The Series of Realtek 8XXX-SOC
Wi-Fi Protected Setup
User Guide V1.8

Change History

version	Date	Remark
1.5	2011/8/4	Add description about WPS2.0 at chapter6
1.6	2011/08/26	Add description about new feature of client mode at chapter7
1.7	2012/03/01	Add description about PIN code brute force attack mitigation
1.8	2012/05/03	Add parameter UPC(Universal Product Code)

1. Introduction

1.1 Purpose

This document describes supported WPS features of the series of Realtek 8xxx-SOC, the instructions of setting up a Wi-Fi network for different scenarios, and the recommended system configuration.

1.2 Scope

This document is aimed to the engineers who have basic knowledge about WPS and will utilize Realtek 8xxx-SDK to develop their products.

1.3 Definitions of Wi-Fi Protected Setup terminologies

(Wi-Fi Protected Setup Specification 1.0h.pdf, p. 11)

WPS: Stands for Wi-Fi Protected Setup; an optional certification program designed to ease set up of security-enabled Wi-Fi networks in the home and small office environment.

Device: An independent physical or logical entity capable of communicating with other Devices across a LAN or WLAN.

Domain: A set of one or more Devices governed by a common authority for the purpose of gaining access to one or more WLANs.

Enrollee: A Device seeking to join a WLAN Domain. Once an Enrollee obtains a valid credential, it becomes a Member.

In-band: Data transfer using the WLAN communication channel.

Out-of-band: Data transfer using a communication channel other than the WLAN

Member: A WLAN Device possessing Domain credentials.

Registration Protocol: A Registration Protocol is a (logically) three party in-band protocol to assign a Credential to the Enrollee. The protocol operates between the Enrollee and the Registrar and may receive support through a proxy. In this document, it is equivalent to “WPS handshake”.

Registrar: An entity with the authority to issue and revoke Domain Credentials. A registrar may be integrated into an AP, or it may be separate from the AP. A registrar may not have WLAN capability. A given Domain may have multiple registrars.

External Registrar: A registrar for an AP’s Domain that runs on a device separate

from the AP.

PushButton Configuration (PBC): A configuration method triggered by pressing a physical or logical button on the Enrollee and on the Registrar.

PIN Configuration: Unique 4- or 8-digit PIN required for each device on the network. PIN is entered into Registrar via a graphical user interface.

WLAN: A Wi-Fi network.

Credential: A data structure issued by a Registrar to an Enrollee, allowing the latter to gain access to the network. For examples, It contains SSID and security settings.

Proxy: The AP can work as a proxy to convey the messages between external registrar and enrollee.

Un-configured State: By default, Realtek 8xxx-SOC will stay in this state when it is shipped from the factory. The SSID is assigned a default value and the security is set to open.

Configured State: In Realtek 8xxx-SOC platform, if it is in un-configured state and the SSID or security is manually changed, or the registration protocol is successfully done, it will switch to this state.

Multiple PBC Sessions: Push Button Configuration is inherently unsecured due to the PIN is 00000000. As a result, only one pair of registrar and enrollee is allowed to initiate the WPS handshake at any time. Any WPS AP should detect whether there is more than one station that starts PBC before the handshake. Similarly, any WPS station should detect whether there is more than one AP that starts PBC. If any side of AP or station detects multiple PBC sessions, it should guide users to use other secure methods such as PIN Configuration.

1.4 Introduction of WPS

Although home Wi-Fi networks have become more and more popular, users still have trouble with the initial set up of network. This obstacle forces users to use the open security and increases the risk of eavesdropping. Therefore, WPS is designed to ease set up of security-enabled Wi-Fi networks and subsequently network management (Wi-Fi Protected Setup Specification 1.0h.pdf, p. 8).

The largest difference between WPS-enabled devices and legacy devices is that users do not need the knowledge about SSID, channel and security settings, but they could still surf in a security-enabled Wi-Fi network. For examples, in the initial network set up, if users want to use the PIN configuration, the only thing they need to do is entering the device PIN into registrar, starting the PIN method on that device and simply wait until the device joins the network. After the PIN method is started on both sides, a registration protocol will be initiated between the registrar and the

enrollee. Typically, a registrar could be an access point or other device that is capable of managing the network. An enrollee could be an access point or a station that will join the network. After the registration protocol has been done, the enrollee will receive SSID and security settings from the registrar and then join the network. In other words; if a station attempts to join a network managed by an access point with built-in internal registrar, users will need to enter station's PIN into the web page of that access point. If the device PIN is correct and valid and users start PIN on station, the access point and the station will automatically exchange the encrypted information of the network settings under the management of AP's internal registrar. The station then uses this information to perform authentication algorithm, join the secure network, and transmit data with the encryption algorithm. More details will be demonstrated in the following sections.

2. Supported WPS features

Currently, the series of Realtek 8xxx-SOC supports WPS features for AP mode, AP+WDS mode, Infrastructure-Client mode, and the wireless root interface of Universal Repeater mode. Other modes such as WDS mode, Infrastructure-Adhoc mode, and the wireless virtual interface of Universal Repeater mode are not implemented with WPS features.

If those unsupported modes are enforced by users, WPS will be disabled. Under the configuration of every WPS-supported mode, the series of Realtek 8xxx-SOC has Push Button method and PIN method. For each method, it offers different security levels included in network credential, such as open security, WEP 64 bits, WEP 128 bits, WPA-Personal TKIP, WPA-Personal AES, WPA2-Personal TKIP, and WPA2-Personal AES. Users could choose either one of the methods at their convenience.

2.1 AP mode

For AP mode, the series of Realtek 8xxx-SOC supports three roles, registrar, proxy, and enrollee in registration protocol. At different scenarios, it will automatically switch to an appropriate role depending on the other device's role or a specific configuration.

2.1.1 AP as Enrollee

If users know AP's PIN and enter it into external registrar, the external registrar will configure AP with a new wireless profile such as new SSID and new security settings. The external registrar does this job either utilizing the in-band EAP (wireless) or out-of-band UPnP (Ethernet). During the WPS handshake, a wireless profile is encrypted and transmitted to AP. If the handshake is successfully done, AP will be re-initialized with the new wireless profile and wait for legacy stations or WPS stations to join its network.

2.1.2 AP as Registrar

The series of Realtek 8xxx-SOC also has a built-in internal registrar. Whenever users enter station's PIN into AP's webpage, click "Start PBC", or push the physical button, AP will switch to registrar automatically. The PBC event will trigger to wlan0

if the pressed time of physical button less than “button_hold_time_for_first_if” in wscd.conf and and initiate a WPS session on wlan0, the PBC event will trigger to wlan1 if the pressed time of physical button more than “button_hold_time_for_first_if” and initiate a WPS session on wlan1. If users apply the same method on station side and the WPS handshake is successfully done, SSID and security settings will be transmitted to that station without the risk of eavesdropping. And then the station will associate with AP in a security-enabled network.

2.1.3 AP as Proxy

At this state, AP is transparent to users. If users want to configure a station or any device that is capable of being an enrollee, they have to enter device’s PIN into an external registrar and choose an appropriate wireless profile. After the PIN is entered, the external registrar will inform AP this event. AP then conveys the encrypted wireless profile between the device and the external registrar. Finally, the device will use the wireless profile and associate with AP. However, the device may connect to other APs if the wireless profile does not belong to the proxy AP. Users must carefully choose the wireless profile or create a wireless profile on an external registrar.

2.2 Infrastructure-Client mode

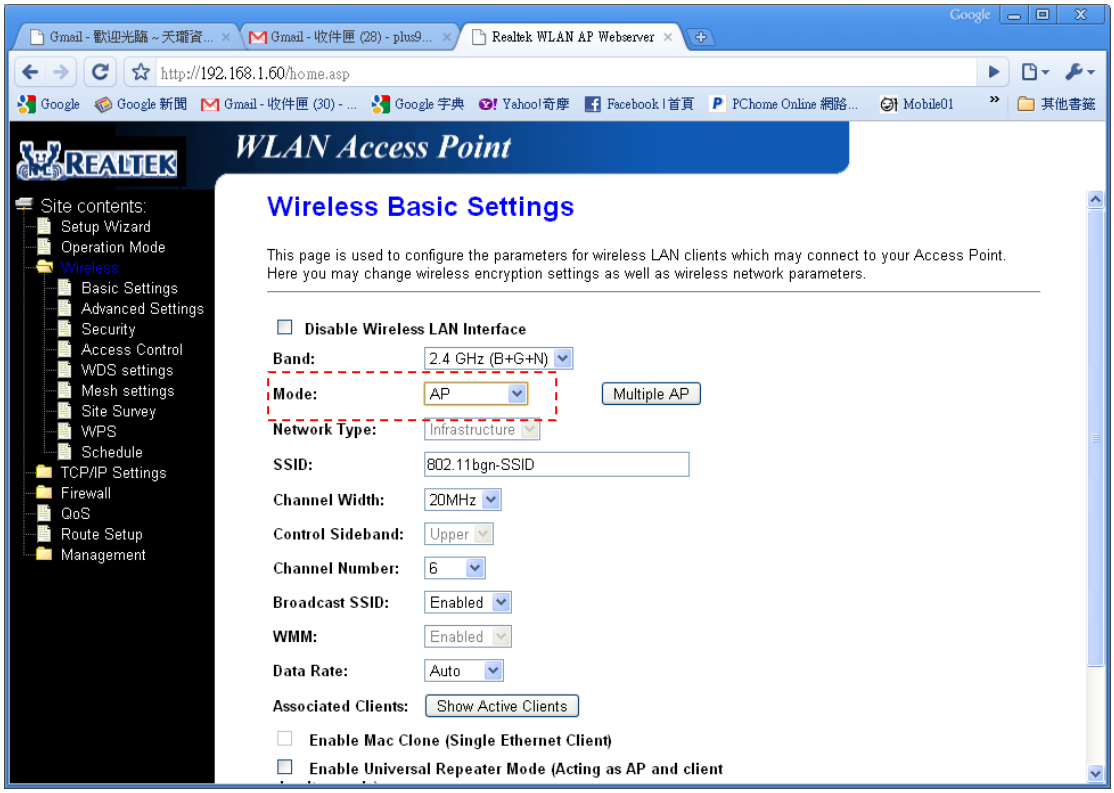
In Infrastructure-Client mode, the series of Realtek 8xxx-SOC only supports enrollee’s role. If users click “Start PIN”, click “Start PBC”, or press the physical button on 8xxx-SOC, it will start to seek WPS AP. The PBC event will trigger to wlan0 if the pressed time of physisical button less than “button_hold_time_for_first_if” in wscd.conf and and initiate a WPS session on wlan0, the PBC event will trigger to wlan1 if the pressed time of physical button more than “button_hold_time_for_first_if” and initiate a WPS session on wlan1. Once users apply the same method on registrar side, 8xxx-SOC will receive the wireless profile upon successfully doing the registration protocol. Then 8xxx-SOC will associate with an AP.

3. Instructions of AP’s and Client’s operations.

3.1 Introduction of AP’s webpages

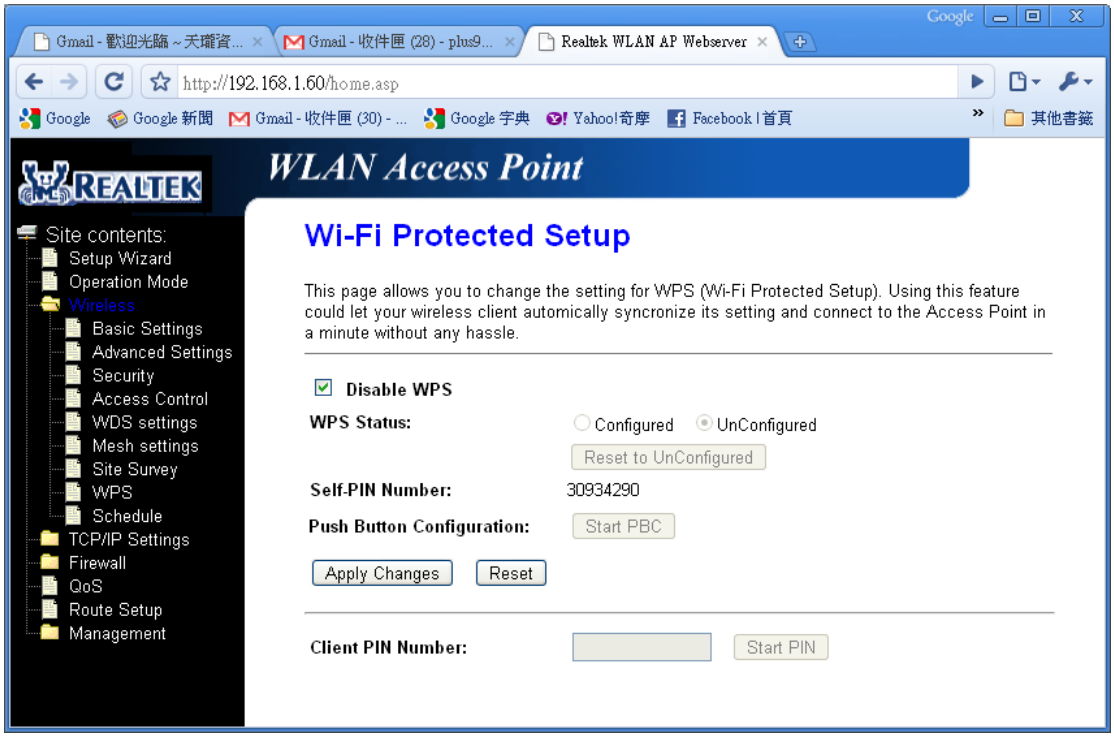
3.1.1 Wireless Basic Settings page

The instructions of operating WPS in AP mode, AP+WDS mode, and Universal Repeater mode are the same. Therefore, only AP mode will be demonstrated in this section and AP will represent those three modes hereafter. However, users could freely switch between those supported modes by selecting the pull-down menu next to “Mode” or check the box “Enable Universal Repeater Mode (Acting as AP and client simultaneously)” and click “Apply Changes” on Wireless Basic Settings page. Please see the figure below.



3.1.2 Wi-Fi Protected Setup page

The following sub-paragraphs will describe the function of each item. The webpage is as below.



3.1.2.1 Disable WPS

Checking this box and clicking “Apply Changes” will enable Wi-Fi Protected Setup. WPS is turned off by default.

3.1.2.2 WPS Status

When AP’s settings are factory default (out of box), it is set to open security and un-configured state. It will be displayed by “WPS Status”. If it already shows “Configured”, some registrars such as Vista WCN will not configure AP. Users can click “Reset to Unconfigured ” to reload factory default settings.

3.1.2.3 Self-PIN Number

“Self-PIN Number” is AP’s PIN. Whenever users want to change AP’s PIN, they could click “Regenerate PIN” and then click “ Apply Changes”. Moreover, if users want to make their own PIN, they could enter four digit PIN without checksum and then click “ Apply Changes”. However, this would not be recommended since the registrar side needs to be supported with four digit PIN.

3.1.2.4 Push Button Configuration

Clicking this button will invoke the PBC method of WPS. It is only used when AP acts as a registrar.

3.1.2.5 Apply Changes

Whenever users want to enable/disable WPS or change AP's PIN, they need to apply this button to commit changes.

3.1.2.6 Reset

It restores the original values of "Self-PIN Number" and "Client PIN Number".

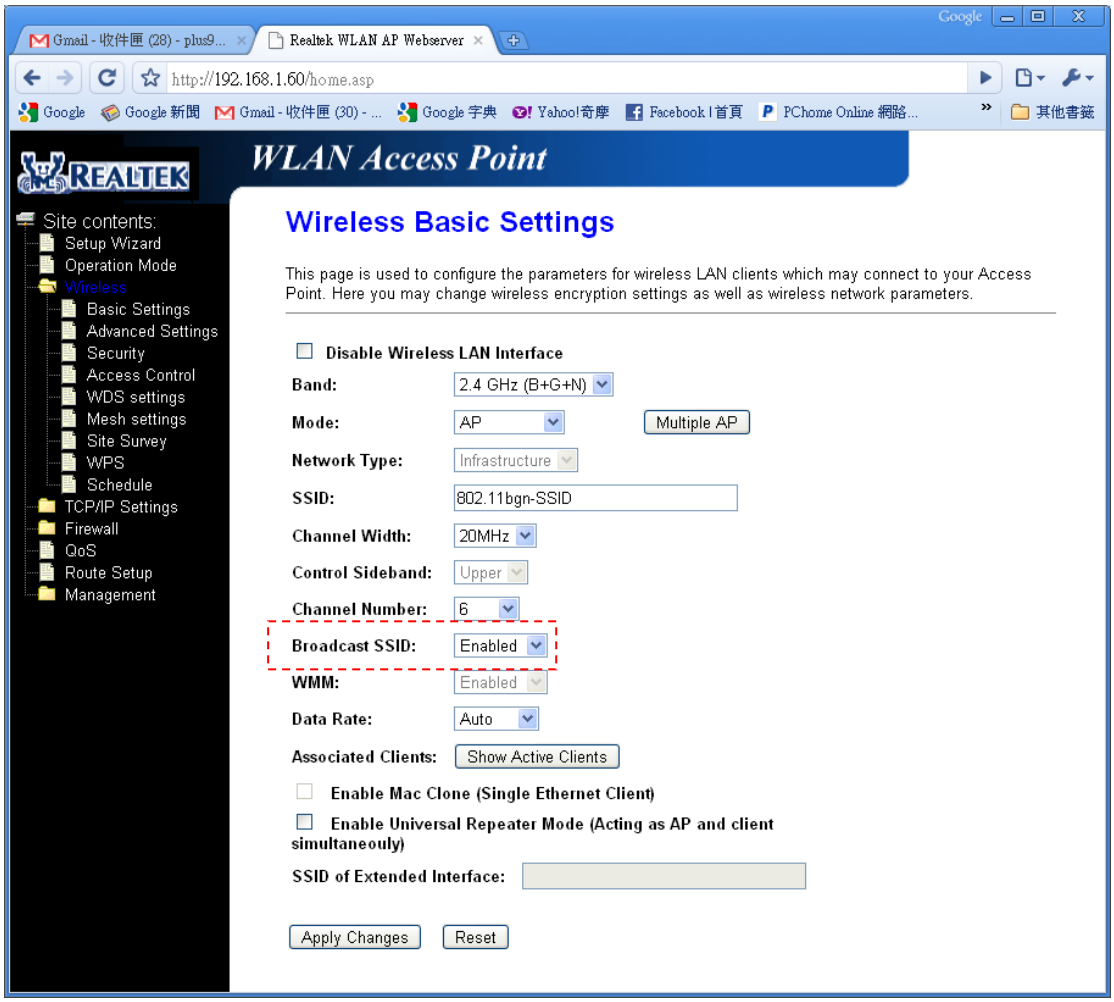
3.1.2.7 Client PIN Number

It is only used when users want their station to join AP's network. The length of PIN is limited to four or eight numeric digits. If users enter eight digit PIN with checksum error, there will be a warning message popping up.

If users insist on this PIN, AP will take it.

3.1.3 Wireless Basic Settings page

Users need to make sure the "Broadcast SSID" file is set to "Enabled". Otherwise, it might prevent WPS from working properly.


Realtek WLAN AP Webserver
http://192.168.1.60/home.asp
WLAN Access Point
Site contents:
Setup Wizard
Operation Mode
Wireless
Basic Settings
Advanced Settings
Security
Access Control
WDS settings
Mesh settings
Site Survey
WPS
Schedule
TCP/IP Settings
Firewall
QoS
Route Setup
Management
Wireless Basic Settings
This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.
Disable Wireless LAN Interface
Band: 2.4 GHz (B+G+N)
Mode: AP
Multiple AP
Network Type: Infrastructure
SSID: 802.11bgn-SSID
Channel Width: 20MHz
Control Sideband: Upper
Channel Number: 6
Broadcast SSID: Enabled
WMM: Enabled
Data Rate: Auto
Associated Clients: Show Active Clients
Enable Mac Clone (Single Ethernet Client)
Enable Universal Repeater Mode (Acting as AP and client simultaneouly)
SSID of Extended Interface:
Apply Changes
Reset

3.2 Operations of AP

3.2.1 AP being an enrollee

In this case, AP will be configured by any registrar either through in-band EAP or UPnP. Here, users do not need to do any action on AP side. They just need AP's device PIN and enter it into registrar. An example from Vista WCN will be given.

1. Make sure AP is in un-configured state. (Figure 3.1)

Figure 3.1

2. Plug the Ethernet cable into AP's LAN port and make sure the IP connection is valid with Vista.

3. Make sure WCN is enabled. Users may need to enable it at the first time. They could open the "Control Panel", open "Administrative Tools", double click "Services", edit properties of "Windows Connect Now", choose the "Startup type" with "Automatic" and click "Start". (Figure 3.2)

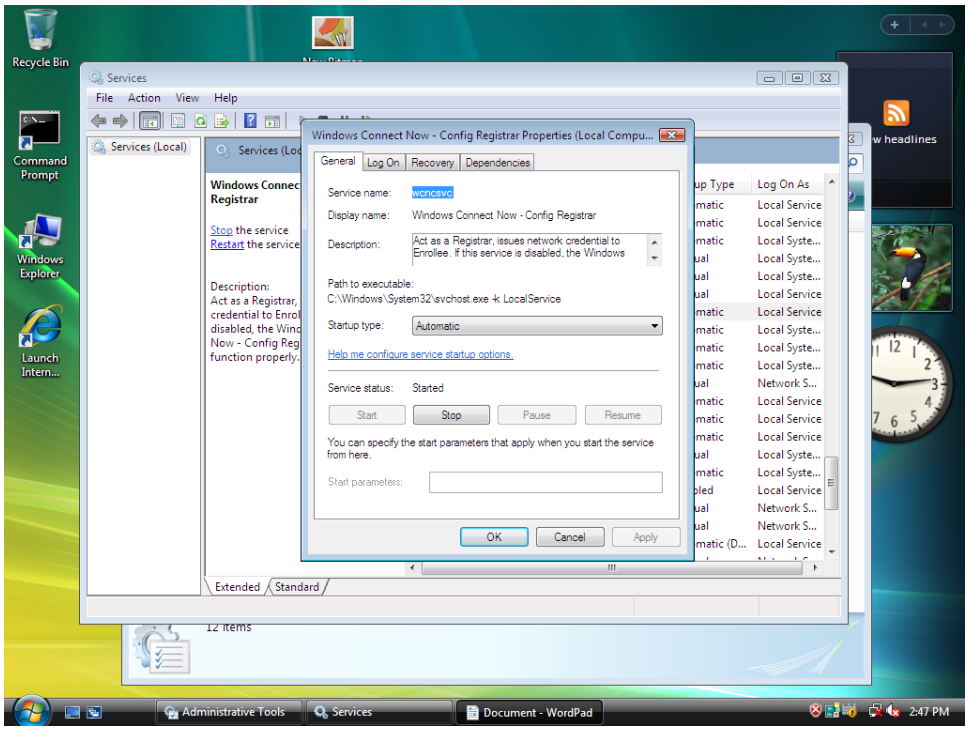


Figure 3.2

4. If the previous steps are done, open Windows Explorer. Go to the Network section. Right-click mouse and select Refresh, and AP's icon will show up. Double click on it. Users could also Click "Add a wireless device" if the icon is not there. Click "next". (Figure 3.3)

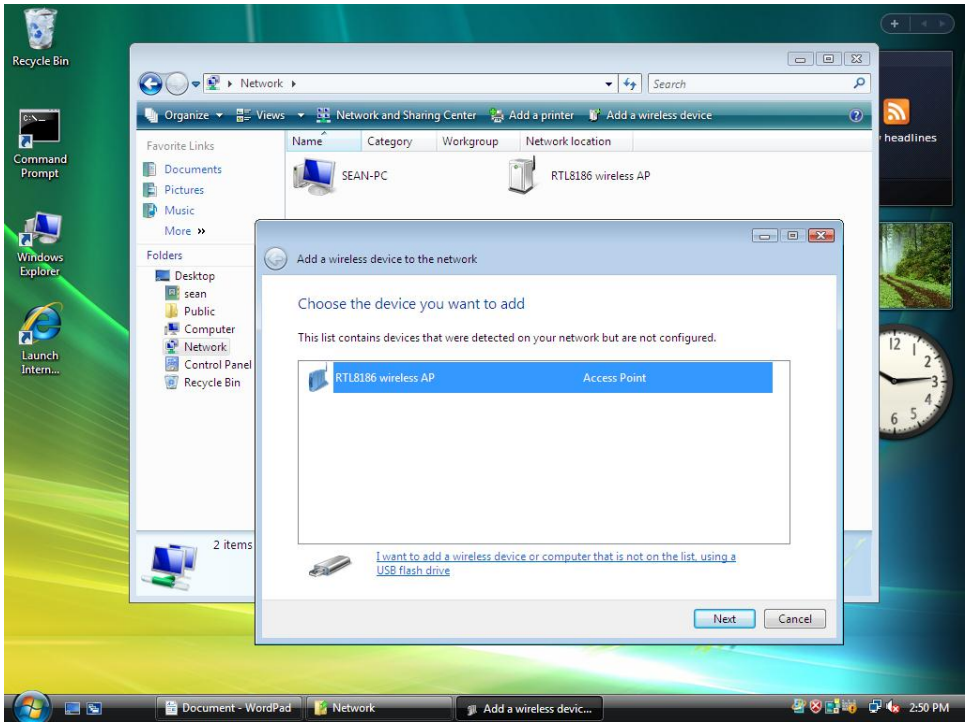


Figure 3.3

5. Enter AP's PIN (Self-PIN Number in Figure 3.1) and click "next". (Figure 3.4)

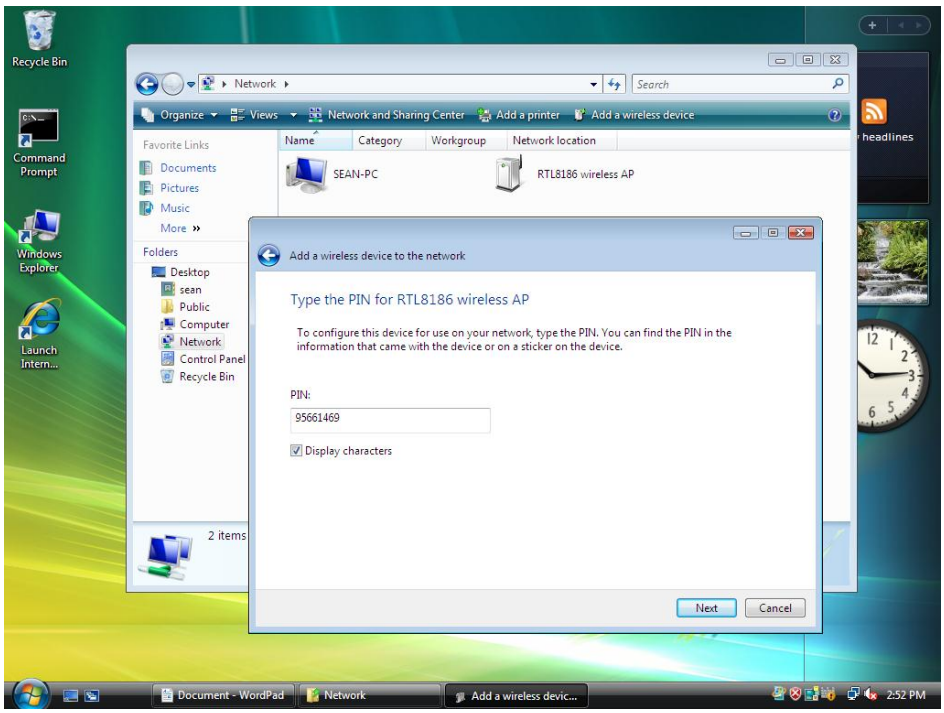


Figure 3.4

6. Select a wireless profile or Click "Create a new Wireless Network Profile". Click "next" (Figure 3.5)

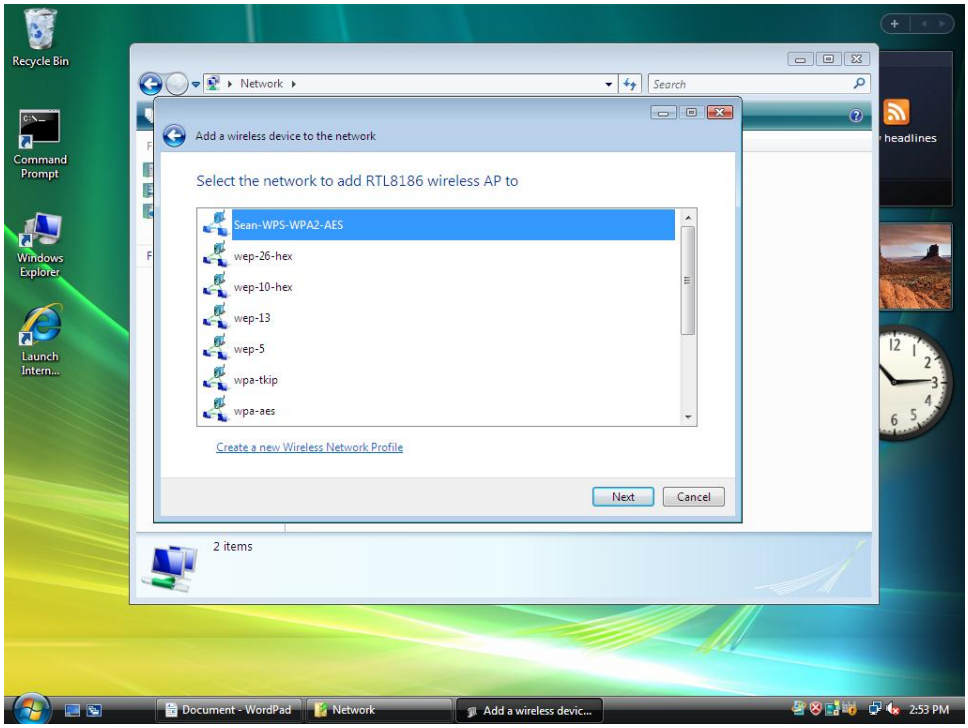


Figure 3.5

7. If the next window is shown as Figure 3.6, then AP is successfully configured by WCN.

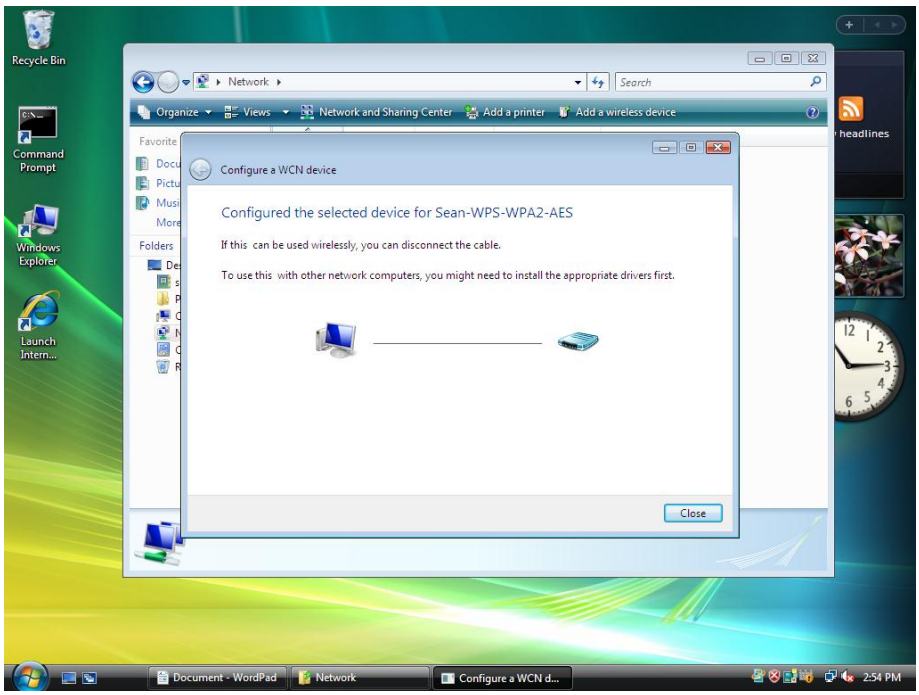


Figure 3.6

8. Finally, AP will become configured (see WPS Status). The authentication algorithm, encryption algorithm, and key assigned by WCN will be displayed below “Key”. (Figure 3.7)

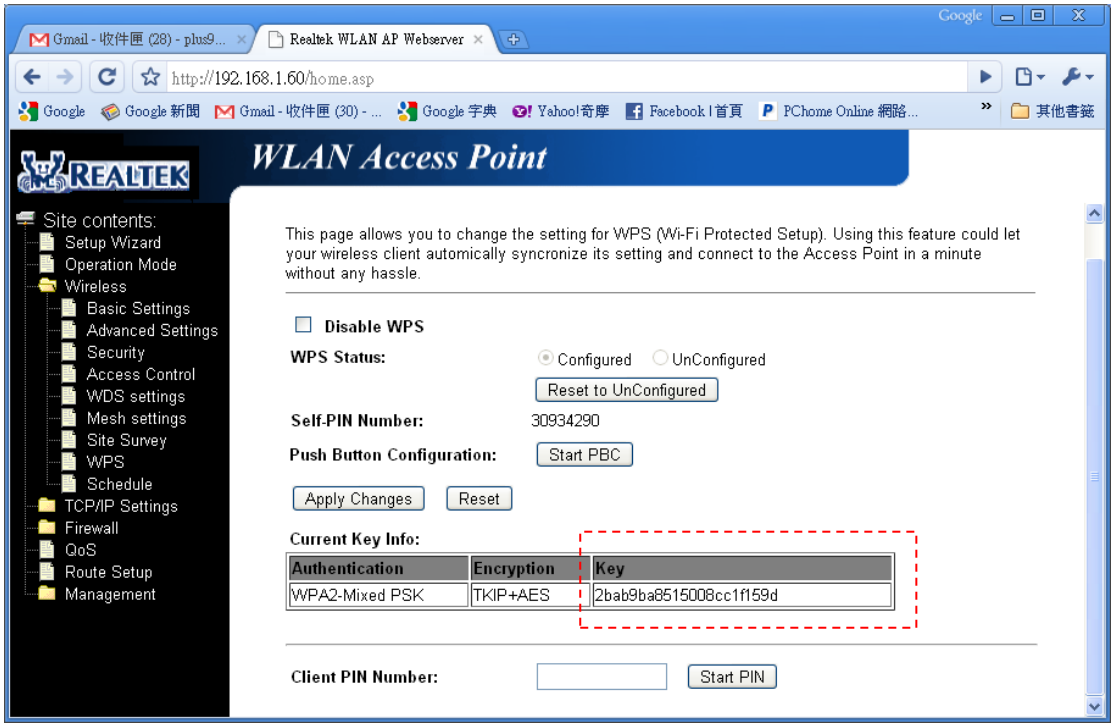


Figure 3.7

9. The SSID field of Wireless Basic Settings page will also be modified with the value assigned by WCN. (Figure 3.8)

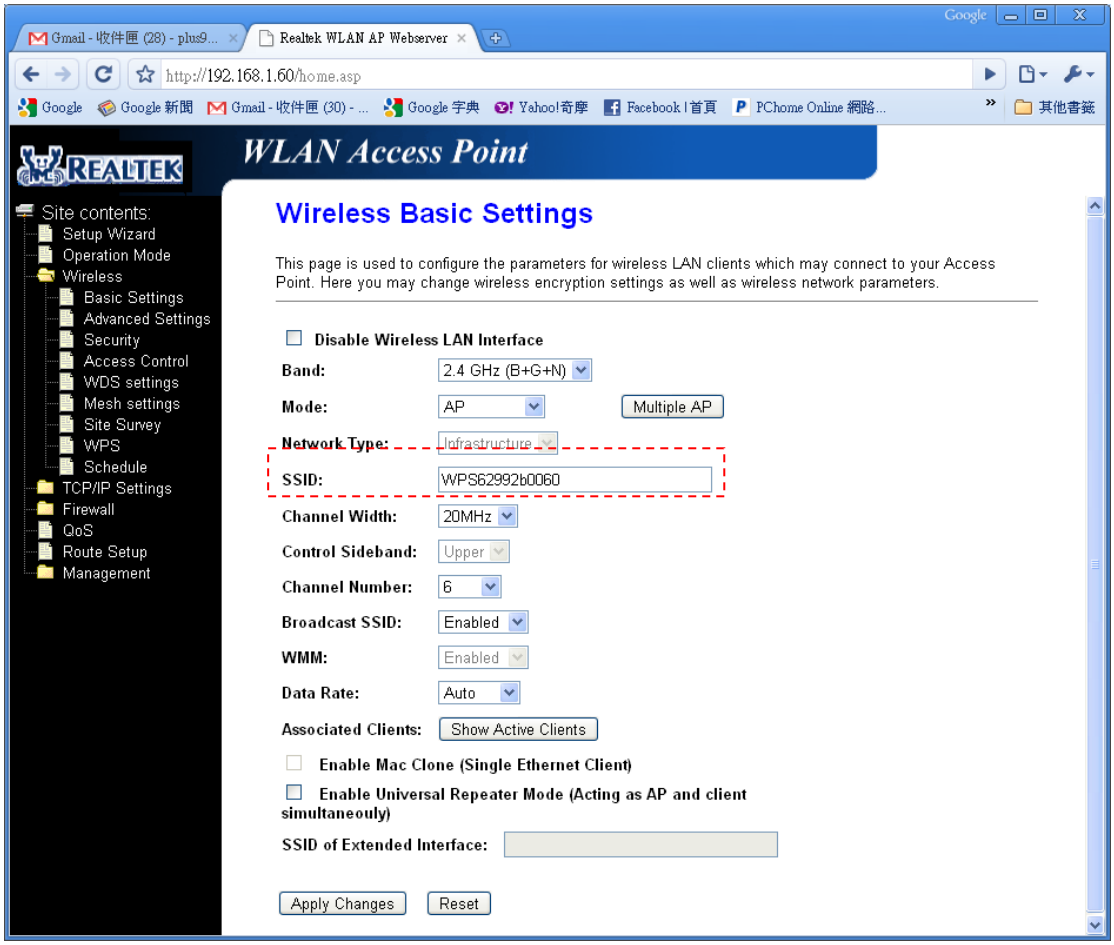


Figure 3.8

3.2.2 AP being a proxy

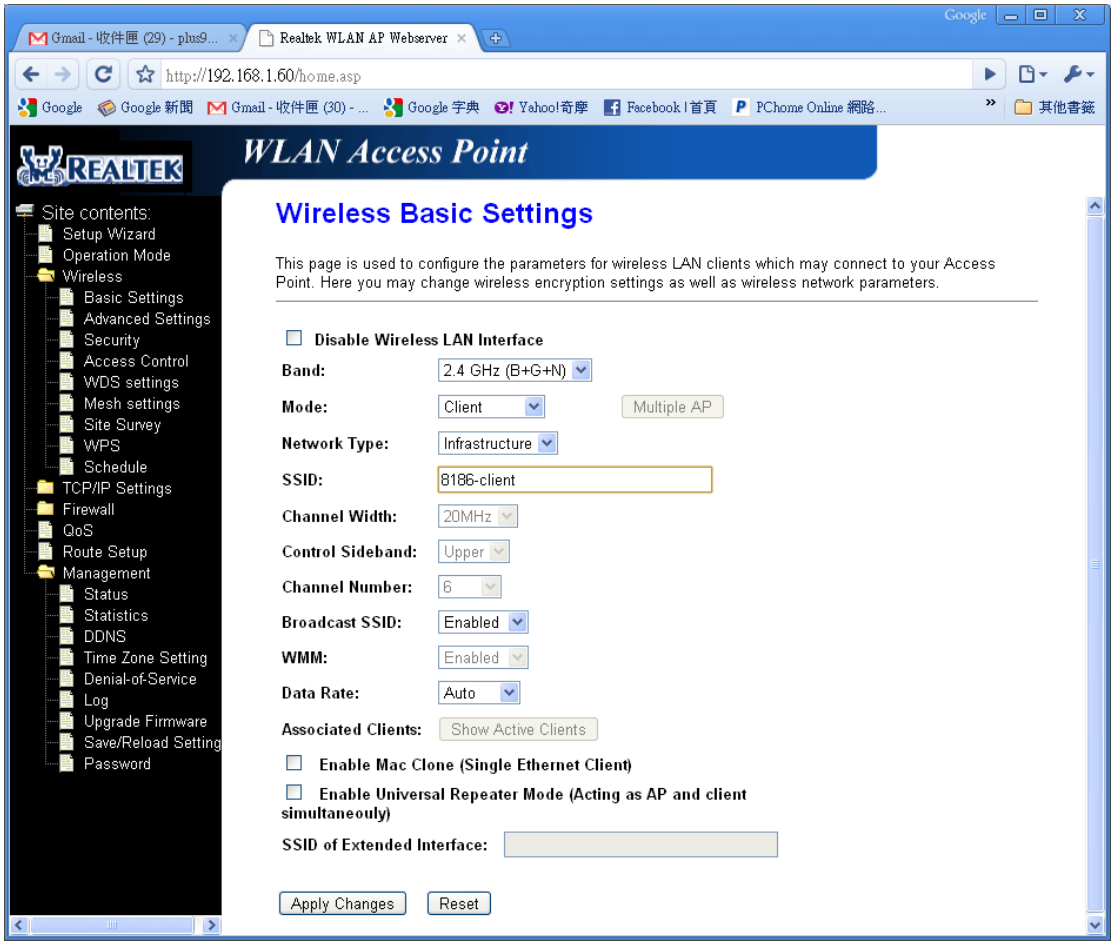
If AP satisfies all of the following conditions, AP will switch to proxy state automatically.

1. AP must be in configured state.
2. AP already established an IP connection with any external registrar.
3. AP is not configuring any devices at this moment. In other words, you are not entering device PIN into AP's WPS webpage, and not pushing PBC button on AP.
4. An external registrar is not configuring AP at this moment. In other words, you are not entering AP's PIN into any external registrar.

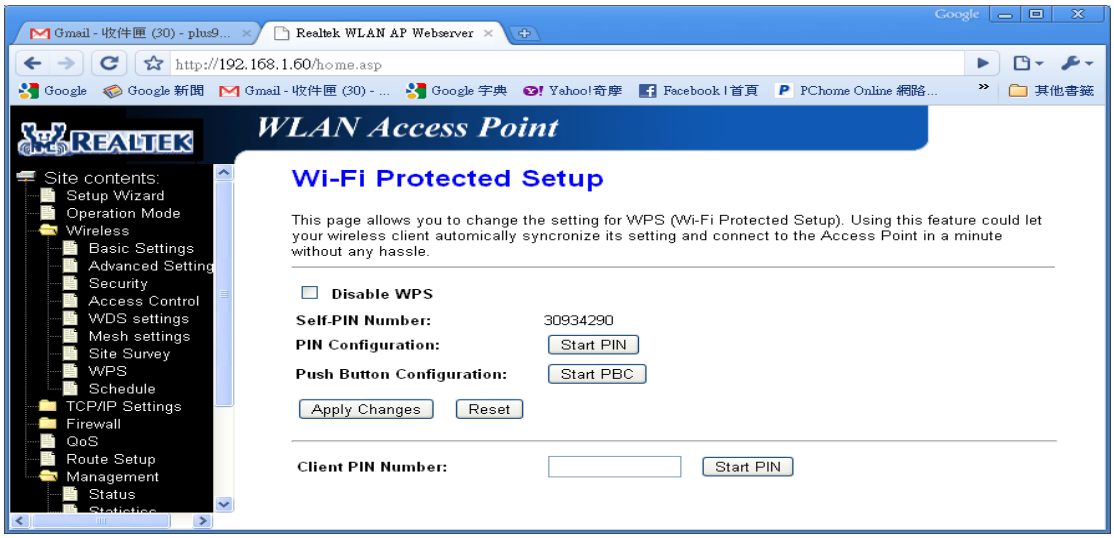
In this scenario, users need to make sure whether AP is in this state. If it is, then operate on station side and registrar side step by step. Here, we will illustrate an

example from Vista WCN and Realtek 8xxx-SOC Infrastructure-Client mode.

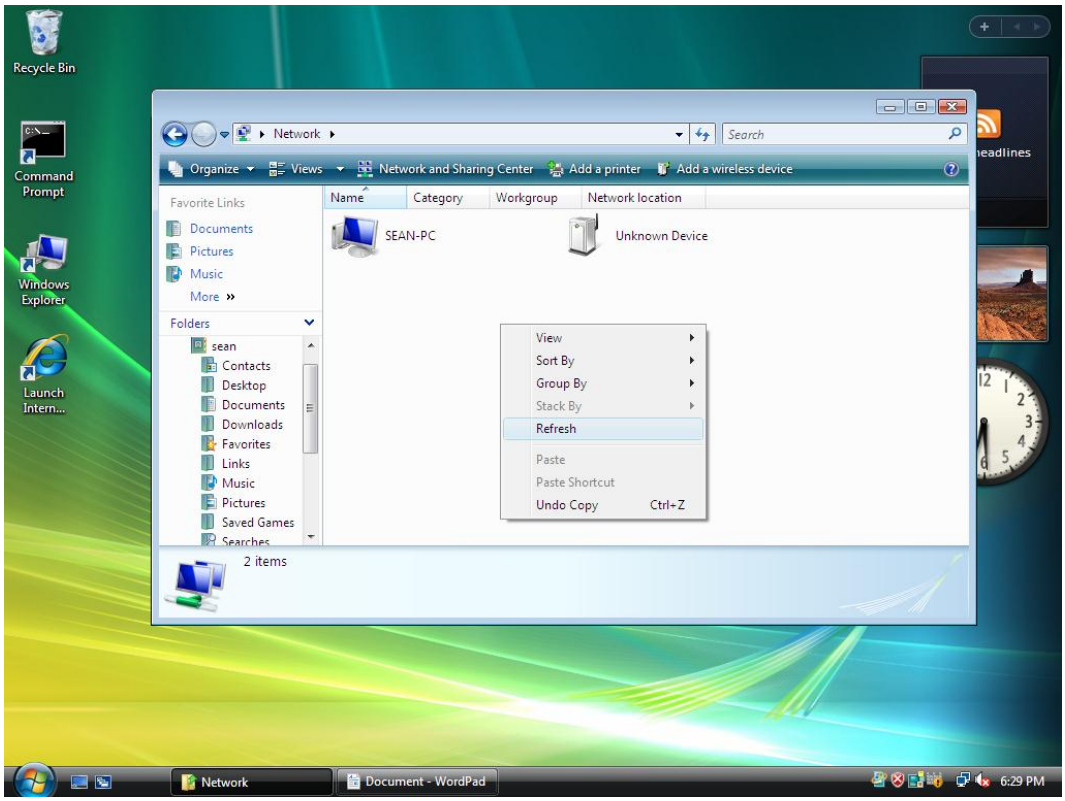
1. Go to the Wireless Basic Settings page of the other Realtek 8xxx-SOC platform. Make sure it is in Infrastructure-Client mode.



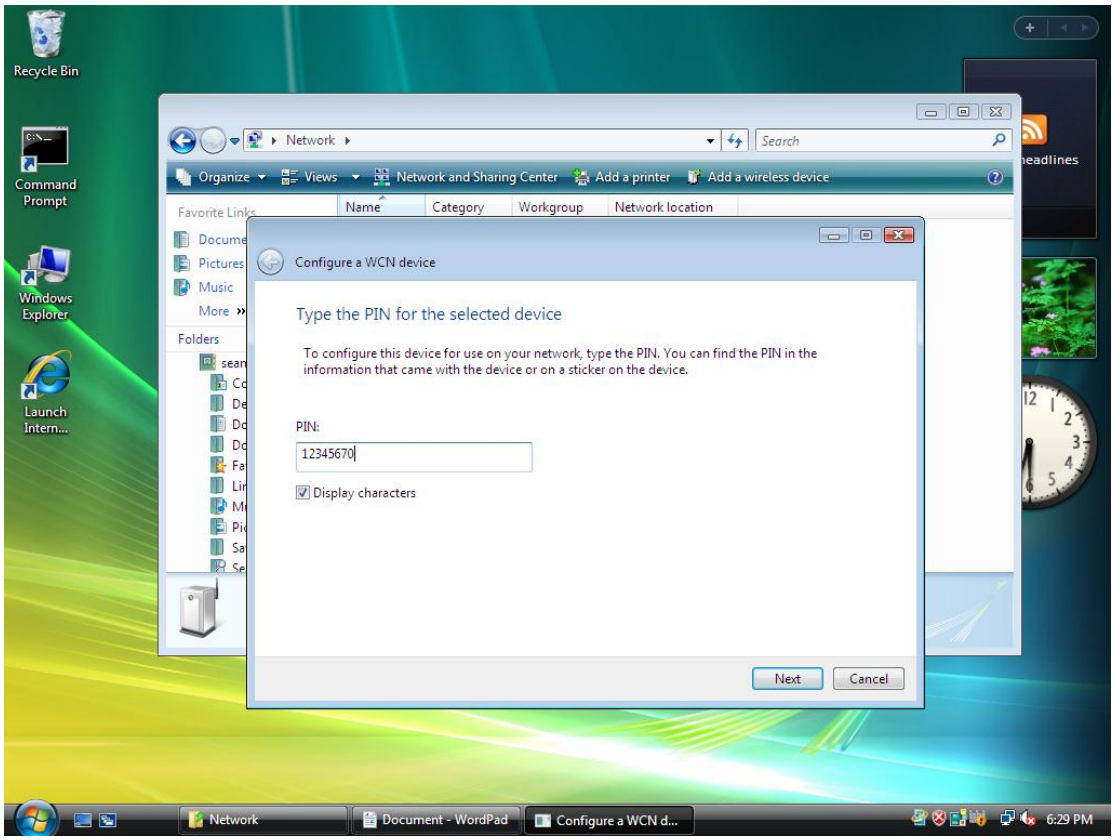
2. Go to the Wi-Fi Protected Setup page and click “Start PIN”.



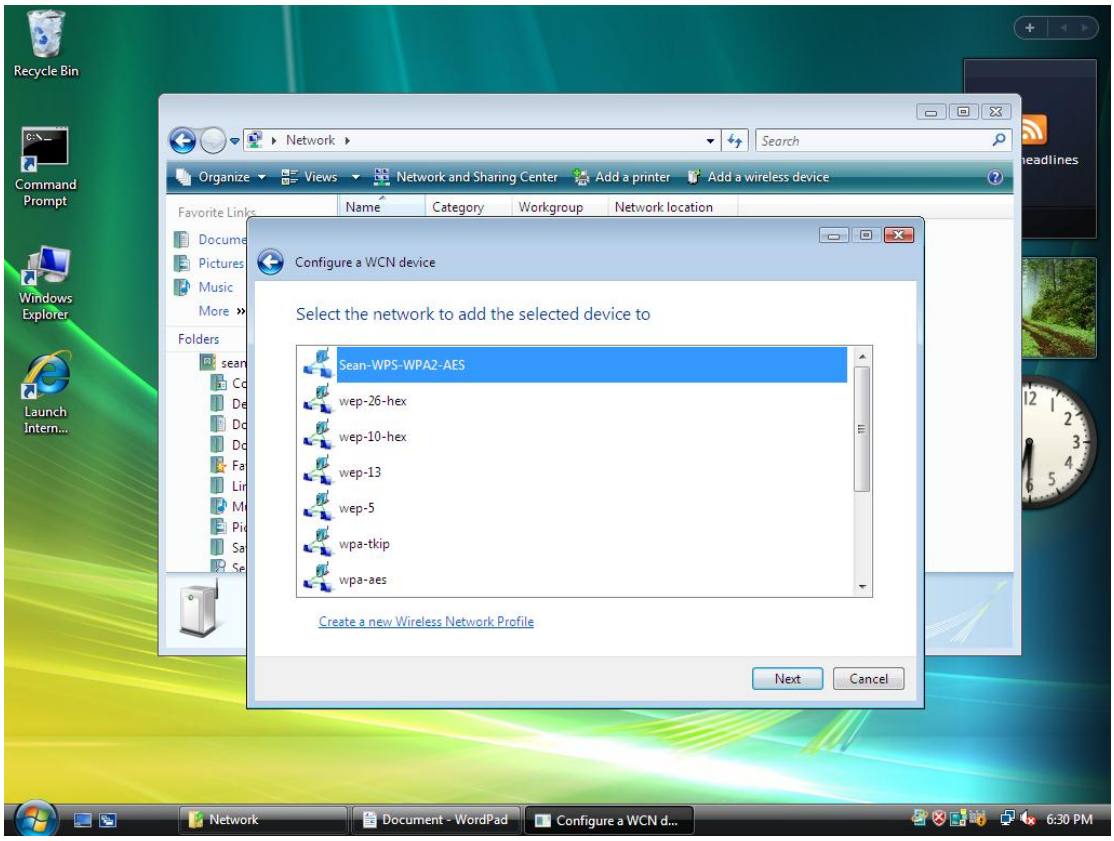
3. Open Windows Explorer on Vista and go to the Network section. Rick-click your mouse and select “Refresh”. After the “Unknown Device” icon shows up, double-click on it.



4. Enter the device PIN.

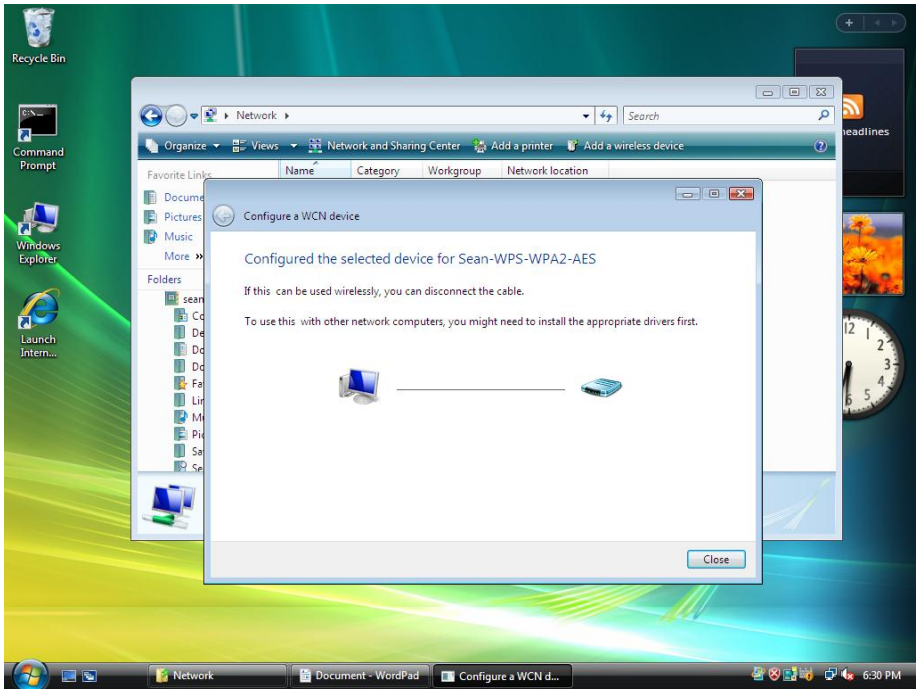


5. Choose the wireless profile previously assigned to the proxy AP.

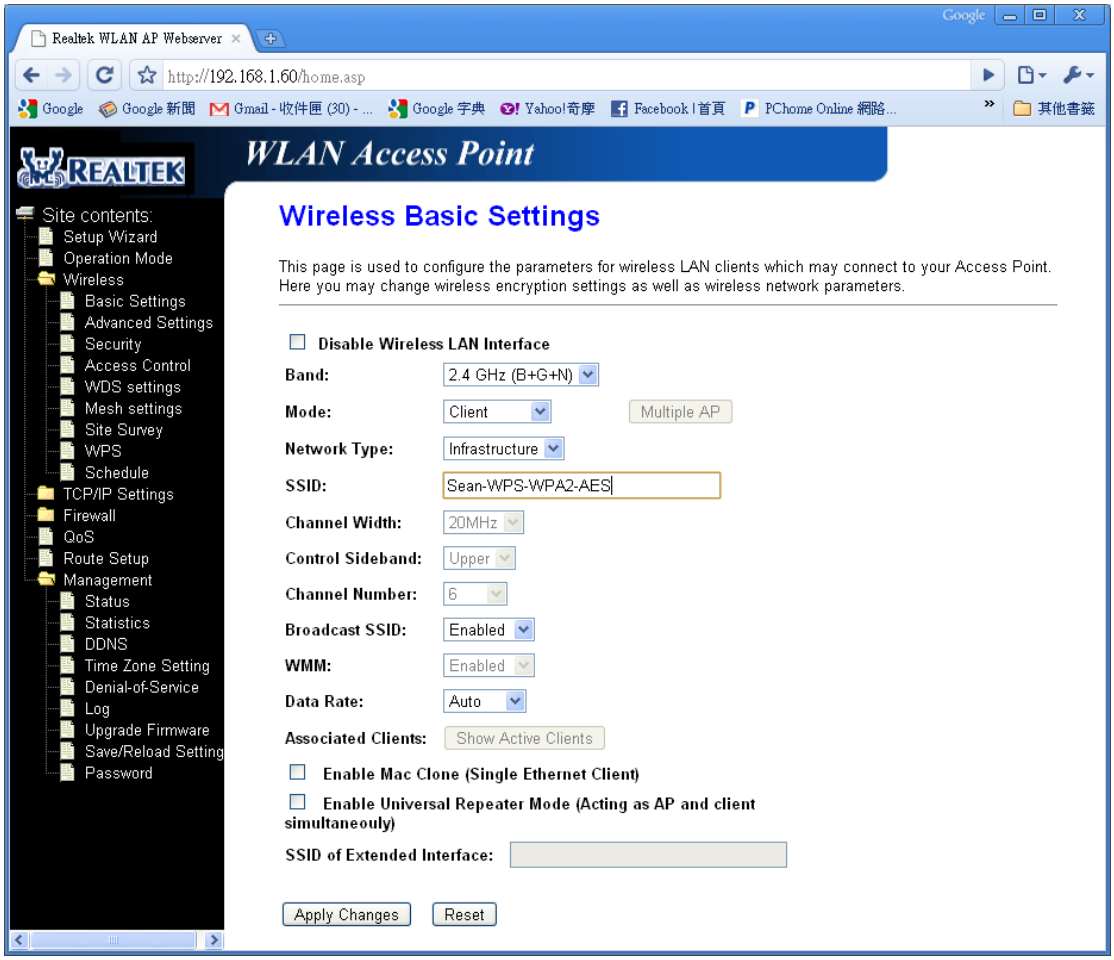


At this moment, WCN will inform AP this event and the LED of AP starts blinking.

6. If WCN had successfully configured Realtek 8xxx-SOC Infrastructure-Client, the LED of AP will be turned off. The window on Vista will be displayed as below.



7. The SSID of Realtek 8xxx-SOC Infrastructure-Client will be assigned according to the wireless profile that you just selected.



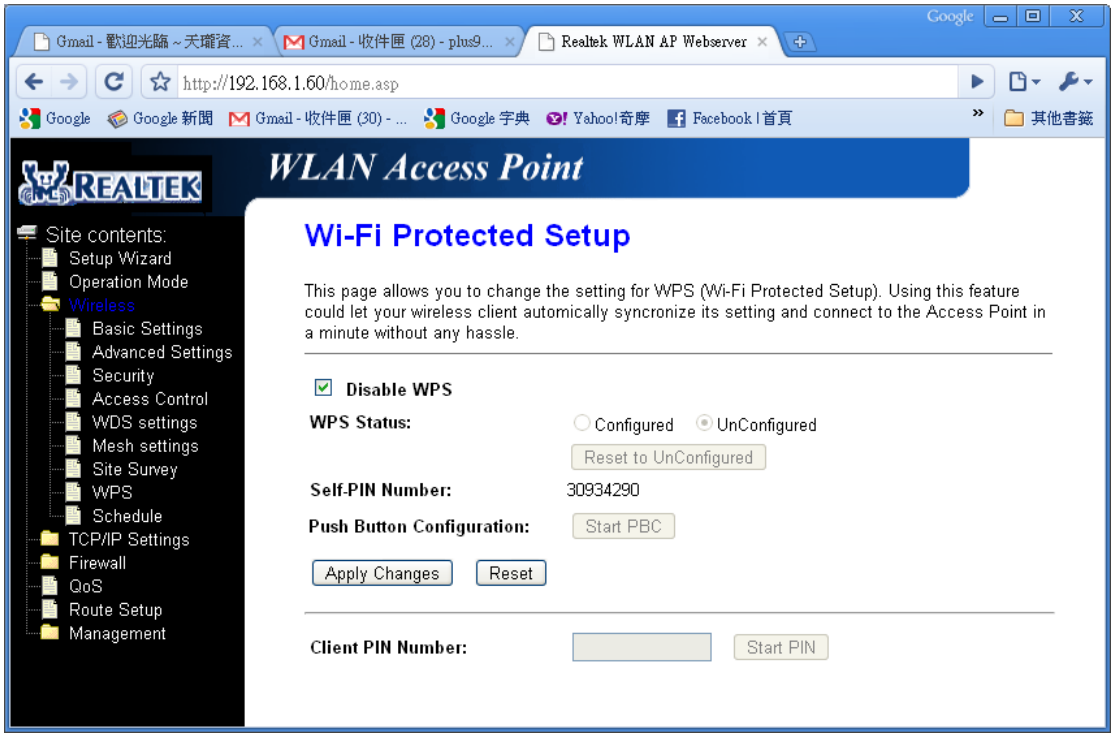
8. The security settings of Realtek 8xxx-SOC Infrastructure-Client will be assigned according to the wireless profile that you just selected.

9. Finally, Realtek 8xxx-SOC Infrastructure-Client will use the SSID and security to associate with the proxy AP.

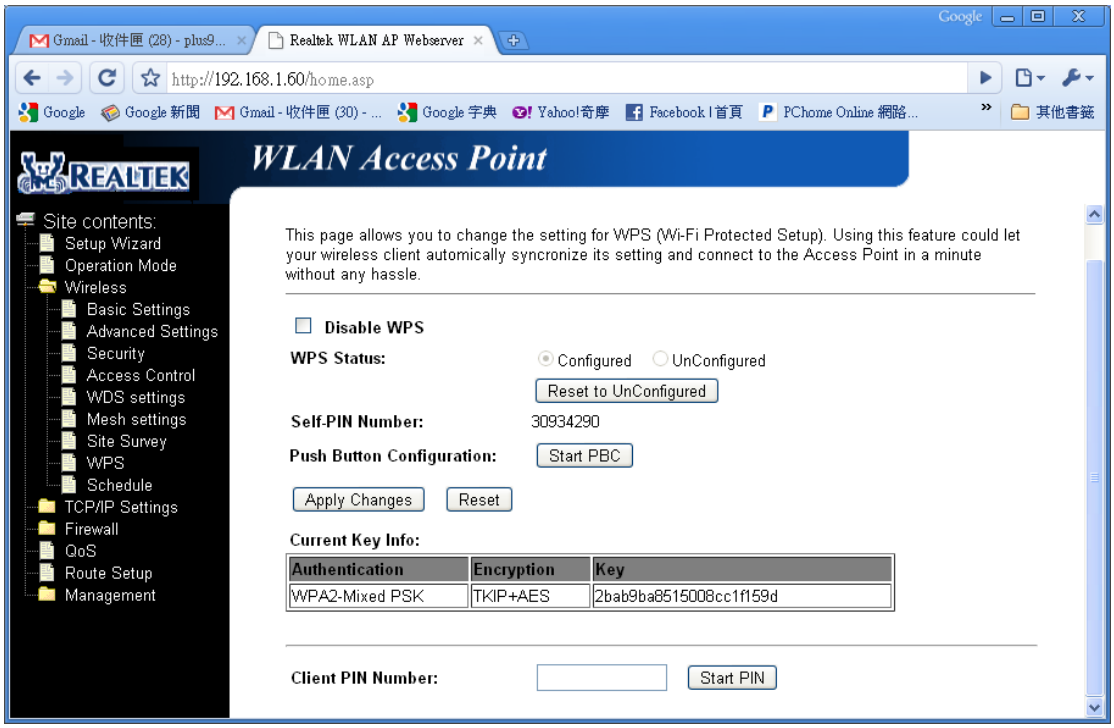
3.2.3 AP being a registrar

3.2.3.1 PIN method

Whenever users enter station's PIN into AP's Wi-Fi Protected Setup page and click "Start PIN", AP will become a registrar. The WPS LED will start blinking until the WPS handshake is successfully done or the session time out occurs. Users must start the PIN method on the station side within two minutes.



If the device PIN is correct and the WPS handshake is successfully done, AP's Wi-Fi Protected Setup page will be shown as below.



Other pages such as Wireless Basic Settings page and Wireless Security Setup page will also be updated appropriately as described in previous sections. In this case, AP is in un-configured state before the station initiates the WPS handshake. According to the WPS spec, AP will create a wireless profile with WPA2-mixed mode and a

random-generated key upon successfully doing the WPS handshake. However, AP will use the original wireless profile and give it to the station if AP is already in configured state. That means all settings of AP will not change. Hence, all WPS related pages keep the same.

3.2.3.2 Push Button method

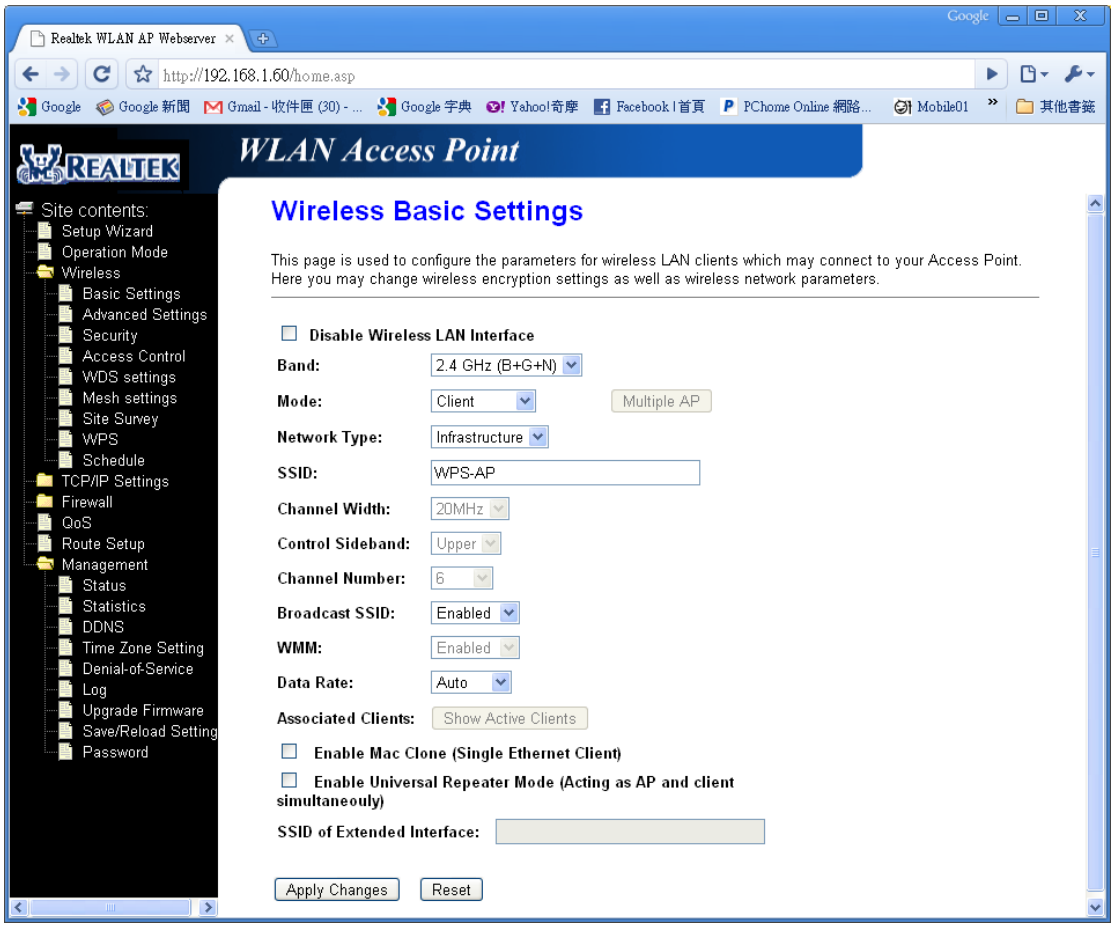
Realtek 8xxx-SOC supports a virtual button “Start PBC” on the Wi-Fi Protected Setup page and a physical button on Realtek 8xxx-SOC evaluation board for Push Button method. If users push any one of them, AP will initiate a WPS session and wait for any station to join. The PBC event will trigger to wlan0 if the pressed time of physical button less than “button_hold_time_for_first_if” in wscd.conf and and initiate a WPS session on wlan0, the PBC event will trigger to wlan1 if the pressed time of physical button more than “button_hold_time_for_first_if” and initiate a WPS session on wlan1. At this moment, AP will detect whether there is more than one station that starts the PBC method. If it happens, AP’s LED will be steady on for 30 seconds to indicate multiple PBC sessions; otherwise, the LED will be blinking until the WPS handshake is successfully done or session time out occurs. When multiple PBC sessions occurs, users should try PIN method.

After users push AP’s PBC button, they must go to station side to push its button within two minutes. If the WPS is successfully done, AP will give its wireless profile to that station. The station could use this profile to associate with AP.

3.3 Operations of Infrastructure-Client’s mode

3.3.1 Wireless Basic Settings

Users need to select “Client” and “Infrastructure” on the Wireless Basic Settings page. They are free to change other settings on this page.



3.3.2 Wi-Fi Protected Setup page

Below is the WPS page of infrastructure-client mode.

3.3.2.1 Disable WPS

Checking this box and clicking “Apply Changes” will disable all WPS functions.

3.3.2.2 Self-PIN Number

It is station’s PIN. The valid format is either four digit numeric PIN or eight digit numeric PIN with checksum. Users are not encouraged to manually enter it because the eight digit PIN will need checksum calculation. They could just click “Regenerate PIN” or enter four digit numeric PIN. Then click “Apply Changes” to save the PIN number to flash memory. However, if users change the device PIN and click “Start PIN”, the PIN number will take effect immediately and be saved to flash memory too.

3.3.2.3 Start PIN

If users decide to use PIN method, click “Start PIN” and enter the Self-PIN Number into registrar side within two minutes. If the WPS handshake is successfully done, the Wireless Basic Settings page and Wireless Security Setup page will be updated appropriately with the given wireless profile. Please refer to section 3.2.2.

3.3.2.4 Start PBC

If users decide to use Push Button method, they could either click “Start PBC” or push the physical button on Realtek 8xxx-SOC evaluation board. The PBC event will trigger to wlan0 if the pressed time of physical button less than “button_hold_time_for_first_if” in wscd.conf and and initiate a WPS session on wlan0, the PBC event will trigger to wlan1 if the pressed time of physical button more than “button_hold_time_for_first_if” and initiate a WPS session on wlan1. In addition, they must push the button on registrar side within two minutes. Upon successfully doing WPS handshake, the Wireless Basic Settings page and Wireless Security Setup page will be updated appropriately with the given wireless profile.

4. System Configuration

In this section, engineers need to know the important parameters for WPS to function correctly. Some parameters are located in the file “wscd.conf”, and some need to be burned in flash. “wscd.conf” is a configuration file that provides static information for WPS daemon. WPS daemon only needs to load this file once and will use those information for the registration protocol throughout its life time. Differently, the parameters located in flash are usually changeable and may be modified by WPS daemon to remember important states. In addition, some parameters are controlled by the webpage. Only setting those parameters appropriately could ensure the WPS functions. More detail will be demonstrated.

4.1 Parameters in wscd.conf

The format of “wscd.conf” is shown as the following:

```
# All words after “#” will not be parsed by WPS daemon and treated as
# comment.
# use ie=1, not use=0
use_ie = 1

# AUTH_OPEN=1, AUTH_WPAPSK=2, AUTH_SHARED=4,
# AUTH_WPA=8,AUTH_WPA2=0x10, AUTH_WPA2PSK=0x20
auth_type_flags = 39

# ENCRYPT_NONE=1, ENCRYPT_WEP=2, ENCRYPT_TKIP=4,
# ENCRYPT_AES=8
encrypt_type_flags = 15

uuid = 63041253101920061228aabbccddeeff
manufacturer = "Realtek Semiconductor Corp."
model_name = "RTL8xxx"
model_num = "EV-2006-07-27"
serial_num = "123456789012347"
device_oui = 0050f204
device_category_id = 6
device_sub_category_id = 1

# PASS_ID_DEFAULT=0, PASS_ID_USER=1, PASS_ID_MACHINE=2,
```

```
# PASS_ID_REKEY=3,
# PASS_ID_PB=4, PASS_ID_REG=5, PASS_ID_RESERVED=6
device_password_id = 0
tx_timeout = 5
resent_limit = 2
reg_timeout = 120
block_timeout = 60
button_hold_time_for_first_if = 5
# end of wscd.conf
```

4.1.1 use_ie

Function : enable(1)/disable(0) the WPS IE. If it is set to 0, the registration protocol may not proceed successfully.

Value : either 0 or 1.

Recommended Value : 1

4.1.2 auth_type_flags

Function : indicates the authentication capability of enrollee in registration protocol.

Value : It is a bitwise OR of the fields in the following table. (Wi-Fi Protected Setup Specification 1.0h.pdf, p. 89)

Value	Description
0x0001	**Open**
0x0004	**Shared**
0x0002	**WPAPSK**
0x0020	**WPA2PSK**

Recommended Value : 39 (bitwise OR of Open, Shared, WPAPSK, and WPA2PSK).

4.1.3 encrypt_type_flags

Function : indicates the encryption capability of enrollee in registration protocol.

Value : It is a bitwise OR of the fields in the following table. (Wi-Fi Protected Setup Specification 1.0h.pdf, p. 94)

Value	Description
0x0001	**None**
0x0002	**WEP**
0x0004	**TKIP**

0x0008 AES

Recommended Value : 15 (bitwise OR of NONE, WEP, TKIP, AND AES).

4.1.4 uuid

Function : It is the universally unique identifier assigned for the device. It also corresponds to UPnP uuid. Each device should have different uuid.

Value : must be 32 hex characters; the last 12 characters will be replaced by the device MAC address in the registration protocol.

Recommended Value : 63041253101920061228aabbccddeeff.

4.1.5 manufacturer

Function : It indicates the manufacturer name of the device.

Value : Any character enclosed by “”.

Recommended Value : “Customers’ company name”

4.1.6 model_name

Function : It indicates the model name of the device.

Value : Any character enclosed by “”.

Recommended Value : N/A.

4.1.7 model_num

Function : It indicates the model number of the device.

Value : Any character enclosed by “”.

Recommended Value : N/A.

4.1.8 serial_num

Function : It indicates the serial number of the device.

Value : Any numeric number enclosed by “”.

Recommended Value : N/A.

4.1.9 device_oui

Function : It indicates the OUI of the device which will be used in 802.11 IE element.

Value : must be 0050f204

Recommended Value : 0050f204.

4.1.10 device_category_id

Function : It is the primary device type.

Value : Any one of the ID Value of the category in table 3.1.10.

(Wi-Fi Protected Setup Specification 1.0h.pdf, p. 110)

Category	ID Value	Sub Category	ID Value
Computer	1	PC	1
		Server	2
		Media Center	3
Input Device	2		
Printers, Scanners, Faxes and Copiers	3	Printer	1
		Scanner	2
Camera	4	Digital Still Camera	1
Storage	5	NAS	1
Network Infrastructure	6	AP	1
		Router	2
		Switch	3
Displays	7	Television	1
		Electronic Picture Frame	2
		Projector	3
Multimedia Devices	8	DAR	1
		PVR	2
		MCX	3
Gaming Devices	9	Xbox	1
		Xbox360	2
		Playstation	3
Telephone	10	Windows Mobile	1

Table 3.1.10

Recommended Value : 6.

4.1.11 device_sub_category_id

Function : It is the sub-device type.

Value : Any one of the ID Value of the sub category in table 3.1.10.

Recommended Value : 1.

4.1.12 device_password_id

Function : It is used to specify which type of password id will be used in the registration protocol.

Value : Currently RTL Realtek 8xxx-SOC only supports PIN, User-specified, and PushBUTTON. (Wi-Fi Protected Setup Specification 1.0h.pdf, p. 92)

Value	Description
0x0000	Default (PIN)
0x0001	User-specified
0x0002	Machine-specified
0x0003	Rekey
0x0004	PushButton
0x0005	Registrar-specified
0x0006 – 0x000F	Reserved

Recommended Value : 0.

4.1.13 tx_timeout

Function : It specifies the time out for transmitting a message in registration protocol.

Value : Any number between 1 and 10; measured by seconds.

Recommended Value : 5.

4.1.14 resent_limit

Function : It specifies the maximal number for re-transmitting a message in registration protocol.

Value : Any number between 0 and 10.

Recommended Value : 2.

4.1.15 reg_timeout

Function : It specifies the time out of registration protocol. When the time out occurs, the WPS handshake ends up.

Value : Any number greater than 60 and smaller than 300; measured in seconds.

Recommended Value : 120.

4.1.16 block_timeout

Function : It specifies the time that an unauthorized station to be blocked.

Value : Any number greater than 10 and smaller than or equal to registration time out; measured by seconds.

Recommended Value : 60.

4.1.17 config_method

for WPS2;if wps1.0 don't define again

CONFIG_METHOD_VIRTUAL_PIN=0x2008 |
CONFIG_METHOD_PHYSICAL_PBC=0x480 |
CONFIG_METHOD_VIRTUAL_PBC=0x680

4.1.18 ProfileDontBothApply

Under dual band AP mode , we maintain two interface (wlan0 , wlan1),if device configured by EAP-base ER or auto-generate, and the profile want not apply to both band then preset the parameter to 1

Recommended Value :0 or don't define

4.1.19 disable_configured_by_exReg

value=2:deny whatever config or unconfig state.

value=1:deny under configured state, allow when unconfig state.

Recommended Value :0 or don't define

4.1.20 auto_lock_down_time

Configurable auto_lock_down_time ,when AP be force

Recommended Value :60 or don't define

4.1.21 UPC

Configurable UPC(Universal Product Code)

Value="UPC-STRING", UPC-STRING length equal 12

4.2 Parameters in flash

There are two groups of parameters related to WPS in the flash. One group is located in the default-setting section. This includes the WPS default settings burned in factories. The other group is located in the current-setting section. Initially, the parameters in these two sections will be burned the same values which are called the out-of-box settings. After the registration protocol is done, some WPS parameters in the current-setting section might be changed, but those WPS parameters in the default-setting section will be never modified. Whenever users start the reload default function of the webpage, the WPS parameters in the current-setting section will be assigned the corresponding values from the default-setting section. This process is called "reset WPS to out-of-box setting". All parameters are shown as below. The parameters prefixed with "DEF" are located in the default-setting section. Otherwise, parameters are in the current-setting section. Currently, Realtek 8xxx-SOC only supports one wireless interface for WPS. If the WPS wireless interface of your

product is “wlan0”, then WLANn will represent WLAN0 in the following sections.

4.2.1 DEF_WLANn_WSC_DISABLE and WLANn_WSC_DISABLE

Function : enable(0)/disable(1) the WPS function. WLANn_WSC_DISABLE could be controlled by the webpage

Value : either 0 or 1.

Recommended Value : 0.

4.2.2 DEF_WLANn_WSC_METHOD and DEF_WLANn_WSC_METHOD

Function : It specifies the configuration methods that could be used in registration protocol. Realtek 8xxx-SOC currently supports PIN and PushButton.

Value : a bitwise OR of PIN (0x1) and PushButton (0x2).

Recommended Value : 3.

4.2.3 DEF_WLANn_WSC_CONFIGURED and WLANn_WSC_CONFIGURED

Function : It records the configuration state. WLANn_WSC_CONFIGURED will be controlled by the webpage or WPS daemon.

Value : either 0 (not configured) or 1 (configured).

Default Value : 0.

4.2.4 DEF_WLANn_WSC_PIN and WLANn_WSC_PIN

Function : It specifies the PIN used in registration protocol. Factories must assign unique four (without checksum) or eight (with checksum) numeric digits to DEF_WLANn_WSC_PIN and WLANn_WSC_PIN of each device before it is shipped out. WLANn_WSC_PIN might be changed by the webpage. The formula of calculating and validating checksum is as below. (Wi-Fi Protected Setup Specification 1.0h.pdf, p. 39)

The formula of calculating checksum:

```
int ComputeChecksum(unsigned long int PIN)
{
    unsigned long int accum = 0;
    PIN *= 10;
    accum += 3 * ((PIN / 10000000) % 10);
    accum += 1 * ((PIN / 1000000) % 10);
    accum += 3 * ((PIN / 100000) % 10);
    accum += 1 * ((PIN / 10000) % 10);
    accum += 3 * ((PIN / 1000) % 10);
```

```
    accum += 1 * ((PIN / 100) % 10);
    accum += 3 * ((PIN / 10) % 10);
    int digit = (accum % 10);
    return (10 - digit) % 10;
}
```

The formula of validating the checksum:

```
bool ValidateChecksum(unsigned long int PIN)
{
    unsigned long int accum = 0;
    accum += 3 * ((PIN / 10000000) % 10);
    accum += 1 * ((PIN / 1000000) % 10);
    accum += 3 * ((PIN / 100000) % 10);
    accum += 1 * ((PIN / 10000) % 10);
    accum += 3 * ((PIN / 1000) % 10);
    accum += 1 * ((PIN / 100) % 10);
    accum += 3 * ((PIN / 10) % 10);
    accum += 1 * ((PIN / 1) % 10);
    return (0 == (accum % 10));
}
```

Note : When the device is upgraded firmware, there is a possibility that the default-setting section and the current-setting section might be reloaded to hard-coded default values due to the mismatched MIB version. In this case, DEF_WLANn_WSC_PIN and WLANn_WSC_PIN will be assigned 12345670. Engineers might want to modify the reference codes to randomly generate device PIN in the case of software-reload-default.

Value : must be four or eight (with checksum) numeric digits.

Recommended Value : eight numeric digits with checksum.

4.2.5 DEF_WLANn_WSC_AUTH and WLANn_WSC_AUTH

Function : It specifies the authentication algorithm of security.

WLANn_WSC_AUTH will be controlled by the webpage or WPS daemon.

Value : In infrastructure-client mode, DEF_WLANn_WSC_AUTH and WLANn_WSC_AUTH must be set to one of the following values.

(Wi-Fi Protected Setup Specification 1.0h.pdf, p. 89)

Value	Description
0x0001	**Open**
0x0002	**WPAPSK**
0x0020	**WPA2PSK**

In AP mode, DEF_WLANn_WSC_AUTH and WLANn_WSC_AUTH could be one of the values or a bitwise OR of WPAPSK and WPA2PSK.

Recommended Value : 1.

NOTE: If engineers decide to modify the recommended value other than Open. They also need to modify other security parameters in the flash. The following demonstrates which parts to modify.

In infrastructure-client mode:

1. If DEF_WLANn_WSC_AUTH and WLANn_WSC_AUTH are set to 0x 2 (WPAPSK), DEF_WLANn_ENCRYPT and WLANn_ENCRYPT need to be set to 0x2.
2. If DEF_WLANn_WSC_AUTH and WLANn_WSC_AUTH are set to 0x 20 (WPA2PSK), DEF_WLANn_ENCRYPT and WLANn_ENCRYPT need to be set to 0x4.

In AP mode: The modified parts are the same as infrastructure-client mode except in the case that DEF_WLANn_WSC_AUTH and WLANn_WSC_AUTH are set to a bitwise OR of WPAPSK and WPA2PSK. In this case DEF_WLANn_ENCRYPT and WLANn_ENCRYPT need to be set to 0x6.

4.2.6 DEF_WLANn_WSC_ENC and WLANn_WSC_ENC

Function : It specifies the encryption algorithm of security. WLANn_WSC_ENC Will be controlled by the webpage or WPS daemon.

Value : In infrastructure-client mode, DEF_WLANn_WSC_ENC and WLANn_WSC_ENC must be one of the following values. (Wi-Fi Protected Setup Specification 1.0h.pdf, p. 110)

Value	Description
0x0001	**None**
0x0002	**WEP**
0x0004	**TKIP**
0x0008	**AES**

In AP mode, DEF_WLANn_WSC_ENC and WLANn_WSC_ENC could be one of the values or a bitwise OR of TKIP and AES.

Recommended Value : 1.

NOTE : If engineers wan to modify DEF_WLANn_WSC_ENC and WLANn_WSC_ENC other than the recommended value. Please follow the instructions below.

In infrastructure-client mode:

1. If DEF_WLANn_WSC_AUTH and WLANn_WSC_AUTH are set

to 0x 2 (WPAPSK) and DEF_WLANn_WSC_ENC and WLANn_WSC_ENC are set to 0x4 (TKIP), DEF_WLANn_WPA_CIPHER_SUITE and WLANn_WPA_CIPHER_SUITE must be set to 1.

2. If DEF_WLANn_WSC_AUTH and WLANn_WSC_AUTH are set to 0x 2 (WPAPSK) and DEF_WLANn_WSC_ENC and WLANn_WSC_ENC are set to 0x8 (AES), DEF_WLANn_WPA_CIPHER_SUITE and WLANn_WPA_CIPHER_SUITE must be set to 2.
3. If DEF_WLANn_WSC_AUTH and WLANn_WSC_AUTH are set to 0x 20 (WPA2PSK) and DEF_WLANn_WSC_ENC and WLANn_WSC_ENC are set to 0x4 (TKIP), DEF_WLANn_WPA2_CIPHER_SUITE and WLANn_WPA2_CIPHER_SUITE must be set to 1.
4. If DEF_WLANn_WSC_AUTH and WLANn_WSC_AUTH are set to 0x 20 (WPA2PSK) and DEF_WLANn_WSC_ENC and WLANn_WSC_ENC are set to 0x8 (AES), DEF_WLANn_WPA2_CIPHER_SUITE and WLANn_WPA2_CIPHER_SUITE must be set to 2.

In AP mode: The modified parts are the same as infrastructure-client mode except in the case that DEF_WLANn_WSC_ENC and WLANn_WSC_ENC are set to a bitwise OR of TKIP and AES. If the authentication algorithm is WPAPSK, DEF_WLANn_WPA_CIPHER_SUITE and WLANn_WPA_CIPHER_SUITE must be set to 3. Moreover, if the authentication algorithm includes WPA2PSK, DEF_WLANn_WPA2_CIPHER_SUITE and WLANn_WPA2_CIPHER_SUITE must be set to 3 as well.

4.2.7 DEF_WLANn_WSC_UPNP_ENABLED and WLANn_WSC_UPNP_ENABLED

Function : enable(1)/disable(0) the UPnP function of WPS. If engineers disable this function, their products will not pass Wi-Fi certification program.

Value : either 0 or 1.

Recommended Value : 1.

4.2.8 DEF_WLANn_WSC_REGISTRAR_ENABLED and WLANn_WSC_REGISTRAR_ENABLED

Function : enable(1)/disable(0) the internal registrar of AP. If engineers disable

this function, their products will not pass Wi-Fi certification program.

Value : either 0 or 1.

Recommended Value : 1.

4.2.9 DEF_WLANn_WSC_PSK and WLANn_WSC_PSK

Function : It provides the key of WPAPSK or WPA2PSK. It is controlled by the webpage or WPS daemon.

Value : The maximal length is 64 characters. If the length is smaller than 64, the value could be any characters; otherwise, the value must be 64 hex characters.

Default Value : Null.

NOTE : If the default security setting is set to WPAPSK or WPA2PSK, then DEF_WLANn_WSC_PSK and WLANn_WSC_PSK must be assigned a legal key which is the same as DEF_WLANn_WPA_PSK and WLANn_WPA_PSK.

4.2.10 DEF_WLANn_WSC_CONFIGBYEXTREG and WLANn_WSC_CONFIGBYEXTREG

Function : This parameter reflects which kind of devices invokes the generation of current security setting.

Value : It could be one of the following.

Value	Description
0	The SSID and security is the same as the out-of-box setting.
1	The SSID and security is generated by internal registrar.
2	The SSID and security is generated by external registrar.
3	The SSID or security is modified via webpage and at lease one enrollee had successfully done the WPS handshake and joined the network.

Default Value : 0.

4.3 MP program related to WPS (only apply to rtl8186)

If the flash layout of your product is programmed by Realtek MP nfjrom, then you need to update the file “apmib.h” of your MP source tree. For more detail, please see the document of Realtek 8196c MP.

4.4 Porting the flash related programs

All WPS related reference codes are implemented under the directory

/AP/goahead-2.1.1/LINUX. Engineers could search the keyword "WIFI_SIMPLE_CONFIG" and modify them appropriately. After the modification, you may need to verify three commands on the console that will be called by WPS daemon. The three commands are
"flash set wlan0 WSC_CONFIGBYEXTREG number",
"flash set wlan0 WSC_CONFIGURED number",
and "flash -param_file wlan0 /tmp/flash_param", where number could be 0 to 3.
If the first two commands are accepted by the console, you need to check whether the flash are written correctly. The method to verify the third command
"flash -param_file wlan0 /tmp/flash_param" is as below.

1. Type the command,
   echo "WSC_CONFIGURED=number" > /tmp/flash_param,
   on the console.
2. Type "flash -param_file wlan0 /tmp/flash_param" on the console.
3. If those two commands are accepted by the console, you need to check whether the flash parameter "WSC_CONFIGURED" is written correctly.

4.5 WPS LED and Button

The gpio-related codes of LED and physical button are located in the file linux-2.x.x\drivers\char\rtl_gpio.c. Engineers need to modify it appropriately to support the following commands that will be called by WPS daemon and response correctly according to the following definition.

1. Initialization:
   echo E > /proc/gpio
2. Button state:
   The WPS daemon will use the following codes to read the button state

```
static int wlioctl_get_button_state(char *interface, int *pState)
{
        char tmpbuf;
        FILE *fp;
        char line[20];

        if ((fp = fopen("/proc/gpio", "r")) != NULL) {
            fgets(line, sizeof(line), fp);
            if (sscanf(line, "%c", &tmpbuf)) {
                if (tmpbuf == '0')
                    *pState = 0;
```

```
            else
                *pState = 1;
        }
        else
            *pState = 0;
        fclose(fp);
    }
    else
        *pState = 0;

    return 0;
}
```

In other words, if users push the button, you need to write "1" to /proc/gpio so that WPS daemon will be informed that users have pushed the button.

3. The WPS LED.

Start blinking every second: echo 2 > /proc/gpio
The LED is off: echo 0 > /proc/gpio
The LED is steady on: echo 1 > /proc/gpio
WPS daemon will execute these three commands to make the LED on or off.

What engineers need to do about the push button and LED is to accept those commands and do the responses correctly. You could either modify the rtl_gpio.c appropriately or implement those codes somewhere as long as your platform accepts those commands and report the button state correctly.

4.6 WPS status for WEB GUI

When user would like to run WPS from WEB GUI, WPS can report the progress for WEB GUI.

For Case "Start PIN":

It is necessary to remove the file "/tmp/wscd_status" first, then you could start the progress of "Start PIN".

For Case "Start PBC":

It is necessary to remove the file "/tmp/wscd_status" first, then you could start the progress of "Start PBC".

When the web page would like get the status of WPS, it can check the value in /tmp/wscd_status, the meaning of the value:

Meaning	Value
WPS Protocol Started	0
Overlapping while PBC	1
WPS Protocol Time-out	2
Success	3
EAPOL_START Sent	4
Received EAPOL-start packet	5
Received EAPOL-request for identity	6
Received EAPOL-response for identity	7
WSC-start Sent	8
M1 Sent	9
M1 Received	10
M2 Sent	11
M2 Received	12
M2D Received	13
M3 Sent	14
M3 Received	15
M4 Sent	16
M4 Received	17
M5 Sent	18
M5 Received	19
M6 Sent	20
M6 Received	21
M7 Sent	22
M7 Received	23
M8 Sent	24
M8 Received	25
Process EAP ACK	26
Process EAP WSC-FAIL	27
HASH Failed	28
HMAC Failed	29
Authentication Failed	30
Invalid PIN code	31
Process EAP-done packet	32

For Case “Cancel”:

When WPS is in progress, user can cancel the progress of WPS any time. Any value can be put into the file “/tmp/wscd_cancel” when user would like to terminate the progress of WPS.

5. Reference

Wi-Fi Protected Setup Specification 1.0h.pdf. Wi-Fi Alliance.

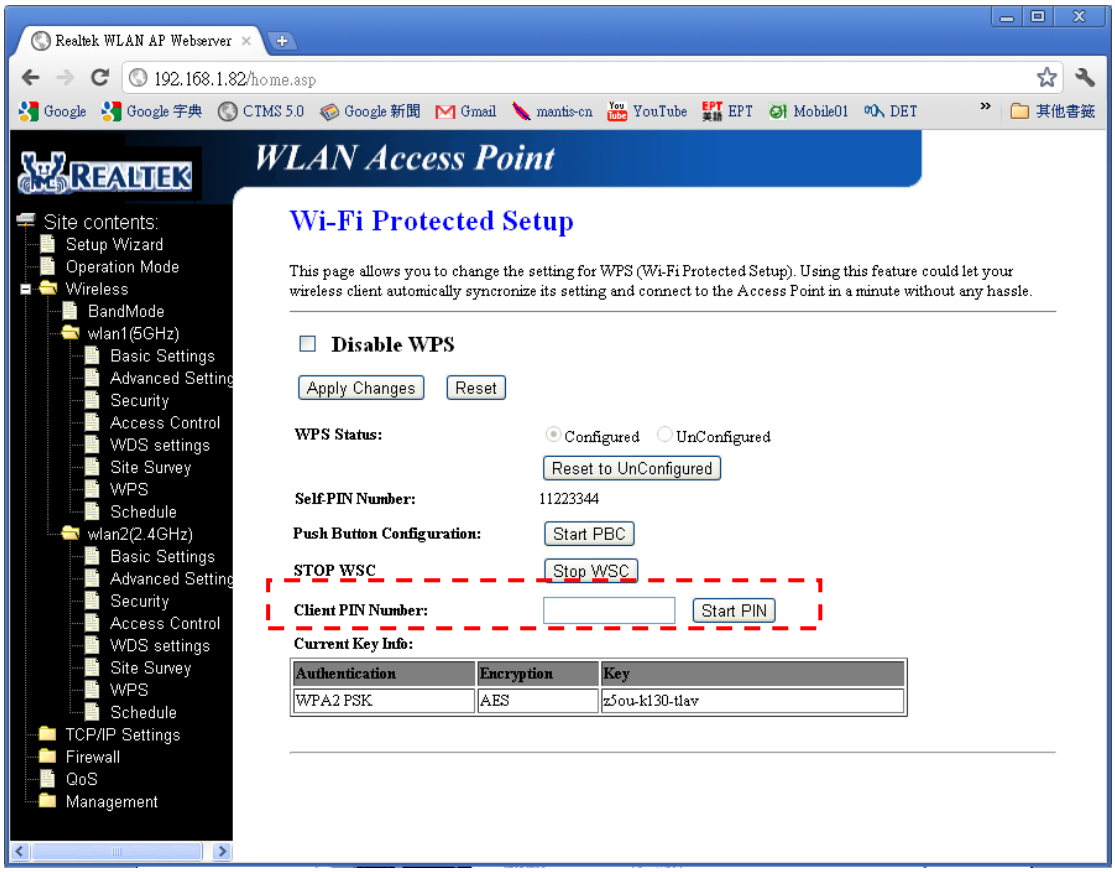
APPEND

chap6. WPS2.0 AP mode GUI

Notice：

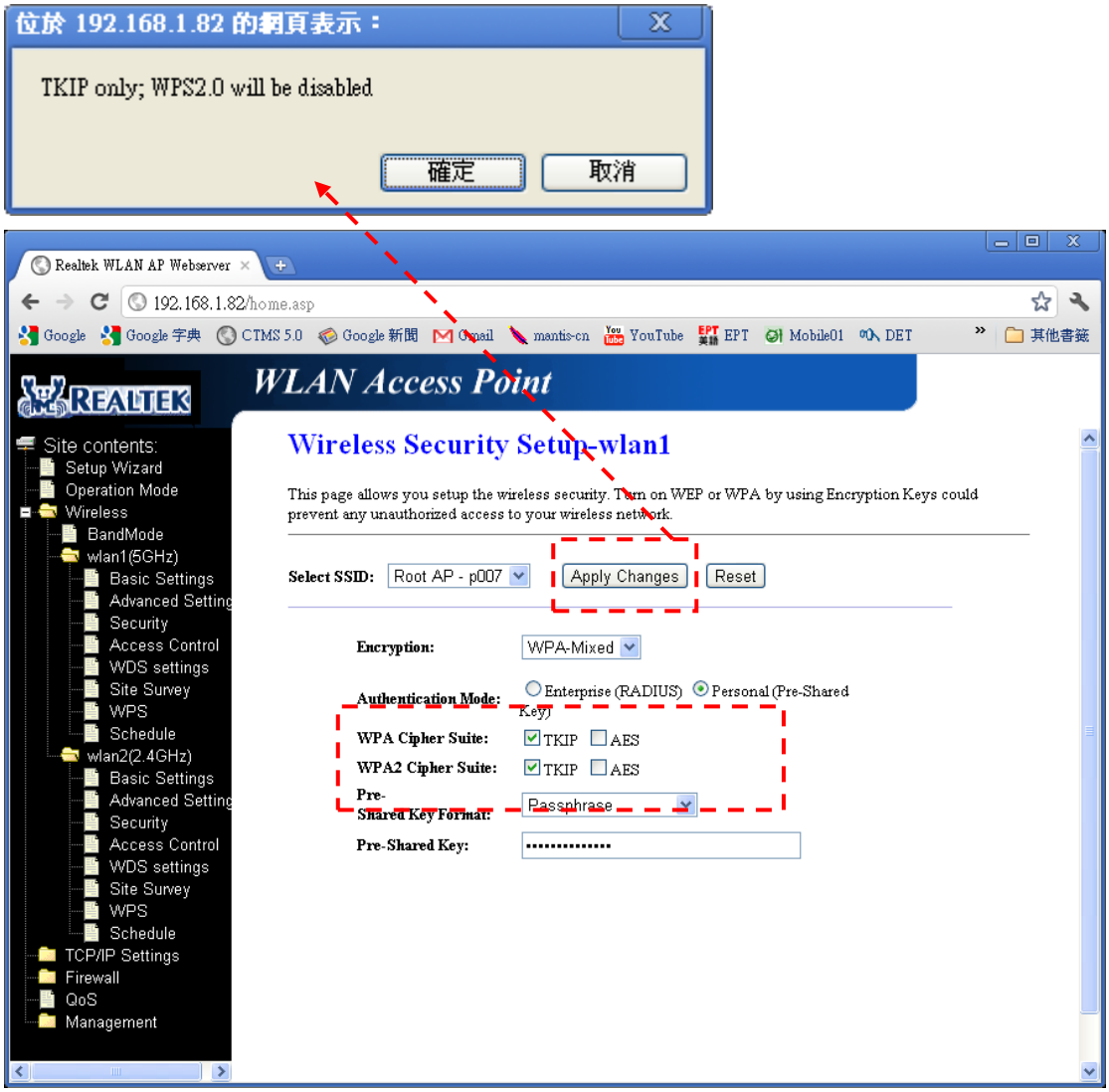
Web page need do some modify for wps2.0 test plan request, if customer is not use our web-page then they must take care self.

1. Input text of client PIN number must support the filter of blank and dash,for example you can input the format likes “1122 3344” or “11 22 3344” or “1122-3344”.

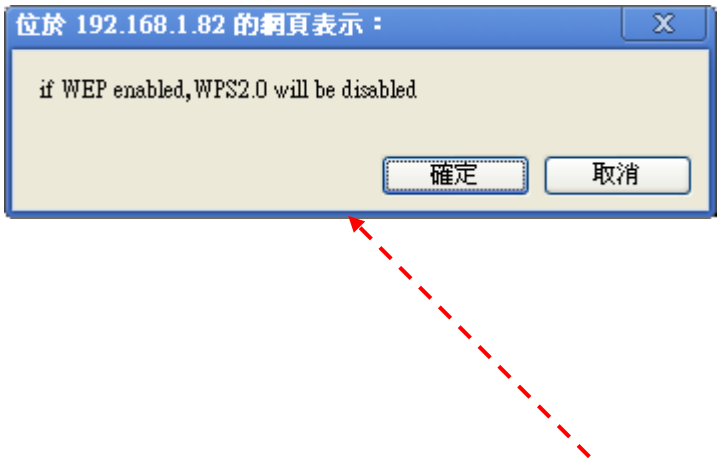


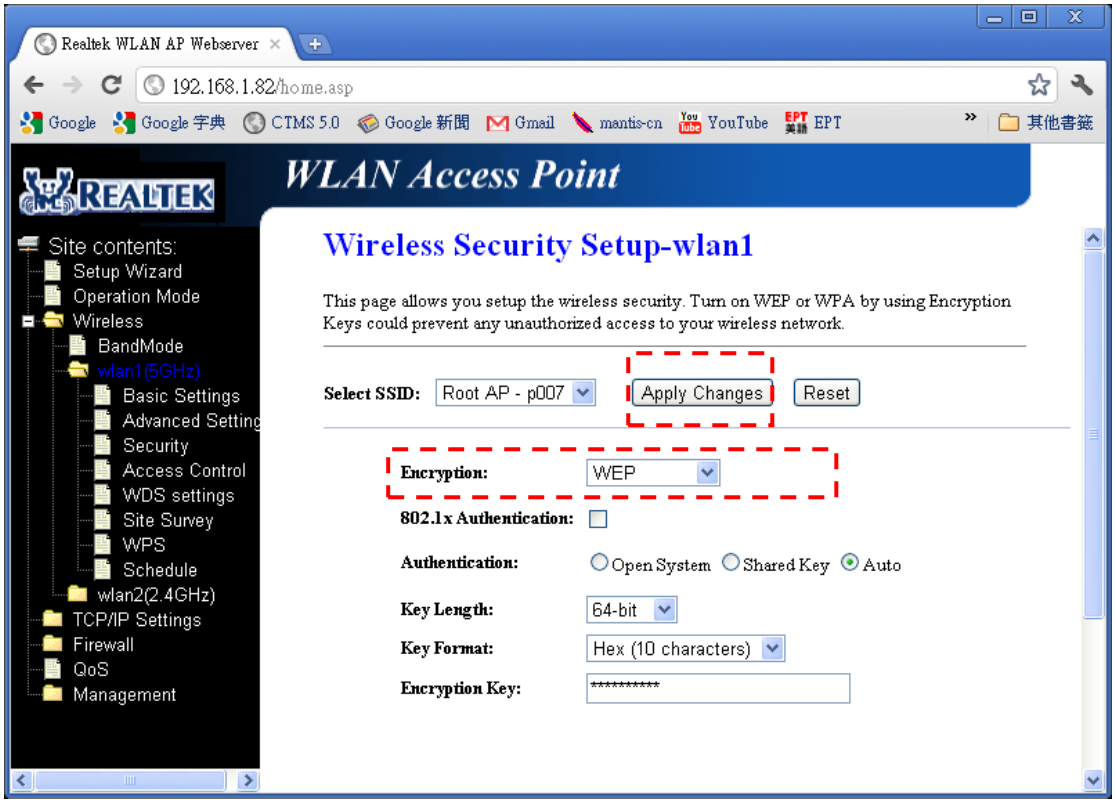
2. Version 2.0 of the WSC specification deprecates the use of ***WEP*** , ***WPA only*** ,***TKIP only***, so under AP mode if user setting security to these deprecated security setting GUI must warning that will bring WPS2 daemon be disabled.

2-1.Under AP mode if security set to TKIP only, GUI must warning that will bring WPS2 daemon be disabled.

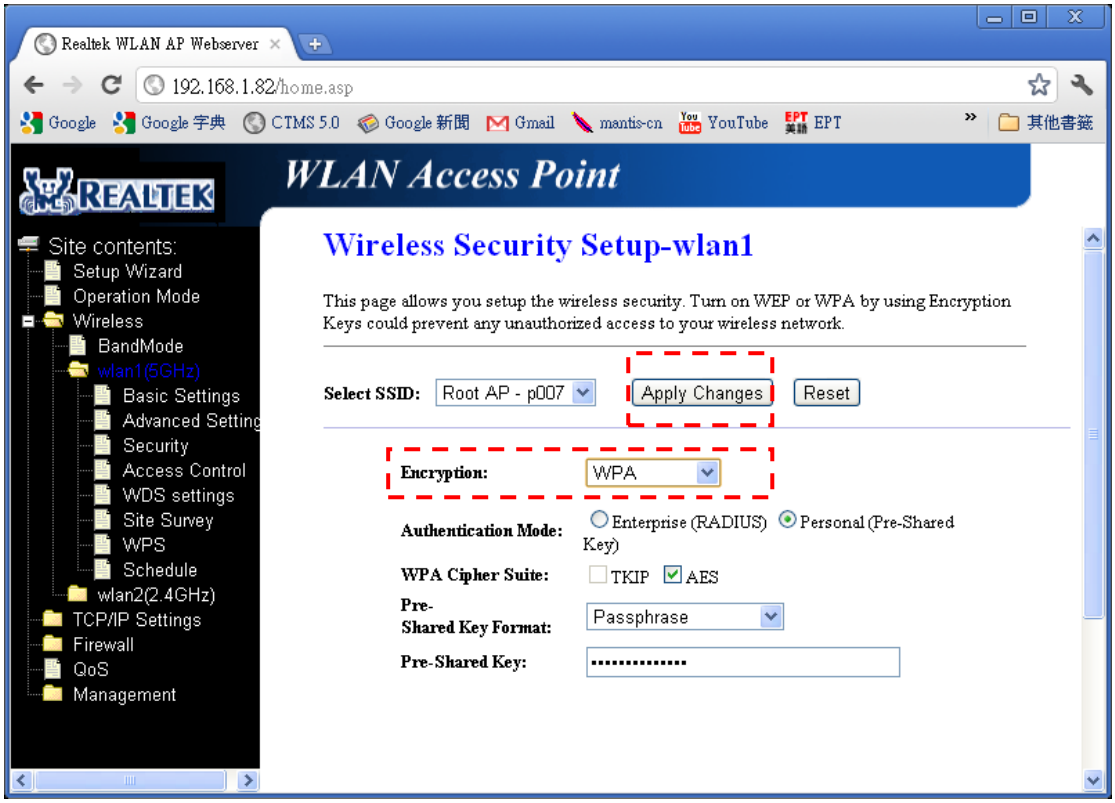


2-2.Under AP mode if security set to WEP, GUI must warning that will bring WPS2 daemon be disabled.

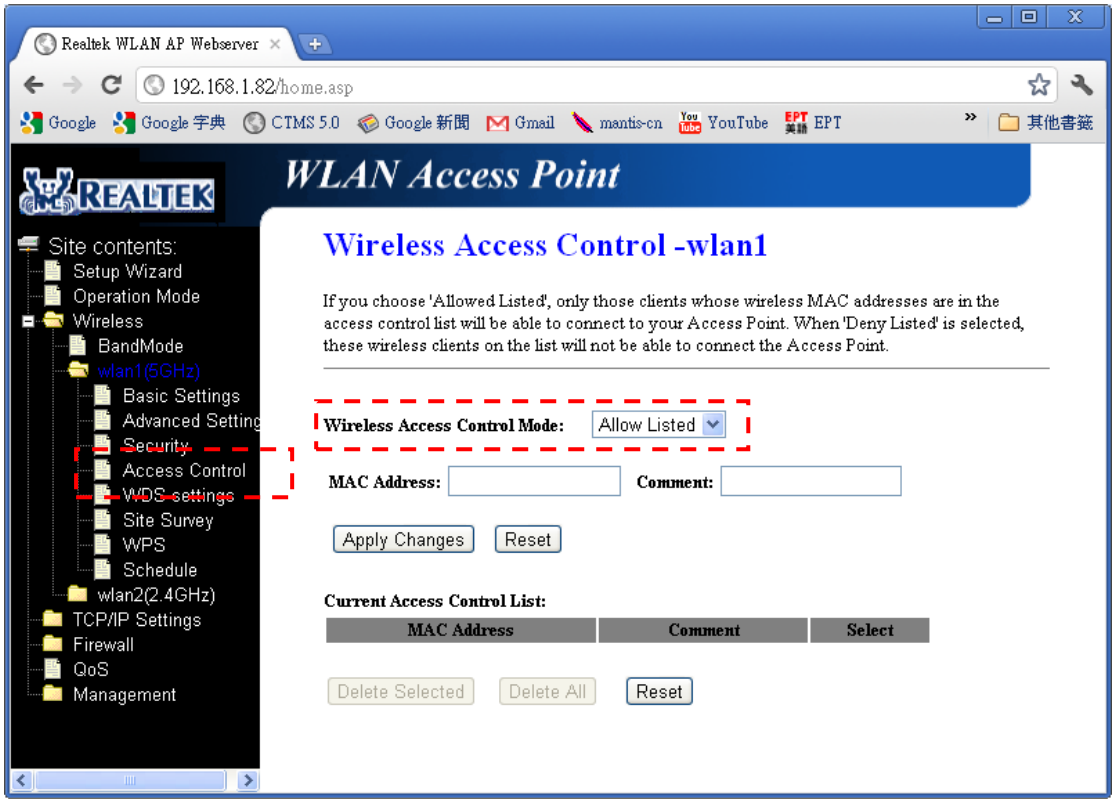




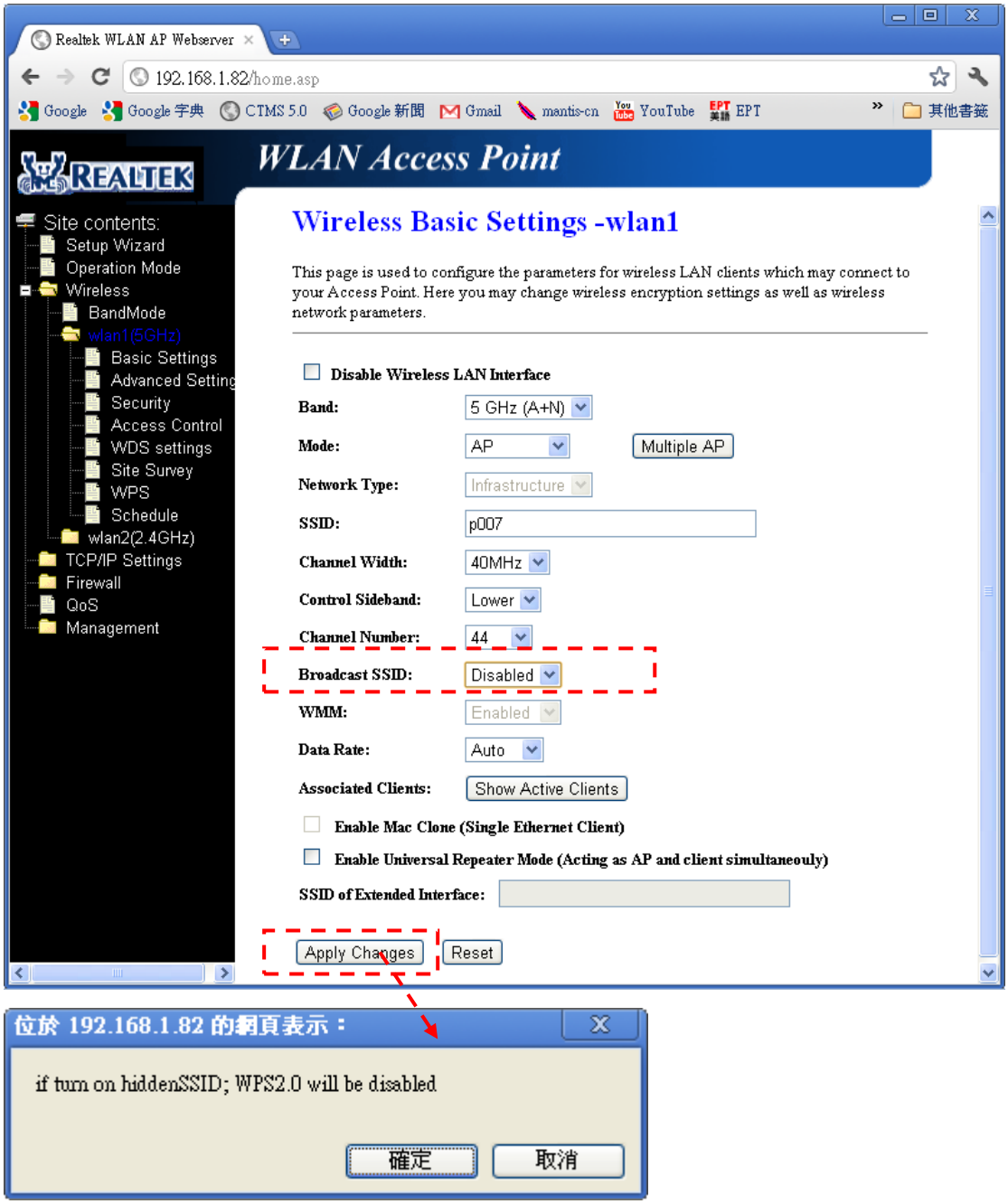
2-3.Under AP mode if security set to WPA only/TKIP only, GUI must warning that will bring WPS2 daemon be disabled.



3. if Access control list is enabled and mode is Allow Listed, GUI must warning that will bring WPS2 daemon be disabled.



4. If Hidden SSID is enabled(broadcast SSID is disabled), GUI must warning that will bring WPS2 daemon be disabled.



Chap7. WPS2.0 client mode GUI(not supported at jungle 2.5.1 now)

After SDK 1.3.1 , WPS2.0 client mode be supported , and have some modify at GUI, the red dotted line in the below picture to show that we add a feature on client mode.

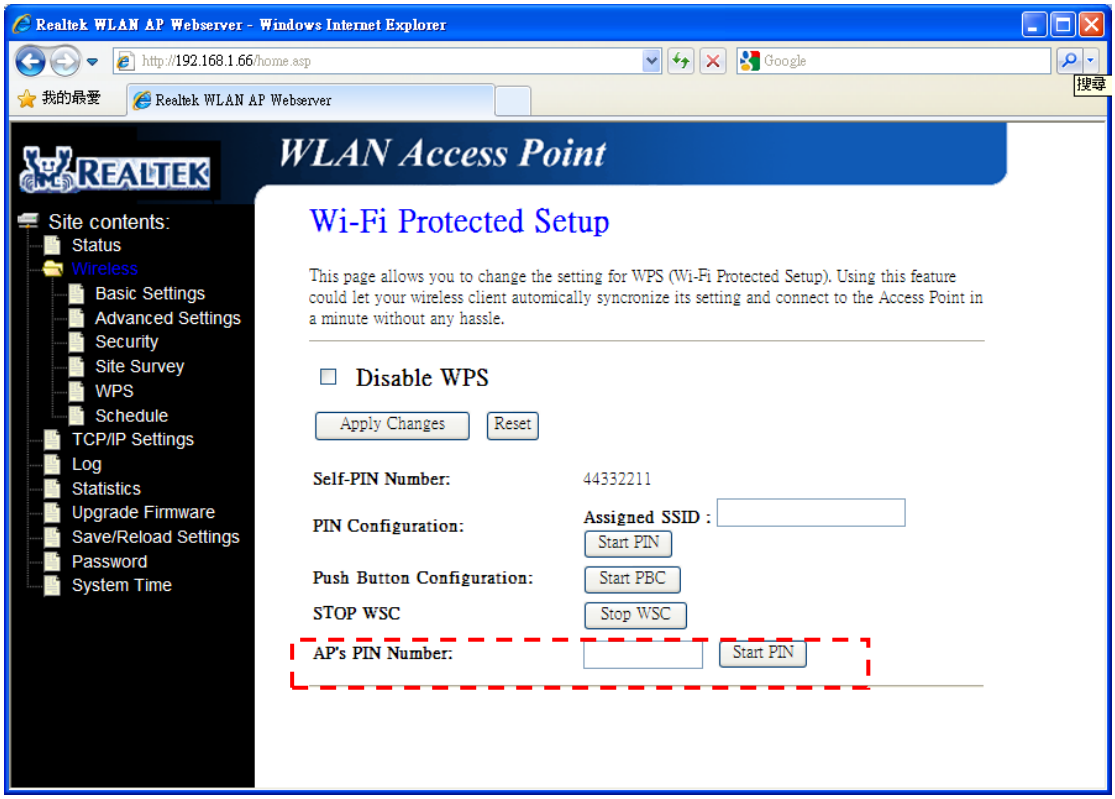
It is not fully support external registrar function, for example it's not support as ER to config enrollee via AP(as proxy).

Feature description:
Client mode can support port of external registrar function

A. if target AP is under configured status , it will learn AP's profile by M7(from AP)
B. if target AP is under un-configured status , it will auto generated profile and configure AP by M8,the auto generated profile like below format

1. SSID
= WPS4965f00660 (WPS(prefix)+length=10, random string)
(in wscd.conf file: disable_auto_gen_ssid=1 , SSID_prefix no setting)
= Prefix+MacAddr
(in wscd.conf file:disable_auto_gen_ssid=1 , SSID_prefix = "some string")
= WLAN0_SSID at flash mib
(in wscd.conf file: disable_auto_gen_ssid no setting or = 0)

2. Auth Type=WPA2PSK (fixed)
3. Encrypt Type=AES (fixed)
4. key=47db9fa753072f8212b4c5 , length=22 , random string



Chap8. WPS PIN brute force attack mitigation

Reference WPS2 SPEC 2.02 version, implement WPS PIN brute force attack mitigation,

enter lock-down state

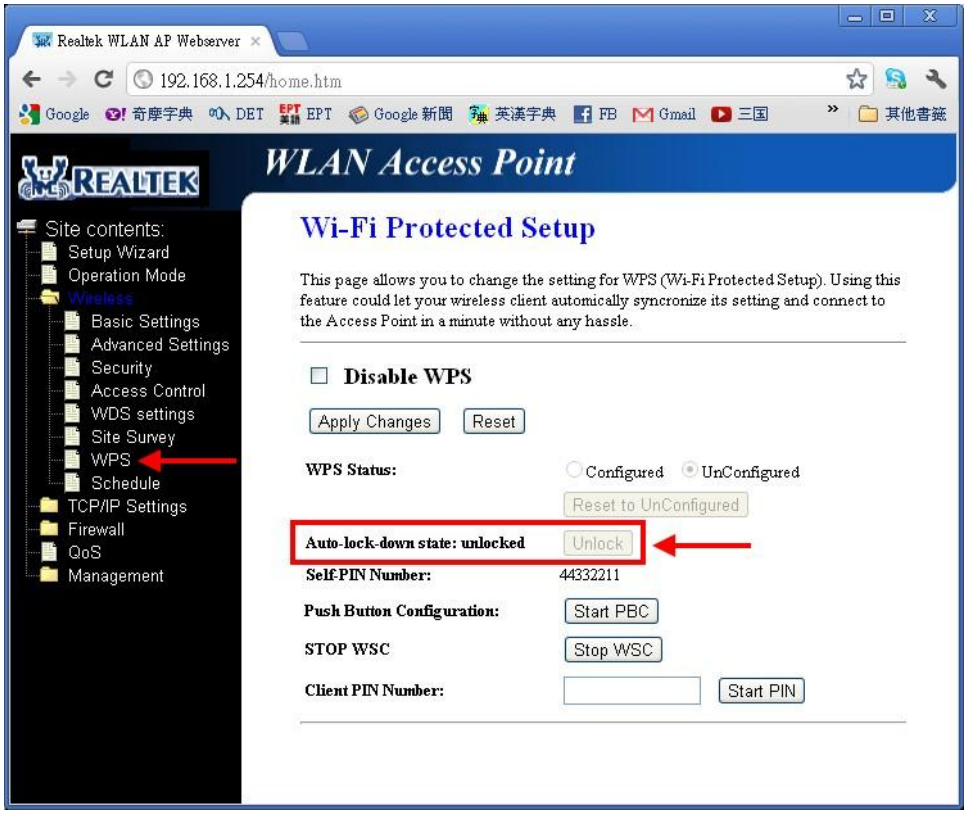
when wscd daemon be attacked by wrong pin code >= MaxPinFailThresHold times then wscd will enter lock-down state and daemon will generated a temp file as "/tmp/wscd_lock_stat"; you can modify MaxPinFailThresHold via wscd.conf, it's defaulr value is 10,valid value 3~10.

exit lock-down state

WPS's lock-down state will continuous until to daemon be restarted(for example system re-init or system power off/on) or user interactive to unlock via web page, so we add 1)text box for show current lock-down state and 2)a button for unlock from locked state, when the unlock button be pushed it will issue a command "wscd -sig_unlock" to signal wscd to unlock, when wscd received signal it will unlock from locked state and remove temp file "/tmp/wscd_lock_stat" by itself.

web page modify, for example

Normal case wscd under unlock, web page as below



When wscd under locked state, web page as below.