WA102880XC

Access Point

AP-500AC

User's Guide

silex technology

Index

1. Introduction

Thank you for purchasing the Access Point AP-500AC (called "AP-500AC" below).

1-1. Introduction

This manual provides information on how to configure and use AP-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.
- This manual was prepared to accurately match the content of each OS, but the actual information shown on the computer monitor may differ from the content of this manual due to future OS version upgrades, modifications, and other changes.
- Although every effort was made to prepare this manual with the utmost accuracy, Silex Technology will not be held liable for any damages as a result of errors, setting examples, or other content.

Trademarks

- Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Ethernet is a trademark of Xerox Corporation.
- 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 AP-500AC.
To ensure safe and proper use, please read the following information carefully before using AP-500AC. The safety instructions include important information on safe handling of AP-500AC and on general safety issues.

< Indication of the warning >

	Danger	"Danger" indicates the existence of a hazard that could result in bodily injury if the safety instruction is not observed.
	Warning	"Warning" indicates the existence of a hazard that could result in material damage if the safety instruction is not observed.

< Indication of the symbol >

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

Danger

 	* Do not allow physical impact: When damaged, turn off your network device, unplug the AC plug of AP-500AC from power outlet (unplug the network cable from Ethernet HUB when receiving power over the Ethernet) and contact your point of purchase. Failure to take this action could cause fire or an electrical shock. * In the following cases, turn off your network device, unplug the AC plug of AP-500AC from power outlet (unplug the network cable from Ethernet HUB when receiving power over the Ethernet) and contact your point of purchase. Failure to take this action could cause fire or an electrical shock. * When AP-500AC emits a strange smell, heat, smoke or sound. * When foreign objects (liquid, metal, etc) gets into AP-500AC.
	* Keep the cord and cables away from children. They may be injured or receive a shock.
	* If your network device has a ground wire, it must be used to prevent electrocution and power surges.
	* Do not disassemble or modify AP-500AC. Contact your point of purchase about repairing AP-500AC. * Do not disassemble or alter the AC adapter bundled with AP-500AC.

Warning

	* When unplugging AP-500AC, do not pull on the cord. The cord may break resulting in fire and/or electric shock. Pull only on the plug.
	* When moving AP-500AC, turn off your network device and AP-500AC by unplugging the power cables from the outlet (if you are receiving power over the Ethernet (PoE), unplug the network cable from the HUB). * Always use the AC adapter bundled with AP-500AC. Other AC adapters may cause AP-500AC to malfunction. * Verify all cables are connected properly and safely before using AP-500AC. * When AP-500AC will not be used for an extended time, disconnect and unplug the power cable.
	* Do not use or store AP-500AC under the following conditions to avoid potential damage to AP-500AC. - Hard vibrations - Tilted or unstable places - Exposure to the direct rays of the sun - Humid or dusty places - Wet place (kitchen or bathroom) - Heated places (near stove or heater) - Wide temperature change - Strong electromagnetic field (near magnet, radio or wireless device)

1-3. User Registration and Customer Services

User registration

To enable us to provide better services (support and repair), please perform the user registration process from our website below:

	URL
USA	http://www.silexamerica.com/support/product-registration/
Europe	http://www.silexeurope.com/en/home/support/registration/
Japan	http://www.silex.jp/register/

Note

- For user registration, a serial number is required. It can be found on the bottom of AP-500AC.

Product Information

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

	URL
USA	http://www.silexamerica.com/
Europe	http://www.silexeurope.com/
Japan	http://www.silex.jp/

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

Customer Support Center

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

Contact Information		
USA	+1-801-748-1199	support@silexamerica.com
Europe	+49-(0)2154-88967-0	support@silexeurope.com
Japan	+81-(0)774-98-3981	support@silex.jp

Note

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

2. About AP-500AC

AP-500AC is an Access Point that supports IEEE 802.11a/b/g/n/ac and can be used as a base station to connect your wireless client devices each other. In addition to high performance wireless connectivity, AP-500AC also supports enterprise-level wireless security and PoE (Power over Ethernet).

Note

- PoE is a technology to supply electrical power over Ethernet cable (Category 5 or above). This technology allows you to connect your PoE supported devices to the Ethernet even in a location without electrical outlet nearby.

2-1. Features

AP-500AC has the following features:

- Works as an Access Point that can connect up to 200 wireless devices. (*1)
- IEEE 802.11a/b/g/n/ac and 2.4GHz/5GHz concurrent wireless connectivity
- With IEEE 802.11n, up to 300Mbps can be reached at 2.4GHz (theoretical value)
- With IEEE 802.11ac, up to 1.3Gbps can be reached at 5GHz (theoretical value)
- Higher security with IEEE 802.1X authentication
- Multi SSID (Up to 8 wireless interfaces can be used)(*2)
- Easy configuration using Smart Wireless Setup feature(*3)
- Web configuration interface
- PoE (Power over Ethernet)
- DHCP server function
- USB Device Server feature allows sharing of various USB devices connected to AP-500AC.

*1 This is the total number of connectable devices for 2.4GHz (100 device) and 5GHz (100 devices)
Up to 100 wireless devices can be connected when TKIP or AUTO is used as wireless encryption.

*2 Up to 8 wireless interfaces can be used; four for 2.4GHz and four for 5GHz.

*3 This is a wireless configuration feature compatible with WPS2.0.

- Advanced configuration (WMM-EDCA setting, etc.)
- Configuration import /export
- Log message feature (access logs, etc.)
- MAC Address filter can allow or deny access of devices.
- WDS (Wireless Distribution System) feature allows wireless communication between the Access Points (AP-500AC).(*4)
- VLAN (Virtual Local Area Network) feature allows to establish virtual network groups.
- Supports the total management software, AMC Manager® (non-free / free program) / AMC Finder (free program)
- Using the AMC Manager®, you can maintain as well as monitor the Silex devices from a remote place, including the bulk configuration, firmware update, etc.

*4 WDS is guaranteed only for Silex brand products that support WDS.

TIP

- When WDS is used for both 2.4GHz and 5GHz bands simultaneously, please do not allow a link between the bands. It may cause a loop communication error.

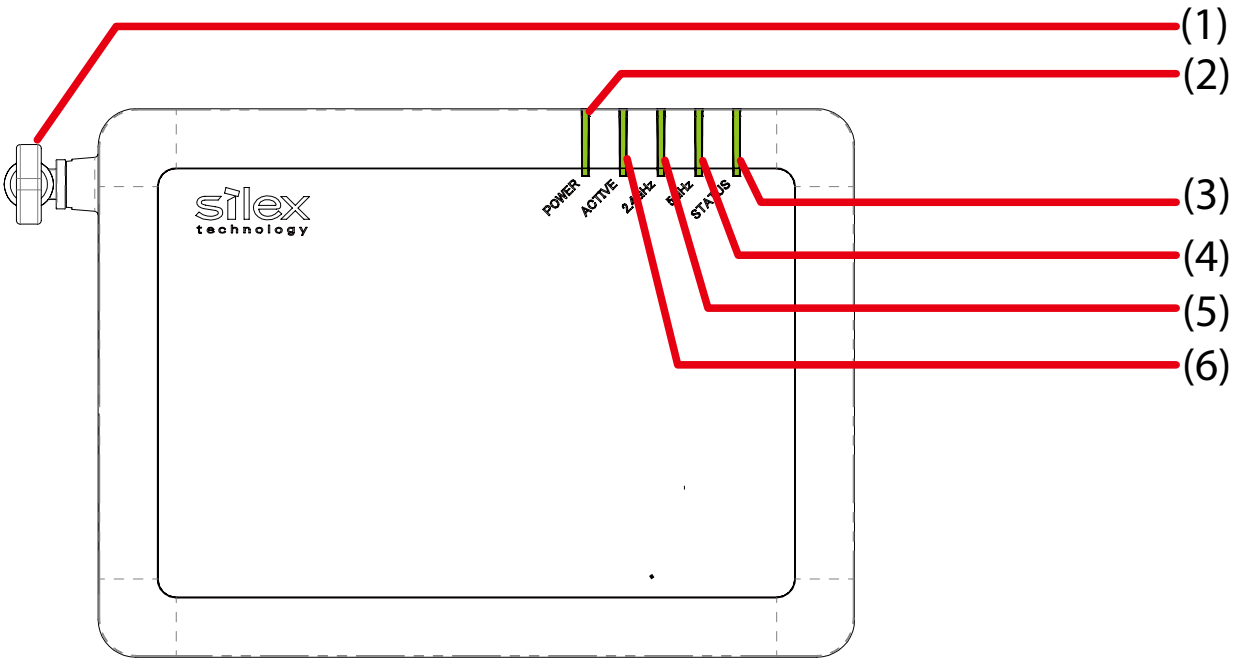
Note

- For details on the "AMC Manager®" and "AMC Finder", please visit our homepage.

2-2. Parts and Functions

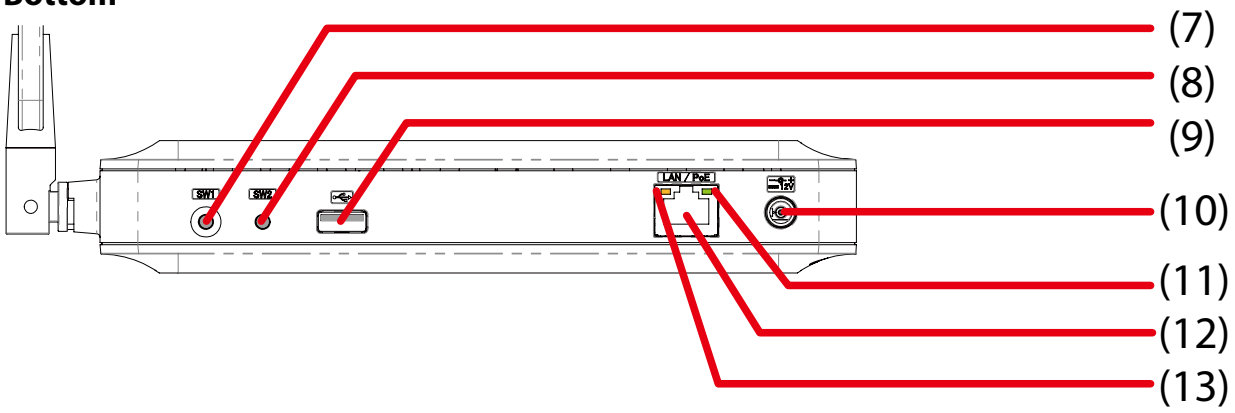
The parts name and functions are as follows:

Front



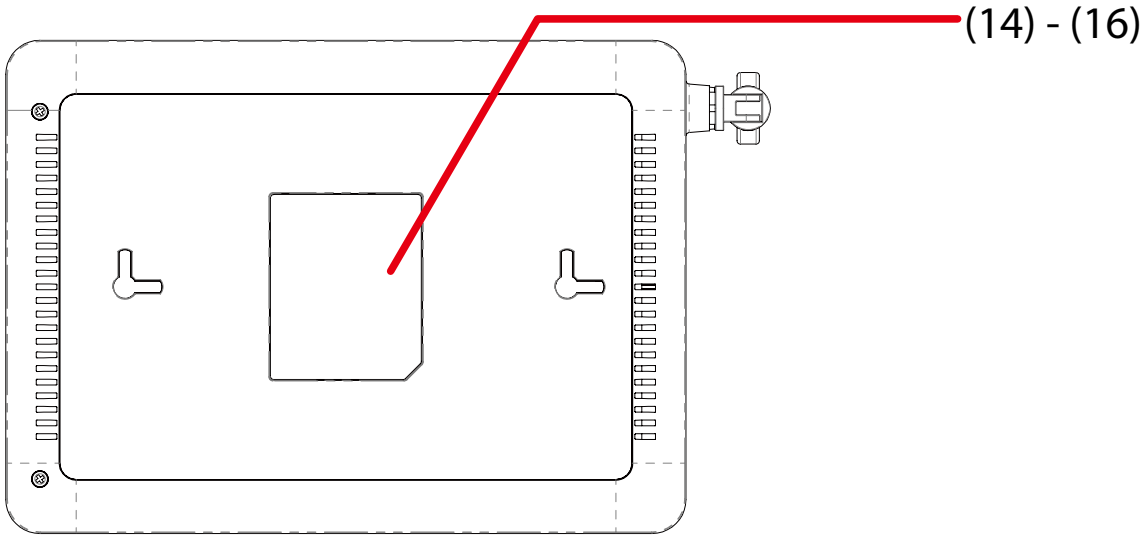
(1)	Wireless LAN Antenna	Wireless antenna for wireless communication		
(2)	POWER LED (Green/Orange/Red)	Green	ON	Powering on
		Red	Blink	USB storage error
			Blink rapidly	USB over current
(3)	STATUS LED (Green/Red)	Green	ON	Smart Wireless Setup is completed (* Turns off in 3 mins)
			Blink	Smart Wireless Setup is in progress
		Red	ON	Smart Wireless Setup failed (* Turns off in 3 mins) (Timeout/Overlap error occur)
			Blink rapidly	Smart Wireless Setup (PIN code method) failed (* Blinks for 1 sec)
			Blink	Updating firmware
(4)	5GHz LED (Green/Orange/Red)	Green	ON	One or more 5GHz wireless interfaces are active
			Blink	Communicating over a wireless LAN
		OFF		5GHz wireless interface is not active. Smart Wireless Setup is in progress at 2.4GHz (* STATUS LED blinks Green)
		Orange	ON	Host AP is connected by WDS
			Blink	Communicating in WDS
		Red	ON	DFS in progress (communication is disabled then) (* Turns off in 1 min)
(5)	2.4GHz LED (Green/Orange/Red)	Green	ON	One or more 2.4GHz wireless interfaces are active
			Blink	Communicating over a wireless LAN
		OFF		2.4GHz wireless interface is not active. Smart Wireless Setup is in progress at 5GHz (* STATUS LED blinks Green)
		Orange	ON	Host AP is connected by WDS
			Blink	Communicating in WDS
(6)	ACTIVE LED (Green/Orange/Red)	Green	ON	Ready
			Blink	Powering on
		Orange	Blink	Running in Configuration Mode
		Red	Blink	Configuration Mode error

Bottom



(7)	Push Switch (SW1)	When pressed together with the one on your wireless device while AP-500AC is active, wireless configuration can be performed. (Smart Wireless Setup)	
(8)	Push Switch (SW2)	Start in **Configuration Mode**	Press and hold this switch for more than 3 sec while AP-500AC is active.
		Factory default configuration	Press and hold this switch while turning on AP-500AC. Release the switch in 2 sec or more after Link LED and Status LED turn on.
(9)	USB Port	Connect a USB cable (A-type connector).	
(10)	AC Connector	Connect an AC adaptor.	
(11)	Link LED (Green)	Turns on when connected to a wired LAN.	
(12)	Network Port	Connect a network cable.	
(13)	Status LED (Yellow)	Blinks while communicating in a wired LAN.	

Back



(14)	Default	
	SSID (2.4GHz/5GHz)	SSID of 2.4GHz/5GHz (default value)
	Key	Network key (default value)
	PIN Code	Authentication mode (default value)
	Authentic	Encryption mode (default value)
	Encryption	PIN code (default value)
	Password	Login password (default value)
	IP Address	IP Address (default value)
(15)	E/A	Ethernet Address
(16)	S/N	Serial Number

2-3. Hardware Specification

Operating environment	Temperature : +0 C to +40 C , +32 F to +104 F	
	Humidity : 20% to 80%RH (Non-condensing)	
Storage environment	Temperature : -10 C to +50 C , +14 F to +122 F	
	Humidity : 20% to 90%RH (Non-condensing)	
EMI	VCCI Class B	
	FCC Part15 SubPart B Class B	
	ICES-003 Class B	
CPU	32bit RISC CPU	
Memory	RAM: 256MByte	
	ROM: 16MByte	
	eMMC: 4GByte	
Wired network interface	10BASE-T/100BASE-TX/1000BASE-T(Auto-sensing) : 1 port	
	Auto MDI/MDIX	
	Power over Ethernet PoE	
Wireless network interface	IEEE 802.11a/b/g/n/ac	
	(For channels you can use, check the regulations in your country.)	
Antenna	Non-directional antenna	
USB interface	USB2.0 Hi-Speed port (A type) : 1 port	
Push Switch	2	For Smart Wireless Setup : 1
		For Configuration Mode/Factory default configuration : 1
LED	Front	POWER LED (Green/Orange/Red)
		ACTIVE LED (Green/Orange/Red)
		2.4GHz LED (Green/Orange/Red)
		5GHz LED (Green/Orange/Red)
		STAT LED (Green/Red)
	Network Port	Status LED (Yellow)
		Link LED (Green)

FCC / IC Notice

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

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

2.4GHz device
FCCID : N6C-SXPCEGN
IC : 4908B-SXPCEGN

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.

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.

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions:
(1) This device may not cause interference; and
(2) This device must accept any interference, including interference that may cause undesired operation of the device.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence.
L'exploitation est autorisée aux deux conditions suivantes :
1) l'appareil ne doit pas produire de brouillage;
2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

- Antenna type
  Embedded PCB Antenna

- Model
  H2B1BC2A1B

- Antenna Gain
  2.12dBi

5GHz device
FCCID : N6C-SXPCEAC
IC : 4908A-SXPCEAC

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

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

FCC Rules Part 15 Subpart C §15.247 and Subpart E / IC RSS-102 §2.6
This equipment complies with FCC/IC radiation exposure limits set forth for an uncontrolled environment and meets the FCC radio frequency (RF) Exposure Guidelines and RSS-102 of the IC radio frequency (RF) Exposure rules. This equipment should be installed and operated keeping the radiator at least 20cm or more away from person's body.

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

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

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

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

RSS-Gen §8.3
This radio transmitter 4908A-SXPCEAC has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

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

- Antenna type
  Flying Lead Antenna

- Model
  KWM-619BMPW9-890

- Antenna Gain
  2.0dBi

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

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

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

2-4. Software Specification

TCP/IP	Network layer	ARP, IP, ICMP
	Transport layer	TCP, UDP
	Application layer	BOOTP, DHCP(Client/Server), HTTP, WINS(NBNS), NTP, SNMP, SSH, JCP(Silex proprietary protocol), SXUPTP(Silex proprietary protocol), SX-KeepAlive(Silex proprietary protocol), SXSMP(Silex proprietary protocol)

2-5. Power Supply

AP-500AC can receive electrical power via a AC adaptor or network cable.

AP-500AC can receive electrical power from the IEEE802.3af compliant power supply unit over a network cable. For details, please see the operating manual that came with your power supply devices.

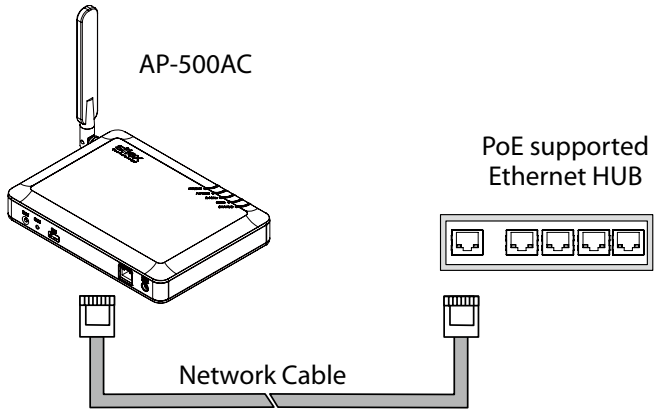
Note

- PoE is a technology to supply electrical power over Ethernet cable (Category 5 or above). This technology allows you to connect your PoE supported devices to the Ethernet even in a location without electrical outlet nearby.

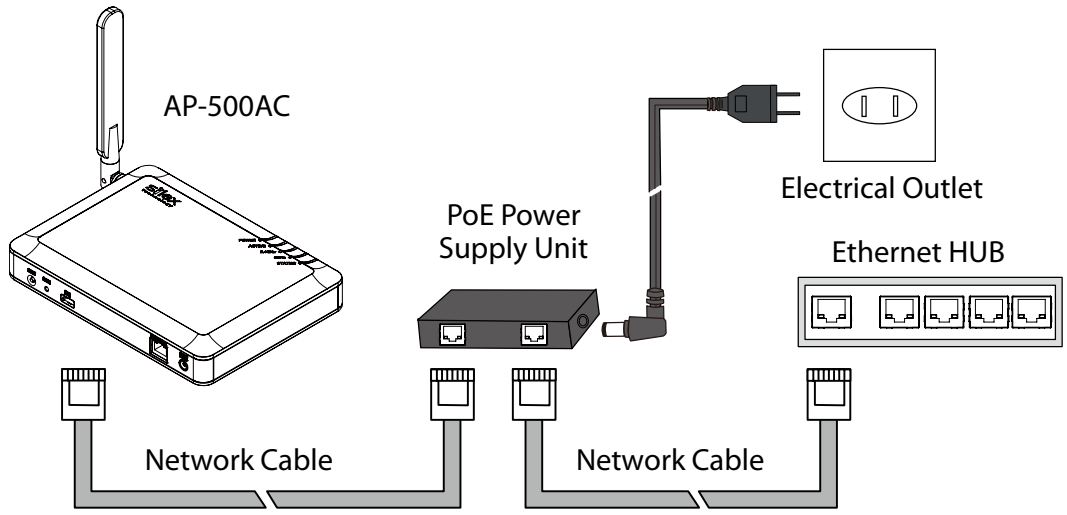
TIP

- When receiving power over Ethernet, you do not have to use the AC adaptor that came with AP-500AC.
- Please remember that power is supplied from the AC adaptor if it is connected to AP-500AC.

Sample connection1: When using a PoE supported HUB



Sample connection2: When using a PoE power supply unit



2-6. Wireless Interference Information

Notes

Do not use AP-500AC near the following devices or places.

- Microwave, pacemaker, etc. of industrial, scientific and medical devices
- Licensed radio station in a factory
- Small power radio station (A non-licensed radio station)

These devices may use the same band. If you use AP-500AC near these devices, the radio waves emitted from AP-500AC may interfere with them.

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

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

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

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

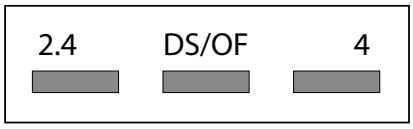
- Please do not disassemble or remodel the product. Such action is prohibited by law.
- Please do not remove the certificate label. Using the product without a label is prohibited.

Wireless devices using 2.4GHz band

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

- Before you use AP-500AC, check that it does not interfere with other devices.
- If interference occurs, stop using AP-500AC or change the wireless band. Please consider to create a wall between these devices to avoid interference. Contact us to 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.

DFS

AP-500AC supports DFS (Dynamic Frequency Selection) of the IEEE 802.11h wireless standard. When radar signals are detected, the channel will automatically be switched to avoid interference with radar systems (e.g. weather radar, etc).

One alternative channel can individually be set for W53/W56 channels beforehand, which will be used when radar signals are detected and the channel needs to be switched.
When alternative channels are not specified or radar signals are detected even for that channel, AP-500AC switches the channel in order of the following:

DFS Channels (5GHz band)

W53	HT20/VHT20		52 > 56 > 60 > 64 > 36
	HT40/VHT40	+	52 > 60 > 36
		-	56 > 64 > 40
	VHT80		36
W56	HT20/VHT20		100 > 104 > 108 > 112 > 116 > 120 > 124 > 128 > 132 > 136 > 140
	HT40/VHT40	+	100 > 108 > 116 > 124 > 132
		-	104 > 112 > 120 > 128 > 136
	VHT80		100 > 116, 104 > 120, 108 > 124, 112 > 128, 116 > 100, 120 > 104, 124 > 108, 128 > 112

TIP

- AP-500AC checks if there are radar signals on the DFS channels when it is powered on. During this time, no wireless communication is allowed to AP-500AC.
- If radar signals are detected during or after AP-500AC is powered on, the channel needs to be changed in order to avoid wireless interference. Therefore, if DFS channels are selected, the channel could be changed automatically.
- The radar signals are monitored for a certain amount of time (*) after it is detected, while wireless communication is disabled on AP-500AC then. Once radar signals are detected, the channel will not be available for 30 mins. (* This time period differs depending on the country.)

2-7. Notes on Security

Because a wireless LAN uses electromagnetic signals instead of a network 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.

2-8. OpenSSL License

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

OpenSSL License

---

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.

* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the rouines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

3. Configuration Using Web Page

This chapter explains how to configure AP-500AC.

3-1. Displaying Web Page of AP-500AC (Initial Configuration)

AP-500AC settings can be configured from its Web page.
When AP-500AC has default setting, the Web page can be displayed by the following methods. Display the Web page using a method appropriate for your environment.

Using a wired LAN

Connect AP-500AC and PC via a wired LAN to display the Web page. It is possible to connect two or more AP-500AC units to a wired LAN to configure them at once. Start from this when you connect AP-500AC to your existing wired LAN.

Configuration Mode

Connect AP-500AC directly to PC using a network cable to display the Web page. AP-500AC can be configured one by one.

Using a wireless LAN

Connect AP-500AC (running as Access Point) from PC wirelessly to display the Web page.

Smart Wireless Setup

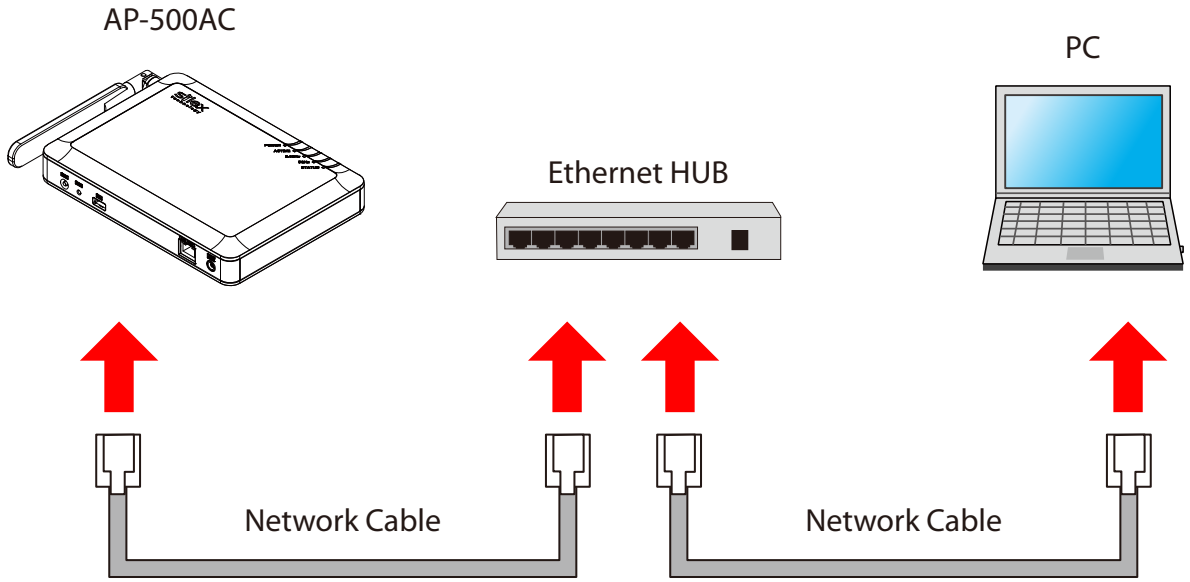
Connect AP-500AC and PC by Smart Wireless Setup to display the Web page.

Using external registrar

Connect AP-500AC and PC using **Set Up a Network** of Windows to display the Web page.

Displaying Web Page Using Wired LAN

Connect AP-500AC and PC via a wired LAN to display the Web page. It is possible to connect two or more AP-500AC units to a wired LAN to configure them at once. Start from this when you connect AP-500AC to your existing wired LAN.



Following items are required:

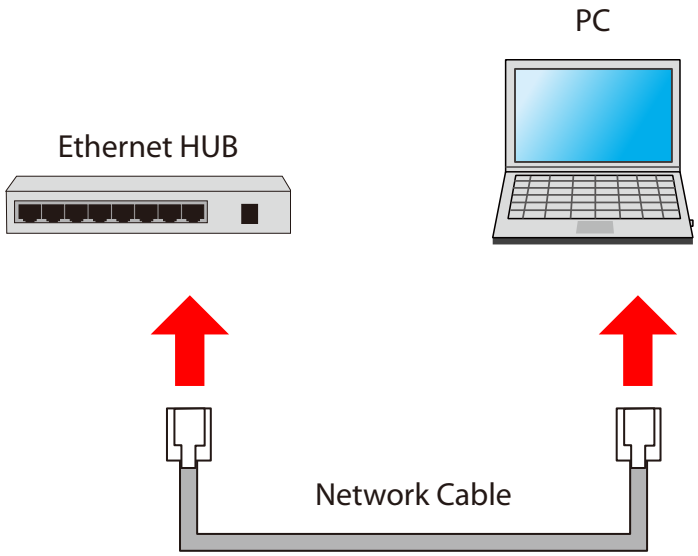
- PC to use for configuration
- Network Cable
- Ethernet HUB

(When receiving power over Ethernet (PoE), PoE Hub or PoE power supply unit is required.)

Note

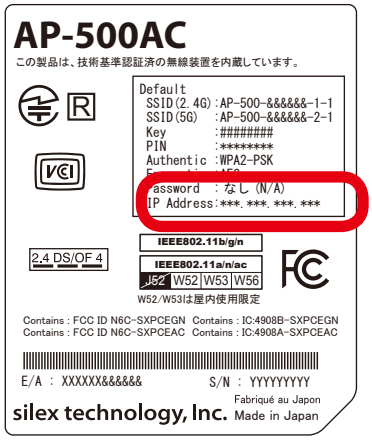
- When there are available LAN ports on the network in which AP-500AC is to be installed, you do not have to purchase a new Ethernet Hub or broadband router as AP-500AC can be connected to the available LAN port.

1. Connect the PC (to use for setup) and Ethernet Hub using a network cable.



2. Check the IP Address of AP-500AC.

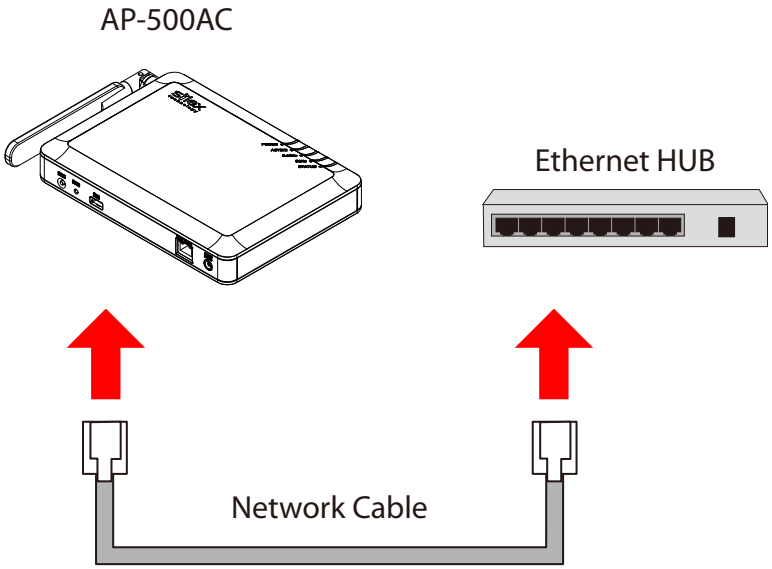
The default IP Address can be found on the back label of AP-500AC.



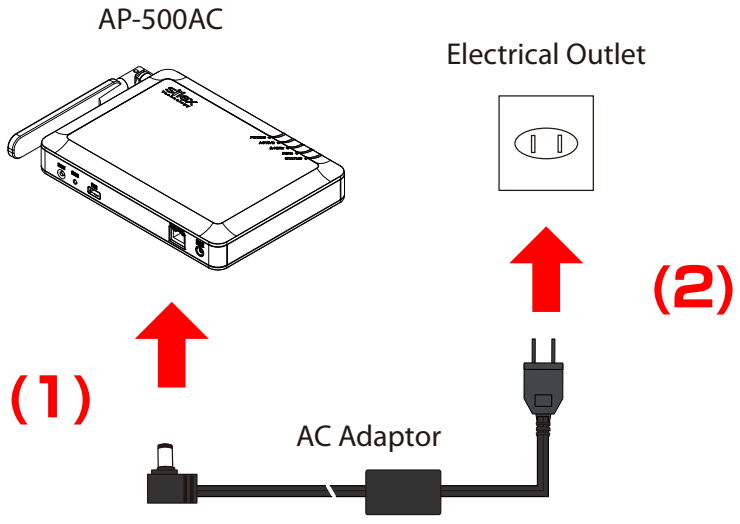
Note

- If AP-500AC was configured for another network in the past and you are not sure what IP Address has been assigned, reset AP-500AC to factory defaults. For how to initialize AP-500AC, refer to **Chapter 5-11 Maintenance Feature** - **Factory Default Configuration**.

3. Connect AP-500AC and Ethernet Hub via a network cable.



4. Connect the AC adapter to AP-500AC and AC plug to a power outlet.



Note

- When receiving a power over Ethernet (PoE), the AC adaptor does not need to be connected. Make sure that the PoE supported HUB or PoE power supply unit is used then.
- To connect two or more AC-500AP units, repeat the process at **2-4**.

5. Change the network settings on the PC to access AP-500AC.

Example:

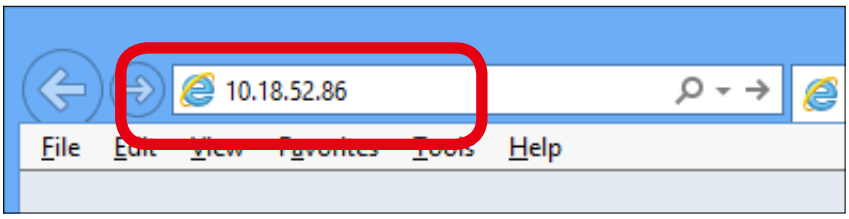
In case the default IP Address of AP-500AC is 10.18.52.86, change the network settings on your PC to the following:

- IP Address : 10.1.2.3
- Subnet Mask : 255.0.0.0

Note

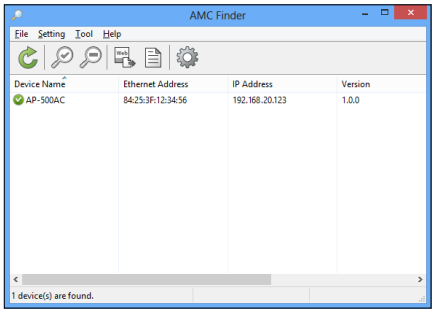
- Please be sure to set a unique address to your PC, that is not used for AP-500AC.

6. Start a Web browser (Internet Explorer, Firefox, etc) on the PC you are using for the setup, enter the IP address of AP-500AC in the address bar and press the ENTER key.

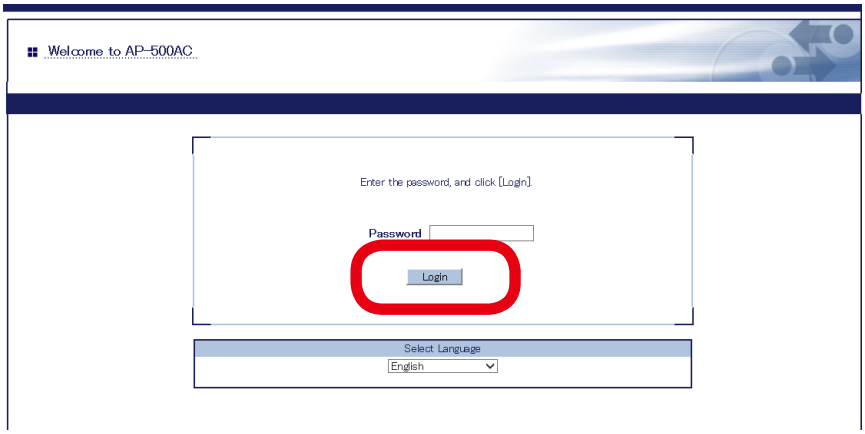


Note

- By using the device search utility "AMC Finder" that can be downloaded from our homepage, it is possible to show all AP-500AC units as a list and access the Web page of each.
  For how to install and use AMC Finder, refer to **5-12. Product Search Utility**.



7. The login menu window is displayed.
Click **Login** to login to the Web page.



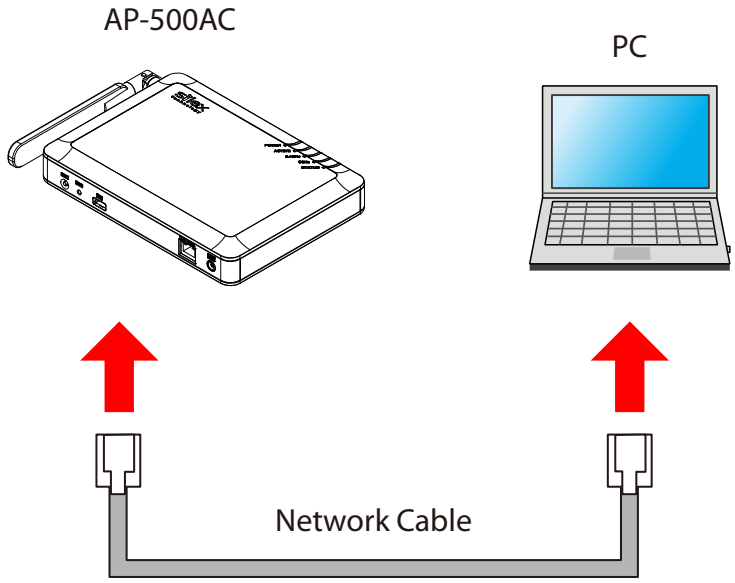
Note

- No password is set by default. In such case, just click **Login**.

Web page has been displayed. Go on to **3-3. Configuration at Web Page**.

Displaying Web Page Using Configuration Mode

Connect AP-500AC directly to PC using a network cable to display the Web page.
AP-500AC can be configured one by one.



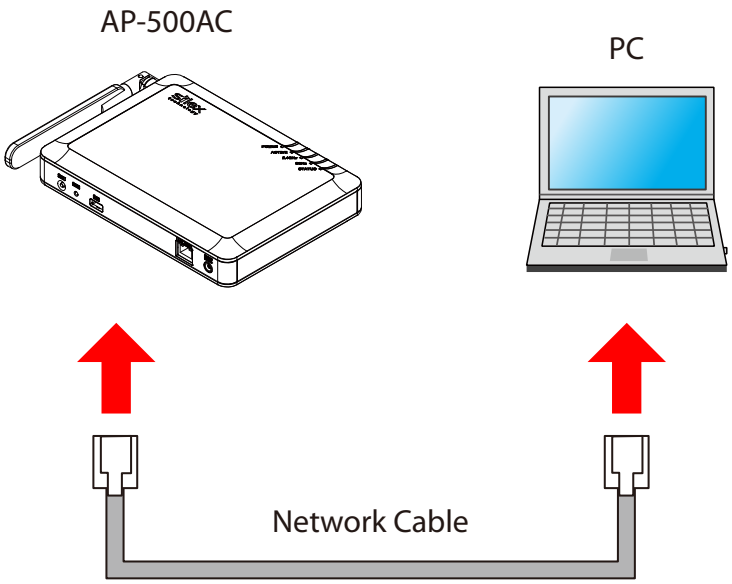
Following items are required:

- PC to use for configuration
- Network Cable

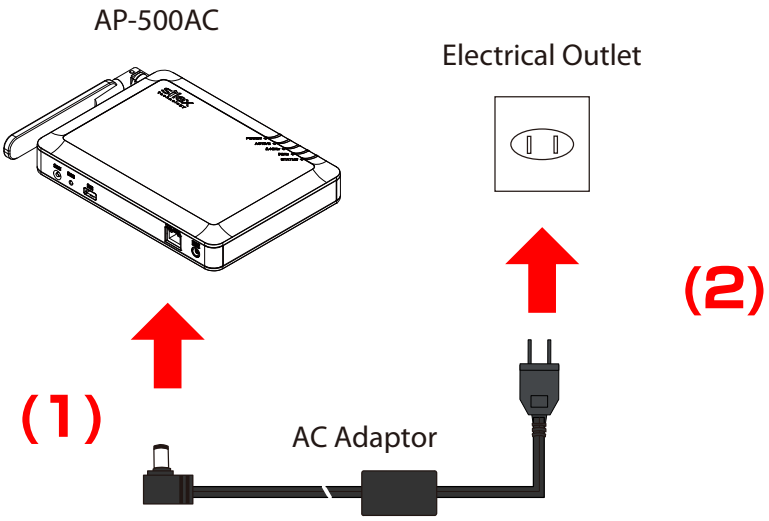
1. If a wireless interface is enabled on the PC (to use for configuration), please disable it temporarily.

Note - If a wireless interface is enabled on the PC, the Web page may not be displayed.

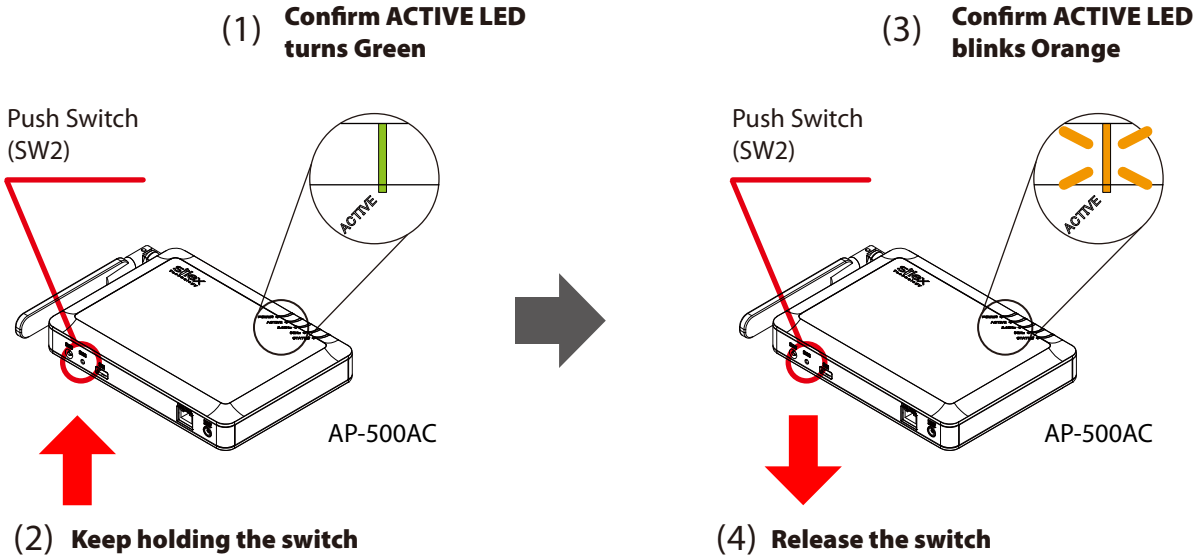
2. Connect AP-500AC and the PC (to use for setup) using a network cable.



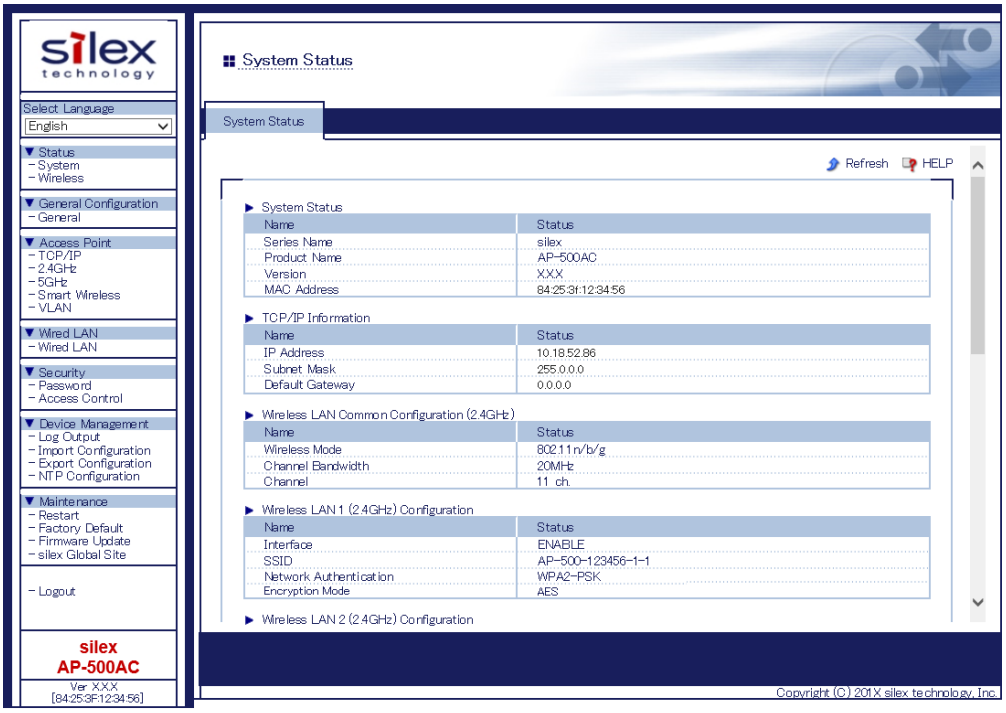
3. Connect the AC adapter to AP-500AC, and the AC adapter's plug to an electrical outlet.



4. When the front ACTIVE LED starts blinking in Green and then turns on to Green, press and hold the push switch with a fine tipped object such as a pen or pencil.
Release the push switch (SW2) when ACTIVE LED starts blinking in Orange (It may take 3sec until blinking).
AP-500AC will start running in the **Configuration Mode** and you will be ready to configure AP-500AC from the PC.

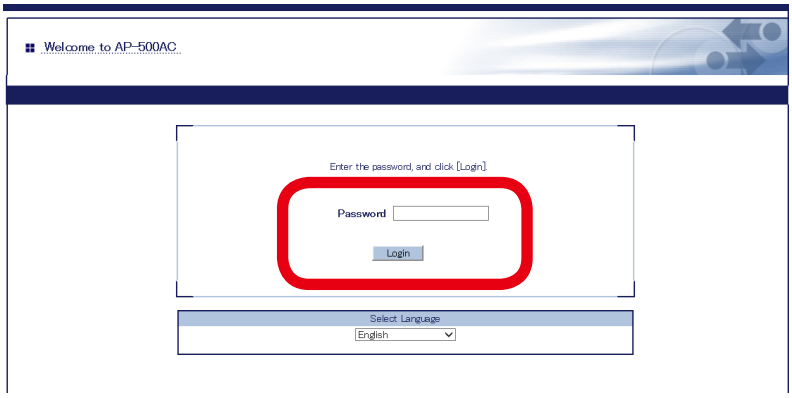


5. Start a Web browser (Internet Explorer, Firefox, etc) on the PC you are using for the setup. The Web page of AP-500AC is displayed.



Note

- If the Web page is not displayed, enter "**http://silex**" in the address bar of the Web browser and press the Enter key.
- If a password is set to AP-500AC, a password entry screen is displayed.
- The password entry screen is not displayed at the initial setup.



Web page has been displayed. Go on to **3-3. Configuration at Web Page**.

Displaying Web Page Using Wireless LAN

Connect AP-500AC and PC wirelessly to display the Web page.

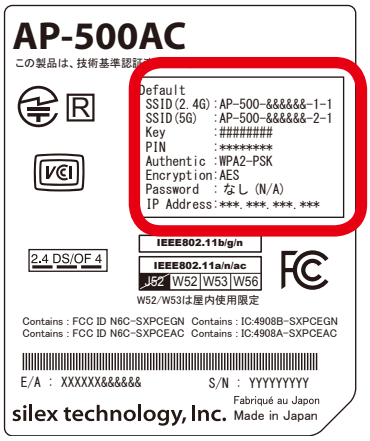
Following items are required:

- PC to use for configuration

TIP

- By default, it is impossible to access Web page as the port filter setting denies HTTP access over a wireless LAN. To use this method, change the port filter setting in advance to allow HTTP access over a wireless LAN.

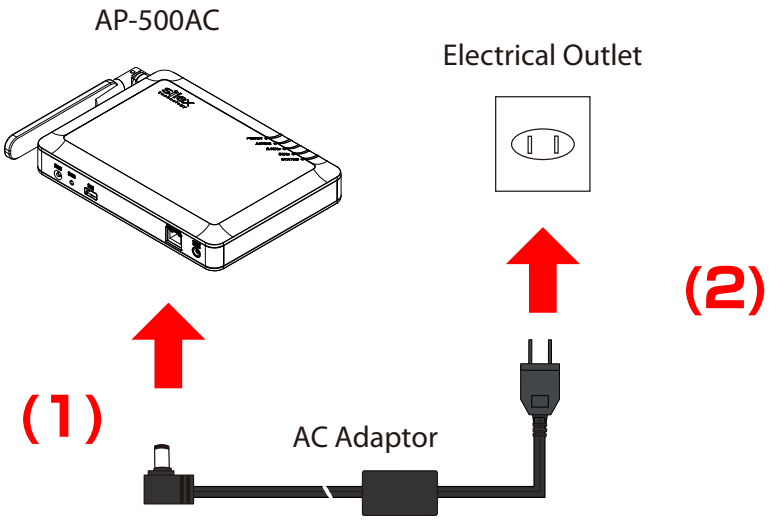
1. Check the SSID, security key and IP Address of AP-500AC.
The default values can be found on the back label of AP-500AC.



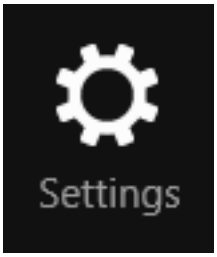
Note

- If AP-500AC was configured for another network in the past and you are not sure what IP Address has been assigned, reset AP-500AC to factory defaults. For how to initialize AP-500AC, refer to **Chapter 5-11 Maintenance Feature** - **Factory Default Configuration**.

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

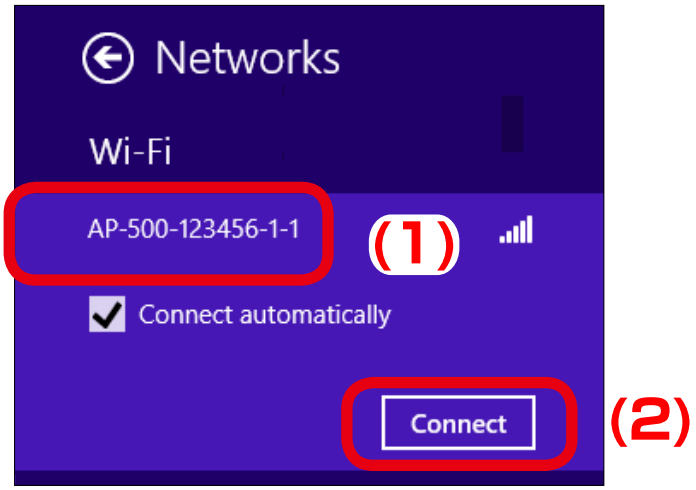


3. Move your cursor to top-right or bottom right corners (when a touch-panel device is used, swipe your finger from the right edge) and click **Settings** from the charm bar.



4. Click the icon below to show the wireless connection window.

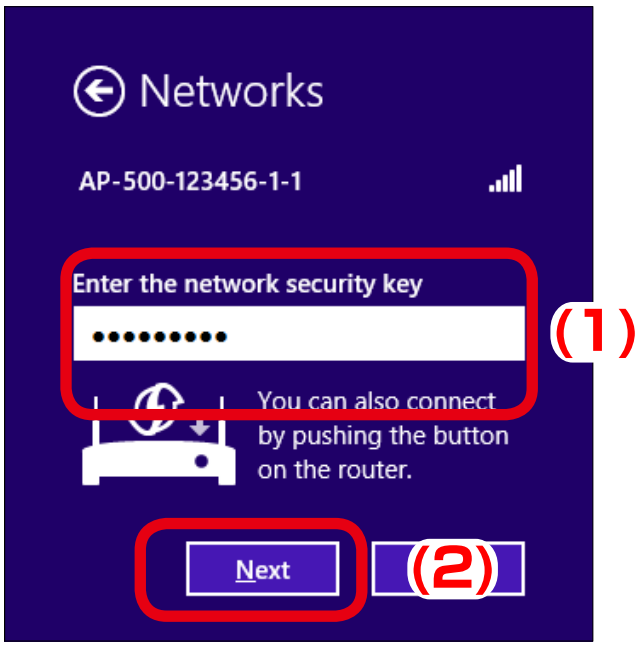
5. Select the SSID configured on AP-500AC from a list and click **Connect**.



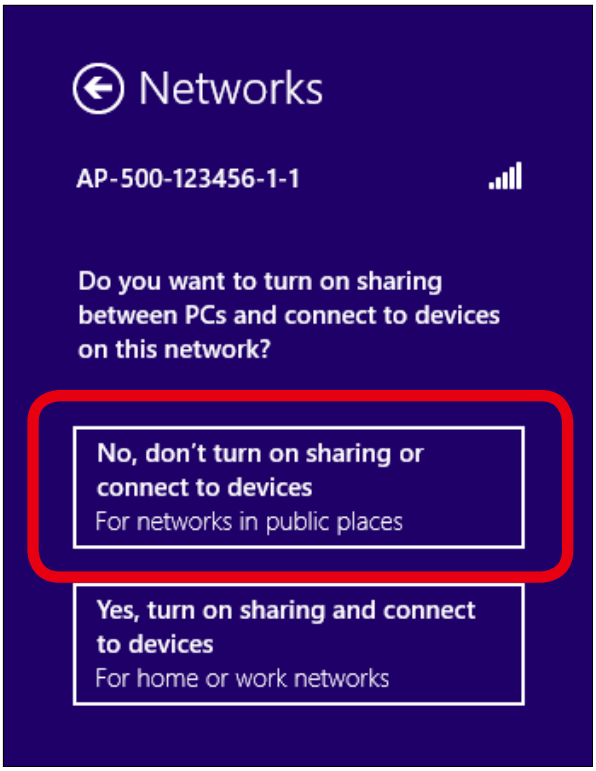
Note

- When **Connect automatically** is checked, the PC will automatically be connected when it is restarted next time.

6. Enter the security key of AP-500AC for **Enter the network security key** and click **Next**.



7. Click **No, don't turn on sharing or connect to devices**.



8. Change the network settings on the PC to access AP-500AC.

Example:

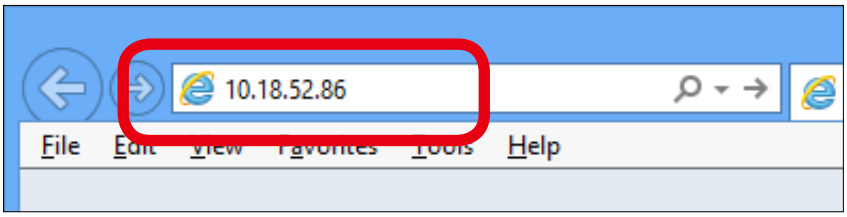
In case the default IP Address of AP-500AC is 10.18.52.86, change the network settings on your PC to the following:

- IP Address : 10.1.2.3
- Subnet Mask : 255.0.0.0

Note

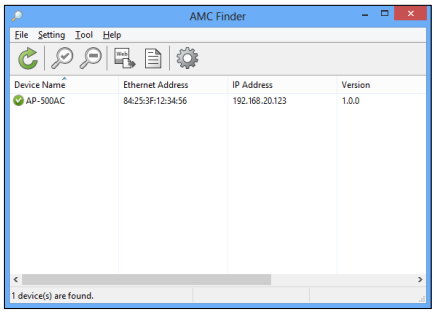
- Please be sure to set a unique address to your PC, that is not used for AP-500AC.

9. Start a Web browser (Internet Explorer, Firefox, etc) on the PC you are using for the setup, enter the IP address of AP-500AC in the address bar and press the ENTER key.

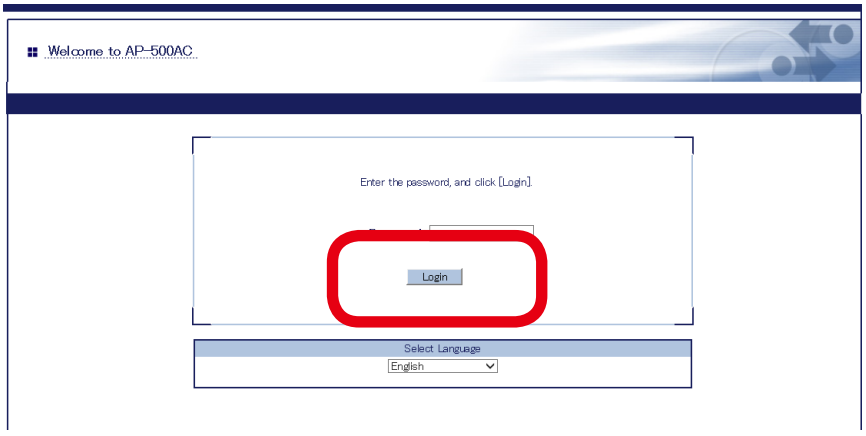


Note

- By using the device search utility "AMC Finder" that can be downloaded from our homepage, it is possible to show all AP-500AC units as a list and access the Web page of each. For how to install and use AMC Finder, refer to **5-12. Product Search Utility**.



10. The login menu window is displayed.
Click **Login** to login to the Web page.



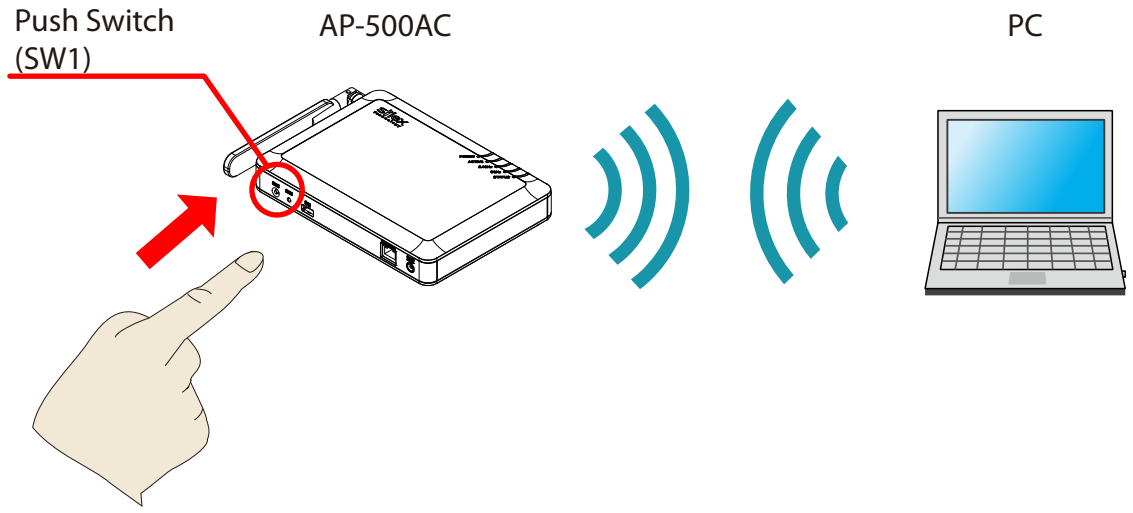
Note

- No password is set by default. In such case, just click **Login**.

Web page has been displayed. Go on to **3-3. Configuration at Web Page**.

Displaying Web Page by Smart Wireless Setup

Use the Smart Wireless Setup switch (push switch SW1) to connect AP-500AC and PC via a wireless LAN as well as display the Web page.



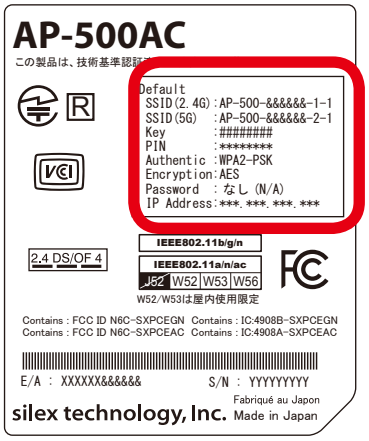
Following items are required:

- PC to use for configuration

TIP

- By default, it is impossible to access Web page as the port filter setting denies HTTP access over a wireless LAN. To use this method, change the port filter setting in advance to allow HTTP access over a wireless LAN.
- During this configuration, please place your PC closer to AP-500AC so that they can communicate better.

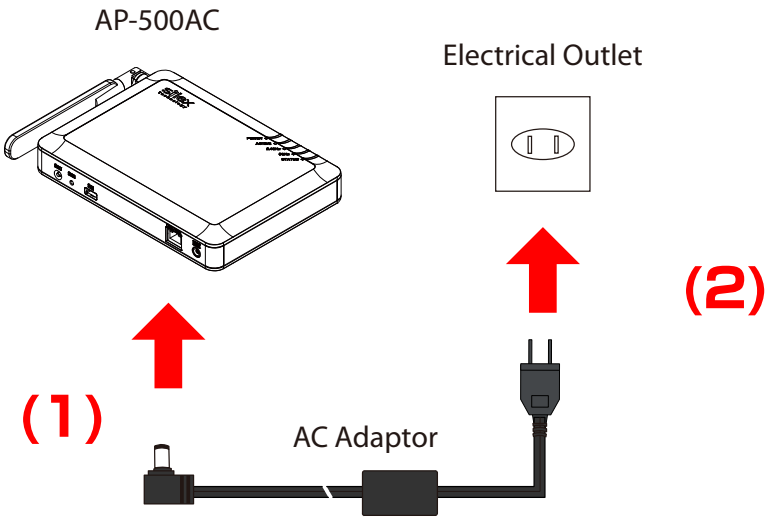
1. Check SSID(2.4GHz) and IP Address of AP-500AC.
The default values can be found on the back label of AP-500AC.



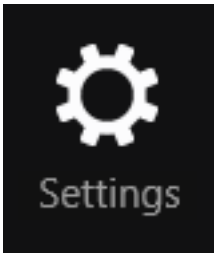
Note

- By default, wireless interface 1 (2.4GHz) is set as wireless interface that can use Smart Wireless Setup.
- If AP-500AC was configured for another network in the past and you are not sure what IP Address has been assigned, reset AP-500AC to factory defaults. For how to initialize AP-500AC, refer to **Chapter 5-11 Maintenance Feature** - **Factory Default Configuration**.

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

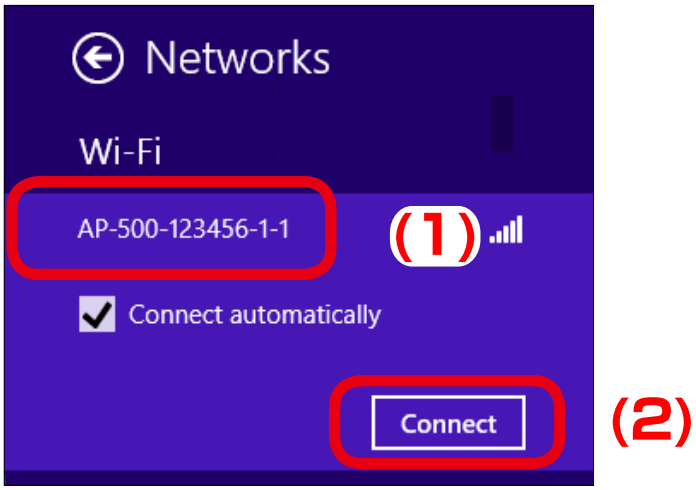


3. Move your cursor to top-right or bottom right corners (when a touch-panel device is used, swipe your finger from the right edge) and click **Settings** from the charm bar.



4. Click the icon below to show the wireless connection window.

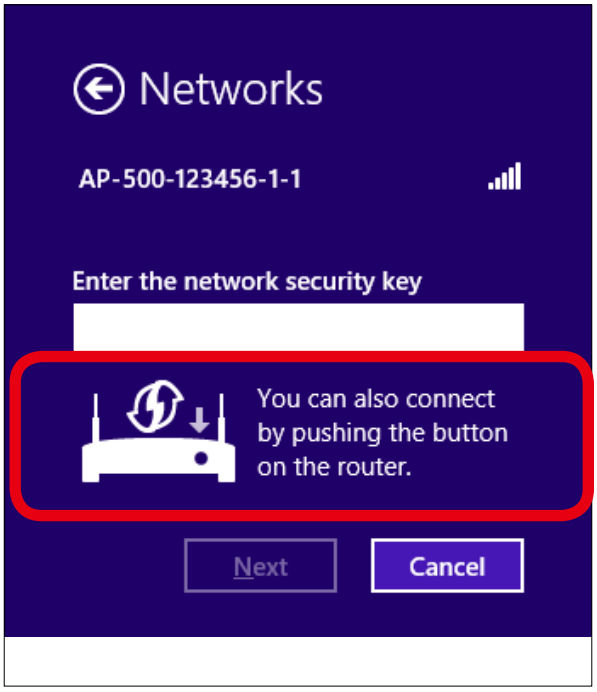
5. Select the SSID configured on AP-500AC from a list and click **Connect**.



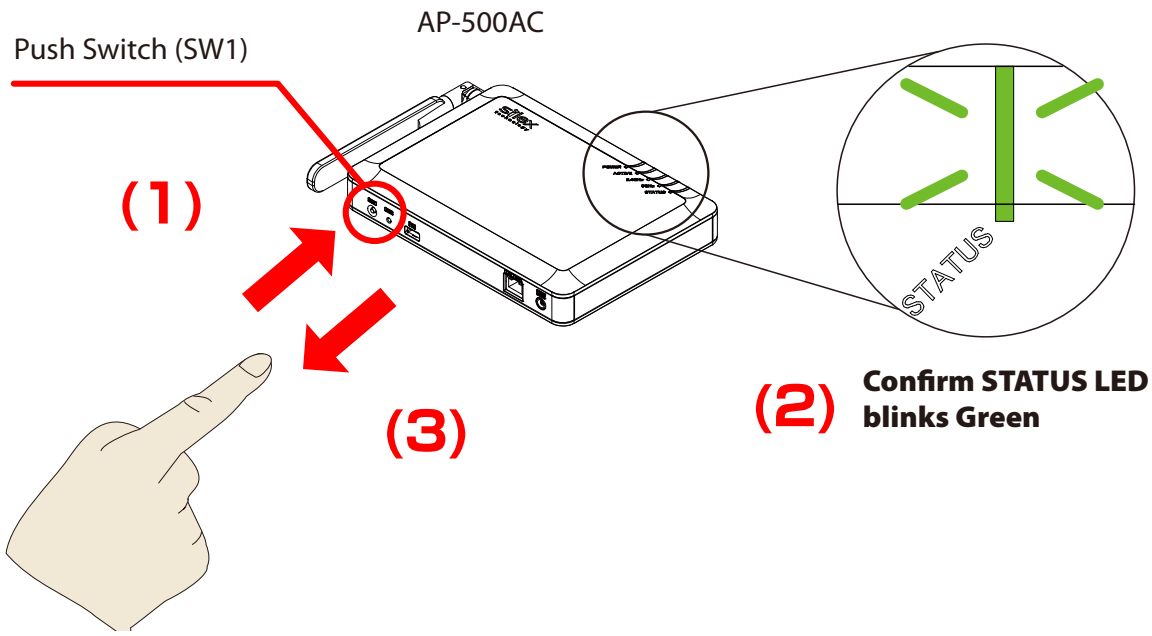
Note

- When **Connect automatically** is checked, the PC will automatically be connected when it is restarted next time.

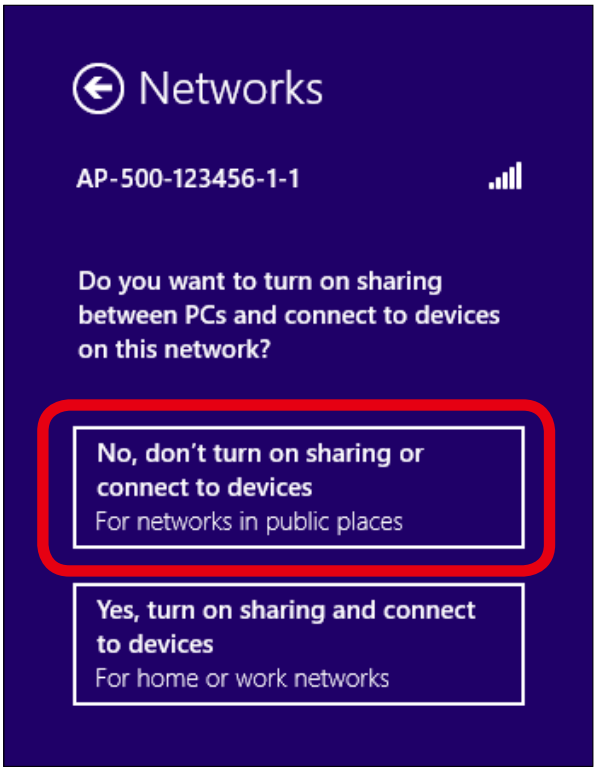
6. The message says **You can also connect by pushing the button on the router.**



7. Press and hold the push switch (SW1). Release it when STATUS LED start blinking in Green.



8. Click **No, don't turn on sharing or connect to devices**.



9. Change the network settings on the PC to access AP-500AC.

Example:

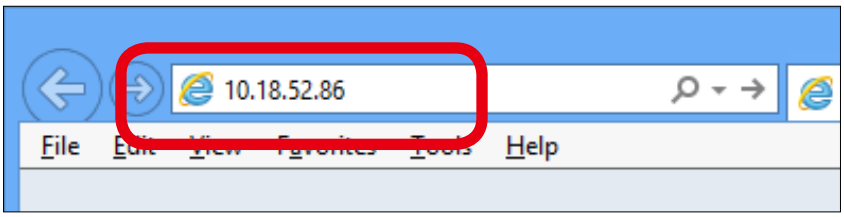
In case the default IP Address of AP-500AC is 10.18.52.86, change the network settings on your PC to the following:

- IP Address : 10.1.2.3
- Subnet Mask : 255.0.0.0

Note

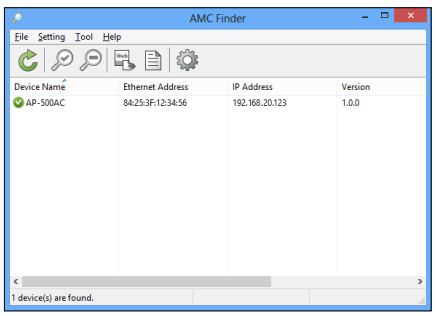
- Please be sure to set a unique address to your PC, that is not used for AP-500AC.

10. Start a Web browser (Internet Explorer, Firefox, etc) on the PC you are using for the setup, enter the IP address of AP-500AC in the address bar and press the ENTER key.

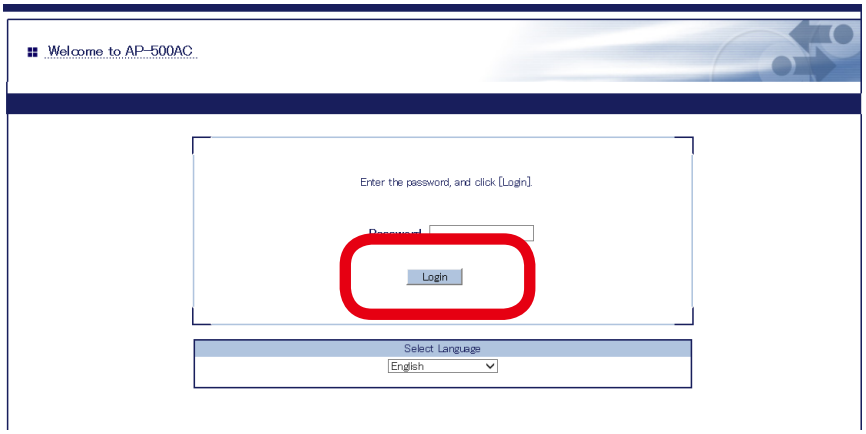


Note

- By using the device search utility "AMC Finder" that can be downloaded from our homepage, it is possible to show all AP-500AC units as a list and access the Web page of each.
  For how to install and use AMC Finder, refer to **5-12. Product Search Utility**.



11. The login menu window is displayed.
Click **Login** to login to the Web page.



Note

- No password is set by default. In such case, just click **Login**.

Web page has been displayed. Go on to **3-3. Configuration at Web Page**.

Displaying Web Page Using External Registrar

Connect AP-500AC and PC using **Set up a new connection or network** of Windows 8 to display the Web page.

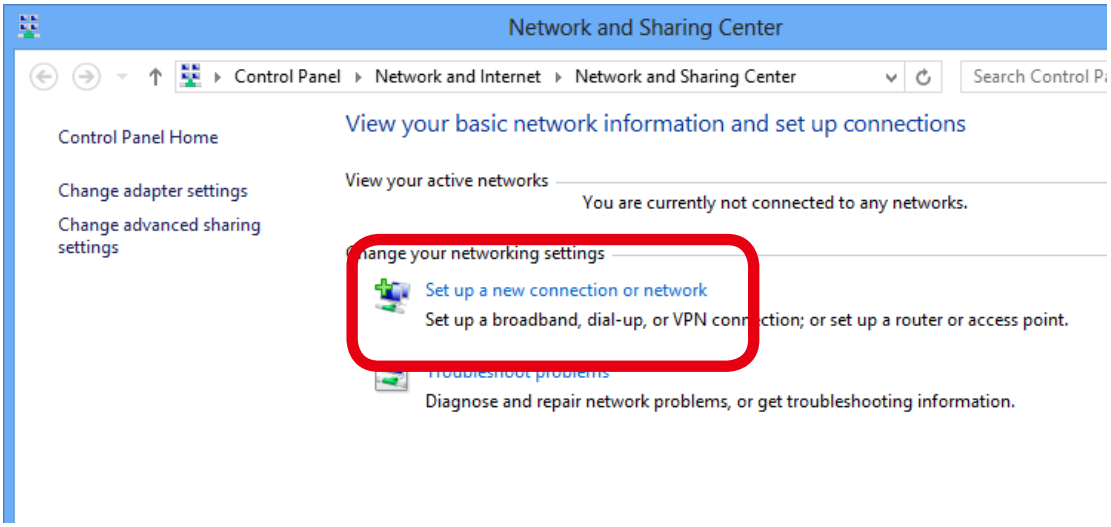
Following items are required:

- PC to use for configuration

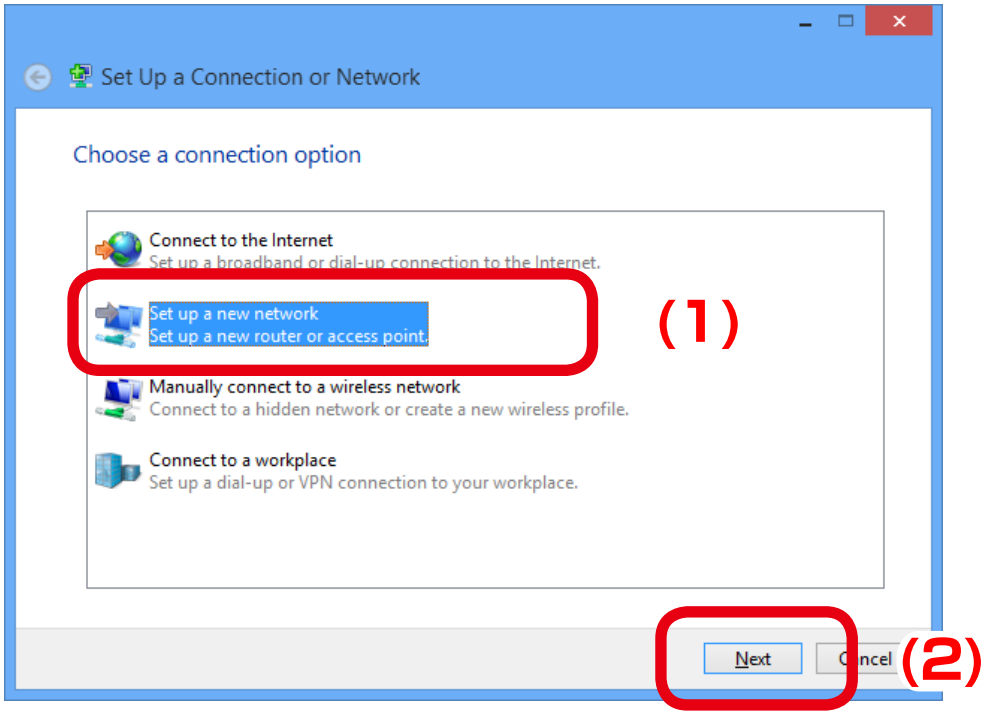
TIP

- To continue this configuration, **External Registrar** must be set to **ENABLE** and **Wireless LAN config status** needs to be **Unconfigured** on AP-500AC. Before you begin, please check these settings at the **Smart Wireless Setup** page on the Web page.
- By default, it is impossible to access Web page as the port filter setting denies HTTP access over a wireless LAN. To use this method, change the port filter setting in advance to allow HTTP access over a wireless LAN.

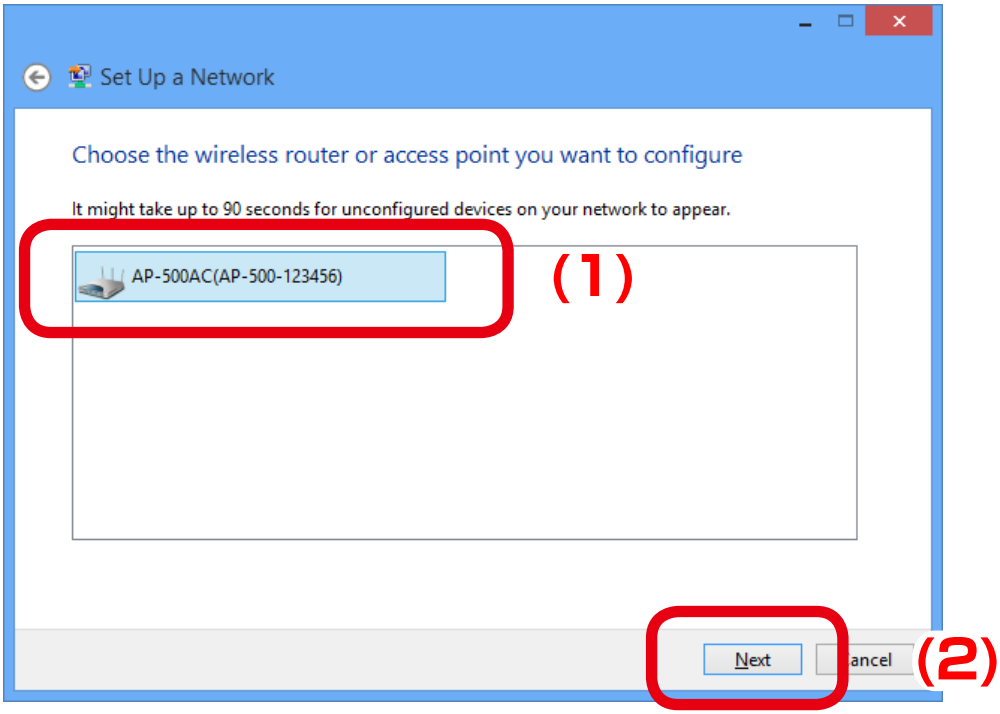
1. On the PC, go **Control Panel** and click **Network and Internet - Network and Sharing Center** and click **Set up a new connection or network**.



2. Select **Set up a new network** and click **Next**.



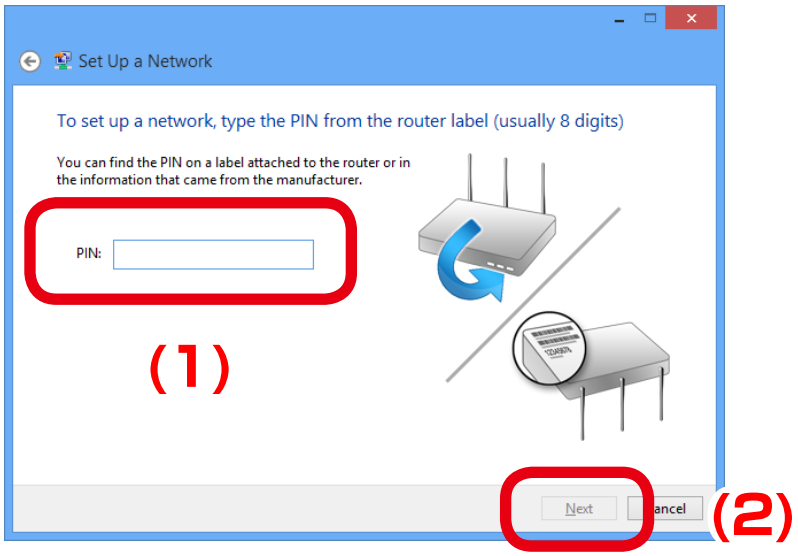
3. Select AP-500AC and click **Next**.



Note

- If two or more of AP-500AC are displayed, select the correct one by checking the host name on the right.

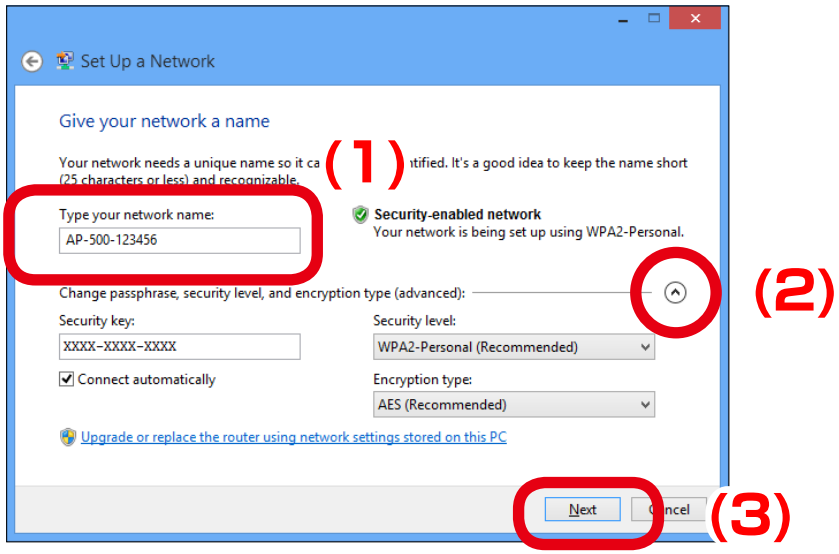
4. Enter the PIN code of AP-500AC to **PIN:** field and click **Next**.



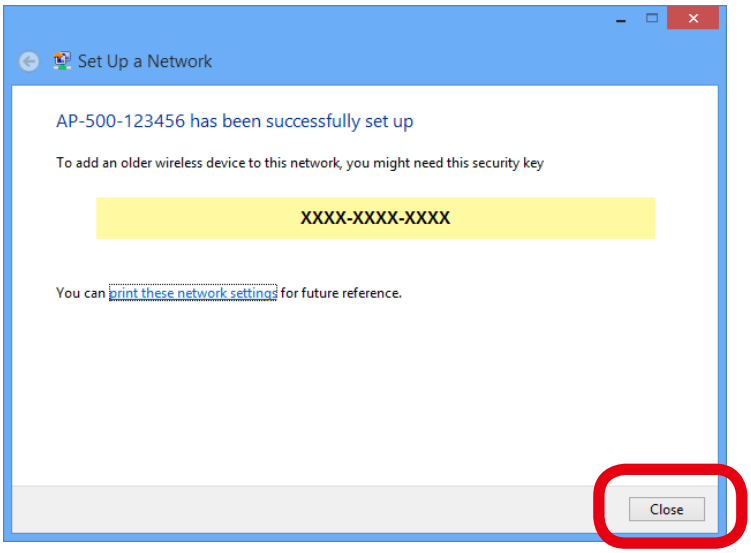
TIP

- PIN code is a 8-digit number that can be found on the bottom label of AP-500AC.

5. Enter an SSID to **Type your network name**.
Click the down arrow button on the right of **Change passphrase, security level and encryption type (advanced)** to configure **Security key**, **Security level, Encryption type** and **Connect automatically**. When finished entering the settings, click **Next**.



6. Click **Close**.



Note

- It is recommended to take notes of the security key.

7. Change the network settings on the PC to access AP-500AC.

Example:

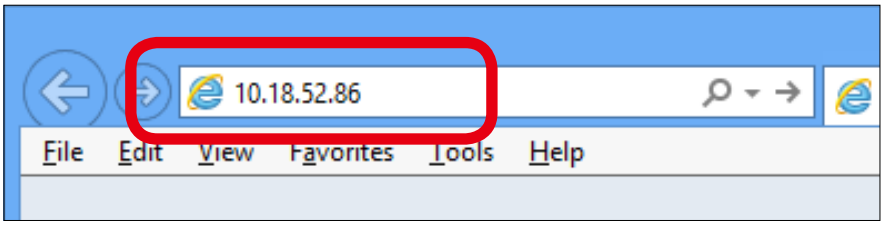
In case the default IP Address of AP-500AC is 10.0.17.34, change the network settings on your PC to the following:

- IP Address : 10.1.2.3
- Subnet Mask : 255.0.0.0

Note

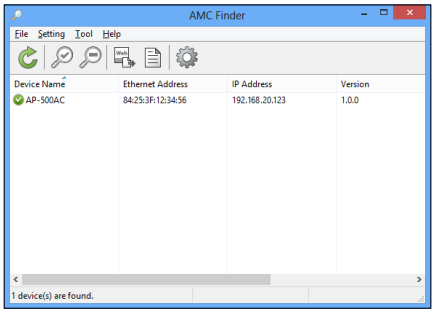
- Please be sure to set a unique address to your PC, that is not used for AP-500AC.

8. Start a Web browser (Internet Explorer, Firefox, etc) on the PC you are using for the setup, enter the IP address of AP-500AC in the address bar and press the ENTER key.

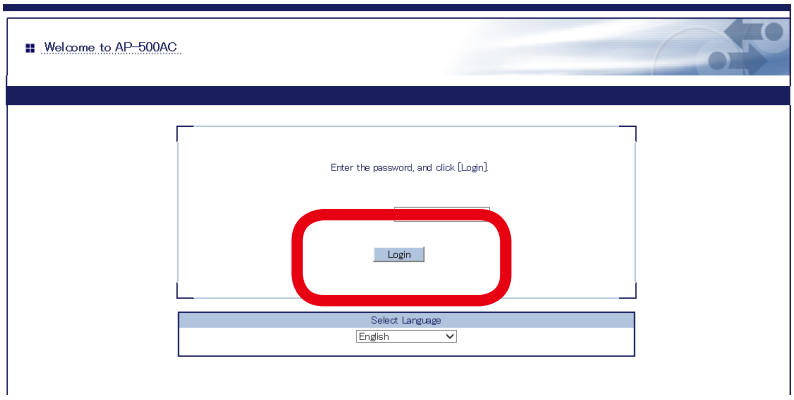


Note

- By using the device search utility "AMC Finder" that can be downloaded from our homepage, it is possible to show all AP-500AC units as a list and access the Web page of each. For how to install and use AMC Finder, refer to **5-12. Product Search Utility**.



9. The login menu window is displayed.
Enter the password and click **Login** to login to the Web page.



Note

- No password is set by default. In such case, just click **Login**.

Web page has been displayed. Go on to **3-3. Configuration at Web Page**.

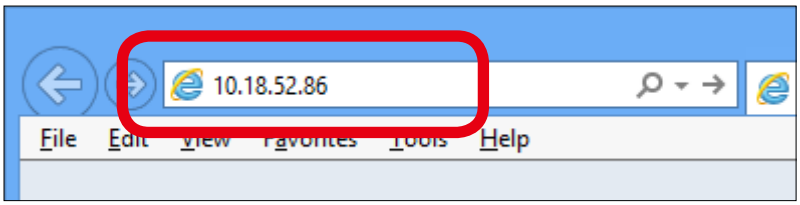
3-2. Displaying Web Page of AP-500AC (After Initial Configuration)

AP-500AC settings can be configured from its Web page.
After the initial configuration is finished, access the Web page of AP-500AC on your PC to change the settings.

TIP

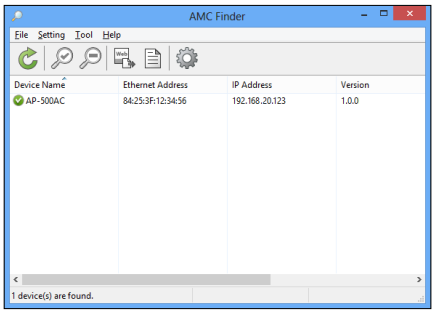
- If the PC is blocked by MAC Address filter of AP-500AC, the Web page cannot be displayed.
- By default, it is impossible to access Web page as the port filter setting denies HTTP access over a wireless LAN. To use this method, change the port filter setting in advance to allow HTTP access over a wireless LAN.

1. Start a Web browser (Internet Explorer, Firefox, etc) on the PC you are using for the setup, enter the IP address of AP-500AC in the address bar and press the ENTER key.

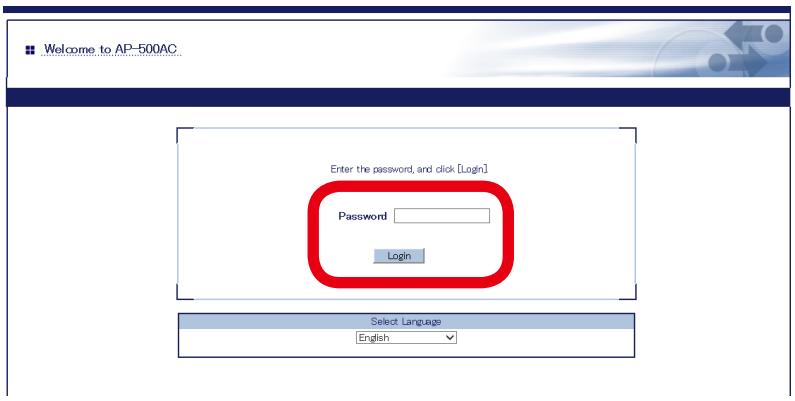


Note

- By using the device search utility "AMC Finder" that can be downloaded from our homepage, it is possible to show all AP-500AC units as a list and access the Web page of each.
  For how to install and use AMC Finder, refer to **5-12. Product Search Utility**.



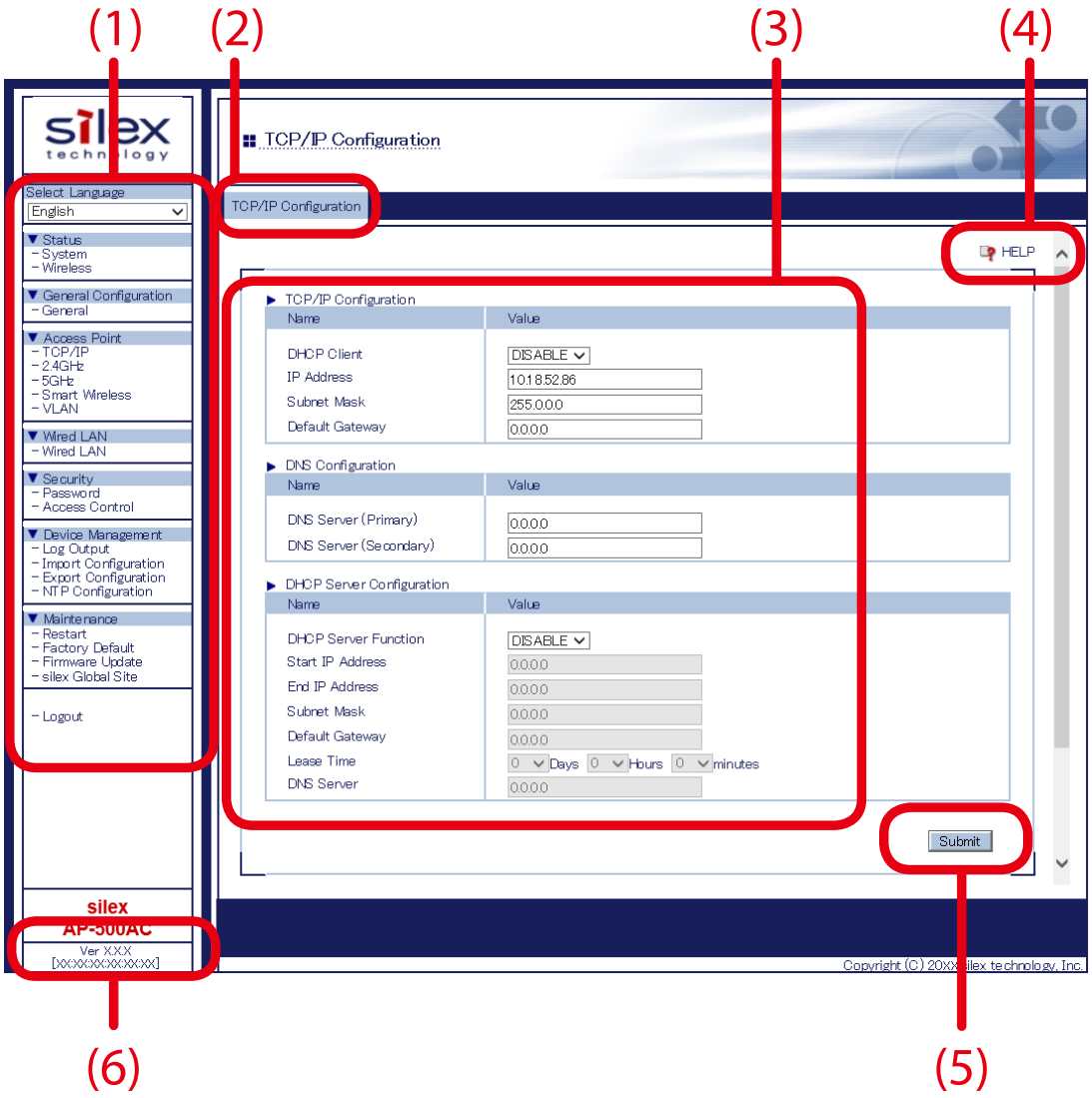
2. The login menu window is displayed.
Enter the password and click **Login** to login to the Web page.



Note

- When no password is set, just click **Login**.

3-3. Configuration at Web Page



(1) Menu

Changes the language (English/Japanese) and provides configuration menu.

(2) Tab

Changes the tabs of configuration.

(3) Configuration page

Provides each setting.

(4) Link to Help page

Opens the Help page that provides explanation on each setting.

(5) Submit button

Saves the settings you configured at each page.

(6) Firmware version / MAC Address

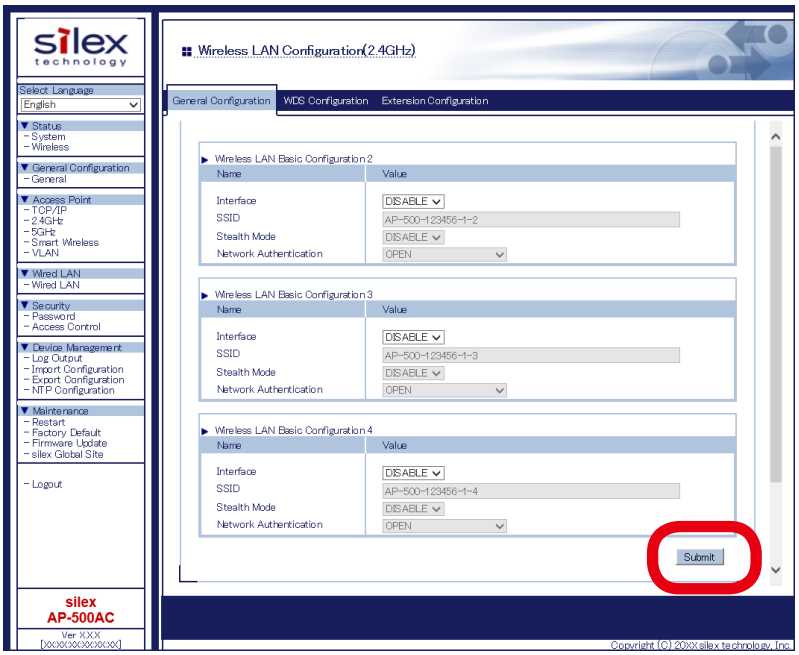
Shows the firmware version and MAC Address of AP-500AC.

Category	Page	Description
Status	System	Shows the system information.
	Wireless	Shows information of the connected wireless client devices.
General Configuration	General	Provides general configuration for TCP/IP and wireless LAN.
Access Point	TCP/IP	Provides the TCP/IP configuration.
	2.4GHz	Provides the wireless LAN configuration (2.4GHz/5GHz). For details on WDS, refer to **5.4 WDS Feature**.
	5GHz	
	Smart Wireless	Provides the settings for Smart Wireless Setup.
	VLAN	Configures the VLAN settings. For details, refer to **5-5. VLAN Feature**.
Wired LAN	Wired LAN	Configures the physical network type.
Security	Password	Configures the password to manage the AP-500AC.
	Access Control	Configures the access control setting. For details on MAC Address filter, refer to **5-6. MAC Address Filter**.
Device Management	Log Output	Configures the log output settings.
	Import Configuration	Configures AP-500AC using a configuration file.
	Export Configuration	Saves the configuration of AP-500AC as a file.
	NTP Configuration	Sets the NTP server to retrieve time information from.
Maintenance	Restart	Restarts AP-500AC.
	Factory Default	Resets AP-500AC to factory default setting.
	Firmware Update	Updates the firmware version of AP-500AC.
	silex Global Site	Displays Silex Technology's homepage.

TIP

- Please be sure to set a password when you connect AP-500AC to a public network.
- Please be sure to use encryption when you connect AP-500AC to the wireless network.
- Wireless bands for IEEE 802.11b/g or IEEE 802.11b/g/n are often in use by other people because the number of devices supporting these standards is growing rapidly. If these wireless modes are used, you may run into issues with having enough communication bandwidth.
- When using AP-500AC outdoors, you must observe the radio regulations of each country. In some countries, the use of particular wireless bands (channels) outdoors is strictly prohibited.
- When using W53 (52/56/60/64ch) or W56 (100/104/108/112/116/120/124/128/132/136/140ch) channels, please be careful of the restrictions addressed at **2. About AP-500AC** - **2-6. Wireless Interference Information** - **DFS**.

1. Click the menu and tabs and configure the settings on each page. When the configuration is finished, click **Submit**.



TIP

- To enable the DHCP server feature, disable the DHCP client feature and assign a static IP Address to AP-500AC.
- MAC Address filter cannot be used on a wireless interface if Smart Wireless Setup is enabled on it. To use MAC Address filter, select the wireless interface that does not use MAC Address filter at **Smart Wireless Setup** page.

Note

- Clicking **Help** on top right of the Web page will open the Help page.
- For details on each configuration item, refer to **A-1. List of All Settings**.
- In each page, click **Submit** button to save the settings you have configured. If other menu is clicked without clicking **Submit** button, the entered information will be cleared.
- Changes will take effect after AP-500AC is restarted.

2. The settings are saved and **Restart** button is displayed.
To continue configuration, click the menu you want to configure next. When necessary settings have been configured, click **Restart**.

Note

- AP-500AC can be restarted from **Restart** page of **Maintenance**.

3. After the **Restart** button is clicked, the progress bar is displayed. When the progress bar reaches the right end, the restart is completed. Close your Web browser.

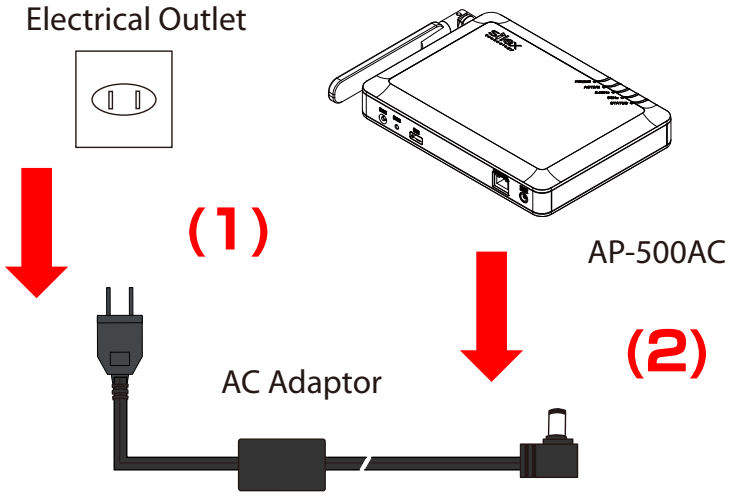
Note

- When restart is completed, ACTIVE LED turns Green on AP-500AC.

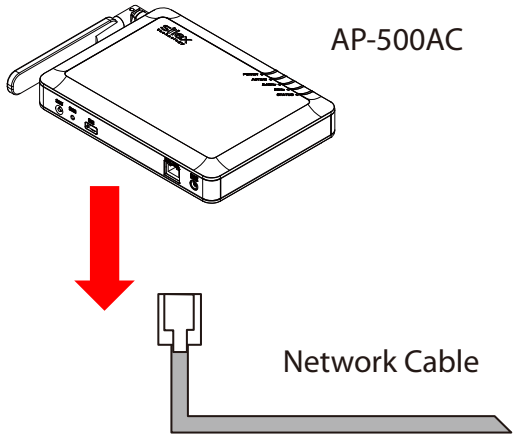
The configuration is completed.

To continue to install AP-500AC to a location of use, unplug the AC adaptor and network cable from AP-500AC according to instructions below.
Go on to **3-4. Installing AP-500AC** then.

1. Unplug the AC plug from the outlet and then AC adaptor from AP-500AC.



2. Unplug the network cable from AP-500AC.



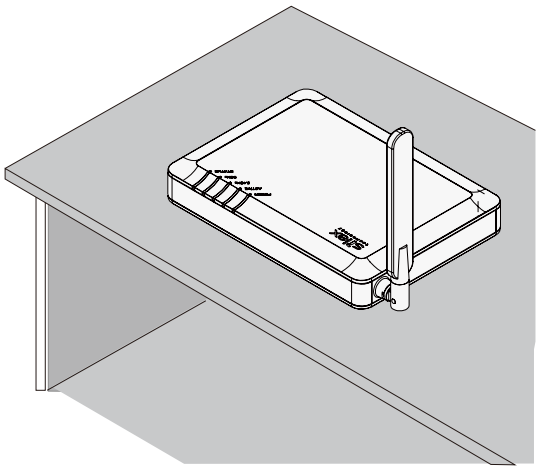
3-4. Installing AP-500AC

Install AP-500AC to a location of use.
Adjust direction of the antenna according to how you have installed the unit.

Location of Installation

When placing the unit on a table

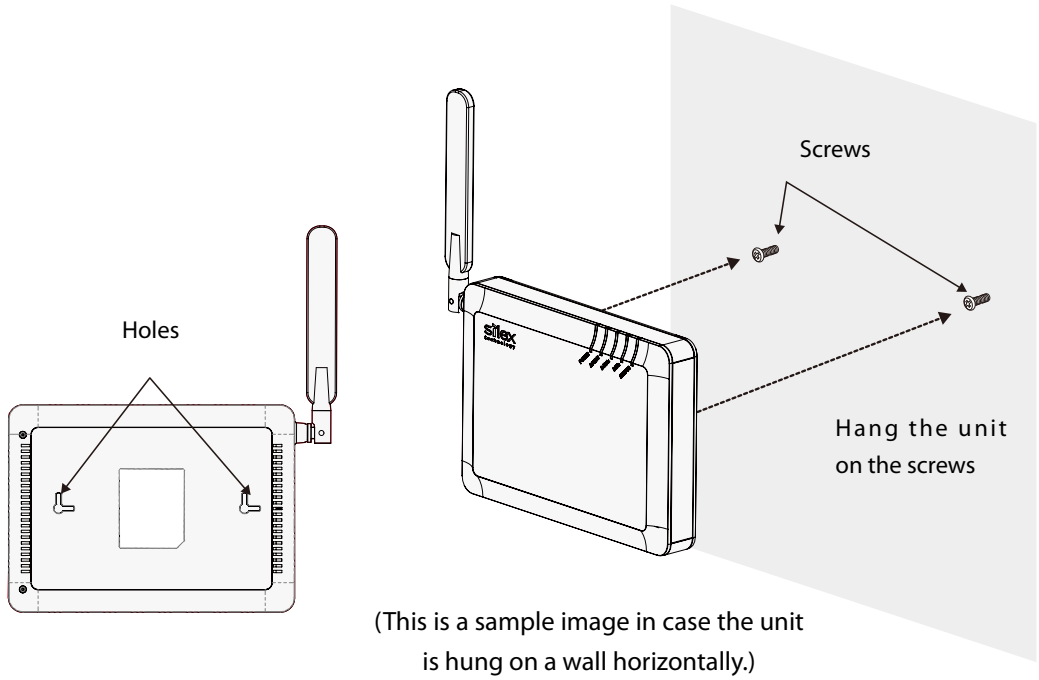
Place the unit on a table with good line of sight.



TIP - Do not place the unit on tilted or unstable surfaces.

When hanging the unit on a wall

Hang the unit on higher position of the wall to make sure of a good line of sight.



(This is a sample image in case the unit is hung on a wall horizontally.)

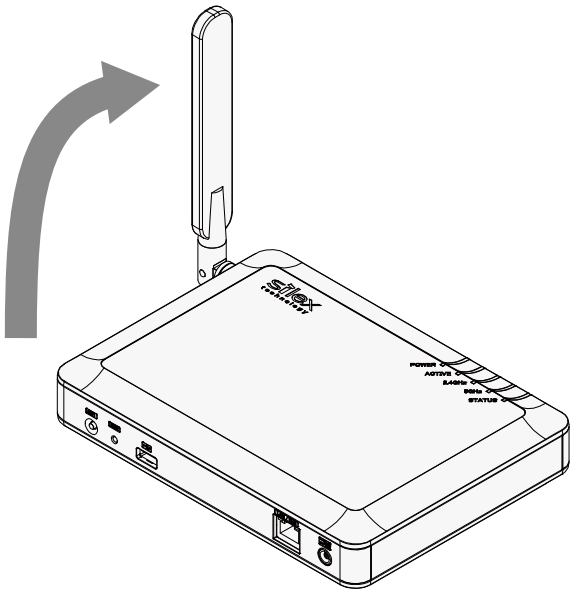
TIP

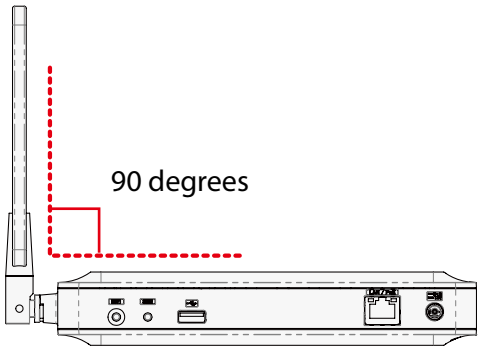
- The screws do not come with the unit. They need to be purchased separately.
- The unit may drop if it is not firmly hung on a wall. After hanging the unit on the screws, slightly move the unit horizontally and vertically to make sure it is fastened.

Change the Antenna Direction

When placing the unit on its bottom

Stand the antenna upright





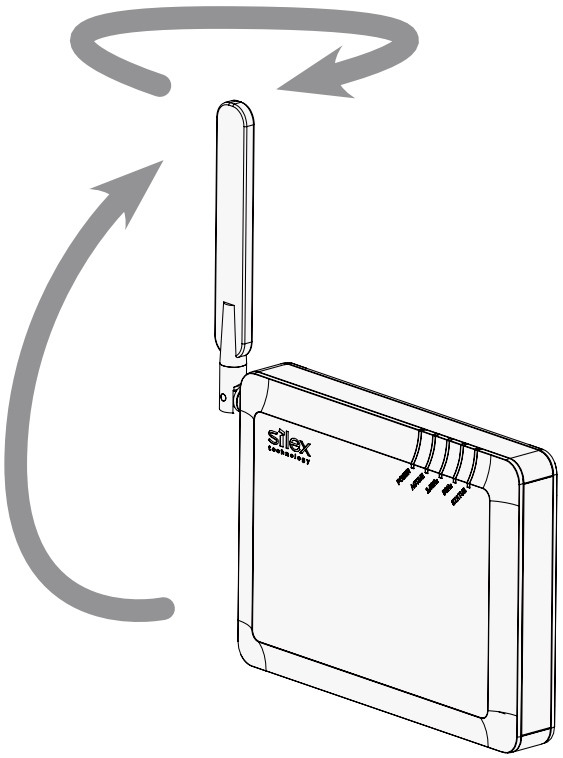
TIP

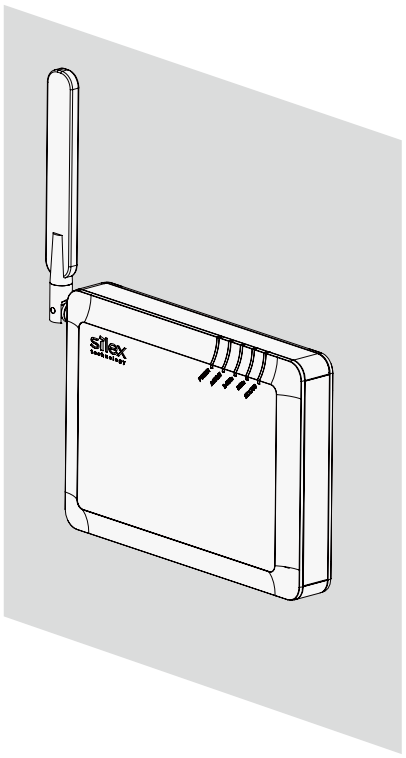
- Do not push the antenna to a wrong direction.
- When you turn the antenna, please be sensitive to the limit of its stopper.

When hanging the unit horizontally on a wall

(2) Turn the antenna

(1) Stand the antenna upright





(3) Hang the unit on a wall

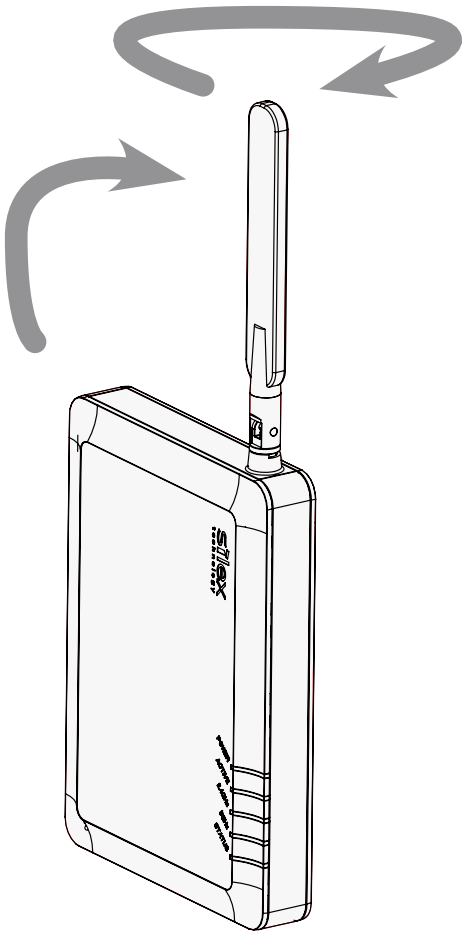
TIP

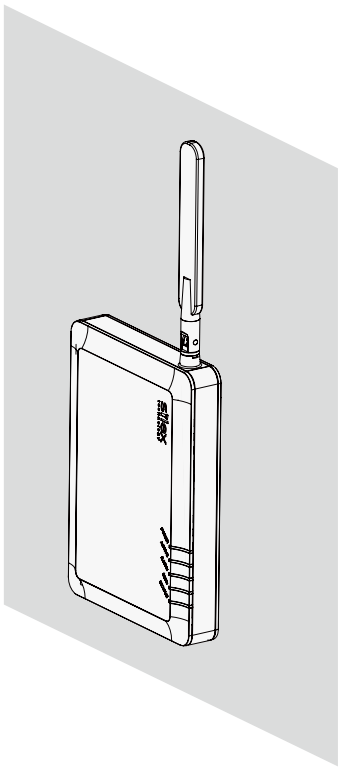
- Do not push the antenna to a wrong direction.
- When you turn the antenna, please be sensitive to the limit of its stopper.

When hanging the unit vertically on a wall

(2) Turn the antenna

(1) Stand the antenna upright





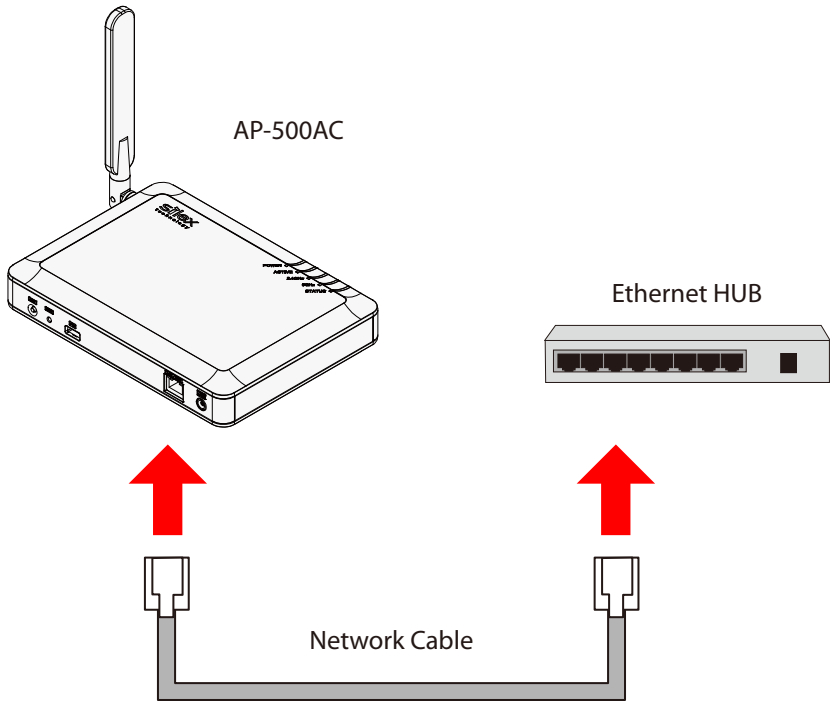
(3) Hang the unit on a wall

TIP

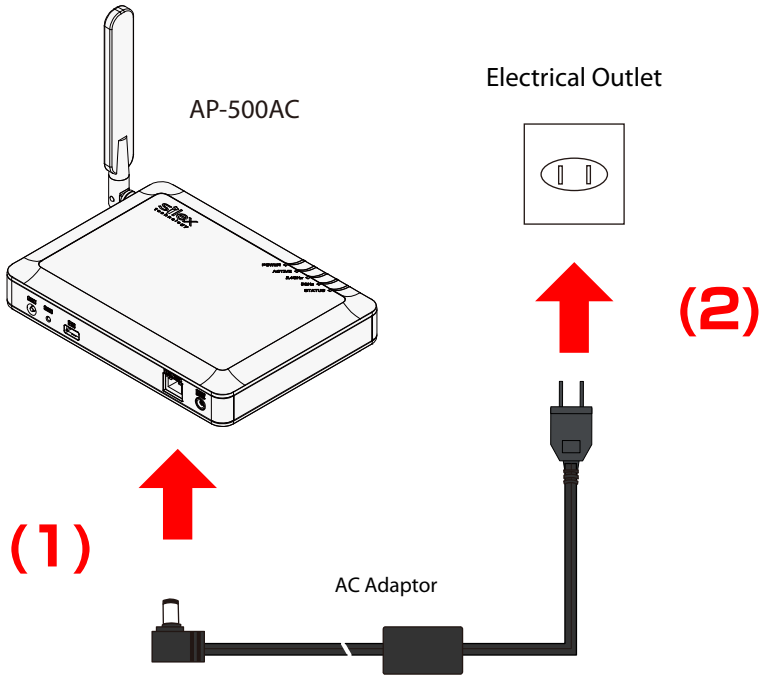
- Do not push the antenna to a wrong direction.
- When you turn the antenna, please be sensitive to the limit of its stopper.

Connect AP-500AC to a network

1. Connect AP-500AC and Ethernet Hub via a network cable.



2. Connect the AC adapter to AP-500AC and AC plug to a power outlet.



Note

- When receiving power over Ethernet (PoE), the AC adaptor does not need to be connected. Make sure that the PoE supported HUB or PoE power supply unit is used then.

4. Connecting Wireless Device

This chapter explains how to connect your PC and wireless devices to AP-500AC.

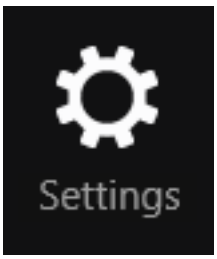
4-1. Connecting PC

Following explains how to connect your PC to AP-500AC as a wireless client device.

Note

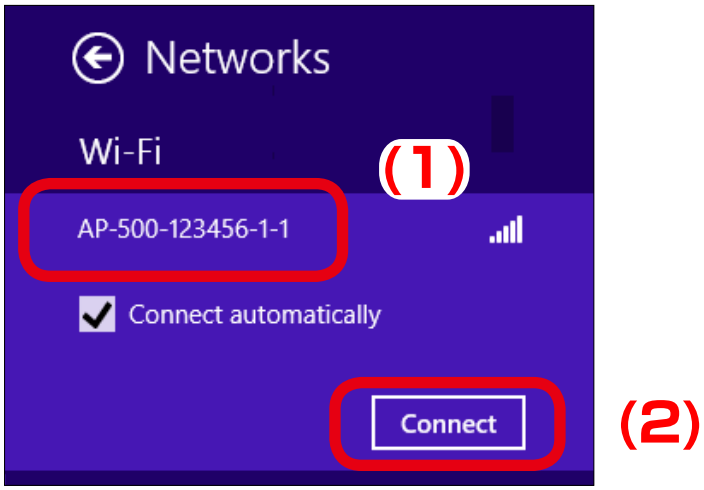
- Before connecting your PC, you need to know **SSID** and **Security Key** configured on AP-500AC (**Pre-Shared Key** or **WEP Key**).
- In the following instructions, the screenshots captured from Windows 8 will be used. When an operating system other than Windows 8 is used, the procedure may be different.

1. Move your cursor to top-right or bottom right corners (when a touch-panel device is used, swipe your finger from the right edge) and click **Settings** from the charm bar.



2. Click the icon below to show the wireless connection window.

3. Select the SSID configured on AP-500AC from a list and click **Connect**.

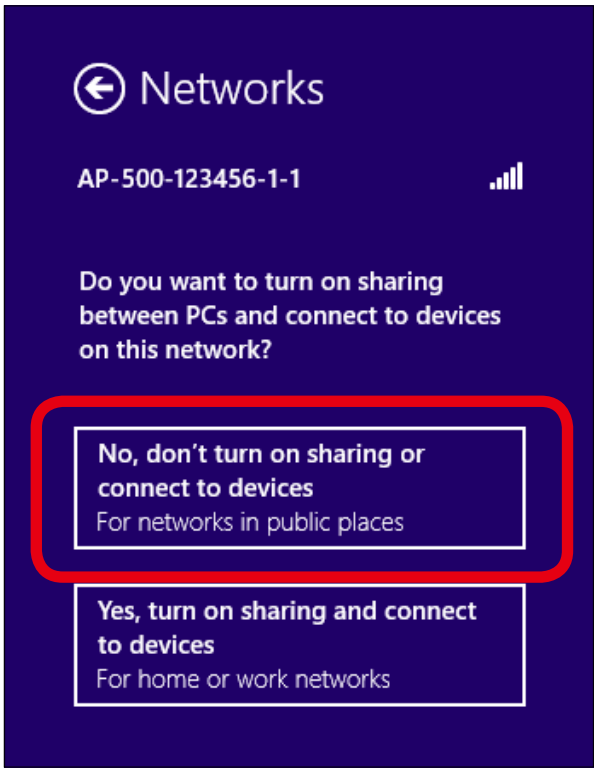


Note

- When **Connect automatically** is checked, the PC will automatically be connected when it is restarted next time.

4. Enter the security key of AP-500AC for **Enter the network security key** and click **Next**.

5. Click **No, don't turn on sharing or connect to devices**.

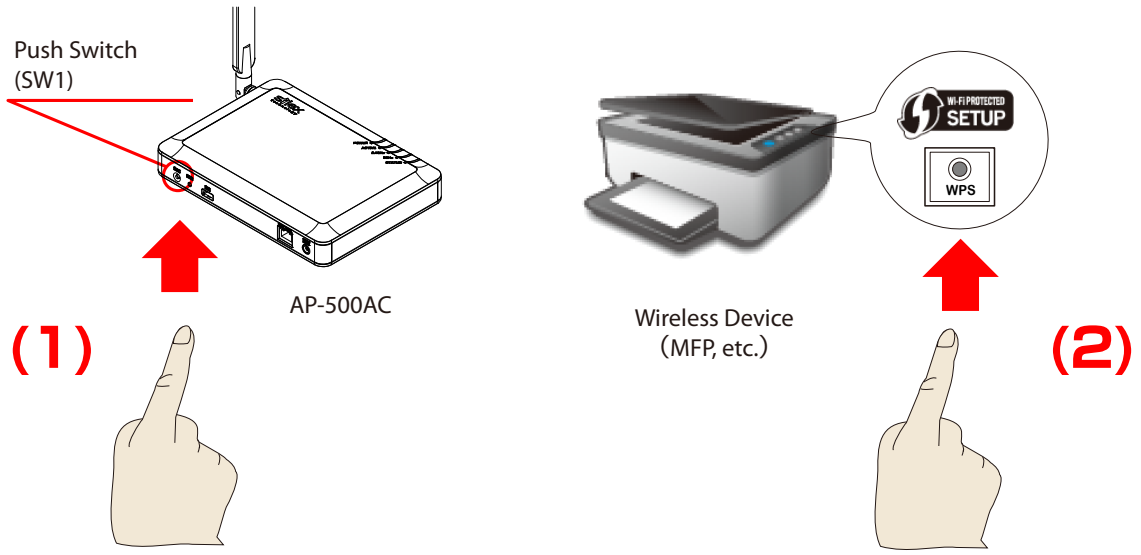


PC has been connected to AP-500AC.

4-2. Connecting Wireless Device Using Smart Wireless Setup Switch

Following explains how to connect wireless client devices to AP-500AC using the Smart Wireless Setup switch (Push Switch SW1).

To configure using the Smart Wireless Setup, the wireless client device needs to support WPS (Wi-Fi Protected Setup). When you are not sure if the wireless client device supports WPS or not, see the operating manual that came with the device or contact the manufacturer.



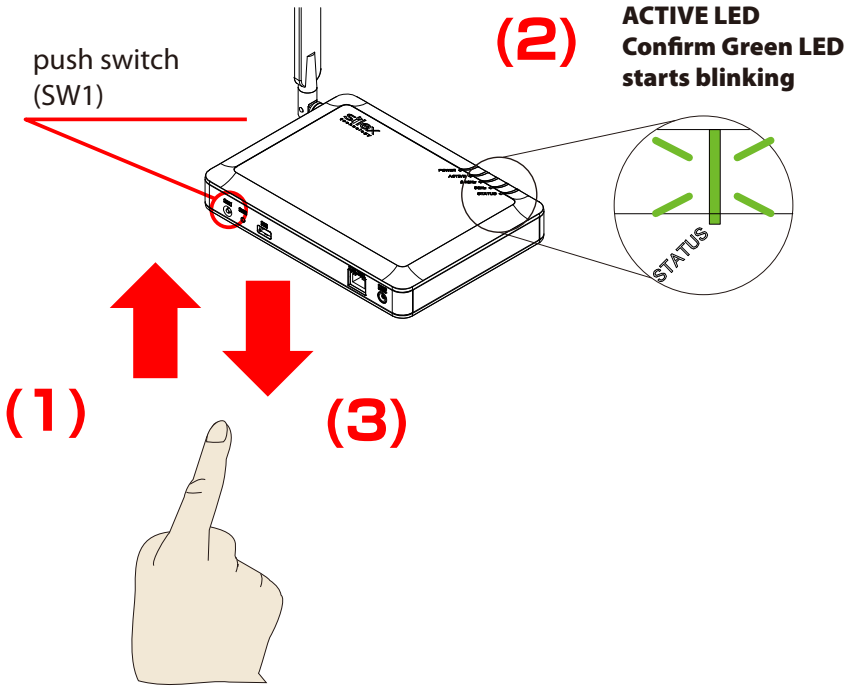
TIP

- During this configuration, please place your wireless device closer to AP-500AC so that they can communicate better.

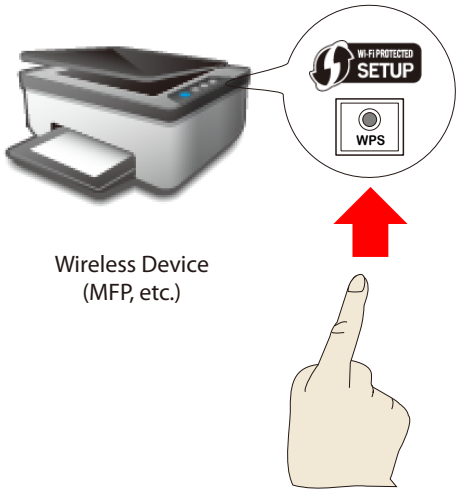
Note

- By default, wireless interface 1 (2.4GHz) is set as wireless interface that can use Smart Wireless Setup.
- When the stealth mode is enabled on AP-500AC, wireless connection method using Smart Wireless Setup cannot be used.

1. Press and hold the push switch (SW1). Release it when STATUS LED start blinking in Green.



2. Press the wireless setup switch also on your wireless device.



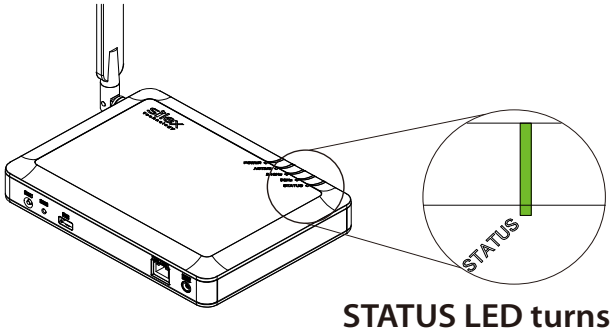
TIP

- Please use only one wireless device. Even if two or more devices are waiting for wireless connections, AP-500AC can configure only one device which has replied first.

Note

- The name, position and shape of the wireless setup switch(WPS button) will differ depending on your wireless device. For details, refer to the operation manual that came with your wireless device.

3. AP-500AC will start to communicate with your wireless device and configure the same wireless settings. The STATUS LED will turn to Green when the configuration is completed.



STATUS LED turns Green

Note

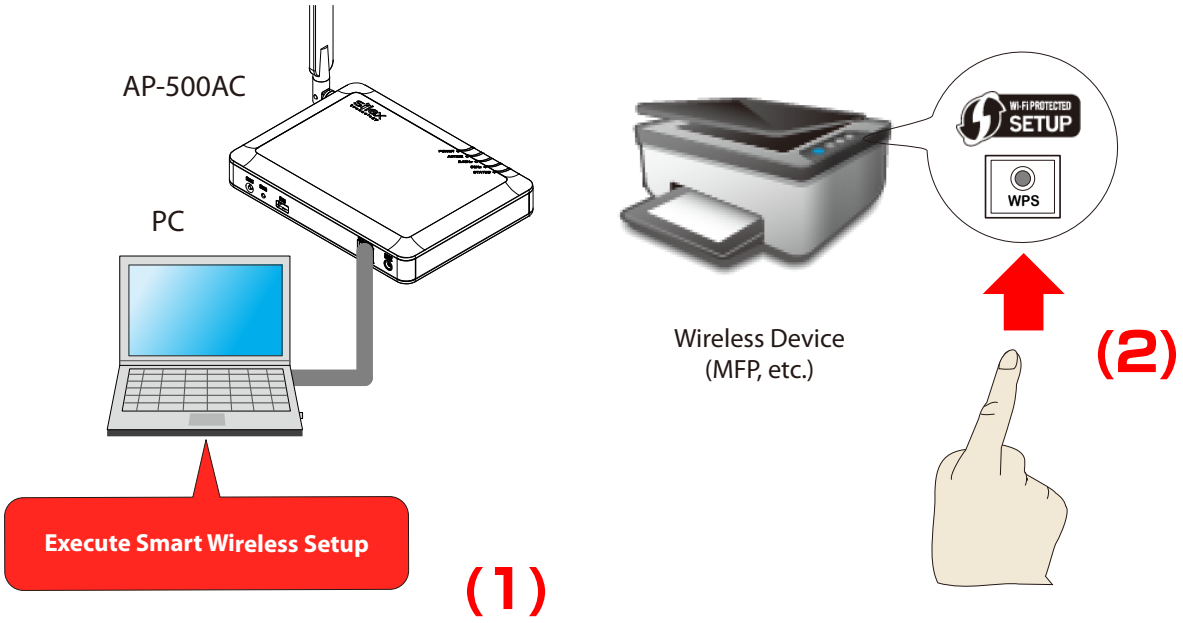
- If STATUS LED turns to Red, the configuration would have failed. Read the notes on this configuration and try again.
- STATUS LED (Green/Red) will turn off in 3 mins.

The wireless client device has been connected to AP-500AC.

4-3. Connecting Wireless Device by Push Button Method of Web Page

Following explains how to connect wireless client devices to AP-500AC using the **Push Button** method of Web page.

To configure using the Smart Wireless Setup, the wireless client device needs to support WPS (Wi-Fi Protected Setup). When you are not sure if the wireless client device supports WPS or not, see the operating manual that came with the device or contact the manufacturer.



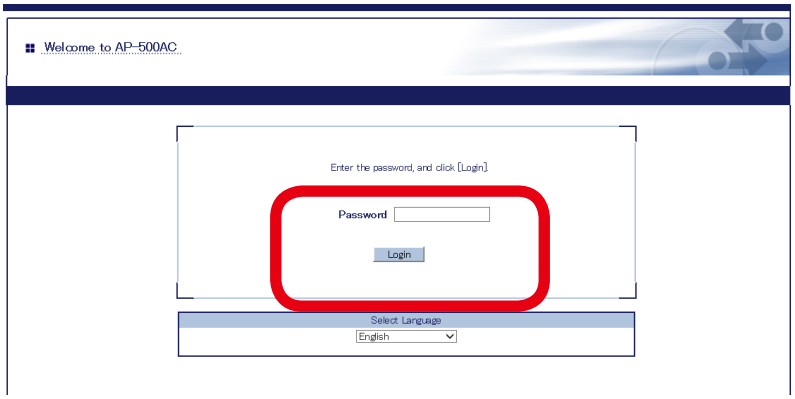
TIP

- During this configuration, please place your wireless device closer to AP-500AC so that they can communicate better.

Note

- By default, wireless interface 1 (2.4GHz) is set as wireless interface that can use Smart Wireless Setup.
- When the stealth mode is enabled on AP-500AC, wireless connection method using Smart Wireless Setup cannot be used.

1. Log in to the Web page of AP-500AC using your Web browser.

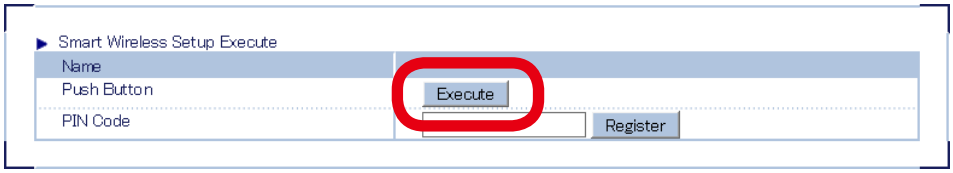


Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu on the Web page, click **Smart Wireless**.

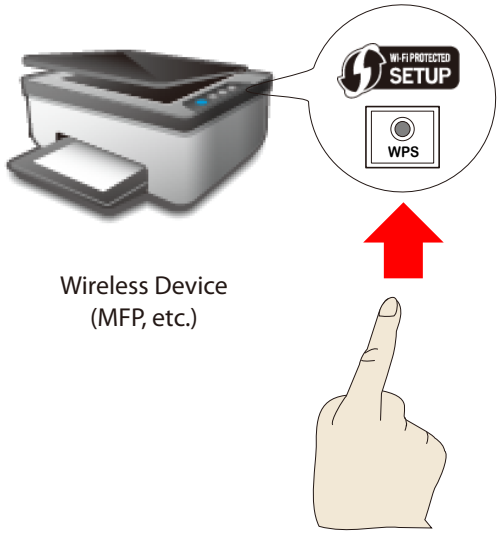
3. Click **Execute** at **Push Button** under **Smart Wireless Setup Execute**.



Note

- The STATUS LED blinks Green when the Smart Wireless Setup is in process.

4. Press the wireless setup switch on your wireless device.



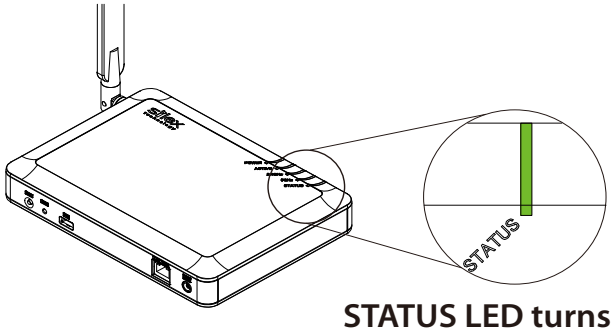
TIP

- Please use only one wireless device. Even if two or more devices are waiting for wireless connections, AP-500AC can configure only one device which has replied first.

Note

- The name, position and shape of the wireless setup switch(WPS button) will differ depending on your wireless device. For details, refer to the operation manual that came with your wireless device.

5. AP-500AC will start to communicate with your wireless device and configure the same wireless settings. The STATUS LED will turn to Green when the configuration is completed.



STATUS LED turns Green

Note

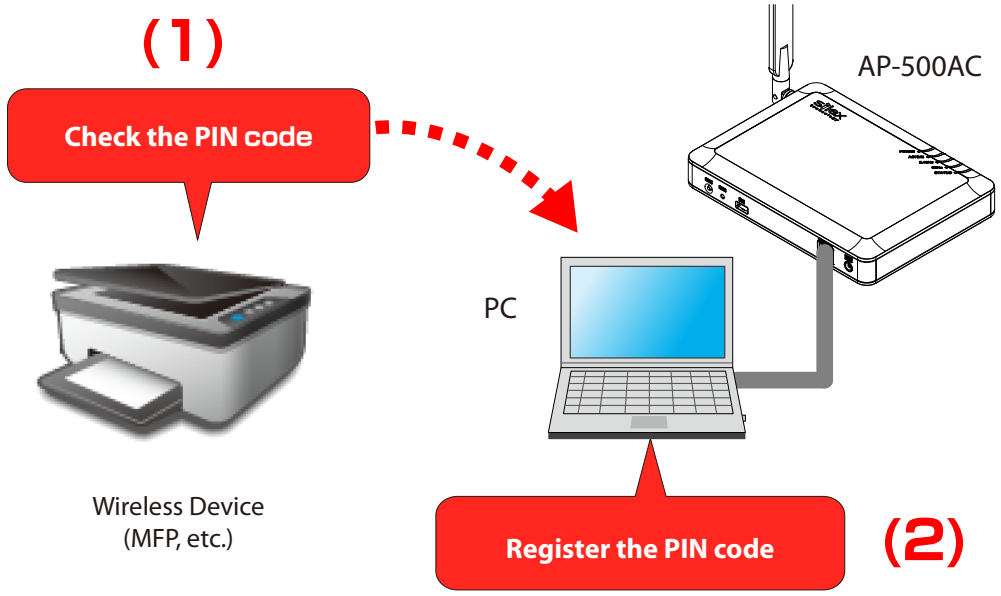
- If STATUS LED turns to Red, the configuration would have failed. Read the notes on this configuration and try again.
- STATUS LED (Green/Red) will turn off in 3 mins.

The wireless client device has been connected to AP-500AC.

4-4. Connecting Wireless Device by Entering PIN Code on Web Page

Following explains how to connect wireless client devices to AP-500AC using the **PIN Code** method of Web page.

To configure using the Smart Wireless Setup, the wireless client device needs to support WPS (Wi-Fi Protected Setup). When you are not sure if the wireless client device supports WPS or not, see the operating manual that came with the device or contact the manufacturer.



TIP

- During this configuration, please place your wireless device closer to AP-500AC so that they can communicate better.

Note

- By default, wireless interface 1 (2.4GHz) is set as wireless interface that can use Smart Wireless Setup.
- When the stealth mode is enabled on AP-500AC, wireless connection method using Smart Wireless Setup cannot be used.

1. Check the PIN code of wireless device to connect to AP-500AC.

Wireless Device
(MFP, etc.)

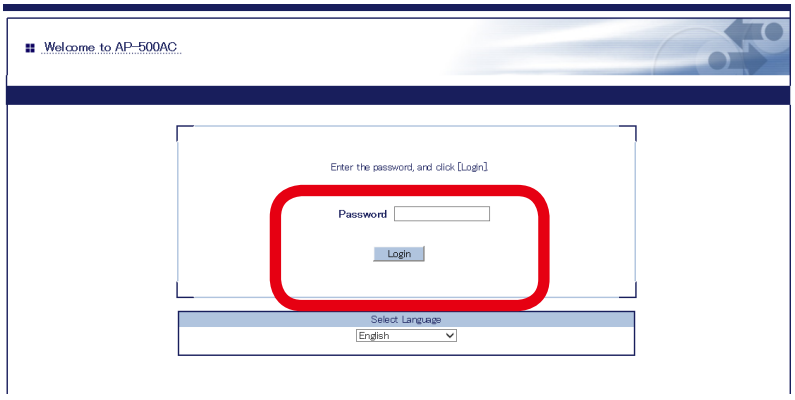
TIP

- Do not enter the PIN code that is described on the back label of AP-500AC.

Note

- For how to know the PIN code, see the operating manual of the wireless device.

2. Log in to the Web page of AP-500AC using your Web browser.

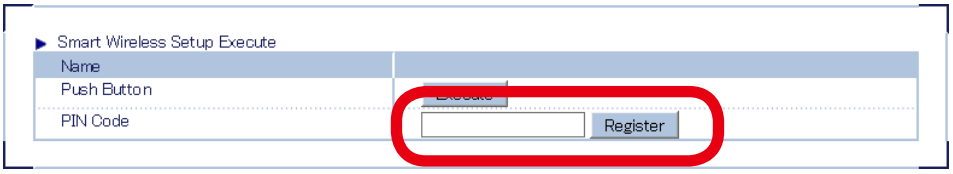


Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

3. From the left menu on the Web page, click **Smart Wireless**.

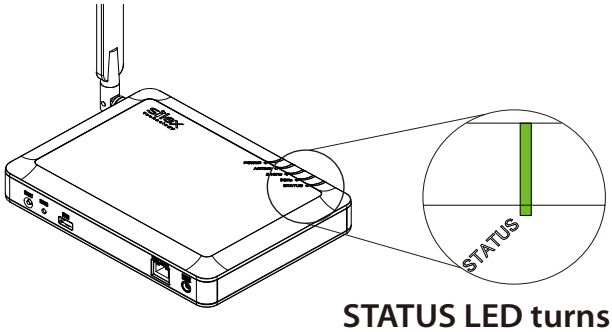
4. Enter the PIN code of wireless device at **PIN Code** under **Smart Wireless Setup Execute** and click **Register**.



Note

- The STATUS LED blinks Green when the Smart Wireless Setup is in process.

5. AP-500AC will start to communicate with your wireless device and configure the same wireless settings. The STATUS LED will turn to Green when the configuration is completed.



STATUS LED turns Green

Note

- If STATUS LED turns to Red, the configuration would have failed. Read the notes on this configuration and try again.
- STATUS LED (Green/Red) will turn off in 3 mins.
- If STATUS LED blinks in Red rapidly for 1 sec, the configuration would have failed. Check the PIN code setting and try again.

The wireless client device has been connected to AP-500AC.

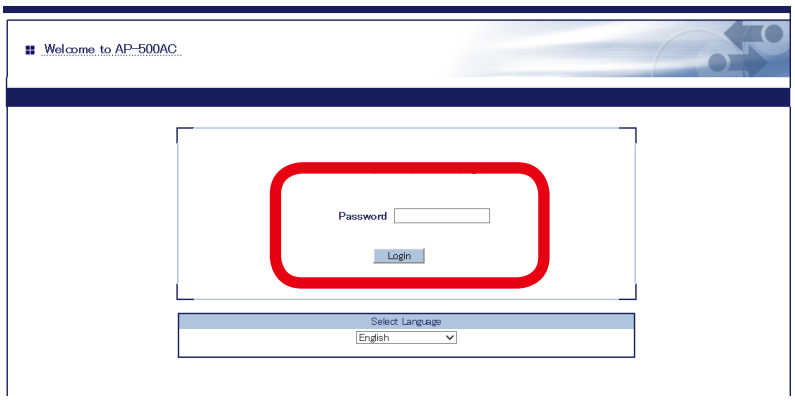
5. Other Features

This chapter explains the other features of AP-500AC.

5-1. System Status of Connected Wireless Device

In addition to TCP/IP and wireless setting information of AP-500AC, the MAC Address, wireless signal strength, etc. of the connected station devices can be seen on the Web page.

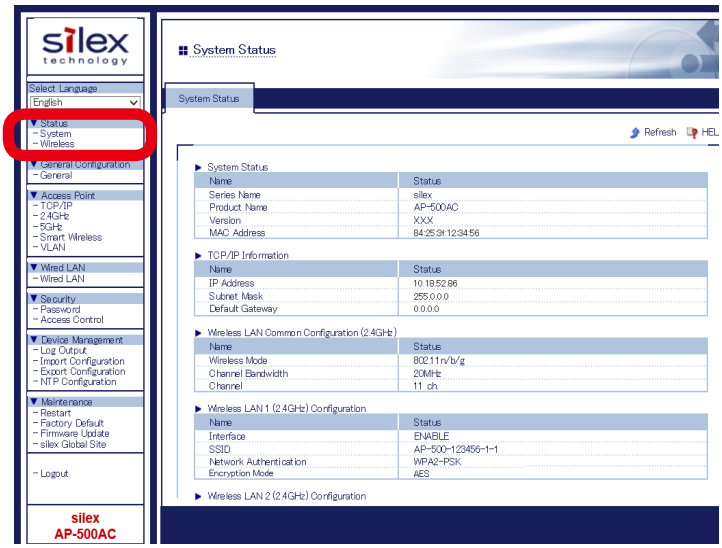
1. Log in to the Web page of AP-500AC using your Web browser.



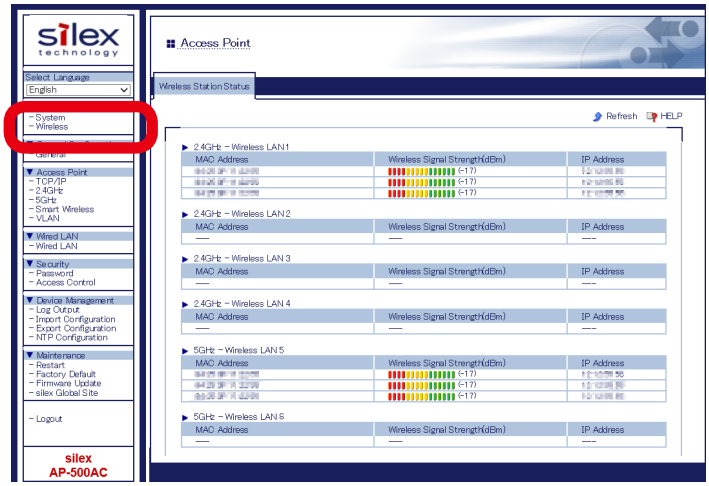
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. The system status page will be displayed after you have logged into the Web page. From the left menu in the Web page, click **System**. This page shows the general settings such as TCP/IP information, Wireless LAN settings, etc.



If you click **Wireless**, the status page for wireless station devices is displayed. In this page, you can check the MAC Address, RSSI (wireless signal strength) and IP Address for the connected wireless station devices.



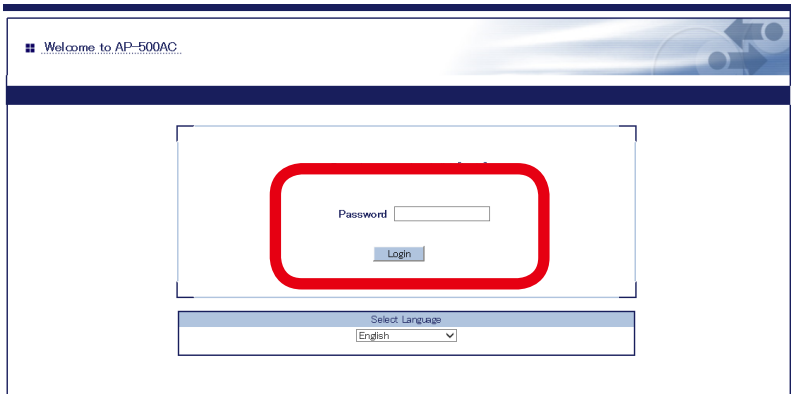
5-2. DHCP Server Feature

If **DHCP Server Function** is used, an IP address can automatically be assigned to PCs or network devices.

TIP

- To assign an IP address to your PC automatically using the DHCP server feature of AP-500AC, your PC must be set to **Obtain an IP address automatically**.

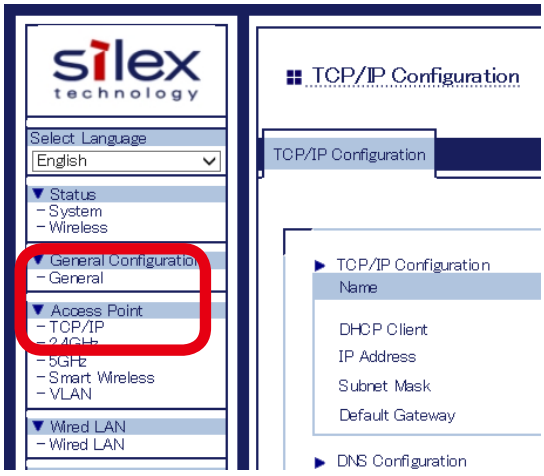
1. Log in to the Web page of AP-500AC using your Web browser.



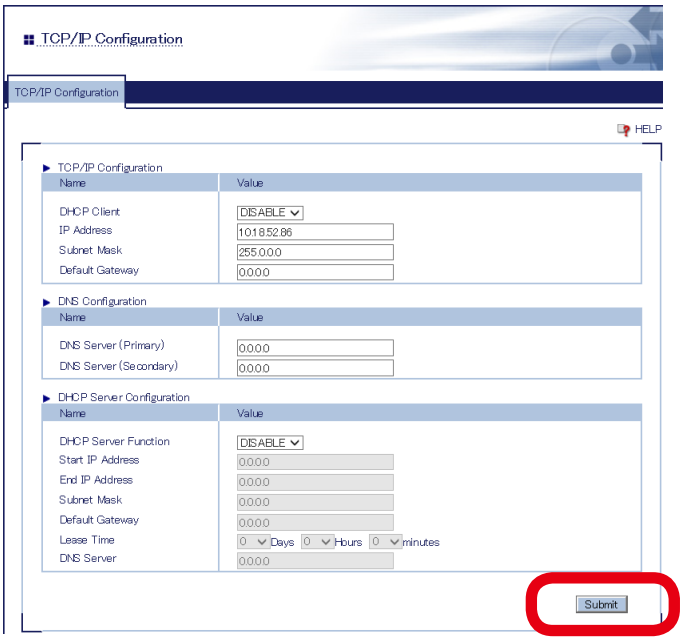
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu in the Web page, click **TCP/IP** or **General**.



3. Select **DISABLE** for **DHCP Client** and configure a static IP Address.
If **ENABLE** is selected at **DHCP Server Function**, the following settings will become available. After entering the settings, click **Submit** on the bottom right of Web page.



DHCP Server Configuration

Name	Description
DHCP Server Function	Enable/Disable the DHCP Server.
Start IP Address	Set the start IP address.
End IP Address	Set the end IP address.
Subnet Mask	Set the subnet mask for IP address range. If 0.0.0.0 is set, the subnet mask appropriate for the Start IP Address will automatically be used.
Default Gateway	Set the gateway address. This is disabled if 0.0.0.0 (default value) is set.
Lease Time	Set the lease time (Days/Hours/Minutes). When the setting is "0Days 0Hours 0Minutes", assigned lease time to client is 10days.
DNS Server	Set the DNS Server address.

TIP

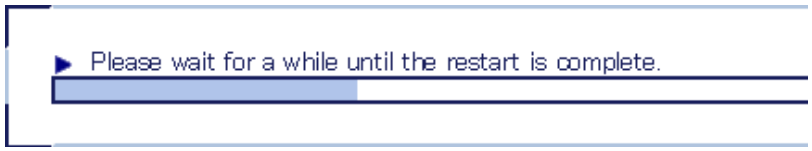
- To use the DHCP server feature, disable the DHCP client feature and assign a static IP Address to AP-500AC.

4. When finished, click **Restart**.

Note

- If you continue to configure the other settings, you do not have to restart. Please restart when you completed all other settings.
- The DHCP Server setting will not take effect unless you restart AP-500AC.

5. After the **Restart** button is clicked, the progress bar is displayed. When the progress bar reaches the right end, the restart is completed.

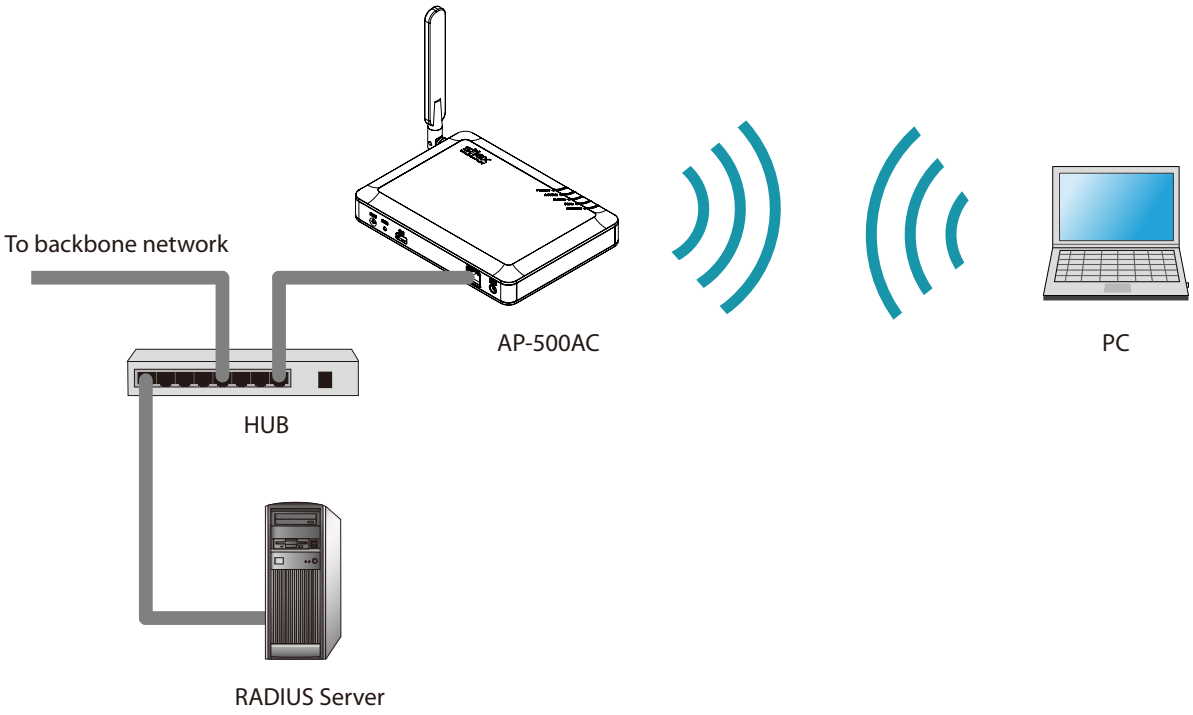


5-3. IEEE802.1X Authentication

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

Network Configuration

Connect the AP-500AC to a network as below when you use the IEEE802.1X authentication.
IP Address of RADIUS server and port number of EAPOL can be set.



IEEE802.1X Authentication

AP-500AC supports the following IEEE802.1X authentication methods.

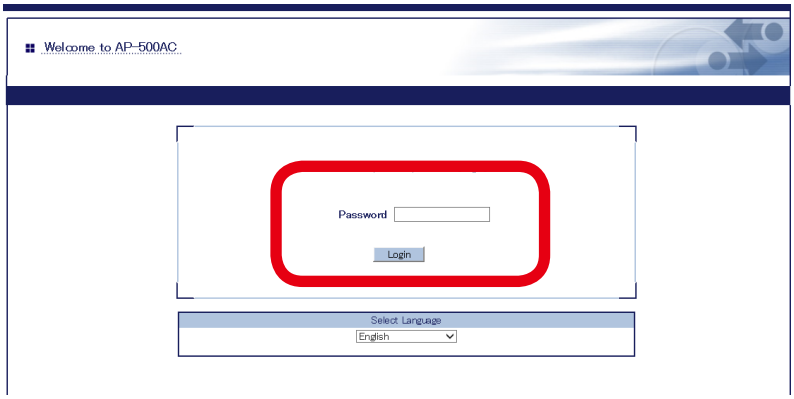
IEEE802.1X Authentication mode
EAP-TLS
EAP-TTLS
PEAP

Note

- EAP-LEAP and EAP-FAST are not supported.

IEEE802.1X Authentication Settings

1. Log in to the Web page of AP-500AC using your Web browser.

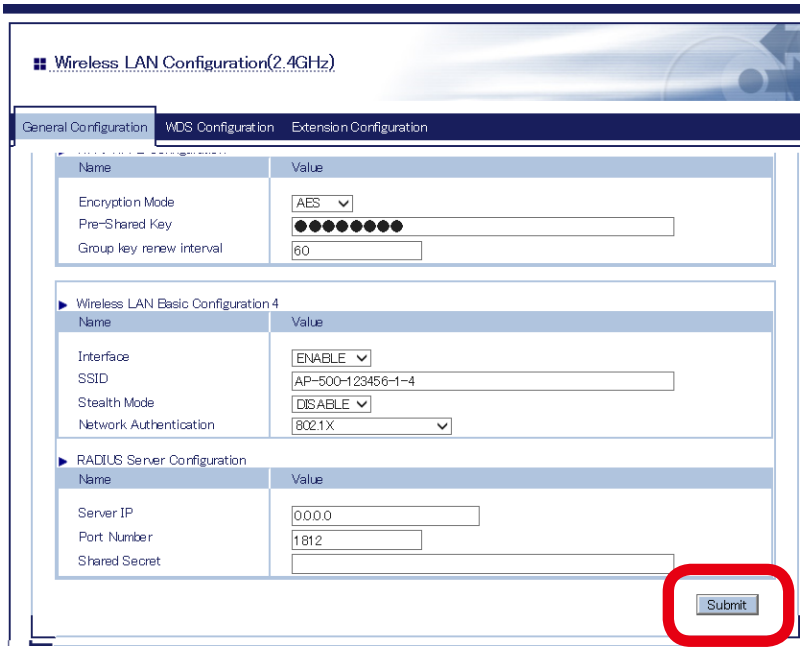


Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. In the Web page, click the band (2.4GHz/5GHz) to use 802.1X authentication from the menu.

3. Configure the settings for wireless interface to use 802.1X authentication and click **Submit** at bottom right of the page.



Network Authentication

Name	Description
802.1X	Uses the 802.1X user authentication. For encryption mode, WEP can be used.
WPA-Enterprise	Uses the 802.1X user authentication. For encryption mode, TKIP/AES/AUTO can be used.
WPA2-Enterprise	Uses the 802.1X user authentication. For encryption mode, AES/AUTO can be used.
WPA/WPA2-Enterprise	Uses the 802.1X user authentication. For encryption mode, AES/AUTO can be used.

RADIUS Server Configuration

Name	Description
Server IP	Set the IP Address of RADIUS server. This can be set only when the network authentication is 802.1X, WPA-Enterprise, WPA2-Enterprise or WPA/WPA2-Enterprise.
Port Number	Set the port number used to communicate with RADIUS server.
Shared Secret	Set the secret key used to communicate with RADIUS server.

Note

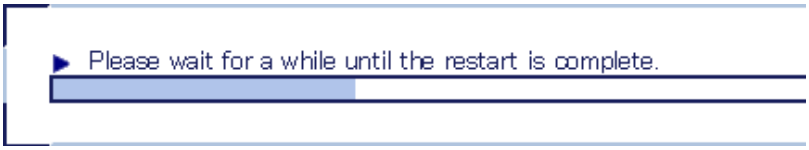
- For details on each configuration item, refer to **A. Appendix** - **A-1. List of All Settings**.
- For 802.11n/802.11ac, Shared / 802.1X authentication and WEP / TKIP encryption cannot be used.

4. When finished, click **Restart**.

Note

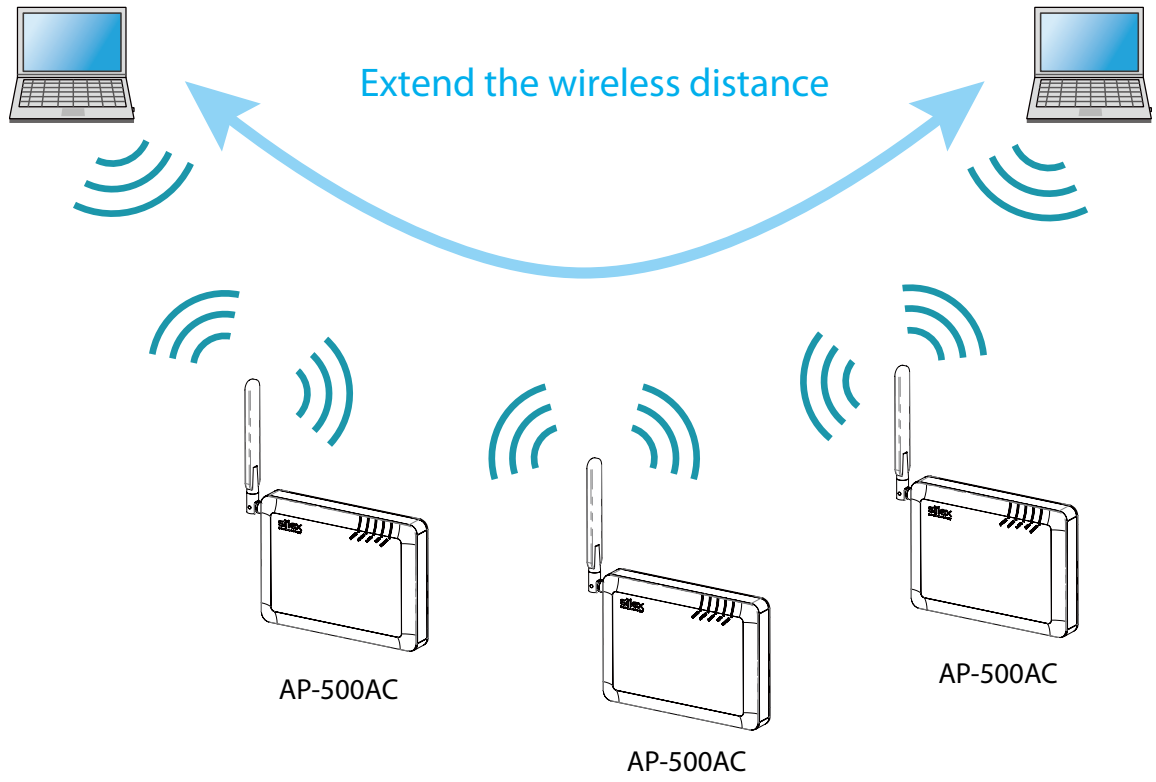
- If you continue to configure the other settings, you do not have to restart. Please restart when you completed all other settings.
- 802.1X authentication setting will not take effect unless you restart AP-500AC.

5. After the **Restart** button is clicked, the progress bar is displayed. When the progress bar reaches the right end, the restart is completed.



5-4. WDS Feature

If this mode is used, two or more AP-500AC Access Points can communicate each other. By linking several Access Points wirelessly, wireless distance can be expanded as well as wireless dead spots can be eliminated. The connection and configuration methods to use WDS are explained.

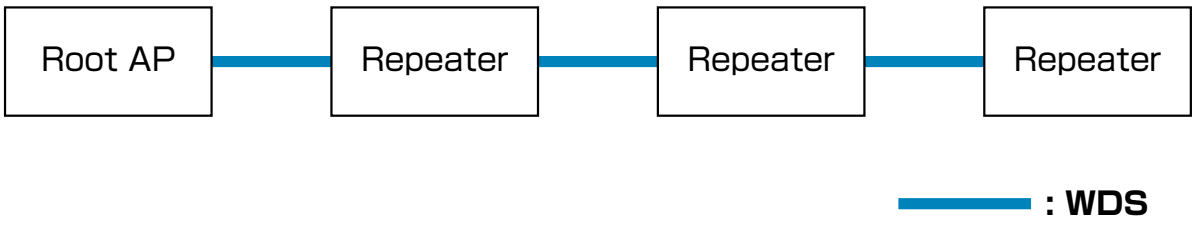


TIP

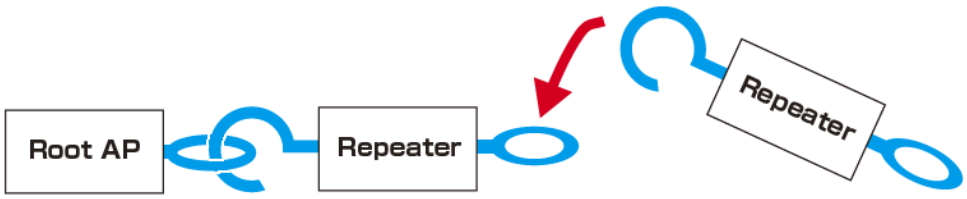
- Please check that all AP-500AC Access Points are running on the same version of firmware.
- In the following instructions, the screenshots captured from Windows 8 will be used. Display may vary depending on your environment and Web browser.
- WDS is guaranteed only for Silex brand products that support WDS.

WDS Connection

The WDS(Wireless Distribution System) is composed of one Root AP (running as a host device) and plural Repeater APs (running as client devices).



When connecting Access Points, use the first AP as Root AP and the second or later APs as Repeater APs. As shown in below image, connect APs starting from the Root AP.

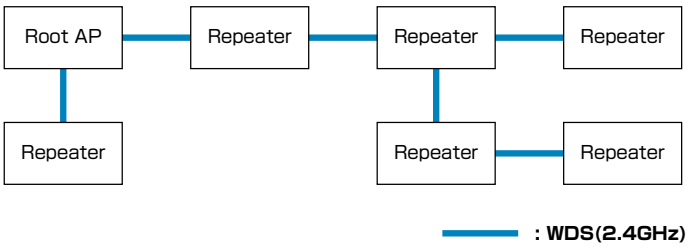


TIP

- For Root AP and Repeater APs to connect in WDS mode, configure the same wireless settings.
  Following settings must be the same:
  - Wireless channel
  - SSID
  - Network authentication
  - Encryption
- When using WDS, the following features cannot be used.
  - **802.1X**, **WPA-Enterprise**, **WPA2-Enterprise**, **WPA/WPA2-Enterprise** (of network authentication)
  - **AUTO** (of channel setting) and DFS band channels (W53(52/56/60/64ch), W56(100/104/108/112/116/120/124/128/132/136/140ch))
  - Privacy Separator
- When numbers of AP-500AC Access Points are connected in WDS, wireless communication speed may slow down.
- We do not guarantee the WDS connection if wireless devices other than AP-500AC are used.

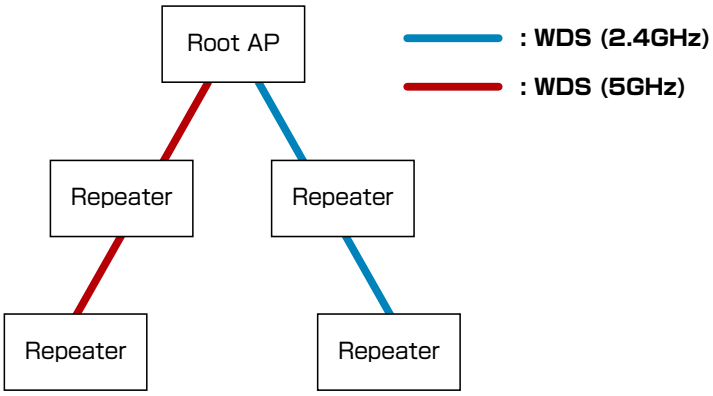
TIP

- Only one Repeater AP can be connected for each 2.4GHz and 5GHz in WDS mode. Please do not allow the setting that connects two or more Repeater APs to Root AP or Repeater AP using the same band. We do not guarantee a successful connection between two or more Repeater APs as shown blow.

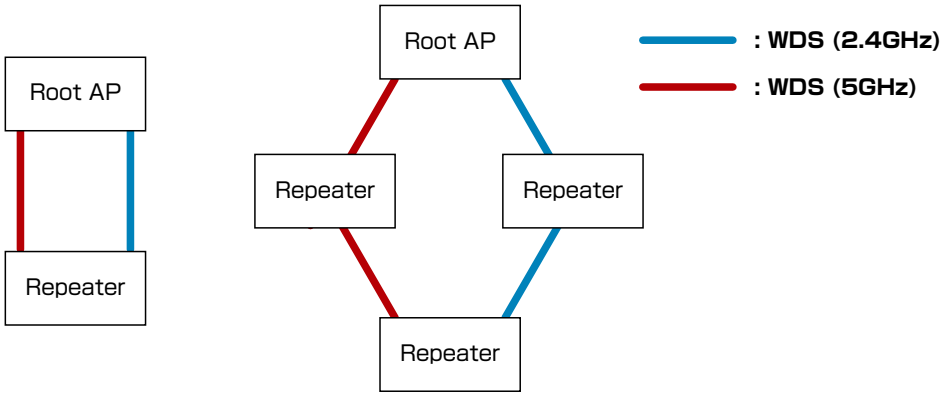


- When WDS is used for both 2.4GHz and 5GHz bands simultaneously, please do not allow a link between the bands. It may cause a loop communication error.

Example of connection for WDS using both 2.4GHz/5GHz bands:



Example of bad connection (loop error) for WDS:

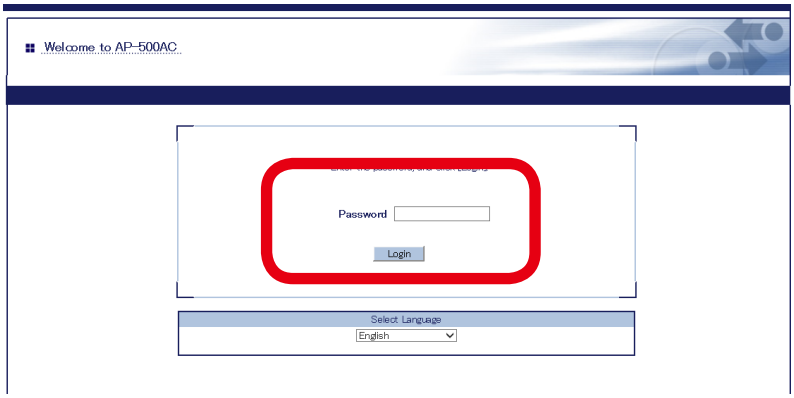


WDS Configuration

How to configure Root AP:

Configure the first unit of AP-500AC as Root AP.

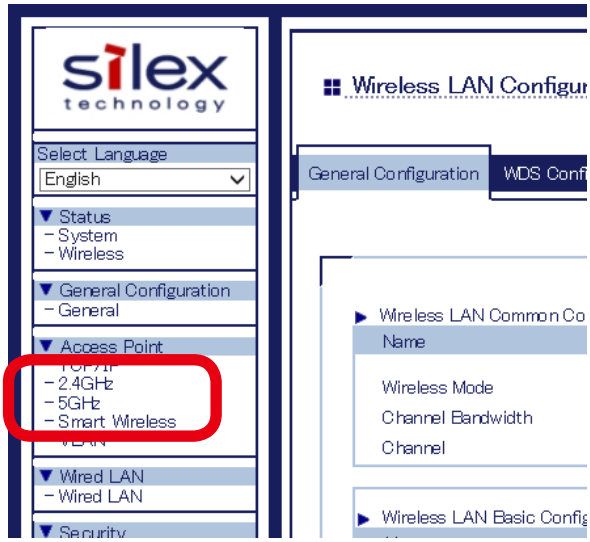
1. Log in to the Web page of AP-500AC to use as Root AP using your Web browser.



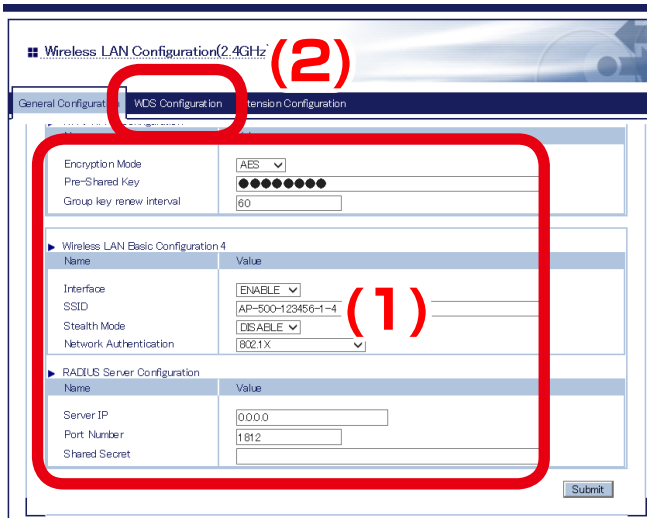
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. Click the band (2.4GHz/5GHz) to use WDS connection from the menu.



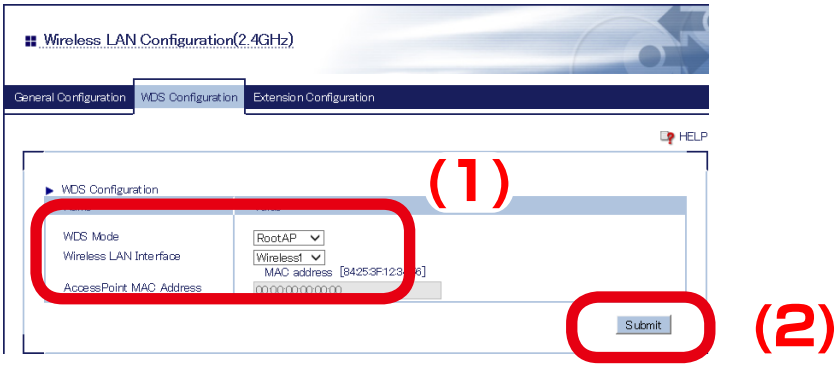
3. Select a wireless interface to use for WDS connection and click **WDS Configuration** tab.



Note

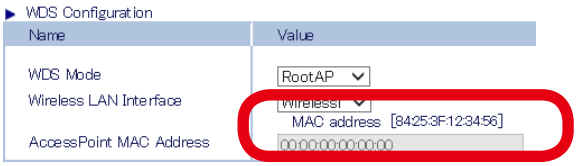
- For details on each configuration item, refer to **A. Appendix** - **A-1. List of All Settings**.
- The wireless settings of the selected interface will be necessary again when you configure Repeater AP. Please take notes of the settings such as channel, SSID, network authentication, encryption mode, etc.

4. Select **Root AP** for **WDS Mode** and select the wireless interface that you have selected to use for WDS connection. Click **Submit** on the bottom right of Web page.



Note

- For details on each configuration item, refer to **A. Appendix** - **A-1. List of All Settings**.
- The MAC Address displayed under the selected interface will be necessary again when you configure Repeater AP. Please take a note of the MAC Address.

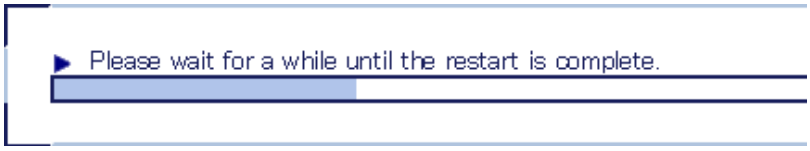


5. When finished, click **Restart**.

Note

- If you continue to configure the other settings, you do not have to restart. Please restart when you completed all other settings.
- The WDS setting will not take effect unless you restart AP-500AC.
- If MAC Address filtering is active, it can block access from the Repeater AP's MAC Address. If the Repeater AP is blocked, you will need to change the filter settings at **Security** - **Access Control** - **MAC Address Filter**.

6. After the **Restart** button is clicked, the progress bar is displayed. When the progress bar reaches the right end, the restart is completed.

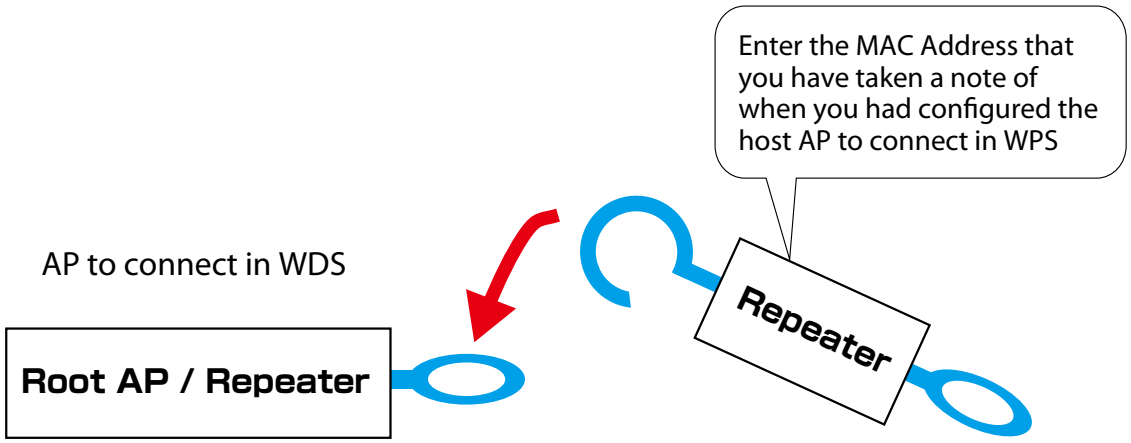


The Root AP setting is completed.

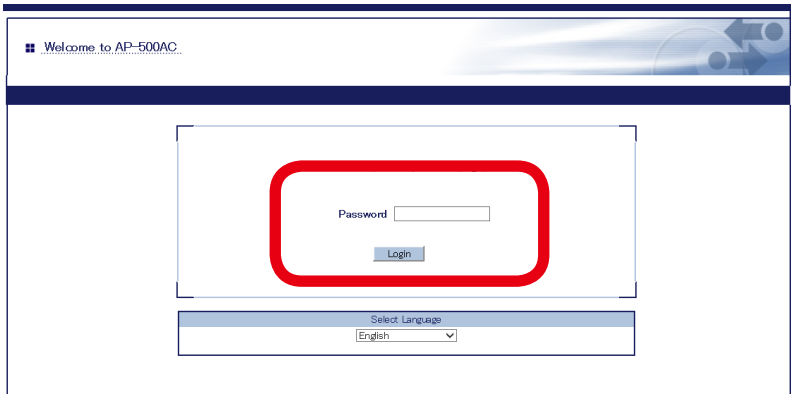
Please continue to Repeater AP configuration.

How to configure Repeater AP:

Set the second or later AP-500AC Access Points as Repeater APs.
The Access Point to connect in WPS can be specified using the MAC Address.
In order to make WDS connection, specify the MAC Address of the host AP to connect in WDS and configure the same wireless settings.



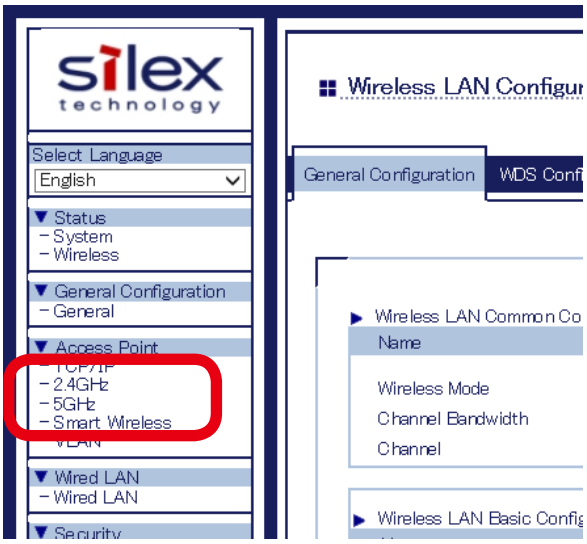
1. Log in to the Web page of AP-500AC to use as Repeater AP using your Web browser.



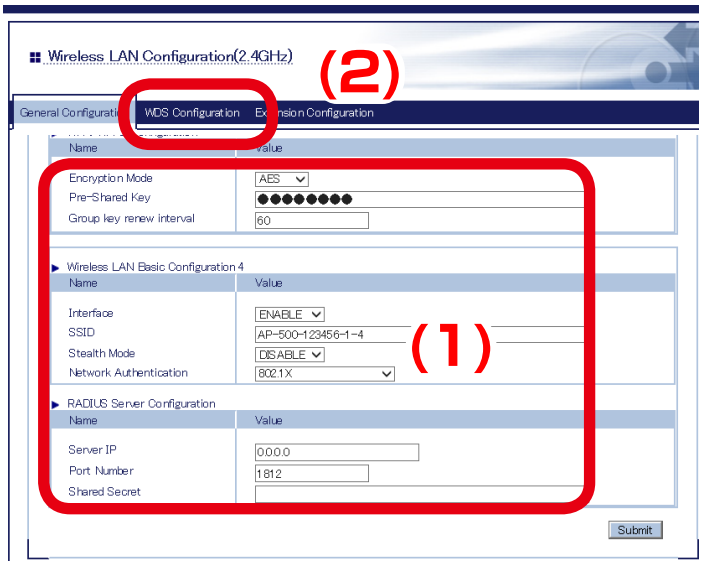
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. Click the band (2.4GHz/5GHz) to use WDS connection from the menu.



3. Select a wireless interface to use for WDS connection and click **WDS Configuration** tab.



Note

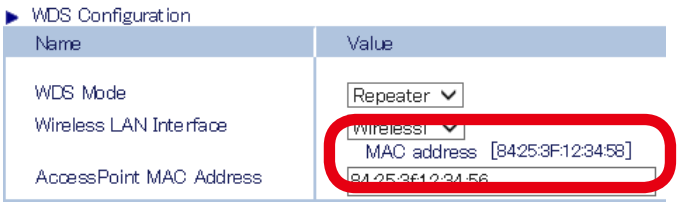
- For details on each configuration item, refer to **A. Appendix** - **A-1. List of All Settings**.
- For the wireless interface, use the same interface as the Root AP which is assigned for WDS connection. Please refer to Step 3 of the Root AP configuration and see the note about wireless settings (channel, SSID, network authentication, and encryption mode).

4. Configure the settings according to the table below and click **Submit**.

Name	Setting
WDS Mode	Repeater
Wireless LAN Interface	Select the interface you have selected to use for WDS connection.
Access Point MAC Address	Enter the MAC Address of the host AP to connect in WDS.

Note

- For details on each configuration item, refer to **A. Appendix** - **A-1. List of All Settings**.
- The MAC Address displayed under the selected interface will be necessary again when you configure another Repeater AP. Please take a note of the MAC Address.

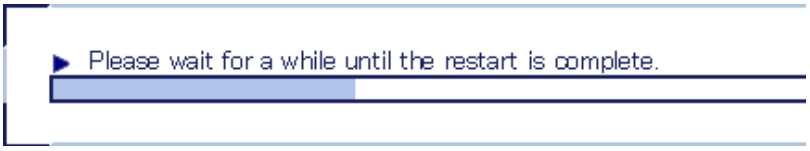


5. When finished, click **Restart**.

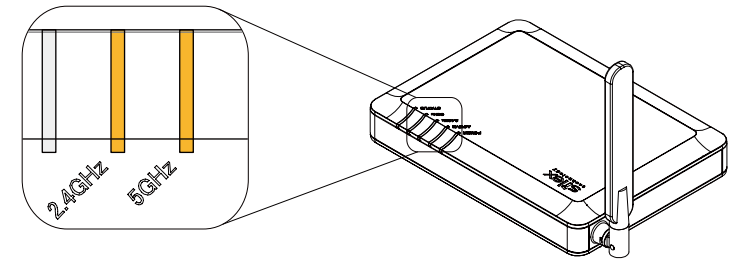
Note

- If you continue to configure the other settings, you do not have to restart. Please restart when you completed all other settings.
- The WDS setting will not take effect unless you restart AP-500AC.

6. After the **Restart** button is clicked, the progress bar is displayed. When the progress bar reaches the right end, the restart is completed.



7. Check that the LED of assigned wireless band turns Orange.



Orange ON : Connected in WDS

AP-500AC

Note

- If the LED of assigned wireless band does not turn Orange, AP-500AC is not connected in WDS. See **5-4. WDS Feature** - **What If WDS Connection Fails?** for a possible solution.
- WDS connection status can also be checked from the Web page. For details, refer to **5-4. WDS Feature** - **Checking WDS Connection Status from Web Page**.

The Repeater AP setting is completed.

To connect more Repeater APs in WDS mode, repeat the same process from Step1-7.

What If WDS Connection Fails?

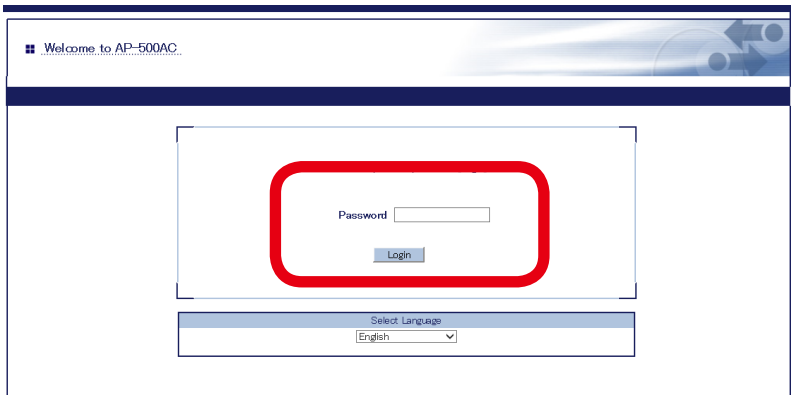
If AP-500AC fails in WDS connection, one of followings might be the reason:
1) The client AP has different wireless settings from the host AP.
2) MAC Address filtering is active on the host AP and it blocks access from the client AP.
3) Too many station devices are connected to the host AP and it has reached the max number of connectable devices.

Follow the instructions below to identify the problems on WDS:

How to check the settings on client AP:

Check the Repeater setting on the client AP.

1. Log in to the Web page of AP-500AC (client AP) using your Web browser.



Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu in the Web page, click **System**.

3. In the **System Status** page, check the status information as shown in a table below:

Setting	Item
Wireless LAN Common Configuration	Channel
Wireless LAN Configuration	Interface
	SSID
	Network Authentication
	Encryption Mode
WDS Information	WDS Mode
	Wireless Interface

The MAC Address used to connect to the host AP in WDS is displayed at **WDS Mode** under **WDS Information**.

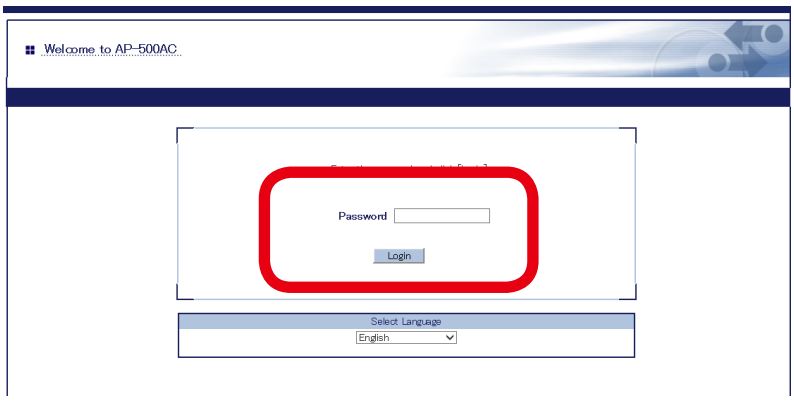
Note

- For details on each configuration item, refer to **A. Appendix** - **A-1. List of All Settings**.
- The confirmed status information will be necessary again when you check the settings on the host AP. Please take notes of the wireless settings such as channel, SSID, network authentication, encryption mode, etc. and the MAC Address.

How to check the settings on host AP:

Check the Root AP or Repeater AP settings of the host AP.

1. Log in to the Web page of AP-500AC (host AP) using your Web browser.



Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu in the Web page, click **System**.

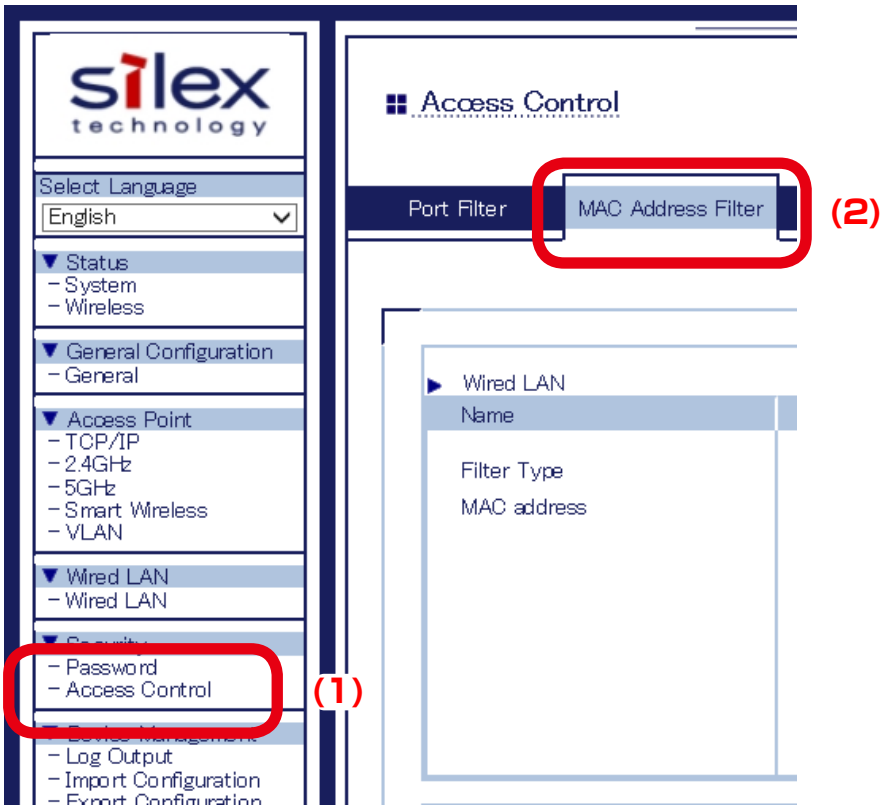
3. In the **System Status** page, check that **WDS Mode** is set to **Root AP** or **Repeater**. Check that status information as show in a table below are the same as those you previously checked at the client AP.

Setting	Item
Wireless LAN Common Configuration	Channel
Wireless LAN Configuration	Interface
	SSID
	Network Authentication
	Encryption Mode
WDS Information	Wireless Interface

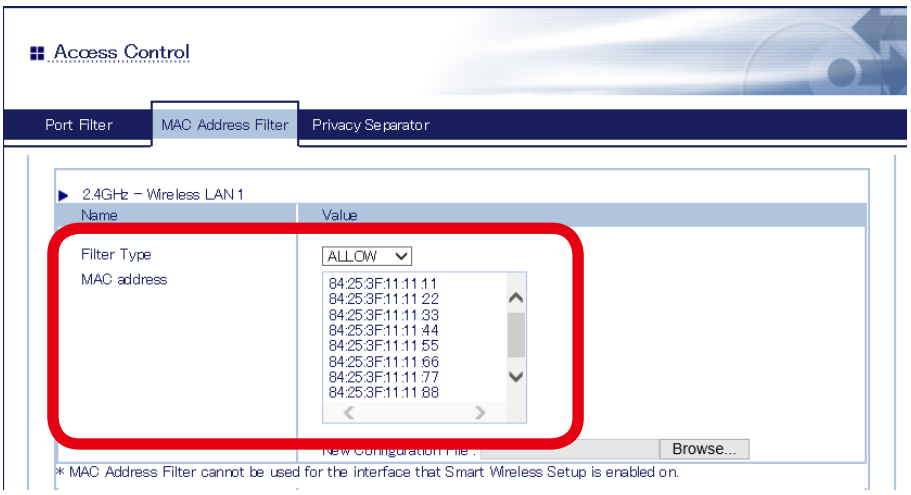
Note

- For details on each configuration item, refer to **A. Appendix** - **A-1. List of All Settings**.
- If the settings are different between the host AP and client AP, change the settings of client AP to match those of host AP. For how to change the settings, refer to **5-4 WDS Feature** - **WDS Configuration**.

4. From the left menu in the Web page, click **Access Control - MAC Address Filter**.



5. Select the wireless interface assigned for WDS connection and check that the MAC Address filter is not set to block access from the client AP.

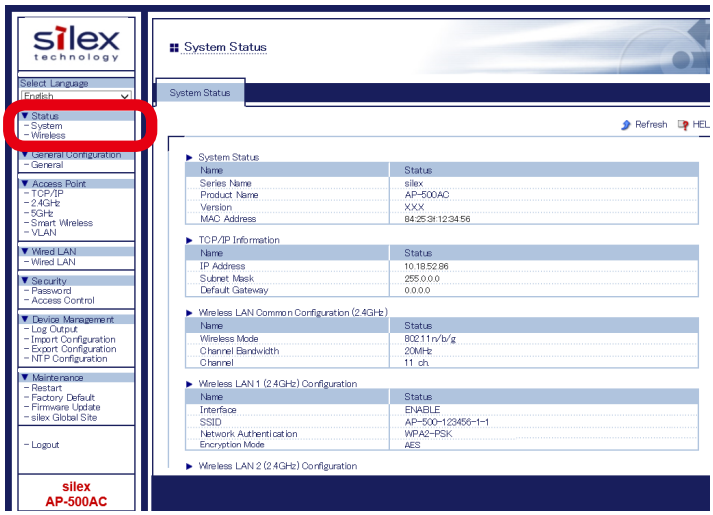


Note

- For details on each configuration item, refer to **A. Appendix** - **A-1. List of All Settings**.
- The client AP connects to the host AP using the "MAC Address used to connect to host AP in WDS" that you have previously checked at the client AP. If access from the client AP is denied, change the setting to allow it.

6. From the left menu in the Web page, click **System**. In the **System Status** page, check the **Encryption Mode** used for the wireless LAN.

The max number of connectable devices for AP-500AC will differ depending on the encryption mode used. Please check that too many station devices or APs exceeding that number are not connected in your environment.

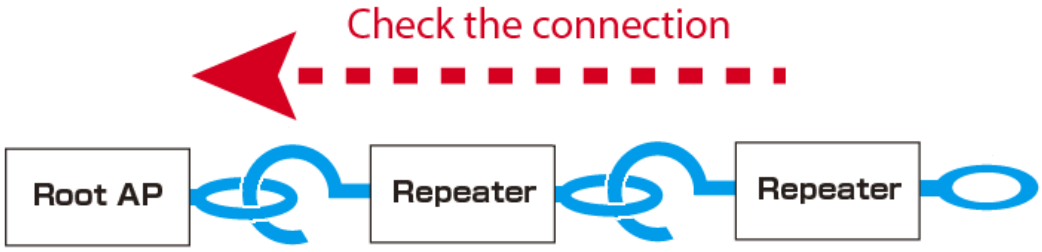


Note

- For details on each configuration item, refer to **A. Appendix** - **A-1. List of All Settings**.
- The max number of connectable station devices will differ depending on the encryption mode used.
  - When using **AES** only: 100 units
  - When using **TKIP** or **AUTO**: 50 units
- In Multi SSID environment, the number of connected devices will be the total number of devices connected on all wireless interfaces. Thus, the max number of connectable devices will differ depending on the encryption mode used on each interface.
  - When all wireless interfaces use **AES** only: 100 units
  - When one or some of the wireless interfaces use **TKIP** or **AUTO**: 50 units
- When using the WDS feature, the Repeater AP connected to AP-500AC as a client AP will consume one of the available connections, while Root AP or Repeater APs connected to AP-500AC as a host AP will NOT consume any connections.

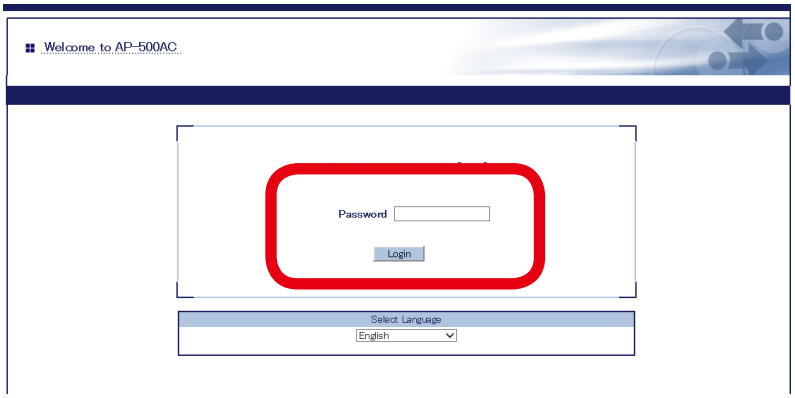
Checking WDS Connection Status from Web Page

To see if AP-500AC is connected in WDS mode properly, check the status page on the Web page in the order from the client (Repeater AP) to the host (Root AP or Repeater AP).
In the Web page, the host AP connected in WDS is displayed.



How to check the WPS connection to the host AP:

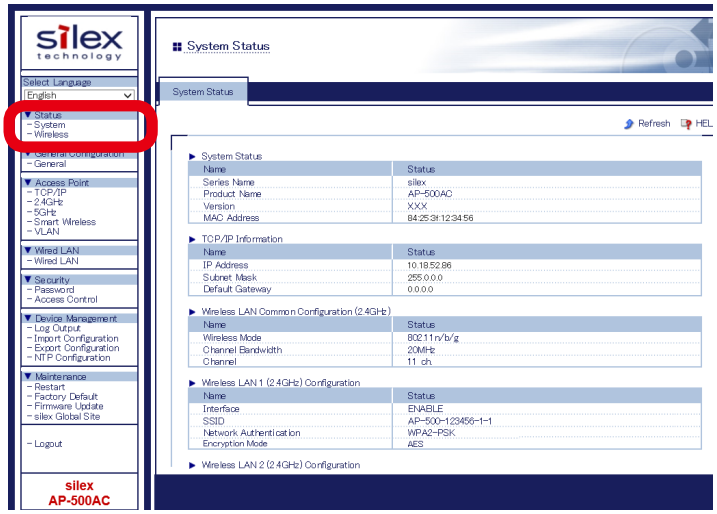
1. Log in to the Web page of the Repeater AP using your Web browser.



Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu in the Web page, click **System**.



3. In the **System Status** page, check the **WDS Information**.

If **Access Point MAC Address** and **Wireless Signal Strength(dBm)** are displayed, the WDS connection is established successfully.

To continue to see the connection status at the host AP, repeat the same process from Step1-3 at the host AP's Web page.

WDS Connection Success:

▶ WDS Information (2.4GHz)

Name	Status
WDS Mode	Repeater [96:25:3F:12:34:58]
Wireless LAN Interface	Wireless LAN1 [AP-500-123456-1-1]
AccessPoint MAC Address	84:25:3F:12:34:56
Wireless Signal Strength(dBm)	(-24)

WDS Connection Failure:

▶ WDS Information (2.4GHz)

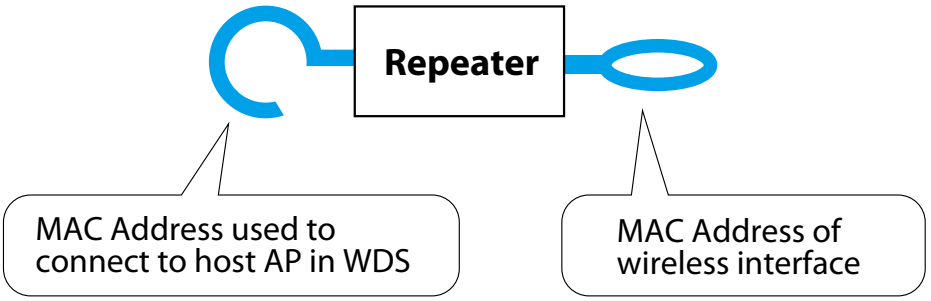
Name	Status
WDS Mode	Repeater [96:25:3F:12:34:58]
Wireless LAN Interface	Wireless LAN1 [AP-500-123456-1-1]
AccessPoint MAC Address	—
Wireless Signal Strength(dBm)	—

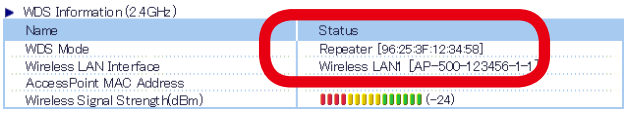
Note

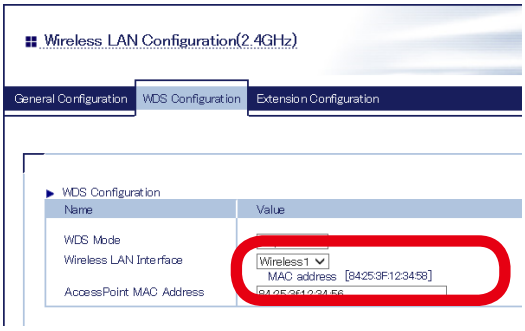
- For details on each configuration item, refer to **A. Appendix** - **A-1. List of All Settings**.
- If **Access Point MAC Address** and **Wireless Signal Strength (dBm)** are not displayed, the WDS connection is not established. In such a case, refer to **5-4. WDS Feature** - **What If WDS Connection Fails?** for possible solutions.
- In the Web page of Root AP, **Access Point MAC Address** and **Wireless Signal Strength (dBm)** are not displayed.

Note

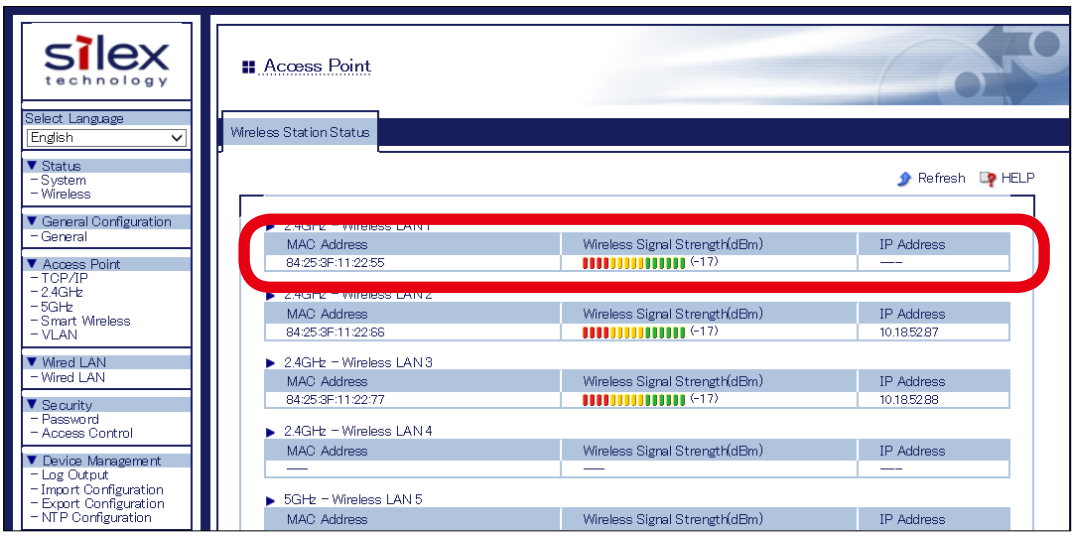
- AP-500AC uses two MAC Addresses for the WDS connection.
- The MAC Address used to connect to the host AP in WDS is displayed in the **System Status** page.
- The MAC Address of the wireless interface is displayed in **WDS Configuration** tab of **Wireless LAN Configuration** page. This will be the MAC Address of the wireless interface assigned for WDS connection.





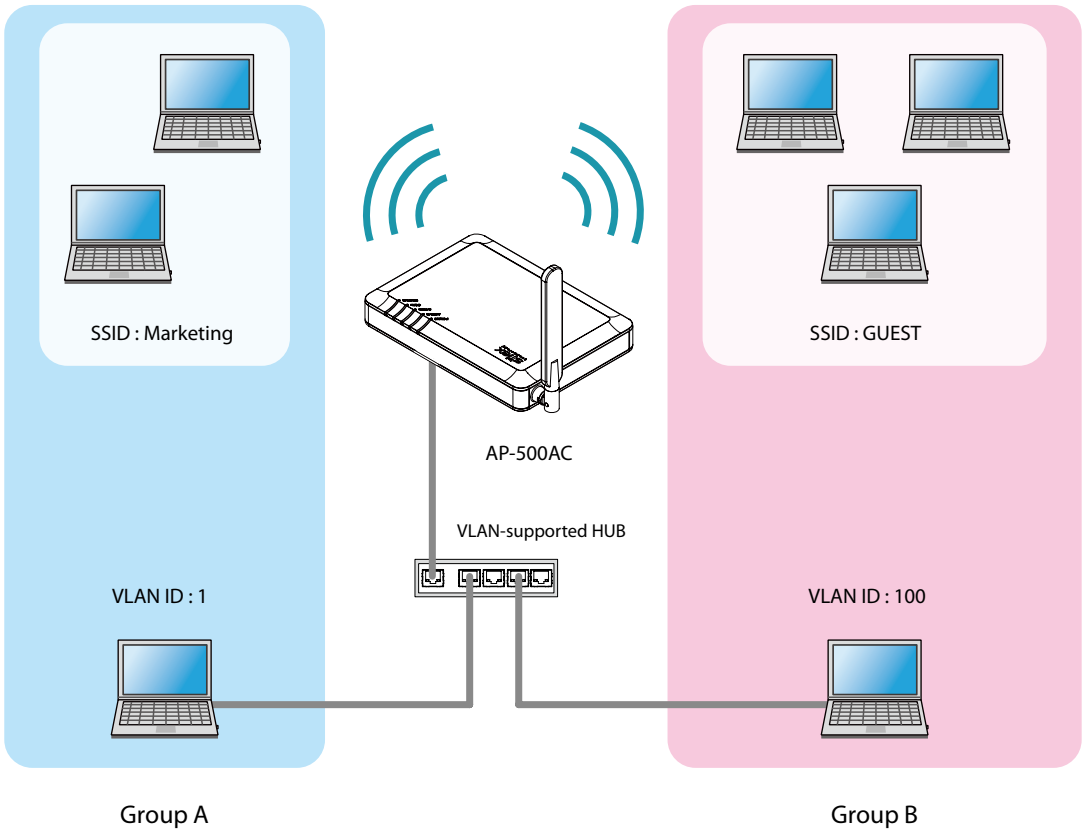


- When connected in WDS, the **Wireless Station Status** page of the host AP shows a list of connected client AP.
- The IP Address of the client AP is not displayed.
- The MAC Address of the client AP will be the MAC Address which the client AP uses to connect to the host AP in WDS mode.



5-5. VLAN Feature

A VLAN ID can be set to the SSID of wireless LAN structured by AP-500AC.
If AP-500AC is used with the switching HUB that supports tagged-VLAN (hereinafter the "VLAN HUB"), you can establish the virtual network groups.
As AP-500AC supports Multi SSID, up to 8 virtual network groups can be established.



Establish the Virtual Network Groups

TIP

- AP-500AC supports the tagged VLAN of IEEE802.1Q compliant.
- Dynamic VLAN is not included.

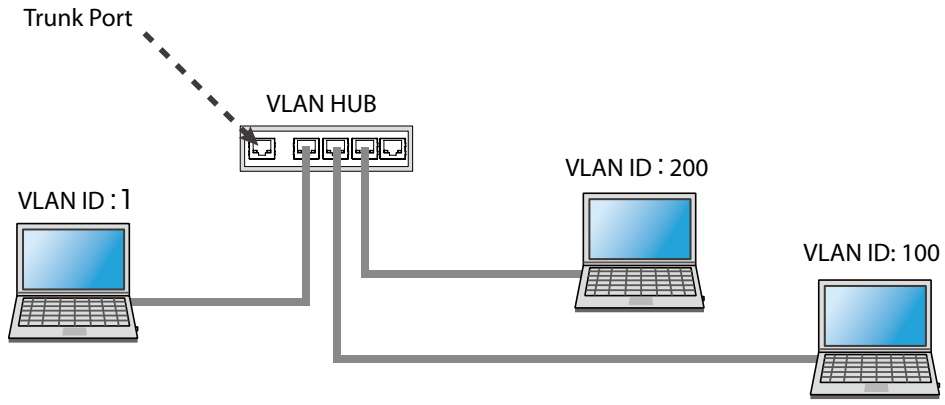
VLAN Configuration

The following explains how to install AP-500AC to where network groups have already been established using a VLAN HUB.

How to check the VLAN information on network:

Check the information below of the existing network.
For details on the VLAN HUB specifications, please see the operation manual that came with your VLAN HUB.

- Position of a trunk port on the VLAN HUB
- VLAN ID of the native VLAN
- VLAN ID of the devices connected to VLAN HUB



TIP

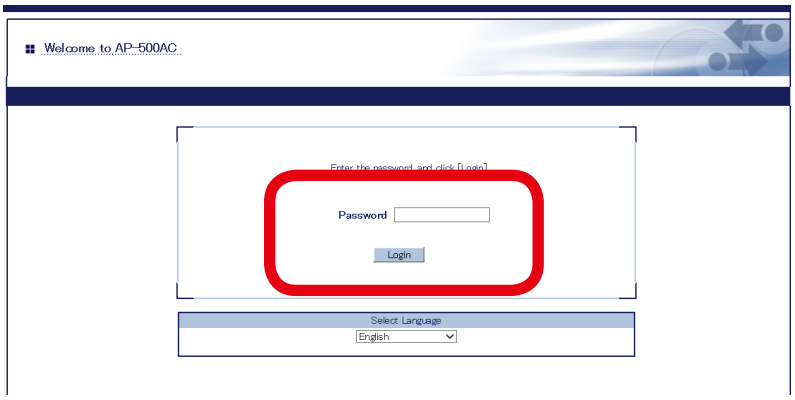
- If there is no available trunk port on the VLAN HUB, create a new one.
- For details on VLAN HUB specifications, please see the operation manual that came with your VLAN HUB.

Note

- The native VLAN is also referred to as untagged VLAN.

How to configure the VLAN setting on AP-500AC:

1. Log in to the Web page of AP-500AC using your Web browser.



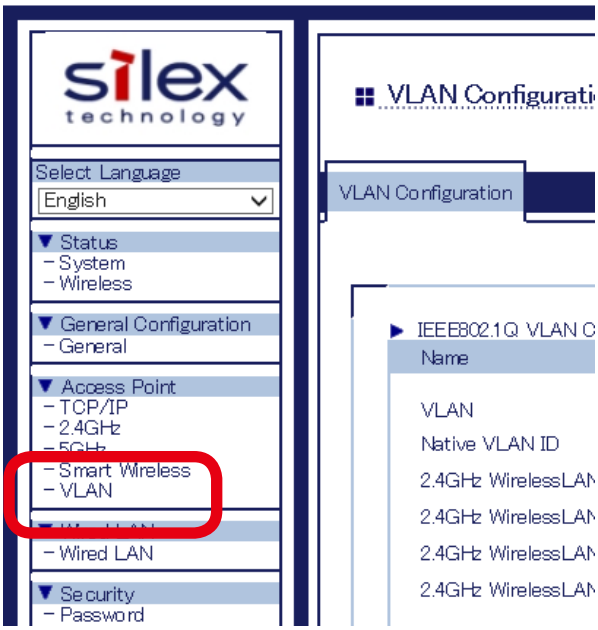
TIP

- When using a VLAN HUB during the configuration, please make sure that you connect AP-500AC to the port that can communicate with your PC.

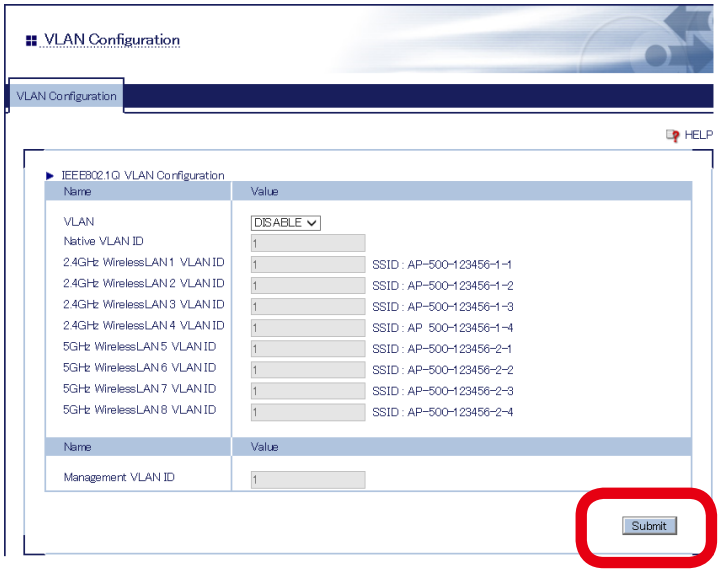
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu in the Web page, click **VLAN**.



3. If **VLAN** is set to **ENABLE**, the VLAN ID settings will become active.
Configure the VLAN ID appropriate for virtual network you wish to establish according to the existing network settings you have checked in advance.
When finished, click **Submit**.



Sample setting

	VLAN ID	SSID
Wireless LAN1	1	MARKETING
Wireless LAN2	100	GUEST
Wireless LAN3	200	SALES

TIP

- For the **Management VLAN ID**, when VLAN feature is enabled and one of following authentication modes is set for **Network Authentication**, enter the same VLAN ID as that of network group where the RADIUS server is installed.
  - **802.1X** - **WPA-Enterprise** - **WPA2-Enterprise** - **WPA/WPA2-Enterprise**

Note

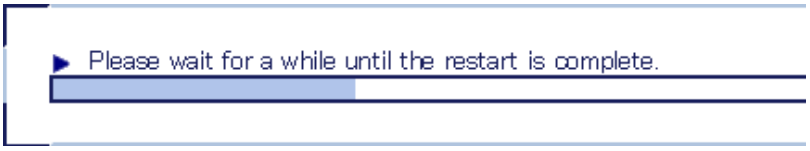
- For details on each configuration item, refer to **A. Appendix - A-1. List of All Settings**.
- For **Native VLAN ID**, enter the native VLAN ID of VLAN HUB that you have checked beforehand.
- For VLAN ID of the wireless LAN 1-8, enter VLAN ID of the devices connected to the HUB that you have checked beforehand.
- After VLAN feature is enabled, you will not be able to configure AP-500AC via the network with a different VLAN ID from management VLAN ID.
- When VLAN feature is set to **ENABLE**, the VLAN ID can also be configured from the wireless general configuration page.
- Even when VLAN feature is enabled, access from non-VLAN HUB is accepted if the same VLAN ID is set for both **Native VLAN ID** and **Management VLAN ID**. It is recommended to set a same VLAN ID for both of these.

4. When finished, click **Restart**.

Note

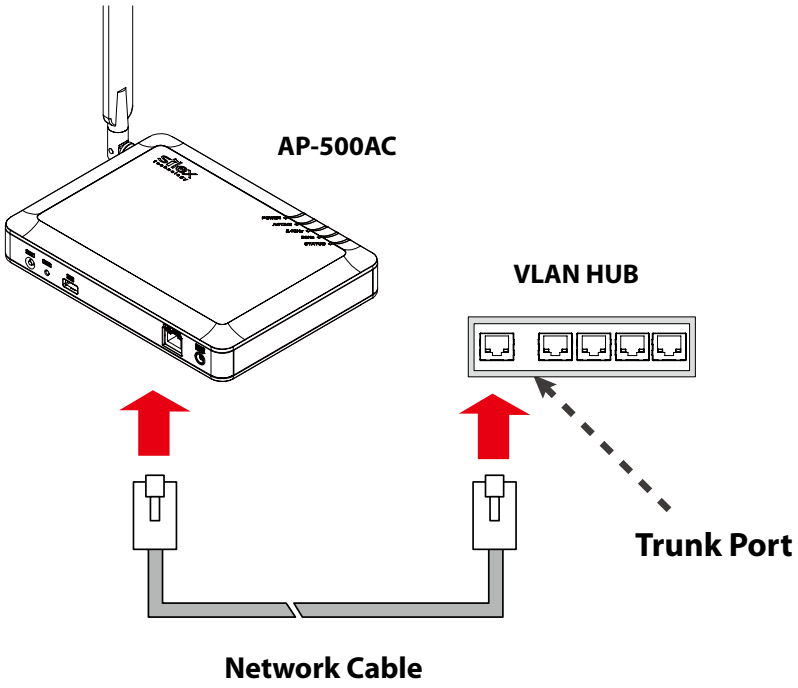
- If you continue to configure the other settings, you do not have to restart. Please restart when you completed all other settings.
- The VLAN setting will not take effect unless you restart AP-500AC.

5. After the **Restart** button is clicked, the progress bar is displayed. When the progress bar reaches the right end, the restart is completed.



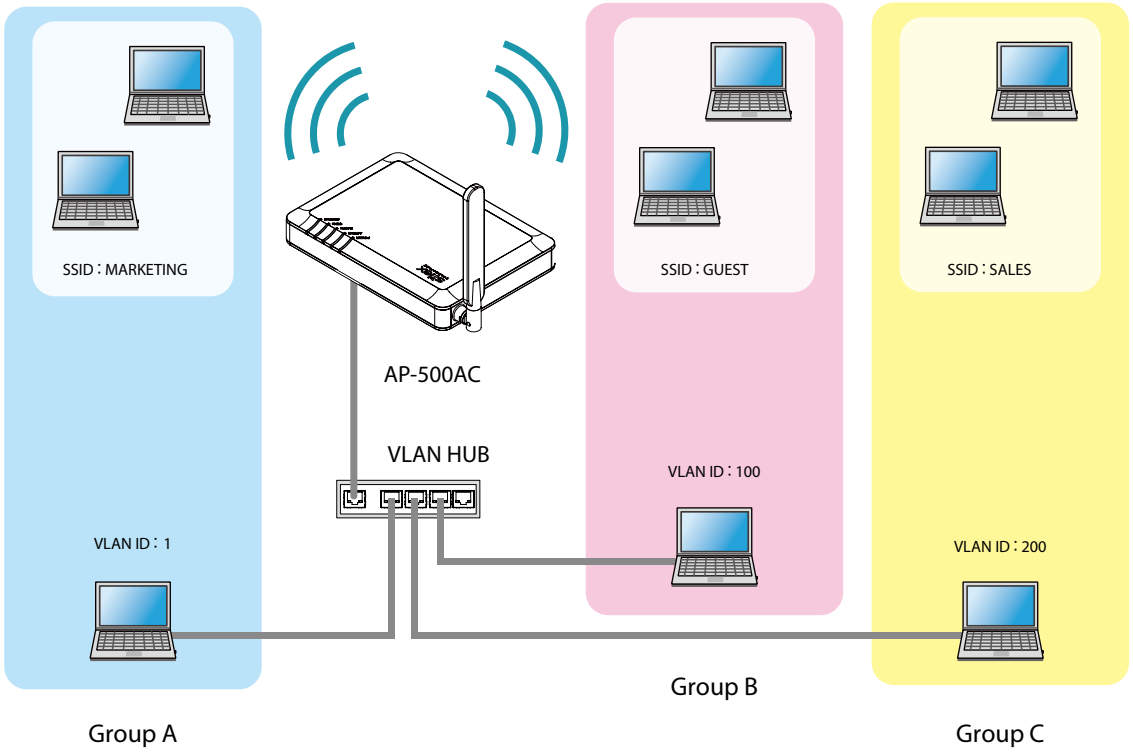
How to connect AP-500AC to a trunk port of VLAN HUB:

Connect a wired LAN port of AP-500AC and a trunk port of VLAN HUB (that you have checked beforehand) using a network cable.



The VLAN configuration is completed.

The virtual network groups will be active based on the VLAN ID setting you configured.



Establish the Virtual Network Groups

TIP

- After the VLAN feature is enabled, you will not be able to configure AP-500AC via the network with a different VLAN ID from management VLAN ID. If you are not sure of the VLAN ID of the management VLAN, you will need to initialize the settings and reconfigure AP-500AC. For how to initialize AP-500AC, refer to **Chapter 5-11 Maintenance Feature** - **How to reset AP-500AC to factory defaults using the Push Switch**.
- To configure AP-500AC wirelessly from a PC running on VLAN-enabled environment, the VLAN ID configured to SSID of the wireless LAN must be the same as management VLAN ID. By defaults, the configuration change via wireless LAN is restricted on AP-500AC since the **Access Control** feature is on. Please change the setting appropriate for your environment.
- For details on each configuration item, refer to **A. Appendix** - **A-1. List of All Settings**.

5-6. Mac Address Filter

It is possible to block access from particular devices to AP-500AC. MAC Address filter can respectively be set for a wired LAN and wireless interface.

Filter Type

By registering the MAC Address to a list, access of devices is allowed or denied based on the filter type below.

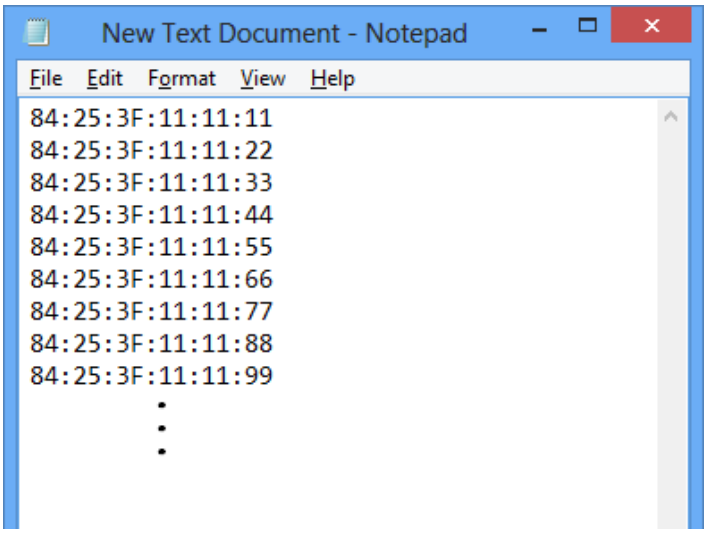
Name	Description
DISABLE	Does not use MAC Address filter. All devices are allowed to access.
ALLOW	Allows access only from devices with the registered MAC Address.
DENY	Denies access from devices with the registered MAC Address.

Note

- If Smart Wireless Setup is enabled on the wireless interface, MAC Address filtering cannot be used on that interface. In order to use MAC Address filtering, disable Smart Wireless Setup or select the wireless interface which does not have MAC Address filter setting at **Smart Wireless Setup** tab.

MAC Address List

Register the MAC Address of devices to allow/deny access to AP-500AC.
To register, create a list of MAC Addresses as a text file and import it to AP-500AC from the Web page.



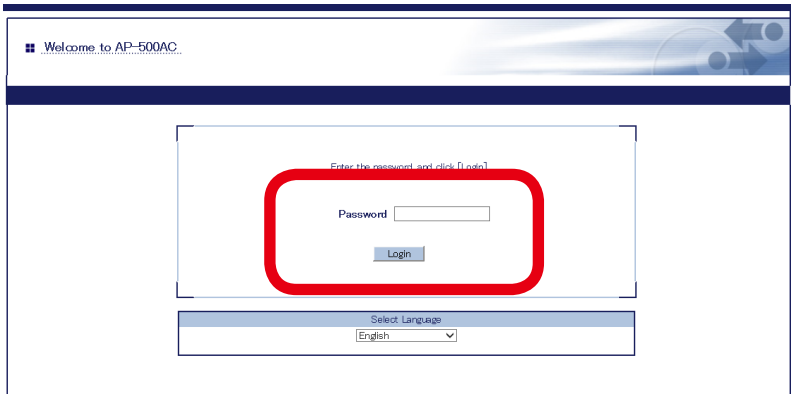
Note

- Create the MAC Address list as a text file using an editor, etc. and save it with any file name.
- In MAC Address list, one MAC Address needs to be described per line.
- Below is the number of MAC Addresses that can be registered for each wired LAN and wireless interface.
  Wired LAN: 32 addresses
  Wireless LAN: 100 addresses

MAC Address Filter Setting

Following explains how to configure the MAC Address filter.

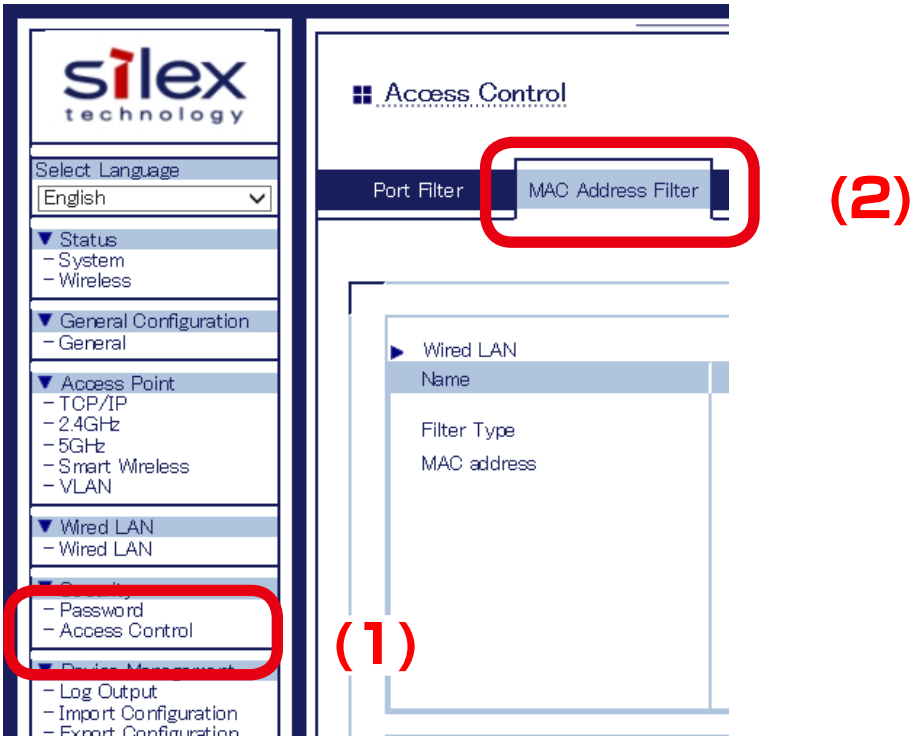
1. Log in to the Web page of AP-500AC using your Web browser.



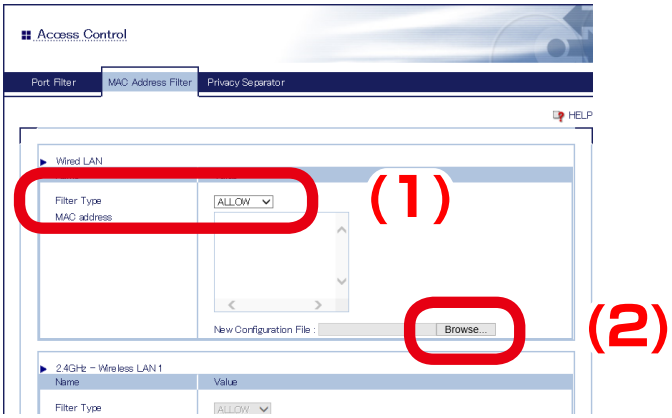
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu in the Web page, click **Access Control - MAC Address Filter**.



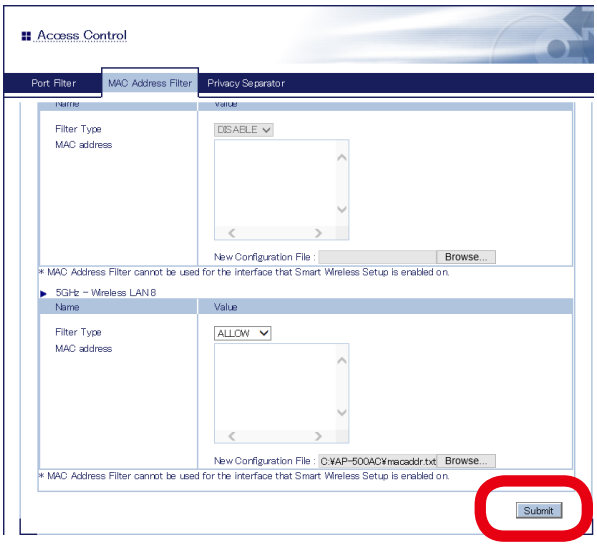
3. Select a filter type for the interface to use MAC Address filter. Click **Browse** and select a file of MAC Address list.



Note

- If Smart Wireless Setup is enabled on the wireless interface, MAC Address filtering cannot be used.

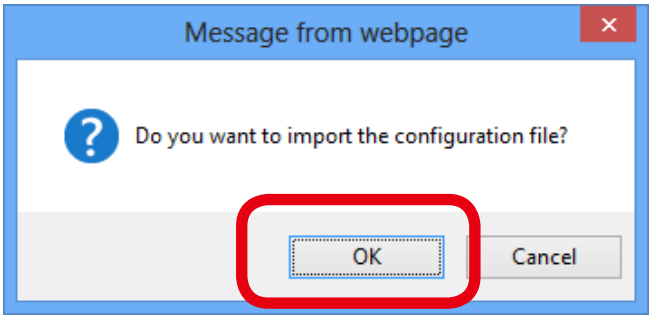
4. When the filter type is selected and the file of MAC Address list is selected for all interfaces to use MAC Address filter, click **Submit**.



Note

- After **Submit** is clicked, MAC Address information of the imported file is displayed on the list of Web page.
- When a file of MAC Address list contains a number of addresses that exceeds the maximum number of registerable addresses on each interface, error message will appear.
- It is impossible to edit the MAC Address information on Web page. To add or remove the address, edit a file of MAC Address list and import it again.

5. A confirmation message is displayed. Click **OK**.

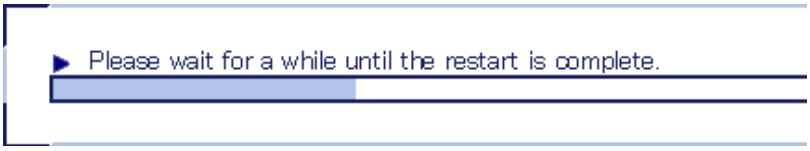


6. When finished, click **Restart**.

Note

- If you continue to configure the other settings, you do not have to restart. Please restart when you completed all other settings.
- The MAC Address Filter setting will not take effect unless you restart AP-500AC.

7. After the **Restart** button is clicked, the progress bar is displayed. When the progress bar reaches the right end, the restart is completed.



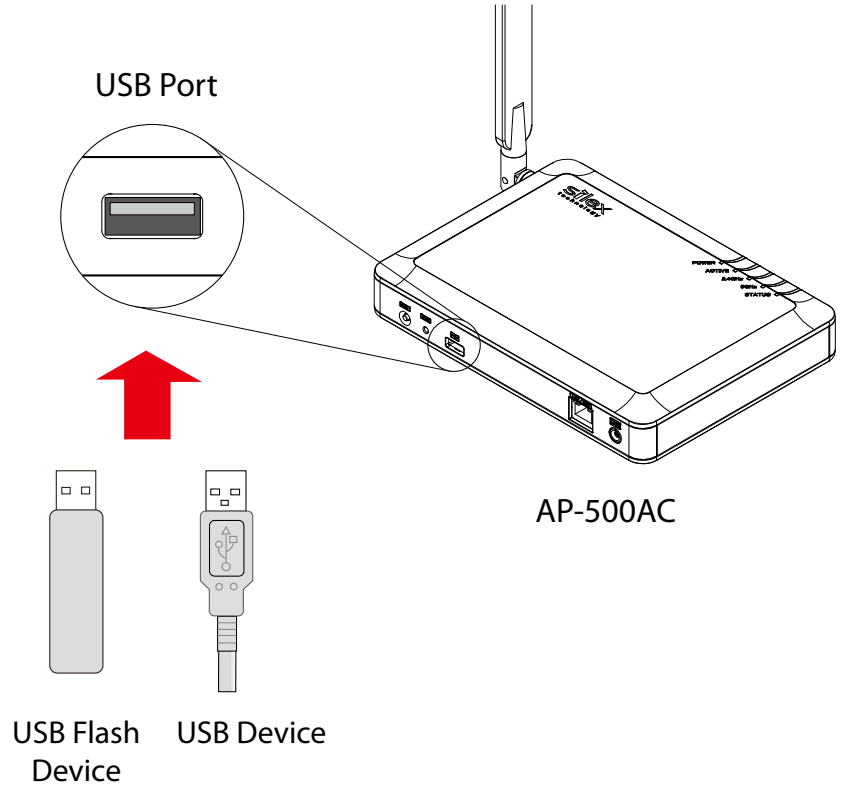
5-7. Device Server Feature

The USB devices connected to AP-500AC can be shared over the network.
To use the device server feature, the USB connection utility, "SX Virtual Link" is required.
How to install and use SX Virtual Link is as follows:

Note

- SX Virtual Link is also used for the log output feature.

Connect the USB device that you wish to share over the network to the USB port of AP-500AC.



Downloading & Installing SX Virtual Link

What is SX Virtual Link?

SX Virtual Link allows you to connect your PC to a USB device that is connected to AP-500AC. Use SX Virtual Link when you connect/disconnect to/from the USB device.

AP-500AC allows you to use USB devices as if they were connected directly to your PC.

How to download SX Virtual Link:

1. Access our website below.

URL	
USA	**http://www.silexamerica.com/**
Europe	**http://www.silexeurope.com/**

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

How to install SX Virtual Link:

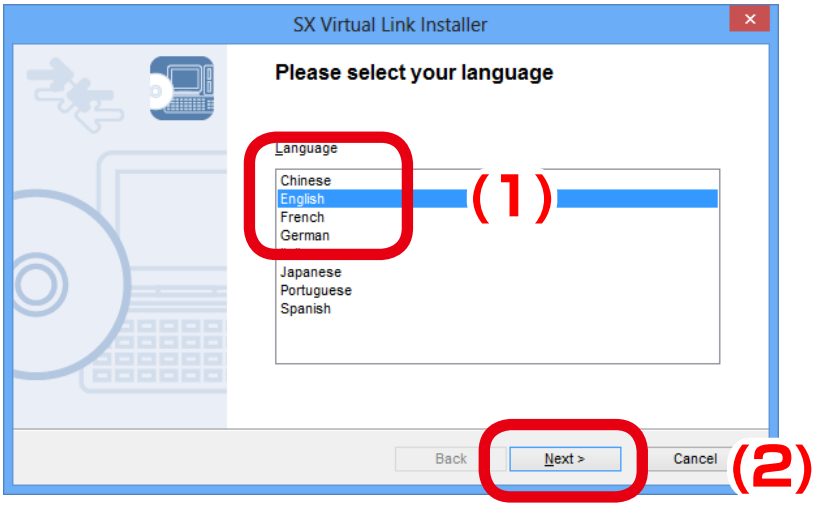
> *TIP*
> - Administrator privilege is required for installation.

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

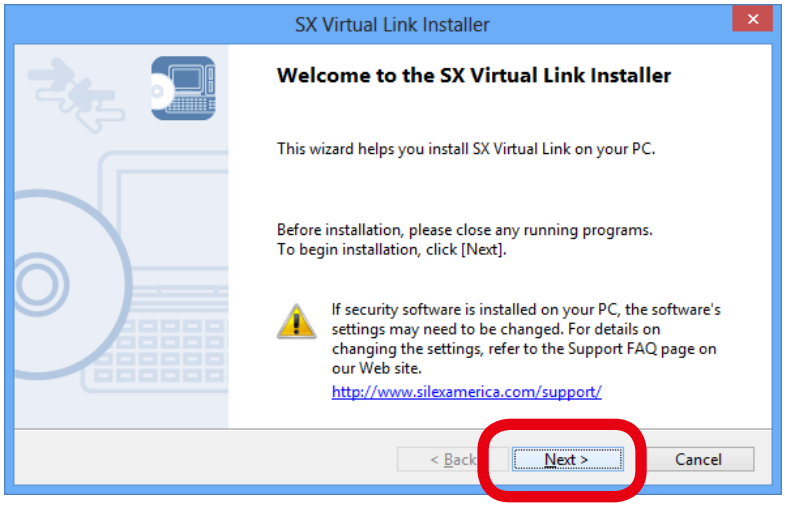
2. The User Account Control message is displayed, click **Yes**.

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

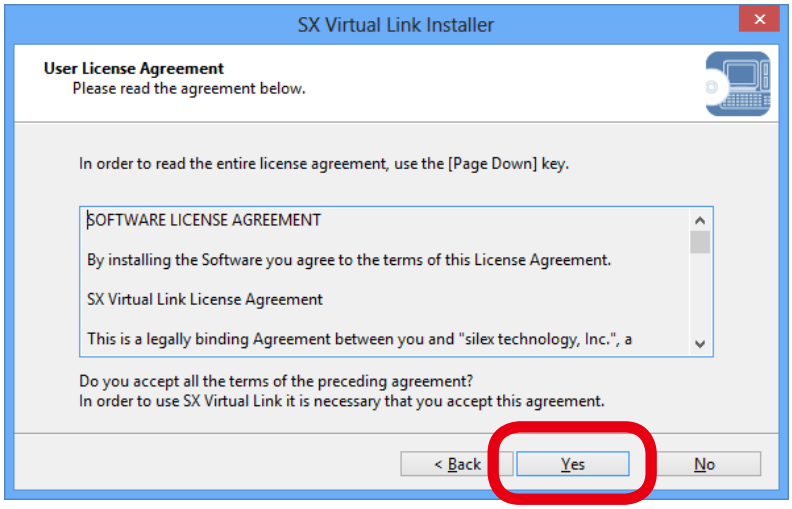
3. SX Virtual Link installer is started and the language selection menu is displayed. Select **English** and click **Next**.



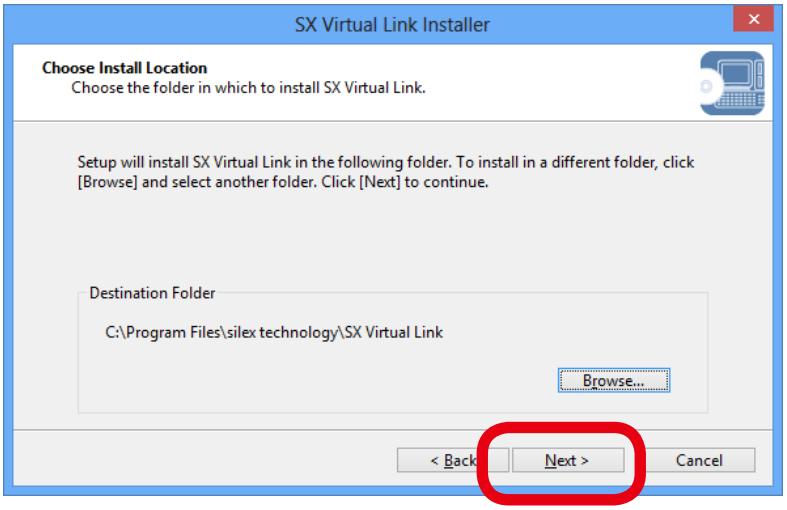
4. Click **Next**.



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



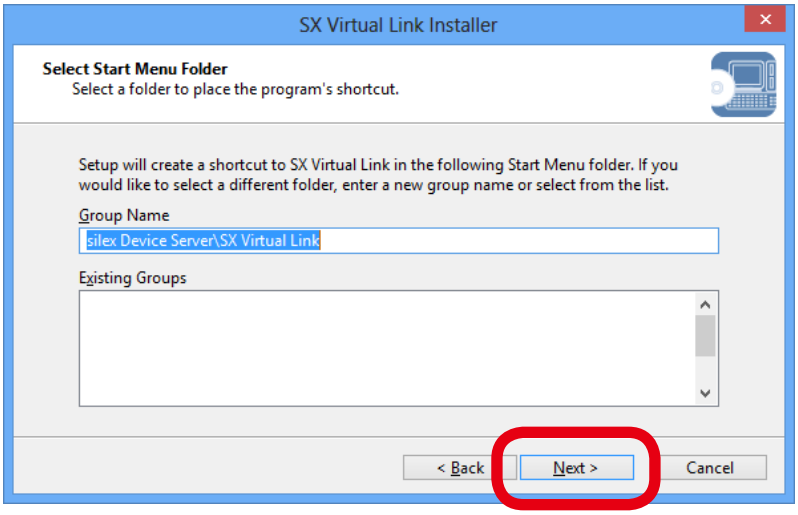
6. Select a folder to install into and click **Next**.



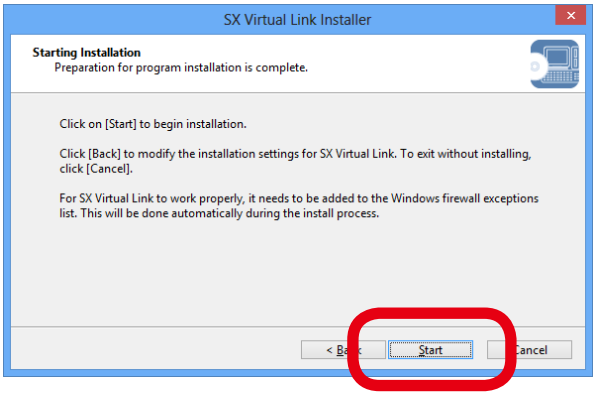
Note

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

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

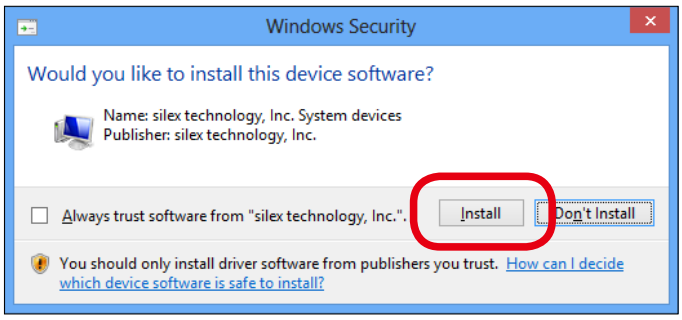


8. Click **Start** to begin the installation.

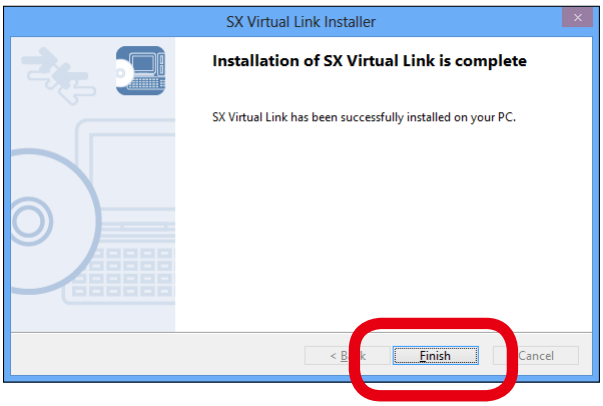


TIP

- When **Windows Security** screen is displayed, click **Install**.



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



TIP

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

Sharing USB Devices over the Network

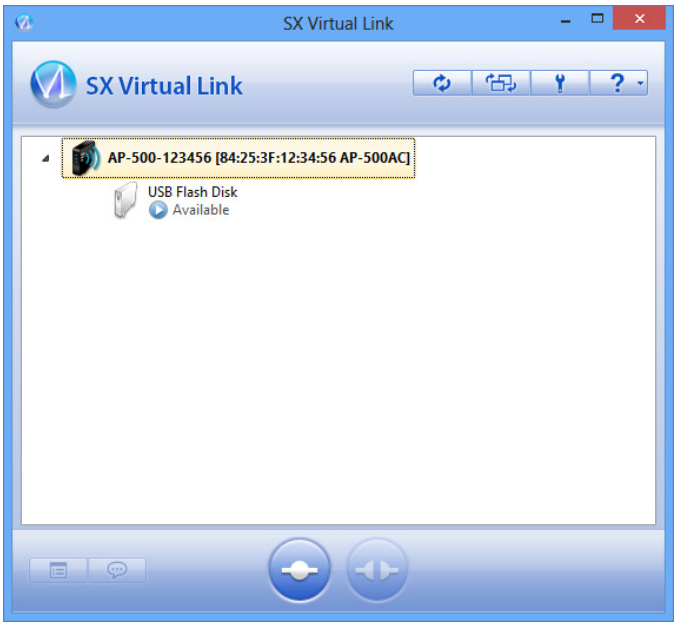
How to start SX Virtual Link:

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

Note

- If SX Virtual Link is not running, click **Start** - **SX Virtual Link**.
- In Windows 7, click the ( ) button on the notification area (bottom right corner of your desktop) to display the tasktray icons.

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



Note

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

How to connect/disconnect to/from USB devices:

1. Select the USB device in SX Virtual Link's main window and connect to it.

2. When successfully connected to the USB device, Windows Plug and Play will run and the USB device will become ready to use.

3. When finished using the USB device, disconnect it using SX Virtual Link.

How to connect:

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

How to disconnect:

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


TIP

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

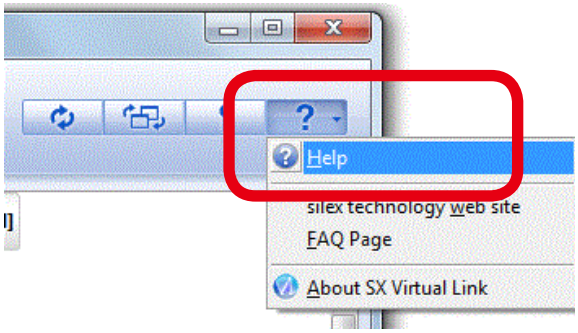

Note

- For details on how to use SX Virtual Link, refer to the Online Help.

How to open the SX Virtual Link's Online Help

1. Start SX Virtual Link.

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



3. Online Help will open.

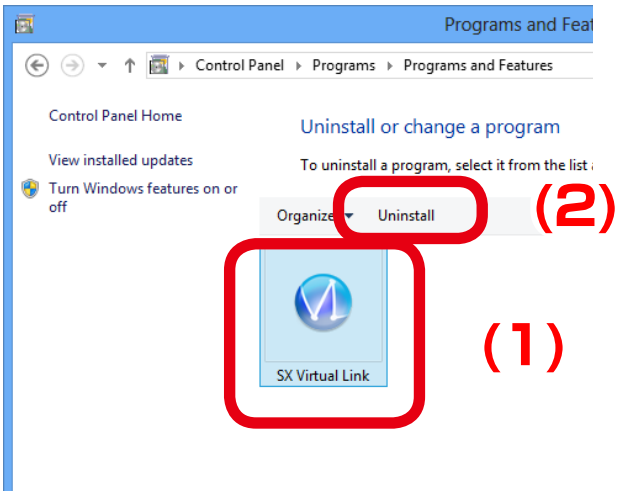
Uninstalling SX Virtual Link

How to uninstall the USB device connection utility, SX Virtual Link is explained.
Follow the procedures below to uninstall SX Virtual Link.

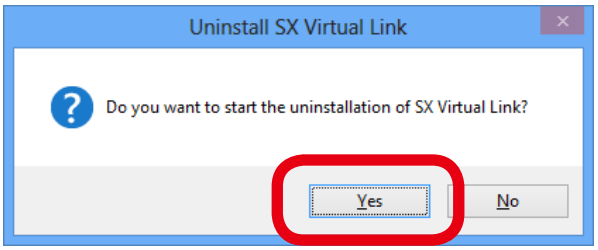
> **TIP**
> - To uninstall SX Virtual Link, administrator privilege is required.

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

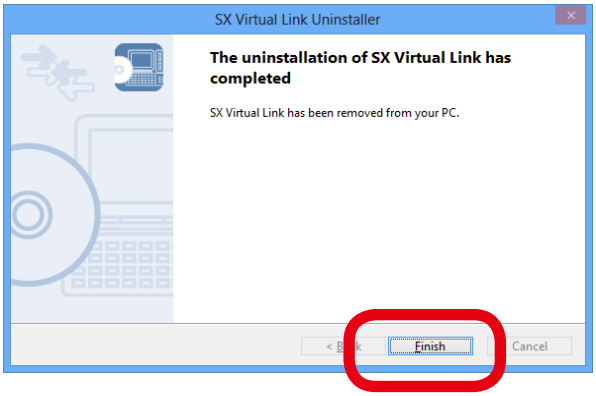
2. Select SX Virtual Link from the list and click **Uninstall**.



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



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



5-8. Log Output

The log information (access log, etc.) can be sent to the Syslog server as well as saved to the USB storage device connected to AP-500AC. Once the log file is saved to the USB storage device, it can be retrieved over a network using SX Virtual link. How to output the log and retrieve it from the USB storage device is explained.

TIP

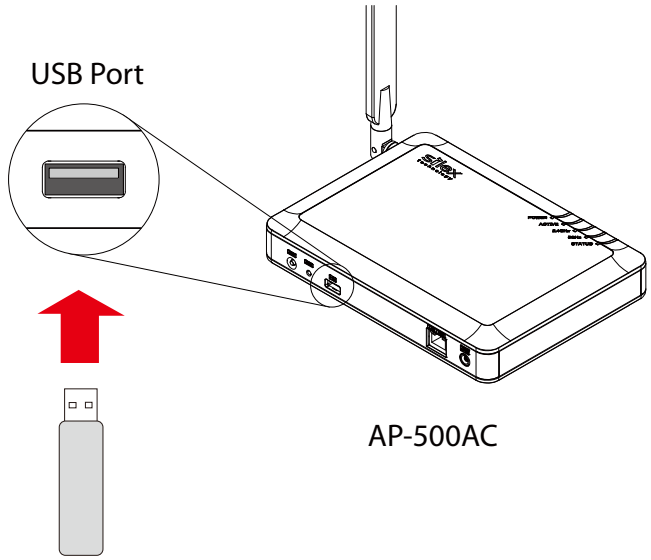
- Display may vary depending on the Web browser.
- Only one USB storage device can be connected to AP-500AC to save the log to the USB storage device. Also, the connected storage device cannot be used over network using SX Virtual Link.
- When removing the USB storage device from AP-500AC, please disable the log output feature beforehand.

The log files are saved as the following formats.

Format		<Date> <Hostname> <Level> <Program> <Message>
Details	Date	System time when the event occurred.
	Hostname	Host name of AP-500AC
	Level	Message level
	Program	Name of the program at which the event occurred.
	Message	Log message for each event - Connection of the stations - Connection/Disconnection request of the stations
Output Sample	Jan 1 09:30:45 AP-500-0109A4 user.debug kernel: sxsyslogd: VAP-0: Connect station.(84:25:3f:01:01:01)	

Getting Started

To retrieve the log information, the USB connection utility, SX Virtual Link is required. For how to install, refer to **5-7. Device Server Feature**.

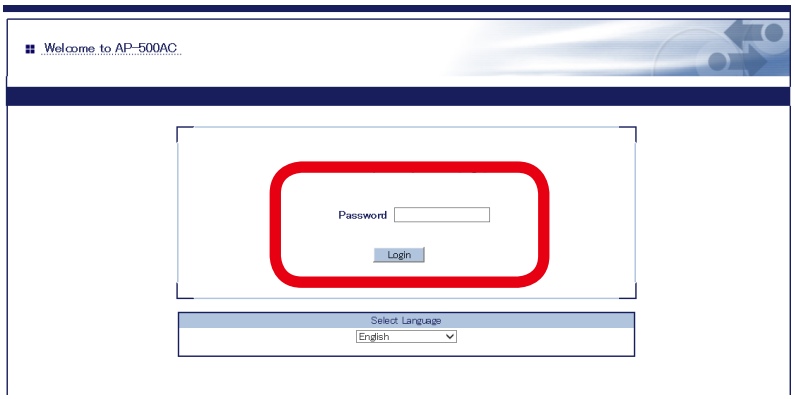


USB Flash Drive

In order to save the log to USB storage device, prepare a USB storage device such as USB flash drive, etc. and connect it to AP-500AC.

Log Output Settings

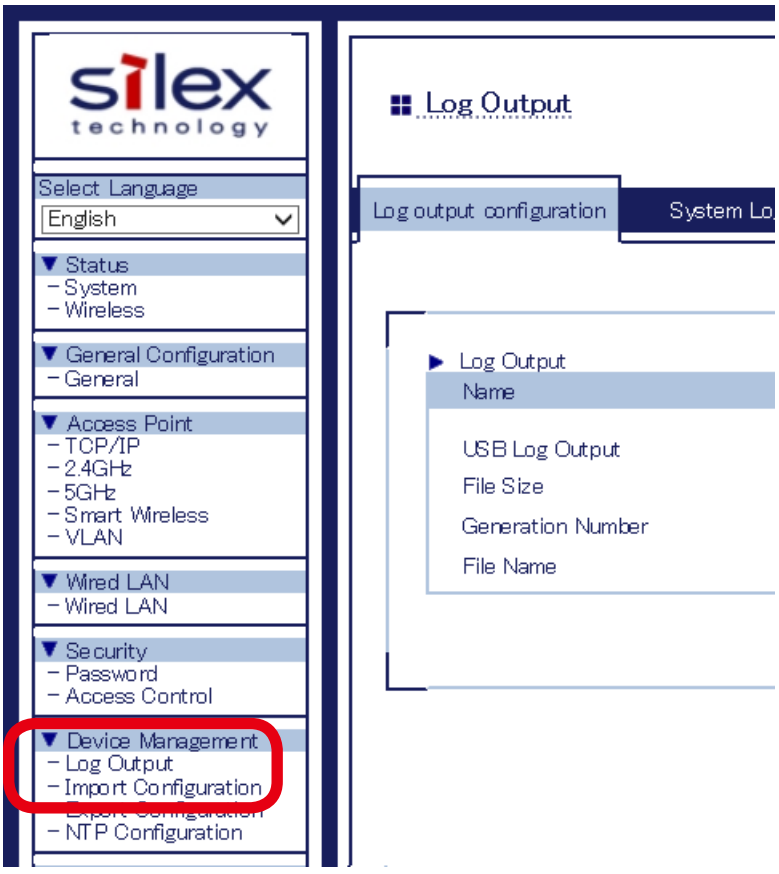
1. Log in to the Web page of AP-500AC using your Web browser.



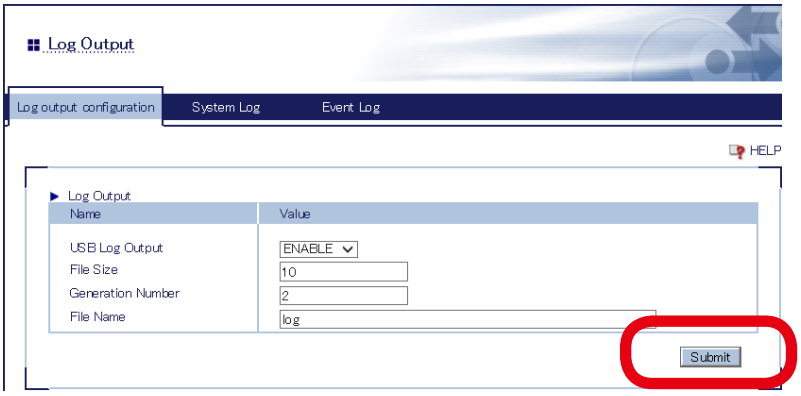
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu on the Web page, click **Log Output**.



3. In the **Log Output** page, specify where to output the log and file names and then click **Submit**.



Note

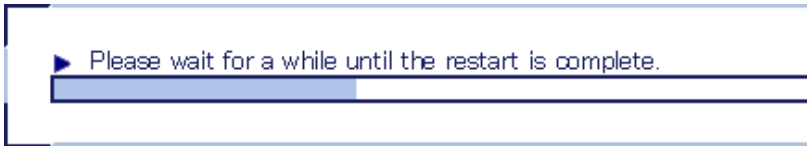
- For details on each configuration item, refer to **A. Appendix** - **A-1. List of All Settings**.

4. When finished, click **Restart**.

Note

- If you continue to configure the other settings, you do not have to restart. Please restart when you completed all other settings.
- The log output will not be started unless AP-500AC is restarted.
- If the log output feature is enabled, the USB storage device connected to AP-500AC are not displayed in SX Virtual Link.

5. After the **Restart** button is clicked, the progress bar is displayed. When the progress bar reaches the right end, the restart is completed.

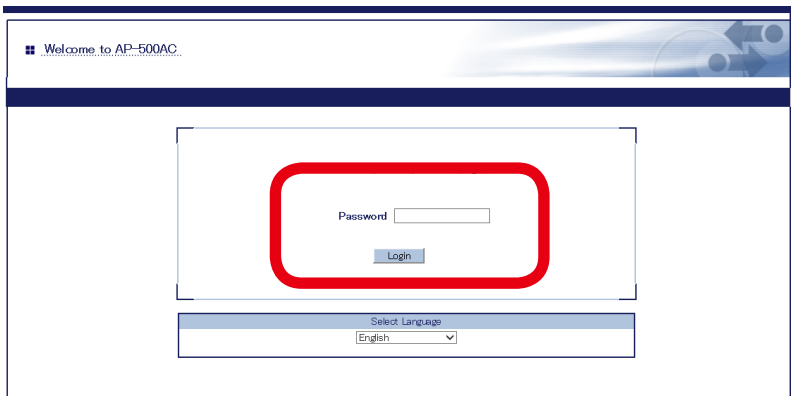


Retrieving the Log Saved into USB Storage Device

To retrieve the log files saved in the USB storage device connected to AP-500AC, disable the USB log output feature first. The log can be retrieved using SX Virtual Link.

How to disable the USB log output:

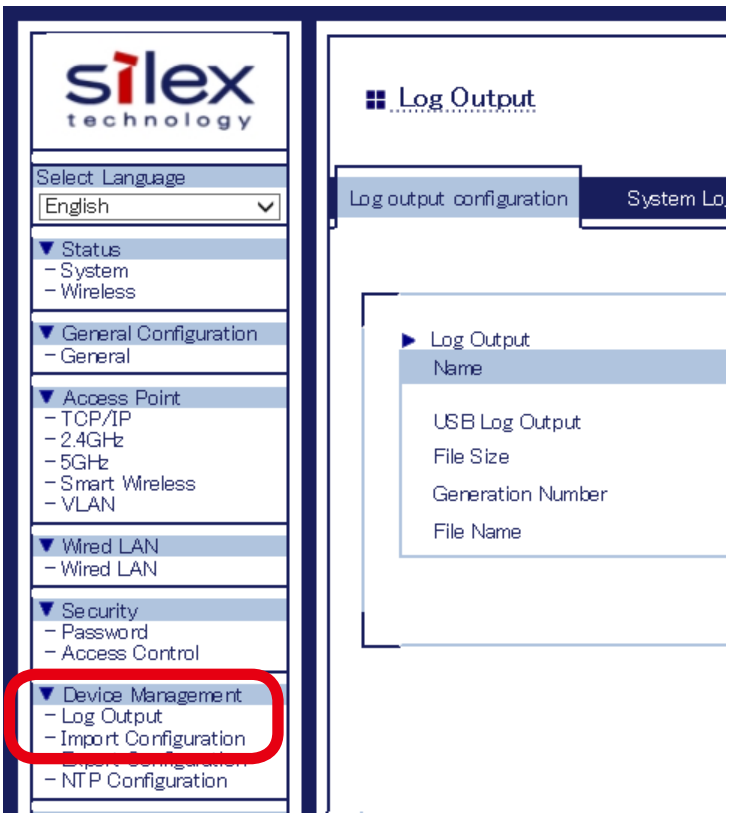
1. Log in to the Web page of AP-500AC using your Web browser.



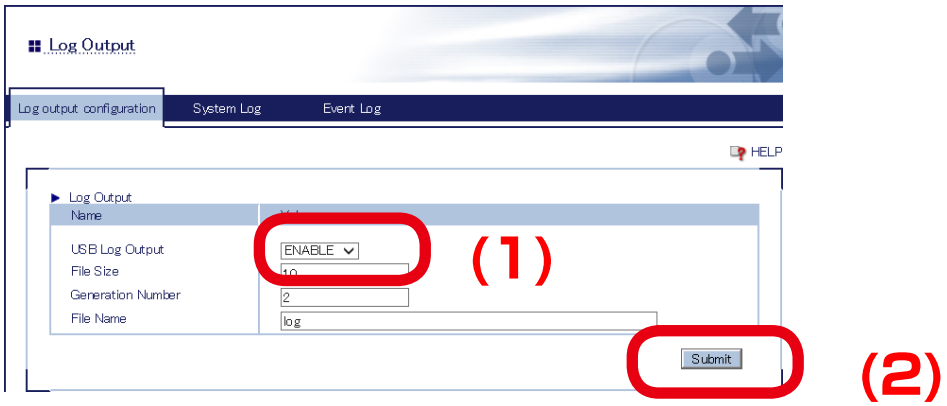
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu on the Web page, click **Log Output**.



3. In the **Log Output** page, select **DISABLE** for **USB Log Output** and click **Submit**.

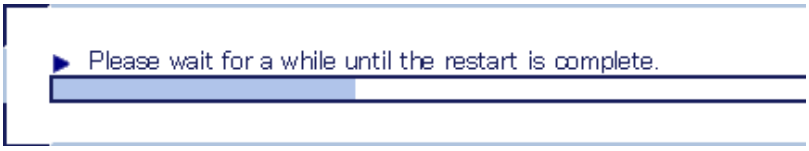


4. When finished, click **Restart**.

Note

- If you continue to configure the other settings, you do not have to restart. Please restart when you completed all other settings.
- The log output will not be stopped unless AP-500AC is restarted.

5. After the **Restart** button is clicked, the progress bar is displayed. When the progress bar reaches the right end, the restart is completed.



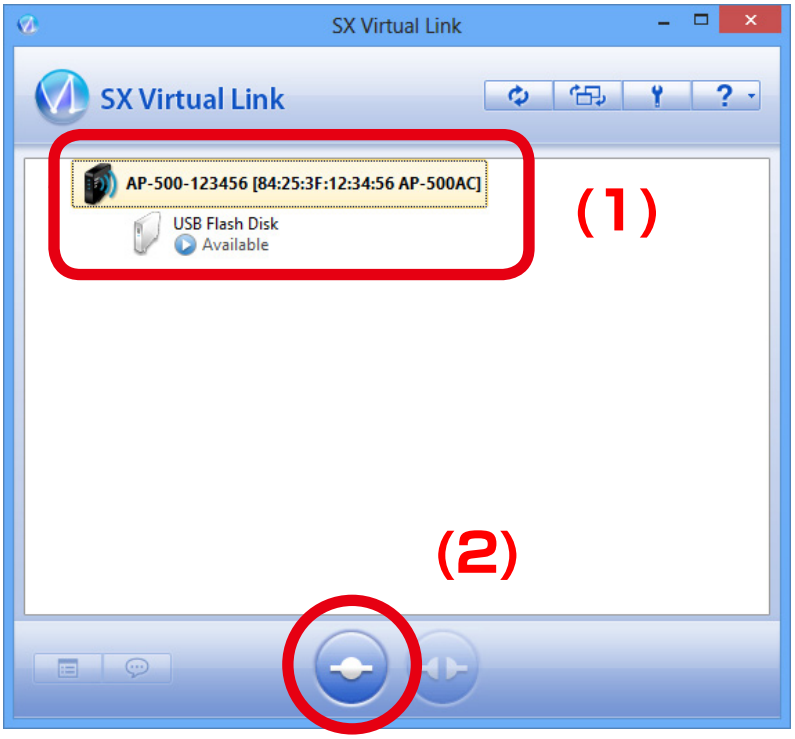
How to retrieve the log files:

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

Note

- If SX Virtual Link is not running, click **Start** - **SX Virtual Link**.
- In Windows 7, click the ( ) button on the notification area (bottom right corner of your desktop) to display the tasktray icons.

2. The SX Virtual Link's main window appears. The USB devices running on a network are displayed in the device list.
Select the USB storage device containing the log file and click **Connect** button.

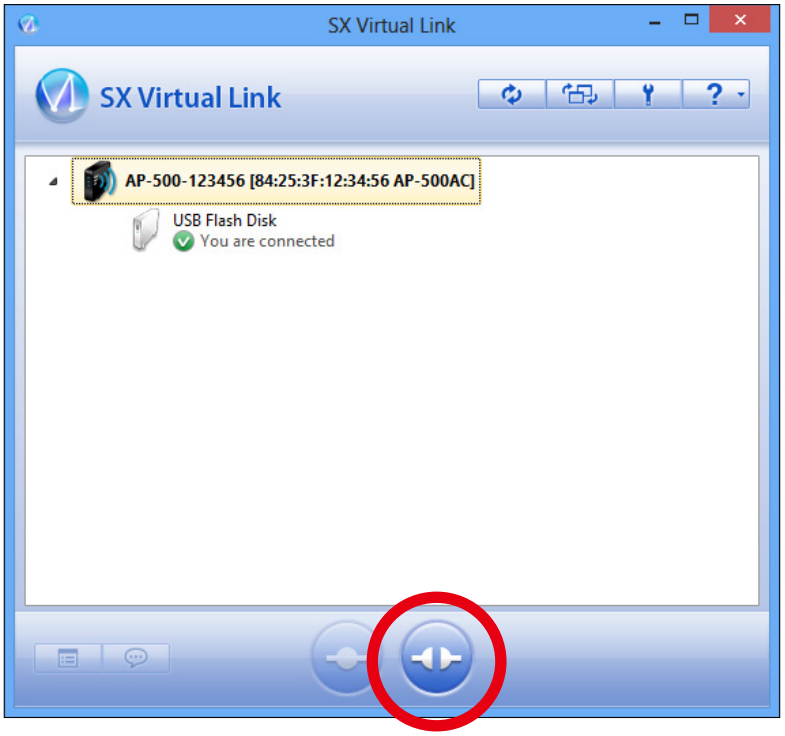


Note

- For details on SX Virtual Link, refer to **5-7. Device Server Feature** - **Sharing USB Devices over the Network**.

3. When successfully connected, Windows Plug and Play will run and the USB storage device will become ready to use. Now you can retrieve the saved log files.

4. When finished retrieving the log files, click **Disconnect** button in SX Virtual Link.

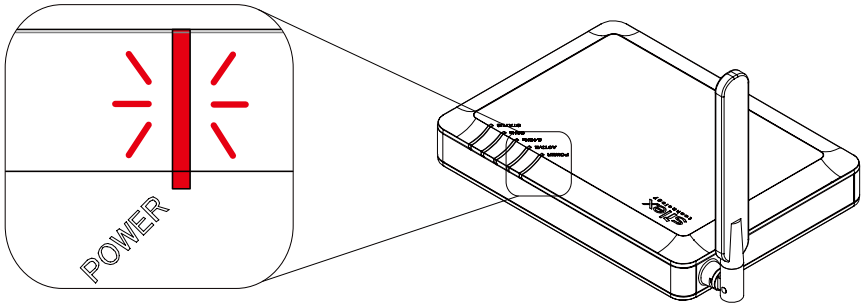


Note

- For details on SX Virtual Link, refer to **5-7. Device Server Feature** - **Sharing USB Devices over the Network**.
- To restart the log output, configure the log output settings again.

Notice When Using the Log Output

Please DO NOT remove the USB storage device while the USB log output is enabled.
When you remove the USB storage device, be sure to disable the USB log output feature beforehand. For how to disable the USB log output, refer to **Retrieving the Log Saved into USB Storage Device** - **How to disable the USB log output**.
If the USB storage device is removed without turning off the USB log output feature, the POWER LED on AP-500AC will blink in Red.



POWER LED : Blinks Red

AP-500AC

If the POWER LED blinks in Red, follow the instructions below to recover from it:

1. Connect the removed USB storage device to the PC to verify that it has not be damaged or corrupted.

Note

- Please format the USB storage device if the data is corrupted.

2. Remove the USB storage device from the PC and reconnect it to AP-500AC.

3. Restart AP-500AC.

Note

- For how to restart AP-500AC, refer to **Chapter 5-11 Maintenance Feature** - **Restarting**.
- The log output will not be started unless AP-500AC is restarted.

5-9. Saving Log

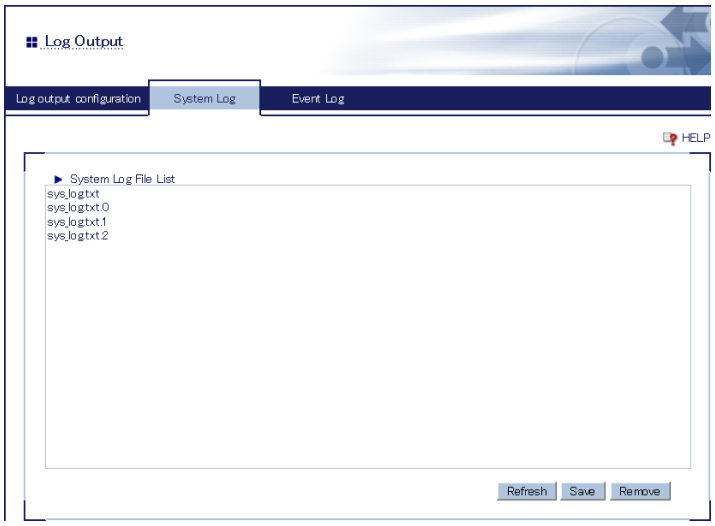
AP-500AC can save the operating log.
Once the log is saved, it can be retrieved or deleted from the Web configuration interface.

Types of Log

There are two types of log that can be saved by AP-500AC.

System Log

Power-on status, operating status, etc. of AP-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.

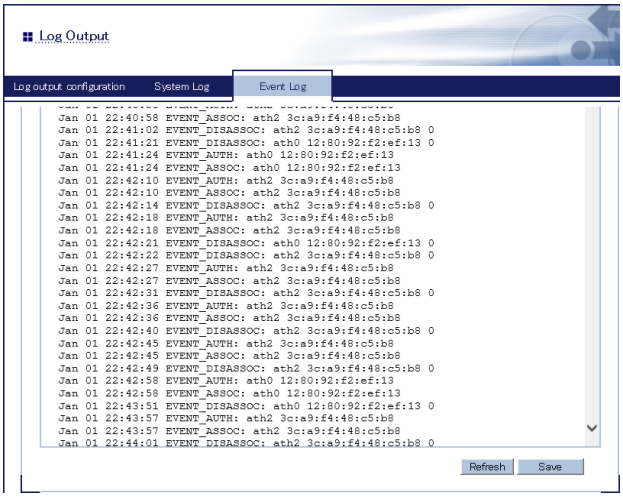


Note

- The system log file will remain even after AP-500AC is reset to factory defaults.
- When a size of log file (file name: **sys_log.txt**) exceeds 10MB, a new file is created. For the existing file, a number will be added to the end of the file name then.
- As the end number of the file name increases one by one when a new log file is created, files with a greater number will be older logs.
- Up to 99 log files can be saved, starting from **sys_log.txt.0** to **sys_log.txt.98**.
- If a new file is created when 99 log files have already been there, the oldest file **sys_log.txt.98** will be deleted.
- Up to 1GB log can be saved.

Event Log

When station devices are connected or disconnected, the log message is saved as a log. In case of a network trouble, you can check the wireless connection status by referring the retrieved event logs.



The event log file is saved as the format below:

Events	Log
Notification of connection	EVENT_AUTH: [I/F] [MACAddr]
	EVENT_ASSOC: [I/F] [MACAddr]
Notification of disconnection	EVENT_DEAUTH: [I/F] [MACAddr] [reason code]
	EVENT_DISASSOC: [I/F] [MACAddr] [reason code]
Configuration mode start	setting mode start
Configuration mode error	setting mode is failed
Smart Wireless Setup started	Smart Wireless Setting start
Smart Wireless Setup finished successfully	Smart Wireless Setting Success [MACAddr]
Smart Wireless Setup timed out	Smart Wireless Setting Timeout
Smart Wireless Setup overlapped	Smart Wireless Setting Overlap
Smart Wireless Setup or others failed	Smart Wireless Setting Failed
Firmware update	Firmware Update [old_version] -> [new_version]
USB storage error occurred	USB Storage error
USB overcurrent occurred	USB Overcurrent Detect
Wireless module error (2.4GHz)	HAL0 module is not created
Wireless module error (5GHz)	HAL1 module is not created

Note

- Only one file is saved for event log.
- Up to 64KB log information can be saved as event log file. When it exceeds 64KB, the information will automatically be deleted from the older one.
- On Web page, all log information of 64KB can be seen.

TIP

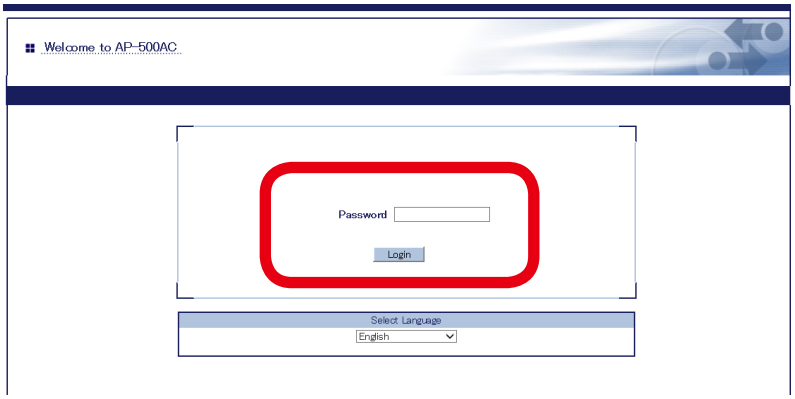
- It is impossible to delete the event log file manually.

Retrieving/Deleting System Log

How to retrieve system log:

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

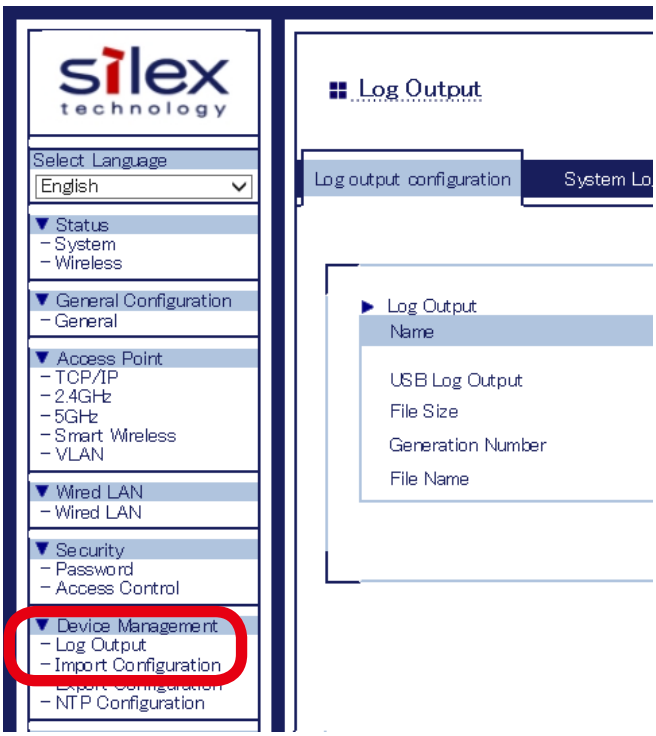
1. Log in to the Web page of AP-500AC using your Web browser.



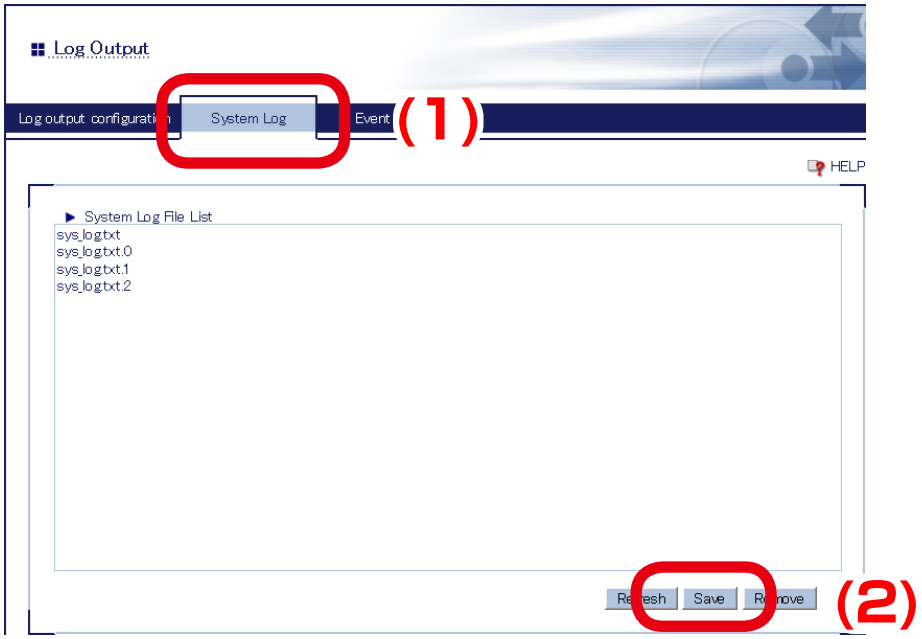
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu on the Web page, click **Log Output**.



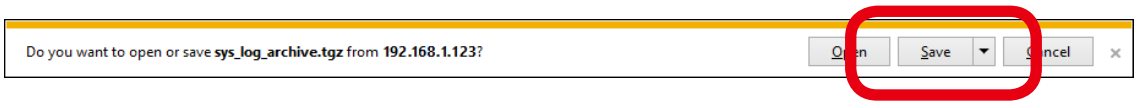
3. Select **System Log** to show a list of the system logs and click **Save** to save them.



TIP

- The log files cannot be saved individually.

4. When the message appears to confirm where to save the compressed file of system logs (**sys_log_archive.tgz**), click **Save**.



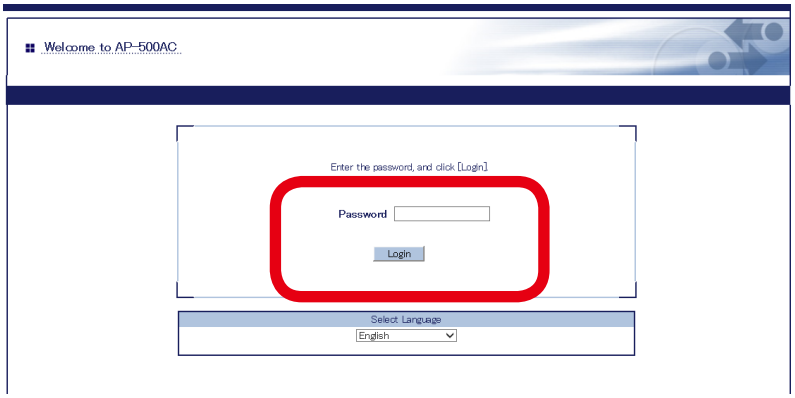
Note

- If ▼ is clicked, **Save as** option can be selected.

How to delete system log:

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

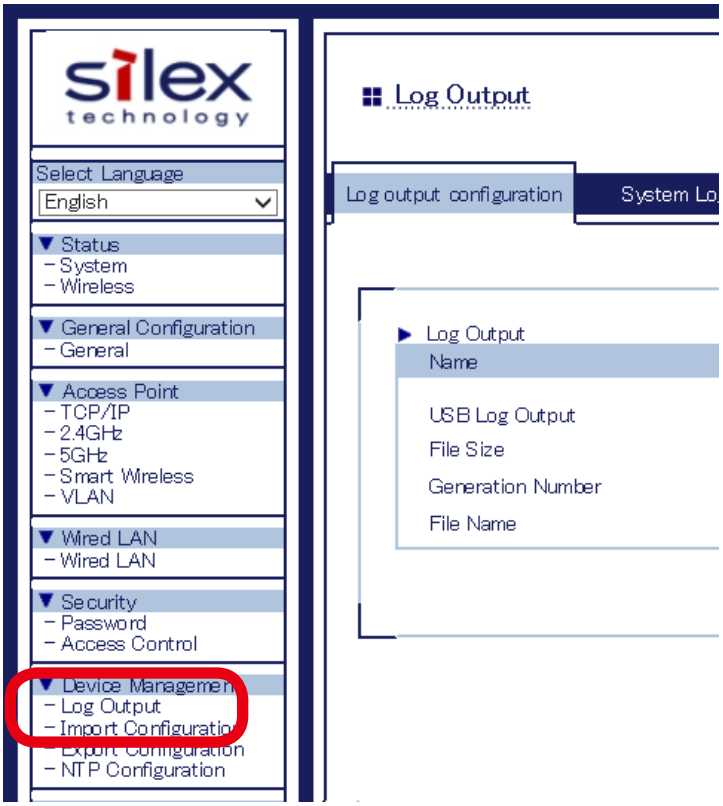
1. Log in to the Web page of AP-500AC using your Web browser.



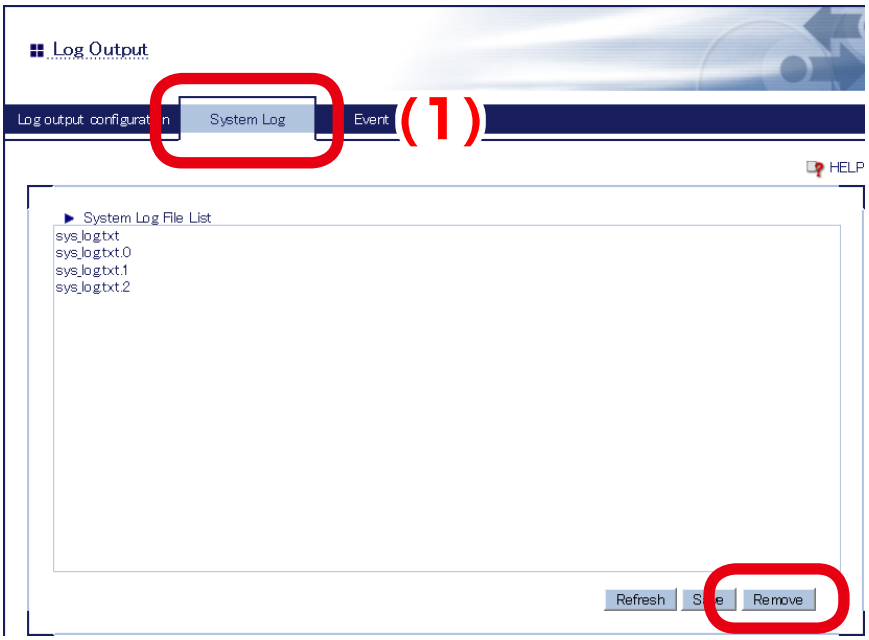
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu on the Web page, click **Log Output**.



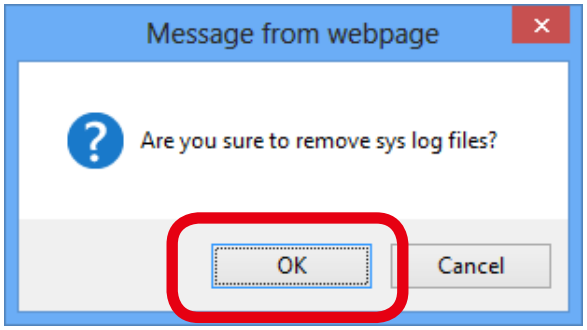
3. Select **System Log** to show a list of the system logs and click **Remove** to delete them.



TIP

- The system log files cannot be deleted individually.

4. Click **OK** to a confirmation message.



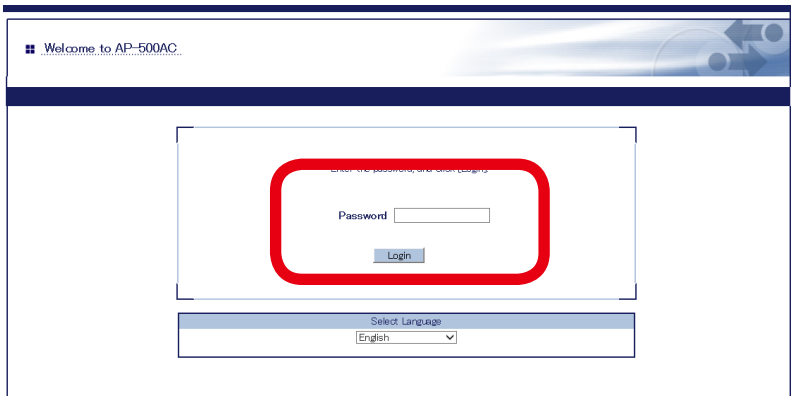
Note

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

Retrieving Event Log

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

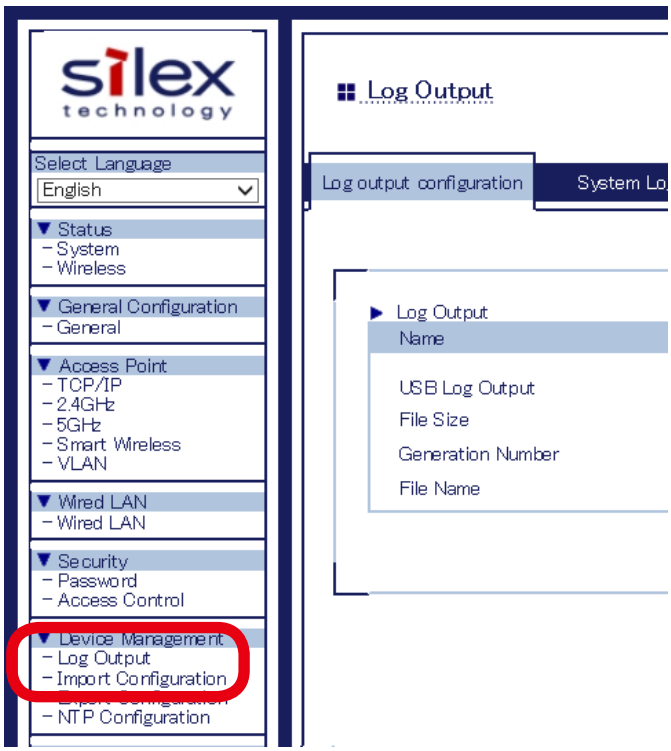
1. Log in to the Web page of AP-500AC using your Web browser.



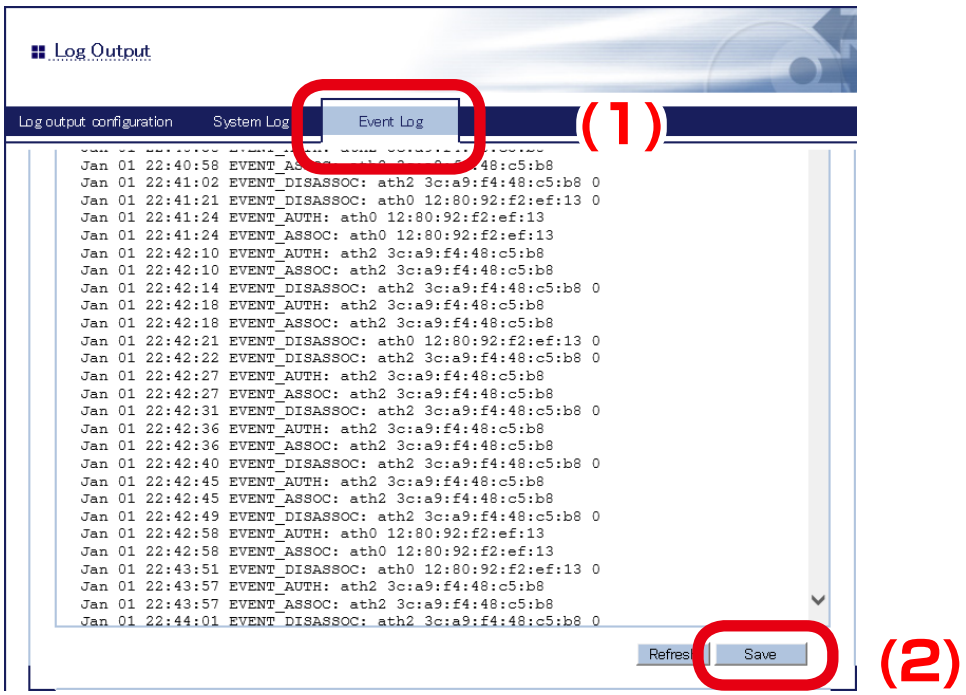
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

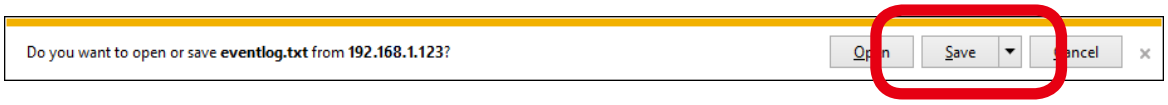
2. From the left menu on the Web page, click **Log Output**.



3. Click **Event Log** to display the event log.
Click **Save** to save the event log.



4. When the message appears to confirm where to save the event log file, click **Save**.

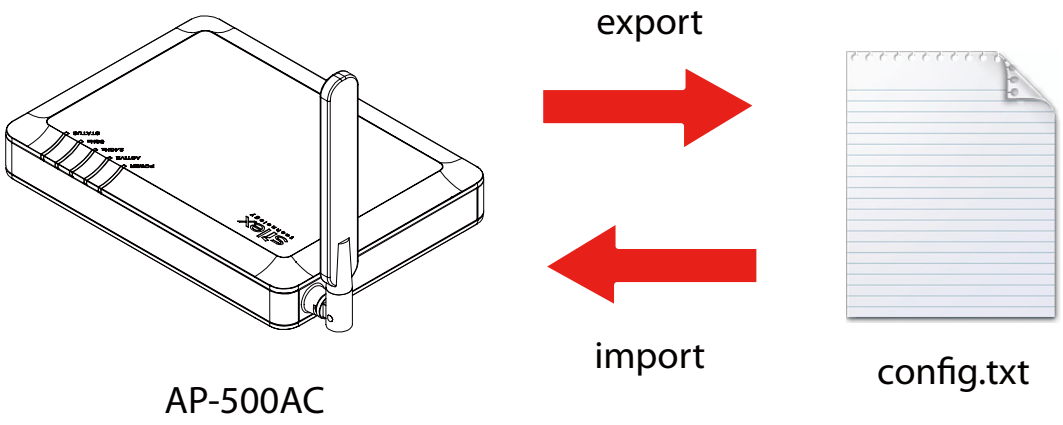


Note

- If ▼ is clicked, **Save as** option can be selected.

5-10. Configuration Import/Export

By exporting the configuration, the current settings can be saved on to an external device. Once the configuration is saved, it can be imported back to AP-500AC anytime to restore the settings.



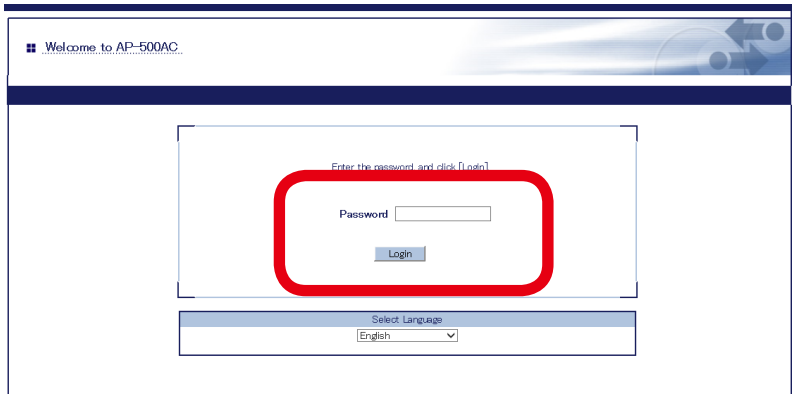
TIP

- The configuration file you can import to AP-500AC must be the one you had exported from AP-500AC.
- After the configuration file is exported, please do not change the file name as well as edit the information. If the file is altered, you may not be able to import.
- If there are differences in firmware versions on AP-500AC between the one exporting the configuration file and the one importing the configuration file, the file may not be imported correctly.

Configuration Export

How to export configuration is explained.

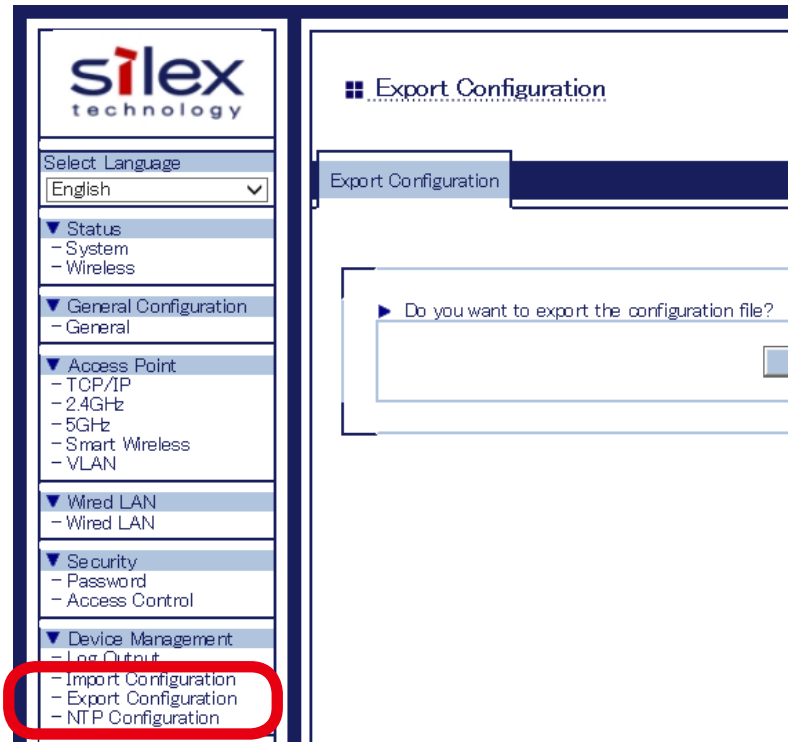
1. Log in to the Web page of AP-500AC using your Web browser.



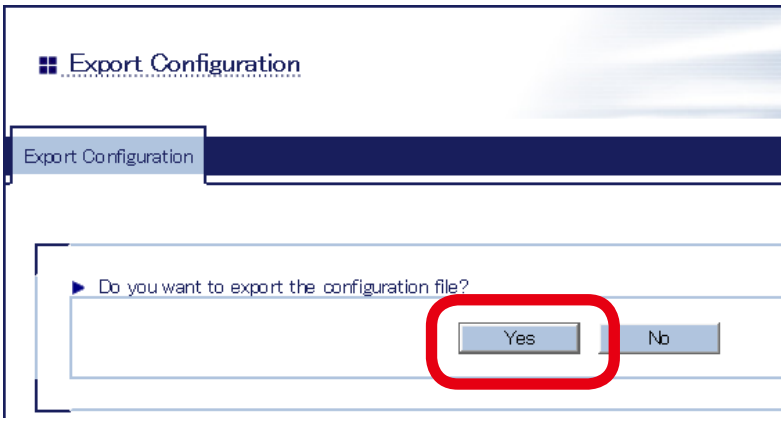
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu on the Web page, click **Export Configuration**



3. In the **Export Configuration** page, click **Yes**.



4. A message dialog to confirm where to save the configuration file (**config.txt**) is displayed. Click **Save**.

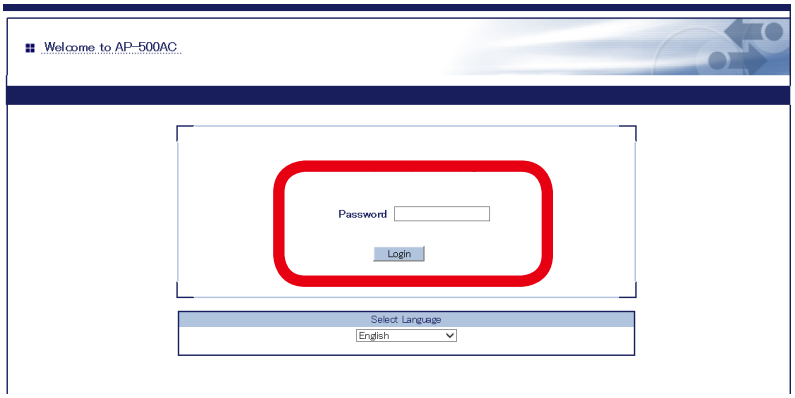
Note

- By clicking ▼, you can select **Save as** option.

Configuration Import

How to import configuration is explained.

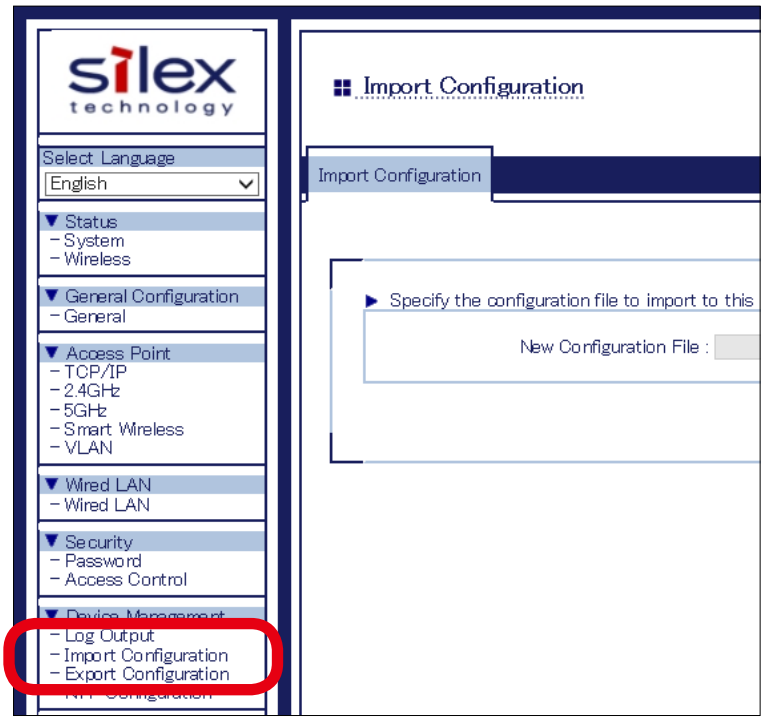
1. Log in to the Web page of AP-500AC using your Web browser.



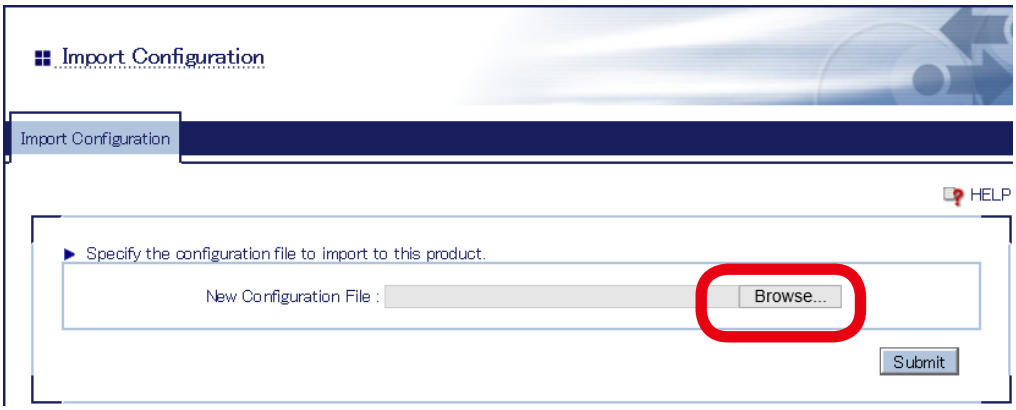
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

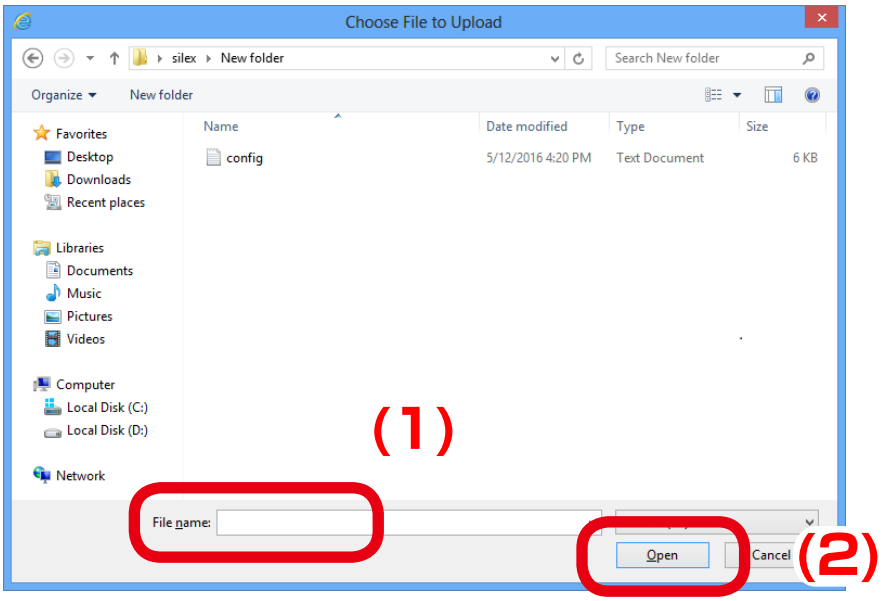
2. From the left menu on the Web page, click **Import Configuration**.



3. In the **Import Configuration** page, click **Browse**.



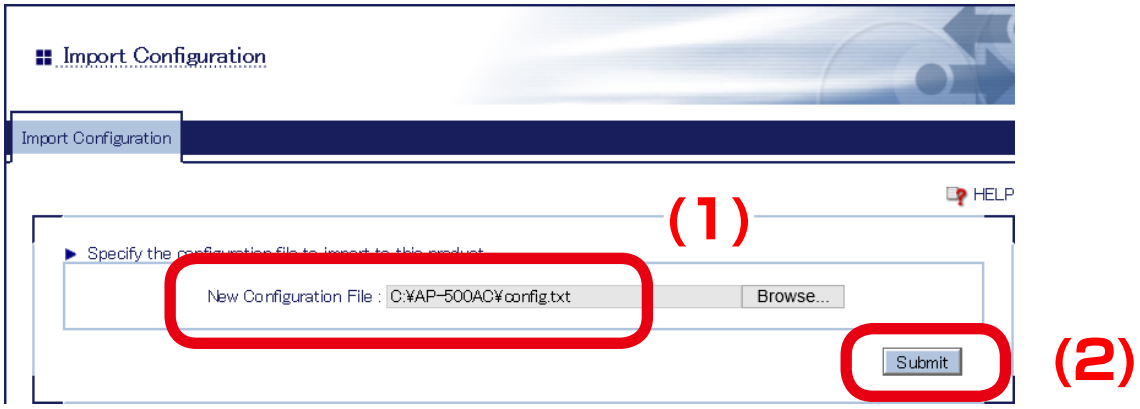
4. A window to select the configuration file (**config.txt**) is displayed.
Select the file to upload and click **Open**.



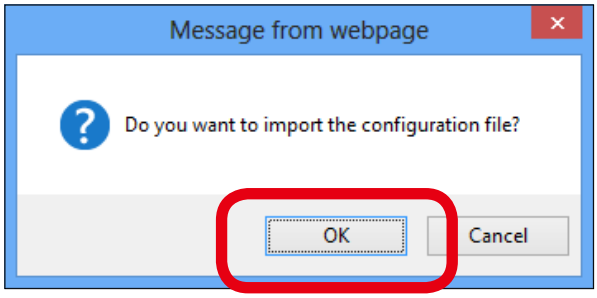
TIP

- The configuration file you can import to AP-500AC must be the one you had exported from AP-500AC.

5. In the **Import Configuration** page, check the configuration file you have selected is displayed at the **New Configuration File** field. Click **Submit**.

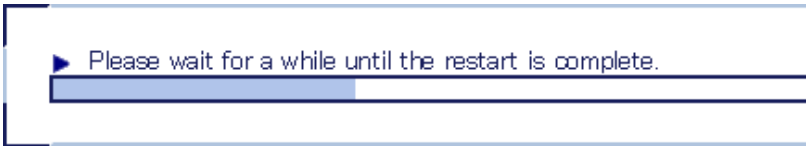


6. Click **OK** in a confirmation message.



7. When finished, click **Restart**.

8. After the **Restart** button is clicked, the progress bar is displayed. When the progress bar reaches the right end, the restart is completed.



5-11. Maintenance Feature

Restarting

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

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

Note - When receiving power over the Ethernet (PoE), unplug the network cable from the HUB.

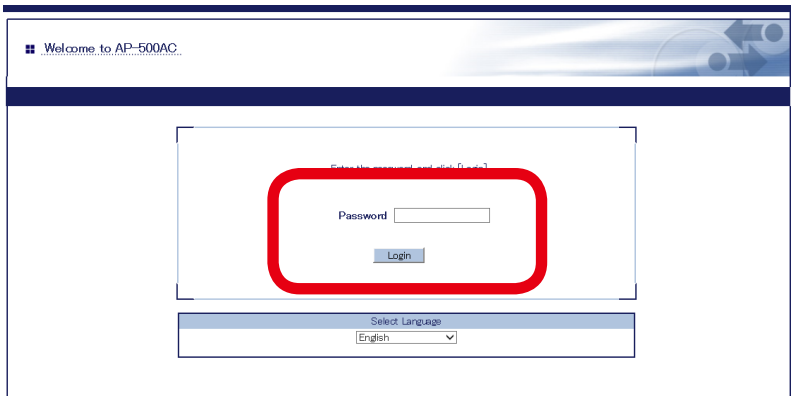
2. Plug the AC adaptor back into the outlet.

Note - When receiving power over the Ethernet (PoE), plug the network cable back into the HUB.

3. When ACTIVE LED starts blinking in Green and then turns to Green, the restart is completed.

How to restart AP-500AC using the Web Page:

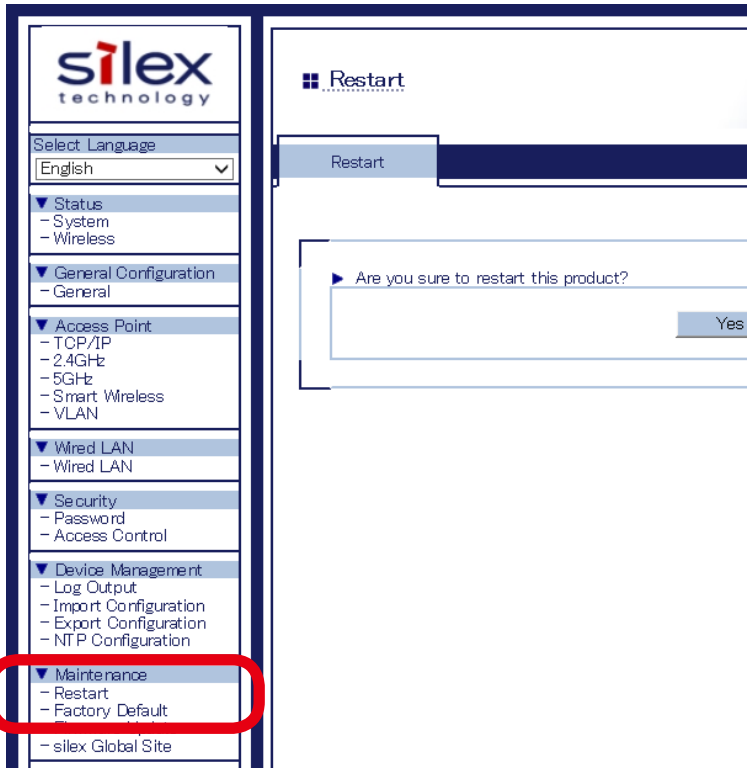
1. Log in to the Web page of AP-500AC using your Web browser.



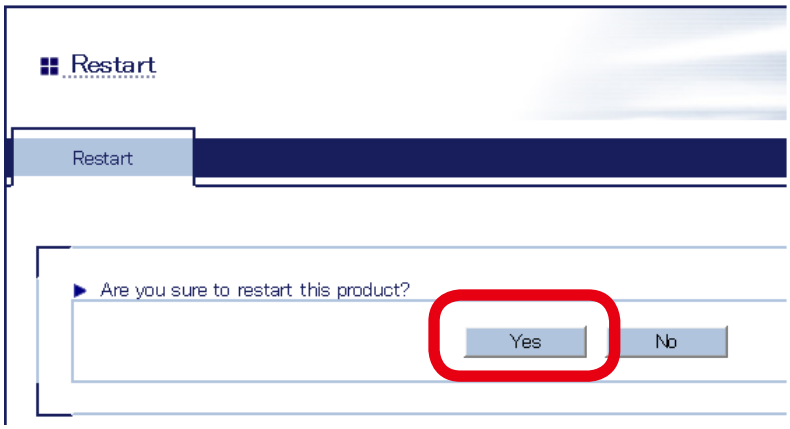
Note

- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

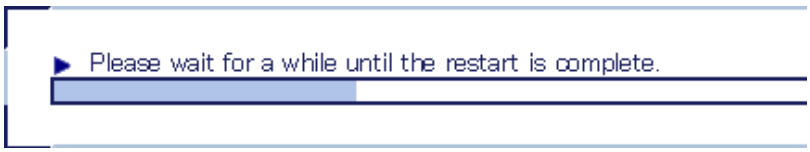
2. From the left menu on the Web page, click **Maintenance** - **Restart**.



3. In the page displayed, click **Yes**.



4. After **Yes** is clicked, the progress bar is displayed. When the progress bar reaches the right end, the restart is completed.



Factory Default Configuration

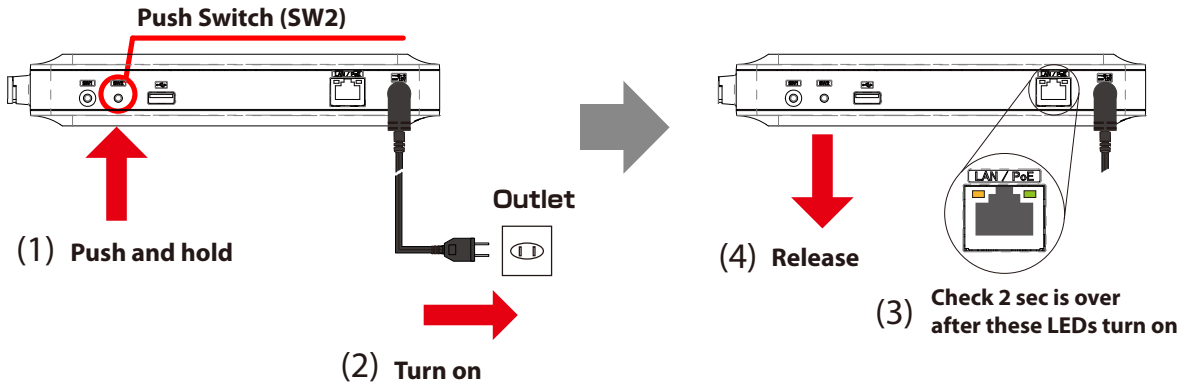
How to reset AP-500AC to factory defaults using the Push Switch:

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

Note

- When receiving power over the Ethernet (PoE), unplug the network cable from the HUB.

2. Press and hold the push switch (SW2) on AP-500AC while inserting the AC plug back into the electrical outlet. Release the push switch in 2 sec or more after the Link LED and Status LED turned on.



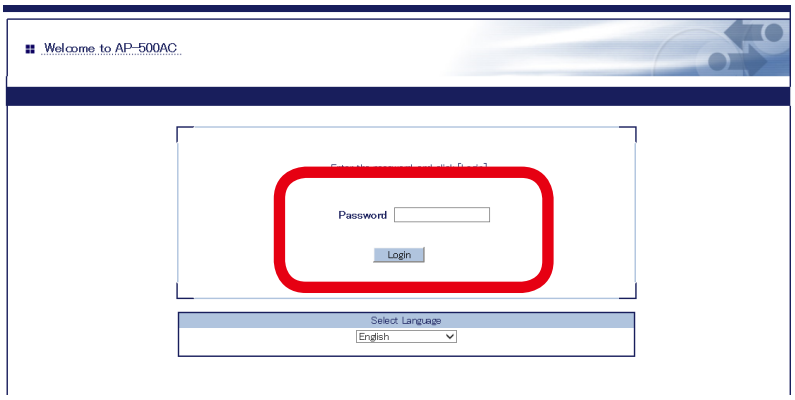
Note

- When receiving power over the Ethernet (PoE), press and hold the push switch (SET1) on AP-500AC while inserting the network cable back into the HUB.

3. When the factory default configuration is completed, AP-500AC is restarted automatically. When ACTIVE LED starts blinking in Green and then turns to Green, restart is completed.

How to reset AP-500AC to factory defaults using the Web page:

1. Log in to the Web page of AP-500AC using your Web browser.

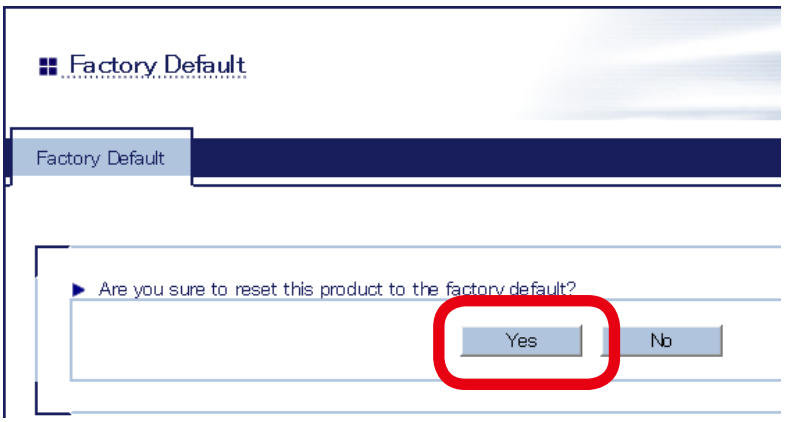


Note

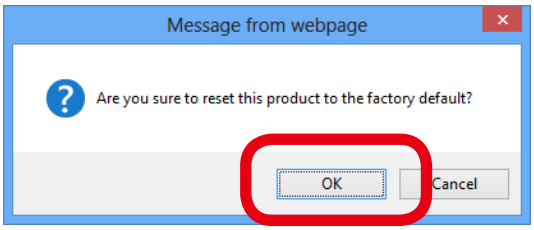
- For how to display the Web page after the initial configuration, refer to **3-2. Displaying Web Page of AP-500AC (After Initial Configuration)**.

2. From the left menu on the Web page, click **Maintenance** - **Factory Default**.

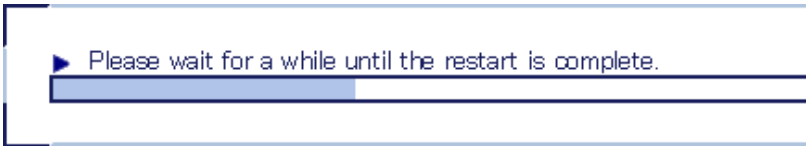
3. In the page displayed, click **Yes**.



4. When a confirmation message is displayed, click **OK**.



5. When the progress bar reaches the right end, the factory default configuration is completed.



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 AP-500AC, refer to the firmware update procedure sheet file contained in the firmware file you download.

Note

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

How to download the firmware file:

1. Access our website below.

URL	
USA	**http://www.silexamerica.com/**
Europe	**http://www.silexeurope.com/**

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

5-12. Product Search Utility

How to install and use the product search utility, "AMC Finder" is explained.

Downloading & Installing the Product Search Utility

How to download the product search utility:

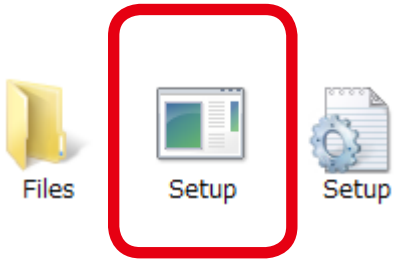
1. Access our website below.

URL	
USA	**http://www.silexamerica.com/**
Europe	**http://www.silexeurope.com/**

2. Go to the support section and download AMC-Finder.

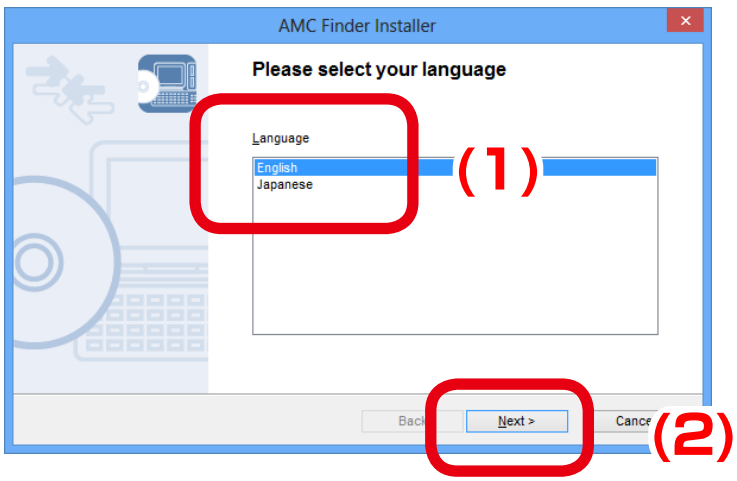
How to install the product search utility:

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

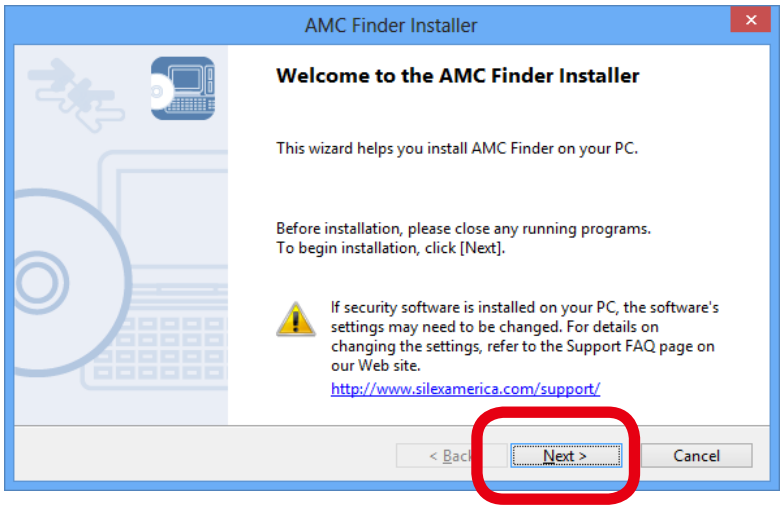


2. The User Account Control message is displayed, click **Yes**.

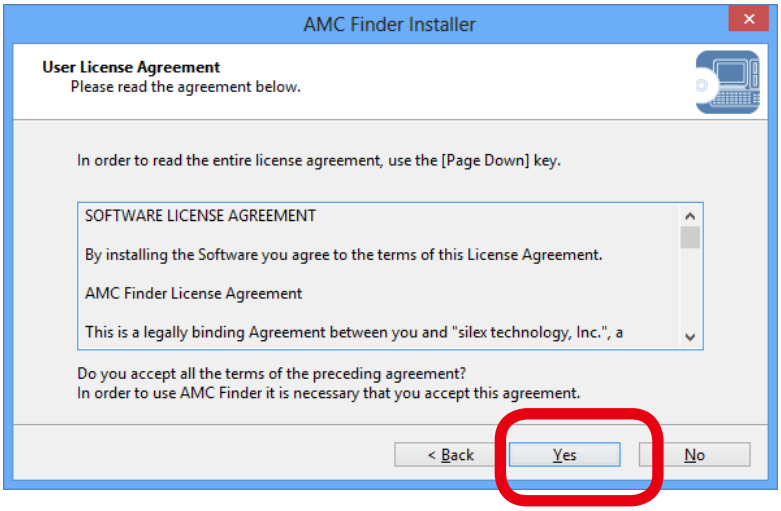
3. AMC Finder installer is started and the language selection menu is displayed. Select **English** and click **Next**.



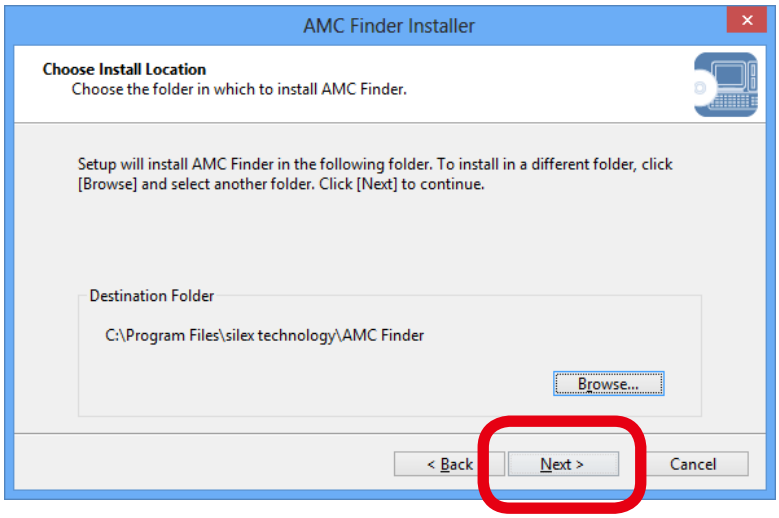
4. Click **Next**.



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



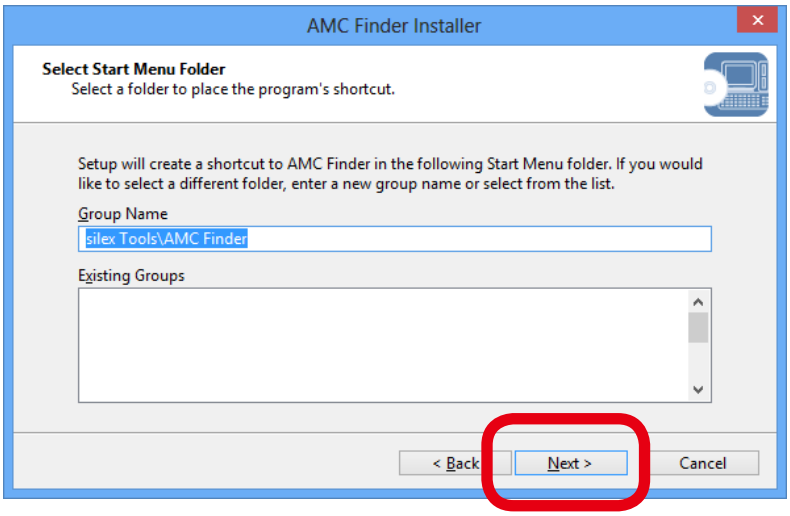
6. Select a folder to install into and click **Next**.



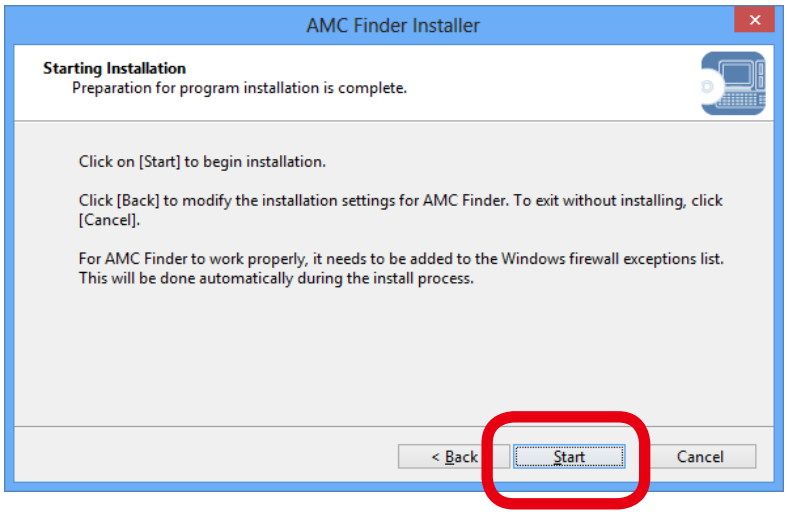
Note

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

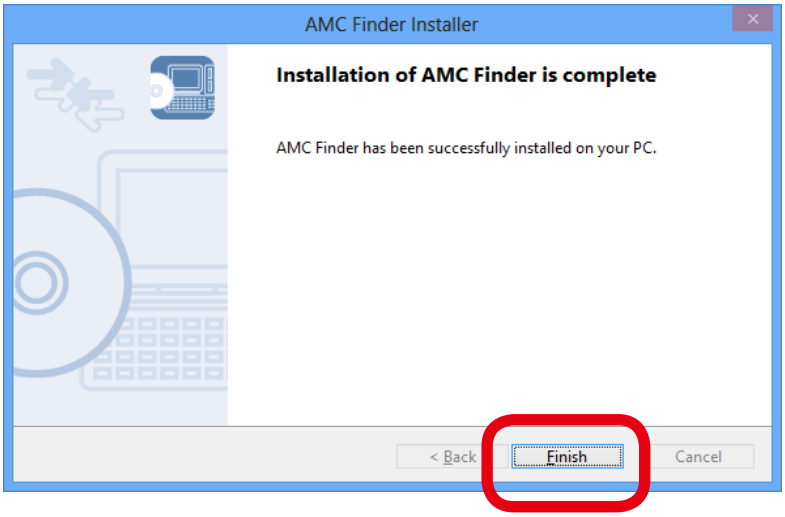
7. Enter a group name to be displayed in the start menu and click **Next**.



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



9. AMC Finder has been installed. Click **Finish**.



Using Product Search Utility

The product search utility, "AMC Finder" displays a list of AP-500AC running on a network. If AMC Finder is used, the Web page can be opened easily.

TIP

- The PC used for this configuration needs to have a proper IP address to communicate with AP-500AC. If you fail to access the Web page of AP-500AC, check the IP address of the PC first. If the IP address is not correct, configure a correct address.
(Example: If the IP address of AP-500AC is "192.168.20.123", the PC must have the address such as "192.168.20.1" which is not used by other network devices.)

Following Web browsers are recommended:

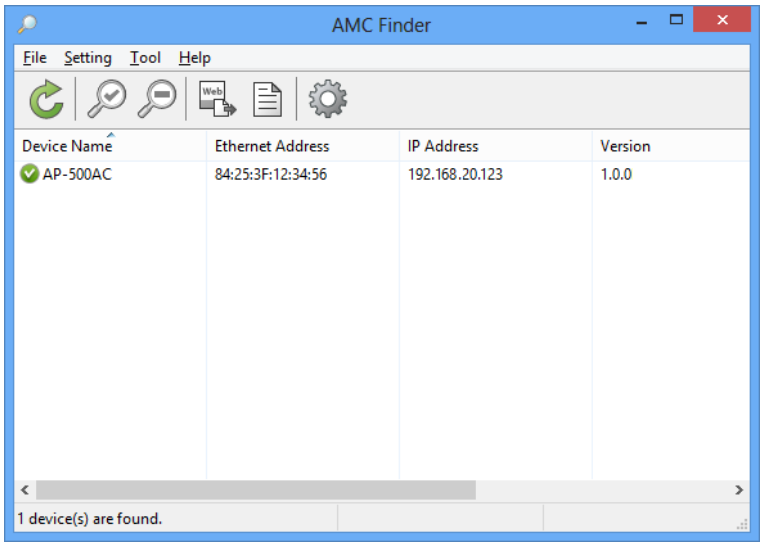
- Microsoft Internet Explorer 5.5 or newer
- Firefox 2.0.0 or newer

Note

- They may vary depending on the version of operating systems or Web browsers.

How to search for AP-500AC:

Start AMC Finder. AP-500AC running on the network will be displayed.

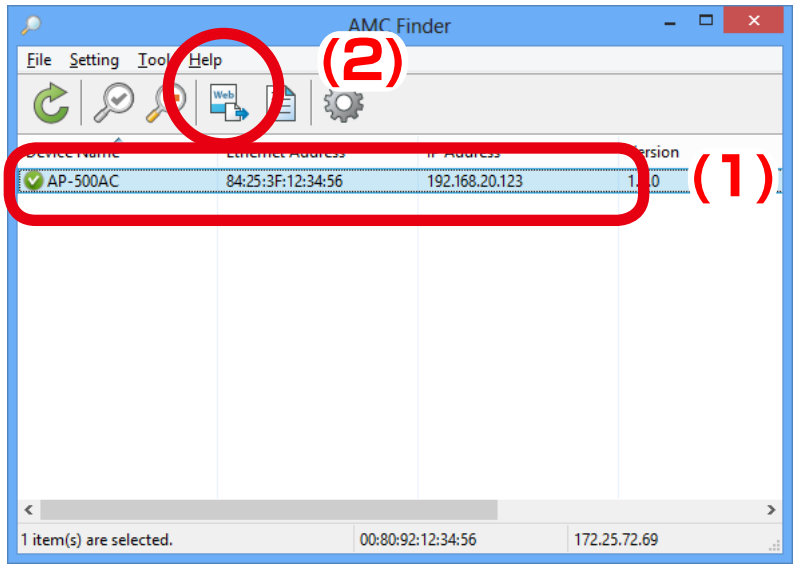


Note

- If AP-500AC is not displayed in the list, click **Refresh**  .

How to access the Web page:

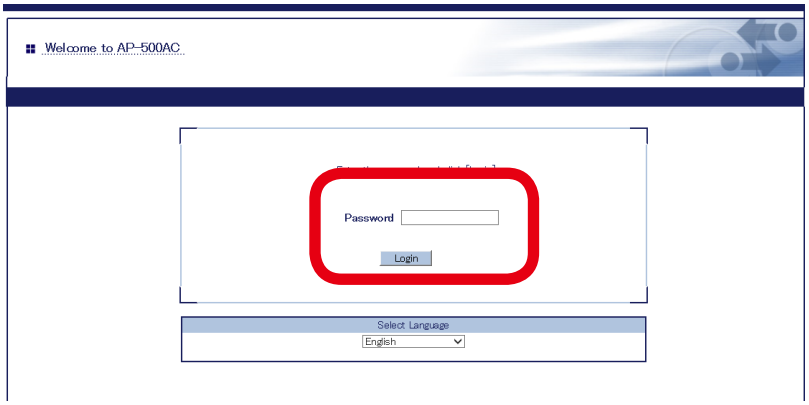
1. Select AP-500AC to configure and click **Configure using Web browser**.



Note

- If two or more of AP-500AC are displayed, select the correct one by checking the IP address and MAC address.

2. The Web browser runs and the login menu for AP-500AC is displayed.
Enter the password and click **Login**.



Note

- No password is set by default. In such case, just click **Login**.

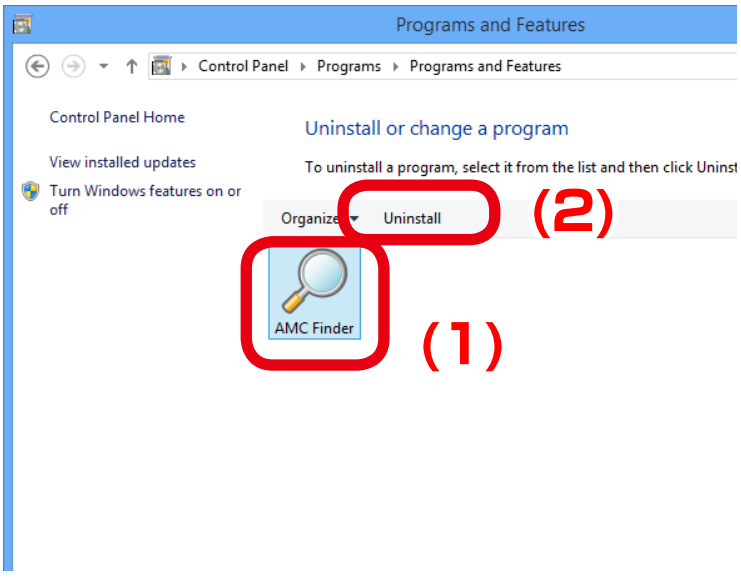
Uninstalling the Product Search Utility

How to uninstall the product search utility, "AMC Finder" is explained.
If AMC Finder is not necessary, you can uninstall it by following the instructions below.

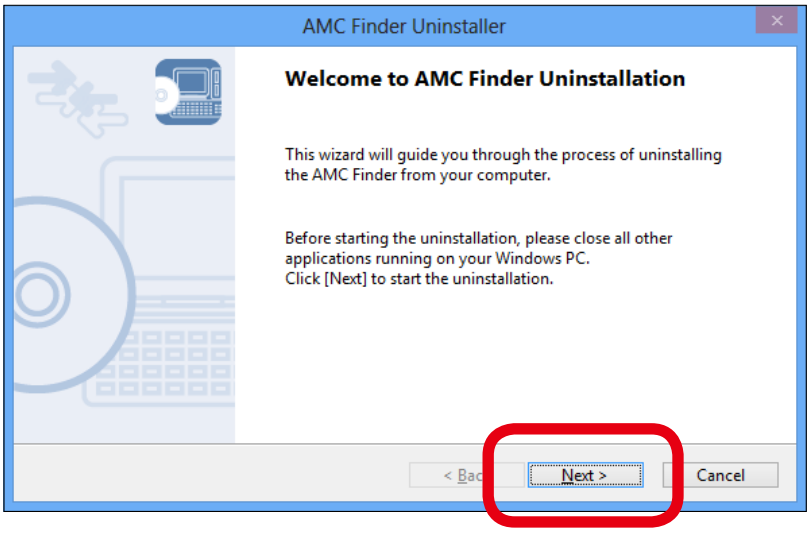
> **TIP**
> - To uninstall AMC Finder, administrator privilege is required.

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

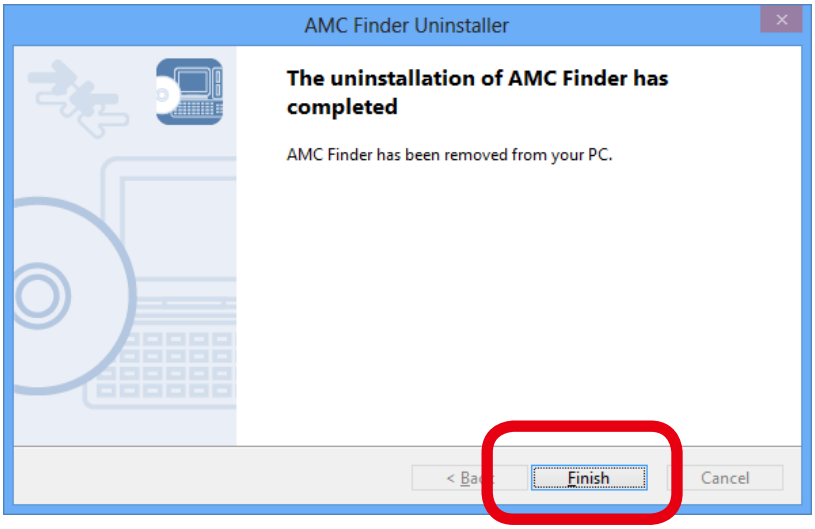
2. Select **AMC Finder** from the list and click **Uninstall**.



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



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



A. Appendix

A-1. List of All Settings

This chapter explains each configuration item available on AP-500AC. Some items can be configured only from the Detail Configuration page. For details, see explanation of each configuration item below.

General Configuration - Device Configuration

Host Name			
		General Configuration	*
		Detail Configuration	-
Details	Set the host name. Be sure to use a unique name that is not used by other devices.		
Range	Up to 15 characters		
Default Value	AP-500-xxxxxx (xxxxxx is a last 6-digit of the Ethernet Address)		

TCP/IP Configuration - TCP/IP Configuration

DHCP Client			
		General Configuration	*
		Detail Configuration	*
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	DISABLE		

IP Address			
		General Configuration	*
		Detail Configuration	*
Details	Set the IP address. When DHCP client is enabled, the IP Address obtained from DHCP server will be applied.		
Range	0.0.0.0 - 255.255.255.255		
Default Value	The default value can be found on the product label (see the bottom of the unit).		

Subnet Mask			
		General Configuration	*
		Detail Configuration	*
Details	Set the subnet mask. When DHCP client is enabled, the Subnet Mask obtained from DHCP server will be applied.		
Range	0.0.0.0 - 255.255.255.255		
Default Value	255.0.0.0		
Note	When set to "0.0.0.0", a subnet mask appropriate for the IP address is automatically assigned.		

Default Gateway			
		General Configuration	*
		Detail Configuration	*
Details	Set the gateway address. If "0.0.0.0" is set, this setting is disabled. When DHCP client is enabled, the Default Gateway obtained from DHCP server will be applied.		
Range	0.0.0.0 - 255.255.255.255		
Default Value	0.0.0.0		

TCP/IP Configuration - DNS Configuration

DNS Server (Primary)

General Configuration	-
Detail Configuration	*

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

DNS Server (Secondary)

General Configuration	-
Detail Configuration	*

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

TCP/IP Configuration - DHCP Server Configuration

DHCP Server Function

General Configuration	*
Detail Configuration	*

Details	Enable/Disable the DHCP server function. Select **ENABLE** to run AP-500AC as a DHCP server to automatically assign an IP address to the PC. Select **DISABLE** if you already have a DHCP server on the network.
Range	ENABLE/DISABLE
Default Value	DISABLE

Start IP Address

General Configuration	*
Detail Configuration	*

Details	Set the start IP address used for DHCP server function to assign the address. The value must be 4 numbers separated by dots and expressed in the format [xxx.xxx.xxx.xxx].
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0

End IP Address

General Configuration	*
Detail Configuration	*

Details	Set the end IP address used for DHCP server function to assign the address. The value must be 4 numbers separated by dots and expressed in the format [xxx.xxx.xxx.xxx].
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0

TCP/IP Configuration - DHCP Server Configuration

Subnet Mask

General Configuration	*	
Detail Configuration	*	

Details	Set the subnet mask for IP addresses to be assigned. The value must be 4 numbers separated by dots and expressed in the format [xxx.xxx.xxx.xxx].
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0
Note	When set to "0.0.0.0", this setting is disabled and a subnet mask appropriate for the start IP address is automatically used.

Default Gateway

General Configuration	*	
Detail Configuration	*	

Details	Set the gateway address. The value must be 4 numbers separated by dots and expressed in the format [xxx.xxx.xxx.xxx].
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0
Note	When set to "0.0.0.0", this setting is disabled and default gateway address is not assigned by DHCP.

Lease Time

General Configuration	*	
Detail Configuration	*	

Details	Set the lease time. If this is set to 0 days + 0 hours + 0 mins, the lease period will be 10 days.
Range	0 days 0 hours 0 mins - 44 days 23 hours 59 mins
Default Value	0 days 0 hours 0 mins

DNS Server

General Configuration	*	
Detail Configuration	*	

Details	Set the DNS server address. The value must be 4 numbers separated by dots and expressed in the format [xxx.xxx.xxx.xxx].
Range	0.0.0.0 - 255.255.255.255
Default Value	0.0.0.0

Wireless LAN Configuration (2.4GHz) - Wireless LAN Common Configuration

Wireless Mode

General Configuration	*
Detail Configuration	*

Details	Select the IEEE 802.11wireless mode.
Range	802.11b, 802.11b/g, 802.11n/b/g
Default Value	802.11n/b/g
Note	802.11b : Uses IEEE802.11b. 802.11b/g : Uses IEEE802.11b or IEEE802.11g. 802.11n/b/g : Uses IEEE802.11n, IEEE802.11b or IEEE802.11g.

Channel Bandwidth

General Configuration	*
Detail Configuration	*

Details	Set the frequency bandwidth. This setting is necessary when using **802.11n/b/g**. In a wireless network, bandwidth is divided up so that more devices can communicate at a time. Each section of bandwidth is called a ' channel ' and each channel has a bandwidth of **20MHz**. If **40MHz** is selected, larger and faster data transmission can be realized.
Range	20MHz/40MHz
Default Value	20MHz
Note	40MHz (High speed) : Uses double bandwidth. Two neighboring bandwidths are combined together for high speed transmission. 20MHz (Standard) : Uses standard (single) bandwidth. If your network becomes unstable when using 40MHz, change it to 20MHz (Standard).

Channel

General Configuration	*
Detail Configuration	*

Details	Set the wireless channel. A channel is the divided frequency bandwidth. In a wireless network, bandwidth is divided up so that more devices can communicate at a time.
Range	(Japan) 1-13/AUTO (US/Canada) 1-11/AUTO (EU) 1-13/AUTO
Default Value	11
Note	If your network becomes unstable due to interference with other wireless devices, it could be improved by changing the channel. The channel you can use will differ depending on the country.

Ext Channel

General Configuration	*
Detail Configuration	*

Details	Set the extended channel when **40MHz** is selected for channel bandwidth. Available extended channels will differ depending on the channel.
Range	1-13
Default Value	Depending on the channel

Wireless LAN Configuration (2.4GHz) - Wireless LAN Basic Configuration 1-4

Interface		General Configuration	*
		Detail Configuration	*
Details	Enable/Disable the wireless LAN interface 1-4.		
Range	ENABLE/DISABLE		
Default Value	Wireless LAN1: ENABLE, Wireless LAN2-4: DISABLE		

SSID		General Configuration	*
		Detail Configuration	*
Details	Set the SSID of the wireless network. 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.		
Range	Up to 32 characters		
Default Value	Wireless LAN1: AP-500-xxxxxx-1-1 Wireless LAN2: AP-500-xxxxxx-1-2 Wireless LAN3: AP-500-xxxxxx-1-3 Wireless LAN4: AP-500-xxxxxx-1-4 (**xxxxxx** is the last 6 digits of the Ethernet Address)		

Stealth Mode		General Configuration	*
		Detail Configuration	*
Details	Enable/Disable the Stealth Mode.		
Range	ENABLE/DISABLE		
Default Value	DISABLE		
Note	If the Stealth Mode is enabled, the Smart Wireless Setup feature can no longer be used.		

Wireless LAN Configuration (2.4GHz) - Wireless LAN Basic Configuration 1-4

Network Authentication

General Configuration	*
Detail Configuration	*

Details	Select the network authentication mode that will be used to connect to your wireless devices. To ensure a secure network, it is recommended to use WPA/WPA2. When IEEE 802.11n is used or when WPA2 is used as authentication method, TKIP encryption cannot be used.
Range	Open, Shared, WPA-PSK, WPA2-PSK, WPA/WPA2-PSK, 802.1X, WPA-Enterprise, WPA2-Enterprise, WPA/WPA2-Enterprise
Default Value	Wireless LAN1 : WPA2-PSK Wireless LAN2-4: Open
Note	Open (Open System): Allows all access without authentication. For encryption mode, WEP can be used. Shared (Pre-Shared Key): Uses WEP key for encryption and allows access only from those with the same WEP key. For encryption mode, WEP can be used. WPA-PSK: Uses PSK for network authentication. For encryption mode, TKIP/AES/AUTO can be selected. The encryption key will be generated by communicating with your wireless devices using a Pre-Shared key. WEP key setting is not used for this mode. WPA2-PSK: Uses PSK for network authentication. For encryption mode, AES/AUTO can be selected. The encryption key will be generated by communicating with your wireless devices using a Pre-Shared key. WEP key setting is not used for this mode. WPA/WPA2-PSK: Uses both WPA-PSK and WPA2-PSK authentication. 802.1X: Uses IEEE 802.1X user authentication and WEP encryption. WPA-Enterprise: Uses IEEE 802.1X user authentication and TKIP/AES/AUTO encryption. WPA2-Enterprise: Uses IEEE 802.1X user authentication and AES/AUTO encryption. WPA/WPA2-Enterprise: Uses IEEE 802.1X user authentication and AES/AUTO encryption. When running in IEEE 802.11n, Shared and IEEE 802.1X authentication modes and WEP and TKIP encryption modes cannot be used.

Wireless LAN Configuration (2.4GHz) - WEP Configuration

WEP			
		General Configuration	*
		Detail Configuration	*
Details	Enable/Disable WEP encryption. If WEP encryption is used, wireless communication will be encrypted using the settings of **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			
		General Configuration	*
		Detail Configuration	*
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 devices.		
Range	1 - 4		
Default Value	1		

WEP Key1-4			
		General Configuration	*
		Detail Configuration	*
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 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.		

Wireless LAN Configuration (2.4GHz) - WPA/WPA2 Configuration

Encryption Mode

General Configuration	*
Detail Configuration	*

Details	Select the encryption mode to use for **WPA-PSK**, **WPA2-PSK**, **WPA/WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise**, **WPA/WPA2-Enterprise** authentication.
Range	TKIP/AES/AUTO
Default Value	AES
Note	When the network authentication mode is **WPA2-PSK**, **WPA/WPA2-PSK**, **WPA2-Enterprise**, **WPA/WPA2-Enterprise**, **TKIP** cannot be used. * The max number of connectable station devices will differ depending on the encryption mode used. - When using **AES** only: 100 units - When using **TKIP** or **AUTO**: 50 units * In Multi SSID environment, the number of connected devices will be the total number of devices connected on all wireless interfaces. Thus, the max number of connectable devices will differ depending on the encryption mode used on each interface. - When all wireless interfaces use **AES** only: 100 units - When one or some of the wireless interfaces use **TKIP** or **AUTO**: 50 units * When using the WDS feature, the Repeater AP connected to AP-500AC as client AP will consume one connection, while Root AP or Repeater APs connected to AP-500AC as host AP will NOT consume any connections.

Pre-Shared Key

General Configuration	*
Detail Configuration	*

Details	Set the Pre-Shared Key to use for TKIP/AES encryption. The Pre-Shared Key is a keyword used to create the encryption key. It is also referred to as ' network key ' or ' password '.
Range	8-63 alphanumeric characters 64 hexadecimal value
Default Value	The sequence of numbers generated by a particular rule based on the Ethernet Address. * The default value can be found on the product label (see the back of the unit).
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.

Group key renew interval

General Configuration	*
Detail Configuration	*

Details	Set the refresh interval for Pre-Shared Key (min). If 0 is set, this setting is disabled.
Range	0 - 1440
Default Value	60

Wireless LAN Configuration (2.4GHz) - RADIUS Server Configuration

Server IP

General Configuration		*
Detail Configuration		*
Details	Set the IP Address of RADIUS server. This needs to be set only when the network authentication is **802.1X**, **WPA-Enterprise**, **WPA2-Enterprise** or **WPA/WPA2-Enterprise**.	
Range	0.0.0.0 - 255.255.255.255	
Default Value	0.0.0.0	

Port Number

General Configuration		*
Detail Configuration		*
Details	Set the port number used to communicate with RADIUS server.	
Range	0 - 65535	
Default Value	1812	

Shared Secret

General Configuration		*
Detail Configuration		*
Details	Set the secret key used to communicate with RADIUS server.	
Range	Up to 64 characters	
Default Value	(None)	

Wireless LAN Configuration (2.4GHz) - WDS Configuration

WDS Mode

		General Configuration	*
		Detail Configuration	*
Details	Set the WDS operation mode to make communication between the Access Points. The WDS network consists of one Root AP (host) and plural Repeater APs (client).		
Range	DISABLE/Root AP/Repeater		
Default Value	DISABLE		
Note	DISABLE: Does not use WDS. RootAP: Runs as Root AP for WDS. This exchanges traffic among Repeater, wired LAN and wireless client device. Repeater: Runs as Repeater for WDS. This exchanges traffic among Root AP, Repeater, wired LAN and wireless client device by connecting to Root AP or Repeater.		

Wireless LAN Interface

		General Configuration	*
		Detail Configuration	*
Details	Select the wireless interface for WDS to make communication between the Access Points.		
Range	Wireless1-4		
Default Value	Wireless1		
Note	The MAC Address displayed under the Wireless Interface is the MAC Address of AP-500AC to use for WDS. This information will be used on Repeater AP which sets AP-500AC as a host AP.		

Access Point MAC Address

		General Configuration	*
		Detail Configuration	*
Details	Set the MAC Address for Root AP or Repeater AP to connect as host AP in WDS mode.		
Range	00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF		
Default Value	00:00:00:00:00:00		
Note	This setting is not necessary on Root AP. The MAC Address for Root AP or Repeater AP to connect as a host AP in WDS can be seen on the Web page of the host AP. Log in to the Web page of the host AP and click **2.4GHz** - **WDS Configuration** - **Wireless LAN Interface**. The MAC Address will be displayed under the **Wireless LAN Interface**.		

Wireless LAN Configuration (2.4GHz) - Extension Configuration

Beacon Interval(msec)

General Configuration	-
Detail Configuration	*

Details	Set the beacon transmission interval (millisec).
Range	20 - 1000
Default Value	100

DTIM

General Configuration	-
Detail Configuration	*

Details	Set the DTIM interval for a wireless LAN.
Range	1 - 255
Default Value	1

Transmit Power(%)

General Configuration	-
Detail Configuration	*

Details	Set the transmission strength level. When a lower strength level is selected, the radio transmission distance is shortened and the scope of search for AP-500AC will be narrowed down. By narrowing down the scope of search, the risk of interference to the other wireless networks could be reduced.
Range	5 - 100
Default Value	100

RTS Threshold

General Configuration	-
Detail Configuration	*

Details	Set the RTS threshold value.
Range	1 - 2346
Default Value	2346

Short Preamble

General Configuration	-
Detail Configuration	*

Details	Enable/Disable the Short Preamble (ON/OFF).
Range	ON/OFF
Default Value	ON
Note	This can be set only when the Wireless Mode is **802.11b** or **802.11b/g**.

A-MPDU

General Configuration	-
Detail Configuration	*

Details	Enable/Disable the A-MPDU (ON/OFF). If this is enabled (ON), higher throughput could be achieved.
Range	ON/OFF
Default Value	ON
Note	This can be set only when the Wireless Mode is **802.11n/b/g**.

Short Guard Interval

General Configuration	-
Detail Configuration	*

Details	Enable/Disable the Short Guard Interval (ON/OFF). If this is enabled (ON), higher throughput could be achieved.
Range	ON/OFF
Default Value	ON
Note	This can be set only when all of the following conditions are met: - Wireless Mode is set to **802.11n/b/g** - Channel bandwidth is set to **40MHz**.

Wireless LAN Configuration (2.4GHz) - QoS(WMM) Configuration (for AP)

BE	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for BE(Best Effort) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax:1 - 15 AIFSN:1 - 15 TxOPLimit: 0 - 8192	
Default Value	ECWmin: 4 ECWmax: 6 AIFSN: 3 TxOPLimit: 0	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

BK	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for (BK: Back Ground) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192	
Default Value	ECWmin: 4 ECWmax: 10 AIFSN: 7 TxOPLimit: 0	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

VI	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for (VI: Video) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192	
Default Value	ECWmin: 3 ECWmax: 4 AIFSN: 1 TxOPLimit: 3008	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

Wireless LAN Configuration (2.4GHz) - QoS(WMM) Configuration (for AP)

VO	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for (VO: Voice) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192	
Default Value	ECWmin: 2 ECWmax: 3 AIFSN: 1 TxOPLimit: 1504	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

Wireless LAN Configuration (2.4GHz) - QoS(WMM) Configuration (for Station)

BE	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for (BE: Best Effort) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192 ACM: ON/OFF	
Default Value	ECWmin: 4 ECWmax: 10 AIFSN: 3 TxOPLimit: 0 ACM: OFF	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

Wireless LAN Configuration (2.4GHz) - QoS(WMM) Configuration (for Station)

BK	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for (BK: Back Ground) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192 ACM: ON/OFF	
Default Value	ECWmin: 4 ECWmax: 10 AIFSN: 7 TxOPLimit: 0 ACM: OFF	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

VI	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for (VI: Video) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192 ACM: ON/OFF	
Default Value	ECWmin: 3 ECWmax: 4 AIFSN: 2 TxOPLimit: 3008 ACM: OFF	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

VO	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for (VO: Voice) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192 ACM: ON/OFF	
Default Value	ECWmin: 2 ECWmax: 3 AIFSN: 2 TxOPLimit: 1504 ACM: OFF	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

Wireless LAN Configuration (5GHz) - Wireless LAN Common Configuration

Wireless Mode

General Configuration	*
Detail Configuration	*

Details	Select the IEEE 802.11wireless mode.
Range	802.11a, 802.11n/a, 802.11ac
Default Value	802.11ac
Note	802.11a : Uses IEEE802.11a. 802.11n/a : Uses IEEE802.11n or IEEE802.11a. 802.11ac : Uses IEEE802.11ac.

Channel Bandwidth

General Configuration	*
Detail Configuration	*

Details	Set the frequency bandwidth. This setting is necessary when using **802.11n/a** or **802.11ac**. In a wireless network, bandwidth is divided up so that more devices can communicate at a time. Each section of bandwidth is called a ' channel ' and each channel has a bandwidth of **20MHz**. If **40MHz** or **80MHz** is selected, larger and faster data transmission can be realized.
Range	20MHz/40MHz/80MHz
Default Value	20MHz
Note	80MHz(Super speed) : Uses four bandwidth. Four adjacent 20MHz bandwidths are combined together for high speed transmission. Even faster than 40MHz. 40MHz (High speed) : Uses double bandwidth. Two adjacent 20MHz bandwidths are combined together for high speed transmission. 20MHz (Standard) : Uses standard (single) bandwidth. If your network becomes unstable when using 40MHz/80MHz, change it to 20MHz (Standard).

Channel

General Configuration	*
Detail Configuration	*

Details	Set the wireless channel. A channel is the divided frequency bandwidth. In a wireless network, bandwidth is divided up so that more devices can communicate at a time.
Range	(Japan) 36/40/44/48/52/56/60/64/ 100/104/108/112/116/120/ 124/128/132/136/140/AUTO (US/Canada) 36/40/44/48/52/56/60/64/ 149/153/157/161/165/AUTO (EU) 36/40/44/48/52/56/60/64/ 100/104/108/112/116/120/124/128/132/136/140/AUTO
Default Value	36
Note	If your network becomes unstable due to interference with other wireless devices, it could be improved by changing the channel. The channel you can use will differ depending on the country. If W53 or W56 channels are used when AP-500AC is turned on or a particular radar is detected, wireless communication is lost for certain period of time (*). (*) The time duration differs depending on the country.

Wireless LAN Configuration (5GHz) - Wireless LAN Common Configuration

Ext Channel

		General Configuration	*
		Detail Configuration	*
Details	Set the extended channel when 40MHz is selected for channel bandwidth. Available extended channels will differ depending on the channel.		
Range	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140		
Default Value	Depending on the channel		

DFS Primary Channel

		General Configuration	-
		Detail Configuration	*
Details	Set the alternative channel used when radar signals are detected during DFS channels are used. If the alternative channel is not specified or radar signal is detected even for that channel, the channel is switched in a certain regulated order. For details on DFS channel switch, refer to **2-6. Wireless Interference Information** - **DFS**.		
Range	NONE/52/56/60/64/ 100/104/108/112/116/120/124/128/132/136/140		
Default Value	None		
Note	When DFS is running on all of channels, AP-500AC will switch the channel in approximately 30 min, from the one specified previously to the other. While the channel switch is in process, 5GHz LED (Red) will turn on.		

Wireless LAN Configuration (5GHz) - Wireless LAN Basic Configuration 5-8

Interface

		General Configuration	*
		Detail Configuration	*
Details	Enable/Disable the wireless LAN interface 5-8.		
Range	ENABLE/DISABLE		
Default Value	Wireless LAN5: ENABLE, Wireless LAN6-8: DISABLE		

SSID

		General Configuration	*
		Detail Configuration	*
Details	Set the SSID of the wireless network. 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.		
Range	Up to 32 characters		
Default Value	Wireless LAN5: AP-500-xxxxxx-2-1 Wireless LAN6: AP-500-xxxxxx-2-2 Wireless LAN7: AP-500-xxxxxx-2-3 Wireless LAN8: AP-500-xxxxxx-2-4 (**xxxxxx** is the last 6 digits of the Ethernet Address)		

Stealth Mode

		General Configuration	*
		Detail Configuration	*
Details	Enable/Disable the Stealth Mode.		
Range	ENABLE/DISABLE		
Default Value	DISABLE		
Note	If the Stealth Mode is enabled, the Smart Wireless Setup feature can no longer be used.		

Wireless LAN Configuration (5GHz) - Wireless LAN Basic Configuration 5-8

Network Authentication

General Configuration	*
Detail Configuration	*

Details	Select the network authentication mode that will be used to connect to your wireless devices. To ensure a secure network, it is recommended to use WPA/WPA2. When IEEE 802.11n or IEEE 802.11ac is used or when WPA2 is used as authentication method, TKIP encryption cannot be used.
Range	Open, Shared, WPA-PSK, WPA2-PSK, WPA/WPA2-PSK, 802.1X, WPA-Enterprise, WPA2-Enterprise, WPA/WPA2-Enterprise
Default Value	Wireless LAN5 : WPA2-PSK Wireless LAN6-8 : Open
Note	Open (Open System): Allows all access without authentication. For encryption mode, WEP can be used. Shared (Pre-Shared Key): Uses WEP key for encryption and allows access only from those with the same WEP key. For encryption mode, WEP can be used. WPA-PSK: Uses PSK for network authentication. For encryption mode, TKIP/AES/AUTO can be selected. The encryption key will be generated by communicating with your wireless devices using a Pre-Shared key. WEP key setting is not used for this mode. WPA2-PSK: Uses PSK for network authentication. For encryption mode, AES/AUTO can be selected. The encryption key will be generated by communicating with your wireless devices using a Pre-Shared key. WEP key setting is not used for this mode. WPA/WPA2-PSK: Uses both WPA-PSK and WPA2-PSK authentication. 802.1X: Uses IEEE 802.1X user authentication and WEP encryption. WPA-Enterprise: Uses IEEE 802.1X user authentication and TKIP/AES/AUTO encryption. WPA2-Enterprise: Uses IEEE 802.1X user authentication and AES/AUTO encryption. WPA/WPA2-Enterprise: Uses IEEE 802.1X user authentication and AES/AUTO encryption. When running in IEEE 802.11n or IEEE 802.11ac, it is impossible to use Shared and IEEE 802.1X authentication modes and WEP and TKIP encryption modes.

Wireless LAN Configuration (5GHz) - WEP Configuration

WEP

General Configuration	*
Detail Configuration	*

Details	Enable/Disable WEP encryption. If WEP encryption is used, wireless communication will be encrypted using the settings of **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

General Configuration	*
Detail Configuration	*

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 devices.
Range	1 - 4
Default Value	1

WEP Key1-4

General Configuration	*
Detail Configuration	*

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 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.

Wireless LAN Configuration (5GHz) - WPA/WPA2 Configuration

Encryption Mode

General Configuration	*
Detail Configuration	*

Details	Select the encryption mode to use for **WPA-PSK**, **WPA2-PSK**, **WPA/WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise**, **WPA/WPA2-Enterprise** authentication.
Range	TKIP/AES/AUTO
Default Value	AES
Note	When the network authentication mode is **WPA2-PSK**, **WPA/WPA2-PSK**, **WPA2-Enterprise**, **WPA/WPA2-Enterprise**, **TKIP** cannot be used. * The max number of connectable station devices will differ depending on the encryption mode used. - When using **AES** only: 100 units - When using **TKIP** or **AUTO**: 50 units * In Multi SSID environment, the number of connected devices will be the total number of devices connected on all wireless interfaces. Thus, the max number of connectable devices will differ depending on the encryption mode used on each interface. - When all wireless interfaces use **AES** only: 100 units - When one or some of the wireless interfaces use **TKIP** or **AUTO**: 50 units * When using the WDS feature, the Repeater AP connected to AP-500AC as client AP will consume one connection, while Root AP or Repeater APs connected to AP-500AC as host AP will NOT consume any connections.

Pre-Shared Key

General Configuration	*
Detail Configuration	*

Details	Set the Pre-Shared Key to use for TKIP/AES encryption. The Pre-Shared Key is a keyword used to create the encryption key. It is also referred to as ' network key ' or ' password '.
Range	8-63 alphanumeric characters 64 hexadecimal value
Default Value	The sequence of numbers generated by a particular rule based on the Ethernet Address. * The default value can be found on the product label (see the back of the unit).
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.

Group key renew interval

General Configuration	*
Detail Configuration	*

Details	Set the refresh interval for Pre-Shared Key (min). If 0 is set, this setting is disabled.
Range	0 - 1440
Default Value	60

Wireless LAN Configuration (5GHz) - RADIUS Server Configuration

Server IP

		General Configuration	*
		Detail Configuration	*
Details	Set the IP Address of RADIUS server. This needs to be set only when the network authentication is **802.1X**, **WPA-Enterprise**, **WPA2-Enterprise** or **WPA/WPA2-Enterprise**.		
Range	0.0.0.0 - 255.255.255.255		
Default Value	0.0.0.0		

Port Number

		General Configuration	*
		Detail Configuration	*
Details	Set the port number used to communicate with RADIUS server.		
Range	0 - 65535		
Default Value	1812		

Shared Secret

		General Configuration	*
		Detail Configuration	*
Details	Set the secret key used to communicate with RADIUS server.		
Range	Up to 64 characters		
Default Value	(None)		

Wireless LAN Configuration (5GHz) - WDS Configuration

WDS Mode

General Configuration	*
Detail Configuration	*

Details	Set the WDS operation mode to make communication between the Access Points. The WDS network consists of one Root AP (host) and plural Repeater APs (client).
Range	DISABLE/Root AP/Repeater
Default Value	DISABLE
Note	DISABLE: Does not use WDS. Root AP: Runs as Root AP for WDS. This exchanges traffic among Repeater, wired LAN and wireless client device. Repeater: Runs as Repeater for WDS. This exchanges traffic among Root AP, Repeater, wired LAN and wireless client device by connecting to Root AP or Repeater.

Wireless LAN Interface

General Configuration	*
Detail Configuration	*

Details	Select the wireless interface for WDS to make communication between the Access Points.
Range	Wireless5-8
Default Value	Wireless5
Note	The MAC Address displayed under the Wireless Interface is the MAC Address of AP-500AC to use for WDS. This information will be used on Repeater AP which sets AP-500AC as a host AP.

Access Point MAC Address

General Configuration	*
Detail Configuration	*

Details	Set the MAC Address for Root AP or Repeater AP to connect as host AP in WDS mode.
Range	00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF
Default Value	00:00:00:00:00:00
Note	This setting is not necessary on Root AP. The MAC Address for Root AP or Repeater AP to connect as a host AP in WDS can be seen on the Web page of the host AP. Log in to the Web page of the host AP and click **5GHz** - **WDS Configuration** - **Wireless LAN Interface**. The MAC Address will be displayed under the **Wireless LAN Interface**.

Wireless LAN Configuration (5GHz) - Extension Configuration

Beacon Interval(msec)

General Configuration	-
Detail Configuration	*

Details	Set the beacon transmission interval (millisec).
Range	20 - 1000
Default Value	100

DTIM

General Configuration	-
Detail Configuration	*

Details	Set the DTIM interval for a wireless LAN.
Range	1 - 255
Default Value	1

Transmit Power(%)

General Configuration	-
Detail Configuration	*

Details	Set the transmission strength level. When a lower strength level is selected, the radio transmission distance is shortened and the scope of search for AP-500AC will be narrowed down. By narrowing down the scope of search, the risk of interference to the other wireless networks could be reduced.
Range	5 - 100
Default Value	100

RTS Threshold

General Configuration	-
Detail Configuration	*

Details	Set the RTS threshold value.
Range	1 - 2346
Default Value	2346

A-MPDU

General Configuration	-
Detail Configuration	*

Details	Enable/Disable the A-MPDU (ON/OFF). If this is enabled (ON), higher throughput could be achieved.
Range	ON/OFF
Default Value	ON
Note	This can be set only when the Wireless Mode is **802.11n/a** or **802.11ac**.

Short Guard Interval

General Configuration	-
Detail Configuration	*

Details	Enable/Disable the Short Guard Interval (ON/OFF). If this is enabled (ON), higher throughput could be achieved.
Range	ON/OFF
Default Value	ON
Note	This can be set only when all of the following conditions are met: - Wireless Mode is set to **802.11n/a** or **802.11ac**

Wireless LAN Configuration (5GHz) - QoS(WMM) Configuration (for AP)

BE	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for BE(Best Effort) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax:1 - 15 AIFSN:1 - 15 TxOPLimit: 0 - 8192	
Default Value	ECWmin: 4 ECWmax: 6 AIFSN: 3 TxOPLimit: 0	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

BK	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for (BK: Back Ground) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192	
Default Value	ECWmin: 4 ECWmax: 10 AIFSN: 7 TxOPLimit: 0	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

VI	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for (VI: Video) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192	
Default Value	ECWmin: 3 ECWmax: 4 AIFSN: 1 TxOPLimit: 3008	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

Wireless LAN Configuration (5GHz) - QoS(WMM) Configuration (for AP)

VO			
		General Configuration	-
		Detail Configuration	*
Details	Change the QoS setting for (VO: Voice) of WMM-EDCA.		
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192		
Default Value	ECWmin: 2 ECWmax: 3 AIFSN: 1 TxOPLimit: 1504		
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.		

Wireless LAN Configuration (5GHz) - QoS(WMM) Configuration (for Station)

BE			
		General Configuration	-
		Detail Configuration	*
Details	Change the QoS setting for (BE: Best Effort) of WMM-EDCA.		
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192 ACM: ON/OFF		
Default Value	ECWmin: 4 ECWmax: 10 AIFSN: 3 TxOPLimit: 0 ACM: OFF		
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.		

Wireless LAN Configuration (5GHz) - QoS(WMM) Configuration (for Station)

BK	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for (BK: Back Ground) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192 ACM: ON/OFF	
Default Value	ECWmin: 4 ECWmax: 10 AIFSN: 7 TxOPLimit: 0 ACM: OFF	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

VI	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for (VI: Video) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192 ACM: ON/OFF	
Default Value	ECWmin: 3 ECWmax: 4 AIFSN: 2 TxOPLimit: 3008 ACM: OFF	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

VO	General Configuration	-
	Detail Configuration	*
Details	Change the QoS setting for (VO: Voice) of WMM-EDCA.	
Range	ECWmin: 1 - 15 ECWmax: 1 - 15 AIFSN: 1 - 15 TxOPLimit: 0 - 8192 ACM: ON/OFF	
Default Value	ECWmin: 2 ECWmax: 3 AIFSN: 2 TxOPLimit: 1504 ACM: OFF	
Note	TxOPLimit must be a multiple of 32. When the entered value is not a multiple of 32, a largest multiple number of 32 not exceeding the entered value will be applied.	

Smart Wireless Setup

Smart Wireless Setup		General Configuration	-
		Detail Configuration	*
Details	Enable/Disable the Smart Wireless Setup.		
Range	ENABLE/DISABLE		
Default Value	ENABLE		

Interface		General Configuration	-
		Detail Configuration	*
Details	Select the wireless interface that you wish to perform Smart Wireless Setup.		
Range	[1]-[8]		
Default Value	[1]		

External Registrar		General Configuration	-
		Detail Configuration	*
Details	Enable/Disable the external registrar.		
Range	ENABLE/DISABLE		
Default Value	DISABLE		

PIN Code		General Configuration	-
		Detail Configuration	*
Details	Set the PIN code for AP-500AC.		
Range	8 digit number (decimal)		
Default Value	The default value can be found on the product label (see the bottom of the unit).		

VLAN Configuration - IEEE 802.1Q VLAN Configuration

VLAN

General Configuration	-
Detail Configuration	*

Details	Enable/Disable the VLAN feature. When set to **ENABLE**, connect a wired LAN port of AP-500AC and trunk port of the VLAN HUB via a network cable.
Range	ENABLE/DISABLE
Default Value	DISABLE
Note	When this setting is enabled, packets of tagged frames are sent to a wired LAN using the wired LAN port as a trunk port.

Native VLAN ID

General Configuration	-
Detail Configuration	*

Details	Set the VLAN ID for native VLAN. Set the same VLAN ID as a trunk port of the VLAN HUB that will be connected to a wired LAN port of AP-500AC.
Range	1-4094
Default Value	1
Note	This setting becomes active only when VLAN is set to **ENABLE**. The received packets of untagged frames will be processed as native VLAN. For packets with the same VLAN ID as the native VLAN, tags will not be added.

Wireless LAN 1-8 VLAN ID

General Configuration	-
Detail Configuration	*

Details	Set the VLAN ID for each Multi SSID of AP-500AC.
Range	1-4094
Default Value	1
Note	This setting becomes active only when VLAN is set to **ENABLE**. The SSID corresponding to each VLAN ID will be displayed on the right.

Management VLAN ID

General Configuration	-
Detail Configuration	*

Details	Set the VLAN ID for management VLAN. When the VLAN is enabled, this will be a VLAN ID to access AP-500AC. To access AP-500AC via wireless LAN, set the same VLAN ID as that of the wireless LAN. When VLAN feature is enabled and one of following authentication modes is set for **Network Authentication**, please enter the same VLAN ID as that of network group where the RADIUS server is installed. - **802.1X** - **WPA-Enterprise** - **WPA2-Enterprise** - **WPA/WPA2-Enterprise**
Range	1-4094
Default Value	1
Note	This setting becomes active only when VLAN is set to **ENABLE**. Access to AP-500AC using IP protocol or FLDP protocol (e.g. Web page, TELNET, Device Server feature) will be limited to the network groups with the same VLAN ID as the management VLAN ID. Access from wireless LAN will also be restricted by **Access Control** feature of AP-500AC. In order to access from wireless LAN, set the wireless LAN of the corresponding protocol to **ENABLE**.

Wired LAN Configuration

Link Speed

General Configuration	-
Detail Configuration	*

Details	Configure the physical network type.
Range	AUTO/10Base-T-Half/10Base-T-Full/100Base-TX-Half/10Base-TX-Full/1000Base-T-Full
Default Value	AUTO
Note	Usually, **AUTO** is used. If a LED on your HUB does not light on when AP-500AC is powered on, change the network type to that of the HUB.

Password Configuration

New Password

General Configuration	-
Detail Configuration	*

Details	Set the administrator password (up to 16 ASCII characters). This password is used for authentication when changing settings from the Web configuration page.
Range	Up to 16 characters
Default Value	(None)

Access Control - Port Filter

SSH

General Configuration	-
Detail Configuration	*

Details	Allow/Deny access using SSH via a wired/wireless LAN. When set to **ENABLE**, access to AP-500AC is allowed. When set to **DISABLE**, access to AP-500AC is denied.
Range	ENABLE/DISABLE
Default Value	Wired LAN : ENABLE / Wireless LAN : DISABLE
Note	This setting is active only when a root password is set on AP-500AC.

HTTP

General Configuration	-
Detail Configuration	*

Details	Allow/Deny access using HTTP via a wired/wireless LAN. When set to **ENABLE**, access to AP-500AC is allowed. When set to **DISABLE**, access to AP-500AC is denied.
Range	ENABLE/DISABLE
Default Value	Wired LAN : ENABLE / Wireless LAN : DISABLE

SNMP

General Configuration	-
Detail Configuration	*

Details	Allow/Deny access using SNMP via a wired/wireless LAN. When set to **ENABLE**, access to AP-500AC is allowed. When set to **DISABLE**, access to AP-500AC is denied.
Range	ENABLE/DISABLE
Default Value	Wired LAN : ENABLE / Wireless LAN : DISABLE

Device Server

General Configuration	-
Detail Configuration	*

Details	Allow/Deny access via a wired/wireless LAN when the Device Server feature of AP-500AC is used. When set to **ENABLE**, access to AP-500AC is allowed. When set to **DISABLE**, access to AP-500AC is denied.
Range	ENABLE/DISABLE
Default Value	Wired LAN : ENABLE / Wireless LAN : DISABLE

Access Control - MAC Address Filter - Wired LAN

Filter Type		General Configuration	-
		Detail Configuration	*
Details	Set a security type for MAC Address filter used over a wired LAN.		
Range	DISABLE/DENY/ALLOW		
Default Value	DISABLE		

MAC Address		General Configuration	-
		Detail Configuration	*
Details	Set the MAC Address filter for a wired LAN. By registering the MAC Address filter, access via a wired LAN can be controlled.		
Range	00:00:00:00:00:01 - FF:FF:FF:FF:FF:FE		
Default Value	00:00:00:00:00:00		
Note	If a filter type is **DISABLE**, access from all devices is allowed. If a filter type is **DENY**, access from the devices registered to MAC Address filter list is denied. If a filter is **ALLOW**, only access from the devices registered to MAC Address filter list is allowed.		

Access Control - MAC Address Filter - Wireless LAN 1 - 8

Filter Type		General Configuration	-
		Detail Configuration	*
Details	Set a security type for MAC Address filtering used over a wireless LAN.		
Range	DISABLE/DENY/ALLOW		
Default Value	DISABLE		
Note	When the Smart Wireless Setup is set to **ENABLE**, MAC Address filtering will not function. To use MAC Address filtering, disable the Smart Wireless Setup or use the wireless interface which does not use MAC Address filtering for the Smart Wireless Setup.		

MAC Address		General Configuration	-
		Detail Configuration	*
Details	Set the MAC Address filter for a wireless LAN. By registering the MAC Address filter, access via a wireless LAN can be controlled.		
Range	00:00:00:00:00:01 - FF:FF:FF:FF:FF:FE		
Default Value	00:00:00:00:00:00		
Note	If a filter type is **DISABLE**, access from all wireless stations is allowed. If a filter type is **DENY**, access from the wireless stations registered to MAC Address filter list is denied. If a filter type is **ALLOW**, only access from the wireless stations registered to MAC Address filter list is allowed.		

Access Control - Privacy Separator - Wireless LAN 1 - 8

Privacy Separator	General Configuration	-
	Detail Configuration	*

Details	Allow/Deny communication among the wireless client devices connected to AP-500AC. If the privacy separator is enabled on the wireless interface, wireless frames are not forwarded to the other wireless interfaces. It is only forwarded to a wired LAN interface.
Range	ON/OFF
Default Value	OFF

Log output configuration - Log Output

USB Log Output

General Configuration	-
Detail Configuration	*

Details	Enable/Disable the USB log output. When set to **ENABLE**, the USB storage device cannot be used over a network using the Device Server feature of AP-500AC.
Range	ENABLE/DISABLE
Default Value	DISABLE

File Size

General Configuration	-
Detail Configuration	*

Details	Specify the log file size (Mbyte).
Range	1-100
Default Value	10

Generation Number

General Configuration	-
Detail Configuration	*

Details	Specify the generation number to save the log.
Range	1-10
Default Value	2

File Name

General Configuration	-
Detail Configuration	*

Details	Specify the log file name.
Range	Alphanumeric character string (1-64 characters)
Default Value	log

TIP

Based on the specified file size and generation number, AP-500AC regularly creates new log files and rotates them by renaming the older version of files.

Example:
File Size: 10MByte
Generation Number: 3
File Name: log

In case of above setting, the log is created up to 3 files ("log.0", "log.1", "log.2") according the rotation procedure below.

(New) log.0 -> log.1 -> log.2 (Old)

1) When the size of log.0 reaches 10MByte, the log.2 is deleted.
2) The log.1 is renamed as log.2.
3) The log.0 is renamed as log.1 and then saved.
4) A new file log.0 is created and then saved.

NTP Configuration - NTP Configuration

NTP

General Configuration	-	
Detail Configuration	*	

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

NTP Server

General Configuration	-	
Detail Configuration	*	

Details	Set the domain name or IP Address for NTP server.
Range	In case of the domain name; Alphanumeric character string (0-128 characters) In case of the IP Address; 0.0.0.0 - 255.255.255.255
Default Value	(None)

Local Time Zone

General Configuration	-	
Detail Configuration	*	

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

A-2. Troubleshooting

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

I don't know the IP Address of AP-500AC.

Solution	Please use the product search utility, "AMC Finder". AMC Finder can search for AP-500AC units connected to a network. For details, refer to **5-12. Product Search Utility**.

I cannot access the Web page of AP-500AC.

HTTP access may be blocked by a port filter function.	
Solution	Log into the Web page of AP-500AC and click **Access Control** - **Port Filter**. In the page displayed, check **ENABLE** is selected for **HTTP**. When **DISABLE** is selected, HTTP access is blocked. By default, this function is disabled for wireless LAN.

Access to AP-500AC may be blocked by MAC Address filter.	
Solution	Log into the Web page of AP-500AC and click **Access Control** - **MAC Address Filter**. In the page displayed, check that access to AP-500AC is not blocked by the MAC Address filter. MAC Address filter can be set respectively for wired LAN and wireless interface. If you do not have a device to access the Web page of AP-500AC, reset AP-500AC to factory default setting. For details on factory default configuration, refer to **5-11. Maintenance Feature** - **How to reset AP-500AC to factory defaults using the Push Switch**.

I cannot access to the USB device connected to AP-500AC

The log output feature may be used. When the USB thumb drive is used for log output, such drive is not displayed in SX Virtual Link.	
Solution	To disable the log output feature, log into the Web page of AP-500AC and click **Log Output** - **Log Output Configuration**. In the page displayed, select **DISABLE** for **USB Log Output**.

Access to device server may be blocked by a port filter function.	
Solution	Click **Access Control** - **Port Filter** and check **ENABLE** is selected for **Device Server**. When **DISABLE** is selected, access to AP-500AC is blocked. By default, this function is disabled for wireless LAN.

Access to device server may be blocked by MAC Address filter.	
Solution	Click **Access Control** - **MAC Address Filter** and check access to AP-500AC is not blocked by MAC Address filter. MAC Address filter can be set respectively for wired LAN and wireless interface.

USB storage error occurred (POWER LED blinks Red).

USB storage device may be removed without stopping the log output feature.	
Solution	Refer **5-8. Log Output** - **Notice When Using the Log Output**.

Configuration Mode error occurred (ACTIVE LED blinks Red).

AP-500AC may be connected to network, not to a PC.	
Solution	Configuration Mode can be started by directly connecting AP-500AC and PC. For details, refer to **3-1. Displaying Web Page of AP-500AC (Initial Configuration)** - **Displaying Web Page Using Configuration Mode**.

USB over current occurred (POWER LED blink Red rapidly).

Overcurrent is detected on USB port.	
Solution	Remove the USB device from AP-500AC.

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Silex Technology:
AP-500AC