-Loop Fastener

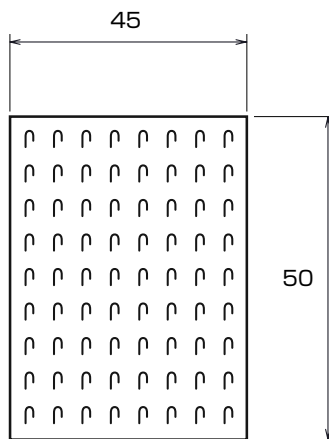
Attach BR-110AX to a mobile cart or device using the hook-and-loop fastener that comes with the product.



- Be careful about the installation orientation. To maintain the IP21 dust and drip protection rating, install BR-110AX with the connector side facing downward (toward the floor).
- Install BR-110AX where the LEDs are visible for status monitoring.

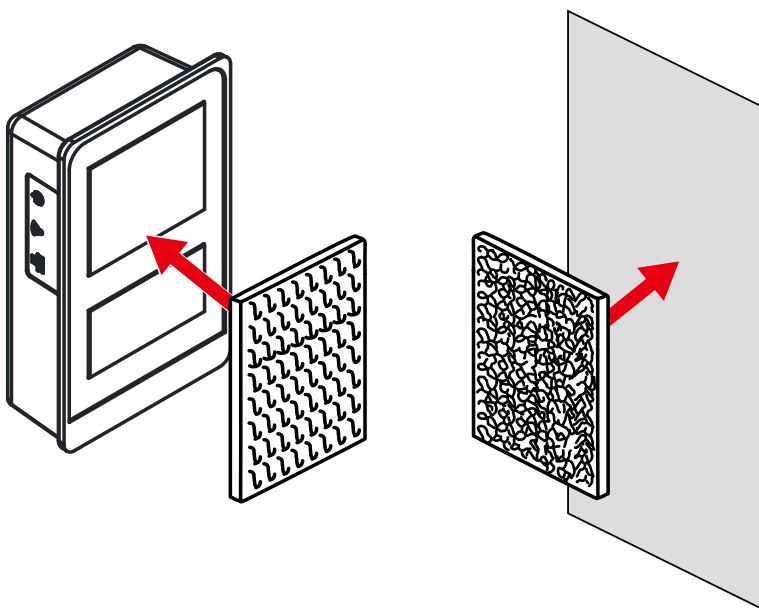


- The hook-and-loop fastener measures 50 x 45 mm.

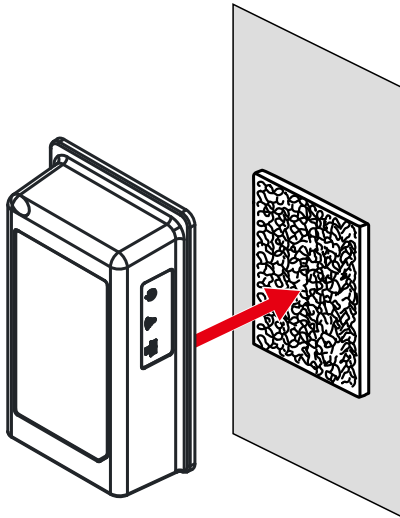


Unit : mm

1. Attach the hook side of the hook-and-loop fastener to the bottom of BR-110AX, and attach the loop side to the device or medical cart that you want to use wirelessly.



2. Attach BR-110AX to the surface of the device where the loop side of the hook-and-loop fastener has been attached.

**TIP**

- To prevent BR-110AX from falling due to its own weight or the weight of cables, make sure that it is securely fastened after installation.

5. Security Enhancement

5-1. Enhancing Security with IEEE 802.1X

BR-110AX supports IEEE 802.1X authentication. By using an authentication server (RADIUS server), only authorized devices can connect to the wireless network.

BR-110AX supports EAP-TLS, EAP-TTLS, and EAP-PEAP for authentication methods.

Enterprise authentication supports TLS 1.2 and TLS 1.3.



Note

- BR-110AX supports FreeRADIUS as the authentication server.



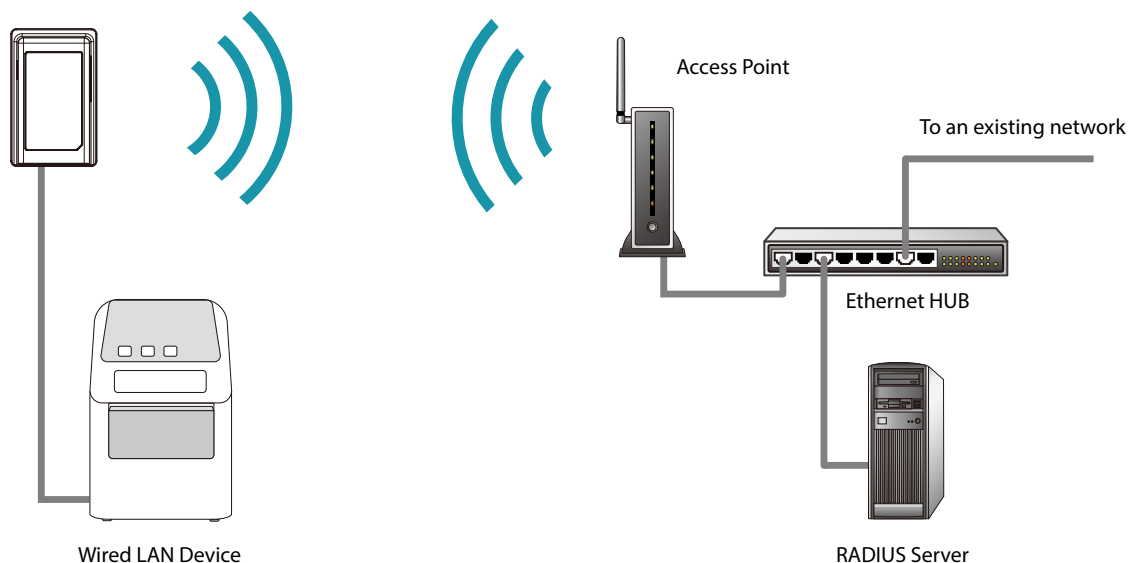
TIP

- IEEE 802.1X authentication is supported only when BR-110AX is operating in Station mode.
- Certificate files of up to 8,192 bytes are supported.

5-1-1. Network Configuration

The below image shows the network configuration when IEEE 802.1X authentication is used.

The configuration consists of BR-110AX (Station), an Access Point (Authenticator), and an authentication server.



TIP

- IEEE 802.1X authentication cannot be used when BR-110AX is operating in Access Point mode.

5-1-2. Using IEEE 802.1X in Station Mode

The following explains how to use IEEE 802.1X authentication when BR-110AX is operating in Station mode. Configure the settings by editing the configuration file.

1. Download the configuration file from BR-110AX. For details, refer to **3-3. Downloading a Configuration File**.
2. Configure the following settings in the configuration file.

Item Name	Description	Sample Setting
WL_STA_NETWORK_AUTH	Network authentication method for Station mode. To use Enterprise authentication, specify one of the following values: 1: WPA / 2: WPA2 / 3: WPA3 / 4: WPA3 EAP 192-bit Mode / 6: WPA/WPA2 / 7: WPA2/WPA3.	3
WL_STA_EAP_TYPE	EAP authentication method Specify 2: PEAP / 3: TLS / or 4: TTLS. * It is impossible to use 1 as it is reserved.	4
WL_STA_EAP_USER_NAME	User name for EAP authentication	user01
WL_STA_EAP_PASSWORD	Password for EAP authentication	password_ eap_01
WL_STA_EAP_INNER_METHOD	EAP inner authentication method Specify 0: MSCHAPv2 / 1: PAP / 2: MSCHAP / or 3: CHAP (TTLS only).	0
WL_STA_EAP_ANONYMOUS	Anonymous identity used for EAP authentication Specify as required.	anonymous

3. On the Web page, click the file selection buttons under **Certificate** to select the CA certificate file, client certificate file, and client private key file as necessary. After making the selections, click **Upload**.

BR-110AX

Config file

Export

Download

Import

Choose File

No file chosen

Upload

Make sure to click the Reboot button to apply the changes.

Certificate

CA certificate

Choose File

No file chosen

Client certificate

Choose File

No file chosen

Client key

Choose File

No file chosen

Upload

Make sure to click the Reboot button to apply the changes.

- 4.** Upload the configuration file to BR-110AX. For details, refer to **3-5. Uploading a Configuration File**.

5-2. Access Control Using the Filter Function

BR-110AX supports the device connection filter function.

If this function is used, communications from the wired connection can be filtered based on MAC addresses or vendor codes.

For addresses to allow connection, up to 4 addresses can be registered using MAC addresses or vendor codes. When the device connection filter function is enabled, communications from unregistered MAC addresses are not forwarded to the wireless LAN, and access to BR-110AX is also blocked.

1. Download the configuration file from BR-110AX. For details, refer to **3-3. Downloading a Configuration File**.
2. Enable the device connection filter function in the configuration file and register up to 4 MAC addresses or vendor codes for devices to allow connection.

Item Name	Description	Sample Setting
WB_SINGLE_SWITCH	Enable/Disable the device connection filter function. When enabled, communication from devices other than registered MAC addresses is blocked.	ENABLE
WB_ETHER_ADDR_FILTER0	MAC address or vendor code of an allowed device (Entry 1).	00:11:22:33:44:55
WB_ETHER_ADDR_FILTER1	MAC address or vendor code of an allowed device (Entry 2).	00:11:22:33:44:66
WB_ETHER_ADDR_FILTER2	MAC address or vendor code of an allowed device (Entry 3).	00:11:22:33:44:67
WB_ETHER_ADDR_FILTER3	MAC address or vendor code of an allowed device (Entry 4).	00:11:22:33:44:68



- Be sure to register the MAC address or vendor code of an allowed device. If the device connection filter function is enabled and no MAC address or vendor code is registered, communications from the wired LAN will no longer be possible.

3. Upload the edited configuration file to BR-110AX. For details, refer to **3-5. Uploading a Configuration File**.

5-3. Hiding the Access Point SSID

When BR-110AX is used in Access Point mode, security can be enhanced by hiding the SSID to prevent third parties from detecting it.

1. Download the configuration file from BR-110AX. For details, refer to **3-3. Downloading a Configuration File**.
2. Enable the SSID hiding (Stealth SSID) function in the configuration file.

Item Name	Description	Sample Setting
WL_SSID_STEALTH_0_0	Enable/Disable the SSID hiding (Stealth SSID) function for Access Point mode.	ENABLE

3. Upload the edited configuration file to BR-110AX. For details, refer to **3-5. Uploading a Configuration File**.



Note

- When the SSID is hidden, the SSID must be configured manually on the connecting device.

5-4. Changing the Login Password

The following describes how to change the login password for the BR-110AX's Web page.



- Be sure not to forget the changed password. If the password is forgotten, BR-110AX must be initialized. For details on the initialization, refer to **9-4. Factory Default Configuration**.

5-4-1. Changing the Password Using the Configuration File

- 1.** Download the configuration file from BR-110AX. For details, refer to **3-3. Downloading a Configuration File**.
- 2.** Configure the following setting in the configuration file.

Item Name	Description	Sample Setting
ROOT_PASSWORD	Specify the password used to log in to BR-110AX.	passbr110



Note

- The current password is not exported to the configuration file and is output as a blank value.

- 3.** Upload the edited configuration file to BR-110AX. For details, refer to **3-5. Uploading a Configuration File**.

5-4-2. Changing the Password from the Web Page

1. Start a Web browser, enter the following URL in the address bar, and press the Enter key.

`https://IP address of BR-110AX/password.shtml`

2. The password setting page appears. Enter a new password and click **Set**.

Set password

Copyright (C) 2026 silex technology, Inc.

3. BR-110AX restarts. The new password becomes effective after the restart is complete.

6.

Communication Performance Settings

6-1. Optimizing Roaming

BR-110AX supports roaming, which enables seamless switching between Access Points while operating in Station mode. The following functions optimize roaming and help maintain stable communication while moving.

Function	Standard	Description
Fast Transition	IEEE 802.11r	Reduces the time required to switch between Access Points.



- If the DTIM interval of the connected Access Point is 196 or greater, disconnection from the Access Point may not be detected.

1. Download the configuration file from BR-110AX. For details, refer to **3-3. Downloading a Configuration File**.
2. Enable the roaming function in the configuration file.

Item Name	Description	Sample Setting
WL_STA_FT_ENABLE	Enable/Disable the Fast Roaming (IEEE 802.11r Fast Transition) function.	ENABLE
WL_STA_SCAN_PERIOD	Specify the scan interval for roaming (0 to 60 seconds).	20
WL_STA_SCAN_RSSI	Specify the RSSI threshold for starting roaming scans (value range: 20 to 95). If this value is set to 70, scanning starts when the RSSI drops below -70 dBm.	70

3. Upload the edited configuration file to BR-110AX. For details, refer to **3-5. Uploading a Configuration File**.

6-2. Giving Priority to Voice and Video Traffic

BR-110AX supports the WMM (Wi-Fi Multimedia) function.

This is a function to add access category information to packets and send them to a wireless LAN according to the specified access category information.

With this function, audio and video data packets are assigned to the access categories with a higher priority, so that the priority of communication can be given to them.

1. Download the configuration file from BR-110AX. For details, refer to **3-3. Downloading a Configuration File**.
2. Configure the default access category in the configuration file.

Item Name	Description	Sample Setting
WL_WME_DEF_AC	Specify the WMM access category to apply to packets for which no priority is set. 0:NONE / 1:AC_BE / 2:AC_BK / 3:AC_VI / 4:AC_VO	4

3. Upload the edited configuration file to BR-110AX. For details, refer to **3-5. Uploading a Configuration File**.



Note

- If a priority is assigned to a packet received from the wired LAN, that priority is used.

6-3. Communicating with an Access Point That Supports the Proxy ARP Function

When there is an Access Point that supports the Proxy ARP function in the network environment, BR-110AX may not be able to communicate with wired LAN devices. This is because, when communicating with such an Access Point, one set of MAC address and IP address is needed, however, BR-110AX allows both the wired LAN device and BR-110AX itself to use different IP addresses for the same MAC address.

By enabling the IP Intercept function, BR-110AX can use the IP address of the device connected to the wired LAN as its own IP address. This allows BR-110AX to be accessed even through an Access Point that supports the Proxy ARP function.



- If the IP Intercept function is enabled, HTTPS and AMC Manager communications of the wireless LAN will not be forwarded to devices on the wired LAN.
- When the IP Intercept function is enabled, BR-110AX uses the same IP address as the wired device. Then, communication between the wired device and BR-110AX will become unavailable. Also, access to the BR-110AX's Web page via the wired LAN will be disabled, however, it will be enabled if BR-110AX is turned to Configuration mode.
- If the wired LAN device is not configured to obtain an IP address from a DHCP server, set **BOOTP_ENABLE** to **DISABLE** and configure the same IP address settings on BR-110AX. If the IP address settings of BR-110AX differ from those of the wired LAN device, communication with the wired LAN device from the wireless LAN is not possible.

1. Download the configuration file from BR-110AX. For details, refer to **3-3. Downloading a Configuration File**.

2. Enable the IP Intercept function in the configuration file.

Item Name	Description	Sample Setting
WB_IP_INTERCEPT	Enable/Disable the IP Intercept function. 0:DISABLE / 1:ENABLE	1

3. Upload the edited configuration file to BR-110AX. For details, refer to **3-5. Uploading a Configuration File**.

7.

Network Functions

7-1. DHCP Server Function

BR-110AX is equipped with a DHCP server function. If there is no network device with a DHCP server function in your network environment, the DHCP server function of BR-110AX can be used to easily assign IP addresses to PCs, tablets, and network devices on the network.

1. Download the configuration file from BR-110AX. For details, refer to **3-3. Downloading a Configuration File**.
2. Enable the DHCP server function in the configuration file.
Then configure the start address, end address, and lease time.

Item Name	Description	Sample Setting
DHCPSRV_ENABLE	Enable/Disable the simple DHCP server function.	ENABLE
DHCPSRV_IP_START	Starting address of the IP address range to assign. The address must belong to the same subnet as the static IP address of BR-110AX.	192.168.0.10
DHCPSRV_IP_END	Ending address of the IP address range to assign. Specify an address that comes after the starting address.	192.168.0.18
DHCPSRV_LEASE_TIME	Lease time for assigned IP addresses (60 to 86400 seconds).	3600

3. Upload the edited configuration file to BR-110AX. For details, refer to **3-5. Uploading a Configuration File**.



TIP

- It is possible to assign IP addresses to a maximum of 9 devices using the DHCP server function of BR-110AX.
- Operation is not guaranteed if another DHCP server or relay agent exists in the same subnet as BR-110AX.

7-2. Time Synchronization

BR-110AX supports the SNTP (Simple Network Time Protocol) client function and can obtain time information from an NTP server.

When time synchronization is successful, BR-110AX retrieves the time every hour. When time synchronization fails, BR-110AX retries at regular intervals (up to 165 seconds).



TIP

- If the time is not synchronized, the recorded date and time of the logs may differ from the actual date and time of events, making it difficult to compare them with logs from the Access Point or connected devices.

1. Download the configuration file from BR-110AX. For details, refer to **3-3. Downloading a Configuration File**.

2. Enable the SNTP function and set the target NTP server in the configuration file.

Item Name	Description	Sample Setting
NTP_ENABLE	Enable/Disable the SNTP client function.	ENABLE
NTP_SERVER_NAME	NTP server to use for time synchronization String of 3 to 253 characters	ntp.nict.jp
TIMEZONE	Time zone for BR-110AX (hour,min,sign) hour: 0 to 24 (hours) min: 0 to 59 (minutes) sign: Indicates the difference from UTC 0: Behind UTC (-) 1: Ahead of UTC (+)	9,0,1



TIP

- To specify an NTP server by domain name, the following conditions must be met:
 - Symbols other than "." and "-" are not used.
 - "." and "-" are not used at the beginning or end of the domain name.
 - Each label separated by "." has 63 characters or fewer.
 - No label begins or ends with "-".
 - The domain name is not composed only of numbers.



Note

- To specify an NTP server by domain name, DNS server settings are required. Up to 2 DNS servers can be configured on BR-110AX.

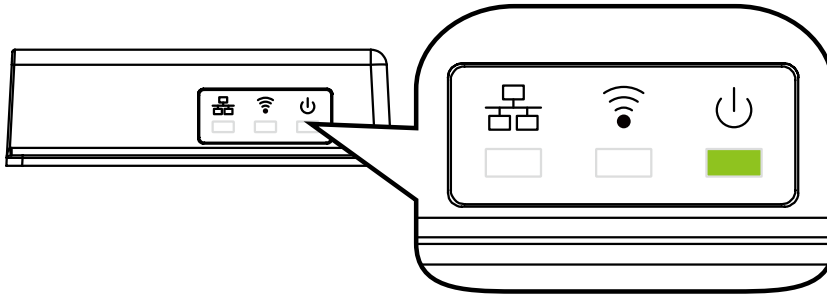
Item Name	Description	Sample Setting
DNS_PRIMARY	Specify the IP address of the primary DNS server to use for BR-110AX.	192.168.0.70
DNS_SECONDARY	Specify the IP address of the secondary DNS server to use for BR-110AX.	192.168.0.71

3. Upload the edited configuration file to BR-110AX. For details, refer to **3-5. Uploading a Configuration File**.

8. Operating Status Check

8-1. Checking the Operating Status Using LEDs

The power status and wireless communication status of BR-110AX can be checked using the LED indicators. For details on LED patterns and their meanings, refer to **2-4-1. LED Indications**.



Note

- Although it is not necessary to always monitor the LEDs, it is recommended to install BR-110AX with the LEDs visible so that the status can be checked in case of an emergency. For details on installation, refer to **4-1. Notes on Installation**.

8-2. Downloading the Logs

BR-110AX can save operating events as logs.

The saved logs can be downloaded from and deleted through the BR-110AX's Web page.

There are two types of log.

System Log

Power-on status, operating status, etc. of BR-110AX are saved as a log file.

The log file can be downloaded from BR-110AX.

In case of a network trouble, you can check the operating status by referring the system logs.

Event Log

When a new event such as power-on/wireless connection/disconnection occurs, it is saved as a log file.

The log file can be downloaded from BR-110AX.

In case of a network trouble, you can check the operating status by referring the event logs.

8-2-1. Downloading the Logs

1. Display the BR-110AX's Web page. For details, refer to **3-2-1. Displaying the BR-110AX's Web Page.**

2. Click **Export** in the page below.

- To download a system log, click **Export** next to **System Log File**.
- To download an event log, click **Export** next to **Event Log File**.

The screenshot displays the BR-110AX web interface. At the top, there are fields for 'Client certificate' and 'Client key', each with a 'Choose File' button and the text 'No file chosen'. Below these is an 'Upload' button and a note: 'Make sure to click the Reboot button to apply the changes.' The 'Reboot System' section contains a 'Reboot' button. The 'Log files' section lists 'System Log file' and 'Event Log file'. For each, there is an 'Export' button (circled in red) and a 'Delete' button. The 'Update firmware image' section at the bottom has an 'Application' field with a 'Choose File' button and 'No file chosen' text, and an 'Upload' button.

- 3.** When a message regarding the log file appears, follow the instructions in the message.

The log download is now complete.

8-2-2. Deleting the Logs

1. Display the BR-110AX's Web page. For details, refer to **3-2-1. Displaying the BR-110AX's Web Page**.
2. Click **Delete** in the page below.
 - To delete a system log, click **Delete** at **System Log File**.
 - To delete an event log, click **Delete** at **Event Log File**.

The screenshot shows the BR-110AX web interface. At the top, there are fields for 'Client certificate' and 'Client key', each with a 'Choose File' button and 'No file chosen' text, followed by an 'Upload' button. Below these is a note: 'Make sure to click the Reboot button to apply the changes.' The next section is 'Reboot System' with a 'Reboot' button. The 'Log files' section contains two rows: 'System Log file' and 'Event Log file'. Each row has an 'Export' button and a 'Delete' button. The 'Delete' button for the 'System Log file' is circled in red. The bottom section is 'Update firmware image' with an 'Application' field, a 'Choose File' button, 'No file chosen' text, and an 'Upload' button.

3. A confirmation dialog is displayed. Click **OK**.
4. The selected log is deleted and BR-110AX restarts.

Success to erase log file. Rebooting...

The log deletion is now complete.

9. Maintenance

9-1. Cleaning BR-110AX

BR-110AX is intended for use in medical environments.

BR-110AX complies with IP21 and has chemical resistance. If the surface of BR-110AX becomes dirty, clean it using one of the following disinfectants.

Disinfectant	Concentration
Ethanol	70% (30% water)
Propanol	60% (40% water)
Sodium Hypochlorite	1% (available chlorine)
Peracetic Acid	0.2%
Hydrogen Peroxide	2%



- Do not use any chemicals other than those listed above. Doing so may cause deterioration of the enclosure or a product malfunction.
- Prevent disinfectants or moisture from entering the connectors when cleaning BR-110AX. Failure to do so may result in product failure.
- When cleaning the label area, gently wipe it using a cloth moistened with disinfectant.
- Do not spray disinfectant directly onto the label area, leave it wet, or rub it forcefully. Doing so may cause the label printing to become faint or discolored.

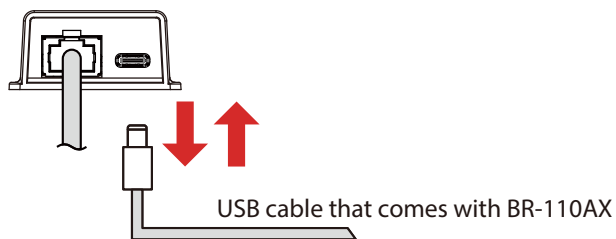
1. Turn off BR-110AX.
2. Wipe the surface of BR-110AX with a soft cloth moistened with one of the disinfectants listed above.
3. Turn on BR-110AX after it has dried completely.

9-2. Restarting BR-110AX

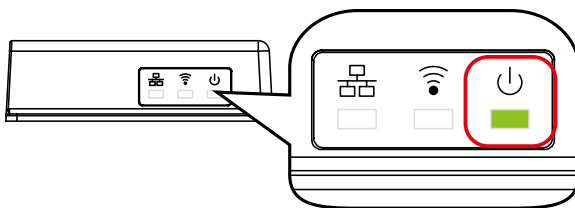
There are two methods to restart BR-110AX; one is to use the USB cable that comes with the product, and the other is to use the BR-110AX's Web page.

9-2-1. How to Restart by Disconnecting a USB Cable

1. Disconnect the USB cable from BR-110AX, and then reconnect it.



2. The restart is complete when the POWER LED lights green.



9-2-2. How to Restart from the Web Page

BR-110AX can be restarted from the BR-110AX's Web page.

The available restart methods are immediate restart, restart at fixed intervals, and restart at a specified date and time.

Restarting BR-110AX Immediately

1. Display the BR-110AX's Web page. For details, refer to **3-2-1. Displaying the BR-110AX's Web Page**.

2. Click **Reboot**.

The screenshot displays the web interface of the BR-110AX. At the top, there are fields for 'Client certificate' and 'Client key', each with a 'Choose File' button and the text 'No file chosen'. Below these is an 'Upload' button and a note: 'Make sure to click the Reboot button to apply the changes.' The main section is titled 'Reboot System' and contains a 'Reboot' button, which is circled in red. Below this is the 'Log files' section, showing 'System Log file' and 'Event Log file' with 'Export' and 'Delete' buttons. The 'Update firmware image' section has an 'Application' field with a 'Choose File' button and an 'Upload' button. The 'Reset factory default' section contains a 'Factory Reset & Reboot' button. At the bottom, there is a footer with 'Version 1.0.0', 'MAC Address 1c:bc:ec:88:aa:77', and 'Copyright (C) 2026 silex technology, Inc.'

3. BR-110AX restarts.

Restarting BR-110AX at Fixed Intervals

BR-110AX can be configured to restart automatically at specified intervals based on its operating time.

1. Download the configuration file from BR-110AX. For details, refer to **3-3. Downloading a Configuration File**.
2. Change the following items in the configuration file.

Item Name	Description	Sample Setting
REBOOT_TYPE	Specify the scheduled reboot method. Set 1 to reboot at fixed intervals.	1
REBOOT_INTERVAL	Specify the reboot interval (60 to 10080 minutes).	90



- The time set for **REBOOT_INTERVAL** is intended as a reference value and does not guarantee an exact reboot interval. The actual reboot interval may vary by several percent.

3. Upload the edited configuration file to BR-110AX. For details, refer to **3-5. Uploading a Configuration File**.

Restarting BR-110AX at a Specified Date and Time

BR-110AX can be configured to restart automatically at a specified date and time every day, every week, or every month.

1. Download the configuration file from BR-110AX. For details, refer to **3-3. Downloading a Configuration File**.
2. Change the following items in the configuration file.

Item Name	Description	Sample Setting
REBOOT_TYPE	Specify the scheduled reboot method. Set 2 to reboot at a specified date and time.	2
REBOOT_SCHEDULE_TYPE	Specify the schedule for automatic reboot. 0: Disable / 1: Daily / 2: Weekly / 3: Monthly	2
REBOOT_DAY	Specify the day or day of the week for automatic reboot. The value range differs depending on the REBOOT_SCHEDULE_TYPE setting. When REBOOT_SCHEDULE_TYPE is 0 or 1: 0 to 31 When REBOOT_SCHEDULE_TYPE is 2: 1 to 7 (1: Sunday / 2: Monday / 3: Tuesday / 4: Wednesday / 5: Thursday / 6: Friday / 7: Saturday) When REBOOT_SCHEDULE_TYPE is 3: 1 to 31	2
REBOOT_TIME	Specify the time at which automatic reboot is performed. Enter a four-digit value in 24-hour format (hhmm). Example: 9:30 AM > 0930 9:30 PM > 2130	0930



Note

- If the specified date does not exist in the month, BR-110AX restarts on the last day of that month.

3. Upload the edited configuration file to BR-110AX. For details, refer to **3-5. Uploading a Configuration File**.

9-3. Updating Firmware

To update BR-110AX to the latest firmware version, download the firmware by following the procedure below. For the update procedure, refer to the instruction manual included with the firmware.

9-3-1. Downloading the Firmware

The latest firmware file can be downloaded from our website. See the instructions below to download it.

1. Access our website below.

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

2. Go to the support section and download the firmware file.

9-4. Factory Default Configuration

This chapter explains how to reset BR-110AX to the factory default settings.



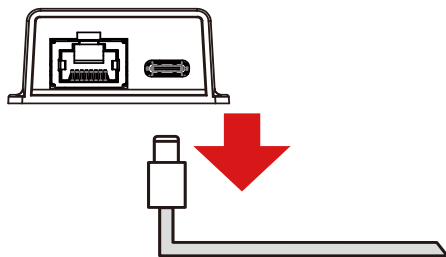
- All settings except the country code are deleted and restored to the factory default settings after initialization. Download any required settings as a configuration file before initialization.



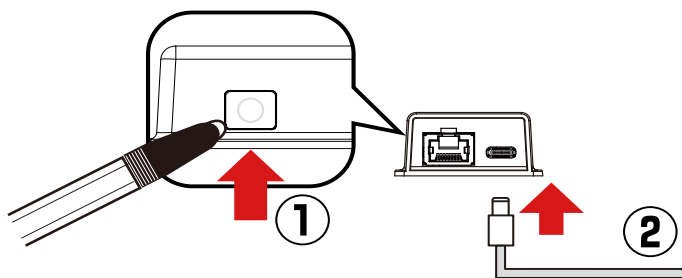
- After initialization, reconfigure the password by referring to **3-2. Initial Password Configuration**, and then reconfigure BR-110AX by referring to **3-5. Uploading a Configuration File**.

9-4-1. Initialization Using the Push Switch

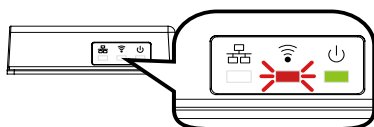
1. Unplug a USB cable from BR-110AX.



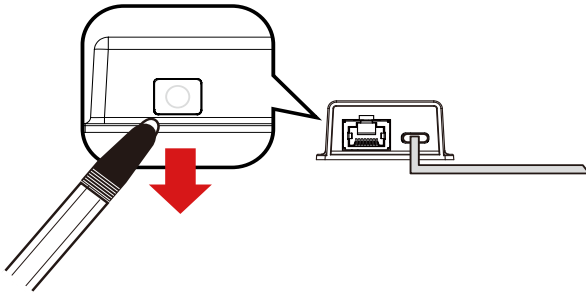
2. While pressing and holding the push switch with a pointed object, reconnect the USB cable to BR-110AX. Continue holding it.



- As long as the push switch is held down, the WLAN LED will keep blinking red.



- 3.** Confirm that at least 5 seconds have elapsed, and then release the push switch. The settings are reset to the factory defaults, and BR-110AX restarts.



9-4-2. Initialization from the Web Page

1. Display the BR-110AX's Web page. For details, refer to **3-2-1. Displaying the BR-110AX's Web Page.**

2. Click **Factory Reset & Reboot.**

The screenshot displays the web interface of the BR-110AX device. At the top, there are sections for 'Client certificate' and 'Client key', each with a 'Choose File' button and a 'No file chosen' status. Below these is an 'Upload' button and a note: 'Make sure to click the Reboot button to apply the changes.' The main content area is divided into several sections: 'Reboot System' with a 'Reboot' button; 'Log files' with 'Export' and 'Delete' buttons for 'System Log file' and 'Event Log file'; 'Update firmware image' with an 'Application' field, 'Choose File' button, and 'Upload' button; and 'Reset factory default' where the 'Factory Reset & Reboot' button is circled in red. At the bottom, there is a footer section containing 'Version 1.0.0', 'MAC Address 1c:bc:ec:8f:aa:7f', and 'Copyright (C) 2026 silix technology, Inc.'

3. BR-110AX is initialized and restarts.

10. Troubleshooting

10-1. Problems During the Setup

I don't know the IP Address of BR-110AX.

Solution	Use the unified device management utility "AMC Manager". AMC Manager can search for BR-110AX units connected to a network. For details on AMC Manager, refer to C-1-1. What is AMC Manager? .
----------	---

An error occurs when accessing the Web page of BR-110AX

If an error occurs when accessing the Web page, you need to check your PC and Web browser settings.

BR-110AX may not be in the same network segment (environment without a router) as your PC.	
Solution	During the initial configuration, place BR-110AX and PC in the same network segment. If BR-110AX can be connected directly to the PC using a LAN cable, connect them directly and access the BR-110AX's Web page in Configuration mode. For details on how to access the Web page in Configuration mode, refer to 3-2-1. Displaying the BR-110AX's Web Page - Displaying the Web Page Using Configuration Mode . If this is not possible, reset BR-110AX to the factory default settings and check again. For details on how to reset BR-110AX to the factory default settings, refer to 9-4. Factory Default Configuration .

If your Web browser is configured to use a proxy server, access to the local network might be blocked.	
Solution	Disable use of the proxy server temporarily or enable access to the local network on your Web browser.

How should I determine the way to assign an IP address to BR-110AX?

There are two ways to assign an IP address to BR-110AX; one is to get an IP address automatically from a DHCP server and the other is to assign an IP address manually. Choose the way to assign an IP address according to your environment.

When there is a DHCP server in the network environment:	
Solution	An IP address can automatically be configured to BR-110AX using the DHCP server. As BR-110AX is set by default to Get IP address automatically, BR-110AX will obtain an IP address appropriate to your network environment from the DHCP server just by powering up BR-110AX.

When there is no DHCP server in the network environment, or when you do not prefer getting an IP address from DHCP server:

Solution

Please assign an IP address manually. Keep the following points in mind regarding the IP address to assign to BR-110AX.

- Assign an IP address unique in the network.
- Assign an IP address that has the same address class as the PC that will use BR-110AX.
e.g. When an IP address of the PC is "192.168.0.xx", assign an address such as "192.168.0.100" that is not used by other network devices.

(Tips about the IP address)

- An IP address is a unique number for identifying network devices. An IP address is indicated with four numbers divided by a period (.), for example "192.168.0.1". The integer from 0 to 255 is used for each number.
- An IP address is, depending on the number assigned, categorized to 3 classes below.
- Numbers making up the IP address are either network numbers indicating network, or host numbers indicating each network device; each number indicates the different meaning based on the IP address class. Each class is categorized as the following diagram which is indicating a network number as n, and a host number as u.
- An IP address with the same network number must be assigned to the network devices in the same network segment.
- There is an address range in the IP address called the private address that could be used freely. In the LAN environment not directly connected to the Internet, an IP address is assigned within the range of the private address.

First 1 digits in IP address	Class	Definition of IP address n: network number u: host number	Size of the network to be used	Private address
0 to 127	A	n.u.u.u	Large network	10.0.0.0 to 10.255.255.255
128 to 191	B	n.n.u.u	Mid-size network	172.16.0.0 to 172.31.255.255
192 to 223	C	n.n.n.u	Small network	192.168.0.0 to 192.168.255.255

10-2. Troubles When Operating in Station Mode

The Link LED is blinking red rapidly.

The bridge function may have been disabled by the protection function because the wired LAN device was replaced while BR-110AX was operating.

Solution	Restart BR-110AX. If BR-110AX is operating in Configuration mode then, WLAN LED is also blinking red rapidly.
----------	--

I cannot communicate with the wired LAN device connected to BR-110AX.

The BR-110AX or wired LAN device may not be operating correctly.

Solution	Please check that the wired LAN device is properly powered on.
----------	--

The connection may be restricted by the MAC address filtering on BR-110AX.

Solution	Check that the connected wired LAN device is not restricted by the device connection filter function.
----------	---

Multiple wired LAN devices may have been connected to BR-110AX using an Ethernet Hub.

Solution	Connect only one wired LAN device to BR-110AX. It is impossible to connect multiple wired LAN devices.
----------	---

The Access Point may be filtering the devices by MAC addresses.

Solution	Check that the Access Point does not filter the MAC address of wired LAN device. The MAC address of BR-110AX can be found on the product label or on the Web page.
----------	---

The Access Point may have a function equivalent to Proxy ARP and it is turned on.

Solution	Check the Proxy ARP function setting of the Access Point. If the function is enabled, change the setting. Otherwise, enable the IP Intercept function of BR-110AX so that such setting does not need to be changed. For details, refer to 6-3. Communicating with an Access Point That Supports the Proxy ARP Function.
----------	--

10-3. Troubles When Operating in Access Point Mode

I cannot connect to BR-110AX wirelessly.

Please check the operation status and configuration of BR-110AX.

The wireless LAN setting may differ between BR-110AX and the connected wireless client device.	
Solution	Connect a LAN cable to BR-110AX and check the wireless LAN settings.

The wireless client device may be connected to a different Access Point that has the same SSID.	
Solution	Set a different SSID between BR-110AX and the Access Point that the wireless client device is unintentionally connected. Or, set the transmission strength lower for that Access Point to shorten the wireless coverage.

Connection is interrupted and disconnected.

BR-110AX may be installed at a location subject to weaker radio wave signals.	
Solution	Reconsider the installation environment and operating conditions to avoid placing BR-110AX too far from the wireless client device or having objects that block wireless signals between them.

Communication speed is too slow.

BR-110AX supports only a 20MHz channel bandwidth.	
Solution	Use BR-110AX in an environment where 20 MHz bandwidth communication is sufficient.

The connected wireless client device may not support the latest wireless standard.	
Solution	Use the wireless client device that supports IEEE 802.11ax.

The group key update interval varies.

The group key update interval is intended as a reference value and does not guarantee an exact interval. The actual group key update interval may vary by several percent.	
Solution	This variation is not a malfunction. Group keys continue to be updated normally, and there is no impact on security.

A. List of All Settings

This chapter describes the settings that can be configured in the configuration file of BR-110AX.

Each setting is explained with the following information:

Item / Item name in configuration file / Details / Range / Default Value

**Note**

- For details on obtaining, editing, and importing a configuration file, refer to **3. How to Configure**.
- Sample configurations are provided for some features. Refer to **A-1-1. Sample Settings for Scheduled Reboot**, **A-2-1. Sample Wireless Settings**, and **A-3-1. Sample SNTP Settings**.

A-1. Product Configuration

Item	DHCP Client Setting
Item name in config file	BOOTP_ENABLE
Details	Specify whether BR-110AX obtains its IP address automatically from a DHCP server.
Range	DISABLE / ENABLE
Default Value	ENABLE

Item	IP Address
Item name in config file	IPADDR
Details	Set the IP address of BR-110AX.
Range	0.0.0.0 to 255.255.255.255
Default Value	169.254.111.111

Item	Subnet Mask
Item name in config file	NETMASK
Details	Set the subnet mask of BR-110AX.
Range	0.0.0.0 to 255.255.255.255
Default Value	255.255.0.0

Item	Default Gateway
Item name in config file	GATEWAY
Details	Specify the default gateway IP address for BR-110AX.
Range	0.0.0.0 to 255.255.255.255
Default Value	0.0.0.0

Item	DHCP Server Setting
Item name in config file	DHCP_SRV_ENABLE
Details	Specify whether the DHCP server function of BR-110AX is enabled or disabled.
Range	DISABLE / ENABLE
Default Value	DISABLE

Item	DHCP Server Start Address
Item name in config file	DHCP_SRV_IP_START
Details	Specify the start address of the IP address range used by the DHCP server function.
Range	0.0.0.0 to 255.255.255.255
Default Value	0.0.0.0

Item	DHCP Server End Address
Item name in config file	DHCP_SRV_IP_END
Details	Specify the end address of the IP address range used by the DHCP server function.
Range	0.0.0.0 to 255.255.255.255
Default Value	0.0.0.0

Item	DHCP Server Lease Time
Item name in config file	DHCPSRV_LEASE_TIME
Details	Specify the lease time for assigned IP addresses (seconds).
Range	60 to 86400
Default Value	3600

Item	Enable/Disable WebUI
Item name in config file	HTTPS_ENABLE
Details	Specify whether access to the BR-110AX's Web page (HTTPS) is enabled or disabled.
Range	DISABLE / ENABLE
Default Value	ENABLE

Item	HTTPS Port Number
Item name in config file	ACCESS_HTTPS_PORT
Details	Specify the port number to use for access to the BR-110AX's Web page (HTTPS).
Range	1 to 65535 * It is impossible to set 60000.
Default Value	443

Item	Scheduled Reboot
Item name in config file	REBOOT_TYPE
Details	Specify the scheduled reboot method (Disable, Interval, or Schedule).
Range	0: DISABLE 1: INTERVAL 2: SCHEDULE
Default Value	0

Item	Scheduled Reboot Interval (Minutes)
Item name in config file	REBOOT_INTERVAL
Details	Specify the interval at which BR-110AX reboots when the interval reboot is selected (minutes).
Range	If REBOOT_TYPE is set to 0 or 2, set 0 to 10080. If REBOOT_TYPE is set to 1, set 60 to 10080.
Default Value	0

Item	Scheduled Reboot Type
Item name in config file	REBOOT_SCHEDULE_TYPE
Details	Specify the schedule type for scheduled reboot (Disable, Daily, Weekly, or Monthly).
Range	0: DISABLE 1: DAILY 2: WEEKLY 3: MONTHLY
Default Value	0

Item	Scheduled Reboot Date/Day of Week
Item name in config file	REBOOT_DAY
Details	Specify the day or day of the week on which a scheduled reboot is performed.
Range	If REBOOT_SCHEDULE_TYPE is 0 or 1, set 0 to 31. If REBOOT_SCHEDULE_TYPE is 2, set 1:Sunday, 2:Monday, 3:Tuesday, 4:Wednesday, 5:Thursday, 6:Friday, 7:Saturday. If REBOOT_SCHEDULE_TYPE is 3, set 1 to 31.
Default Value	0

Item	Scheduled Reboot Time
Item name in config file	REBOOT_TIME
Details	Specify the time at which a scheduled reboot is performed.
Range	Set the time in hhmm format. hh: 0 to 23 mm: 0 to 59
Default Value	0000

Item	Country Code
Item name in config file	WL_REGCODE
Details	This is the country or region (country code) where BR-110AX is used. * This item is provided for reference only and cannot be changed.
Range	CA/DE/JP *The supported countries/regions are listed below. CA: United States, Canada DE: Europe, United Kingdom JP: Japan
Default Value	The value differs depending on the country or region of use.

Item	IP Intercept Mode
Item name in config file	WB_IP_INTERCEPT
Details	Specify whether the IP Intercept function is enabled or disabled.
Range	0: DISABLE 1: ENABLE
Default Value	1

Item	Password
Item name in config file	ROOT_PASSWORD
Details	Specify the login password for BR-110AX.
Range	1 to 15 characters
Default Value	(None)

A-1-1. Sample Settings for Scheduled Reboot

Rebooting at specified intervals

Item Name	Sample Setting
REBOOT_TYPE	1
REBOOT_INTERVAL	120

Rebooting daily at 6:00 AM

Item Name	Sample Setting
REBOOT_TYPE	2
REBOOT_SCHEDULE_TYPE	1
REBOOT_DAY	0
REBOOT_TIME	0600

A-2. Wireless LAN Configuration

Item	SSID (for Station mode)
Item name in config file	WL_STA_SSID
Details	Specify the SSID of the Access Point to connect when BR-110AX is operating in Station mode.
Range	A string of up to 32 characters
Default Value	(None)

Item	WPA Authentication Method (for Station mode)
Item name in config file	WL_STA_NETWORK_AUTH
Details	Specify the network authentication method to use when BR-110AX is operating in Station mode.
Range	0: OPEN / 1: WPA / 2: WPA2 / 3: WPA3 / 4: WPA3 EAP 192-bit Mode / 6: WPA/WPA2 / 7: WPA2/WPA3 * It is impossible to use 5 since it is reserved.
Default Value	0 (OPEN)

Item	Fast Roaming
Item name in config file	WL_STA_FT_ENABLE
Details	Specify whether the Fast Roaming (IEEE 802.11r) function is enabled or disabled when BR-110AX is operating in Station mode.
Range	DISABLE / ENABLE
Default Value	DISABLE

Item	Pre-shared Key (for Station mode)
Item name in config file	WL_STA_WPA_PSK
Details	Specify the WPA pre-shared key (passphrase) to use when BR-110AX is operating in Station mode.
Range	String of 8 to 63 bytes, or a 64-character hexadecimal value (WPA/WPA2 only)
Default Value	(None)

Item	EAP Authentication Method
Item name in config file	WL_STA_EAP_TYPE
Details	Specify the EAP authentication method to use for IEEE 802.1X authentication.
Range	0: NONE / 2: PEAP / 3: TLS / 4: TTLS * It is impossible to use 1 since it is reserved.
Default Value	0

Item	EAP Passphrase / EAP Private Key Password
Item name in config file	WL_STA_EAP_PASSWORD
Details	The meaning of this value differs depending on the EAP authentication method. When the EAP authentication method is 3, it is used as the password for the private key of the client certificate. When the EAP authentication method is 2 or 4, it is used as the password for EAP authentication.
Range	String of 1 to 64 characters
Default Value	(None)

Item	EAP User Name
Item name in config file	WL_STA_EAP_USER_NAME
Details	Specify the user name to use for EAP authentication.
Range	EAP user name of 1 to 64 characters
Default Value	(None)

Item	EAP Inner Authentication Method
Item name in config file	WL_STA_EAP_INNER_METHOD
Details	Specify the EAP inner authentication method.
Range	0: MSCHAPv2 / 1: PAP / 2: MSCHAP / 3: CHAP
Default Value	0

Item	EAP Anonymous Identity
Item name in config file	WL_STA_EAP_ANONYMOUS
Details	Specify the anonymous identity to use for EAP authentication.
Range	String of 1 to 64 characters
Default Value	(None)

Item	Power Saving Mode
Item name in config file	WL_STA_PS_MODE
Details	Specify whether the power-saving function is enabled or disabled when BR-110AX is operating in Station mode.
Range	DISABLE / ENABLE
Default Value	ENABLE

Item	Roaming Scan Interval
Item name in config file	WL_STA_SCAN_PERIOD
Details	Specify the scan interval to use for roaming (seconds).
Range	0 to 60
Default Value	20

Item	Roaming Scan RSSI Threshold
Item name in config file	WL_STA_SCAN_RSSI
Details	Specify the RSSI threshold that triggers roaming scans. The higher the value, the more frequently roaming is performed, however, the frequent roaming may cause unstable communication. For example, if this value is set to 70, scanning starts when the RSSI falls below -70 dBm.
Range	20 to 95
Default Value	70

Item	Default Access Category
Item name in config file	WL_WME_DEF_AC
Details	Specify the WMM access category to apply for packets with no priority settings.
Range	0: NONE 1: AC_BE 2: AC_BK 3: AC_VI 4: AC_VO
Default Value	0

Item	Connected Device Address
Item name in config file	WB_ETHER_ADDR
Details	Specify the MAC address of the wired LAN device to bridge.
Range	MAC address However, the following addresses cannot be used: - MAC address of BR-110AX - Broadcast address - Multicast address - Locally administered address (whose U/L bit, the second bit of the first octet, is set to 1) If 00:00:00:00:00:00 is specified, a bridge target device will automatically be detected.
Default Value	00:00:00:00:00:00

Item	Wireless Channel
Item name in config file	WL_CHANNEL_0
Details	Specify the channel to use when BR-110AX is operating in Access Point mode.
Range	2.4GHz : 1 to 13 5GHz : 36,40,44,48
Default Value	6

Item	SSID (for Access Point mode)
Item name in config file	WL_SSID_0_0
Details	Specify the SSID to use when BR-110AX is operating in Access Point mode.
Range	String of up to 32 characters
Default Value	(None)

Item	Stealth SSID
Item name in config file	WL_SSID_STEALTH_0_0
Details	Specify whether SSID hiding (Stealth SSID) is enabled or disabled when BR-110AX is operating in Access Point mode.
Range	DISABLE / ENABLE
Default Value	DISABLE

Item	WPA Authentication Method (for Access Point mode)
Item name in config file	WL_AP_NETWORK_AUTH_0_0
Details	Specify the network authentication method to use when BR-110AX is operating in Access Point mode.
Range	0 to 3 0: OPEN 1: WPA 2: WPA2 3: WPA3
Default Value	0

Item	Pre-shared Key (for Access Point mode)
Item name in config file	WL_WPA_PSK_0_0
Details	Specify the WPA pre-shared key to use when BR-110AX is operating in Access Point mode.
Range	String of 8 to 63 bytes, or a 64-character hexadecimal value
Default Value	(None)

Item	Device Connection Filter
Item name in config file	WB_SINGLE_SWITCH
Details	Specify whether the device connection filter function is enabled or disabled.
Range	DISABLE / ENABLE
Default Value	DISABLE

Item	Allowed Address 1
Item name in config file	WB_ETHER_ADDR_FILTER0
Details	Specify the MAC address or vendor code of a device to allow connection (entry 1).
Range	MAC address or vendor code. If the lower three bytes of the MAC address are all 0, it will be treated as a vendor code.
Default Value	(None)

Item	Allowed Address 2
Item name in config file	WB_ETHER_ADDR_FILTER1
Details	Specify the MAC address or vendor code of a device to allow connection (entry 2).
Range	MAC address or vendor code. If the lower three bytes of the MAC address are all 0, it will be treated as a vendor code.
Default Value	(None)

Item	Allowed Address 3
Item name in config file	WB_ETHER_ADDR_FILTER2
Details	Specify the MAC address or vendor code of a device to allow connection (entry 3).
Range	MAC address or vendor code. If the lower three bytes of the MAC address are all 0, it will be treated as a vendor code.
Default Value	(None)

Item	Allowed Address 4
Item name in config file	WB_ETHER_ADDR_FILTER3
Details	Specify the MAC address or vendor code of a device to allow connection (entry 4).
Range	MAC address or vendor code. If the lower three bytes of the MAC address are all 0, it will be treated as a vendor code.
Default Value	(None)

Item	Wireless Operation Mode When BR-110AX is Powered On
Item name in config file	SX_SREG_SX_CONNECT_STARTUP
Details	Specify the wireless operation mode to use when BR-110AX is powered on (Station mode / Access Point mode).
Range	2 / 4 2: Access Point mode 4: Station mode * It is impossible to use 0, 1, 3 as they are reserved.
Default Value	4

A-2-1. Sample Wireless Settings

When using EAP-TLS with WPA3 EAP 192-bit Mode

Item Name	Sample Setting
SX_SREG_SX_CONNECT_STARTUP	4
WL_STA_SSID	Network_01
WL_STA_NETWORK_AUTH	4
WL_STA_EAP_TYPE	3
WL_STA_EAP_USER_NAME	user01
WL_STA_EAP_PASSWORD	key_pass01

* CA certificate file, client certificate file, and client private key file are required.

When using EAP-PEAP with WPA3-Enterprise

Item Name	Sample Setting
SX_SREG_SX_CONNECT_STARTUP	4
WL_STA_SSID	Network_01
WL_STA_NETWORK_AUTH	3
WL_STA_EAP_TYPE	2
WL_STA_EAP_USER_NAME	user02
WL_STA_EAP_PASSWORD	pass02
WL_STA_EAP_INNER_METHOD	0
WL_STA_EAP_ANONYMOUS	eap_string

* Certificate files are not required.



Note

- To use certificate files for IEEE 802.1X authentication, upload the required files by following the instructions at **5-1-2. Using IEEE 802.1X in Station Mode.**

A-3. Application Configuration

Item	IP Address of Primary DNS Server
Item name in config file	DNS_PRIMARY
Details	Specify the IP address of the primary DNS server to use for BR-110AX.
Range	0.0.0.0 to 255.255.255.255
Default Value	0.0.0.0

Item	IP Address of Secondary DNS Server
Item name in config file	DNS_SECONDARY
Details	Specify the IP address of the secondary DNS server to use for BR-110AX.
Range	0.0.0.0 to 255.255.255.255
Default Value	0.0.0.0

Item	SNTP Server Setting
Item name in config file	NTP_SERVER_NAME
Details	Specify the NTP server to use for time synchronization.
Range	String of 3 to 253 characters
Default Value	(None)

Item	SNTP Client Setting
Item name in config file	NTP_ENABLE
Details	Specify whether the SNTP client function is enabled or disabled.
Range	DISABLE / ENABLE
Default Value	DISABLE

Item	Time Zone
Item name in config file	TIMEZONE
Details	Specify the time zone for BR-110AX in the format of "hour,min,sign".
Range	hour : 0 to 24 (hours) min : 0 to 59 (minutes) sign : Indicates the time difference from UTC. 0 : Behind UTC (-) 1 : Ahead of UTC (+)
Default Value	0,0,0

Item	AMC Manager
Item name in config file	ACCESS_SMP
Details	Specify whether access from AMC Manager is enabled or disabled.
Range	DISABLE / ENABLE
Default Value	ENABLE

A-3-1. Sample SNTP Settings

When enabling the SNTP function and setting the time zone to Japan standard time (GMT+9)

Item Name	Sample Setting
NTP_ENABLE	ENABLE
NTP_SERVER_NAME	ntp.server01.jp
TIMEZONE	9,0,1

B. Specifications

B-1. Hardware Specifications

Wired Network Interface	10BASE-T/100BASE-TX (Auto Negotiation): 1 port Auto MDI/MDIX
Push Switch	1
LED	POWER LED (Green) WLAN LED (Green/Red/Orange) LINK LED (Green/Red/Orange)
Supported Devices	Devices equipped with an RJ-45 LAN port
Maximum Number of Connectable Devices	1
Power Supply	USB Type-C connector Operating voltage: DC5.0V±5%
Operating environment	Temperature: 0°C to +40°C
	Humidity: 20% to 90% RH (non-condensing)
Storage environment	Temperature: -20°C to +70°C
	Humidity: 10% to 93% RH (non-condensing)
Dimensions	Approx. 48mm x 77mm x 22mm
Weight	Approx. 36g
EMI	VCCI Class B
Radio Certification	FCC
Dust and Drip Protection	IP21
Chemical Resistance	Ethanol 70% (30% water) Propanol 60% (40% water) Sodium Hypochlorite 1% (available chlorine) Peracetic Acid 0.2% Hydrogen Peroxide 2%
Vibration Resistance	IEC60068-2-6 IEC60068-2-64
Shock Resistance	IEC60068-2-27

Wireless network interface

IEEE 802.11a	Frequency	5GHz			
	Channel	W52	36, 40, 44, 48		
		W53	52, 56, 60, 64		
		W56	(US/CA) 100, 104, 108, 112, 116, 132, 136, 140, 144 (EU/UK) 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140		
		W58	149, 153, 157, 161, 165		
IEEE 802.11b	Frequency	2.4GHz			
	Channel	(US/CA) 1 to 11 (EU/UK) 1 to 13			
IEEE 802.11g	Frequency	2.4GHz			
	Channel	(US/CA) 1 to 11 (EU/UK) 1 to 13			
IEEE 802.11n	Frequency	2.4GHz/5GHz			
	Channel	2.4GHz	(US/CA) 1 to 11		
			(EU/UK) 1 to 13		
		5GHz	W52	36, 40, 44, 48	
			W53	52, 56, 60, 64	
			W56	(US/CA) 100, 104, 108, 112, 116, 132, 136, 140, 144 (EU/UK) 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	
	W58		149, 153, 157, 161, 165		

IEEE 802.11ac	Frequency	5GHz			
	Channel	W52	36, 40, 44, 48		
		W53	52, 56, 60, 64		
		W56	(US/CA) 100, 104, 108, 112, 116, 132, 136, 140, 144 (EU/UK) 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140		
		W58	149, 153, 157, 161, 165		
IEEE 802.11ax	Frequency	2.4GHz/5GHz			
	Channel	2.4GHz	(US/CA) 1 to 11 (EU/UK) 1 to 13		
		5GHz	W52	36, 40, 44, 48	
			W53	52, 56, 60, 64	
			W56	(US/CA) 100, 104, 108, 112, 116, 132, 136, 140, 144 (EU/UK) 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	
			W58	149, 153, 157, 161, 165	



- W52 and W53 channels of 5GHz band cannot be used outdoors.
- W53 and W56 channels cannot be used when BR-110AX is operating in Access Point mode.

B-2. Software Specifications

Supported Web browser	Microsoft Edge 143 or newer
-----------------------	-----------------------------

Configuration Mode Operation

Network layer	ARP, IP, ICMP
Transport layer	TCP, UDP
Application layer	DHCP Client, DNS Client, SNTP Client, DHCP Server (simple server function only), DNS Server (simple reply function only), HTTPS, SXSMP(*), NetBIOS over TCP/IP (Name Service only)

Normal Operation

Network layer	ARP, IP, ICMP
Transport layer	TCP, UDP
Application layer	DHCP Client, DNS Client, SNTP Client, DHCP Server, HTTPS, SXSMP(*)

(*) Silex Technology's proprietary protocol



TIP

- BR-110AX supports IPv4 only and does not support IPv6.

B-3. Security Information

B-3-1. Access Control Mechanism

Web Page

Information	Access Control Method	Encryption Mode
Network settings (Network assets)	Accesses are controlled using an administrator password.	Communications are encrypted using HTTPS
Security settings (Security assets)	Accesses are controlled using an administrator password.	Communications are encrypted using HTTPS

AMC Manager/Bulk Configuration with Import File

Information	Access Control Method	Encryption Mode
Network settings (Network assets)	Accesses are controlled using an administrator password.	Communications are encrypted using a unique algorithm
Security settings (Security assets)	Accesses are controlled using an administrator password.	Communications are encrypted using a unique algorithm

FLDP/BR

Information	Access Control Method	Encryption Mode
Network settings (Network assets)	Accesses are allowed only from the devices on the same wired network.	No encryption
Security settings (Security assets)	Accesses are allowed only from the devices on the same wired network.	No encryption

B-3-2. Key Information

Wireless Communication - Key Information

Encryption Algorithm	Key Length
TKIP	128bit
AES	128bit

Client Certificate / CA Certificate - Key Information

Encryption Algorithm	Key Information
RSA	Key Length: 2048bit, 3072bit, 4096bit
ECDSA	Supported Curves: P-256, P-384, P-521

B-3-3. Known Vulnerabilities

The BR-110AX has the following known vulnerabilities:

- Vulnerabilities that cannot be exploited in the specific conditions of the equipment

There are no such vulnerabilities.

- Vulnerabilities that have been mitigated to an acceptable residual risk

There are no such vulnerabilities.

- Vulnerabilities that have been accepted on a risk basis

- Configuration import and export of BR-110AX uses unencrypted files. The configuration Web interface uses HTTPS and restricts access using a password. In addition, the wireless LAN is protected by appropriate encryption methods. Although these measures provide a certain level of security, handle configuration files with care.
- The wireless client function of BR-110AX supports insecure encryption modes such as TKIP.
- When Enterprise authentication is used with the wireless LAN function of BR-110AX, TLS v1.2 and TLS v1.3 encryption methods are supported.
- Communications of FLDP/BR are not encrypted.

Configuration Utility

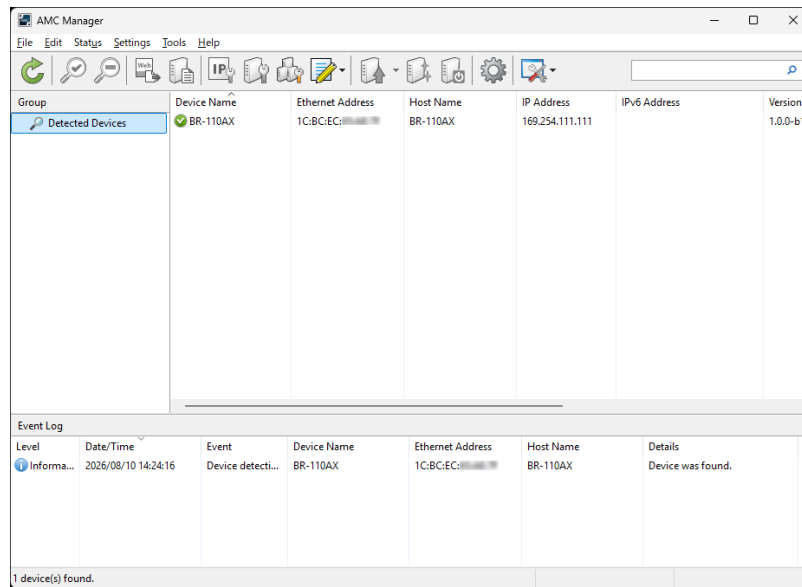
BR-110AX supports the utility below.

- AMC Manager

C-1. AMC Manager

C-1-1. What is AMC Manager?

AMC Manager is the unified device management utility that provides remote status monitoring and individual/bulk configuration for Silex devices over an IP network. It can display the operating status of BR-110AX on the list and such information can be used conveniently for device management.



For AMC Manager, there are a free version "AMC Manager Free" and a non-free version "AMC Manager". When a non-free version is used, more devices can be managed and configured at once and the plug-in utilities such as Mesh Monitor, etc. can be used.

Function	AMC Manager® Free (Free version)	AMC Manager® (Non-free version)
Number of devices that can be displayed	Up to 10 devices	Up to 10,000 devices
Number of devices that can be controlled at a time	Up to 10 devices	Up to 10,000 devices
Number of groups that can be created	Up to 2 groups	Up to 100 groups
Number of devices that can be registered per group	Up to 10 devices	Up to 1,000 devices
Plug-in utility	Unavailable	Available



- To use AMC Manager (non-free version), the license key needs to be purchased.
- If you are interested in purchasing the license, please contact us. For the contact information, refer to **D-2. Customer Support Center**.

How to Download AMC Manager

AMC Manager® can be downloaded from the Silex Technology's website.

1. Access the URL below to download it.

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

2. When the website is displayed, click **Resources** > **Support Center** from the top menu.

3. Click **Software Download**.

4. In the **Software Download** page, click **AMC Manager**.

5. Download AMC Manager.



Note

- For information on how to install AMC Manager, refer to the AMC Manager® User's Manual.

D. Product Information and Customer Services

D-1. Product Information

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

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

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

D-2. 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 Silex Technology Customer Support.

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



Note

- Visit the Silex Technology website for the latest FAQ and product information.