Wireless Bridge

BR-500AC

User's Manual

silex technology

WA106560XH

Index

1. Introduction 1

1-1. Introduction 1

Disclaimers 1

Trademarks 1

1-2. Safety Instructions 2

1-3. Product Information and Customer Services 5

Product Information 5

Customer Support Center 5

2. About BR-500AC 7

2-1. Features 8

2-2. Parts and Functions 10

2-3. Hardware Specification 12

2-4. Software Specification 17

2-5. Use of Radio Waves 18

Notes on Usage 18

2-6. Notes on Security 20

3. Before You Begin 21

3-1. Operating Mode 21

Single Client Mode 22

Multi-Client Mode 23

3-2. Configuration Method 24

Easy Configuration Using Configuration Mode 25

Wireless Configuration Using Smart Wireless Setup (Push Switch) 26

Wireless Configuration Using Smart Wireless Setup (PIN Code) 27

3-3. Necessary Wireless Setting Information 28

4. How to Configure BR-500AC 29

4-1. Starting Configuration Mode for Password Settings 30

Starting BR-500AC in Configuration Mode 30

Password Configuration 32
4-2. Easy Configuration Using Configuration Mode 34
Configuration 34
Connecting Non-wireless Devices 37
4-3. Configuration Using Smart Wireless Setup (Push Switch) 39
Configuration 40
Connecting Non-wireless Devices 44
4-4. Configuration Using Smart Wireless Setup(PIN Code) 46
Checking a PIN Code 47
Configuration 49
Connecting Non-wireless Devices 51
5. List of Functions 53
5-1. How to Access Web Configuration Interface 54
Configuration via Web Configuration Interface 55
5-2. IEEE802.1X Authentication 57
Network Configuration 57
IEEE802.1X Authentication 59
Certificate Standard 61
MAC Address Filtering 62
Before Using the IEEE802.1X Authentication 62
IEEE802.1X Authentication Settings 63
5-3. Saving Log 66
Types of Log 66
Retrieving/Deleting System Log 70
Retrieving/Deleting Event Log 74
Time Synchronization of Log 78
5-4. Address Management Table 79
About Address Management Table Feature 79
Registering Address to Management Table 80
Deleting Address from Management Table 82

5-5. WME Function 84
Default Access Category Setting 84
5-6. Communicating with a Wireless Router with Proxy ARP Function 86
IP Intercept Function 87
Accessing Web Page of Non-wireless Device 89
5-7. Maintenance 91
Restarting 91
Factory Default Configuration 93
Firmware Update 95

A. Appendix 99

A-1. List of All Settings 99
A-2. Troubleshooting 116
A-3. What's AMC Manager®? 119
How to Download AMC Manager® 119
A-4. Security Information 120
Access Control Mechanism 120
Key Information 121
Known Vulnerabilities 122

Blank page

1. Introduction

Thank you for purchasing the Wireless Bridge BR-500AC (hereinafter the "BR-500AC").

1-1. Introduction

This manual provides information on how to configure and use the BR-500AC.
Please read the Safety Instructions carefully before you begin.

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-500AC 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.

Trademarks

- AMC Manager® is a registered trademark of Silex Technology, Inc.
- Microsoft, Windows and Microsoft Edge are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Wi-Fi, Wi-Fi Protected Setup, WMM, Wi-Fi Multimedia, WPA(Wi-Fi Protected Access), WPA2 and WPA3 are trademarks or registered trademarks of Wi-Fi Alliance.
- Safari is trademarks of Apple Inc., registered in the United States and other countries.
- Other company names and product names contained in this manual are trademarks or registered trademarks of their respective companies.

1-2. Safety Instructions

This page provides the safety instructions for safe use of BR-500AC.
To ensure safe and proper use, please read the following information carefully before using BR-500AC. The safety instructions include important information on safe handling of BR-500AC and on general safety issues.

< Meaning of the warnings >

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

< Meaning of the symbols >

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

Warning

 	* Do not allow physical impact. When damaged, turn off the connected devices, unplug the AC plug of BR-500AC from a power outlet and contact your point of purchase. Failure to take this action could cause fire or an electrical shock. * In the following cases, turn off the connected devices and unplug the AC plug of BR-500AC from a power outlet and contact your point of purchase. Failure to take this action could cause fire or an electrical shock. * When BR-500AC emits a strange smell, smoke or sound or becomes too hot to touch. * When foreign objects (metal, liquid, etc.) gets into BR-500AC.
	* Keep the cords and cables away from children. It may cause an electrical shock or serious injury.
	* If a ground wire is supplied with your device to use with, connect it to the ground terminal in order to prevent an electrical shock. Do not connect the ground wire to gas pipe, water pipe, lighting rod or telephone ground wire. It may cause malfunction.
	* Do not disassemble or modify BR-500AC. It may cause fire, electrical shock or malfunction. * Do not disassemble or modify the AC adaptor that came with BR-500AC. It may cause fire, electrical shock or malfunction.
	* Do not use BR-500AC with the equipment that directly affects the human life (medical equipment such as the life support equipment and operating room equipment) and with the system that has a significant impact on the human safety and the maintenance of public functions (nuclear equipment, aerospace equipment, etc.).

Caution

	* Do not pull on the cord to disconnect the plug from the power supply. The code may be broken, which could result in fire or an electrical shock.
	* When removing BR-500AC, disconnect the AC plugs of both BR-500AC and the other devices you are using with. * Verify all codes or cables are plugged correctly before using BR-500AC. * When BR-500AC will not be used for a long time, unplug the power cables of BR-500AC and the other devices you are using with.
	* Use the AC adaptor supplied with BR-500AC. Other AC adaptors may cause malfunction. * Do not use or store BR-500AC 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.)

1-3. Product Information and Customer Services

Product Information

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

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

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

Customer Support Center

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

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

Note

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

Blank page

2. About BR-500AC

BR-500AC is the wireless bridge which allows to use a non-wireless device (10/100/1000BASE-T network device) as a wireless device. With 2.4G/5GHz band support, various non-wireless devices can easily be connected over a wireless network.
The enterprise security feature will ensure safe and secure use of wireless communication at an office, factory, etc. where a higher security is required.

2-1. Features

BR-500AC has the following features:

Giving unlimited locations for your non-wireless devices

As you do not have to care wiring conditions in order to establish your environment, choices of location greatly expand in any kinds of scenes such as office, factory, school, commercial facility, etc. where the layout change is frequently required or effective layout of equipment needs to be carefully considered for a work line. Also, cost reductions is largely expected as you will no longer have to pay for wiring construction.

IEEE 802.11a/b/g/n/ac

BR-500AC supports communications at both 2.4GHz/5GHz bands. Using 5GHz band will help to avoid radio interference with 2.4GHz band which is most commonly used in the market.

Advanced security

The following security features are supported:
- Open (WEP)
- WPA3-Personal (AES)
- WPA2-Personal (AES)
- WPA/WPA2-Personal (AUTO)
- WPA3-Enterprise (AES)
- WPA2-Enterprise (AES)
- WPA/WPA2-Enterprise (AUTO)

TIP

- To ensure secure wireless communication, use a wireless network that uses WPA3-Personal or WPA3-Enterprise for network authentication and AES for encryption.

Note

- For WPA3-Enterprise, WPA2-Enterprise and WPA/WPA2-Enterprise, IEEE802.1X authentication method can be used.

Two types of operating mode

[Single Client Mode]

- Bridges a single non-wireless device connected to a LAN port of the BR-500AC over wireless network.
- For the MAC address to use for wireless LAN connection, the MAC address of the device connected to a LAN port of the BR-500AC will be used (MAC address transparent feature).
- Stops bridging when someone changed the device being connected to a wired LAN port of the BR-500AC to the other one (security feature).

[Multi-Client Mode]

- Up to 16 non-wireless devices can be bridged over wireless network if a HUB is connected to a LAN port of the BR-500AC.
- For a MAC address to use for wireless LAN connection, the MAC address of the BR-500AC will be used.

Easy access to the Web configuration interface

Without changing the setting of the PC you use for setup, the Web configuration interface of BR-500AC can easily be accessed.

Wireless Configuration Using a Push Switch

BR-500AC support the wireless configuration using Smart Wireless Setup. If your wireless router (Access Point) supports WPS (Wi-Fi Protected Setup), you can configure the wireless settings easily using the push switch.

Supports "AMC Manager® "(non-free program / free program)

BR-500AC supports the total management software, "AMC Manager®" .
The AMC Manager® provides the useful features as follows:
- Remote device control and monitoring
- Bulk configuration and firmware updates
- System time synchronization (version 3.2.0 or later)

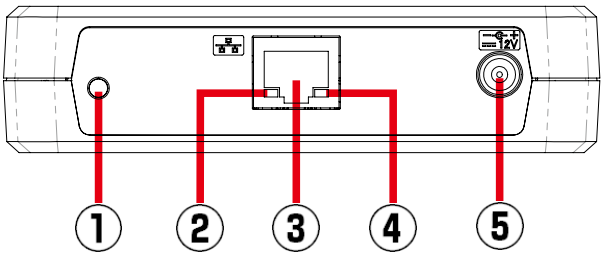
Note

- To use the functions above, your Access Point or wireless router needs to support the same functions.
- For details on the "AMC Manager®", please visit our homepage.
- To use the "AMC Manager®", an IP address needs to be configured to the BR-500AC.
- BR-500AC can be used in Infrastructure mode only. Ad hoc mode is not supported.

2-2. Parts and Functions

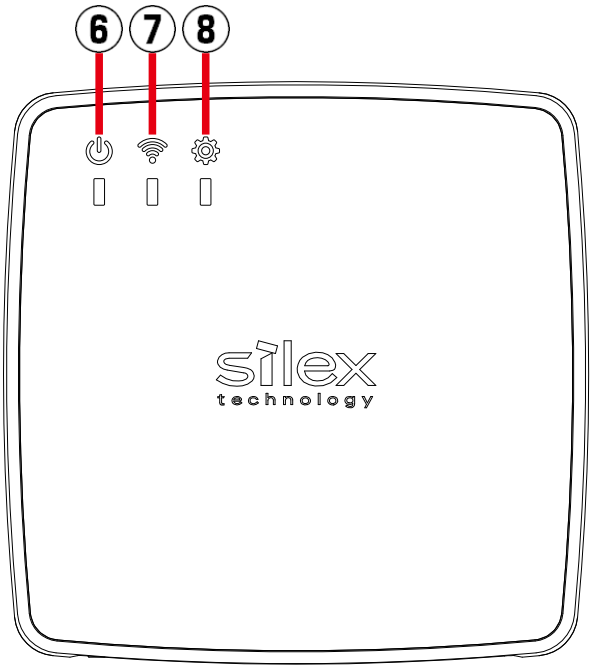
The parts name and functions are as follows:

Front

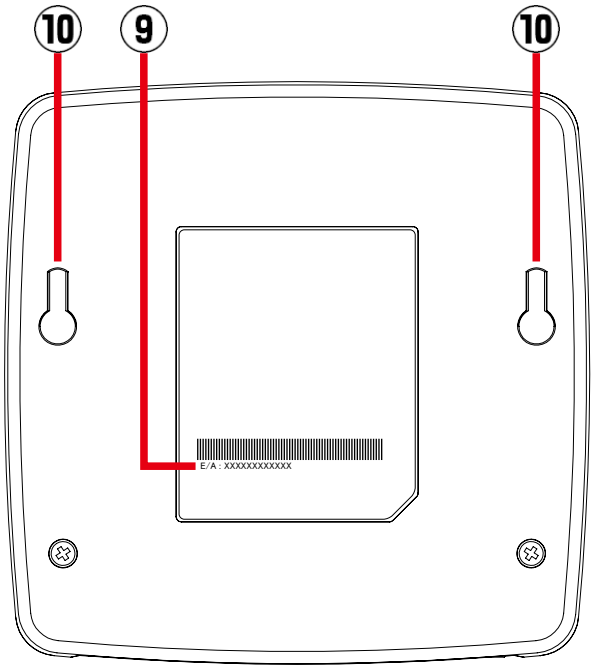


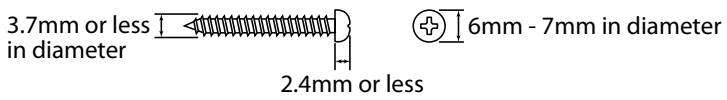
(1)	Push Switch	Start in Configuration Mode	Press and hold this switch for 5 sec while BR-500AC is active.
		Wireless configuration using Smart Wireless Setup	Press and hold this switch for 10 sec while BR-500AC is active.
		Factory default configuration	Press and hold the push switch while turning on BR-500AC. Release the switch when the WLAN LED turns green and then to red.
(2)	Link LED (Green/Orange)	ON (Green)	Linked in wired LAN(1000BASE-T).
		BLINK (Green)	Receiving packets in wired LAN(1000BASE-T).
		ON (Orange)	Linked in wired LAN(100BASE-TX/10BASE-T).
		BLINK (Orange)	Receiving packets in wired LAN(100BASE-TX/10BASE-T).
		OFF	Wired LAN is not connected.
(3)	LAN port	Connect a LAN cable.	
(4)	Power LED (Yellow)	ON (Yellow)	Powered on.
		OFF	Powered off.
(5)	Connector	Connect an AC adaptor.	

Top



Bottom



(6)	POWER LED (Green/Red/Orange)	ON (Green)	Powered on.
		BLINK (Orange)	Updating the firmware.
		OFF	Powered off.
		* In case of a wired LAN port error, the POWER LED (red) blinks rapidly while the STATUS LED (green) is on. * In case of a wireless LAN module error, the POWER LED (red) blinks rapidly while the WLAN LED (green) is on.	
(7)	WLAN LED (Green/Red/Orange)	ON (Green)	Running in Infrastructure mode.
		BLINK (Green)	Processing setup using the Smart Wireless Setup.
		OFF	Wireless LAN is OFF.
		* Blinks green together with the STATUS LED when operating in Configuration Mode. * Turns green and then to red during the initialization.	
(8)	STATUS LED (Green)	ON (Green)	AP is connected.
		BLINK (Green)	Transferring data.
		OFF	AP is not connected.
		* Blinks green together with the WLAN LED when operating in Configuration Mode.	
(9)	MAC Address	MAC Address of BR-500AC	
(10)	Screw Hole	Use to mount BR-500AC on the wall (purchase two screws separately). - Distance between the left and right screw holes: 90mm - Necessary gap between the wall and the screw head: 2mm or more - Recommended screw size:  For the length of the screw, select the appropriate one according to the material and thickness of the wall. Silex Technology is not responsible for any loss or damage resulting from falling. Make sure that BR-500AC is securely fixed to the wall so that it does not fall due to the weight of the unit and cable.	

2-3. Hardware Specification

Operating environment	Temperature : 0 degrees to +40 degrees	
	Humidity : 20% to 80%RH (Non-condensing)	
Storage environment	Temperature : -10 degrees to +50 degrees	
	Humidity : 20% to 90%RH (Non-condensing)	
EMI	VCCI Class B FCC Class B ICES Class B CE / UKCA Class B	
Wired network interface	10BASE-T/100BASE-TX/1000BASE-T (Auto-sensing) :1 port Auto MDI/MDIX	
Wireless network interface	IEEE 802.11a/b/g/n/ac	
Channel	(USA/CA) 2.4GHz: 1-11ch 5GHz: (W52) 36,40,44,48 (W53) 52,56,60,64 (W56) 100,104,108,112,116,132,136,140,144 (W58) 149,153,157,161,165 (USA) 2.4GHz: 1-11ch 5GHz: (W52) 36,40,44,48 (W53) 52,56,60,64 (W56) 100,104,108,112,116,120,124,128,132,136,140,144 (W58) 149,153,157,161,165 (EU/UK) 2.4GHz: 1-13ch 5GHz: (W52) 36,40,44,48 (W53) 52,56,60,64 (W56) 100,104,108,112,116,120,124,128,132,136,140	
Push Switch	1	
LED	Top	POWER (Green / Red / Orange) WLAN (Green / Red / Orange) STATUS (Green)
	LAN Port	Power (Yellow) Link (Green/ Orange)
Compatible devices	Network devices with LAN port (RJ-45)	
Max number of connectable devices	When operating in **Single Client Mode** : 1 device When operating in **Multi-Client Mode** : 16 devices	

Reliability Test

<table>
<tr><th rowspan="2">Test Name</th><th rowspan="2">Standard</th><th rowspan="2">Description</th><th colspan="2">Results</th></tr>
<tr><th>Operation</th><th>Appearance</th></tr>
<tr><td>Temperature / Humidity cycle test</td><td>-</td><td>Check the operation under the following conditions.
- Confirm that the communication does not stop.
<table>
<tr><td>Step</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr>
<tr><td>℃</td><td>+25</td><td>-5</td><td>-5</td><td>+45</td><td>+45</td><td>-5</td></tr>
<tr><td>%RH</td><td>OFF</td><td>OFF</td><td>OFF</td><td>OFF</td><td>OFF</td><td>OFF</td></tr>
<tr><td>Time</td><td>0:05</td><td>1:00</td><td>2:00</td><td>1:00</td><td>2:00</td><td>1:00</td></tr>
<tr><td>Step</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td></tr>
<tr><td>℃</td><td>-5</td><td>+45</td><td>+45</td><td>+45</td><td>25</td><td>25</td></tr>
<tr><td>%RH</td><td>OFF</td><td>OFF</td><td>20</td><td>90</td><td>40</td><td>OFF</td></tr>
<tr><td>Time</td><td>4:00</td><td>1:00</td><td>2:00</td><td>6:00</td><td>1:00</td><td>0:10</td></tr>
</table></td><td>Possible</td><td>NA</td></tr>
<tr><td>High temperature operation test</td><td>-</td><td>Check that the product operates for 8 hours or more at a temperature of +45℃ .</td><td>Possible</td><td>NA</td></tr>
<tr><td>Low temperature operation test</td><td>-</td><td>Check that the product operates for 4 hours or more at a temperature of -5℃ .</td><td>Possible</td><td>NA</td></tr>
<tr><td>Low/High temperature startup test</td><td>-</td><td>Power on the product and check the communication according to the steps below.
(1) Leave the product for 2 hours at a temperature of -5℃ /+45℃ without powering it on.
(2) Power on the product for 5 times at 30-minute intervals.</td><td>Possible</td><td>NA</td></tr>
<tr><td>Storage temperature test</td><td>-</td><td>After leaving the product under the following conditions, check that it operates at room temperature.
Confirm that the housing is not deformed or damaged.
Temp / Time: 55℃ / 20 - 95%RH / 8H (no power-supply)
Temp / Time: -15℃ / 8H (no power-supply)</td><td>Possible</td><td>No damages</td></tr>
<tr><td>Power on/off test</td><td>-</td><td>Confirm that the product powers on under the following conditions.
Number of power-on tests: 2,000 times
Interval of power-off (seconds): 1, 2, 3, 4, 5, 10, 20, 30, 40, 50</td><td>Possible</td><td>NA</td></tr>
<tr><td>Electrostatic discharge test</td><td>IEC61000-4-2</td><td>Confirm that the product meets the performance criteria B during or after the test under the following conditions.
Discharge capacitance: 150pF
Discharging resistance: 330Ω
Indirect discharge: 4kV or more
Contact discharge: 4kV or more
Air discharge: 8kV or more
Application upper limit: Specified value ±10%</td><td>Possible</td><td>NA</td></tr>
<tr><td>Fast transient /burst test</td><td>IEC61000-4-4</td><td>Confirm that the product meets the performance criteria B during or after the test under the following conditions.
Level: Power ±1000V
IO ±500V
Burst length: 15 milliseconds
Burst period: 300 milliseconds
Frequency: 5kHz
Applied: L, N, PE, CLMP
Application upper limit: Specified value ±10%</td><td>Possible</td><td>NA</td></tr>
</table>

Test Name	Standard	Conditions	Results	
			Operation	Appearance
Shock test	JIS C60068-2-27	Shock waveform: Half sine wave Shock direction: 6 directions Duration: 11 milliseconds Acceleration: 98m/s^2 (10G) Number of tests: 1,000 times per direction (total 6,000 times)	Possible	No damages
Vibration test	JIS C60068-2-6	Vibration waveform: Sine wave Vibration direction: X, Y, Z Frequency: 10 - 150Hz Acceleration: 4.9m/s^2 (0.5G) Duration: 2 hours for 3 axes	Possible	No damages
Package drop test	ISO 4180 (JIS Z0200 Level I)	Packing box Drop height: 80cm Number of drops: 10 times (drop from a face: 6 times/ drop from an edge: 3 times/drop from a corner:1 time)	Possible	No damages
External force test	JIS C 62368	Force: 250N Direction: 6 directions Duration: 5 minutes for each face	Possible	No damages
Ceiling test	JIS C 62368	Installation type: Screw hook Force: 5.5N (6 directions) Duration: 1 minute for each direction	Possible	No damages

* Possible: The product can operate during the test.

* No damages: There are no damages on appearance after completing the test.

Notice to US Customers

Contains FCC ID : N6C-SXPCEAC2

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.

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 §15.105(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.

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

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

FCC Rules Part 15 Subpart C §15.247(g) / Subpart E
This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

FCC Rules Part 15 Subpart C §15.247 and Subpart E
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment and meets the FCC radio frequency (RF) Exposure Guidelines. This equipment should be installed and operated keeping the radiator at least 20cm or more away from person's body.

Notice to Canadian Customers

Contains IC : 4908A-SXPCEAC2

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

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 2 §6.2.2.2
for indoor use only (5150-5350 MHz)

Pour usage intérieur seulement (5150-5350 MHz)

RSS-247 Issue 2 §6.4
Data transmission is always initiated by software, which is the passed down through the MAC, through the digital and analog baseband, and finally to the RF chip. Several special packets are initiated by the MAC. These are the only ways the digital baseband portion will turn on the RF transmitter, which it then turns off at the end of the packet. Therefore, the transmitter will be on only while one of the aforementioned packets is being transmitted. In other words, this device automatically discontinue transmission in case of either absence of information to transmit or operational failure.

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

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

CE

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

UKCA

UK

Restrictions or Requirements in the UK

2-4. Software Specification

Configuration Mode Operation

Network layer	ARP, IP, ICMP, FLDP/BR
Transport layer	TCP, UDP
Application layer	DHCP Client (*1), DNS Client, NTP Client, HTTPS, SXSMP (TCP/UDP#59999/60000) (*2), DNS Server (simple reply function only), DHCP Server (simple server function only), NetBIOS over TCP/IP (Name Service only)

Normal Operation

Network layer	ARP, IP, ICMP, FLDP/BR
Transport layer	TCP, UDP
Application layer	DHCP Client (*1), DNS Client, NTP Client, HTTPS, SXSMP (*2)

(*1) BOOTP is not supported.

(*2) Silex Technology's proprietary protocol

TIP

- For Multi-Client mode, only ARP, IPv4 and IPv6 communication is bridged.

2-5. Use of Radio Waves

Notes on Usage

When using BR-500AC near the medical devices

The radio wave interference may adversely affect the operation of medical devices such as pacemakers. When using BR-500AC 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-500AC 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-500AC 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-500AC, make sure that no radio wave interference occurs. For example, if there is a microwave oven near BR-500AC, check the proper communication beforehand while actually using the microwave oven.

Do not use BR-500AC 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-500AC, it will not cause any problems. However, when they approximate BR-500AC, sound or image noise may occur.

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

BR-500AC can connect through wood or glass, but may have troubles connecting through reinforced concrete/metal.

BR-500AC complies with the certification of conformance to technical standards. Please pay attention to the following points:

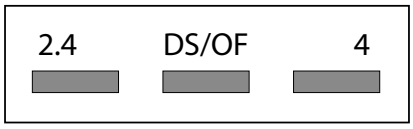
- Please do not disassemble or remodel the product. Such action is prohibited by law.
- Please do not remove the certificate label. Using the product without a label is prohibited.

Wireless devices using 2.4GHz band

The same frequency band of BR-500AC is used for a microwave, industry, science, medical equipment and licensed in room or low power (non-licensed) radio stations.

- Before you use BR-500AC, check that it does not interfere with other devices.
- If interference occurs, stop using BR-500AC 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.

2-6. 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.

3. Before You Begin

This chapter explains each operating mode and available configuration methods for BR-500AC as well as the wireless setting information you need to check out before the configuration.

Before starting the initial configuration, a password needs to be set for BR-500AC.
For details, refer to **4-1. Starting Configuration Mode for Password Settings**.

3-1. Operating Mode

BR-500AC has 2 operating modes below.
Please use the one appropriate for your environment.

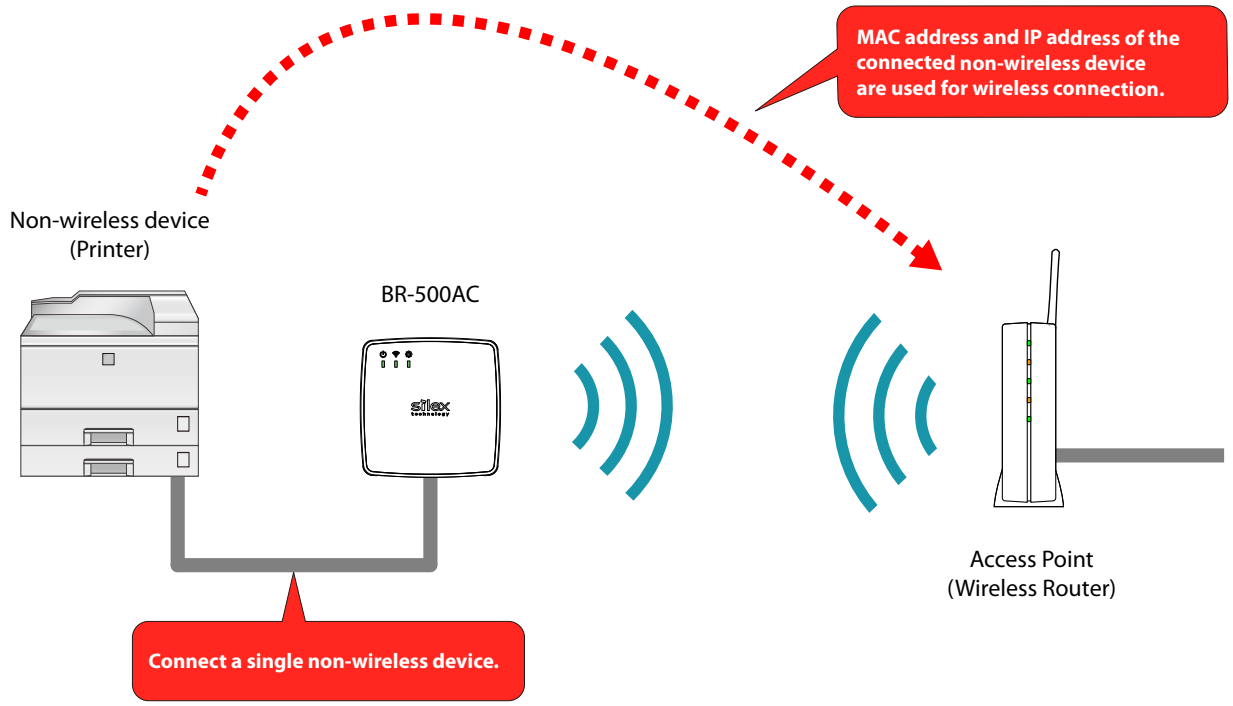
- Single Client Mode
- Multi-Client Mode

Note

- The operating mode can be configured on the Web configuration interface which can be accessed when the BR-500AC operates in Configuration Mode.
- By defaults, the operating mode is set to **Single-Client Mode**.

Single Client Mode

Use this mode when you connect a single non-wireless device to the BR-500AC. As the MAC address and IP address of the connected device are used for wireless LAN connection, you can use the device as if it is directly connected to a wireless LAN.

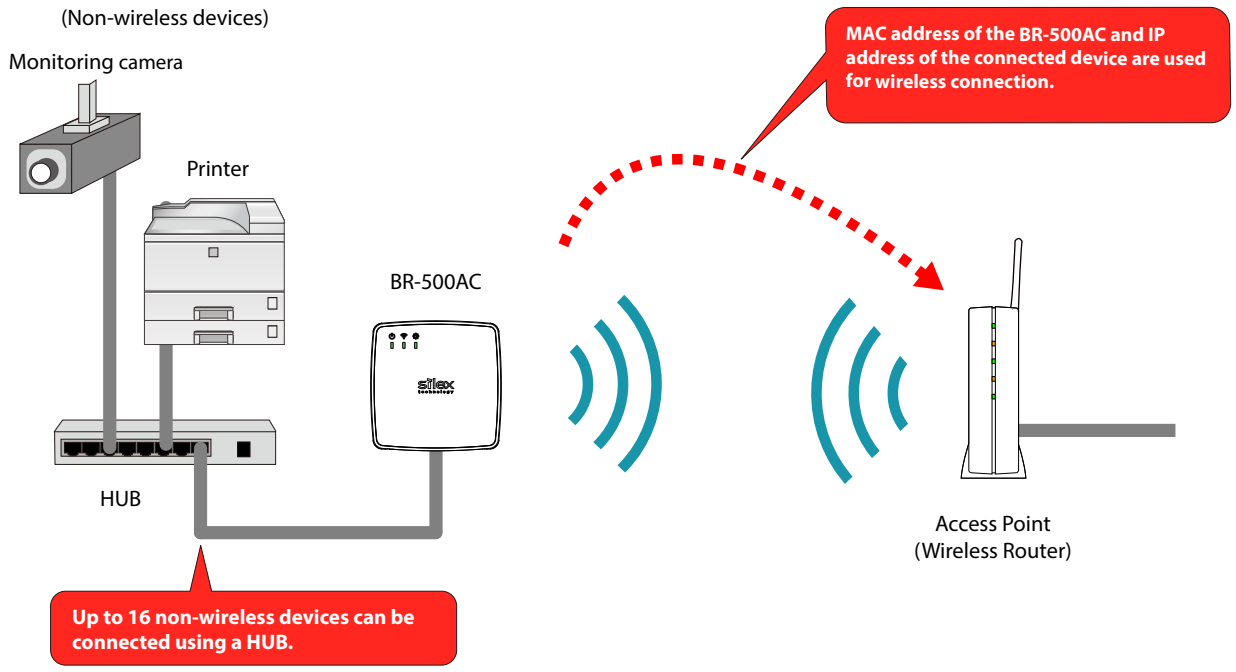


TIP

- If a wireless router with a Proxy ARP function exists in the network environment, BR-500AC may not be able to communicate with non-wireless devices. In such a case, enabling the IP Intercept function can solve the problem. For details, refer to **5-6. Communicating with a Wireless Router with Proxy ARP Function**.
- Only one device can be connected to a LAN port.
- The following actions are treated as an error. If one of these occurs, the bridge function will abort.
  - Connecting multiple devices to a LAN port using a HUB
  - Changing the device connected to a LAN port to the other device while BR-500AC is running.
- If the connection is lost on a LAN port while communication is in progress, wireless bridging will be disabled until it is reconnected.
- The devices with multiple MAC addresses cannot be used.
- Due to restrictions of the protocols, "**View full map**" of "**Network and Sharing Center**" is not fully supported on Windows 7.

Multi-Client Mode

Use this mode when you connect multiple non-wireless devices to BR-500AC.
By using a HUB on the LAN port, up to 16 devices can be connected.
For wireless LAN connection, the MAC address of the BR-500AC and the IP address of the connected device will be used.



TIP

- If a wireless router with a Proxy ARP function exists in the network environment, BR-500AC may not be able to communicate with non-wireless devices. In such a case, disable the Proxy ARP function of the wireless router.
- The devices with multiple MAC addresses cannot be used.
- When Multi-Client Mode is on, only ARP, IPv4 and IPv6 are supported. The following protocols are not supported.
  - Protocols with a mechanism to check the source MAC address
  - Protocols with a system to run with a MAC address that is contained in the packet data

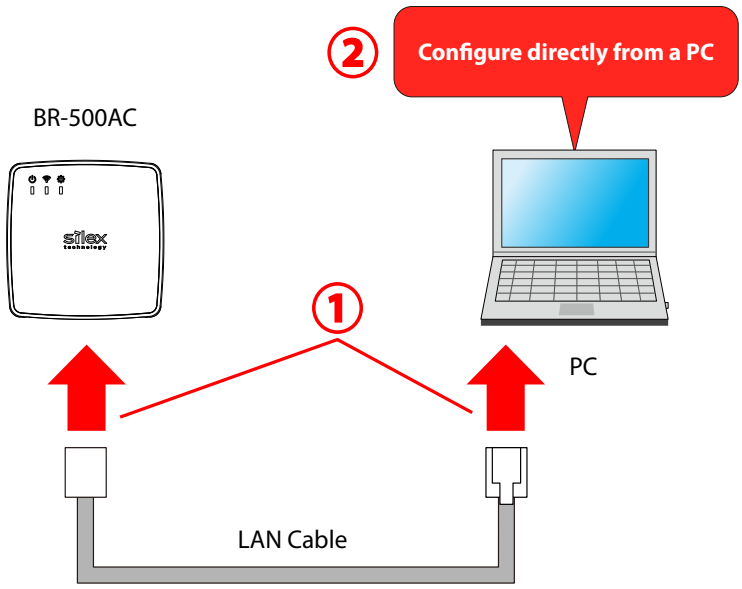
3-2. Configuration Method

There are 3 configuration methods as follows.
Please select the one appropriate for your environment.

- Easy configuration using Configuration Mode
- Wireless configuration using Smart Wireless Setup (Push Switch)
- Wireless configuration using Smart Wireless Setup (PIN code)

Easy Configuration Using Configuration Mode

In this configuration method, you connect the BR-500AC to a PC using a LAN cable to configure the settings from the PC.
By connecting the BR-500AC to the PC and starting it in Configuration Mode, the Web configuration interface can be accessed. Select the Access Point the BR-500AC should wirelessly connect to and enter the Network Key on the configuration interface.
Depending on your environment, you may need to check the wireless LAN information beforehand.

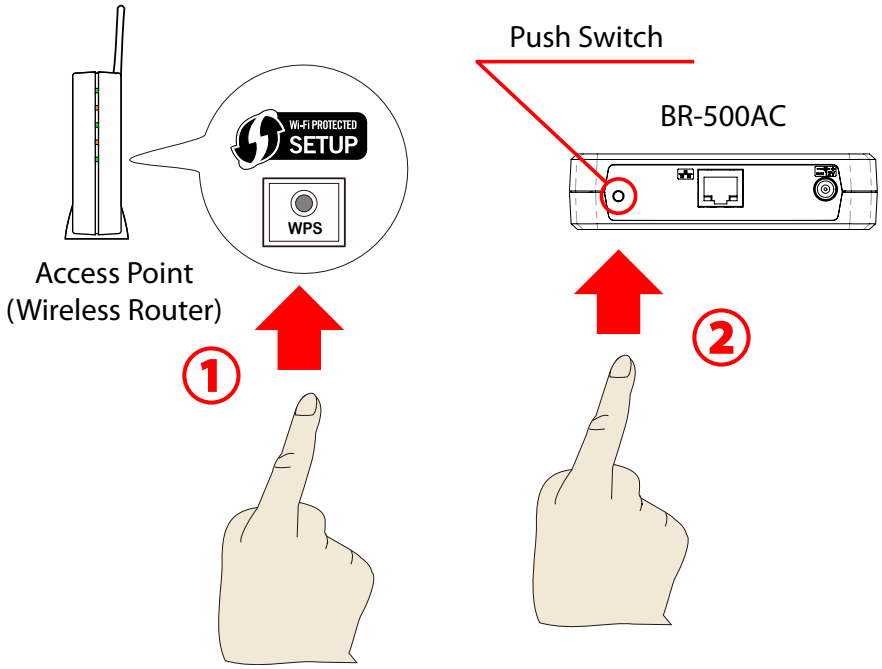


Note

- In this configuration method, only "**SSID**" and "**Network Key**" are needed to connect to a wireless LAN, however, further configuration is required in the following cases.
- Access Point is operating in a stealth mode.
- Access Point is using the Shared authentication
- Access Point is using the Open authentication and the WEP key index other than "1".
- Too many wireless networks are active (up to 32 wireless networks can be shown by BR-500AC).

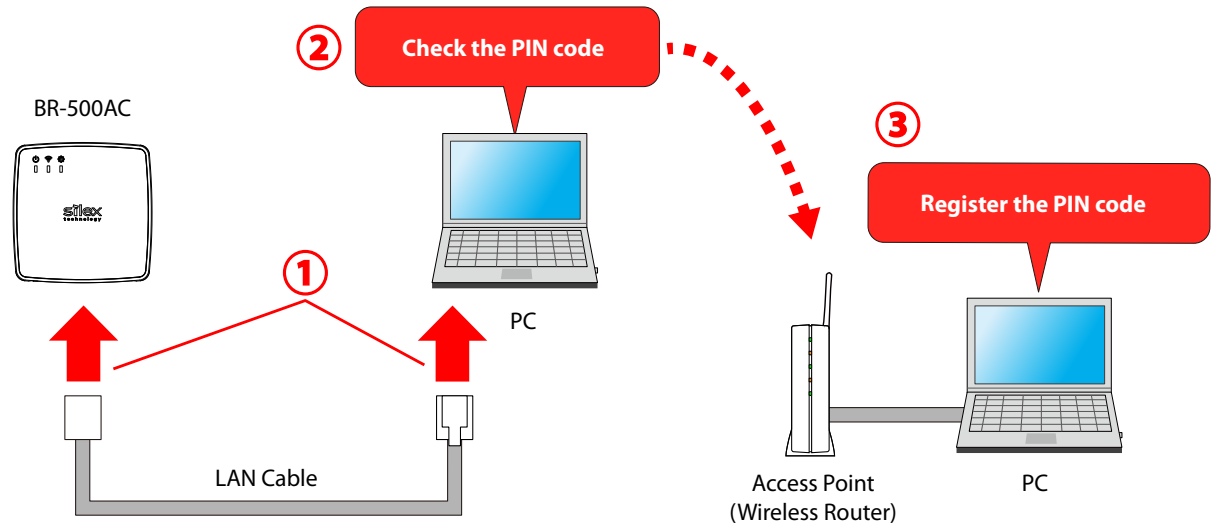
Wireless Configuration Using Smart Wireless Setup (Push Switch)

In this configuration method, you can automatically configure the wireless settings by pressing the wireless connection button on your Access Point (wireless router) and the push switch on BR-500AC. You will not have to get wireless setting information beforehand, as configuration is automatically handled by the BR-500AC and your Access Point.
For this configuration method, an Access Point supporting WPS(Wi-Fi Protected Setup) is required. To see if your Access Point supports WPS, refer to the operation manual that came with your Access Point or contact the manufacturer.



Wireless Configuration Using Smart Wireless Setup (PIN Code)

In this configuration method, you can automatically configure the wireless settings by entering the PIN code of BR-500AC on your Access Point (wireless router).
The PIN code can be identified from the Web configuration interface of BR-500AC. To access the Web configuration interface, connect the BR-500AC directly to a PC using a LAN cable and start it in Configuration Mode.
You will not have to get wireless setting information beforehand, as configuration is automatically handled by the BR-500AC and your Access Point. For this configuration method, an Access Point supporting WPS(Wi-Fi Protected Setup) is required. To see if your Access Point supports WPS, refer to the operation manual that came with your Access Point or contact the manufacturer.



Note

- Two PCs are required for this configuration; one for the BR-500AC and the other one for your Access Point.

3-3. Necessary Wireless Setting Information

When you configure BR-500AC using the Configuration Mode, the wireless settings need to be configured appropriately for your environment. As the same wireless settings must be configured for both BR-500AC and your Access Point, you need to get the necessary setting information of your Access Point beforehand.

Note

- If you plan to configure the BR-500AC using Smart Wireless Setup, you will not have to get the wireless setting information.

TIP

- The wireless setting information explained in this page is specific to your network and cannot be provided by Silex technical support. For how to confirm each setting, please refer to the operation manual that came with your router or contact the manufacturer.
- Depending on your Access Point, WPS may need to be enabled manually. For details, refer to the operation manual that came with your Access Point.
- If a security feature such as MAC Address filtering is enabled on your Access Point, change the setting so that BR-500AC can communicate with your Access Point. For details, refer to the operation manual that came with your Access Point.
- For the IEEE802.1X authentication, refer to **5-2. IEEE802.1X Authentication**.

SSID	The SSID is an ID that distinguishes a wireless LAN network from others. For wireless devices to communicate with each other on a wireless network, they must share the same SSID. (The SSID is also referred to as "ESSID".) Depending on your Access Point, it may have several SSIDs. If there are different SSIDs for a game console and computer, use the one for the computer.	
Encryption Mode	No Encryption	Uses no encryption for wireless communication. (In this case, you do not have to get any of your settings beforehand.)
	WEP	If WEP encryption is used, wireless communication will be encrypted using the settings for "WEP Key 1-4" and "Key Index". Set the same "WEP Key Size(64bit/128bit)", "WEP Key" and "Key Index" as the wireless device you wish to connect.
	WPA / WPA2/ WPA3	Uses PSK for network authentication. The encryption key will be generated by communicating with the Access Point using a Pre-Shared key. WEP key setting is not used for this mode. Set the same "Pre-Shared key" and "Encryption Mode"(AUTO/AES*) as the wireless device you wish to connect. The Pre-Shared key is also referred to as "Network Key" or "Password". * For WPA2/WPA3, only AES is supported. For the Pre-Shared Key, 8-63 alphanumeric characters or 64 hexadecimal value (numbers 0-9 and letters A-F) can be used. (Only for WPA/WPA2)

4. How to Configure BR-500AC

This chapter explains how to configure BR-500AC.
Following configuration methods are available:

1) Configuration using Configuration Mode
2) Configuration using Smart Wireless Setup (Push Switch)
3) Configuration using Smart Wireless Setup (PIN code)

Note

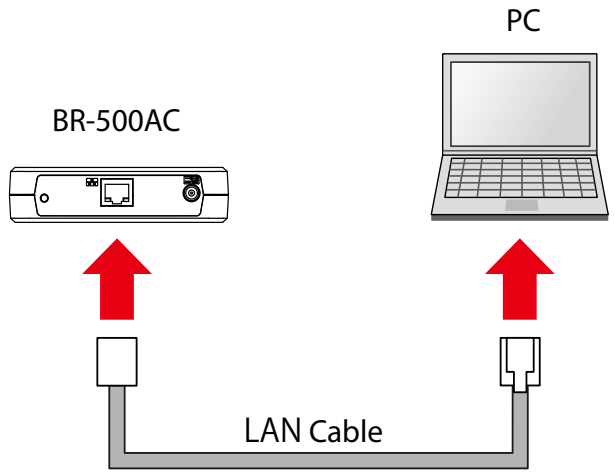
- For details on each configuration method, refer to **3-2. Configuration Method**.

Before starting the initial configuration, a password needs to be set for BR-500AC.
Refer to **4-1. Starting Configuration Mode for Password Settings** to set a password.

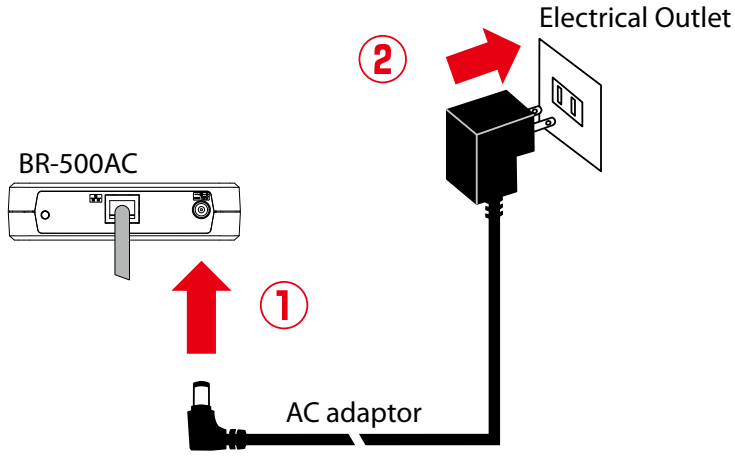
4-1. Starting Configuration Mode for Password Settings

Starting BR-500AC in Configuration Mode

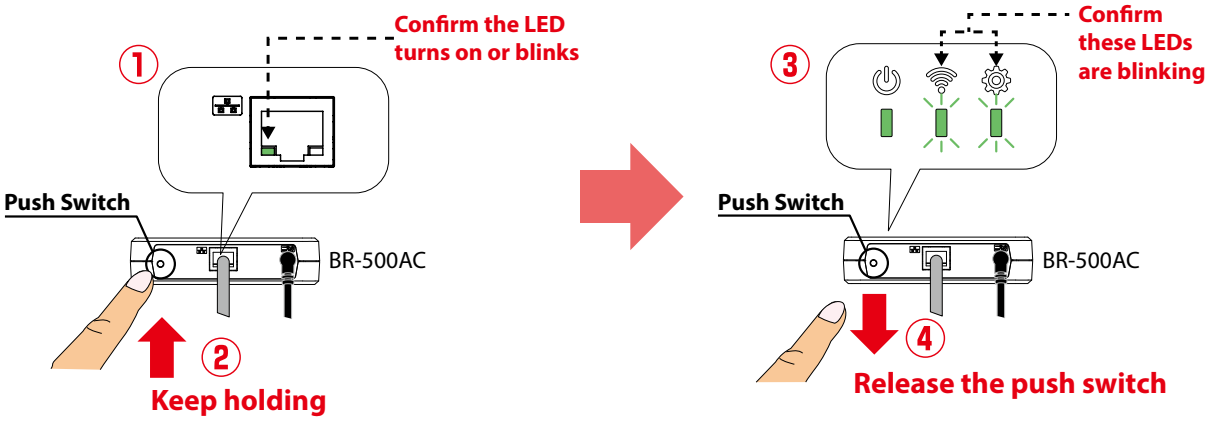
1. Connect BR-500AC and the PC (to use for setup) using a LAN cable.



2. Connect the AC adaptor to BR-500AC, and the AC adaptor's plug to an electrical outlet.

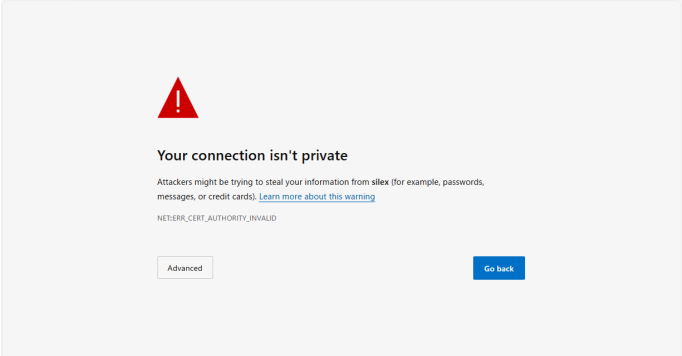


3. When the POWER LED turns green and the Link LED turns on or blinks, press and hold the push switch on the front of BR-500AC.
In 5 seconds, the WLAN LED and STATUS LED will start to blink green together. Release the push switch then.
BR-500AC will start running in the Configuration Mode and be ready to configure from the PC that has been connected to BR-500AC via a LAN cable.



Password Configuration

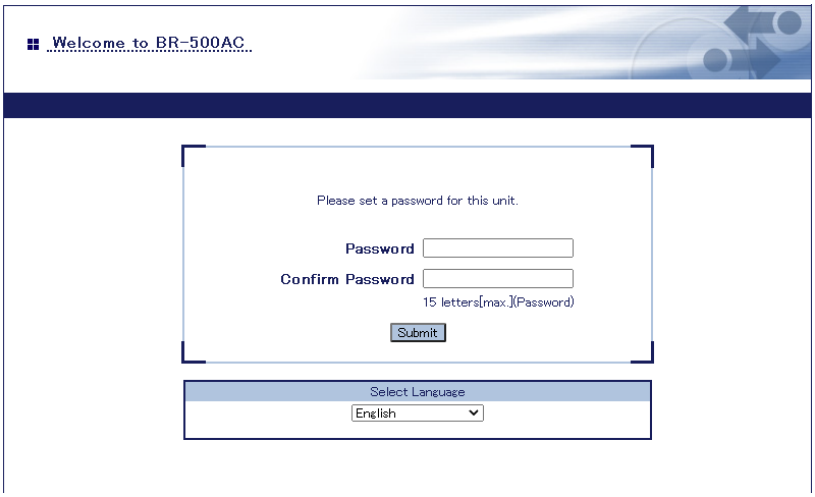
1. As the Configuration Mode is turned on, the Web browser will launch and display the BR-500AC's Web page on the PC connected to BR-500AC.
If the Web browser does not launch, enter "**https://silex**" in the address bar of the Web browser and press the Enter key.
If a warning screen appears, click **Advanced** and then click **Continue to xxxxxx (unsafe)**.



Note

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

2. Start a Web browser on the PC you are using for the setup. When the login password configuration page appears.
Enter the password to configure for BR-500AC and click **Submit**.



TIP

- The login password configuration page is displayed only when BR-500AC is configured for the first time.
- Recommended Web browsers: Microsoft Edge / Safari.

3. The password registration will perform and BR-500AC will be restarted.
When all LEDs turn off and then the POWER LED turns green, the restart is finished.

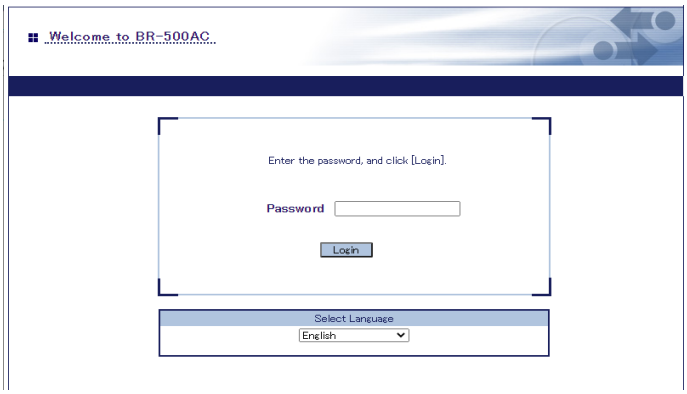
4-2. Easy Configuration Using Configuration Mode

Configuration

How to configure BR-500AC using the Configuration Mode is explained.

1. Refer to **4-1. Starting Configuration Mode for Password Settings** - **Starting BR-500AC in Configuration Mode** to start BR-500AC in the Configuration Mode.

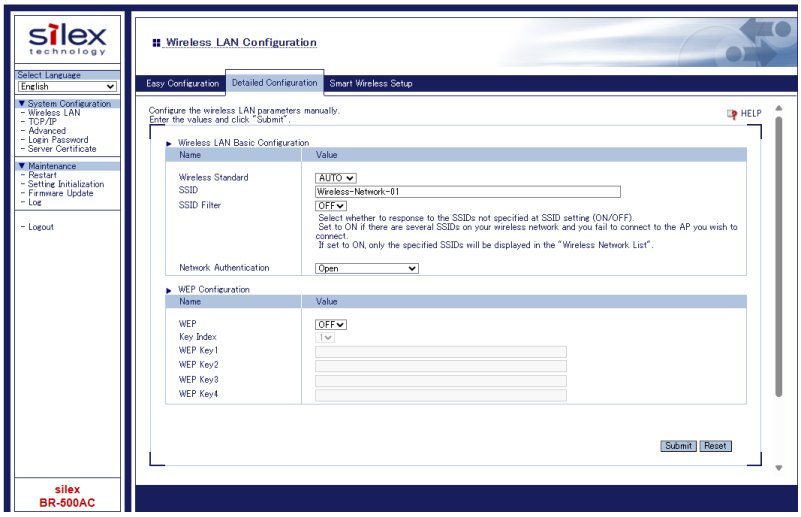
2. The login page is displayed.
   Enter the password for BR-500AC and click **Login**.



TIP

- If the entered password is incorrect, you will not be able to log in for a certain period of time.
- Be sure to log out the Web page when you have finished using it.

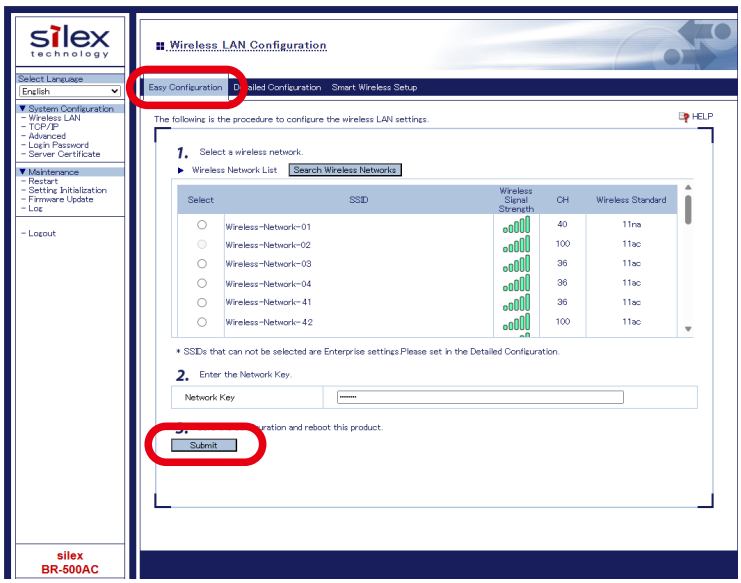
3. The Web page of BR-500AC is displayed.



TIP

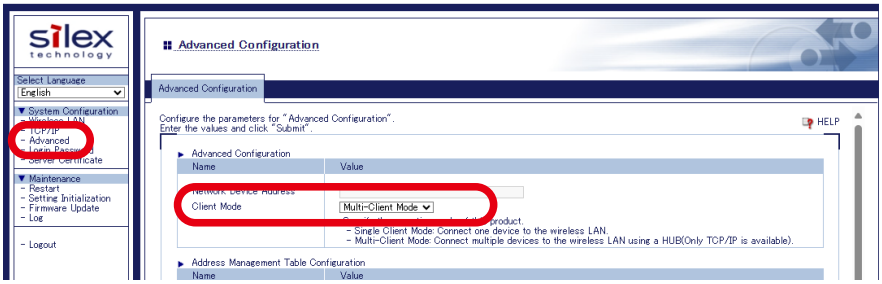
- To start the configuration, the PC and BR-500AC need to communicate each other properly.
- Confirm that an IP Address is correctly configured to the PC.
- If a wireless LAN is enabled on your PC, please disable it.
- If a static IP address is set to the PC, the Web configuration interface cannot be displayed in the following cases:
  - An IP address of the different segment is entered to the address bar, when the default gateway address is not configured to the PC.
  - A URL ("www.silextechnology.com", etc.) is entered to the address bar when the name resolution is disabled (DNS server address is not registered or NetBIOS is disabled).

4. Click **Easy Configuration** at the top of the page.
Select the destination network from **Wireless Network List** and enter the WEP Key or Shared Key for **Network Key**.
Click **Submit** when finished.

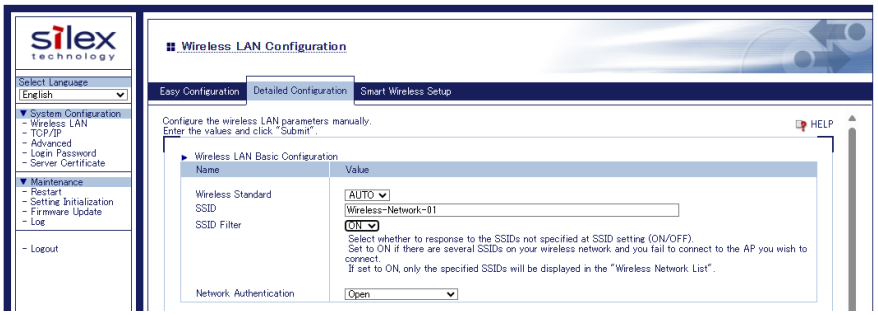


Note

- For network key, usable characters will differ depending on the AP to connect.
- For WEP key, enter 5 or 13 characters or 10 or 26 digit hexadecimal value. For details, refer to **WEP Key 1-4** at **A-1. List of All Settings**.
- For Pre-Shared key, enter 8-63 characters or 64 hexadecimal value. For details, refer to **Pre-Shared Key** at **A-1. List of All Settings**.
- To connect multiple network devices using an Ethernet HUB, click **Advanced** and select **Multi-Client Mode** for **Client Mode**.



- If the Access Point is operating in a stealth mode, it is not displayed at **Wireless Network List**. In such a case, click **Detailed Configuration** on the top, enter the detailed setting information of the Access Point and click **Submit**. For details on each setting, please refer to the HELP on Web configuration interface.
- To use the IEEE802.1X authentication, click **Detailed Configuration** on the top, enter the detailed setting information of the Access Point and click **Submit**. For details on each setting, please refer to the HELP on Web configuration interface.
- Up to 32 Access Points can be displayed at **Wireless Network List**.
- If the Access Point you wish to connect is not displayed in the list, you may have reached the maximum number of wireless devices that BR-500AC can detect and show in the list. In that case, use the SSID filter to display the necessary Access Point only.
  To use the SSID filter, click **Detailed Configuration** on the top, enter the SSID of the Access Point you wish to connect, select **ON** at **SSID Filter** and click **Submit**. The SSID filter will become active after the PC is restarted.



Note

- If the **Detailed Configuration** tab is not displayed, click **Wireless LAN** from the page menu.

5. When the confirmation message is displayed, click **Restart** to restart BR-500AC.

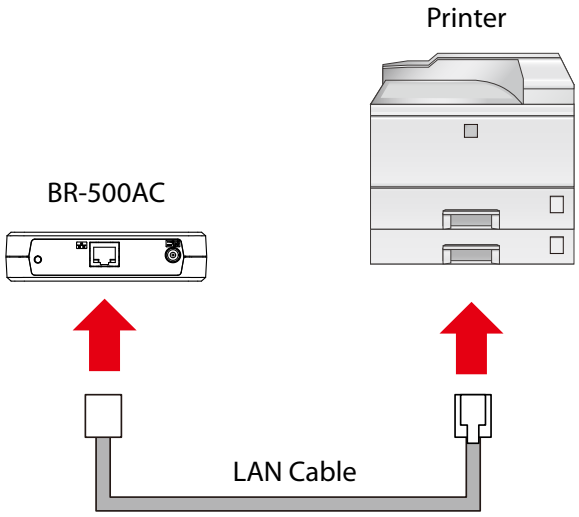
6. BR-500AC is restarted to take effect of the new setting.
The configuration has been completed.

When you wish to bridge the PC used for this configuration wirelessly, restart the PC.
To bridge another device wirelessly, turn off both BR-500AC and PC, remove the BR-500AC from the PC and connect the BR-500AC to the device you wish to use wirelessly using a LAN cable. For details, refer to **Connecting Non-wireless Devices** in the next page.

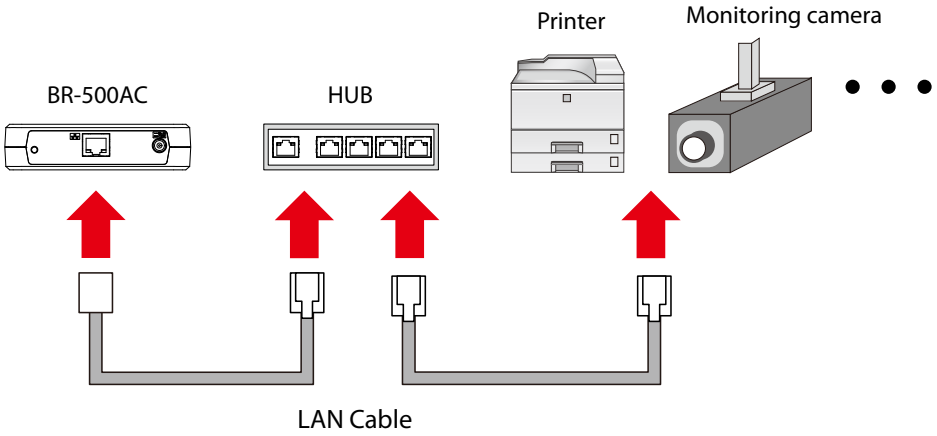
Connecting Non-wireless Devices

1. Turn off the non-wireless device that you wish to use wirelessly and connect the BR-500AC to it using a LAN cable. The connection method will vary depending on each operating mode.

How to Connect in Single Client Mode



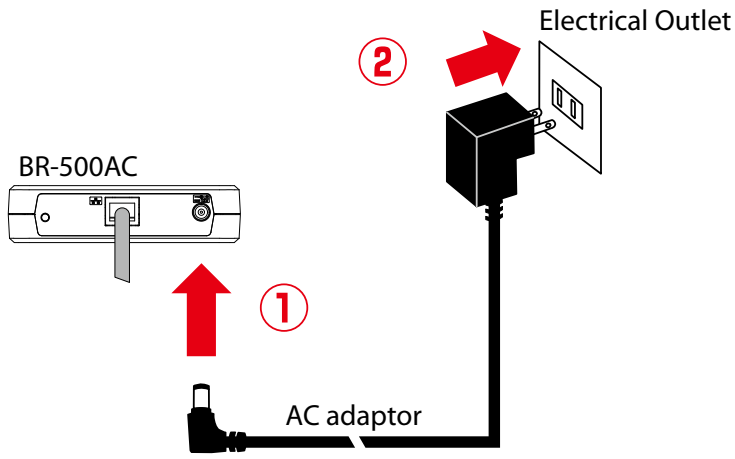
How to Connect in Multi-Client Mode



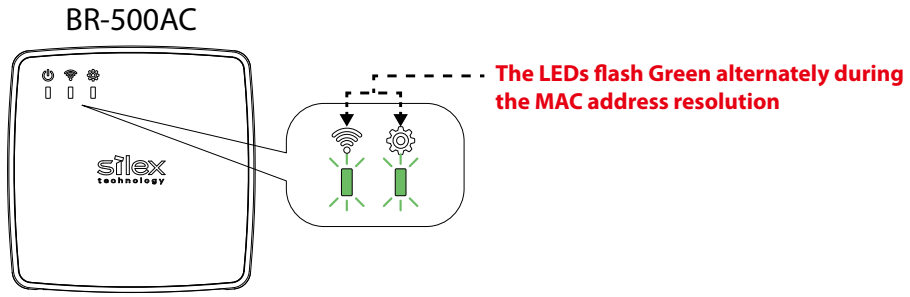
Note

- For details on each operating mode, refer to **3-1. Operating Mode**.

2. Connect the AC adaptor to the BR-500AC and the AC plug to the outlet.



3. Turn on the non-wireless device connected to the BR-500AC.
During the MAC address resolution, the WLAN LED and STATUS LED will flash green alternately. When the LED status has changed from it, the BR-500AC will be ready to use. You can use the non-wireless device over a wireless network.



Note

- Depending on the non-wireless device you have connected, further network settings may need to be configured to that device. In such a case, please configure it according to the operating manual that came with your device.
- When you turn on the BR-500AC and your non-wireless device, be sure to turn on the BR-500AC first. Do not press the push switch then.

4-3. Configuration Using Smart Wireless Setup (Push Switch)

The wireless settings can be configured easily using the push switch if your Access Point supports WPS(Wi-Fi Protected Setup). How to configure the wireless settings using the push switch is explained below.

- A password needs to be set for BR-500AC beforehand.
- Please check that the Access Point supporting WPS is installed on your network.
- This configuration method is not available if the Access Point is operating in a stealth mode.
- To ensure proper communication during this configuration, please temporarily move the BR-500AC closer to the Access Point.
- The WPS feature may need to be enabled on your Access Point manually. For details, see the operating manual that came with your Access Point.
- If a security feature such as MAC address filtering is enabled on your Access Point, disable it temporarily.
- If the SSID filter is enabled on the BR-500AC when Smart Wireless Setup is executed, the SSID filter function will temporarily be disabled.
- To connect multiple devices using a HUB, use **Multi-Client Mode**. See **5-1. How to Access Web Configuration Interface** to change the operating mode.

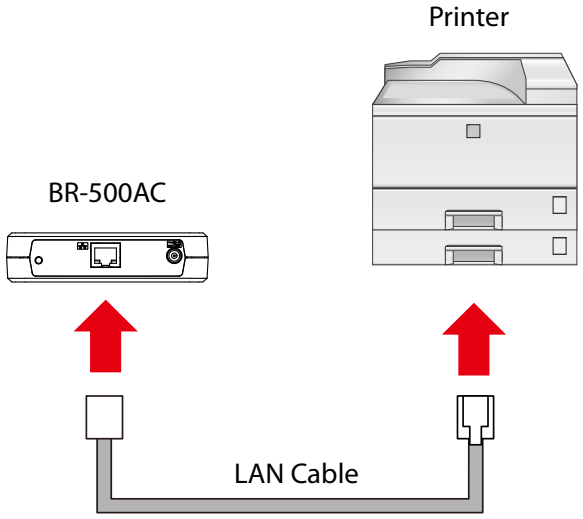
Configuration

When the operating mode is **Single Client Mode**, you need to connect a non-wireless device to the BR-500AC in order to start the configuration.
When the operating mode is **Multi-Client Mode**, you do not have to connect a non-wireless device. In such a case, start from **2** in this section.

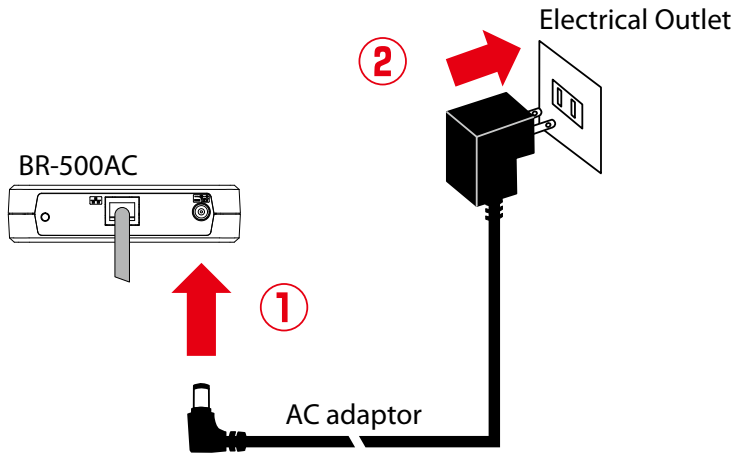
Note

- By defaults, the operating mode is set to **Single Client Mode**.
- To see which operating mode your BR-500AC is running on, start the BR-500AC in the Configuration Mode and access the Web page.

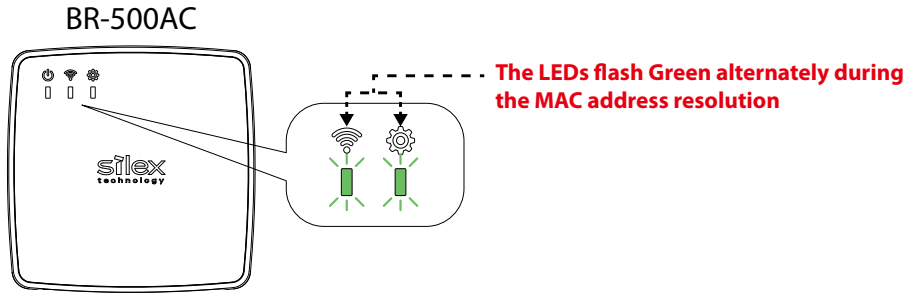
1. Turn off the non-wireless device that you wish to use wirelessly and connect the BR-500AC to it using a LAN cable.



2. Connect the AC adaptor to the BR-500AC and the AC plug to the outlet.



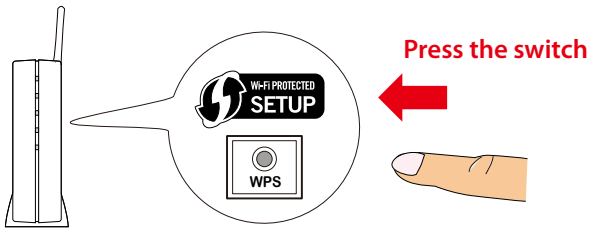
3. Turn on the non-wireless device connected to the BR-500AC.
During the MAC address resolution, the WLAN LED and STATUS LED will flash green alternately. When the LED status has changed from it, the BR-500AC will be ready to configure using Smart Wireless Setup.



Note

- Depending on the non-wireless device you have connected, further network settings may need to be configured to that device. In such a case, please configure it according to the operating manual that came with your device.
- When you turn on the BR-500AC and your non-wireless device, be sure to turn on the BR-500AC first. Do not press the push switch then.

4. Press the WPS button on your Access Point.
Confirm that your Access Point is ready for a wireless connection to be made.

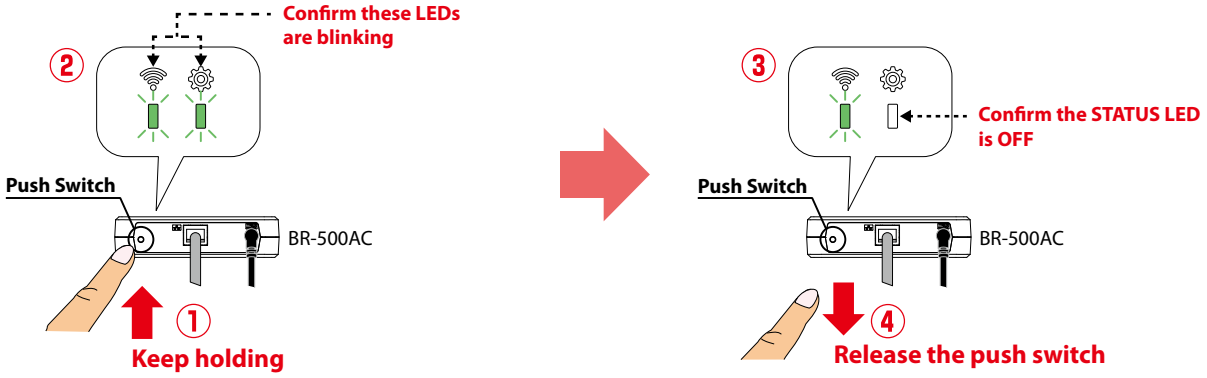


Access Point

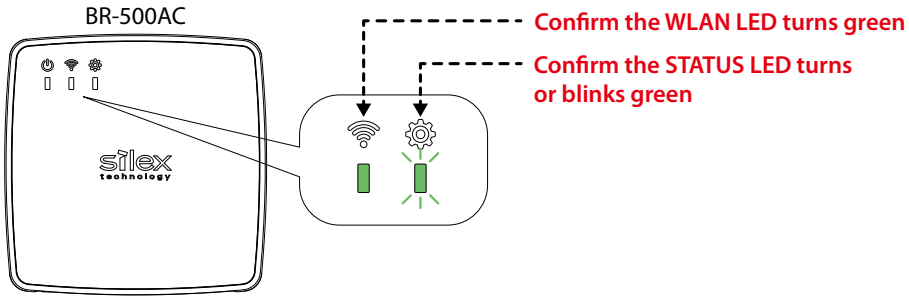
Note

- The name, position and shape of the WPS button will differ depending on your Access Point. For details, refer to the operation manual that came with your Access Point.
- Please use only one Access Point. If two or more Access Points are waiting for wireless connections, BR-500AC will not be able to connect properly.

5. Press and hold the push switch at the front of BR-500AC. The WLAN LED and STATUS LED will start to blink green together.
In 5 seconds, the WLAN LED will continue to blink while the STATUS LED will turn off.
Release the push switch then.



6. The BR-500AC and the Access Point will start to communicate each other.
When the configuration finished successfully, the WLAN LED turns green and the STATUS LED turns or blinks green.



Note

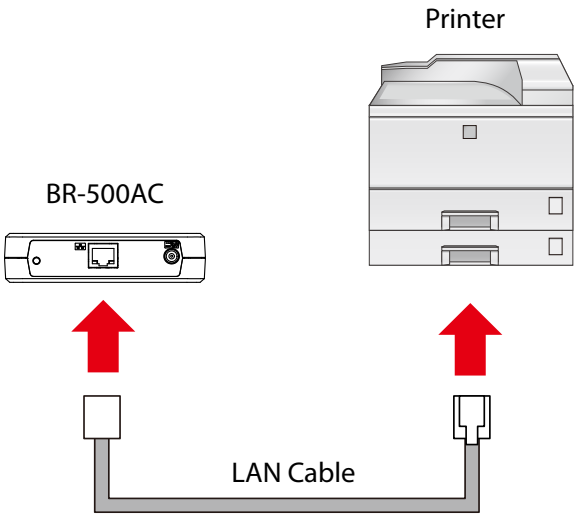
- It may take a while to complete the wireless configuration depending on your environment.
- When wireless configuration has failed, the WLAN LED will flash rapidly.
  In such a case, read the instructions carefully and start from **4** again.

If you plan to use BR-500AC in **Single Client Mode**, you can keep using the connected non-wireless device to use it wirelessly.
To replace it with the other non-wireless device, turn off the BR-500AC and replace the connected non-wireless device to it. See **Connecting Non-wireless Devices** in the next page for how to connect the BR-500AC and non-wireless device using a LAN cable.
To change the operating mode, start the BR-500AC in configuration mode. For details, refer to **5-1. How to Access Web Configuration Interface**.

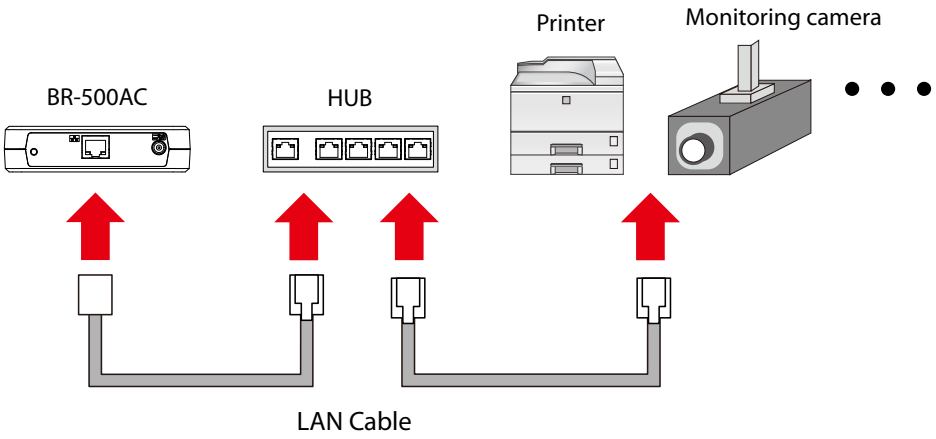
Connecting Non-wireless Devices

1. Turn off the non-wireless device that you wish to use wirelessly and connect the BR-500AC to it using a LAN cable. The connection method will vary for each operating mode.

How to Connect in Single Client Mode



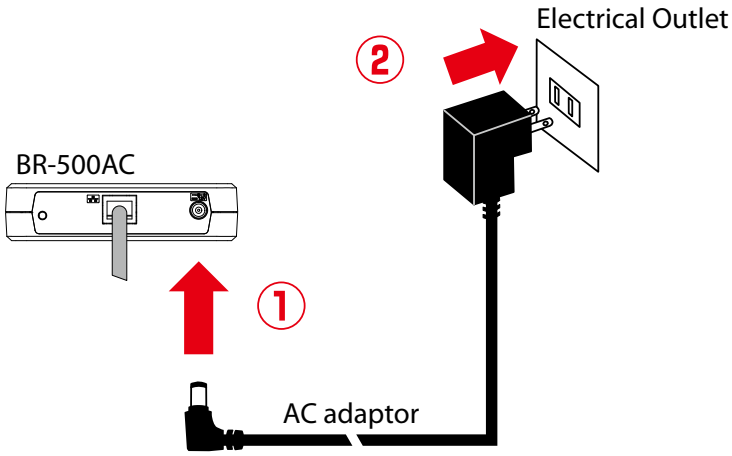
How to Connect in Multi-Client Mode



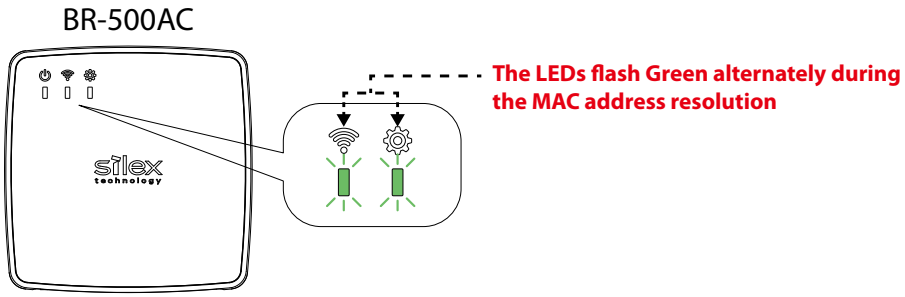
- For details on each operating mode, refer to **3-1. Operating Mode**.

Note

2. Connect the AC adaptor to the BR-500AC and the AC plug to the outlet.



3. Turn on the non-wireless device connected to the BR-500AC.
During the MAC address resolution, the WLAN LED and STATUS LED will flash green alternately. When the LED status has changed from it, the BR-500AC will be ready to use. You can use the non-wireless device over a wireless network.



Note

- Depending on the non-wireless device you have connected, further network settings may need to be configured to that device. In such a case, please configure it according to the operating manual that came with your device.
- When you turn on the BR-500AC and your non-wireless device, be sure to turn on the BR-500AC first. Do not press the push switch then.

4-4. Configuration Using Smart Wireless Setup(PIN Code)

The wireless settings can be configured easily using the PIN code when your Access Point supports WPS(Wi-Fi Protected Setup). How to configure the wireless settings using the PIN code is explained below.

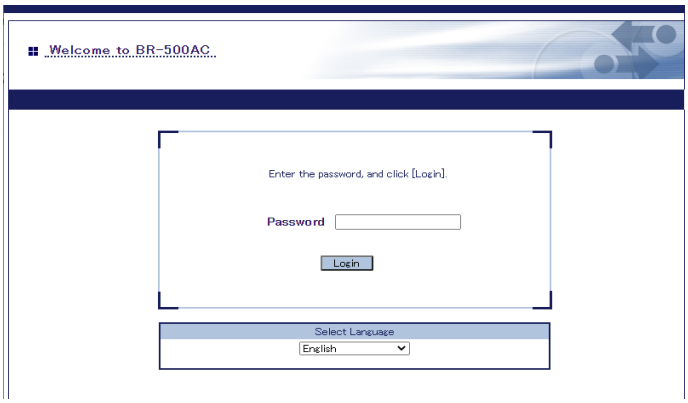
TIP

- A password needs to be set for BR-500AC beforehand.
- Please check that the Access Point supporting WPS is installed on your network.
- This configuration method is not available if the Access Point is operating in a stealth mode.
- To ensure proper communication during this configuration, please temporarily move the BR-500AC closer to the Access Point.
- The WPS feature may need to be enabled on your Access Point manually. For details, see the operating manual that came with your Access Point.
- If a security feature such as MAC address filtering is enabled on your Access Point, disable it temporarily.
- If the SSID filter is enabled on the BR-500AC when Smart Wireless Setup is executed, the SSID filter function will temporarily be disabled.
- To connect multiple devices using a HUB, use **Multi-Client Mode**. See **5-1. How to Access Web Configuration Interface** to change the operating mode.

Checking a PIN Code

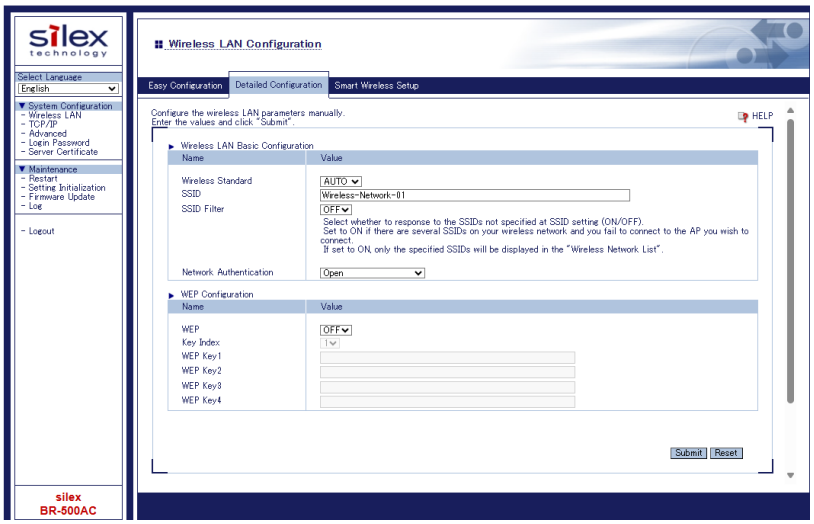
1. Access the Web page of BR-500AC using the Web browser.

2. The login page is displayed.
Enter the password for BR-500AC and click **Login**.



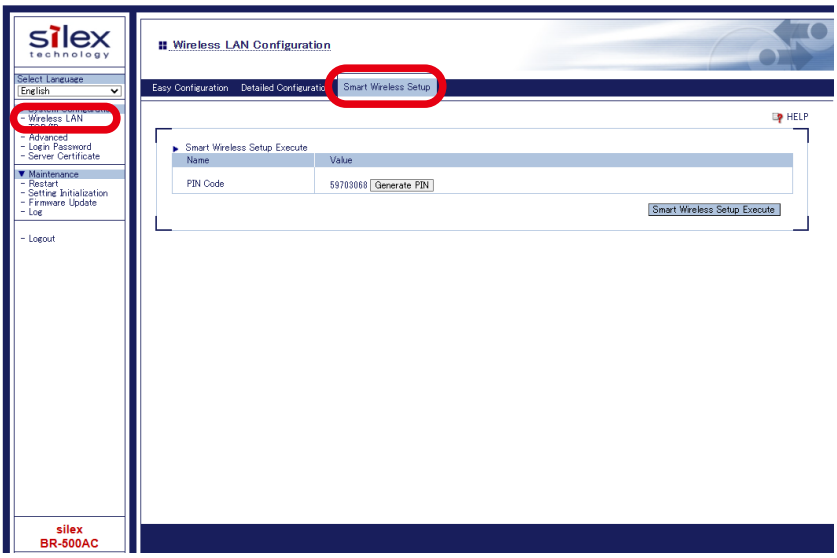
TIP
- If the entered password is incorrect, you will not be able to log in for a certain period of time.
- Be sure to log out the Web page when you have finished using it.

3. The Web page of BR-500AC is displayed.



TIP
- To start the configuration, the PC and BR-500AC need to communicate each other properly.
- Confirm that an IP Address is correctly configured to the PC.
- If a wireless LAN is enabled on your PC, please disable it.
- If a static IP address is set to the PC, the Web configuration interface cannot be displayed in the following cases:
  - An IP address of the different segment is entered to the address bar, when the default gateway address is not configured to the PC.
  - A URL ("www.silextechnology.com", etc.) is entered to the address bar when the name resolution is disabled (DNS server address is not registered or NetBIOS is disabled).

4. In the Web configuration interface, click **Wireless LAN** - **Smart Wireless Setup** and check the PIN code. Keep this screen displayed as it will be used again at **Configuration** in the next page. Do not click the **Smart Wireless Setup Execute** yet.



TIP

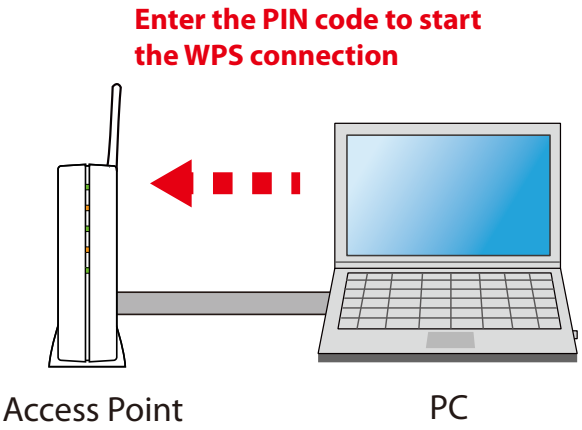
- Do not click the **Smart Wireless Setup Execute** yet.
  It will need to be clicked at **Configuration** in the next page.

Note

- To change the PIN code, click the **Generate PIN**. A new PIN code will be generated automatically.

Configuration

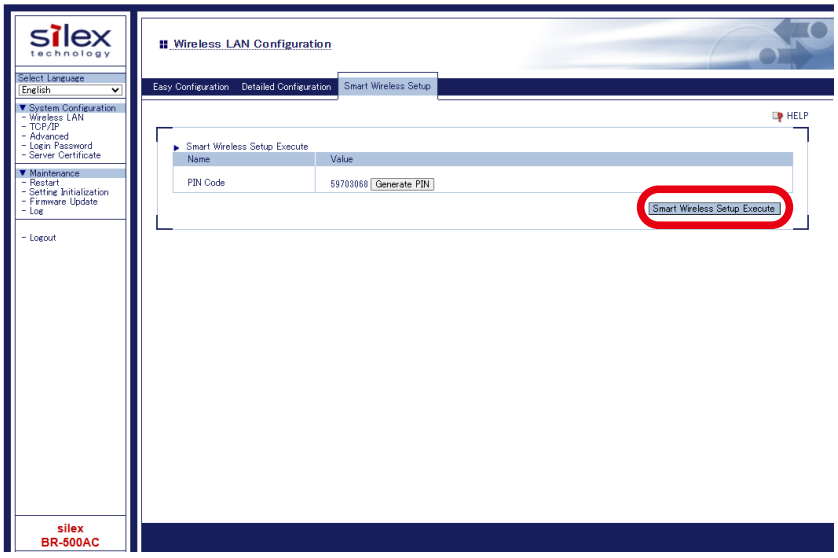
1. Access the configuration interface of the Access Point. Enter the PIN code and start the WPS connection from the Access Point.



Note

- The method to enter the PIN code on Access Point will differ depending on each Access Point. For details, refer to the operating manual that came with your Access Point.

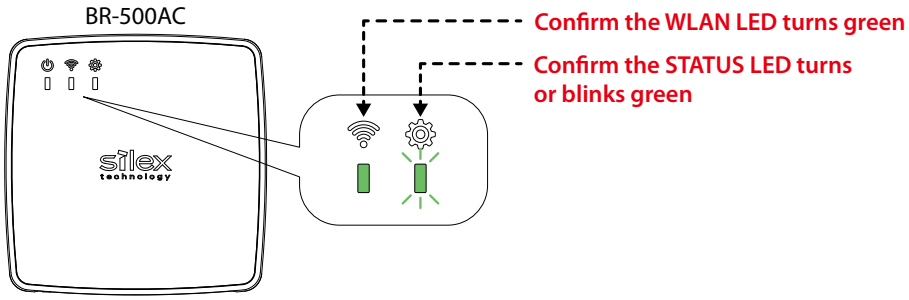
2. Go back to the **Smart Wireless Setup** page of the BR-500AC and click the **Smart Wireless Setup Execute**.



TIP

- If Smart Wireless Setup is started on the BR-500AC earlier than the Access Point, the configuration may fail.

3. The BR-500AC and the Access Point will start to communicate each other.
The wireless configuration is successfully completed when the WLAN LED turns green and the STATUS LED turns or blinks green.



Note

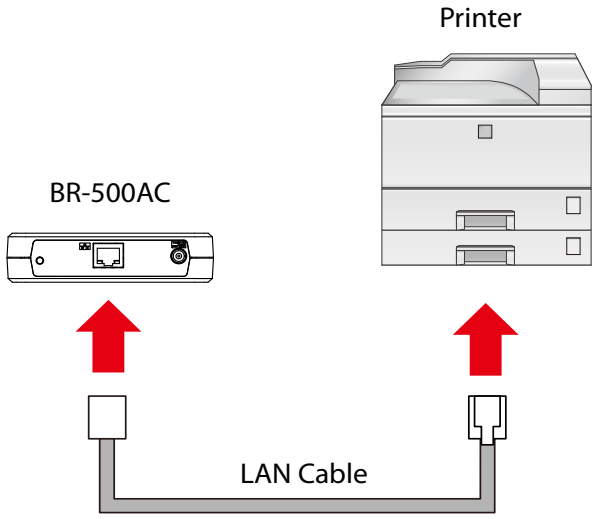
- It may take up to 2 min to finish the wireless configuration depending on your environment.
- When wireless configuration has failed, the WLAN LED will flash rapidly.
  In such a case, read the **TIP** at the beginning of **4-4. Configuration Using Smart Wireless Setup(PIN Code)** and try again.
- To change the PIN code, see **Checking a PIN Code**.

If you plan to use the PC wirelessly (the one you have been using for this configuration), restart the PC. To use the other non-wireless device wirelessly, turn off the BR-500AC and the PC, and connect the BR-500AC to the non-wireless device using a LAN cable. For details, refer to **Connecting Non-wireless Devices** in the next page.

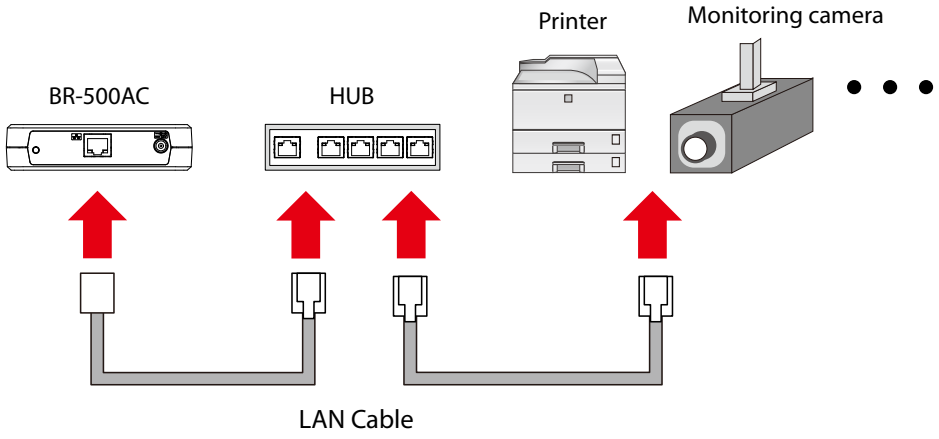
Connecting Non-wireless Devices

1. Turn off the non-wireless device that you wish to use wirelessly and connect the BR-500AC to it using a LAN cable. The connection method will vary for each operating mode.

How to Connect in Single Client Mode



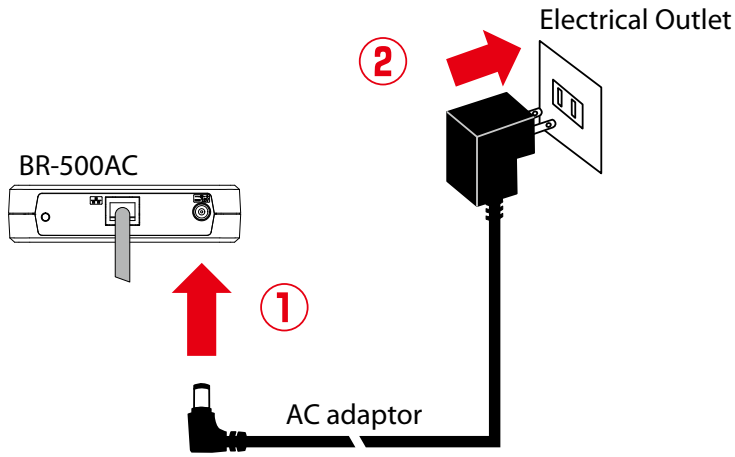
How to Connect in Multi-Client Mode



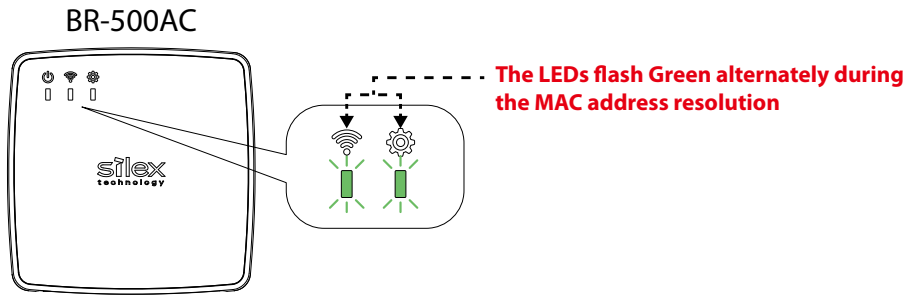
Note

- For details on each operating mode, refer to **3-1. Operating Mode**.

2. Connect the AC adaptor to the BR-500AC and the AC plug to the outlet.



3. Turn on the non-wireless device connected to the BR-500AC.
During the MAC address resolution, the WLAN LED and STATUS LED will flash green alternately. When the LED status has changed from it, the BR-500AC will be ready to use. You can use the non-wireless device over a wireless network.



Note

- Depending on the non-wireless device you have connected, further network settings may need to be configured to that device. In such a case, please configure it according to the operating manual that came with your device.
- When you turn on the BR-500AC and your non-wireless device, be sure to turn on the BR-500AC first. Do not press the push switch then.

5. List of Functions

This chapter explains the BR-500AC functions.

5-1. How to Access Web Configuration Interface

The Web page of BR-500AC can be accessed by one of the following methods.
Make sure that the configuration is performed when BR-500AC is directly connected to the PC or used on a secure network.

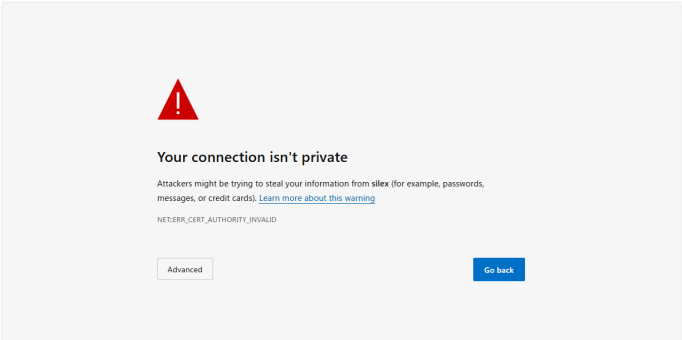
Access the Web page using the IP address

Enter **https://[IP address of BR-500AC]** in the address bar of your Web browser and press the Enter key.

Access the Web page using the Configuration Mode

Start BR-500AC in the Configuration Mode. For details, refer to **4-1. Starting Configuration Mode for Password Settings** - **Starting BR-500AC in Configuration Mode**.
The Web browser will launch and display the BR-500AC's Web page.
If the Web browser does not launch automatically, enter **https://silex** in the address bar, and then press the Enter key to display it manually.

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



TIP

- When a NAT function is used, configuration via the BR-500AC's Web page must not be done through the router.

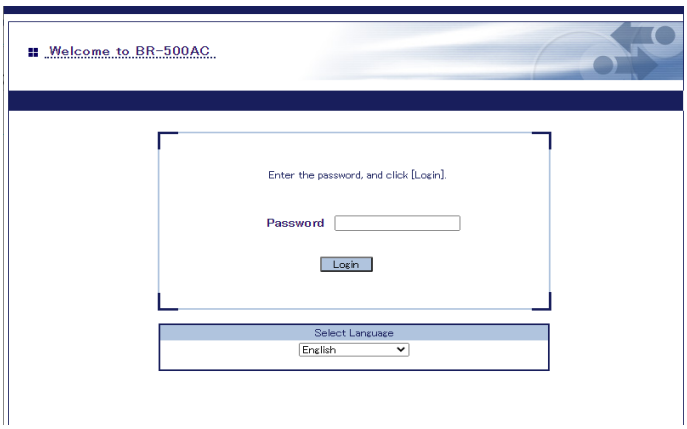
Note

- The IP address of BR-500AC can be identified using AMC Manager®.
- For how to download AMC Manager®, refer to **A-3. What's AMC Manager®?**.
- The display of warning screen may differ depending on the Web browser and its version.

Configuration via Web Configuration Interface

1. Access the Web page of BR-500AC using the Web browser.

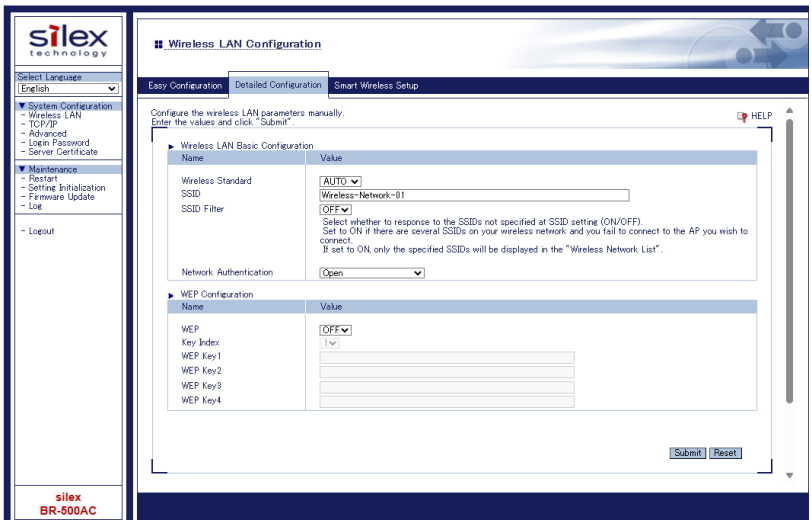
2. The Web browser is started and the login page of BR-500AC is displayed.
Enter the password for BR-500AC and click **Login**.



TIP

- Recommended Web browsers: Microsoft Edge / Safari.
- If a static IP address is set to the PC, the Web configuration interface cannot be displayed in the following cases:
  - An IP address of the different segment is entered to the address bar, when the default gateway address is not configured to the PC.
  - A URL ("www.silextechnology.com", etc.) is entered to the address bar when the name resolution is disabled (DNS server address is not registered or NetBIOS is disabled).
- If the entered password is incorrect, you will not be able to log in for a certain period of time.
- Be sure to log out the Web page when you have finished using it.

3. The Web configuration interface of BR-500AC is displayed. In the Web configuration interface, the operating mode, wireless setting, etc. can be changed.



- BR-500AC needs to be restarted for changes to take effect.

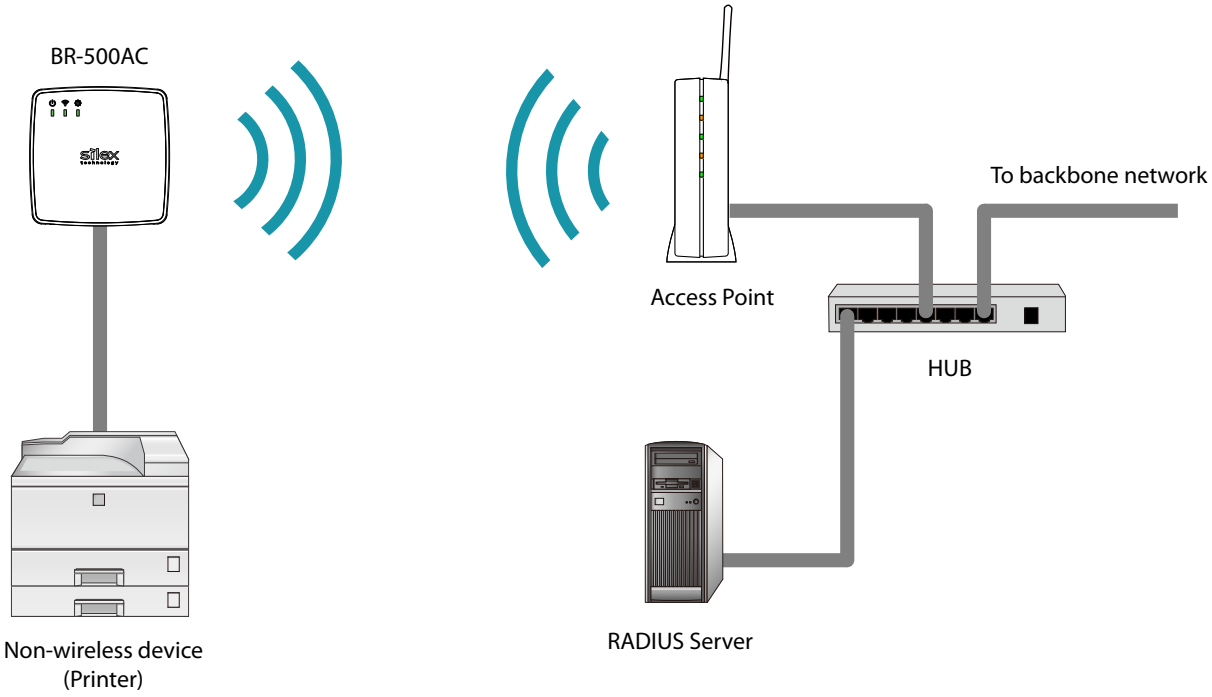
Note

5-2. IEEE802.1X Authentication

BR-500AC supports the IEEE802.1X authentication.
To use the IEEE802.1X authentication, a RADIUS server is needed.

Network Configuration

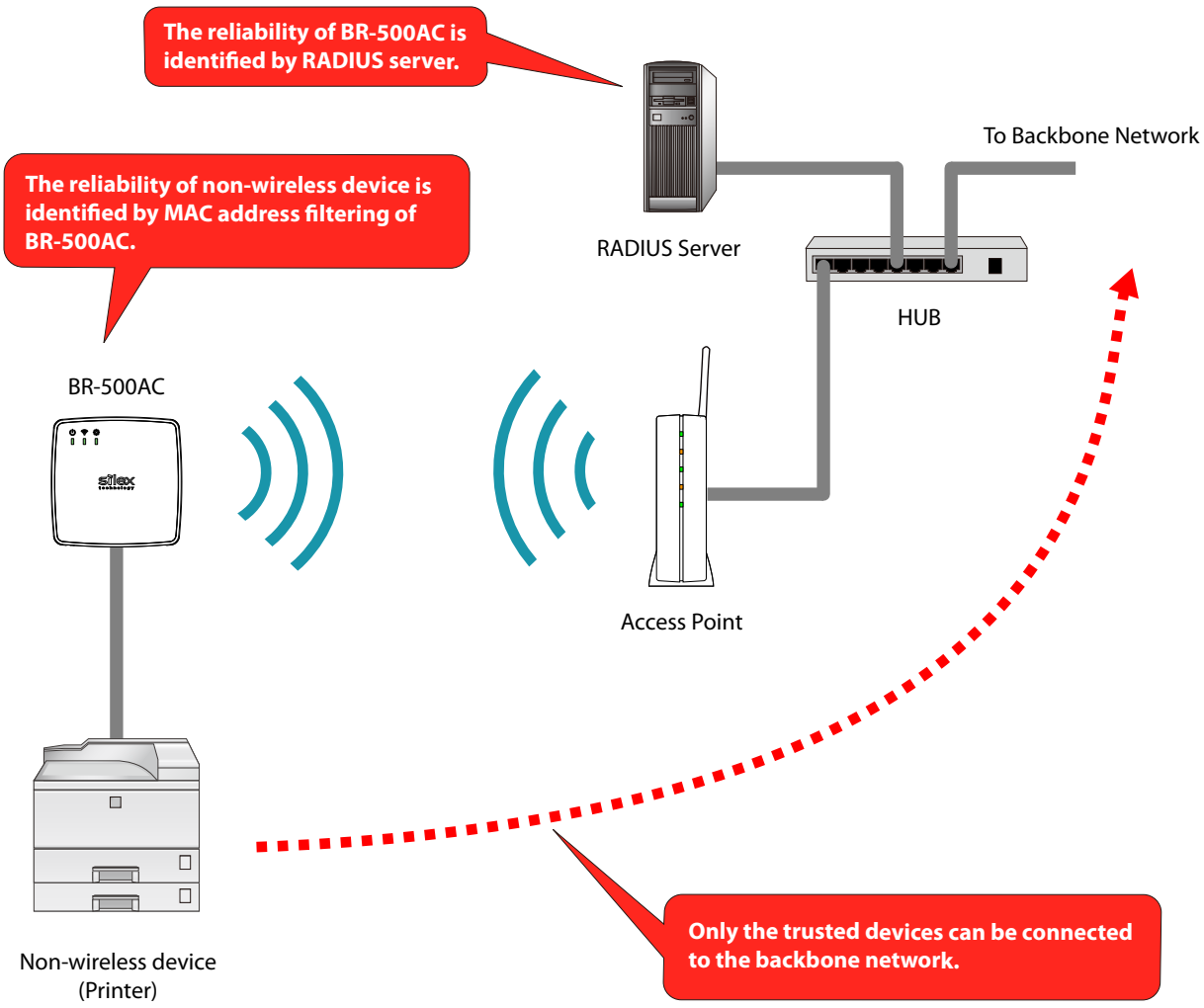
Connect the BR-500AC to a network as below when you use the IEEE802.1X authentication. The RADIUS server identifies the reliability of BR-500AC as an authentication host, while BR-500AC identifies the reliability of RADIUS server as an authentication client to identify the reliability of the network to connect to.



When using the authentication method that requires a certificate, get the necessary certificate issued by the certificate authority and import it to the BR-500AC.
To use this function, register the MAC address of non-wireless device with BR-500AC. The reliability of non-wireless devices connected to BR-500AC is identified using the MAC address filtering.

TIP

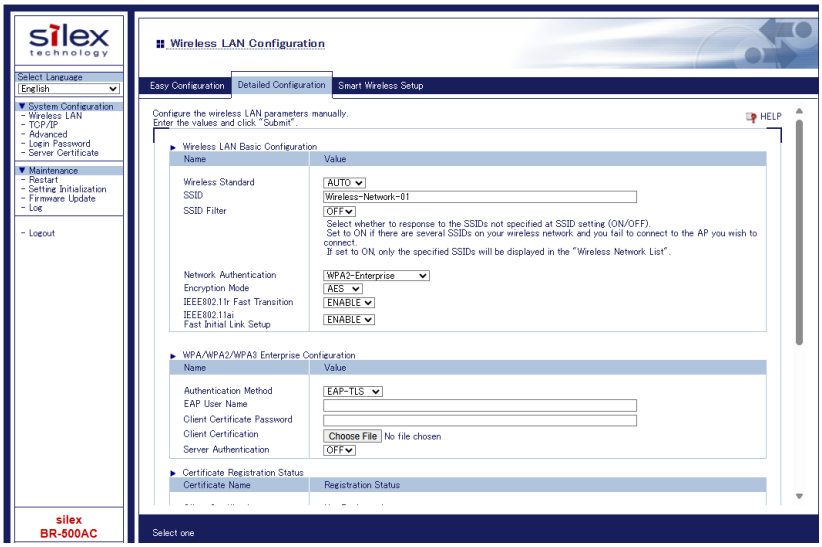
- IEEE802.1X authentication is supported only for wireless network.


The reliability of BR-500AC is identified by RADIUS server.
To Backbone Network
The reliability of non-wireless device is identified by MAC address filtering of BR-500AC.
RADIUS Server
HUB
BR-500AC
Access Point
Non-wireless device (Printer)
Only the trusted devices can be connected to the backbone network.

IEEE802.1X Authentication

BR-500AC supports the following IEEE802.1X authentication methods.
These can be set using the Web page.

IEEE802.1X Authentication mode
EAP-TLS
EAP-TTLS
PEAP
EAP-FAST
LEAP



Settings on each authentication mode

The compatible settings on each authentication mode are as follows.
For details, refer to **Appendix A-1. List of All Settings**.

Name	IEEE802.1X Authentication Mode				
	EAP-TLS	EAP-TTLS	PEAP	EAP-FAST	LEAP
EAP User Name	Necessary	Necessary	Necessary	Necessary	Necessary
EAP Password	-	Necessary	Necessary	Necessary	Necessary
Inner Authentication Method	-	Necessary	Necessary	-	-
Server Authentication	Optional	Optional	Optional	-	-
CA Certificate	(*1)	(*1)	(*1)	-	-
Auto PAC Provisioning	-	-	-	Optional	-
PAC File Distribution	-	-	-	(*2)	-
PAC Password	-	-	-	(*2)	-
Client Certification	Necessary	-	-	-	-
Client Certificate Password	Optional	-	-	-	-

Note	(*1) Necessary when the Server Authentication is ON. (*2) Necessary when the Auto PAC Provisioning is OFF.

Name	Details
EAP User Name	This is an ID and password for the RADIUS server to identify the client.
EAP Password	
Inner Authentication Method	Specify the authentication protocol to use. For PEAP, MSCHAPv2 is used.
Server Authentication	Enable(ON) / Disable(OFF) the reliability check of the RADIUS server. When ON is selected, CA certificate is required to verify the server certificate.
CA Certificate	This is a CA certificate to authenticate the RADIUS server.
Auto PAC Provisioning	Enable(ON) / Disable(OFF) the automatic PAC distribution. When OFF is selected, the PAC file generated by the RADIUS server is required.
PAC File Distribution	This is the file used for manual provisioning. This file is generated by the RADIUS server. To analyze a password-set PAC file, you need the password.
PAC Password	
Client Certification	Use this to check the client reliability. To read out the secret key from the client certificate, a password is required.
Client Certificate Password	

- Please create the client certificate and the CA certificate separately. BR-500AC does not support the certificate composed of multiple certificate files.

Certificate Standard

When using the authentication mode which uses a certificate, get the necessary certificate issued from the certificate authority and import it to the BR-500AC.
The BR-500AC supports the following certificates:

Certificate Standard

The certificate supports the standards as follows:

Certificate	Item	Compatible standards
Client certificate	X509 certificate version	v3
	Public key algorithm	RSA
	Public key size	512bit, 1024bit, 2048bit, 4096bit
	Signature algorithm	SHA1/SHA2(SHA-224,SHA-256,SHA-384,SHA-512) withRSA MD5withRSA
	X509v3 extended key usage	Client authentication (1.3.6.1.5.5.7.3.2)
CA certificate	Public key algorithm	RSA
	Public key size	512bit, 1024bit, 2048bit, 4096bit
	Signature algorithm	SHA1/SHA2(SHA-224,SHA-256,SHA-384,SHA-512) withRSA MD5withRSA

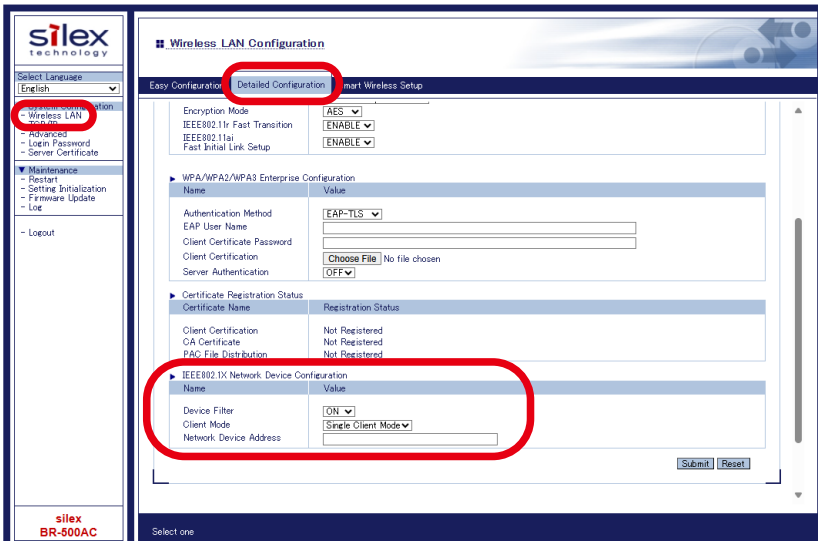
Certificate Saving Format

The following saving formats are supported:

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

MAC Address Filtering

When the IEEE802.1X authentication is used, access to the BR-500AC from non-wireless devices needs to be controlled so that access from unauthorized devices can be blocked. Check the MAC address of non-wireless device to allow an access, and register it to the Web page of BR-500AC.



Before Using the IEEE802.1X Authentication

In order to use the IEEE802.1X authentication on BR-500AC, the information below will be required.

(1) User name and password to access the RADIUS server

To access the RADIUS server, the user name and password are required. Also, when using the authentication method that requires a certificate, the certificate file will be needed.

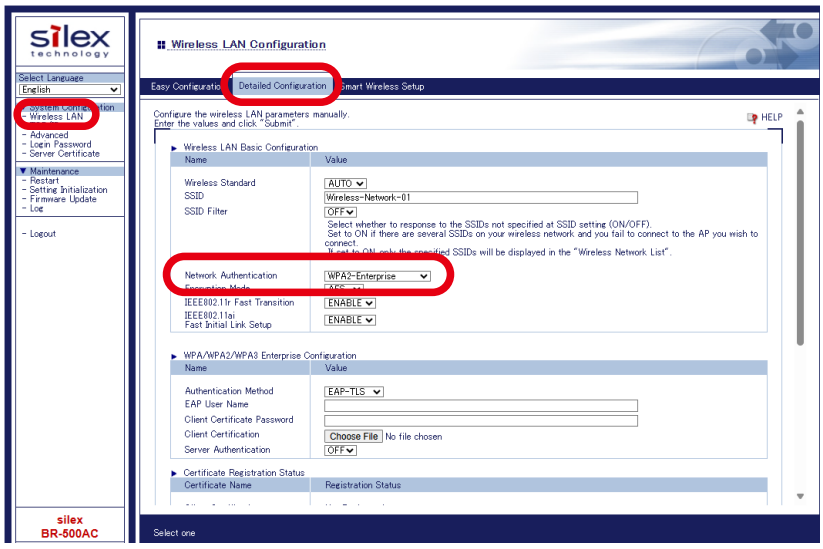
(2) MAC address of the non-wireless device

BR-500AC allows bridging only for those with the registered MAC address. The MAC address information is required to allow them to be bridged using BR-500AC.

IEEE802.1X Authentication Settings

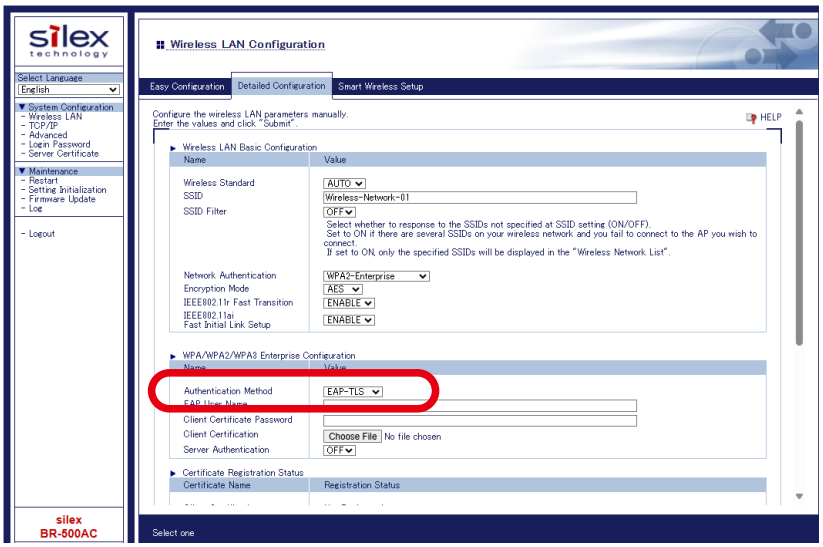
How to configure the IEEE802.1X authentication setting is explained.
To use the authentication method that requires a certificate, import the certificate file.

1. In the Web configuration interface of the BR-500AC, click **Wireless LAN** - **Detailed Configuration**.
In the **Detailed Configuration** page, select one of the followings for **Network Authentication**.
- WPA2-Enterprise
- WPA3-Enterprise
- WPA/WPA2-Enterprise



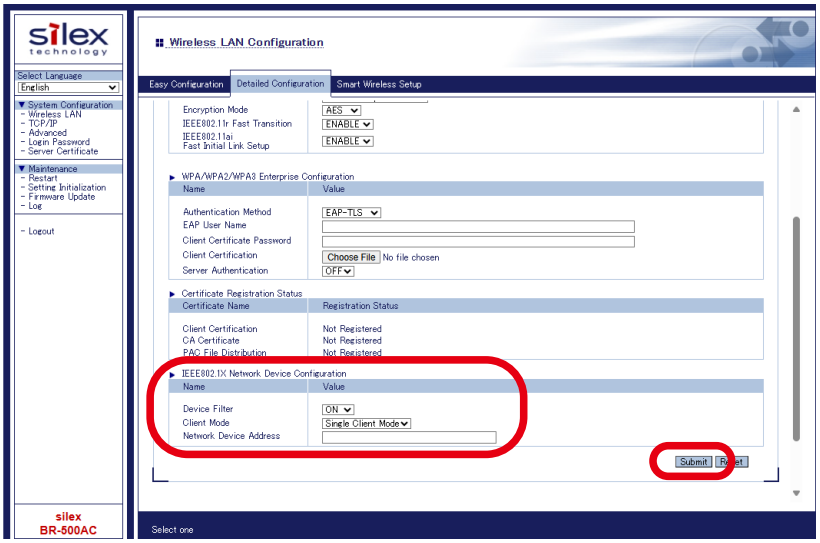
2. Select one of the followings for **Authentication Method**.

- EAP-TLS
- EAP-TTLS
- PEAP
- EAP-FAST
- LEAP



* Settings will vary depending on the IEEE802.1X authentication mode you select.

3. Enter the MAC address of the non-wireless device (the one you want to use wirelessly using BR-500AC) to **Network Device Address** under **IEEE802.1X Network Device Configuration**, and click **Submit**.



TIP

- When the IEEE802.1X authentication is used, access to the BR-500AC from non-wireless devices needs to be restricted so that access from unauthorized devices can be blocked.
- The BR-500AC bridges only the devices whose MAC address is registered to **Network Device Address**. Check the MAC address of the non-wireless device to bridge and register it to **Network Device Address**.
- Please configure this even when you connect only one non-wireless device in a **Single Client Mode**.
- In **Multi-Client Mode**, register the MAC addresses of all non-wireless devices connected to the BR-500AC (up to 16 addresses).

Note

- The following MAC addresses cannot be used for this setting:
  - Broadcast address
  - Multicast address
  - The address composed of 12 zeros
  - Duplicated address (when operating in Multi-Client Mode)

4. When the confirmation message is displayed, click **Restart** to restart BR-500AC.

5. The BR-500AC will be restarted and the IEEE802.1X authentication will take effect.

The configuration has now been completed.
Turn off the BR-500AC and connect it to the non-wireless device using a LAN cable. Refer to **Connecting Non-wireless Devices** for details.

5-3. Saving Log

BR-500AC can save the operating log.
Once the log is saved, it can be retrieved or deleted from the Web configuration interface.

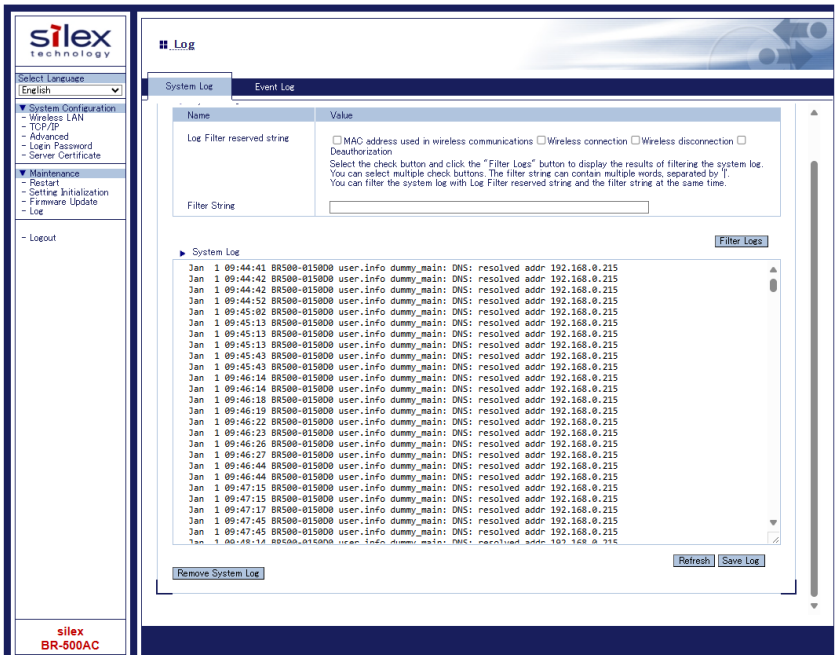
Types of Log

There are two types of log that can be saved by BR-500AC.
Details of each log are as follows.

System Log

Power-on status, operating status, etc. of BR-500AC are saved as a log file.
In case of a network trouble, you can check the operating status by referring the retrieved system logs.

The system log can be viewed or retrieved or deleted from the **System Log** page of Web configuration interface.
By using the log filter, only the specified log can be displayed.



When the system log is saved, the event log and the other files are generated that will include the operating status.

File name		Description
System		Product information
Process		Process information
Client		Client list of the station bridge function
Meminfo		Memory information
log	messages(.x)	system log
	event_log.txt(.x)	event log

Note

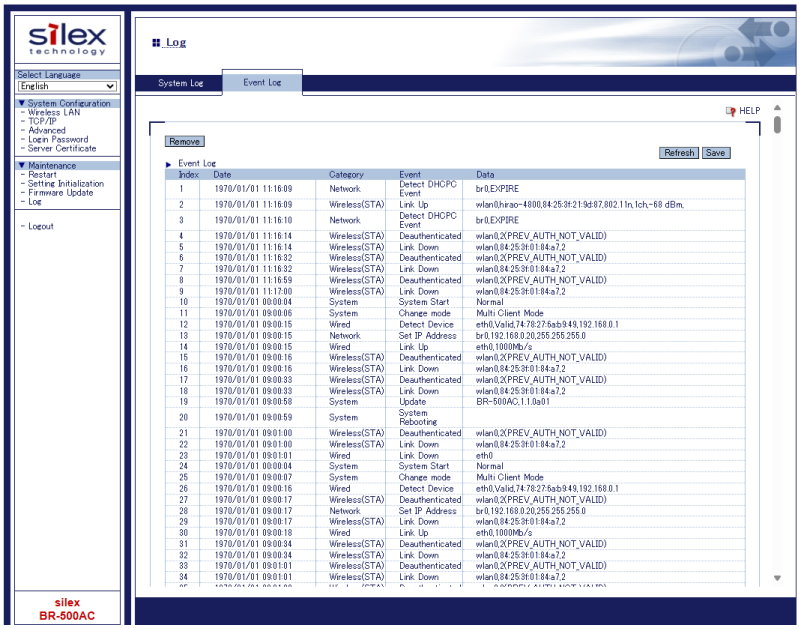
- The system log is saved into the "log" partition of flash memory.
- Each file is 200Kbyte, and 10 rotated files are saved. (Total 11 files (2.2Mbyte) are saved.)

Event Log

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

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

The event log can be viewed or retrieved or deleted from the **Event Log** page of the Web configuration interface.



The event log contains the following information items.

Events other than those listed in this table may also be notified.

Category	Events	Added information	Description
System	System Start		BR-500AC started.
	System Rebooting		BR-500AC restarted.
	Update	Model Name, Version Information	Firmware update was executed.
	Initialize		Setting was initialized.
	Change mode	Single Client Mode	BR-500AC operated in Single Client Mode.
		Multi Client Mode	BR-500AC operated in Multi-Client Mode.
		Setting Mode	BR-500AC operated in Configuration Mode.
		Smart Wireless Setup	Smart Wireless Setup was executed.
		Kitting Mode	BR-500AC operated in kitting mode.
		Find Ethernet Address	When Single Client Mode is on, BR-500AC started to detect the MAC address of the connected wired LAN devices.
	Error	Wired LAN	Wired LAN port error occurred.
		Wireless LAN module	Wireless LAN module error occurred.

Category	Events	Added information	Description
Network	Set IP Address	IF Name, IP Address, Subnet Mask	IP address was configured.
	Detect DHCPC Event	IF Name, BOUND	IP address was assigned by the DHCP Client.
		IF Name, EXPIRE	A lease period for DHCP Client was expired and the IP address was invalidated.
		IF Name, IPV4LL	DHCP Client set a link-local address.
	Set DNS Resolver	DNS Primary, DNS Secondary	DNS Resolver setting was updated.
Wired	Link Up	IF Name, Link Speed	BR-500AC connected to wired LAN.
	Link Down	IF Name	BR-500AC disconnected from wired LAN.
	Detect Device	IF Name, Invalid, MAC address	Unregistered devices were detected. Single Client : Unregistered device (MAC address) was detected on wired LAN. Multi-Client : Device (MAC address) not registered to the MAC address filter of IEEE802.1X authentication was detected.
		IF Name, Adopt, MAC address	Single Client : BR-500AC set the registered or detected MAC address of the wired LAN device to the bridge interface.
		IF Name, Store, MAC address, IP address	Multi-Client : BR-500AC set the detected MAC address of the wired LAN device to the address table.
		IF Name, Valid, MAC address, IP address	Wired device was detected.
		IF Name, Expired, MAC address, IP address	Wired LAN device information was lost when Multi-Client Mode is on.
Wireless (STA)	Link Up	IF Name, SSID, MAC address of AP, 802.11mode, Channel, Radio Strength, Tx Rate	BR-500AC connected to wireless LAN.
	Link Down	IF Name, MAC address of AP, Reason Code	BR-500AC disconnected from wireless LAN.
	Deauthenticated	IF Name, Reason Code	Deauthenticated packet was received, and wireless connection was disconnected.
Smart Wireless Setup	Success		Smart Wireless Setup finished successfully.
	Overlapped		Smart Wireless Setup failed since multiple APs were detected.
	Timeout		AP was not detected during Smart Wireless Setup.

Note

- The event log is saved into the "log" partition of flash memory.
- Each file is 200Kbyte, and only 1 rotated file is saved. (Total 2 files (400Kbyte) are saved.)

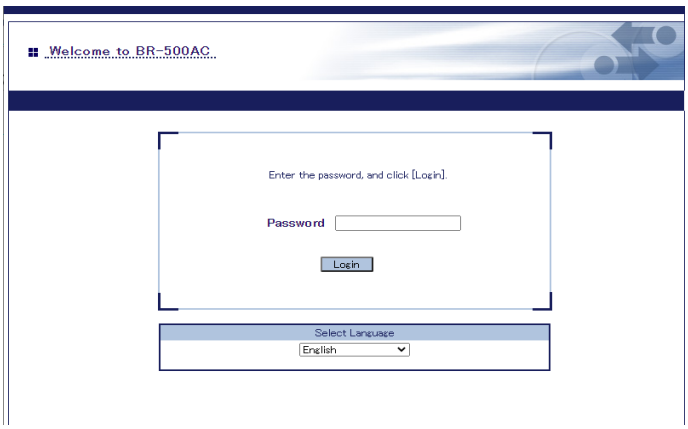
Retrieving/Deleting System Log

How to retrieve system log:

The system log saved on BR-500AC can be accessed from the Web configuration interface.

1. Access the Web page of BR-500AC using the Web browser.

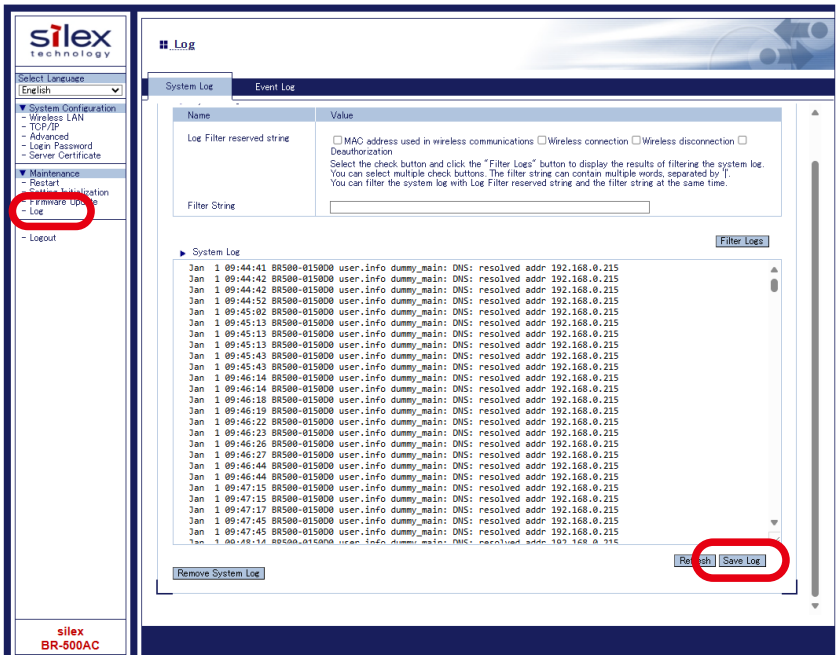
2. The Web browser is started and the login page of BR-500AC is displayed.
   Enter the password for BR-500AC and click **Login**.



TIP

- Recommended Web browsers: Microsoft Edge / Safari.
- To start the configuration, the PC and BR-500AC need to communicate each other properly.
- Confirm that an IP Address is correctly configured to the PC.
- If a wireless LAN is enabled on your PC, please disable it.
- If a static IP address is set to the PC, the Web configuration interface cannot be displayed in the following cases:
  - An IP address of the different segment is entered to the address bar, when the default gateway address is not configured to the PC.
  - A URL ("www.silextechnology.com", etc.) is entered to the address bar when the name resolution is disabled (DNS server address is not registered or NetBIOS is disabled).
- If the entered password is incorrect, you will not be able to log in for a certain period of time.
- Be sure to log out the Web page when you have finished using it.

3. The Web page of BR-500AC is displayed.
Click **Log** and click **Save Log** to save all logs.



TIP
- The log files cannot be saved individually.

4. The message for compressed file of all system logs (sys_log_archive.tgz) appears.
Click **Open file** or "**...**" for the desired option.

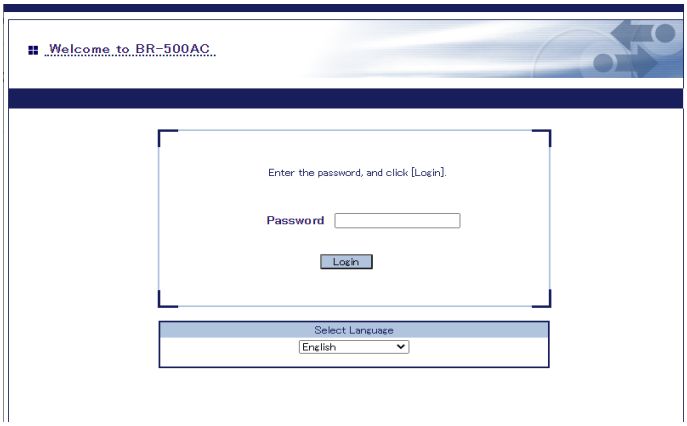
The system log has been saved.

How to delete system log:

The system log saved on BR-500AC can be deleted from the Web configuration interface.

1. Access the Web page of BR-500AC using the Web browser.

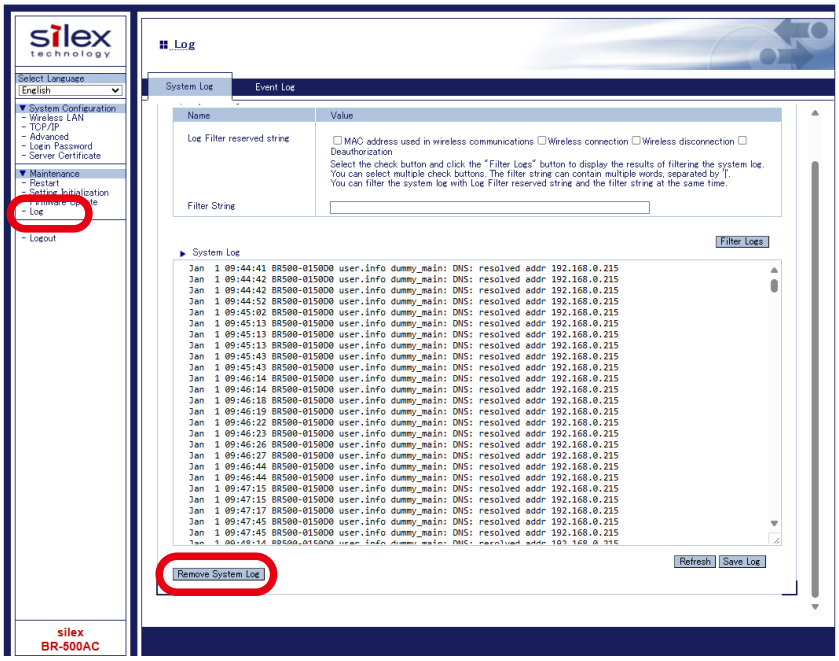
2. The Web browser is started and the login page of BR-500AC is displayed.
   Enter the password for BR-500AC and click **Login**.



TIP

- Recommended Web browsers: Microsoft Edge / Safari.
- To start the configuration, the PC and BR-500AC need to communicate each other properly.
- Confirm that an IP Address is correctly configured to the PC.
- If a wireless LAN is enabled on your PC, please disable it.
- If a static IP address is set to the PC, the Web configuration interface cannot be displayed in the following cases:
  - An IP address of the different segment is entered to the address bar, when the default gateway address is not configured to the PC.
  - A URL ("www.silextechnology.com", etc.) is entered to the address bar when the name resolution is disabled (DNS server address is not registered or NetBIOS is disabled).
- If the entered password is incorrect, you will not be able to log in for a certain period of time.
- Be sure to log out the Web page when you have finished using it.

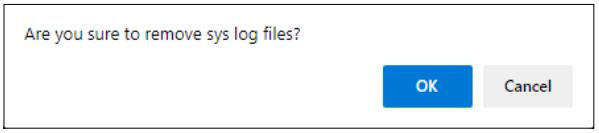
3. The Web page of BR-500AC is displayed.
Click **Log** and click **Remove System Log**.



TIP

- The system log files cannot be deleted individually.

4. When the confirmation dialog is displayed, click **OK**.
All system logs are deleted.



Note

- If **Cancel** is clicked, the system log will not be deleted.

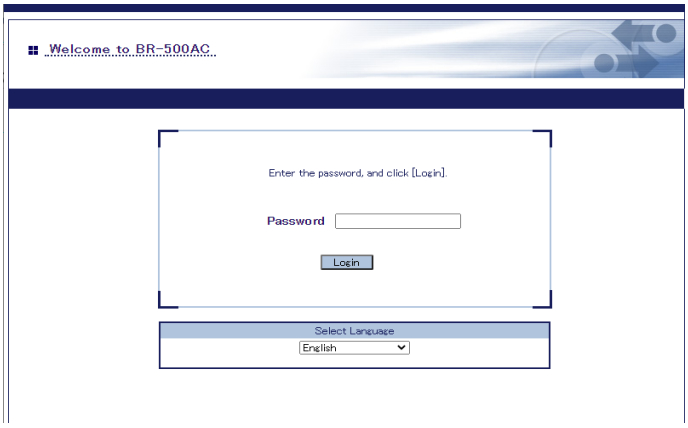
The system log has been deleted.

Retrieving/Deleting Event Log

How to retrieve the event log is explained.
The event log saved on BR-500AC can be accessed from the Web configuration interface.

1. Access the Web page of BR-500AC using the Web browser.

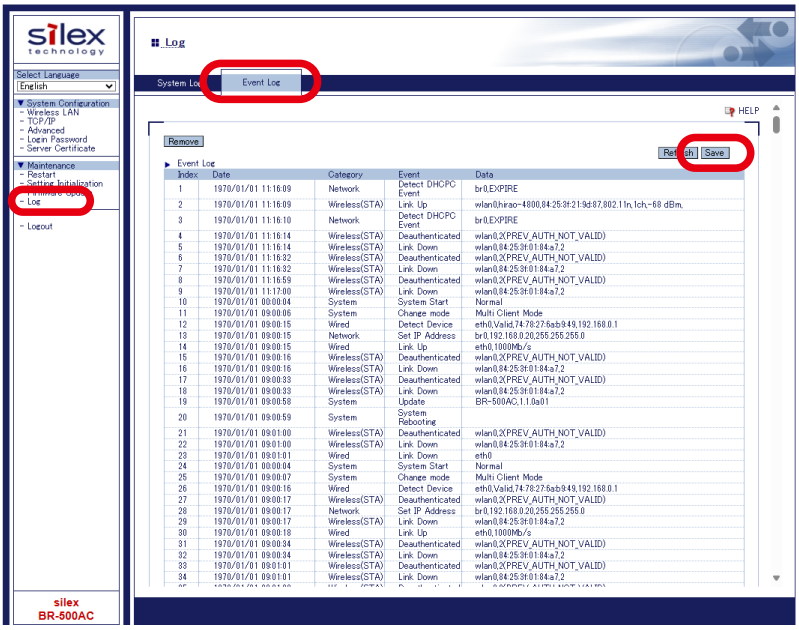
2. The Web browser is started and the login page of BR-500AC is displayed.
Enter the password for BR-500AC and click **Login**.



TIP

- Recommended Web browsers: Microsoft Edge / Safari.
- To start the configuration, the PC and BR-500AC need to communicate each other properly.
- Confirm that an IP Address is correctly configured to the PC.
- If a wireless LAN is enabled on your PC, please disable it.
- If a static IP address is set to the PC, the Web configuration interface cannot be displayed in the following cases:
  - An IP address of the different segment is entered to the address bar, when the default gateway address is not configured to the PC.
  - A URL ("www.silextechnology.com", etc.) is entered to the address bar when the name resolution is disabled (DNS server address is not registered or NetBIOS is disabled).
- If the entered password is incorrect, you will not be able to log in for a certain period of time.
- Be sure to log out the Web page when you have finished using it.

3. The Web page of BR-500AC is displayed.
Click **Log** - **Event Log** and click **Save** to save all logs.



TIP

- The event log can only be saved to one file.

4. The message for event log file appears. Click **Open file** or "**. . .**" for the desired option.

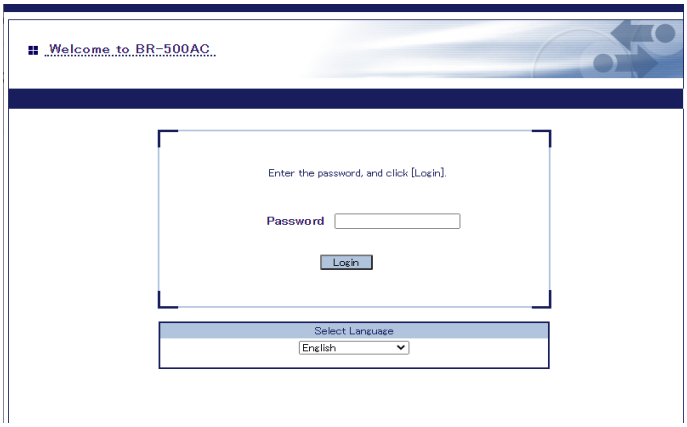
The event log has been saved.

How to delete event log:

The event log saved on BR-500AC can be deleted from the Web configuration interface.

1. Access the Web page of BR-500AC using the Web browser.

2. The Web browser is started and the login page of BR-500AC is displayed.
   Enter the password for BR-500AC and click **Login**.



TIP

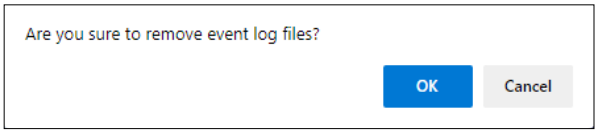
- Recommended Web browsers: Microsoft Edge / Safari.
- To start the configuration, the PC and BR-500AC need to communicate each other properly.
- Confirm that an IP Address is correctly configured to the PC.
- If a wireless LAN is enabled on your PC, please disable it.
- If a static IP address is set to the PC, the Web configuration interface cannot be displayed in the following cases:
  - An IP address of the different segment is entered to the address bar, when the default gateway address is not configured to the PC.
  - A URL ("www.silextechnology.com", etc.) is entered to the address bar when the name resolution is disabled (DNS server address is not registered or NetBIOS is disabled).
- If the entered password is incorrect, you will not be able to log in for a certain period of time.
- Be sure to log out the Web page when you have finished using it.

3. The Web page of BR-500AC is displayed.
Click **Log** - **Event Log** and click **Remove**.

TIP

- The event log cannot be deleted individually.

4. When the confirmation dialog is displayed, click **OK**.
All event logs are deleted.



Note

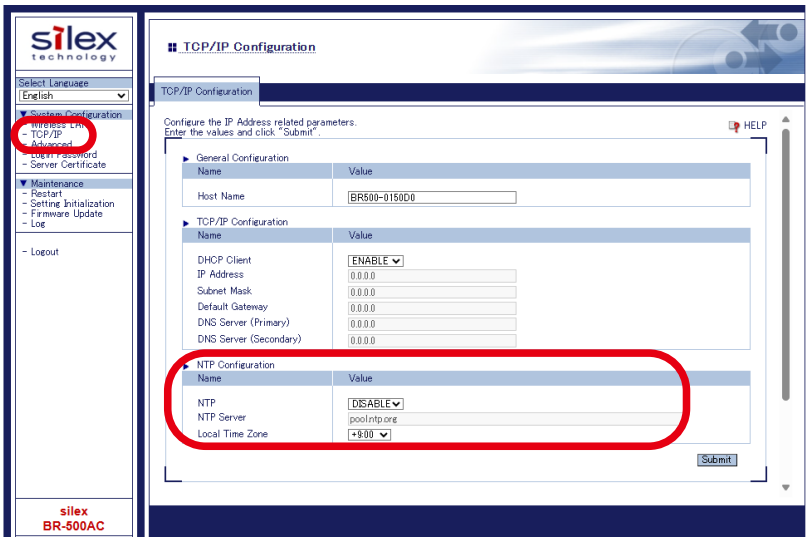
- If Cancel is clicked, the event log will not be deleted.

The event log has been deleted.

Time Synchronization of Log

BR-500AC has the NTP client function. The time of BR-500AC can be synchronized with the NTP server to describe it on the system log and event log.

To configure the NTP setting, open the Web page of BR-500AC and click **TCP/IP** from the menu. The setting can be configured at **NTP Configuration**.



Note

- For how to access the Web page of BR-500AC, refer to **5-1. How to Access Web Configuration Interface**.
- For details on the NTP setting, refer to **A-1. List of All Settings**.

5-4. Address Management Table

In **Multi-Client Mode**, up to 16 non-wireless devices can be shared over network by saving combination of MAC address and IP Address of such devices to BR-500AC.
The combination information is saved automatically when BR-500AC started communication with non-wireless devices, but if the address management table feature is used, it is possible to manually add or delete the combination information.

About Address Management Table Feature

How to register combination of MAC address and IP address will differ depending on whether the address management table feature is enabled or disabled (ON/OFF).
If this feature is ON, the management table information is used for the combination information (MAC address + IP address) of non-wireless devices to connect to BR-500AC.
The addresses are automatically registered to the management table when the devices are added while BR-500AC is active. When this function is OFF, the management table setting is not used.

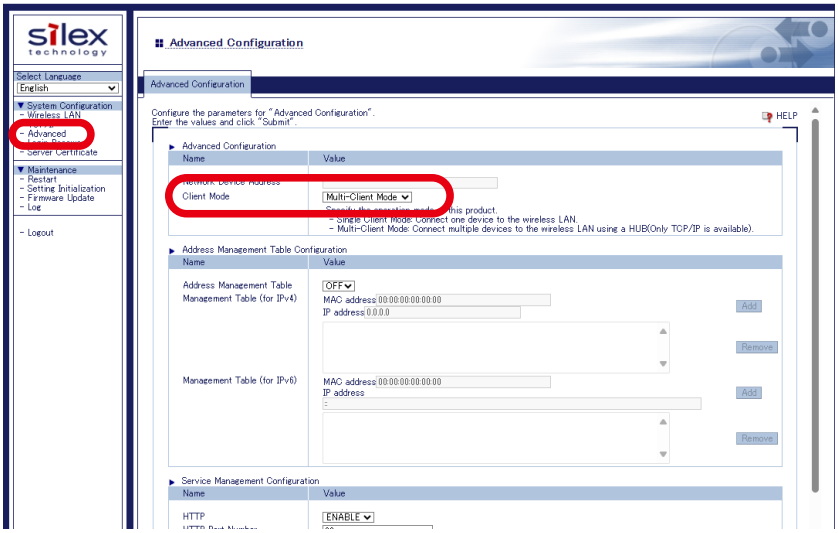
TIP

- Only unicast address is supported for MAC address and IP address.
- BR-500AC checks the existence of device information to save at 5 sec interval. If BR-500AC is turned off before the saving process is completed, the device information is not saved in the address management table.
- Up to 16 sets of combination information can be registered to the management table. If 16 sets of combination information are already registered, new one cannot be added. Delete unnecessary information then.

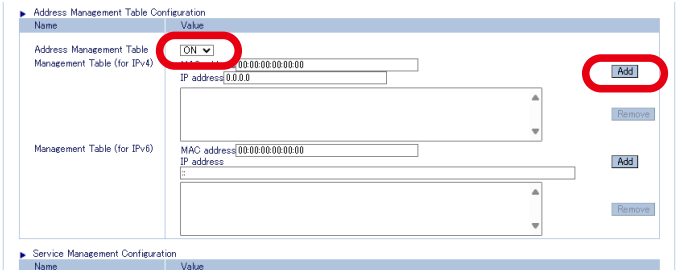
Registering Address to Management Table

Following explains how to register combination of MAC address and IP address to management tables (IPv4/IPv6).

1. In the Web configuration interface of the BR-500AC, click **Advanced**.
Select **Multi-Client Mode** for **Client Mode**.



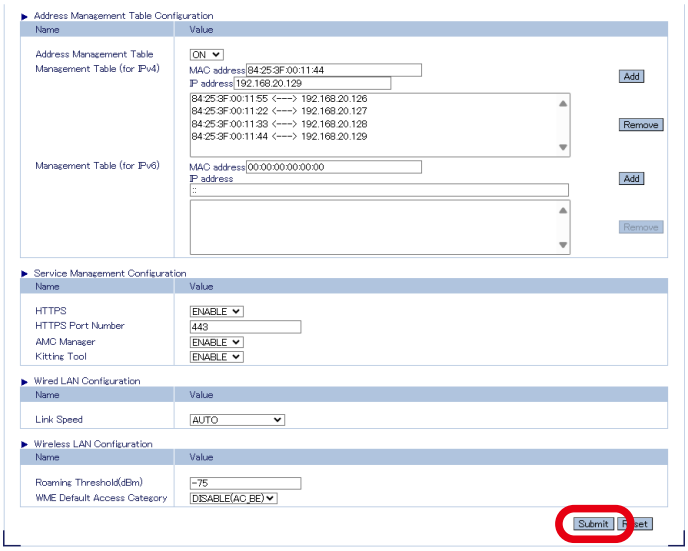
2. Select **ON** for **Address Management Table**, enter the MAC address and IP address and click **Add**.
Repeat the same process to register more sets of information.



- To register a combination of MAC address and IPv6 address, add it to **Management Table (for IPv6)**.

Note

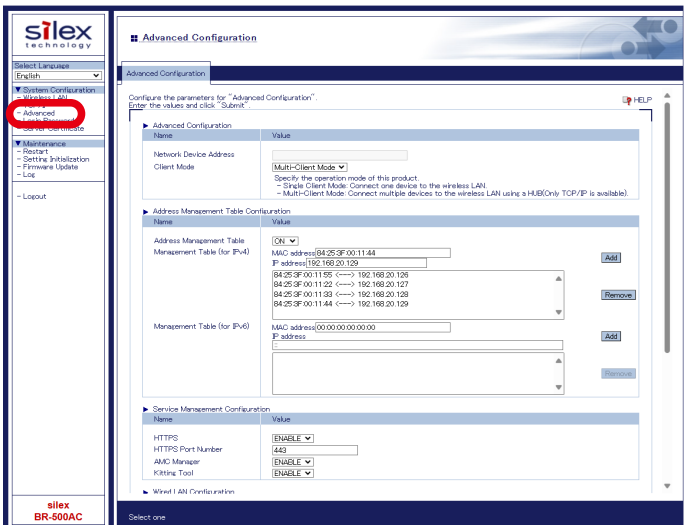
3. The combination information is listed in the management table.
Click **Submit**.



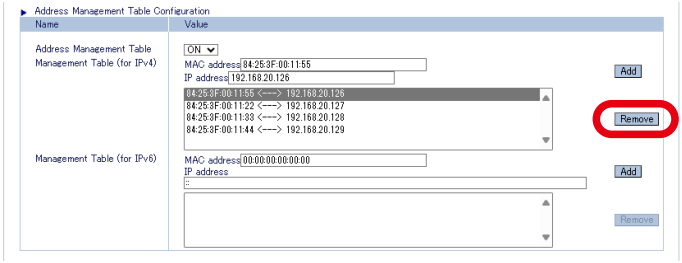
Deleting Address from Management Table

Following explains how to delete combination of MAC address and IP address from management tables (IPv4/IPv6).

1. In the Web configuration interface of the BR-500AC, click **Advanced**.



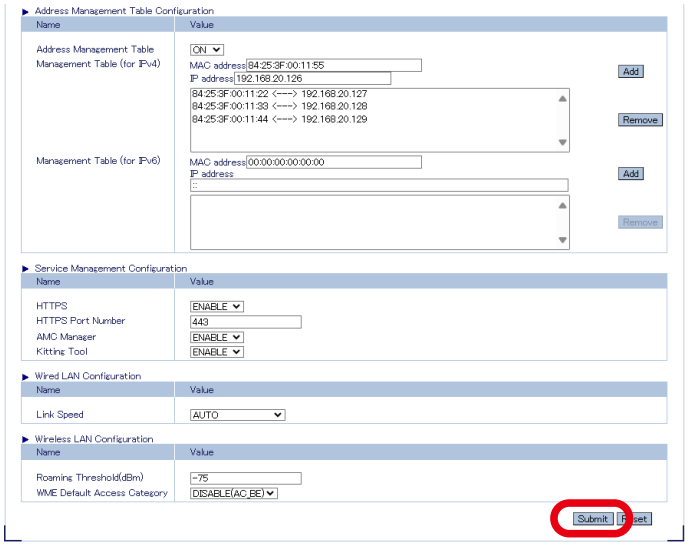
2. At the address management table, select combination of MAC address and IP address from the list and click **Remove**. Repeat the same process to delete more sets of information.



Note

- To select multiple items, hold down the Ctrl key to select them.
- To remove a combination of MAC address and IPv6 address, click **Remove** at **Management Table (for IPv6)**.

3. Click **Submit**.



5-5. WME Function

BR-500AC supports the WME (Wireless Multimedia Extensions) function.
This is a function to add access category information to wireless packets and sends them to the Access Point according to a priority of the received wired packets. The Access Point handles wireless packets according to the 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. It is also possible to set the access category (default access category) to assign when there is no priority setting on the wired packets. If the priority setting does not exist on the packets received from the connected wired device, the access category information appropriate for the default access category setting is added to the wireless packet.

Note

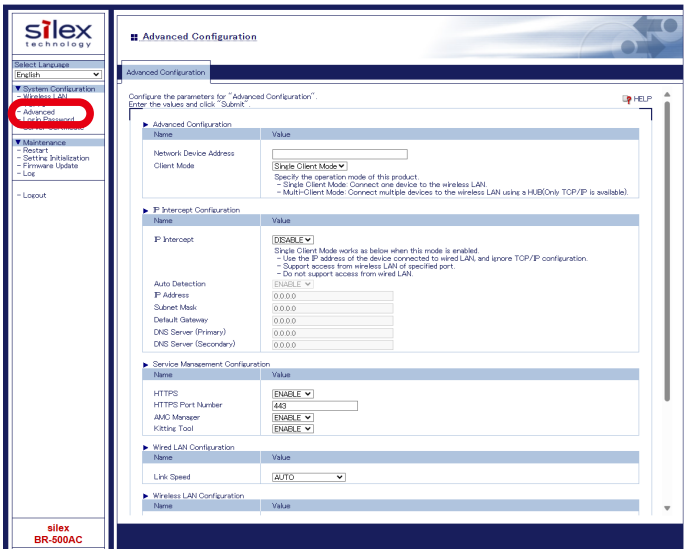
- WME function works in the same way as WMM (Wi-Fi Multimedia).

TIP

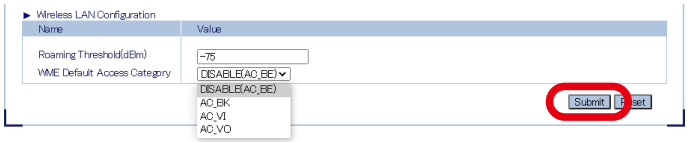
- To establish wireless communication using the WMM function, the Access Point will need to support WMM.

Default Access Category Setting

1. In the Web configuration interface of the BR-500AC, click **Advanced**.



2. Select the default access category to use and click **Submit**.



5-6. Communicating with a Wireless Router with Proxy ARP Function

If a wireless router with the Proxy ARP function exists in the network environment, BR-500AC may not be able to communicate with non-wireless devices.
This is because, when communicating with such a router, one set of MAC address and IP address is needed, however, BR-500AC allows both the non-wireless device and BR-500AC itself to use different IP addresses for the same MAC address.
Even then, if BR-500AC is used in Single Client Mode, enabling the IP Intercept function allows communication with the non-wireless device without having to change any settings of the wireless router.
Please note that if BR-500AC is used in Multi-Client Mode, the Proxy ARP function of the wireless router must be disabled.

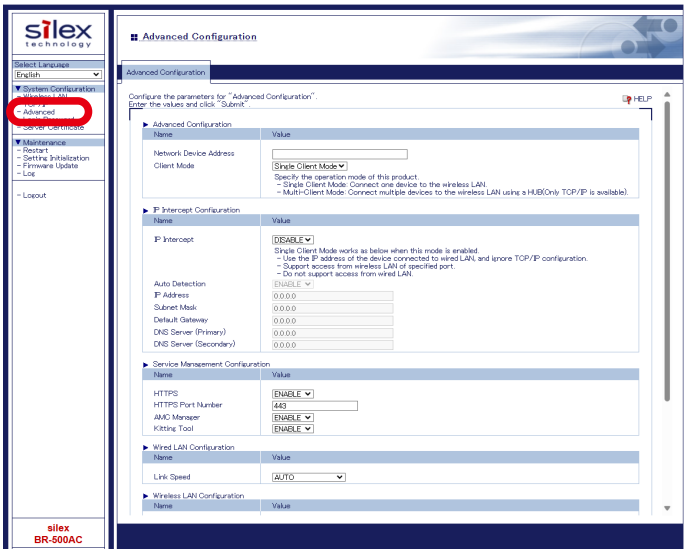
The following explains how to configure the IP Intercept function.


TIP

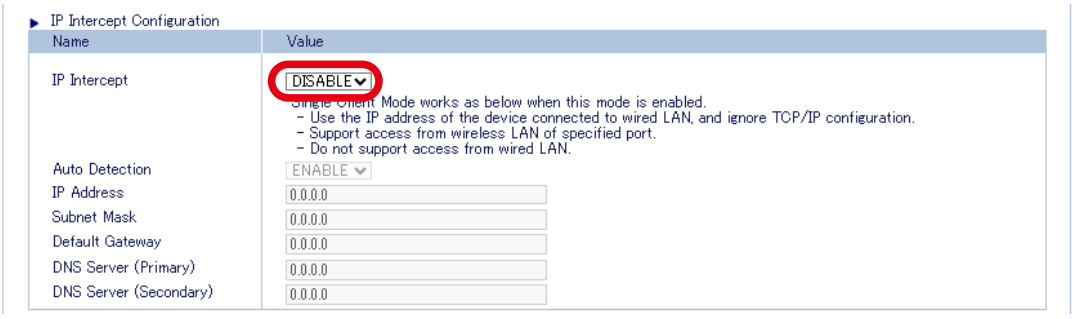
- When **IP Intercept** and **Auto Detection** are enabled, BR-500AC cannot be accessed via wireless LAN until the IP address of the non-wireless device is detected.
- When **IP Intercept** is enabled, BR-500AC uses the same IP address as the non-wireless device. Then, communication between the non-wireless device and BR-500AC will become unavailable. Also, access to the BR-500AC's Web page via the wired LAN will be disabled, however, it will be enabled if BR-500AC is set to Configuration Mode.

IP Intercept Function

1. In the Web configuration interface of the BR-500AC, click **Advanced**.



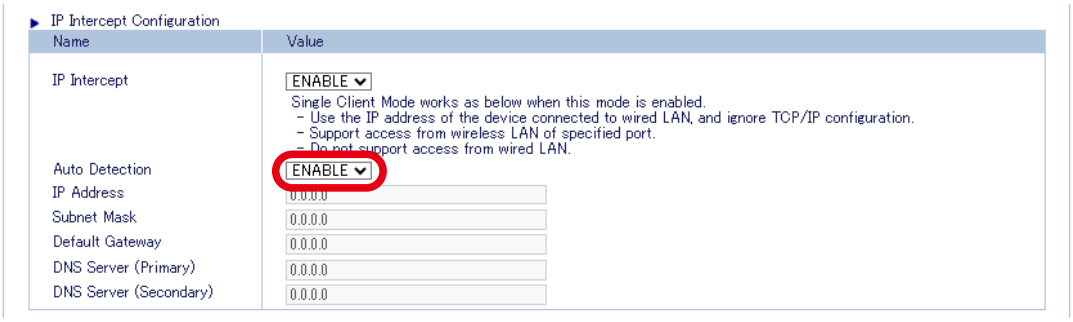
2. Select **ENABLE** for **IP Intercept**.



Note

- The above settings are not displayed when **Client Mode** is **Multi-Client Mode**.

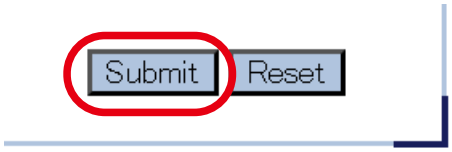
3. When the non-wireless device is set to obtain an IP address from a DHCP server, select **ENABLE** for **Auto Detection**.



TIP

- If the non-wireless device is not set to obtain an IP address from a DHCP server, the **Auto Detection** setting must be disabled, and the same IP address information of the non-wireless device must be set to BR-500AC as well. If this setting differs from that of the non-wireless device, the non-wireless device cannot be communicated via the wireless LAN.

4. Click **Submit**.



To access the BR-500AC's Web page when **IP Intercept** is enabled, enter the following to the address bar of your Web browser.

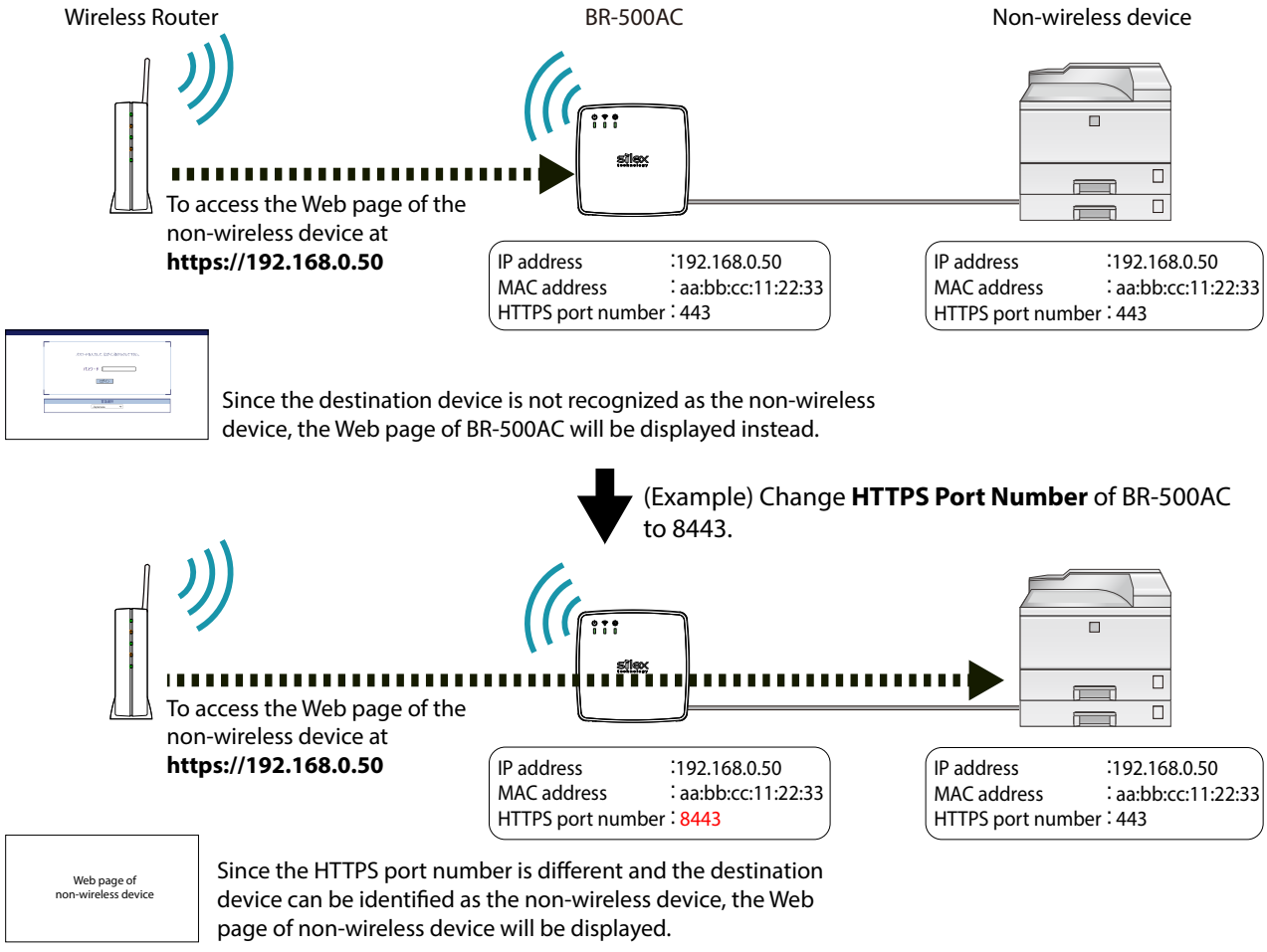
- https:// IP address of non-wireless device

TIP

- When **Auto Detection** is disabled, enter the following:
  - https://the value set to **IP Address** of **IP Intercept Configuration**

Accessing Web Page of Non-wireless Device

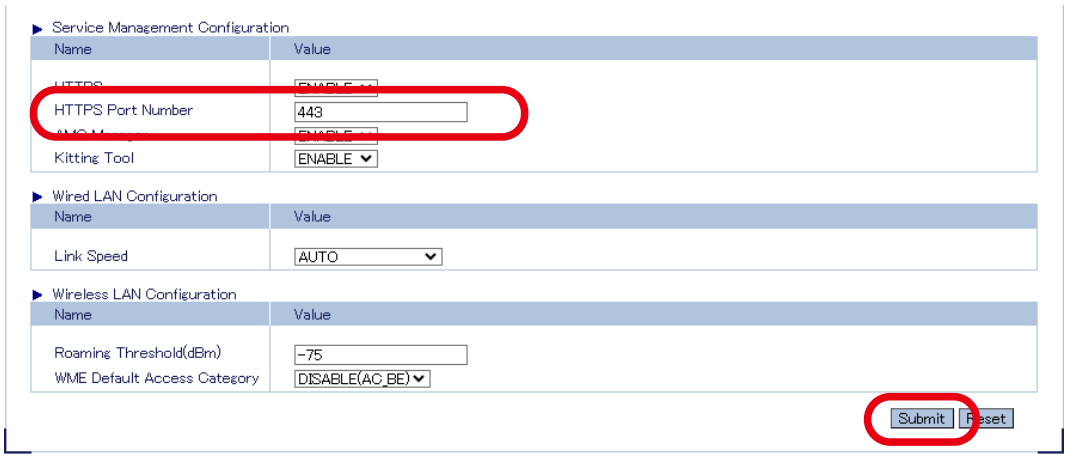
When the IP Intercept function is enabled, the Web page of the non-wireless device cannot be accessed via the wireless LAN.
Since the MAC address, IP address, and HTTPS port number are identical between BR-500AC and the non-wireless device, access to the Web page of the non-wireless device is taken as access to BR-500AC itself.
However, if the HTTPS port number of BR-500AC is changed in the Service Management Configuration, the Web pages of BR-500AC and the non-wireless device can be accessed respectively.



The following explains how to change the settings at Service Management Configuration.

1. In the Web configuration interface of the BR-500AC, click **Advanced**.

2. Change the default values at **HTTPS Port Number** and click **Submit**.



TIP

- For **HTTPS Port Number**, set the value that does not conflict with any reserved port numbers or the port numbers in use by non-wireless devices.

To access the BR-500AC's Web page when **HTTPS Port Number** is changed from the default value, enter the following to the address bar of your Web browser.

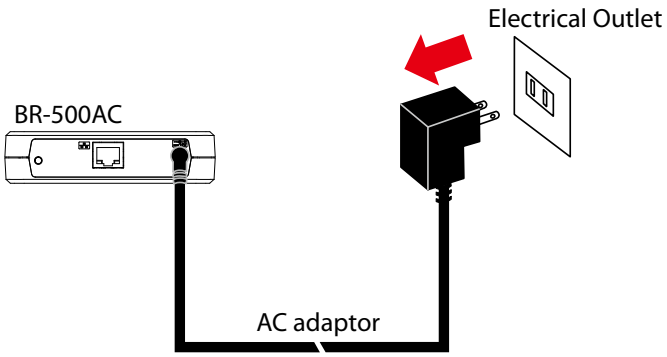
- https:// IP address of non-wireless device : HTTPS port number

5-7. Maintenance

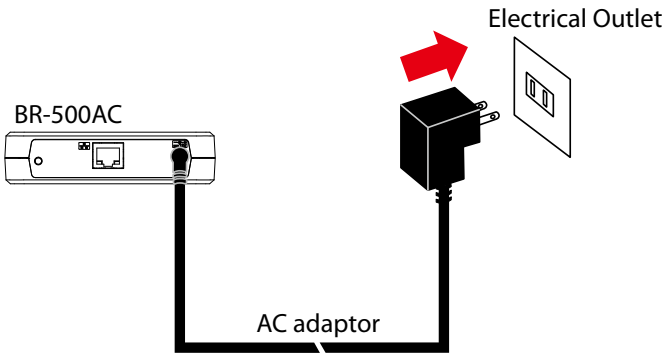
Restarting

How to restart BR-500AC by unplugging the AC adaptor:

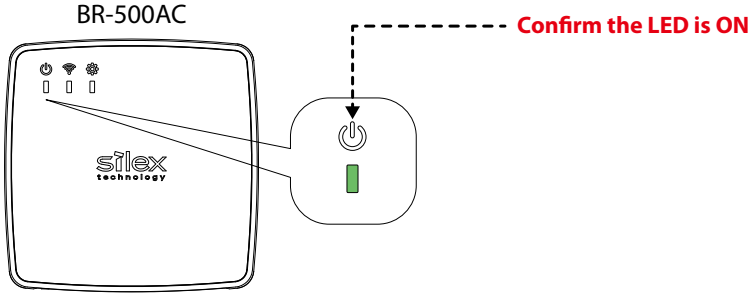
1. Unplug the AC adaptor of BR-500AC from the outlet.



2. Plug the AC adaptor back into the outlet.

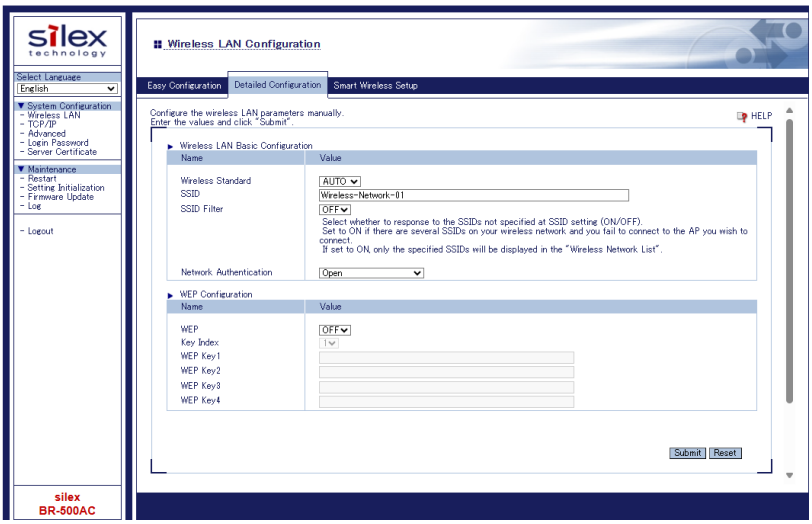


3. When the POWER LED turns green, the restart is completed.
After the restart, the BR-500AC will start in a normal mode.

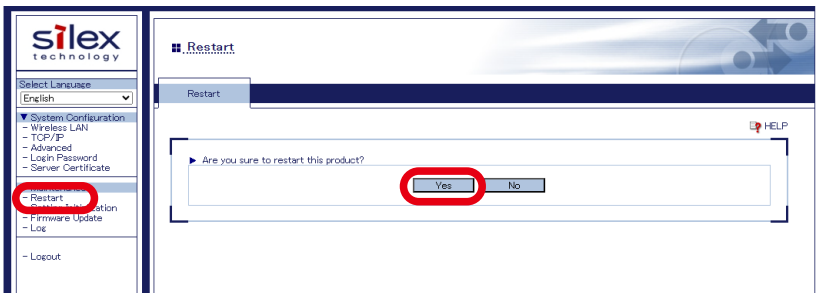


How to restart BR-500AC using the Web configuration interface:

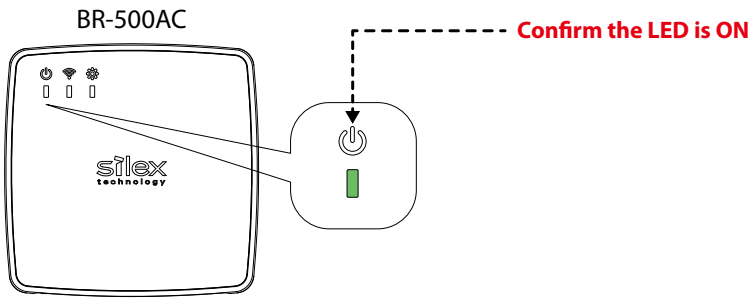
1. Access the Web page of BR-500AC using the Web browser.



2. From the left menu on the Web configuration interface, click **Restart**.
In the page displayed, click **Yes**.



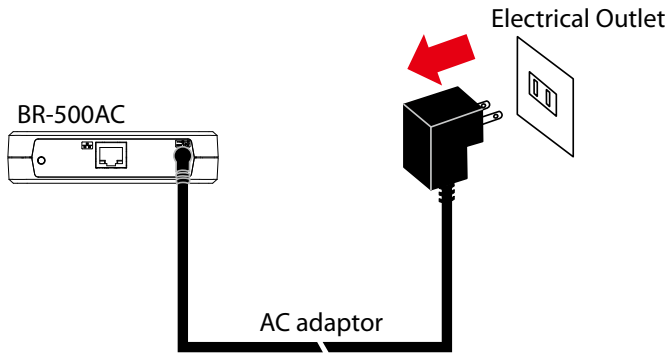
3. When the POWER LED turns green after all LEDs turn off, the restart is completed.
After the restart, the BR-500AC will start in a normal mode.



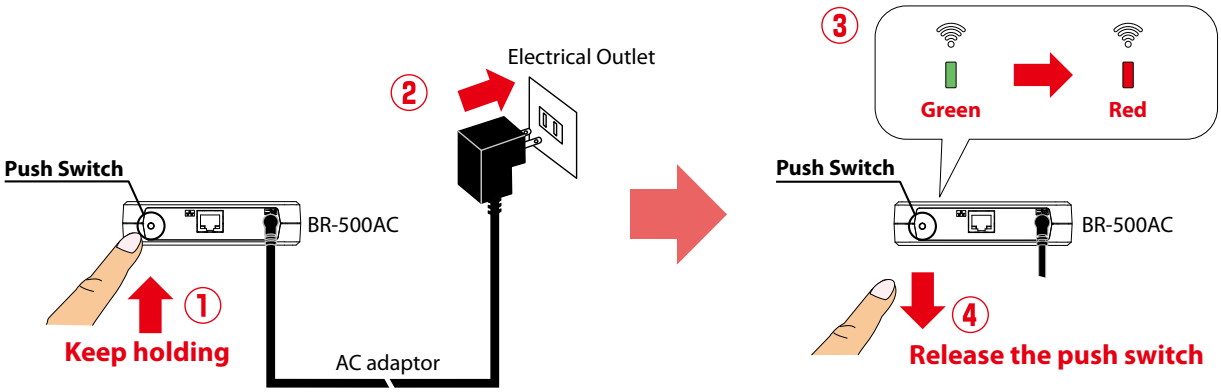
Factory Default Configuration

How to reset BR-500AC to factory defaults using the Push Switch:

1. Unplug the AC adaptor of BR-500AC from the outlet.

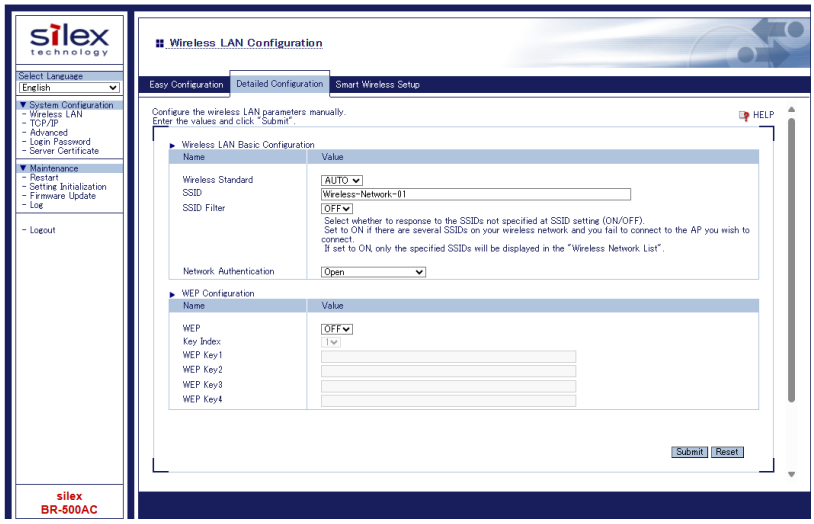


2. Press and hold the push switch on the front while inserting the AC adaptor back into the electrical outlet.
When the WLAN LED turns green and then to red, release the push switch. The factory default configuration begins.
After the factory default configuration is completed, the BR-500AC will start in a normal mode.

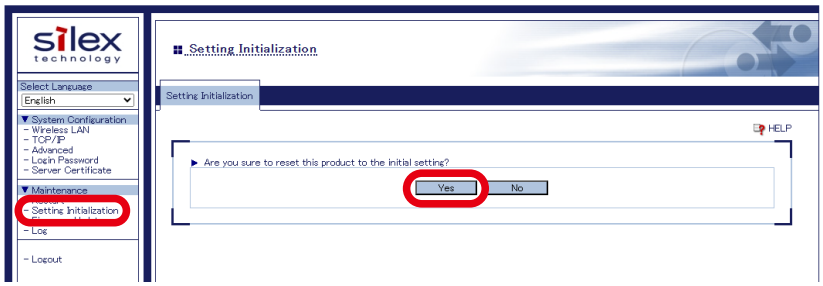


How to reset BR-500AC to factory defaults using the Web configuration interface:

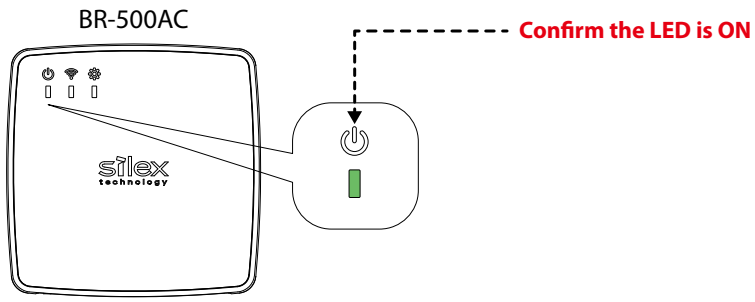
1. Access the Web page of BR-500AC using the Web browser.



2. From the left menu on the Web page, click **Setting Initialization**.
In the page displayed, click **Yes**.



3. After the factory default configuration is completed, the BR-500AC will automatically restart. When the POWER LED turns green after all LEDs turn off, the restart is completed.
After the restart, the BR-500AC will start in a normal mode.



Firmware Update

The latest firmware file can be downloaded from our website.
See the instructions below to download the firmware file. For how to upload the firmware file to BR-500AC, refer to the firmware update procedure sheet file contained in the firmware file you download.
To update the firmware, a password needs to be set to BR-500AC beforehand.

Note

- The current firmware version can be identified at the bottom left of the Web configuration interface.

How to download the firmware file:

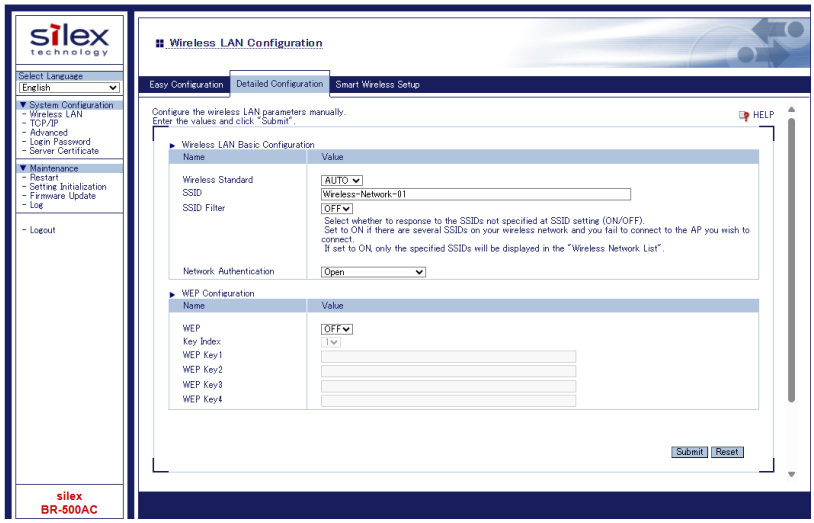
1. Access our website below.

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

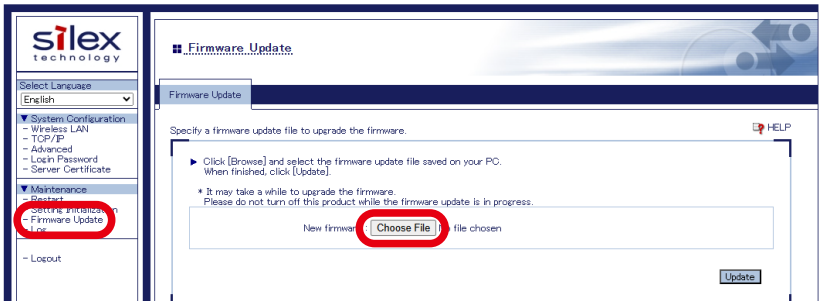
2. Go to the support section and download the firmware file.

How to update the BR-500AC's firmware:

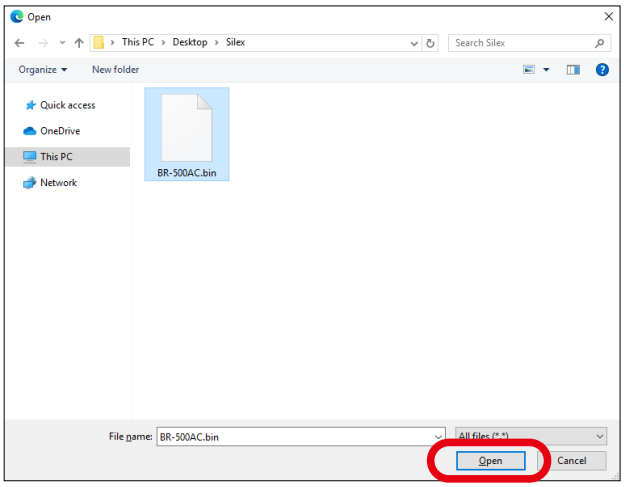
1. Access the Web page of BR-500AC using the Web browser.



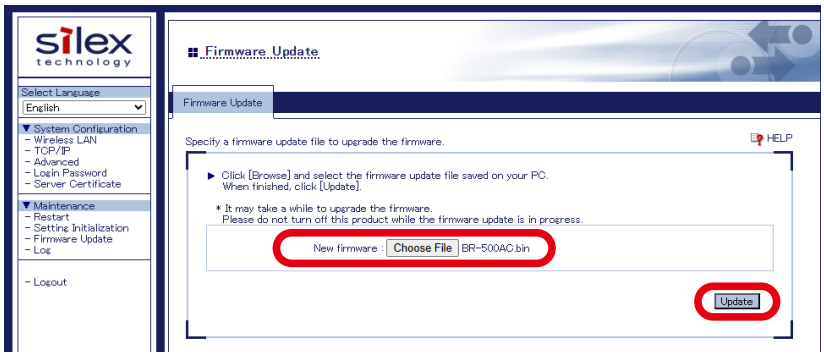
2. From the left menu on the Web page, click **Firmware Update**.
In the page displayed, click the button to the right of **New firmware**.



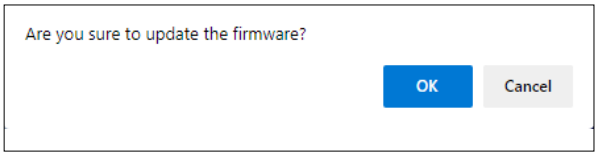
3. In the file selection dialog, select a new firmware file and click **Open**.



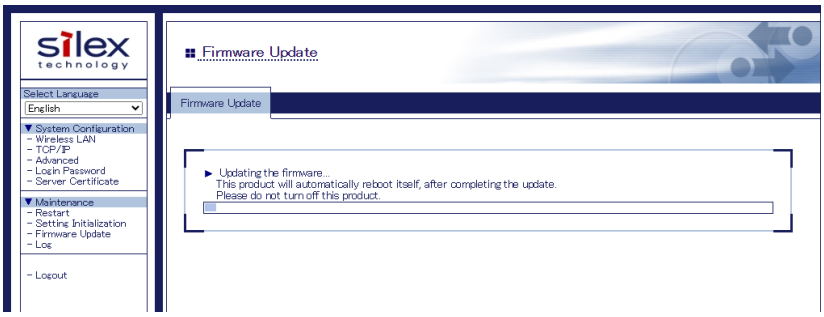
4. Check that the specified firmware file is displayed at **New firmware**, and click **Update**.

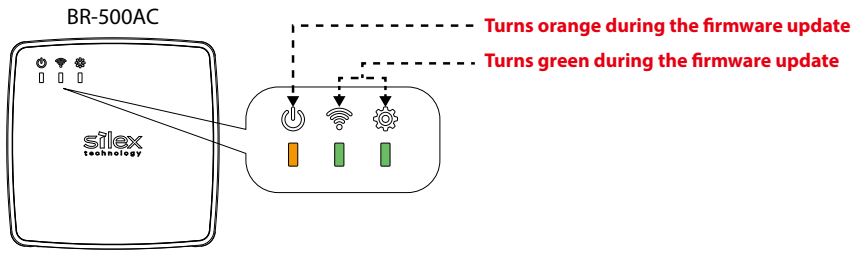


5. When the confirmation dialog is displayed, click **OK**.



6. The firmware update begins.
When the firmware update is in progress, the POWER LED turns orange, and the WLAN LED and STATUS LED turn green.





TIP

- Do not turn off BR-500AC or close the Web browser while the firmware update is in progress.

7. When the LED light pattern is changed, the firmware update is complete.

A. Appendix

A-1. List of All Settings

The BR-500AC has the following configuration items:

Wireless LAN - Easy Configuration	
Select a wireless network.	
Details	Select the SSID of the Access Point (or other wireless devices) to connect from **Wireless Network List**.
Range	Access Point of the wireless network to connect
Default Value	(None)
Enter the Network Key.	
Details	Enter the WEP Key or Pre-Shared Key of the wireless network for **Network Key**.
Range	WEP Key or Pre-Shared key
Default Value	(None)
Note	For network key, usable characters will differ depending on the AP to connect. For details on WEP key, refer to **WEP Key 1-4** at **A-1. List of All Settings**. For details on Pre-Shared key, refer to **Pre-Shared Key** at **A-1. List of All Settings**.

Wireless LAN - Detailed Configuration - Wireless LAN Basic Configuration

Wireless Standard

Details	Select the wireless standard.
Range	AUTO / 2.4GHz / 5GHz
Default Value	AUTO
Note	Access Points of the selected wireless standard will be connected.

SSID

Details	Set the SSID to connect to the wireless network (up to 32 characters).
Range	1 - 32 characters
Default Value	BR500-xxxxxx (xxxxxx is the last 6 digits on MAC address of the BR-500AC.)
Note	The SSID is an ID that distinguishes a wireless LAN network from others. For wireless devices to communicate with each other on a wireless network, they must share the same SSID.

SSID Filter

Details	Select whether to response to the SSIDs not specified at SSID setting (ON/OFF).
Range	ON / OFF
Default Value	OFF
Note	Set to **ON** if there are several SSIDs on your wireless network and you fail to connect to the AP you wish to connect. If set to **ON**, only the specified SSIDs will be displayed in the **Wireless Network List**.

Network Authentication

Details	Select the network authentication mode.
Range	Open / WPA2-Personal / WPA3-Personal / WPA/WPA2-Personal WPA2-Enterprise / WPA3-Enterprise / WPA/WPA2-Enterprise
Default Value	Open

The following items are displayed when **Network Authentication** is **Open**.

- Wireless LAN - Detailed Configuration - WEP Configuration

Wireless LAN - Detailed Configuration - WEP Configuration	
WEP	
Details	Enable/Disable the WEP encryption. If WEP encryption is used, wireless communication will be encrypted using the settings for "**WEP Key 1-4**" and "**Key Index**".
Range	ON/OFF
Default Value	OFF
Note	If encryption is not enabled, data is not encrypted and is sent as is. To ensure higher security, enabling encryption is recommended.
Key Index	
Details	Select the number of the WEP key to use for encryption (1-4). This setting must be the same as that of your wireless device.
Range	1 - 4
Default Value	1
WEP Key1-4	
Details	Set the WEP key for WEP encryption. Up to 4 WEP keys can be set. This setting must be the same as that of your wireless devices. A WEP key must be entered using hexadecimal or alphanumeric characters.
Range	5 or 13 characters 10 or 26 digit hexadecimal value
Default Value	(None)
Note	In most cases, alphanumeric characters are used. Enter 5 characters if the key size is 64bit or 13 characters if the key size is 128bit. For Hexadecimal, a value consists of numbers (0-9) and English letters (A-F). Enter a 10-digit value if the key size is 64bit or a 26-digit value if the key size is 128bit. Usable characters will differ depending on the AP to connect.

The following items are displayed when **Network Authentication** is **WPA2-Personal**.

- Wireless LAN - Detailed Configuration - Wireless LAN Basic Configuration
- Wireless LAN - Detailed Configuration - WPA/WPA2 Personal Configuration

Wireless LAN - Detailed Configuration - Wireless LAN Basic Configuration

Encryption Mode

Details	Select the encryption mode.
Range	AES
Default Value	AES

IEEE802.11r Fast Transition

Details	Enable/Disable the IEEE802.11r Over-the-Air FT (Fast Basic Service Set Transition) function. When this function is enabled, a process of key exchange with the destination AP can be simplified at a time of roaming, by sharing the key information with another AP on the same network beforehand.
Range	ENABLE/DISABLE
Default Value	ENABLE
Note	The following functions are not supported. - Over-the-DS FT - FT Resource Request protocol A time of roaming may take longer depending on the combination with other settings of BR-500AC.

Wireless LAN - Detailed Configuration - WPA/WPA2 Personal Configuration

Pre-Shared Key

Details	Set the Pre-Shared Key to use for encryption. The Pre-Shared Key is a keyword used to create the encryption key. It is also referred to as ' security key ' , ' network key ' or ' password '.
Range	8-64 alphanumeric characters * Hexadecimal string for 64 characters
Default Value	12345678
Note	In most case, alphanumeric characters are used (8-63 characters). For Hexadecimal, a value consists of numbers (0-9) and English letters (A-F). * This setting must be the same as that of your wireless devices. Usable characters will differ depending on the AP to connect.

The following items are displayed when **Network Authentication** is **WPA3-Personal**.

- Wireless LAN - Detailed Configuration - Wireless LAN Basic Configuration
- Wireless LAN - Detailed Configuration - WPA3 Personal Configuration

Wireless LAN - Detailed Configuration - Wireless LAN Basic Configuration	
Encryption Mode	
Details	Select the encryption mode.
Range	AES
Default Value	AES

Wireless LAN - Detailed Configuration - WPA3 Personal Configuration	
Pre-Shared Key	
Details	Set the Pre-Shared Key to use for encryption. The Pre-Shared Key is a keyword used to create the encryption key. It is also referred to as ' security key ' , ' network key ' or ' password '.
Range	8-63 alphanumeric characters
Default Value	12345678
Note	In most case, alphanumeric characters are used (8-63 characters).

The following items are displayed when **Network Authentication** is **WPA/WPA2-Personal**.

- Wireless LAN - Detailed Configuration - Wireless LAN Basic Configuration
- Wireless LAN - Detailed Configuration - WPA/WPA2 Personal Configuration

Wireless LAN - Detailed Configuration - Wireless LAN Basic Configuration	
Encryption Mode	
Details	Select the encryption mode.
Range	AUTO
Default Value	AUTO

Wireless LAN - Detailed Configuration - WPA/WPA2 Personal Configuration	
Pre-Shared Key	
Details	Set the Pre-Shared Key to use for encryption. The Pre-Shared Key is a keyword used to create the encryption key. It is also referred to as ' security key ' , ' network key ' or ' password '.
Range	8-64 alphanumeric characters * Hexadecimal string for 64 characters
Default Value	12345678
Note	In most case, alphanumeric characters are used (8-63 characters). For Hexadecimal, a value consists of numbers (0-9) and English letters (A-F). * This setting must be the same as that of your wireless devices. Usable characters will differ depending on the AP to connect.

The following items are displayed when **Network Authentication** is set to **WPA2-Enterprise**, **WPA3-Enterprise**, or **WPA/WPA2-Enterprise**.

- Wireless LAN - Detailed Configuration - Wireless LAN Basic Configuration
- Wireless LAN - Detailed Configuration - WPA/WPA2/WPA3 Enterprise Configuration
- Wireless LAN - Detailed Configuration - Certificate Registration Status
- Wireless LAN - Detailed Configuration - IEEE802.1X Network Device Configuration

Wireless LAN - Detailed Configuration - Wireless LAN Basic Configuration

Encryption Mode

Details	Select the encryption mode.
Range	AES / AUTO
Default Value	AES (when WPA2-Enterprise or WPA3-Enterprise is set) AUTO (when WPA/WPA2-Enterprise is set)
Note	When the network authentication mode is **WPA2-Enterprise** or **WPA3-Enterprise**, **AUTO** cannot be used. When the network authentication mode is **WPA/WPA2-Enterprise**, **AES** cannot be used.

IEEE802.11r Fast Transition

Details	This setting is displayed when the network authentication mode is **WPA2-Enterprise** and the Authentication Method is **EAP-TLS** / **EAP-TTLS**/ **PEAP**. Enable/Disable the IEEE802.11r Over-the-Air FT (Fast Basic Service Set Transition) function. When this function is enabled, a process of key exchange with the destination AP can be simplified at a time of roaming, by sharing the key information with another AP on the same network beforehand.
Range	ENABLE/DISABLE
Default Value	ENABLE
Note	The following functions are not supported. - Over-the-DS FT - FT Resource Request protocol A time of roaming may take longer depending on the combination with other settings of BR-500AC.

IEEE802.11ai Fast Initial Link Setup	
Details	This setting is displayed when the network authentication mode is **WPA2-Enterprise** and the Authentication Method is **EAP-TLS**. Enable/Disable the IEEE802.11ai FILS (Fast Initial Link Setup) authentication. If this function is enabled, re-authentication process is simplified using the key acquired by PMK cache or ERP(EAP Re-authentication Protocol), when reconnecting to an AP that has been once connected using the IEEE802.1X authentication.
Range	ENABLE/DISABLE
Default Value	ENABLE
Note	The following FILS authentication methods are supported. - FILS Shared Key authentication without PFS (perfect forward security) The following methods are not supported. - FILS Shared Key authentication with PFS - FILS Public Key authentication with PFS A time of roaming may take longer depending on the combination with other settings of BR-500AC.

Wireless LAN - Detailed Configuration - WPA/WPA2/WPA3 Enterprise Configuration

Authentication Method	
Details	Select the authentication mode.
Range	EAP-TLS / EAP-TTLS / PEAP / EAP-FAST / LEAP
Default Value	EAP-TLS
Note	**EAP-TLS** Provides two-way authentication between the client and RADIUS server using a certificate. **EAP-TTLS**, **PEAP** This is the authentication method using EAP-TLS, providing the client authentication using a user name / password. **EAP-FAST** In this authentication, the authentication process is tunneled by the PAC (Protected Access Credential) which is issued from the RADIUS server. **LEAP** One kind of EAP protocols used for PPP authentication. The authentication performs using a user name / password between the RADIUS server and client.

EAP User Name	
Details	Set the ID for the server to identify the client.
Range	1 - 64 characters
Default Value	(None)

EAP Password	
Details	This setting is displayed when the Authentication Method is **EAP-TTLS** / **PEAP** / **EAP-FAST** / **LEAP**. Set the password for the server to identify the client.
Range	1 - 32 characters
Default Value	(None)

Client Certificate Password	
Details	This setting is displayed when the Authentication Method is **EAP-TLS**. Set a client certificate password to use for client authentication. This setting is necessary when a password is set to the client certificate.
Range	1 - 32 characters
Default Value	(None)

Client Certification	
Details	This setting is displayed when the Authentication Method is **EAP-TLS**. Select a client certificate to use for client authentication.
Range	A certificate file used to authenticate BR-500AC

Inner Authentication Method	
Details	This setting is displayed when the Authentication Method is **EAP-TTLS** / **PEAP**. Select the authentication protocol to use. In case of PEAP, only MSCHAPv2 can be used.
Range	PAP / CHAP / MSCHAP / MSCHAPv2
Default Value	PAP (for EAP-TTLS) / MSCHAPv2 (for PEAP)

Server Authentication	
Details	This setting is displayed when the Authentication Method is **EAP-TLS** / **EAP-TTLS** / **PEAP**. Set whether to verify the server reliability. When **ON** is selected, CA Certificate for server authentication is required.
Range	ON / OFF
Default Value	OFF

CA Certificate	
Details	This setting is displayed when the Authentication Method is **EAP-TLS** / **EAP-TTLS** / **PEAP** and the Server Authentication is **ON**. Select a CA certificate to use for server authentication.
Range	CA certificate to use for server authentication

Auto PAC Provisioning	
Details	This setting is displayed when the Authentication Method is **EAP-FAST**. Enable/Disable the automatic distribution of the PAC (Protected Access Credential).
Range	ON / OFF
Default Value	OFF
Note	When **OFF** is selected, the PAC file generated by the server will need to be registered.

PAC File Distribution	
Details	This setting is displayed when the Authentication Method is **EAP-FAST** and Auto PAC Provisioning is **OFF**. Register the PAC file issued from the server to use for manual distribution of PAC (Protected Access Credential)
Range	The PAC file issued from the server to use for manual distribution of PAC (Protected Access Credential)

PAC Password	
Details	This setting is displayed when the Authentication Method is **EAP-FAST** and Auto PAC Provisioning is **OFF**. Set a password to parse the PAC file generated by the server.
Range	1 - 63 characters
Default Value	(None)

Wireless LAN - Detailed Configuration - Certificate Registration Status

Client Certification	
Details	When the client certificate is registered, the issuer and the valid period of the certificate are displayed.
Default Value	Not Registered

CA Certificate	
Details	When the CA certificate is registered, the issuer and the valid period of the certificate are displayed.
Default Value	Not Registered

PAC File Distribution	
Details	When the PAC file is registered, 'Registered' is displayed.
Default Value	Not Registered

Wireless LAN - Detailed Configuration - IEEE802.1X Network Device Configuration

Device Filter

Details	Enable/Disable filtering for the devices registered to the network device address.
Range	ON / OFF
Default Value	ON
Note	If the device filter is disabled, communication will be bridged even for devices not registered to the network device address. The device authentication (one security feature of IEEE802.1X authentication) will not be assured then.

Client Mode

Details	Set the operating mode.
Range	Single Client Mode / Multi-Client Mode
Default Value	Single Client Mode

Network Device Address

Details	This setting can be configured when the Device Filter setting is **ON**. Register the MAC address of devices to be connected to LAN port of the BR-500AC when the IEEE802.1X authentication is used.
Range	MAC address (in **Multi-Client Mode**, up to 16 addresses can be registered)
Default Value	(None)
Note	One MAC Address can be registered for **Single Client Mode** while 16 MAC Addresses can be registered for **Multi-Client Mode**.

Wireless LAN - Smart Wireless Setup - Smart Wireless Setup Execute

PIN Code

Details	The PIN code of BR-500AC is displayed.
Range	The value is automatically generated by clicking the button.
Default Value	Automatically generated

Smart Wireless Setup Execute

Details	Execute the wireless configuration by Smart Wireless Setup.
Range	(Smart Wireless Setup Execute button)
Default Value	-

TCP/IP - TCP/IP Configuration - General Configuration

Host Name

Details	Set the host name. Be sure to use a unique name that is not used by other devices.
Range	1-15 characters * The following symbols and spaces cannot be used. `~!@#$^&*()=+[]{}|;:'",<>/?
Default Value	BR500-xxxxxx (xxxxxx is the last 6 digits on MAC address of the BR-500AC.)

The following items cannot be configured when **IP Intercept** is **ENABLE**.

- TCP/IP - TCP/IP Configuration - TCP/IP Configuration

TCP/IP - TCP/IP Configuration - TCP/IP Configuration

DHCP Client

Details	Enable/Disable the DHCP protocol. To assign an IP address using DHCP, the DHCP server must be running in your subnetwork.
Range	ENABLE/DISABLE
Default Value	ENABLE

IP Address

Details	Set the IP address. If the DHCP is enabled on your network, the IP Address obtained from it will be applied.
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0

Subnet Mask

Details	Set the subnet mask. If the DHCP is enabled on your network, the Subnet Mask obtained from it will be applied.
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0
Note	When set to "0.0.0.0", a subnet mask appropriate for the IP address is automatically assigned.

Default Gateway

Details	Set the gateway address. If "0.0.0.0" is set, this setting is disabled. When the DHCP is enabled on your network, the Default Gateway obtained from it will be applied.
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0

DNS Server (Primary)

Details	Set the DNS server (primary) address. When the DHCP is enabled, the obtained DNS server address will be applied.
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0

DNS Server (Secondary)

Details	Set the DNS server (secondary) address. When the DHCP is enabled, the obtained DNS server address will be applied.
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0

TCP/IP - TCP/IP Configuration - NTP Configuration

NTP

Details	Enable/Disable the NTP protocol.
Range	ENABLE/DISABLE
Default Value	DISABLE

NTP Server

Details	This setting can be configured when the NTP setting is **ENABLE**. Set the domain name for NTP server. When this is not set, the NTP function is disabled.
Range	1-128 characters
Default Value	pool.ntp.org

Local Time Zone

Details	Set the local time zone.
Range	-12:00 - +12:00
Default Value	+9:00

Advanced - Advanced Configuration - Advanced Configuration

Network Device Address

Details	This setting can be entered when the Client Mode is **Single Client Mode**. This is the function to identify the devices connected to the wired LAN port of BR-500AC. Only devices with the registered MAC address are allowed to access.
Range	MAC Address
Default Value	(None)
Note	When the MAC address is not registered, this function is disabled.

Client Mode

Details	Set the operating mode.
Range	Single Client Mode / Multi-Client Mode
Default Value	Single Client Mode
Note	Select **Single Client Mode** to bridge only one device connected to a LAN port of the BR-500AC. In **Single Client Mode**, not only TCP/IP but various communication protocols can be used. Select **Multi-Client Mode** to bridge several devices using a HUB on the LAN port of BR-500AC. In **Multi-Client Mode**, only ARP, IPv4 and IPv6 protocol can be used.

The following items are displayed when **Client Mode** is **Single Client Mode**.

- Advanced - Advanced Configuration - IP Intercept Configuration

Advanced - Advanced Configuration - IP Intercept Configuration

IP Intercept

Details	Enable/Disable the IP Intercept function. When there is a wireless router with a Proxy ARP function, communication may not be established with non-wireless devices. By enabling this function and setting the same IP address as the non-wireless device, communication can be established. For details, refer to **5-6. Communicating with a Wireless Router with Proxy ARP Function**.
Range	ENABLE/DISABLE
Default Value	DISABLE

Auto Detection

Details	This setting can be configured when the IP intercept function is enabled. If this function is enabled, IP address information of the connected non-wireless device will automatically be detected and be used to configure BR-500AC. A DHCP server must be running on network and the non-wireless device must be set to obtain an IP address from the DHCP server, then.
Range	ENABLE/DISABLE
Default Value	ENABLE

IP Address

Details	Set an IP address of the non-wireless device connected to BR-500AC to use when **Auto Detection** is **DISABLE**.
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0
Note	This is a different setting from **IP Address** of the **TCP/IP Configuration** page.

Subnet Mask

Details	Set a subnet mask of the non-wireless device connected to BR-500AC to use when **Auto Detection** is **DISABLE**.
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0
Note	This is a different setting from **Subnet Mask** of the **TCP/IP Configuration** page.

Default Gateway

Details	Set a default gateway of the non-wireless device connected to BR-500AC to use when **Auto Detection** is **DISABLE**.
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0
Note	This is a different setting from **Default Gateway** of the **TCP/IP Configuration** page.

DNS Server (Primary)	
Details	Set a DNS server (primary) address of the non-wireless device connected to BR-500AC to use when **Auto Detection** is **DISABLE**.
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0
Note	This is a different setting from **DNS Server (Primary)** of the **TCP/IP Configuration** page.

DNS Server (Secondary)	
Details	Set a DNS server (secondary) of the non-wireless device connected to BR-500AC to use when **Auto Detection** is **DISABLE**.
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0
Note	This is a different setting from **DNS Server (Secondary)** of the **TCP/IP Configuration** page.

The following items are displayed when **Client Mode** is **Multi-Client Mode**.

- Advanced - Advanced Configuration - Address Management Table Configuration

Advanced - Advanced Configuration - Address Management Table Configuration	
Address Management Table	
Details	Enable/Disable the address management table feature to use in **Multi-Client Mode** (**ON**/**OFF**). When **ON** is set, combination information of MAC address and IP address will be used from management tables (IPv4/IPv6) for connected non-wireless devices.
Range	ON / OFF
Default Value	OFF
Note	Only unicast address is supported for MAC address and IP address. BR-500AC checks the existence of device information to save at 5 sec interval. If BR-500AC is turned off before the saving process is completed, the device information is not saved in the address management table.
Management Table (for IPv4)	
Details	Register combination of MAC address and IP address (IPv4).
Range	Up to 16 sets of MAC address and IP address (IPv4)
Default Value	MAC address 00:00:00:00:00:00 IP address 0.0.0.0
Management Table (for IPv6)	
Details	Register combination of MAC address and IP address (IPv6).
Range	Up to 16 sets of MAC address and IP address (IPv6)
Default Value	MAC address 00:00:00:00:00:00 IP address ::

Advanced - Advanced Configuration - Service Management Configuration

HTTPS

Details	Enable/Disable accessing the Web page using HTTPS protocol. If this function is enabled, HTTP communications are encrypted to enhance security.
Range	ENABLE/DISABLE
Default Value	ENABLE
Note	If this setting is disabled, the Web page of BR-500AC cannot be accessed unless Configuration Mode is used.

HTTPS Port Number

Details	Set the port number to use for HTTPS protocol. To access BR-500AC via HTTPS after the default value is changed, use the format "**https://BR-500AC's IP address: this setting**".
Range	1-65535
Default Value	443

AMC Manager

Details	Enable/Disable accessing BR-500AC using AMC Manager®.
Range	ENABLE/DISABLE
Default Value	ENABLE

Kitting Tool

Details	Enable/Disable accessing BR-500AC using Kitting Tool.
Range	ENABLE/DISABLE
Default Value	ENABLE

Advanced - Advanced Configuration - Wired LAN Configuration

Link Speed

Details	Sets the link speed for the wired network. Usually, "**AUTO**" is used.
Range	AUTO / 10BASE-T-Half / 10BASE-T-Full / 100BASE-TX-Half / 100BASE-TX-Full
Default Value	AUTO
Note	If a Link LED on the connected device does not light on when BR-500AC is powered on, change the network type to that of the connected device.

Advanced - Advanced Configuration - Wireless LAN Configuration

Roaming Threshold(dBm)

Details	Set the roaming threshold value (-35 to -95). If a greater value is set, frequency of roaming is increased, however, communication may become unstable.
Range	-35 to -95
Default Value	-75
Note	A time of roaming may take longer depending on the combination with other settings of BR-500AC.

WME Default Access Category

Details	Set the access category to use for wireless communication when there is no priority setting for communication from the connected wired device.
Range	DISABLE (AC_BE) / AC_BK / AC_VI / AC_VO
Default Value	DISABLE (AC_BE)
Note	The priority differs depending on the access category to set. Order of priority: (1) **AC_VO** (audio) (2) **AC_VI** (video) (3) **AC_BE** (best effort) (4) **AC_BK** (background)

Login Password - Password Configuration

Please input the password.

Details	Configure the password to manage the BR-500AC. This password is used for authentication to login to the Web configuration interface of BR-500AC.
Range	1 - 15 characters
Default Value	(None)

Server Certificate - Server Certificate Config - Server Certificate Create

Common Name	
Details	Set a name of BR-500AC.
Range	1 to 64 characters
Default Value	BR500-xxxxxx (xxxxxx is the last 6 digits of the MAC address, and letters are uppercase)

Organizational Unit Name	
Details	Enter the organization unit name.
Range	Up to 64 characters
Default Value	(None)

Organization Name	
Details	Enter the organization name.
Range	Up to 64 characters
Default Value	(None)

Locality Name	
Details	Enter the locality/city name.
Range	Up to 128 characters
Default Value	(None)

State or Province Name	
Details	Enter the state/province name.
Range	Up to 128 characters
Default Value	(None)

Country/Region code	
Details	Enter the code (two characters) representing your country or region.
Range	2 characters
Default Value	US

A-2. Troubleshooting

This section provides the solutions for possible troubles you may experience when you are configuring or using the BR-500AC.

My Access Point is not displayed in the Wireless Network List of the Web configuration interface.

The Access Point may not be active.	
Solution	Please check that the Access Point is operating correctly.

The Access Point may be operating in a stealth mode.	
Solution	Configure the detailed settings of the wireless network at **Detailed Configuration** of the Web configuration interface to connect to the Access Point. Remember that Access Points operating in a stealth mode will not be displayed in the list.

Too many wireless devices may be operating, exceeding the maximum number of devices the BR-500AC can show on (up to 32 devices).	
Solution	Up to 32 wireless devices can be displayed at **Wireless Network List**. To show your Access Point in the list, use **SSID Filter** so that only the specified networks are displayed there. Even when the Access Point is not displayed in the list, it can be connected by configuring the wireless settings at **Detailed Configuration** of the Web configuration interface.

I failed to connect to a wireless network using Smart Wireless Setup.

The WPS feature may be disabled on the Access Point.	
Solution	Check that the Access Point supports the WPS feature. Depending on the Access Point, you may need to manually enable the WPS feature. For details, see the operating manual that came with your Access Point.

The password configuration may not be completed on BR-500AC.	
Solution	To use the Smart Wireless Setup function (Push Switch), a password must be set to BR-500AC. For details, refer to **4-1. Starting Configuration Mode for Password Settings**.

A LAN port error has occurred (POWER LED: Blinks rapidly (Red), WLAN LED: OFF, STATUS LED: ON (Green)).

The bridge feature may be aborted as the non-wireless device is unplugged and changed to the other device on the LAN port.	
Solution	Restart the BR-500AC. In **Single Client Mode**, if the non-wireless device is unplugged and changed to the other device, BR-500AC will abort bridging of that device, taking such occurrence as an error. Also, when the MAC address filtering is used to restrict the devices to bridge, you will need to change the setting registered to **Network Device Address**. This error does not occur in **Multi-Client Mode**. The restart is not required then.

Several devices may have been connected to the BR-500AC using a HUB, though it is operating in **Single Client Mode**.	
Solution	In **Single Client Mode**, connect only one device to the LAN port of BR-500AC. To use several devices, use **Multi-Client Mode**.

I cannot communicate with the non-wireless device connected to BR-500AC.

The BR-500AC or non-wireless device may not be operating correctly.	
Solution	Please check the LED status on BR-500AC. Please also check that the non-wireless device is properly powered on.

The connection may be restricted by the MAC address filtering on BR-500AC.	
Solution	See the setting at **Network Device Address** to check that access of the connected device is not restricted by the MAC address filtering.

16 or more non-wireless devices may be connected when BR-500AC is operating in **Multi-Client Mode**.	
Solution	Check how many non-wireless devices are connected to BR-500AC. Up to 16 non-wireless devices can be connected when BR-500AC is operating in **Multi-Client Mode**.

16 sets of combination information may be registered to the management table.	
Solution	When BR-500AC is operating in **Multi-Client Mode** and the address management table feature is enabled, up to 16 sets of combination information are automatically registered to the management table. As they are not deleted automatically after registered, please manually delete unnecessary ones.

The wireless router may be filtering the devices by MAC addresses.	
Solution	Check that the wireless router does not filter the following MAC addresses: **Single Client Mode**: MAC address of non-wireless device **Multi-Client Mode**: MAC address of BR-500AC The MAC address of BR-500AC can be found on the product label or on the Web page.

The wireless router may have a function equivalent to Proxy ARP and it is turned on.	
Solution	Check the Proxy ARP function setting of the wireless router. If the function is enabled, change the setting. However, if **Single Client Mode** is turned on and the IP Intercept function of BR-500AC is enabled, it does not need to be changed. For details, refer to **5-6. Communicating with a Wireless Router with Proxy ARP Function**.

The imported IEEE802.1X certificate cannot be deleted.

It is impossible to delete the imported certificate only.	
Solution	To delete the imported certificate, initialize the BR-500AC. **NOTE:** The imported certificate is validated only when it is used. Even if you keep the certificate, it has no impact on the authentication process since the imported certificate is used only with the compatible authentication method.

I cannot connect to BR-500AC in Ad hoc mode.

BR-500AC does not support Ad hoc mode.	
Solution	Only Infrastructure mode can be used.

A-3. What's AMC Manager®?

AMC Manager® is an integrated device management software that can monitor and configure the Silex products remotely over an IP network. If AMC Manager® is used, the operating status of BR-500AC units can be checked in a list view.
There are two versions of AMC Manager®; the one is AMC Manager Free (free version) and the other one is AMC Manager (non-free version).
AMC Manager® can be downloaded from the Silex Technology's website.

Note

- To use AMC Manager (non-free version), a license key needs to be purchased. Please contact Silex Technology to purchase a license key.
- For details on the "AMC Manager®" , please visit our homepage.
- To use the "AMC Manager®", an IP address needs to be configured to the BR-500AC.

How to Download AMC Manager®

1. Access the Silex Technology's website (**https://www.silextechnology.com/**).

2. When the website is displayed, click **Support Center** in the bottom of the page.

3. Click **Software Download**.

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

5. Download AMC Manager®.

A-4. Security Information

Access Control Mechanism

The following shows the access control method and encryption mode for the product information.

Web Page

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

AMC Manager/BR Kitting Utility

Information	Access Control Method	Encryption Mode
Network settings (Network assets)	Accesses are controlled using an administrator password.	Communications are encrypted using a unique algorithm
Network settings (Network 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
Network settings (Network assets)	Accesses are allowed only from the devices on the same wired network.	No encryption

Key Information

Wireless Communication - Key Information

Encryption Algorithm	Key Length
WEP	64bit, 128bit
TKIP	128bit
AES	128bit

Client Certificate / CA Certificate - Key Information

Encryption Algorithm	Key Length
RSA	512bit, 1024bit, 2048bit, 4096bit

Known Vulnerabilities

The BR-500AC has the following known vulnerabilities:

- Vulnerabilities that cannot be exploited in the specific conditions of the equipment
  - In case a firmware update fails, BR-500AC starts in recovery mode to retry it. Then, unsecured HTTP communication starts but BR-500AC does not connect to a wireless LAN. Also, any operations other than the firmware update are not possible.

- Vulnerabilities that have been mitigated to an acceptable residual risk

  There are no such vulnerabilities.

- Vulnerabilities that have been accepted on a risk basis
  - The wireless client function of BR-500AC supports insecure encryption modes such as WEP and TKIP.
  - The wireless client function of BR-500AC supports one of the IEEE 802.1X authentication methods 'EAP-FAST' that uses the insecure TLS version 'TLSv1.0'.
  - The wireless LAN client function of BR-500AC supports the use of certificates with a short public key length (e.g. 512bit, 1024bit) for IEEE 802.1X authentication. However, communication using such certificates is not secure.
  - Communications of FLDP/BR are not encrypted.