Mitel WLAN Adapter

ADMINISTRATOR GUIDE

Release 1.3

Mitel®

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

© Copyright 2017, Mitel Networks Corporation

All rights reserved

Mitel WLAN Adapter Administrator Guide
Release 1.3 - November 2017

Software License Agreement

Mitel, hereinafter known as “Seller”, grants to Customer a personal, worldwide, non-transferable, non-sublicenseable and non-exclusive, restricted use license to use Software in object form solely with the Equipment for which the Software was intended. This Product may integrate programs, licensed to Mitel by third party Suppliers, for distribution under the terms of this agreement. These programs are confidential and proprietary, and are protected as such by copyright law as unpublished works and by international treaties to the fullest extent under the applicable law of the jurisdiction of the Customer. In addition, these confidential and proprietary programs are works conforming to the requirements of Section 401 of title 17 of the United States Code. Customer shall not disclose to any third party such confidential and proprietary programs and information and shall not export licensed Software to any country except in accordance with United States Export laws and restrictions.

Customer agrees to not reverse engineer, decompile, disassemble or display Software furnished in object code form. Customer shall not modify, copy, reproduce, distribute, transcribe, translate or reduce to electronic medium or machine readable form or language, derive source code without the express written consent of the Seller and its Suppliers, or disseminate or otherwise disclose the Software to third parties. All Software furnished hereunder (whether or not part of firmware), including all copies thereof, are and shall remain the property of Seller and its Suppliers and are subject to the terms and conditions of this agreement. All rights reserved.

Customer's use of this software shall be deemed to reflect Customer's agreement to abide by the terms and conditions contained herein. Removal or modification of trademarks, copyright notices, logos, etc., or the use of Software on any Equipment other than that for which it is intended, or any other material breach of this Agreement, shall automatically terminate this license. If this Agreement is terminated for breach, Customer shall immediately discontinue use and destroy or return to Seller all licensed software and other confidential or proprietary information of Seller. In no event shall Seller or its suppliers or licensors be liable for any damages whatsoever (including without limitation, damages for loss of business profits, business interruption, loss of business information, other pecuniary loss, or consequential damages) arising out of the use of or inability to use the software, even if Seller has been advised of the possibility of such damages.

Software License Agreement 1
Mitel WLAN Adapter 5
Features 5
Basic structure 6
Hardware specifications 6
Software specifications 7
Interface specifications 9
Wired LAN specifications 9
WLAN specifications 9
Supported modes 9
Supported channels 10
Supported authentication methods 11
Supported encryption methods 11
Others 12
Operational specifications 13
Operating and communication modes 13
Standard operation mode 13
Setting mode 18
Setting mode function specifications 19
TCP/IP specifications 19
IP address 19
How to determine the IP address 19
HTTP specifications 22
Supported web browsers 22
Setting function 22
Configuration by homepage 22
LED specifications 35
Power on 35
Push switch 36
IEEE802.1X authentication function 37
Function structure 37
Supported standards 37
IEEE802.1X authentication method 37
TLS tunneling encryption method 38
Certification specifications 38
Certification file format 38
802.1X authentication method 38

EAP-TLS 39
EAP-TTLS 39
PEAP 39
EAP-FAST 39
LEAP 39
MAC address filtering function 39
Setting item list 41
Firmware update function 44
Firmware update using homepage 44
Firmware update using FLDP (Silex original protocol for firmware update) 44
Firmware update using the production mode 44
kernel / roofts duplication function 45
Smart wireless setup 46
Set up the smart wireless 46
Set up smart wireless using the push switch 46
Smart wireless setup (push switch) LED state 46
Set up smart wireless using the PIN code method 47
Smart wireless setting (PIN Code) LED state 48
Smart wireless setting process flow 48
FLDP/BR 50
Configure Wi-Fi SSID on MiVoice IP phones 51

Mitel WLAN Adapter

The Mitel WLAN (WLAN) Adapter is a wireless bridge that can add a wireless connection feature to non-wireless devices with a 10/100/1000BASE-T wired LAN interface. It allows any Ethernet enabled device (such as Mitel's product line of IP phones) to join a secure, high-speed network. It is software transparent, meaning no changes to drivers, management tools, or applications are needed.

It allows flexibility to locate Ethernet devices in places where running cables is difficult or impossible. It supports industry leading security including WPA, WPA2, and WEP, plus 802.1x authentication with the most commonly used EAP types.

Features

- Supports two operating modes; Multi-client mode and Single-client mode.
- In a Multi-client mode, multiple devices with a wired LAN port can be connected to the existing WLAN with a device, such as a Ethernet Switch connected to its LAN port (see Note 1).
- Supports WLAN standards; IEEE802.11a/11b/11g/11n
- Supports configuring WLAN country settings while writing firmware.
- Supports wireless data encryption; WEP (64/128Bit), WPA-PSK (TKIP/AES), and WPA2-PSK (AES).
- Supports IEEE802.1X authentications (EAP-TLS/EAP-TTLS/PEAP/EAP-FAST/LEAP) (See Note 2). The Mitel WLAN Adapter can connect to an authenticated network using a RADIUS server.
- Supports 10Base-T/100Base-TX/1000Base-T for wired LAN.
- Supports AUTO MDI/MDIX for wired LAN.
- Automatically recognizes a connection of 10Base-T, 100Base-TX, or 1000Base-T with AutoNegotiation function.
- Supports configuring the Mitel WLAN Adapter with HTTP by starting in the Setting mode.
- Supports updating firmware using a flash memory.
- Supports `FLDR/BR` command.
- Supports the Smart Wireless Setting (see Note 3) for an easy wireless setup.
- Supports the new EU wireless standard of EN300328 V1.8.1.
- Supports AMC Manager to remotely control operations like monitoring, changing settings, firmware updating, or rebooting, all at once (see Note 4).
- Supports PoE.
- Supports configuring Wi-Fi network on MiVoice 6900 series IP phones.

Notes:

1. Multi-client mode does not support the WLAN communications using protocols other than TCP/IP (IPv4 and IPv6).
2. The IEEE802.1X authentication function is only supported for the WLAN port.
3. The wireless setting is compatible with WPS2.0.
4. Each operation can be controlled from the wireless side only.

Basic structure

Hardware specifications

The following table provides the Hardware specifications of the Mitel WLAN Adapter:

Item	Specs		
CPU	Armada370 88F6W11 （Marvell） CPU Clock ＝ 800MHz		
Wired LAN I/F	10Base-T/100Base-TX/1000Base-T × 1Port (Auto-Detect) AutoMDI/MDIX		
Wireless LAN I/F	SX-PCEAN2		
	802.11a	Frequency Range	5GHz
		Data Transfer Method	OFDM
		Data Transfer Rate	54/48/36/24/18/12/9/6(Mbps)
		Channel	36-64ch, 100-140ch, 149-165ch
	802.11b	Frequency Range	2.4GHz
		Data Transfer Method	DS-SS
		Data Transfer Rate	11/5.5/2/1(Mbps)
		Channel	1-13ch
	802.11g	Frequency Range	2.4GHz
		Data Transfer Method	OFDM
		Data Transfer Rate	54/48/36/24/18/12/9/6(Mbps)
		Channel	1-13ch
	802.11n (5GHz)	Frequency Range	5GHz
		Data Transfer Method	MIMO-OFDM
		Data Transfer Rate	MCS0, 1, 2, 3, 4, 5, 6, 7 (1Stream) MSC8, 9, 10, 11, 12, 13, 14, 15(2Stream)
		Channel	36-64ch, 100-140ch
	802.11n (2.4GHz)	Frequency Range	2.4GHz
		Data Transfer Method	MIMO-OFDM
		Data Transfer Rate	MCS0, 1, 2, 3, 4, 5, 6, 7 (1Stream) MSC8, 9, 10, 11, 12, 13, 14, 15(2Stream)
		Channel	1-13ch
ROM	SPI Flash ROM256Mbit（32MByte）		
RAM	DDR3 1066 Memory 1Gbit （128MByte）		

LED	Link LED（Internal RJ45）（Green） Status LED （Internal RJ45）（Orange） Power LED：Red WLAN LED：Red/Green STATUS LED：Green
SW	Push Switch × 1
Loader F/W	u-boot

Software specifications

Item	Specification
Product name	WLAN Adapter
OS	Linux (kernel 3.2.54)
Network I/F	Wired LAN / WLAN
Basic protocol (in Setting mode)	**Network layer** ARP, IP **Transport layer** TCP, UDP **Application layer** HTTP, DNS (only for Simple response function), DHCP (only for simple server function）， NetBIOS over TCP/IP (only for Name server） JCP (UDP#19541), **Other** FLDP FLDP/BR SX-SMP
(in regular operation mode)	**Other** FLDP FLDP/BR
Wireless Security	WEP(64/128Bit)
	WPA-PSK(TKIP/AES)
	WPA2-PSK(AES)
	802.1X (EAP-TLS/EAP-TTLS/PEAP/EAP-FAST/LEAP)
OpenSSL	Version 0.9.8o
Web browser	Recommended web browsers: • Internet Explorer 8 or later • Safari 4.0.0 or later
Webpage languages	• Japanese • English
Administrator password	Product configurations are password-protected
Remote initialization	The following can be controlled on a web browser: • Restart of the Product • Setting initialization

LED	Total 5LEDs: • RJ45：2LEDs Link LED ：Green Status LED ：Orange • PCB: 3LEDs Power LED：Red WLAN LED：Red/Green STATUS LED：Green
PushSW	1 switch • TFTP mode • Setting initialization mode • Operation mode change (only for setting)
F/W Update	• JCUPWIN (FLDP) Only via the wired LAN port • Web (HTTP)
Shipping inspection tool	SxFactory version 2.0.5 or later

Interface specifications

Wired LAN specifications

The following are the specifications of the wired LAN interface of the Mitel WLAN Adapter:

- Supports 10Base-T/100Base-TX/1000Base-T
- Supports AutoMDI/MDIX

Note: The Jumbo Frame is not supported.

You can connect your device through the wired LAN port of the Mitel WLAN Adapter to use in the existing WLAN environment.

WLAN specifications

The Mitel WLAN Adapter supports the following wireless standards for 5 GHz and 2.4 GHz bands:

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11a
- IEEE 802.11n

The MAC address for the WLAN connections varies depending on the communication mode. For more information, see “Single-client mode” on page 13 and “Multi-client mode” on page 17.

Restrictions

- Until the device is connected in the WLAN environment, all packets received through the wired LAN port will be deleted.
- When the device is disconnected in the WLAN environment, all the packets received through the wired LAN port will be deleted, and cannot be retrieved.

Supported modes

The Mitel WLAN Adapter supports the Infrastructure Mode.

Infrastructure mode

The Mitel WLAN Adapter can operate in the Infrastructure mode.

- The Mitel WLAN Adapter connects to a wireless network consisting of an access point.
- Setup information (for example, wireless channels) is automatically configured according to the wireless network.
- 802.11n is not available for encryption methods of WEP or TKIP.
  802.11a or 802.11b/g operates at up to 54Mbps.
- The following table specifies available authentication and encryption methods:

Authentication method	Encryption method
Open	None WEP
Shared	WEP
WPA2 PSK	AES
WPA/WPA2 PSK	AES AUTO
WPA@ EAP	AES
WPA/WPA2 EAP	AES AUTO

Supported channels

The Mitel WLAN Adapter supports wireless channels of 2.4 GHz and 5 GHz (W52, W53, W56, and W58) bands.

The following wireless channels are available:

- 2.4 GHz (802.11 n/b/g, 802.11 b/g)
  1 to 13 ch
- 5 GHz (802.11 n/a, 802.11 a)
  W52: 36, 40, 44, 48
  W53: 52, 56, 60, 64
  W56: 100, 104, 108, 112,
  116, 120, 124, 128,
  132, 136, 140
  W58: 149, 153, 157, 161, 165

On the WLAN network, the Mitel WLAN Adapter uses the same channel. When the wireless network is built in Adhoc mode, only 2.4GHz band and W52 channels can be used.

Product destinations

Available channels vary depending on where the Mitel WLAN Adapter is deployed:

		WW				
	US	JP	EU	AU	NZ	CA
2.4GHz	1-13ch	1 to 11ch	1-11ch	1-13ch	1-13ch	1-11ch
5 GHz	W52	W52	W52	W52	W52	W52
	W53	W53	W53	W53	W53	W53
	W56	W56	W56	W56?1	W56	W56*1
		W58	W58	W58	W58	W58

*1 Except 120ch to 128ch (5600MHz - 5640MHz)

Automatic destination setting

When the destination is set to **WW**, the Mitel WLAN Adapter collects information of nearby access points when it is powered on, and then automatically determines the range of wireless channels.

Operating specifications

- When the Mitel WLAN Adapter is powered on, it collects the destination information (country code) contained in beacon emitted from nearby access points. When such information is being collected, WLAN packets are not sent from the Mitel WLAN Adapter.
- The Mitel WLAN Adapter does not connect to access points when destination information is being collected. Also, the two LEDs on the Mitel WLAN Adapter (WLAN and STATUS) will blink simultaneously.
- Collection of destination information will be performed for all channels (1-13ch, W52, W53, W56, W58).
- For the destination information, information of access point with highest signal strength will be applied.
- There is no timeout for collecting destination information. The collection is repeated if the destination information is not obtained after searching through all channels.
- Smart Wireless Setup cannot be used when the destination information is being collected.
- Allows using the Setting mode when the destination information is being collected. However, easy wireless configuration and Smart Wireless Setup (PIN code method) cannot be used. When the Setting mode is used, collection of destination information is terminated.
- Allows updating the firmware through a wired LAN network even when the destination information is being collected.

Supported authentication methods

The Mitel WLAN Adapter supports the following authentication methods:

- Open
- Shared
- WPA PSK
- WPA2 PSK
- IEEE802.1X (EAP)

Supported encryption methods

The Mitel WLAN Adapter supports the following encryption methods:

- WEP encryption method
  - Supporting 128-bit WEP (104 effective) and 64-bit WEP (40 effective)
  - For WEP key setting, 26-characters and 10-characters are processed as hexadecimal input, while 13-characters and 5-characters are character-string inputs.
- TKIP/AES

  WPA-PSK supports two encryption methods; TKIP and AES. WPA2-PSK supports AES encryption method.

  - For ASCII, input PSK in 8 to 63 characters. You can use single-bite alphanumeric and symbols.
  - For hexadecimal notation, input 64 characters for PSK. You can use characters of 0 to 9, A to F, and a to f.

Others

A-MSDU is disabled.

Operational specifications

Operating and communication modes

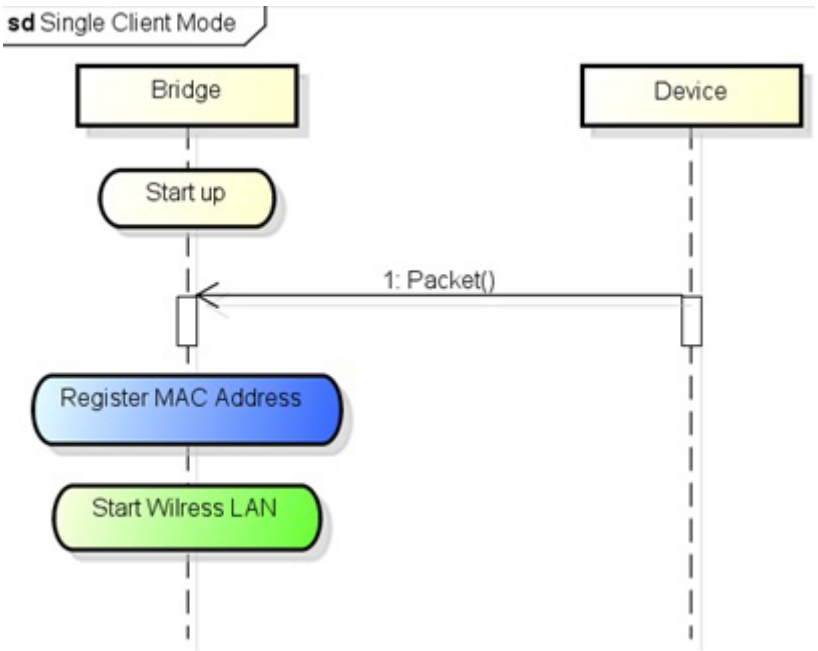
The Mitel WLAN Adapter supports two operating modes, two communication modes, and two setting modes.

Standard operation mode

In this mode, only the bridge function can be operated. The setting functions are not available. When the IP address of the Mitel WLAN Adapter is set, and if a device on a wireless network can access the IP address, the setting function is available even in the normal operation mode. When the Mitel WLAN Adapter is turned on or re-started, the Mitel WLAN Adapter starts in this mode.

Single-client mode

The Single-client mode can connect one device, which is connected to the wired LAN port through a LAN cable, in the WLAN environment. The MAC address for the WLAN environment is the MAC address (source address) of the first packet received through the wired LAN port. This allows the device connected to the wired LAN port appear as connected directly to the WLAN. This mode supports a function to register the MAC address for the WLAN to the Mitel WLAN Adapter (wired LAN port connected device identifying function).

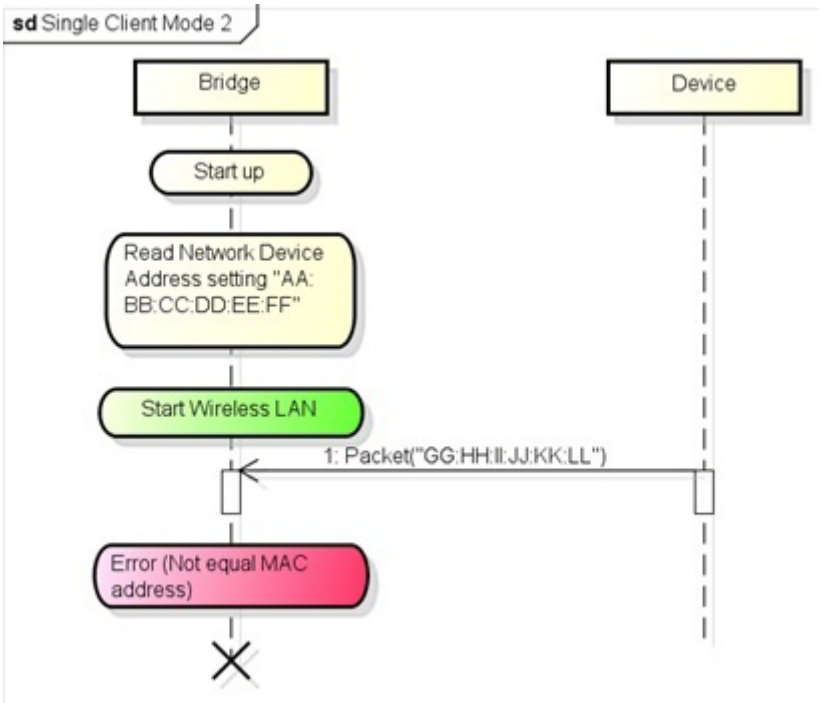


Wired LAN port connected device identifying function

This function is available only in the Single-client mode, and identifies the device connected to the wired LAN port of the Mitel WLAN Adapter. By registering the MAC address to **Connected Device Address**, only devices with registered MAC addresses can be communicated.

A non-registered device, when connected, is recognized as an error, and the front LED flashes and stops the bridge function.

Note: When no MAC address is registered to the **Connected Device Address**, this function is disabled.



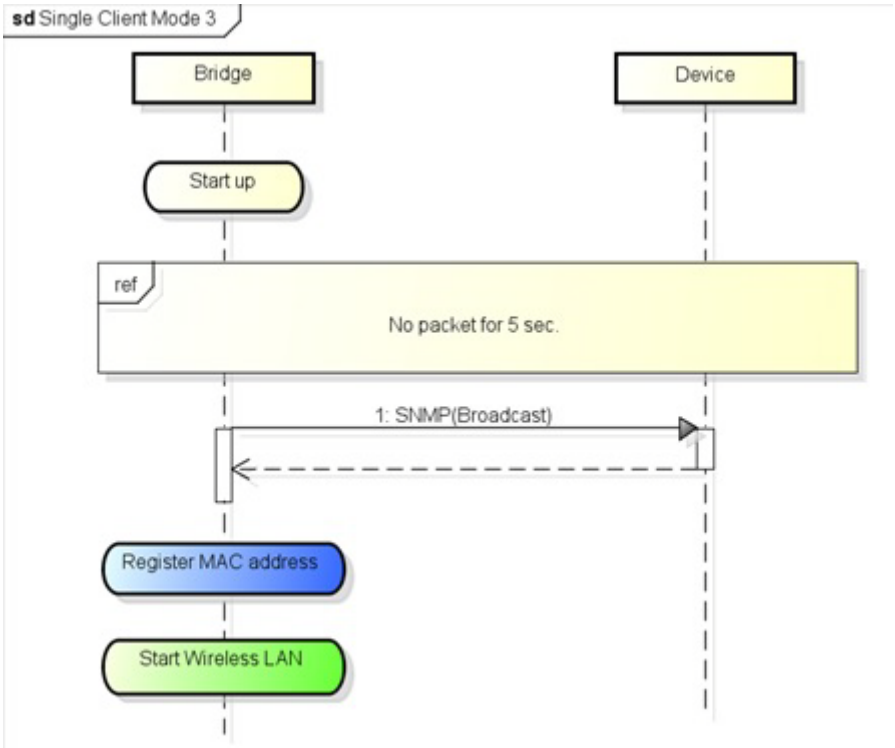
Automatic wired LAN port connected device MAC address acquiring function

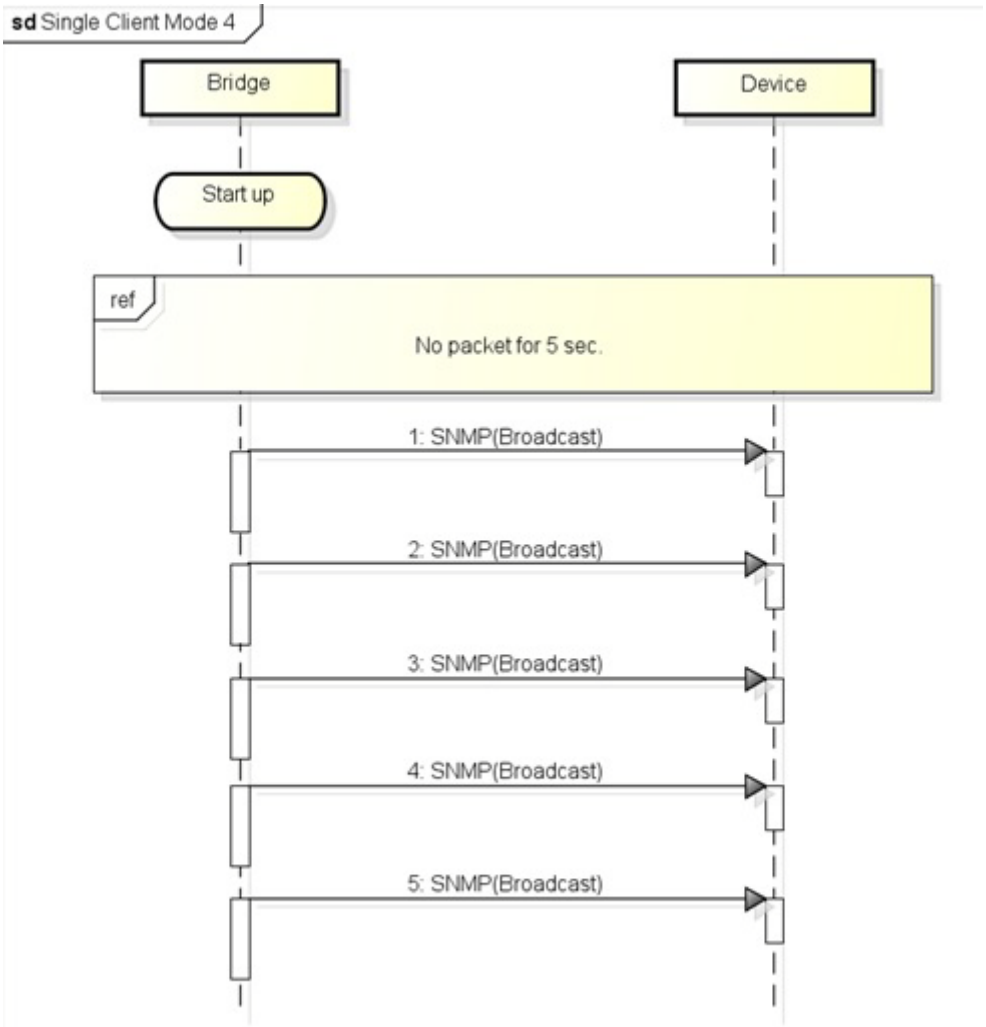
This is available only in the Single-client mode. General purpose devices usually transmit some packets for address resolution when the wired LAN link is established. Some devices, however, do not send any packets at all. This function gets a MAC address automatically even when such a device is connected.

Note: Even with this function some devices may not send response packets. In such a case, see “Wired LAN port connected device identifying function” on page 13.

This function broadcasts SNMP Request packets (OID: sysDesc, Source IP address: 192.0.0.192) when the connected device has not transmit packets even 5 seconds after the wired LAN port link is established.

This is repeated five times to prompt the device to send packets.


sd Single Client Mode 3
Bridge
Device
Start up
ref
No packet for 5 sec.
1: SNMP(Broadcast)
Register MAC address
Start Wireless LAN



Restrictions

- Only one device can be connected to the wired LAN port.
- Multiple device connection is not allowed with a Ethernet Switch.
- When the product is operational (Single-client mode or Setting mode), you cannot switch the device connected to the wired LAN port.
  When the connected device is changed, WLAN connectivity cannot be established until the WLAN is disconnected, and the Mitel WLAN Adapter is turned on again.

Note: When more than one device is connected by mistake, the error LED (at the front) blinks and the bridge function is terminated.

- The Single-client mode cannot be used for a device with more than one MAC address (for example, load-balancing PC)
- View Full Map: The Network and Sharing Center function in Windows Vista or Windows 7 is not fully supported because of restrictions of the used protocol.

Note: The View Full Map function in Windows Vista or Windows 7 uses the Link Layer Topology Discovery (LLTD) protocol, and sends some special packets between 00-0D-3A-D7-F1-40 and 00-0D-3A-FF-FF-FF to the source MAC address.

Multi-client mode

The Multi-client mode is used to connect Mitel WLAN Adapter's wired LAN port and multiple devices to a WLAN environment through a Ethernet Switch. The MAC address of Mitel WLAN Adapter is used for WLAN connection. A maximum of 16 devices can be connected to a WLAN environment at once under the Multi-client mode. (The internal specifications and software capability can allow up to 32 device connections at a time)

Restrictions

- The Multi-client mode is not available for a device with more than one Mac address (for example, load-balancing PC)
- TCP/IP (IPv4 and IPv6) protocol is available. Other communication protocols are not supported.
- The following IPv6 packets are not covered by the bridge operation:
  - Inverse Neighbor Advertisement (one way from wired LAN to WLAN)
  - Fragment Header (transferred as-is)
  - Authentication Header (transferred as-is)
  - Encapsulating Security Payload (transferred as-is)

TCP/IP set up

Use the TCP/IP set up to access the Mitel WLAN Adapter from a device on WLAN.

IP address set up

Enable Dynamic Host Control Protocol (DHCP) to dynamically get an IP address. The dynamically received IP address cannot be stored in the setup information. To use a fixed address, disable DHCP to enter the IP address.

DHCP client

RFC2131/RFC2132 is supported to get an IP address, subnet mask, gateway address, WINS server address, DNS server address, and the default domain name from the DHCP server.

- To set an IP address with DHCP, a work station where the DHCP server is operating is required.
- Windows NT’s OS DHCP server (Microsoft’s enhancement is included) is supported.
- DHCP Request is issued always as a broadcast (255.255.255.255). DHCP’s RenewRequest (Request to renew the period to use the address) will be issued to the server that received the address.
- When DHCP is not available, retry will be done every 30 seconds for three times.
- When an IP address is already set, the originator address and DHCP CIADDR (client IP Address) field uses the preset IP address.
- When an IP address is not set, the originator address and CIADDR is 0.0.0.0.

Link-local address

Link-local address is used when other ways to set up (manual setting or DHCP) fail to get an IP address.

Randomly choose an IP address from 169.254.1.0 to 169.254.254.255 and then broadcast an ARP request on the network to check if the IP address is not used by any other device. If you receive an ARP reply, the IP address is considered to be in use and then another IP address is retried.

As Link-local address is to be used on a small network, it cannot be used on multiple networks. As the packet with the assigned IP address cannot be routed, the communicable range is limited to the same network.

When an IP address cannot be obtained from DHCP, even when the manual setting is enabled, the Link-local address works.

Setting mode

The Setting mode is an operation mode used to configure the Mitel WLAN Adapter.

The Setting mode performs through the wired LAN. Use the push switch to change to the Setting mode from the standard operation mode. For more information, see “Push switch” on page 36.

When the product performs under the Setting mode, the Auto Resolution Function is running as described in “IP address” on page 19. Therefore, there is no need to confirm IP address of the Mitel WLAN Adapter or a PC used for configuration.

> **Note:** Even in the normal operation mode, if the IP address is set in the TCP/IP, setting on the web can be done by accessing the IP address from the device on wireless.

Setting mode function specifications

TCP/IP specifications

The following lists the TCP/IP specifications:

- Complying with IP Version 4
- IP routing: 0
- Maximum number of UDP sessions: 8
- Maximum UDP data gram length: 2048 octets for sending/receiving
- UDP checksum is skipped while transmission (always 0)
- Maximum number of TCP sessions: 32 (one session is used for LISTEN)
- TCP window size: up to 32768 octets for sending or receiving

IP address

The following functions are available in the Setting mode. The IP address of the Mitel WLAN Adapter is automatically configured in response to a condition of connected device for setup.

- Simple DHCP Server function
- Proxy ARP response function
- Proxy DNS response function
- Proxy NBNS (NetBIOS Name Service) function

The following section specifies how to determine its IP address.

How to determine the IP address

Dynamic retrieving setting to configure device IP address

In case that the method to determine setting device's IP address is dynamic (using DHCP), the simple DHCP server function of this product dynamically allocates the following values, and the IP address of the product is set to 92.168.0.215.

Parameter	Setting value
IP address	192.168.0.1
Subnet mask	255.255.255.0
Default gateway address	192.168.0.215
DNS server address	192.168.0.215
Lease time	0xffffffffsec

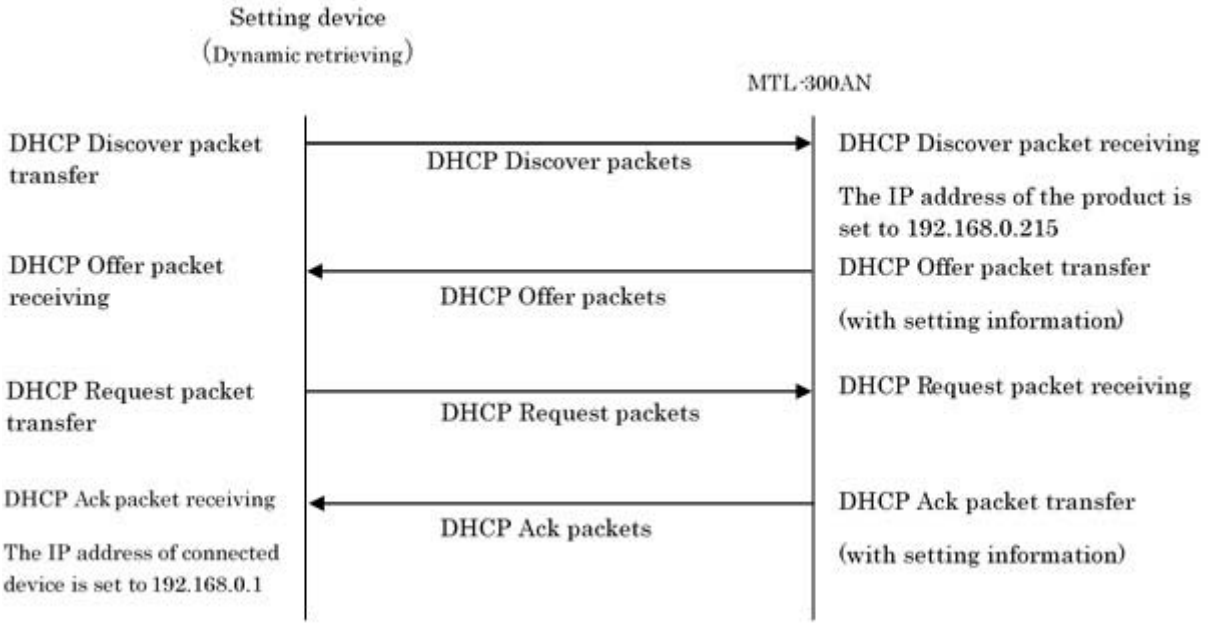


Figure 1: Procedure to decide IP address by simple DHCP server function

If DHCP Request packet transfer is made by the device for configuration before DHCP Discover packet transfer, the DHCP NAK packet transfer is made to delete old information.

Fixed IP address for setting device

In case that an IP address of the setting device is fixedly allocated, this product uses an IP address dynamically according to the packets sent by the device.

Address determination using proxy ARP response function

When ARP Requests packets are sent by the device for configuration, the destination IP address (target IP address) of ARP Request packets is allocated to this product, and the ARP reply packets are transferred.

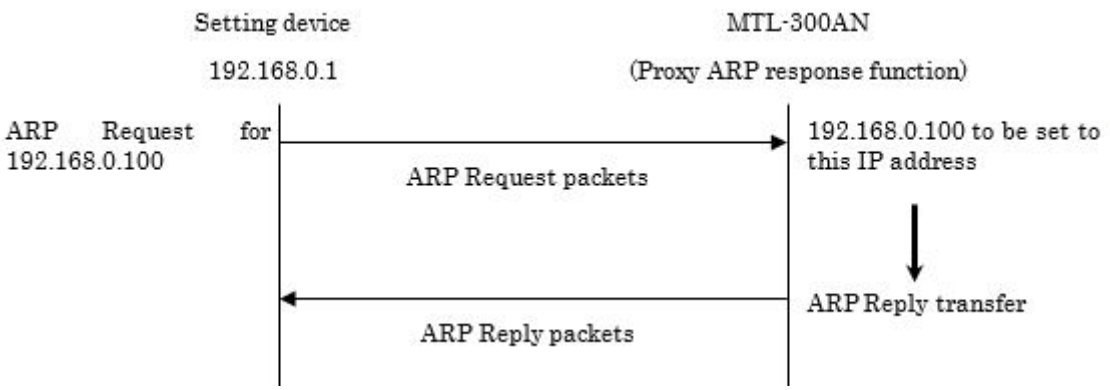


Figure 2: IP address setting procedure using proxy ARP response function

Address determination using proxy DNS response function

If the name resolution process is executed by the setting device using DNS Query packets, DNS Response packet transfer is made using the Proxy DNS response function of the Mitel WLAN Adapter. The IP address of the product is set to the A record of DNS Response packets.

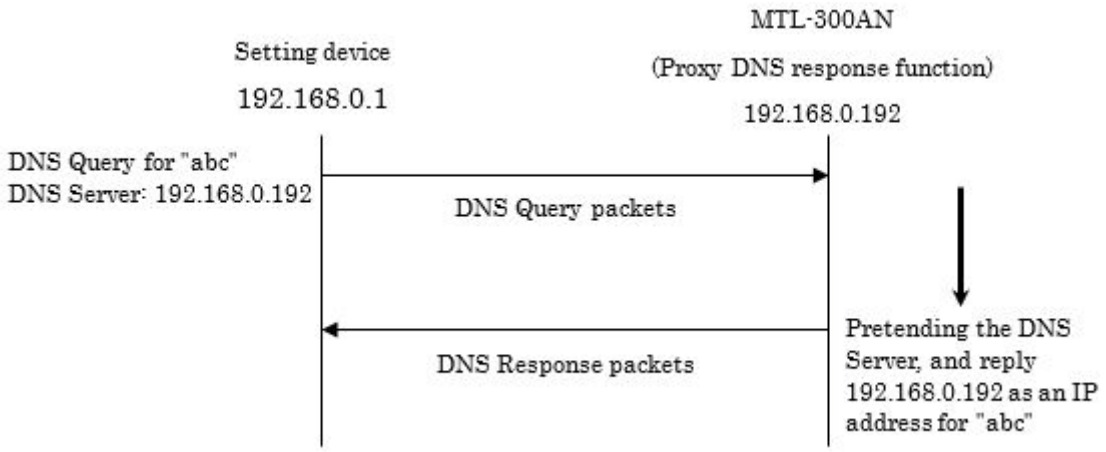


Figure 3: IP address setting procedure using proxy DNS response function

Address determination using Proxy NBNS (NetBIOS Name Server) response function

If the name resolution process is executed by the setting device using NBNS Query packets, NBNS Response packet transfer is made using Proxy NBNS response function of the Mitel WLAN Adapter. The IP address of the Mitel WLAN Adapter is set in the NBNS response packets.

In case that NBNS Query packets are transferred by network broadcasting, an IP address (NBNS Query packet source IP address + 1) is assigned as the IP address of the Mitel WLAN Adapter.

> **Note:** If the lowest 1 byte of the source IP address is 254, an address which is lower 1 byte, 253 is allocated. In case the product IP address is in the same segment of the source IP address, the address will not be changed.

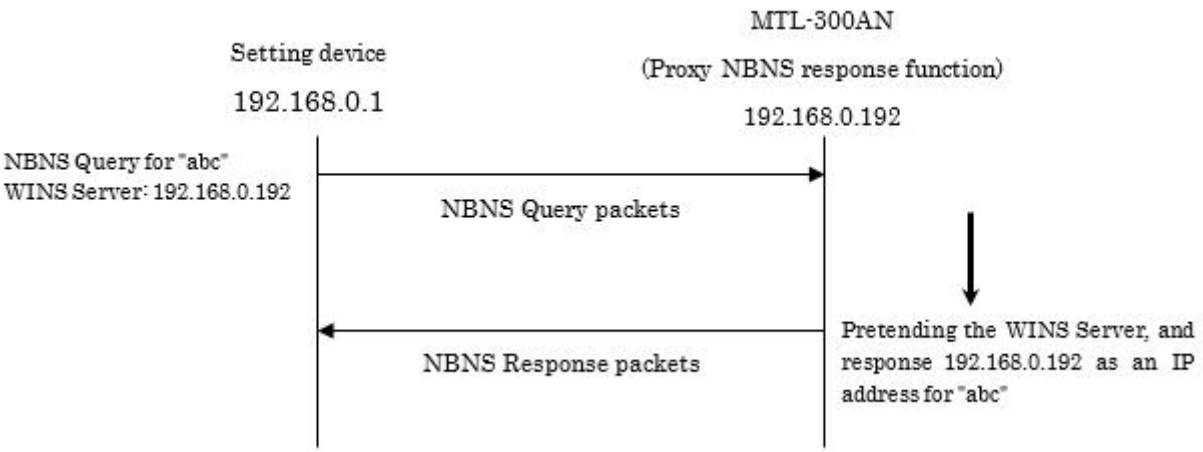


Figure 4: IP address setting procedure using NBNS Query packets

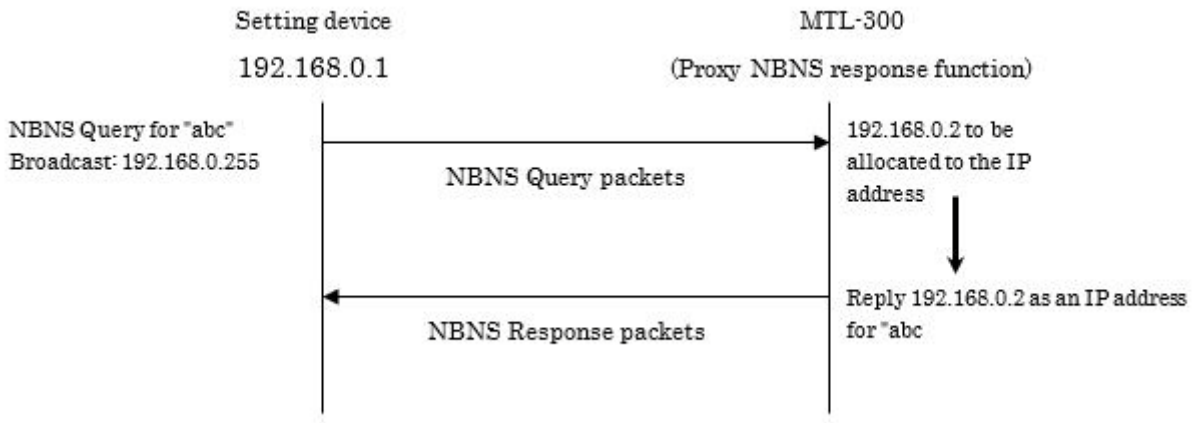


Figure 5: IP address setting procedure using NBNS query packets (network broadcasting)

HTTP specifications

The Mitel WLAN Adapter supports HTTP. You can configure the Mitel WLAN Adapter setting using a web browser:

The following lists the HTTP specifications:

- Maximum number of sessions: 8
- Compliant with HTTP1.0 (RFC1945)
- Protected by a password to prohibit access other than the administrator
  The password is not configured by the factory default.

Supported web browsers

The Mitel WLAN Adapter supports the following web browsers:

- Microsoft Internet Explorer 8 or later
- Safari 4.0.0 or later

Setting function

Configuration by homepage

You can configure the Mitel WLAN Adapter using the homepage, including restarting and restoring factory default.

How to access homepage

Start the Mitel WLAN Adapter in the Setting mode to access the homepage. Specify any URL on the address bar of the web browser in the connected device (PC for configuration) to open the homepage.

- After the web browser is open, keep the same URL or IP address until the set up mode is closed.

- When an IP address is set and the device on the wireless can access the IP address, even in normal operation mode, you can open the website by accessing the IP address.

Restrictions

If the PC's IP address is static allocated, the homepage is not available under the following conditions.

- You can access only with No. 80 HTTP protocol standard port number.
- Add http://to the URL if the browser does not add automatically.
- To assign an IP address on URL, use an address in the same segment as the PC’s IP.
- With Name Resolution disabled (no DNS Server address is registered, NetBIOS disabled), when a name (for example, http://mitel) is assigned, the set up screen is not displayed.

Security function

The homepage is protected by using a password to prevent unauthenticated setting changes. The login page is displayed before you access the homepage to configure the product.

Enter the password to access the homepage.

By default, no password is set and the password enter page is not displayed.

Language option

The homepage is available in Japanese and English.

Select the language you wish to use from the login page or **Language Option** in the left pane.

Login page

If a password is set to the product, the following login page is displayed. Enter the password to access the homepage.

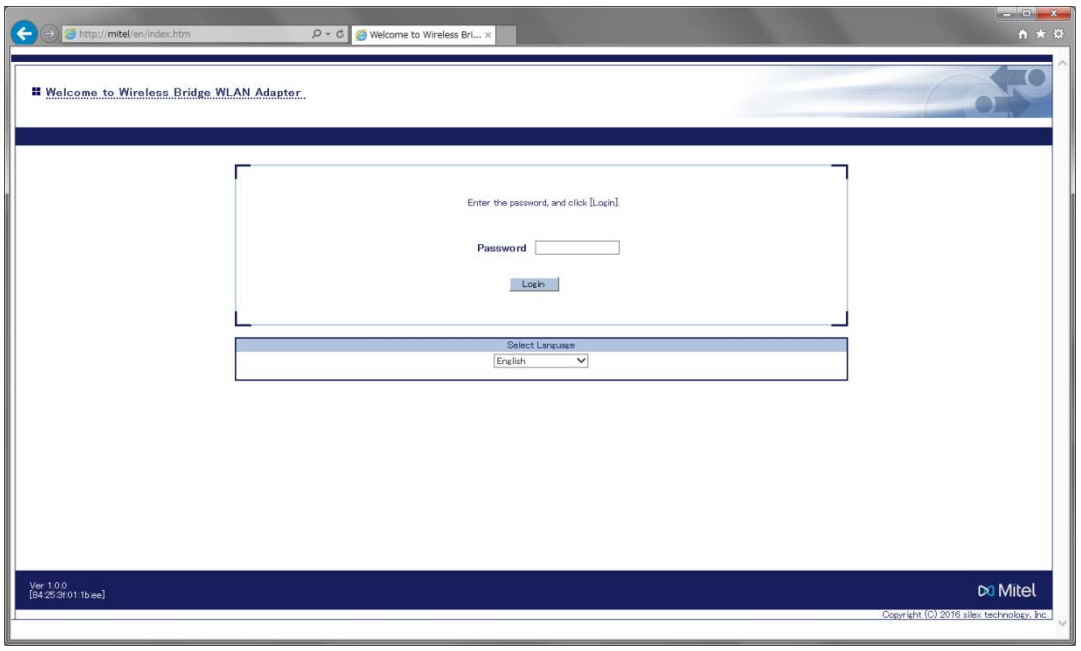


Figure 6: Login page

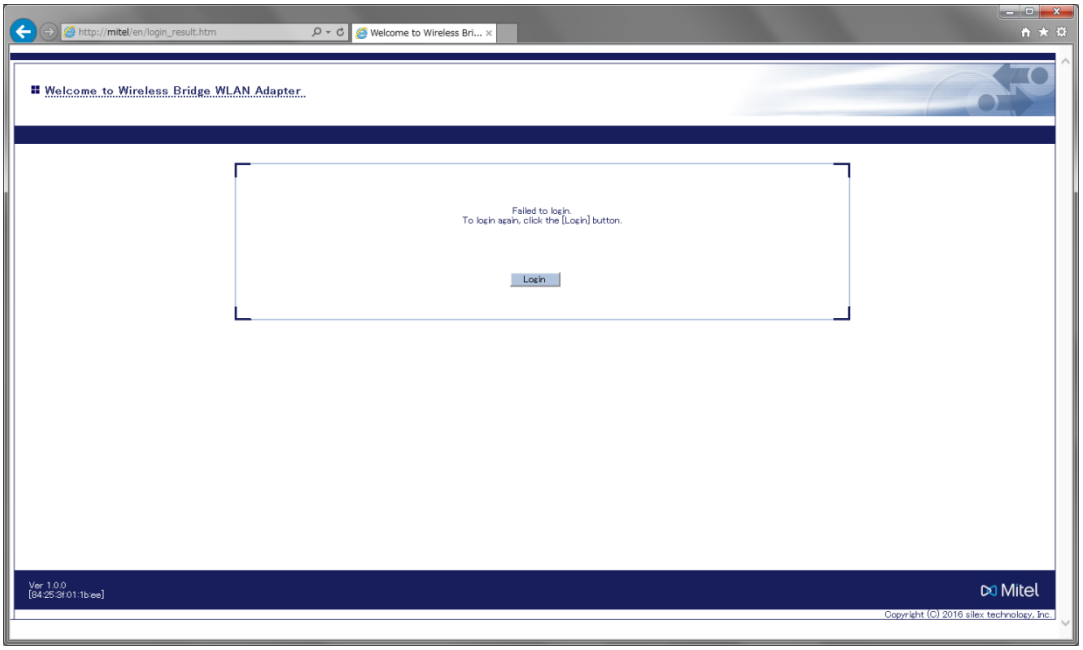


Figure 7: Login error page

WLAN setting page

The WLAN setting page consists of following three pages:

- Easy Configuration page
- Detailed Configuration page
- Smart Wireless Setup page

Easy Configuration page

In the Easy Configuration page, you can select a connecting device from the list, which is searched by the wireless network. WLAN setting is available by entering a network key (WEP key or pre-shared key). The WEP key index is automatically set to 1 when the network authentication method is Open, and the wireless network with WEP key is configured from the Easy Configuration page. If the WEP key index in the connected wireless network is other than 1, communications cannot be established. Wireless settings are not supported for a wireless network with shared authentication method.

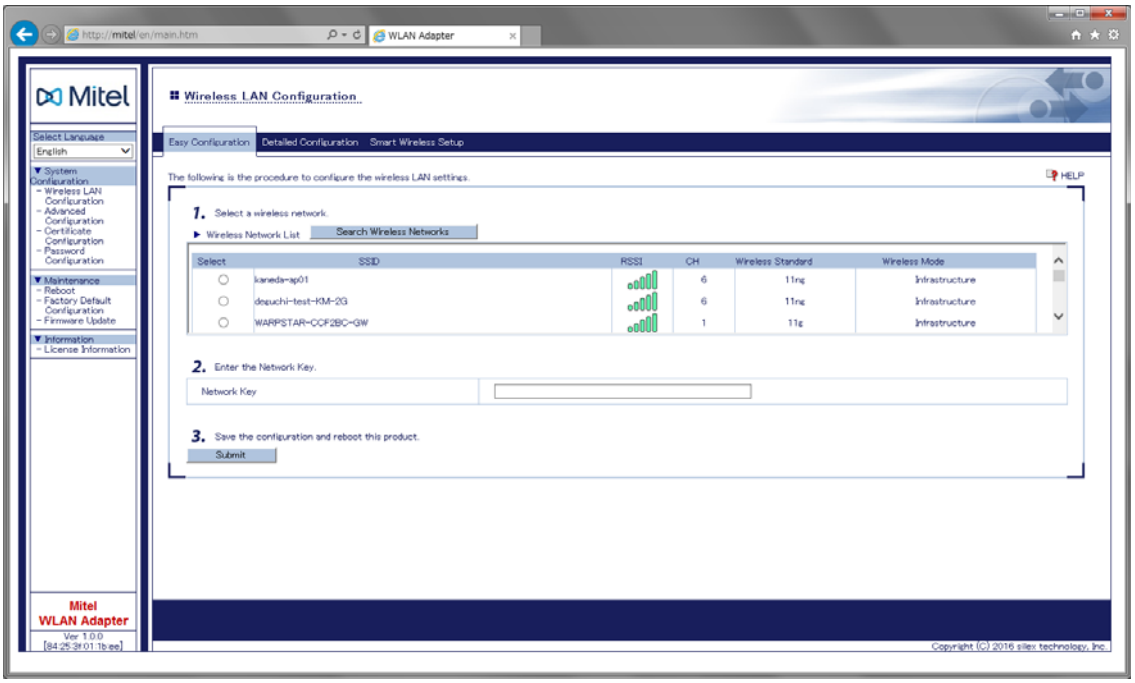


Figure 8: Easy Configuration page

Wireless network list

The wireless connections in the network is detected by the Mitel WLAN Adapter. Up to 32 wireless connections can be listed in descending order of radio intensity. Wireless connection search is conducted or updated by accessing to the WLAN Configuration page after the product is started, or by pressing the **Search Wireless Networks** button. Access points with stealth AP functionality are not detected.

If wireless connections are already registered to the Mitel WLAN Adapter's flash memory, these connections are listed at the top with their option buttons already selected.

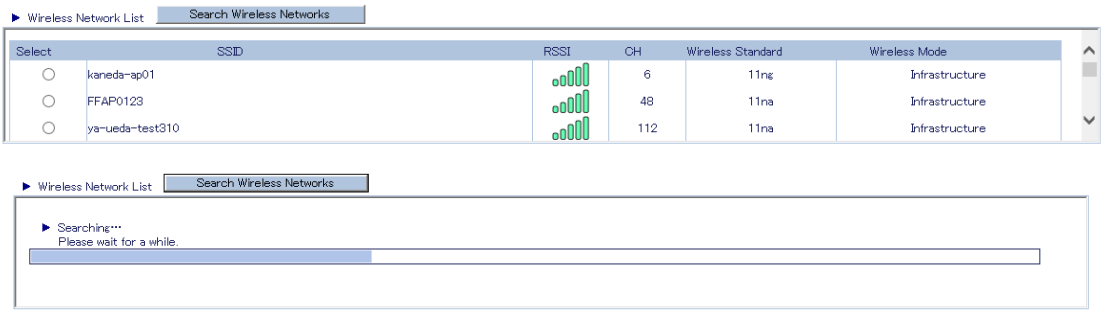


Figure 9: Wireless Network list and search progress bar

Detailed Configuration page

The following WLAN setting is available in the Detailed Configuration page.

Table 1: WLAN Basic Configuration

Item	Default	Available value
Operating Mode	Infra.	Infra.
SSID	“SXxxxxxx” "xxxxxx" is the last 6 digits of the product MAC address	1 to 32 character string

SSID Filter	OFF	OFF / ON
Wireless Standard	AUTO	AUTO / 2.4GHz / 5GHz
Channel	“11”	Selectable from the list box
Network Authentication	Open	Open / Shared / WPA / WPA2 / WPA/WPA2 Mixed Mode
IEEE802.1X Authentication	OFF	OFF / ON

Table 2: WEP Configuration

Item	Default	Available value
WEP	OFF	OFF / ON
Key Index	1	Selectable from the list box
WEP Key 1	""	5/10 characters (64bit） or 13/26 characters (128bit) (password)
WEP Key 2	""	5/10 characters (64bit） or 13/26 characters (128bit) (password)
WEP Key 3	""	5/10 characters (64bit） or 13/26 characters (128bit) (password)
WEP Key 4	""	5/10 characters (64bit） or 13/26 characters (128bit) (password)

Table 3: WPA/WPA2 Configuration

Item	Default	Available value
Encryption Mode	AES	AES / AUTO
Pre-Shared Key	"silex technology, Inc."	String of 8 to 64 characters

Table 4: IEEE802.1X Authentication Configuration

Item	Default	Available value
IEEE802.1X Authentication Type	EAP-TLS	EAP-TLS / EAP-TTLS / PEAP / EAP-FAST / LEAP

Table 5: Inner Authentication Method Configuration

Item	Default	Available value
Inner Authentication Method	PAP	PAP / CHAP / MSCHAP / MSCHAPv2

Table 6: Server Certificate Verification Configuration

Item	Default	Available value
Server Certificate Verification	OFF	OFF / ON

Table 7: IEEE802.1X User Configuration

Item	Default	Available value
IEEE802.1X User Name	“”	64 characters or less

Password	“”	32 characters or less

Table 8: EAP-FAST Configuration

Item	Default	Available value
PAC Auto-distribution	OFF	OFF / ON

Table 9: IEEE802.1X Network Device Configuration

Item	Default	Available value
Device Filter	ON	OFF / ON
Network Device Address	“”	MAC address (available up to 16 under Multi-client mode)

> **Note:** The **Default Filter** item can be enabled only when the destination is US. When this item is set to **OFF**, a caution on security is displayed.

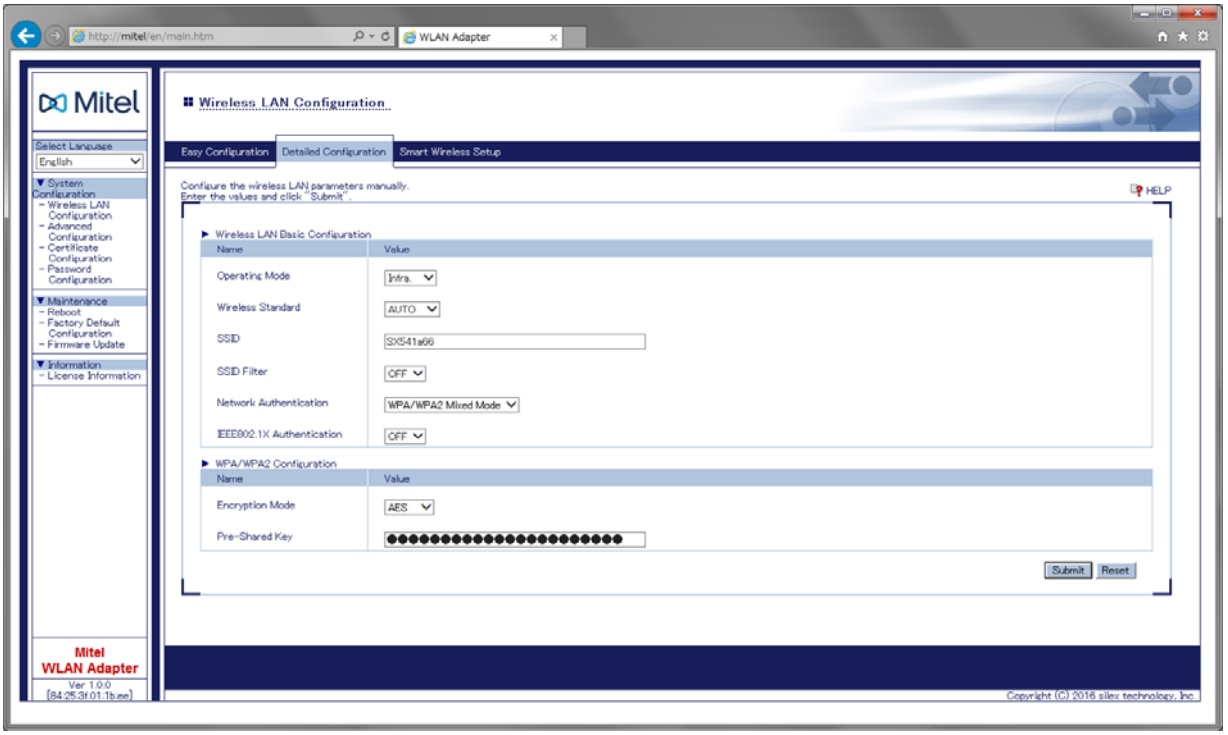


Figure 10: Detailed Configuration page

Smart Wireless Setup page

On the Smart Wireless Setup page, you can execute with PIN code and renew the PIN code.

Table 10: Smart Wireless Setup Execution

Item	Default	Available value
PIN code	-	Every click will renew the PIN code.
Execution	-	Smart Wireless Setup will be executed (PIN code)

Note: By default, automatically generated PIN code is displayed.

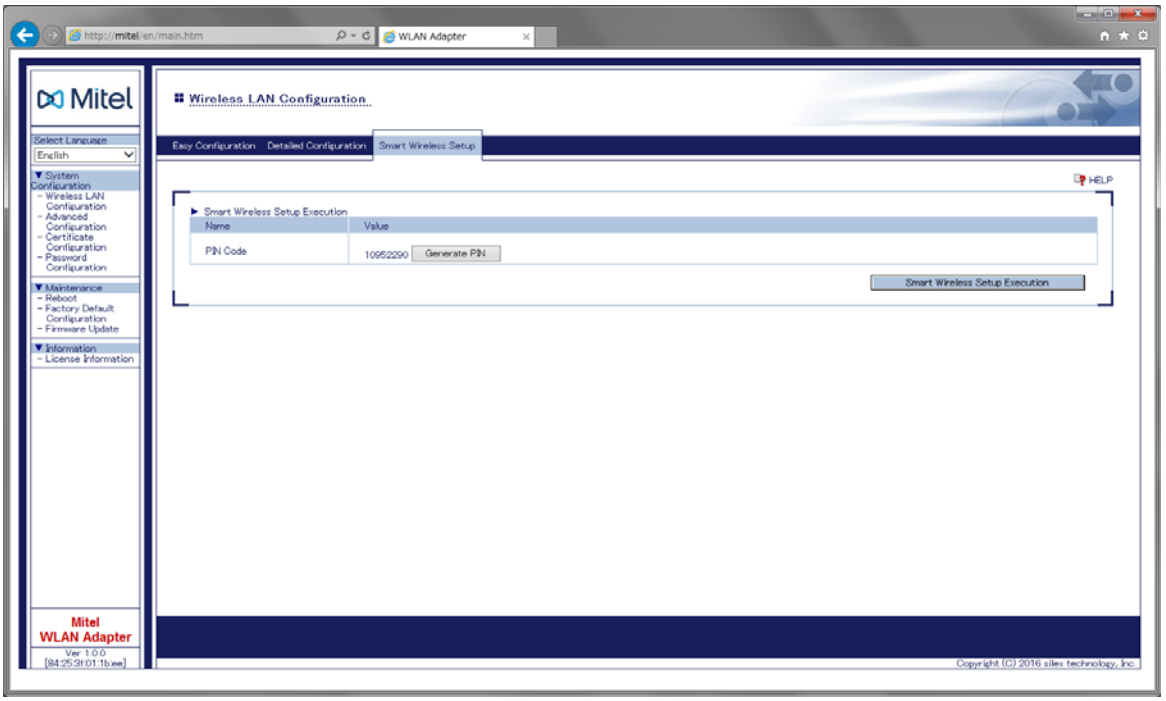


Figure 11: Smart Wireless Setup page

Push the **Execute Smart Wireless Setup** button to view the window below to execute Smart Wireless Setup (PIN Code).

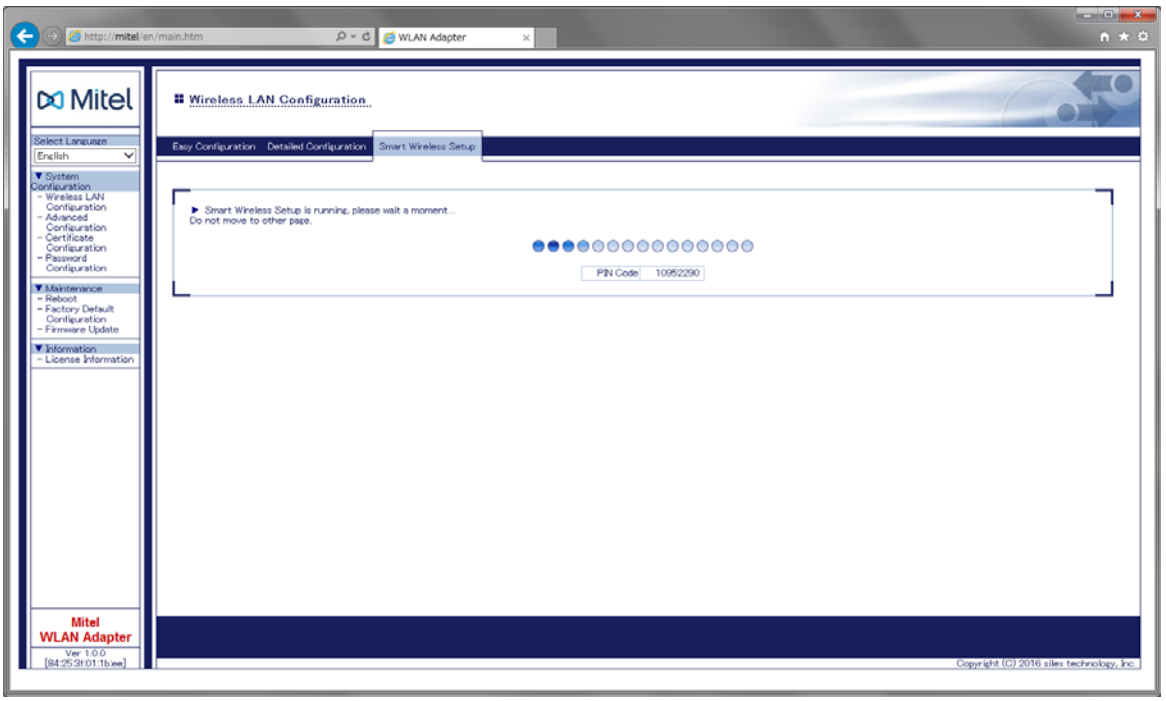


Figure 12: Smart Wireless Setup (PIN Code) is executed

If you move to another page while the Smart Wireless Setup is being executed, the operation becomes unstable.

Advanced Configuration page

The following settings are available on the Advanced Configuration page.

Table 11: Advanced Configuration

Item	Default	Available value
LAN Interface	AUTO	AUTO / 10BASE-T-Half / 10BASE-T-Full / 100BASE-TX-Half / 100BASE-TX-Full / 1000BASE-T- Full
Network Device Address	“”	MAC address
Client Mode	Multi-client mode	Single-client mode/ Multi-client mode

Table 12: TCP/IP Configuration

Item	Default	Available value
DHCP	DISABLE	ENABLE / DISABLE
IP Address	0.0.0.0	0.0.0.0 - 255.255.255.255
Subnet Mask	0.0.0.0	0.0.0.0 - 255.255.255.255
Default Gateway	0.0.0.0	0.0.0.0 - 255.255.255.255

Table 13: Push Switch Configuration

Item	Default	Available value
Time before turning into Configuration Mode	5	5 to 60
Time before starting Smart Wireless Setup	10	5 to 60

Note: The time difference between items must be 5 seconds or longer.

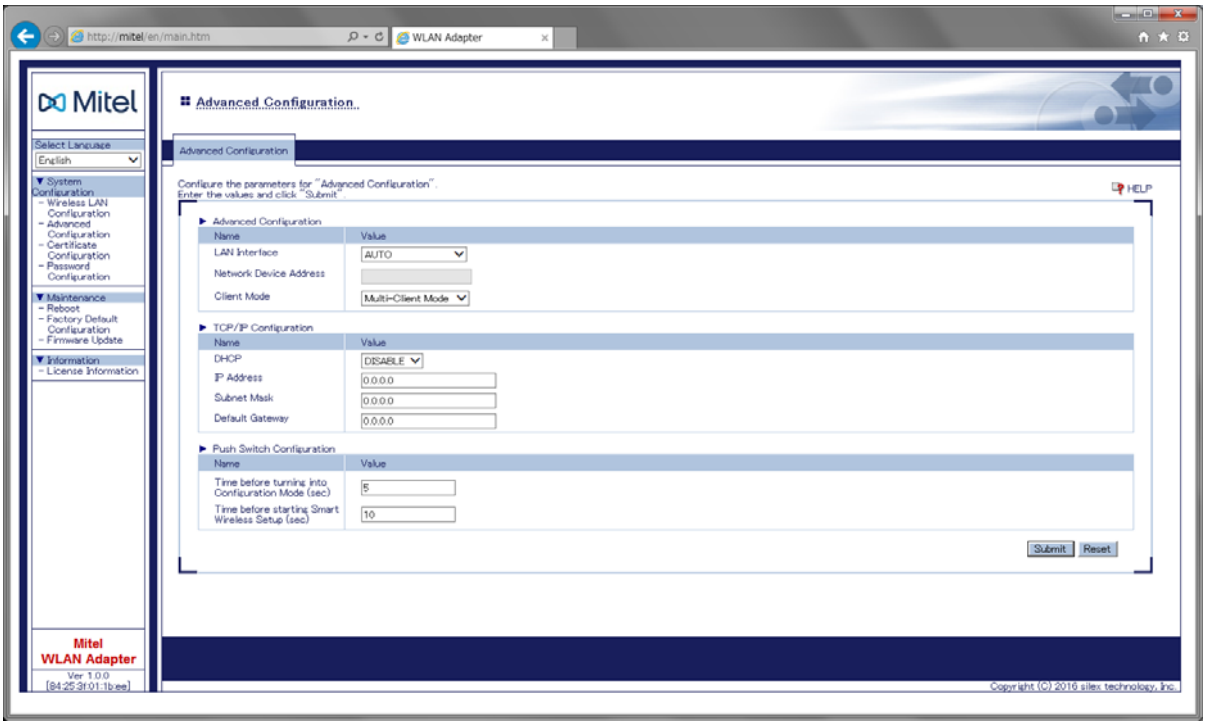


Figure 13: Advanced Configuration page

Certificate Configuration page

The following settings are available in the Certificate Configuration page.

Table 14: Client Certificate

Item	Default	Available value
Certificate File	“”	Client certification
Password	“”	1 to 32 characters

Table 15: CA Certificate

Item	Default	Available value
Certificate File	“”	CA certification

Table 16: PAC File

Item	Default	Available value
PAC File	“”	PAC file

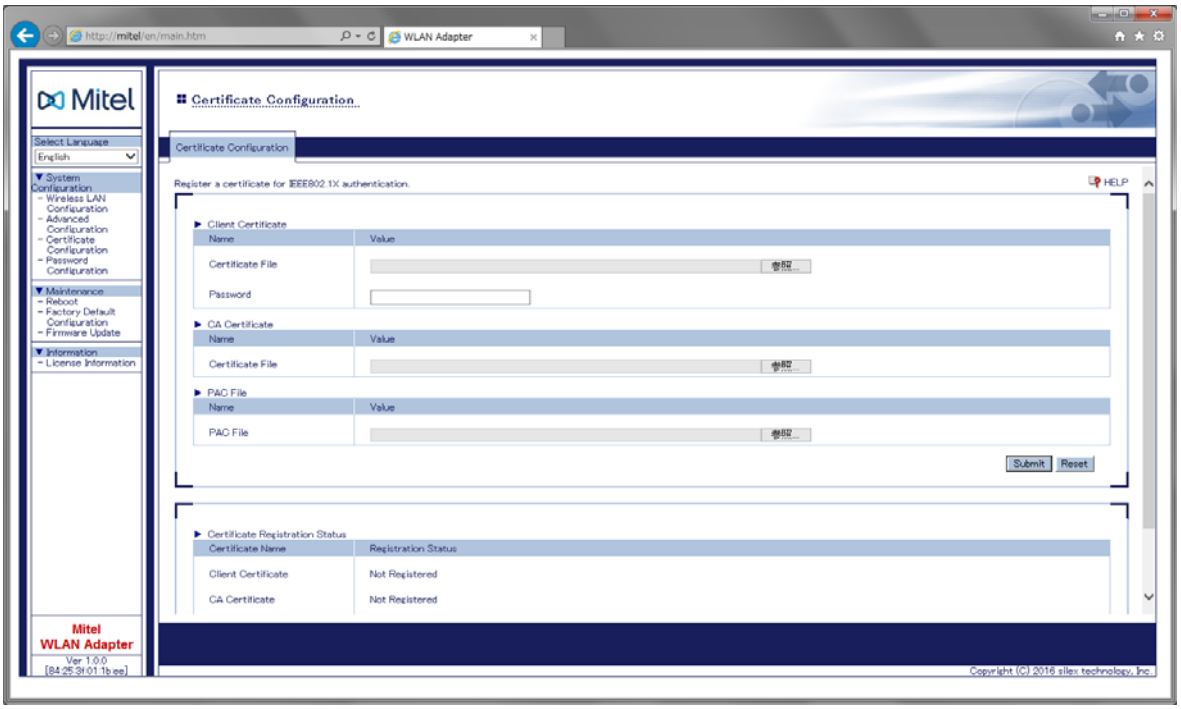


Figure 14: Certificate Configuration page

Password Configuration page

You can use the Password Configuration page to configure a password to access the product homepage.

Table 17: Password Configuration

Item	Default	Available value
New Password	“”	15 characters or less
Confirm New Password	“”	15 characters or less

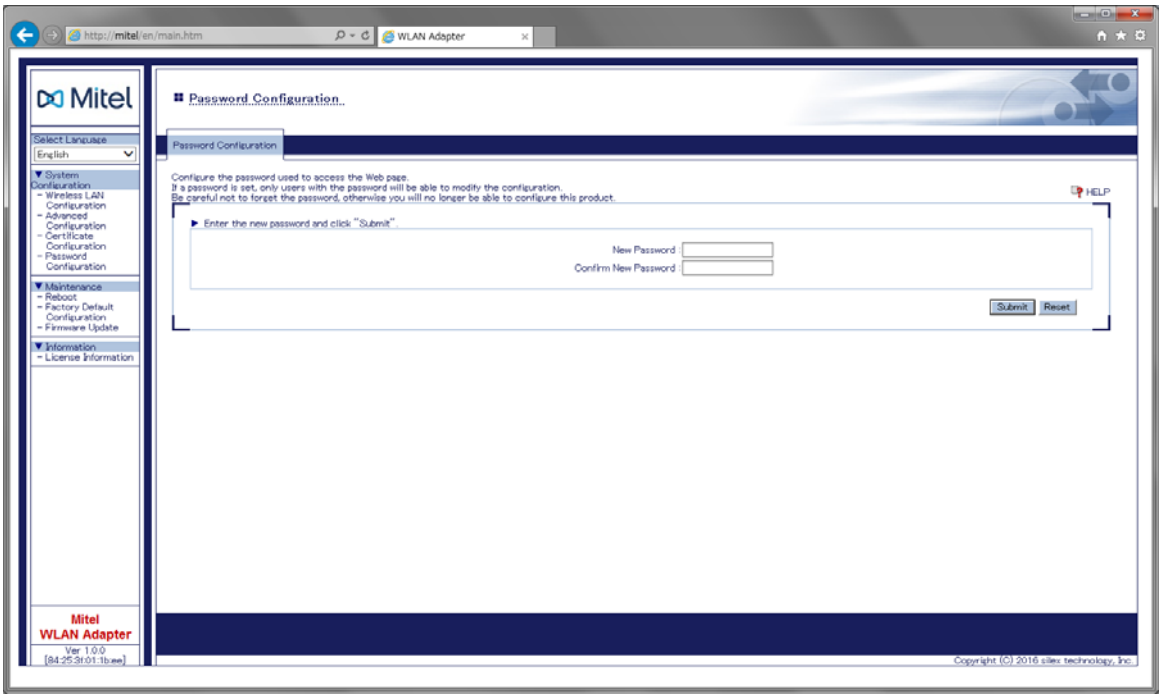


Figure 15: Password Configuration page

Reboot and initialize the Mitel WLAN Adapter

You can reboot the Mitel WLAN Adapter or restore factory default setting from the homepage.

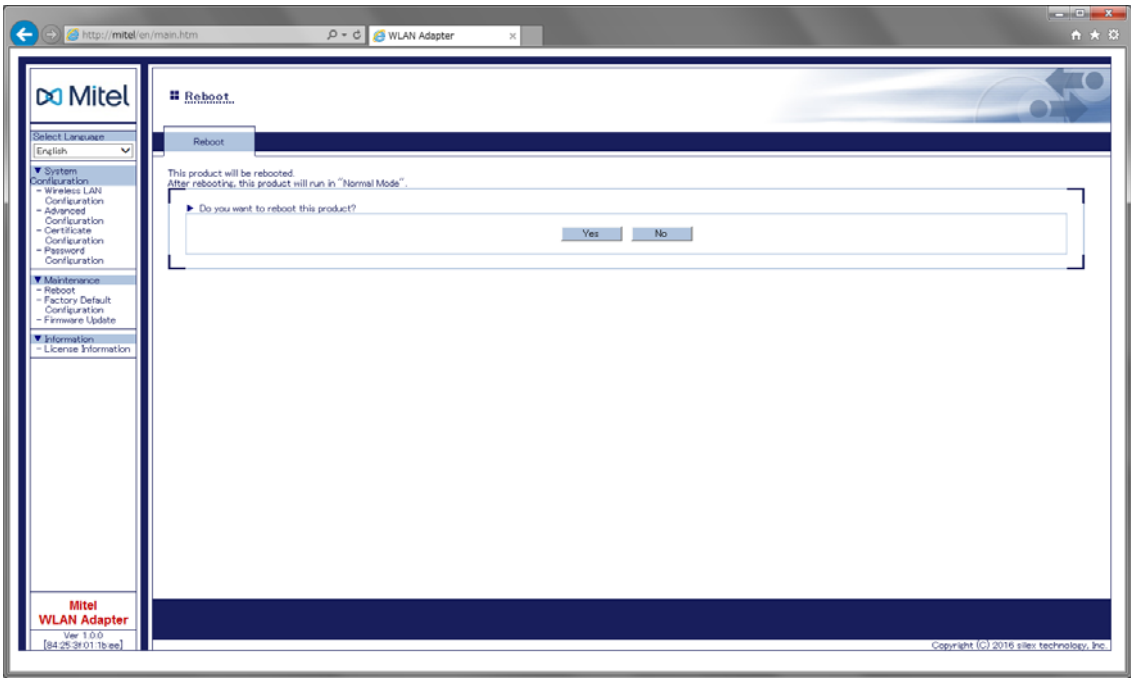


Figure 16: Reboot page

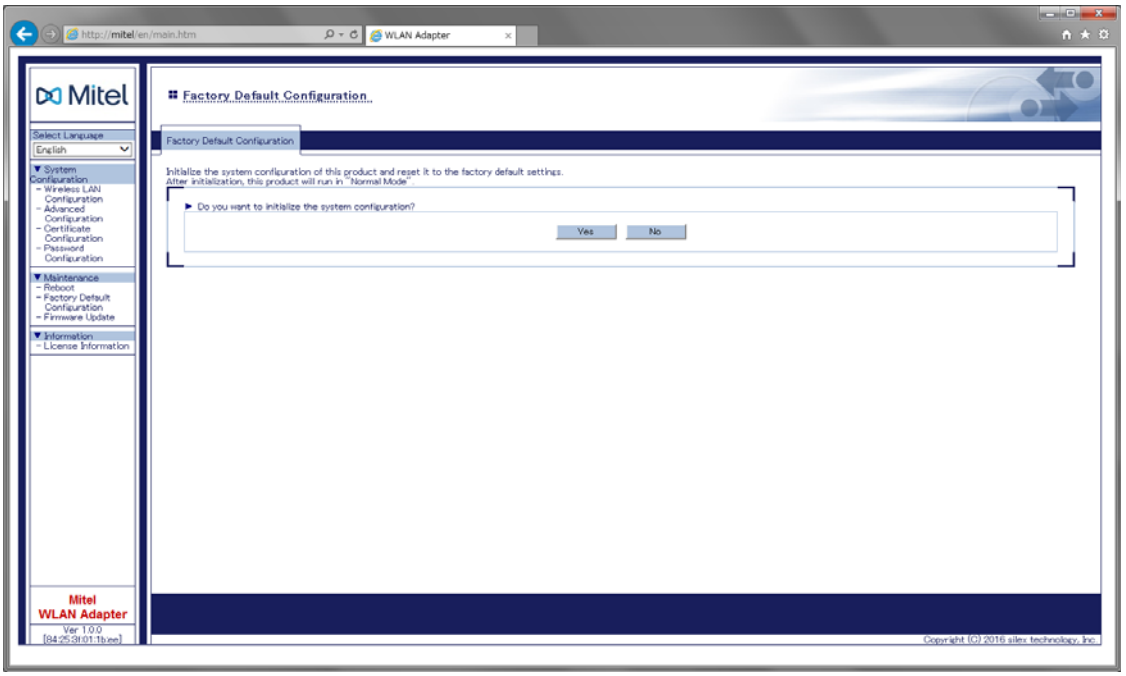


Figure 17: Factory Default Configuration page

License Information page

You can use the License Information page to view information about OpenSSL used for the Mitel WLAN Adapter.

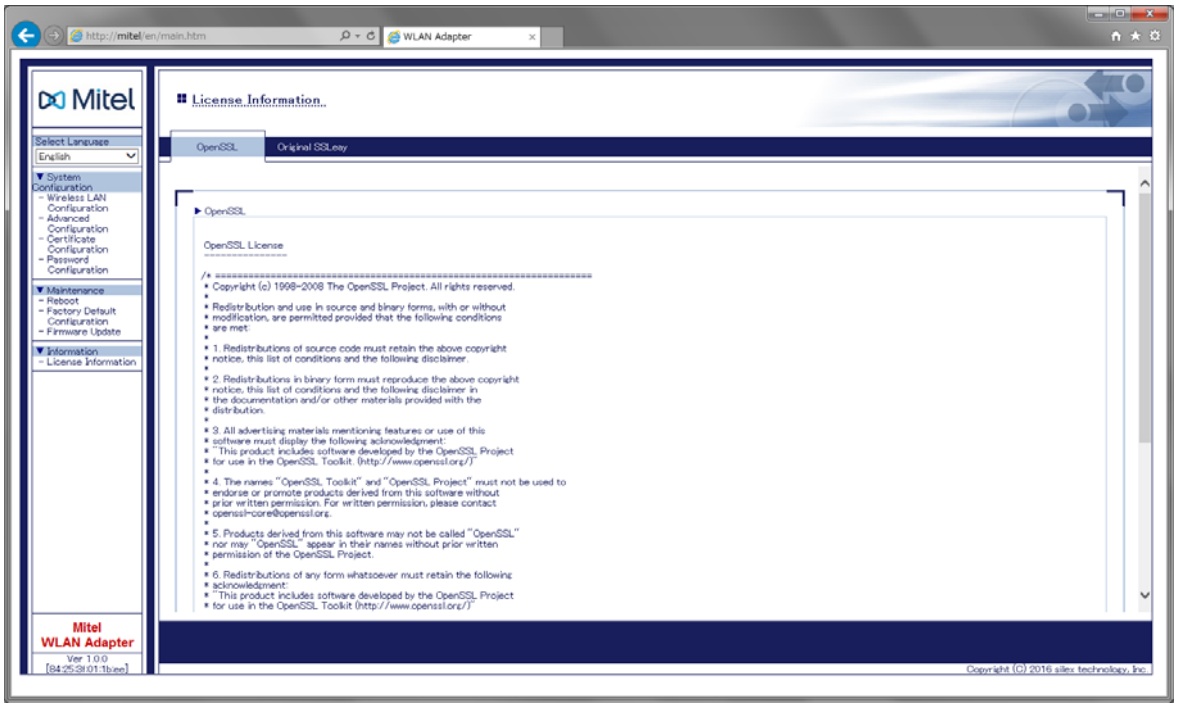


Figure 18: OpenSSL License page

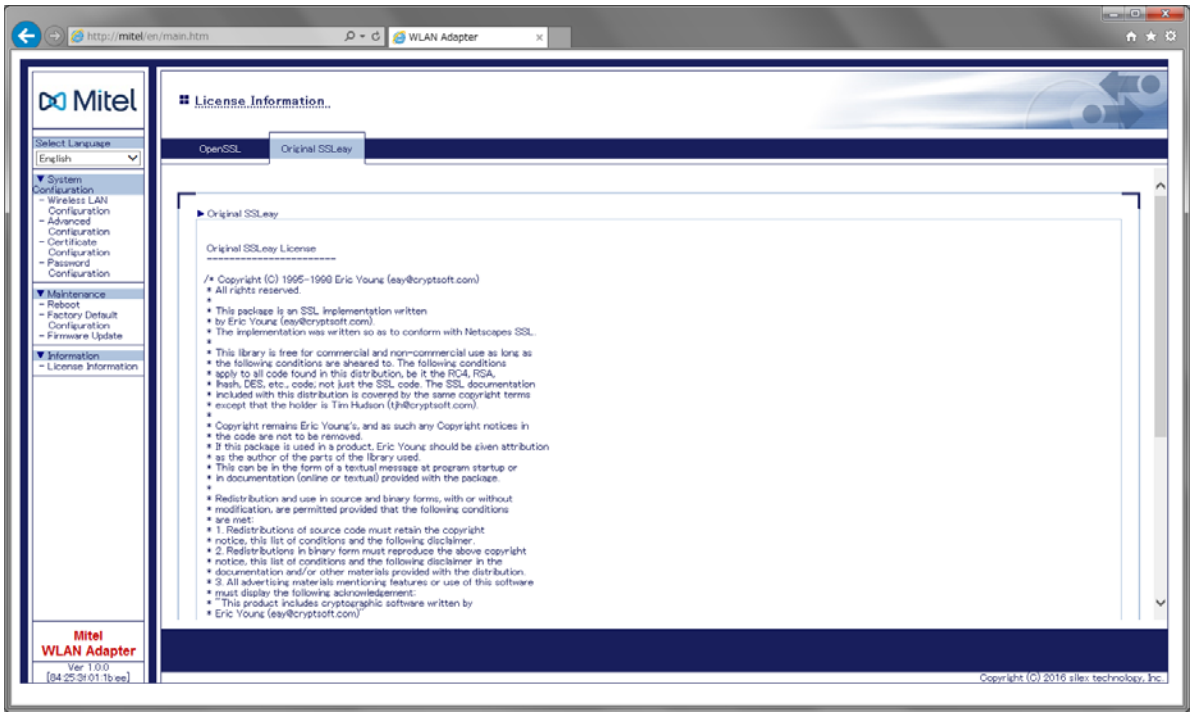


Figure 19: Original SSLeay License page

Help pages

Each system setting page has a link to **Help**. Click the link to view the help for the page.

Select the items from the list box for sub-menus.

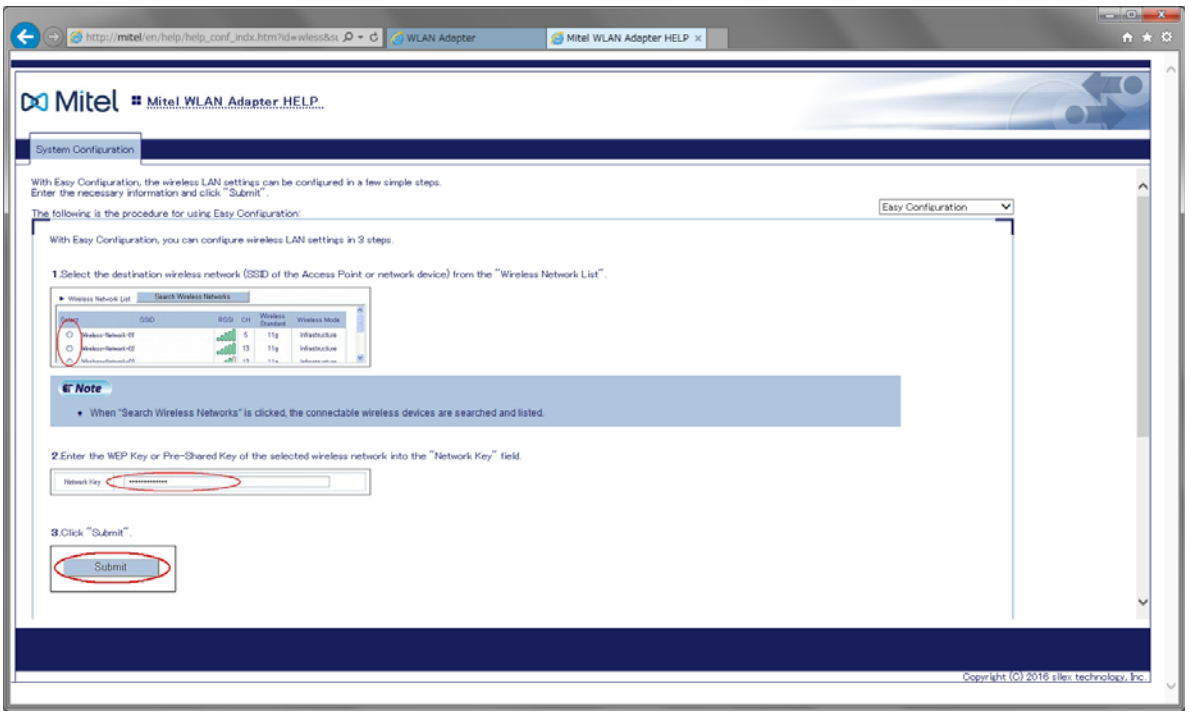


Figure 20: Help page

Product information

You can see the product name, firmware version and MAC address on the bottom-left of each page.

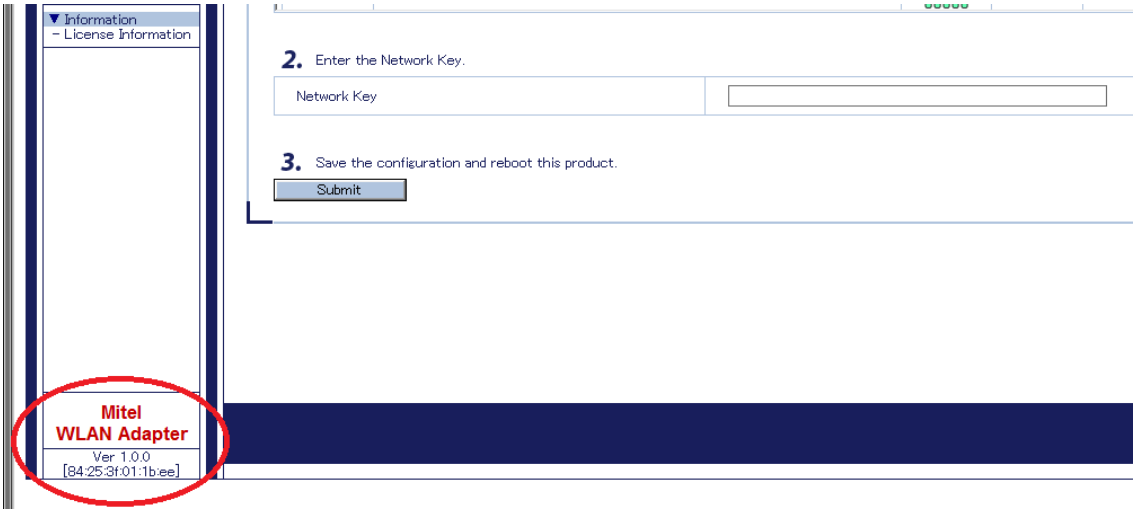


Figure 21: Product information

LED specifications

Following sections describe performance of LEDs on the Mitel WLAN Adapter.

Power on

When power is applied, the **Power** LED (Red) on the top enclosure is turned on. Until the MAC address is resolved for WLAN connection, **WLAN** LED (Green) and **STATUS** LED (Green) blinks at 1-second frequency.

Table 18: Standard operation mode

Location		Description
Top surface	Power	ON (Lighting up)
	WLAN	ON: Operating under Infra. Mode OFF: Operating under Ad Hoc mode
	STATUS	ON: Linking Flash: Receiving packets
Wired LAN connector	Link LED (Green)	ON: Wired LAN linking
	Status LED (Orange)	Flashes to receive packets while Link LED is ON

Table 19: Setting mode

Location		Description
Top surface	Power	ON
	WLAN	Fast blinking
	STATUS	

Table 20: Wired LAN port error

Location		Description
Top surface	Power	Blinking
	WLAN	OFF
	STATUS	ON

Table 21: Wireless module error

Location		Description
Top surface	Power	Blinking
	WLAN	ON
	STATUS	OFF

Push switch

The Mitel WLAN Adapter has one non-lock typed push button switch. The following table describes the push switch specifications.

Function	Operation
Startup with Setting mode	Turn on the switch when the device is on. Press and hold the switch for the period previously set (Setup mode shifting time, 5 seconds by default). Then the two Green LEDs (**WLAN** and **STATUS**) on the front flashes every 2 seconds to start the mode.
Start Smart Wireless Setup (Push-button)	Turn on the switch when the device is on. Press and hold the switch for the period previously set (Setup mode shifting time, 10 seconds by default). Then the **WLAN** LED on the front flashes every 1 second while the **STATUS** LED turns off to start the mode.
Restore factory setting	Push the switch down and power on the Mitel WLAN Adapter. The Greed LED for wired LAN connector illuminates. After 2 seconds, the LED changes to red. Then release the switch, and all configured data is deleted. The product is turned with factory default.
Startup with Production mode	Press the switch and power on the Mitel WLAN Adapter. When the Orange LED for wired LAN connector is turned on. Then release the switch in 2 seconds. The production mode starts.

Note: PushSW operation is disabled in the Setting mode.

IEEE802.1X authentication function

The Mitel WLAN Adapter supports IEEE802.1X authentication functions. A Remote Authentication Dial-In User Service (RADIUS) server is required for IEEE802.1X authentication.

Function structure

The following figure shows the network structure to use the IEEE802.1X authentication function.

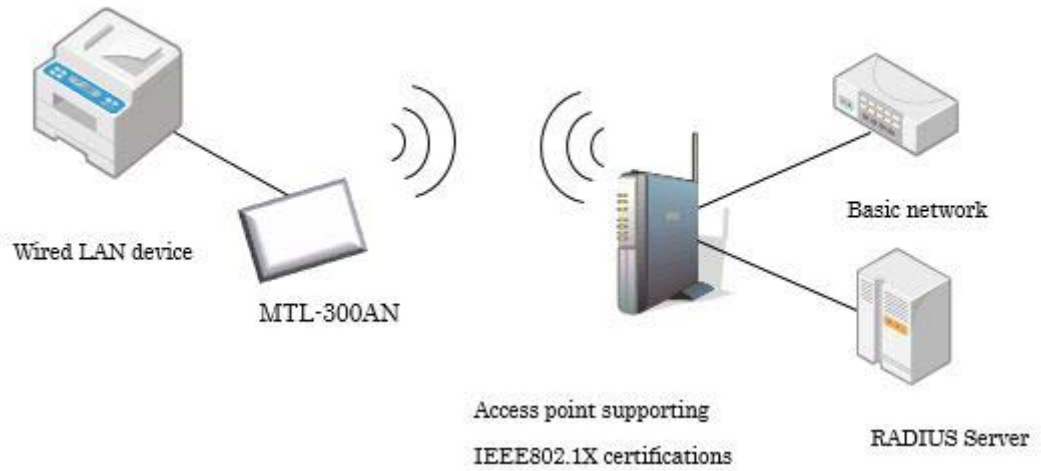


Figure 22: Figure22: IEEE802.1X authentication network structure

In the IEEE802.1X authentication network, the RADIUS server certifies 802.1X, and confirms authentication of the Mitel WLAN Adapter and the connected network by authenticating the RADIUS server. The certification is used to confirm each other's authentication. To use the IEEE802.1X authentication function, you require the necessary certification from the certificate authority, and then import the certificates to the RADIUS server and the Mitel WLAN Adapter beforehand.

The device to be connected to the Mitel WLAN Adapter wired LAN port must be identified for the IEEE802.1X authentication function. To identify devices, register the MAC address of connected devices to the Mitel WLAN Adapter.

Supported standards

IEEE802.1X authentication method

The Mitel WLAN Adapter supports the following IEEE802.1X authentication methods:

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

TLS tunneling encryption method

TLS tunneling supports the following encryption methods:

Encryption method	Key size
Triple-DES	192bit
DES	64bit
RC4	128bit

Certification specifications

The following table lists the available certifications:

Certificate	Item	Supported Specs
Client certificate	X509 Cert. version	v3
	Public key algorithm	RSA
	Public key size	512bit, 1024bit, 2048bit
	Signature algorithm	SHA1withRSA SHA224withRSA SHA256withRSA SHA384withRSA SHA512withRSA MD5withRSA
	X509v3 expanded key usage	Client authentication (1.3.6.1.5.5.7.3.2)
CA certificate	Public key algorithm	RSA
	Public key size	512bit, 1024bit, 2048bit
	Signature algorithm	SHA1withRSA SHA224withRSA SHA256withRSA SHA384withRSA SHA512withRSA MD5withRSA

Certification file format

The following table lists the supported file formats for certifications.

Item	Supported specs.
Client certificate	PKCS#12, pfx Includes a secret key of the certification.
CA certification for Server authentication	DER (Binary encoded X509) PEM (DER text format using BASE64 encoding)

802.1X authentication method

The following sections describes the main setting items for each authentication method.

EAP-TLS

Item	Description	Necessity
IEEE802.1X User name	ID for the server to identify a client.	Must
Client certificate	Used to confirm client's credibility	Must
Password	Used to confirm client's credibility	Must
CA certificate	CA certification to authenticate the server	Must

EAP-TTLS

Item	Description	Necessity
IEEE802.1X User name	ID for the server to identify a client.	Must
Password	Used by the server for client authentication.	Must
CA certificate	CA certification to authenticate the server	optional
Inner Authentication Method	Specifies an authentication protocol to use.	Must
Server Certificate Verification	Determines to conduct server credibility verification. If it is ON, a CA certification will be required for server certification examination.	Optional

PEAP

Item	Description	Necessity
IEEE802.1X User name	ID for the server to identify a client.	Must
Password	Used by the server for client authentication.	Must
CA Certificate	CA certification for server authentication.	Optional
Inner Authentication Method	Specifies an authentication protocol to use. "MSCHAPv2" is only available for PEAP.	Must
Server Certificate Verification	Determines to conduct server credibility verification. If it is ON, a CA certification will be required for server certification examination.	Optional

EAP-FAST

Item	Description	Necessity
IEEE802.1X User name	ID for the server to identify a client.	Must
Password	Used by the server for client authentication.	Must
PAC File	File created by the server and to be used for Manual Provisioning	Optional
PAC Auto-distribution	Determines to conduct auto distribution of PAC file. If it is OFF, a PAC file generated by the server will be required.	Optional

LEAP

Item	Description	Necessity
IEEE802.1X User name	ID for the server to identify a client.	Must
Password	Used by the server for client authentication.	Must

MAC address filtering function

To avoid security concerns, you must register MAC address of devices connected to the wired LAN port of the Mitel WLAN Adapter before using the IEEE802.1X authentication function. The

Mitel WLAN Adapter does not establish communication with IEEE802.1X-certified WLAN network if the MAC address of connected devices is not registered.

The number of MAC addresses that can be registered varies depending in the operation mode.

Operation mode	Number of filters
Single-client mode	1unit
Multi-client mode	Up to 16 units

> **Note:** The filter function is different from the **Connected Device Address** defined in the Advanced Setting page. If a MAC address is registered to the **Connected Device Address** in the Advanced Setting page. the same MAC address is automatically applied to Single-client mode, and the setting cannot be changed.

The following MAC address cannot be registered to the MAC address filter:

- Broadcast address
- Multicast address
- All "0" address
- Duplicated address (in the Multi-client mode only)

Setting item list

The following tables describe setting items and references for the Mitel WLAN Adapter.

Table 22: WLAN Basic Configuration

Setting item	Setting range	Default (Factory setting)
Operating Mode	Infra.	Infra
SSID	1 to 32 characters	SXxxxxxx "xxxxxx" is the last 6digits of MAC address)
SSID Filter	OFF / ON	OFF
Wireless Standard	AUTO / 2.4GHz / 5GHz	AUTO
Network Authentication	Open / Shared / WPA / WPA2 / WPA/WPA2 Mixed Mode	Open
IEEE802.1X Authentication	OFF / ON	OFF

Table 23: WEP Configuration

Setting item	Setting range	Default (Factory setting)
WEP	OFF / ON	OFF
Key Index	Selectable from the list box	1
WEP Key1	String of 5/10 (64bit) or 13/26 (128bit) characters	None
WEP Key2	String of 5/10 (64bit) or 13/26 (128bit) characters	None
WEP Key3	String of 5/10 (64bit) or 13/26 (128bit) characters	None
WEP Key4	String of 5/10 (64bit) or 13/26 (128bit) characters	None

Table 24: WPA/WPA2 Configuration

Setting item	Setting range	Default (Factory setting)
Encryption Mode	AES / AUTO	AES
Pre-Shared Key	8 to 64 characters	silex technology, Inc.

Table 25: IEEE802.1X Authentication Configuration

Setting item	Setting range	Default (Factory setting)
IEEE802.1X Authentication Type	EAP-TLS / EAP-TTLS / PEAP / EAP-FAST / LEAP	EAP-TLS

Table 26: Inner Authentication Method Configuration

Setting item	Setting range	Default (Factory setting)
Inner Authentication Method	PAP / CHAP / MSCHAP / MSCHAPv2	PAP

Table 27: Server Certificate Verification Configuration

Setting item	Setting range	Default (Factory setting)

Server Certificate Verification	OFF / ON	OFF

Table 28: IEEE802.1X User Configuration

Setting item	Setting range	Default (Factory setting)
IEEE802.1X User Name	Character string of 64 characters or less	None
Password	Character string of 32 characters or less	None

Table 29: EAP-FAST Configuration

Setting item	Setting range	Default (Factory setting)
PAC Auto-distribution	OFF / ON	OFF

Table 30: IEEE802.1X Network Device Configuration

Setting item	Setting range	Default (Factory setting)
Device Filter	OFF / ON	ON
Network Device Address	MAC address (up to 16 addresses for the Multi-client mode)	None

Table 31: Smart Wireless Setup

Setting item	Setting range	Default (Factory setting)
PIN code	Automatically generated with the button	Automatically generated value
Execution	- (Smart Wireless Execution button)	-

Table 32: Advanced Configuration

Setting item	Setting range	Default (Factory setting)
LAN Interface	AUTO / 10BASE-T-Half / 10BASE-T-Full / 100BASE-TX-Half / 100BASE-TX-Full / 1000BASE-T-Full	AUTO
Network Device Address	MAC address	None
Client Mode	Single-client mode/ Multi-client mode	Multi-client mode
IEEE802.11g Ad hoc Mode	OFF / ON	ON

Table 33: TCP/IP Configuration

Setting item	Setting range	Default (Factory setting)
DHCP	ENABLE / DISABLE	DISABLE
IP Address	0.0.0.0 - 255.255.255.255	0.0.0.0
Subnet Mask	0.0.0.0 - 255.255.255.255	0.0.0.0
Default Gateway	0.0.0.0 - 255.255.255.255	0.0.0.0

Table 34: Push Switch Configuration

Setting item	Setting range	Default (Factory setting)

Time before turning into Configuration Mode	5 to 60	5
Time before starting Smart Wireless Setup	5 to 60	10

Table 35: Client Certificate

Setting item	Setting range	Default (Factory setting)
Certificate File	Certification file to be used to authenticate the Mitel WLAN Adapter using the IEEE802.1X authentication function	None
Password	Password to get the secret key from the client certification (1 to 32 characters)	None

Table 36: CA Certificate

Setting item	Setting range	Default (Factory setting)
Certificate File	CA certification file to authenticate a certification sent by the RADIUS Server for the IEEE802.1X authentication function.	None

Table 37: PAC File

Setting item	Setting range	Default (Factory setting)
PAC File	PAC file generated by the server and is used to distribute PAC (Protected Access Credential) manually using EAP-FAST authentication method.	None

Table 38: Password Configuration

Setting item	Setting range	Default (Factory setting)
New password	String of 15 characters or less	None
Confirm New Password	String of 15 characters or less	None

Firmware update function

The Mitel WLAN Adapter uses a flash memory and allows users to update firmware.

You can update the firmware using any one of the following methods:

- Using homepage
- Using FLDP
- Using production mode

Firmware update using homepage

You can update the Mitel WLAN Adapter firmware from the homepage. Upload a binary file generated for a version upgrade. After the upgrade, the Mitel WLAN Adapter automatically restarts and the new firmware takes effect.

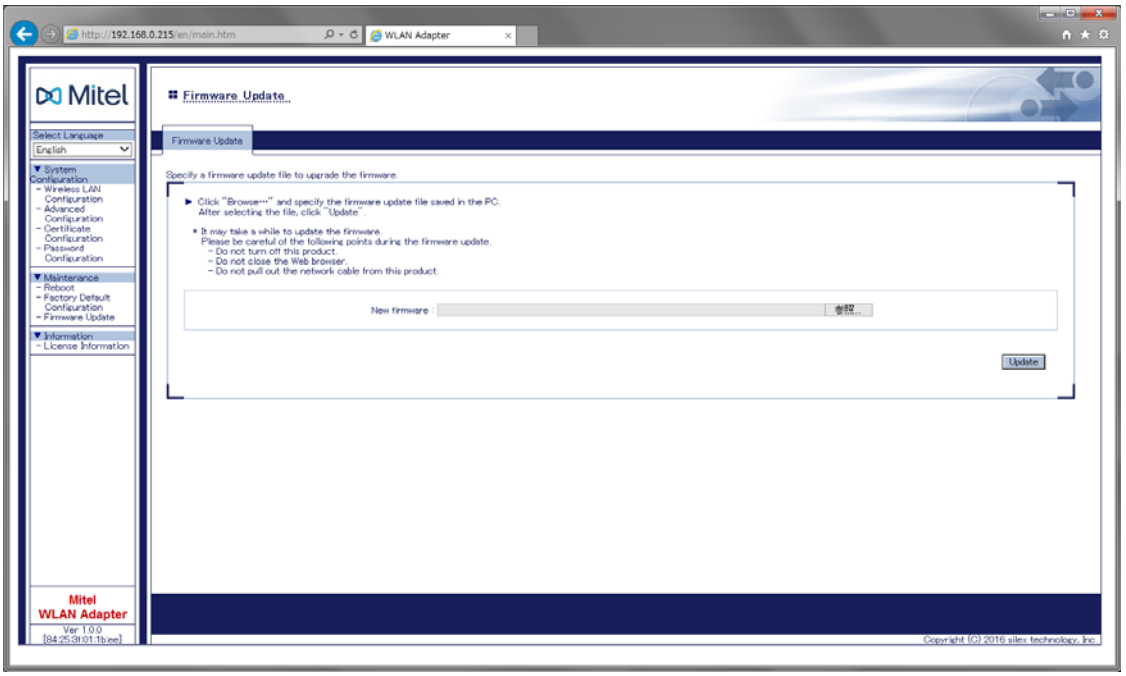


Figure 23: Firmware Update page

Firmware update using FLDP (Silex original protocol for firmware update)

The Mitel WLAN Adapter updates firmware using Silex original protocol (FLDP) through a PC connected to the wired LAN.

Upload data (Motorola S format) using a Silex's special version-upgrading tool, and the firmware is updated.

Firmware update using the production mode

The Mitel WLAN Adapter consists of both production and standard operation modes. The production mode is enabled when the firmware update fails during a standard operation mode. Use the push switch to activate the production mode when turning on the Mitel WLAN Adapter. Prepare a file image on the TFTP server, and FLDP updates firmware in the production mode.

Note: This mode can be used only in production.

kernel / roofts duplication function

You can use the kernel and roofts function as a fall-back to update the firmware in the event of a failure.

The following below describes the Flash ROM mapping the Mitel WLAN Adapter:

Offset	Size
0x00000000	Mtd0:uboot(512KB)
0x00080000	Mtd1:uboot-env(64KB)
0x00090000	Mtd2:reserved(448KB)
0x00100000	Mtd3:config0(512KB)
0x00180000	Mtd4:config1(512KB)
0x00200000	Mtd5:kernel1(3,072KB)
0x00500000	Mtd6:reserved(6,144KB)
0x00b00000	Mtd7:rootfs1(5,120KB)
0x01000000	Mtd8:kernel2(3,072KB)
0x01030000	Mtd9:rootfs2(5,120KB)
0x01800000	Mtd10:check_1(64KB)
0x01810000	Mtd11:check_2(64KB)
0x01820000	Mtd12:reserved(8064KB)

Smart wireless setup

This chapter explains how to set up WLAN with the smart wireless setup.

Set up the smart wireless

You can set up smart wireless using any one of the following ways:

- Push switch - Press each button of the access point and the client to set ESSID and security.
- PIN code - Use 8 digit PIN code to designate the client to set ESSID and security.

Set up smart wireless using the push switch

1. Start a WPS supported AP.
2. Start the product in normal operation mode.
3. Press the button on the AP to switch to PBC mode (for more information, refer the AP's handling manual)
4. Switch to smart wireless setup mode of the product.
   Press the push switch with the power on. After the pre-set time of the smart wireless setup time (10 seconds in default settings), the **WLAN** LED blinks rapidly and the **STATUS** LED is turned off. Then release the switch.
   - To return to the normal operation mode, press and hold the push switch for 5 seconds longer than the longer preset time of either the setup mode time or smart wireless time.
   - The smart wireless setup will not start until the MAC address for WLAN is resolved (the **WLAN** LED and the **STATUS** LED blinks rapidly)
5. Execute the smart wireless setup.
6. Setting is complete.

Notes:

1. When an AP is not detected in 120 seconds after the smart wireless setup (push switch) is started, timeout occurs to end the process (WPS). The **WLAN** LED blinks rapidly with the **STATUS** LED off. In 10 seconds, the AP returns to the normal operation mode.
2. When more than one WPS-PBC AP is detected, an error (overlap) occurs (WPS). The **WLAN** LED blinks four times (the **STATUS** LED is off). In 10 seconds, the AP returns to the normal operation mode.

Smart wireless setup (push switch) LED state

The following table provides the LED states for the smart wireless setup using the push switch method.

State	LED name	LED blinking patter (Filled cell means LED on. One cell is 0.25 sec.)	Time
Holding button (10–15 sec.)	Power		5 sec.
	WLAN		
	STATUS		
Processing	Power		120 sec.
	WLAN		
	STATUS		
Error / Timeout	Power		10 sec.
	WLAN		
	STATUS		
Overlap	Power		10 sec.
	WLAN		
	STATUS		

Note: The time for Switch Kept On above is the default value.

Set up smart wireless using the PIN code method

1. Start a WPS supported AP.
2. Start the product in normal operation mode.
3. Switch to the setup mode of the product.
4. Press the push switch with the power on. After the pre-set time of the setup time (5 seconds in default settings), the two **WLAN** LEDs (**WLAN** and **STATUS**) blinks rapidly to start the setup mode. Then release the switch.
    - To return to the normal operation mode, press and hold the push switch for 5 seconds longer than the longer preset time of either setup mode time or smart wireless time set up time.
5. In the web page, select **Wireless Setting** and then **Smart Wireless Setting** to view the PIN code.
6. Assign the PIN code to the AP and start WPS PIN on the AP (for more information, refer to the AP's handling manual)
7. In the web page, click **Smart Wireless Setup** to start smart wireless setting
8. Setting is complete.

Note: When an AP is not detected in 120 seconds after the smart wireless setup (pin code) is started, timeout occurs to end the process (WPS). The **WLAN** LED blinks rapidly with the **STATUS** LED off. In 10 seconds, the AP returns to the normal operation mode.

Smart wireless setting (PIN Code) LED state

The following table describe the LED states for the smart wireless setup using the PIN code method.

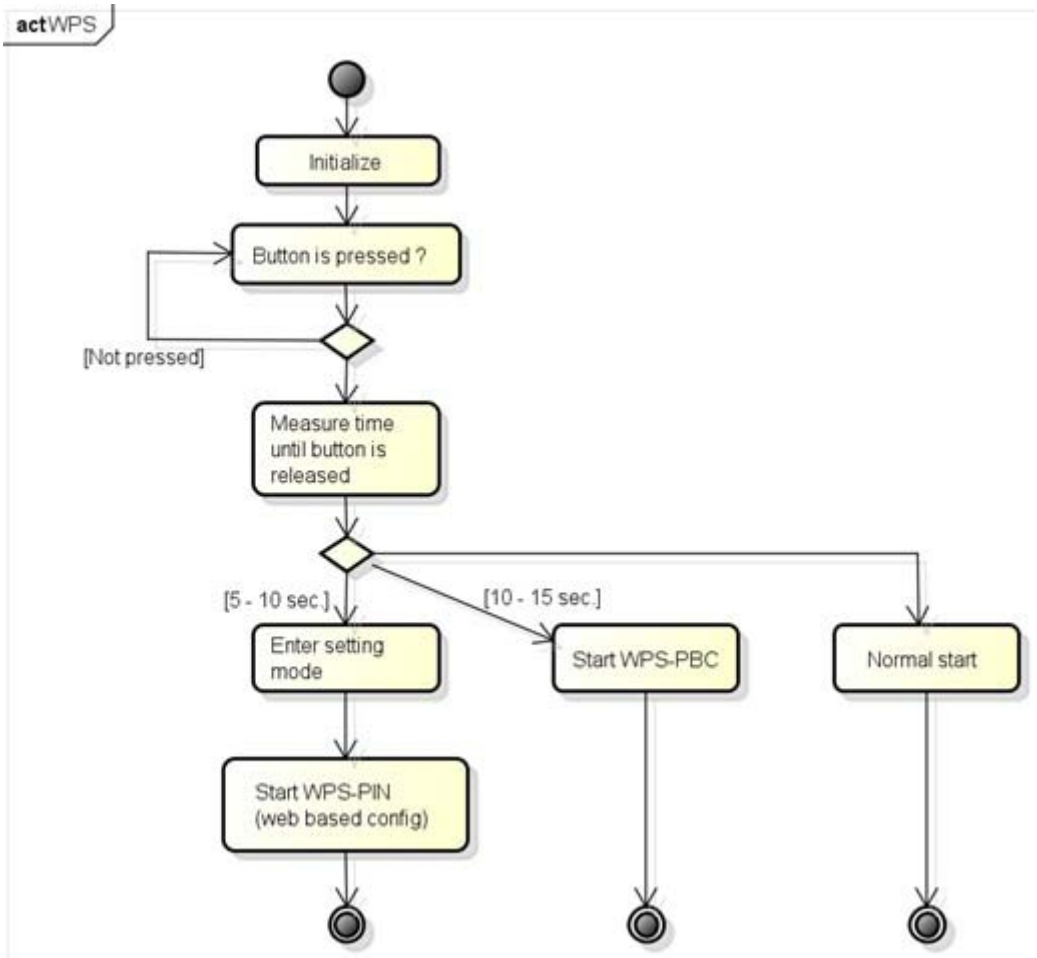
State	LED name	LED blinking patter (Filled cell means LED on. One cell is 0.25 sec.)	Time
Holding button (10–15 sec.)	Power		5 sec.
	WLAN		
	STATUS		
Processing	Power		120 sec.
	WLAN		
	STATUS		

> **Note:** The time for Switch Kept On above is the default value.

Smart wireless setting process flow

The following flowchart provides the steps to switch from normal operation mode to smart wireless setup (push switch or PIN code method).

> **Note:** The setup mode time and smart wireless setup time indicated in the below flowchart are of the default settings.


actWPS
Initialize
Button is pressed ?
[Not pressed]
Measure time until button is released
[5 - 10 sec.]
[10 - 15 sec.]
Enter setting mode
Start WPS-PBC
Normal start
Start WPS-PIN (web based config)

FLDP/BR

FLDP/BR is a protocol to exchange data between the product and the target device. This protocol is bridged to WLAN. The product consists the MAC address of the FLDP/BR frame sender.

The following functions are added to the Mitel WLAN Adapter's FLDP/BR:

- Get an AP list / Specify a connecting AP.
- The IP phone specifies a connecting AP from the list.
- Security
- Does not allow control by any device except by the connected IP phone.
- Get signal strength.
- Provides signal strength from the AP in grades.
- Tell disconnection.
- Tell disconnection to the IP phone.

Configure Wi-Fi SSID on MiVoice IP phones

The Mitel MiVoice 6900 series IP phones allow you to connect to a Wi-Fi network through IP phone settings when connected to a Mitel WLAN adapter.

For details, refer to the *Mitel Wireless LAN Adapter Setup Guide* or the model specific *MiVoice IP Phone User Guide*.

> **Note:** When the WLAN adapter is connected to a MiVoice 6930 or 6940 IP phone, the DHCP discovery interludes at approximately 30 seconds and the Wi-Fi settings menu displays on the phone.

© Copyright 2017, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation, including itself and subsidiaries and authorized entities. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.