Siselectron
TECHNOLOGY

User Guide

SWM3530

Dual Band Long Range Wireless Outdoor Access Point

Table of Contents

Introduction

Key Features

- Up to 29 dBm transmit power enabling long range connectivity
- Supports IEEE 802.11ac/a/b/g/n wireless standards with up to 450 Mbps data rate on 2.4 GHz band and 1300 Mbps on 5 GHz band
- Three detachable 5 dBi 2.4 GHz omni-directional antennas
- Three detachable 7 dBi 5 GHz omni-directional antennas
- Mesh Supported (2.4 GHz)
- Can be used with included power adapter or via PoE with PoE 802.3at - capable switches or injectors
- Dual Band/Three Stream
- Band Steering shifts Dual Band clients to 5 GHz for better throughput performance
- Secured Guest Network option available

Introduction

The SWM 3530 is a high-powered, long-range 3x3 Dual- Band Wireless 802.11ac/a/b/g/n Outdoor Access Point with speeds up to 450 Mbps on 2.4 GHz and 1300 Mbps on 5 GHz band. It can be configure as an: Access Point, Client Bridge, or WDS (AP, Station & Bridge). The SWM 3530 is designed to operate in a variety of outdoor environments. Its high-powered, long-range characteristics make it a cost-effective alternative to ordinary Access Points that don't have therangeandreachtoconnecttoagrowingnumbe wireless users who wish to connect to a business network. The SWM 3530 supports the 2.4 GHz frequency band under 802.11b/g/n mode while at the same time providing 5 GHz band under 802.11ac/a/n mode for

communicating to and from 5 GHz capable computers, tablets or smart phones or transferring files. Several SWM3530s can be deployed in a campus setting using the 5 GHz band as a backhaul to provide multiple 2.4 GHz wireless cells for computers or mobile devices in common outdoor areas.

The SVM 3530 also supports wireless encryption including Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) Encryption, and IEEE 802.1x with RADIUS.

System Requirements

The following are the Minimum System Requirements in order to configure the device.

- Computer with an Ethernet interface or wireless network capability
- Windows OS (XP, Vista, 7), Mac OS, or Linux-based operating systems
- Web-Browsing Application (i.e.: Internet Explorer, Firefox, Safari, or another similar browser application)

Package Contents

The SWM 3530 package contains the following items:*

- SWM 3530 Access Point
- 3 detachable 5 dBi 2.4 GHz omni-directional antennas • 3 detachable 7 dBi 5 GHz omni-directional antennas
- PowerAdapter (48V/0.8A)
- PoE Injector (EPE-48GR)
- Grounding Cable
- Pole Mount Bracket
- Wall Mount Base
- Mounting Screw Set
- Quick Installation Guide

*(all items must be in package to issue a refund)

Technical Specifications

Standard: IEEE802.11ac/a/n
on 5 GHz IEEE802.11b/g/n
on 2.4 GHz IEEE802.3at

Antenna
6 External N-type Antennas
- 3 x detachable 5 dBi 2.4 GHz omni-directional antennas
- 3 x detachable 7 dBi 5 GHz omni-directional antennas

Physical Interface
2 x 10/100/1000 Gigabit Ethernet Port with PoE support
- LAN1 Port: IEEE 802.3at PoE Input
- LAN2 Port: IEEE 802.3af PoE Output
- Both Ethernet Ports support Surge Protection to 6KV

LED Indicator
Power
LAN 1
LAN 2
2.4 GHz
5 GHz

Power Requirements
External Power Adapter, DC IN, 48V/0.8A
IEEE 802.3at support

Operation Modes
Access Point
WDS
Mesh

WDS Detail
WDS AP WDS
Bridge
WDS Station

Mesh Detail
Mesh AP
Mesh Only (2.4 GHz)

Management
Auto Channel Selection
Multiple SSID: 16 SSIDs, 8 SSIDs per Radio
BSSID
SNMP V1/V2c/V3
MIB I/II, Private MIB
VLAN Tag/VLAN Pass-through
Clients Statistics
Save Configuration as User Default
Fast Roaming
E-Mail Alert
RADIUS Accounting
Guest Network Band
Steering
Fast Handover

MIB
I/II
Private MIB

Spanning Tree Protocol
Supports 802.1d Spanning Tree Protocol

Control
CLI Supported
Distance Control (Ack Timeout)
802.1X Supplicant (CB Mode)
Multicast Supported
Auto Reboot

Security
WEP Encryption - 64/128/152 bit
WPA/WPA2 Personal (WPA-PSK using TKIP or AES) WPA/WPA2 Enterprise (WPA-PSK using TKIP or AES) Hides SSID in beacons
MAC address filtering, up to 50 MACs
Wireless STA (Client) connection list Https Support
SSH Support

QoS (Quality of Service)
Complaint with IEEE 802.11e standard

Certifications
FCC/IC/CE

Waterproof
IP68-Rated

Physical/Environment Conditions
Operating:
Temperature: -4 °F to 158 °F (-20 °C to 70 °C)
Humidity (non-condensing): 90% or less
Storage:
Temperature: -22 °F to 176 °F (-30 °C to 80 °C)
Humidity (non-condensing): 90% or less

Physical Interface

Dimensions and Weights

Length: 11.22"
Width: 8.58"
Depth: 2.10"
Weight: 4.17 lbs

1 2.4 GHz Antennas: Detachable 5 dBi 2.4 GHz omni-directional

2 5 GHz Antennas Detachable 7 dBi 5 GHz omni-directional

3 LAN Port 1 (802.3at PoE Input): Ethernet port for RJ-45 cable.

4 LAN Port 2 (802.3af PSE Output): Ethernet port for RJ-45 cable.

5 LED Indicators: LED lights for Power, LAN Port 1, LAN Port 2, 2.4 GHz Connection and 5 GHz Connection.

6 Ground

7 Mounting Holes: Using the provided hardware, the SWM 3530 can be attached to a wall or pole.

Computer Settings

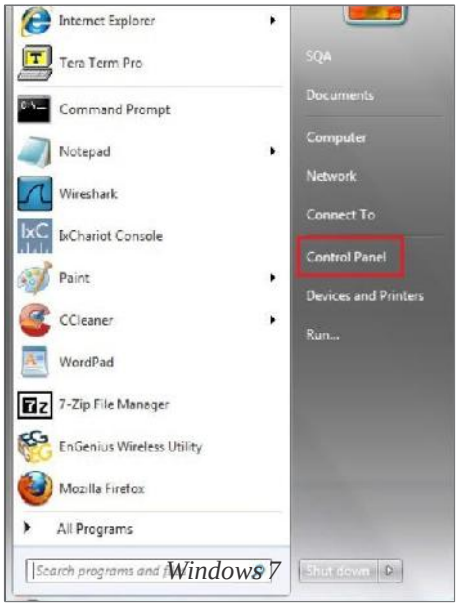
Before You Begin

Windows XP/Windows 7

In order to use the SWM 3530, you must first configure the TCP/IPv4 connection of your Windows OS computer system.

1. Click the Start button and open the Control Panel.

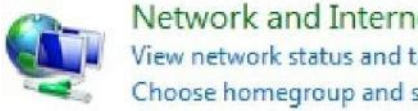
Windows XP

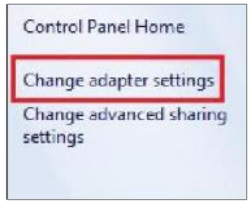


Windows 7

2a. In Windows XP, click Network Connections.

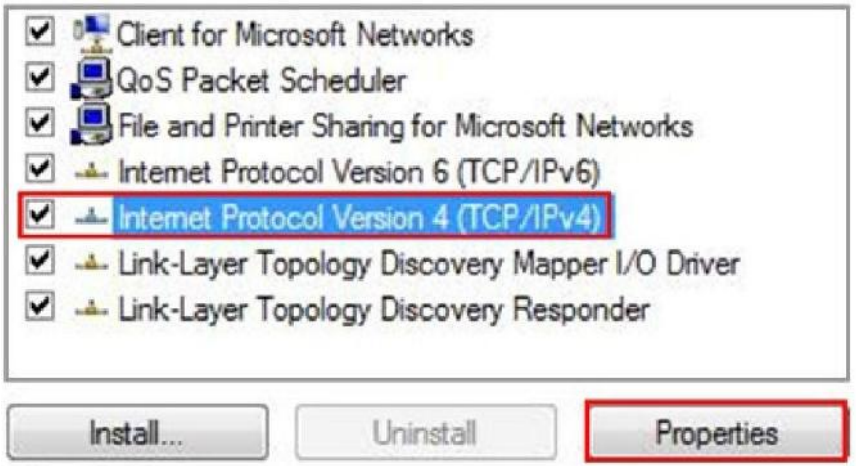
2b. In Windows 7, click View Network Status and Tasks in the Network and Internet section, then select Change adapter settings.





3. Right click on Local Area Connection and select Properties.

4. Select Internet Protocol Version 4 (TCP/IPv4) and then select Properties.



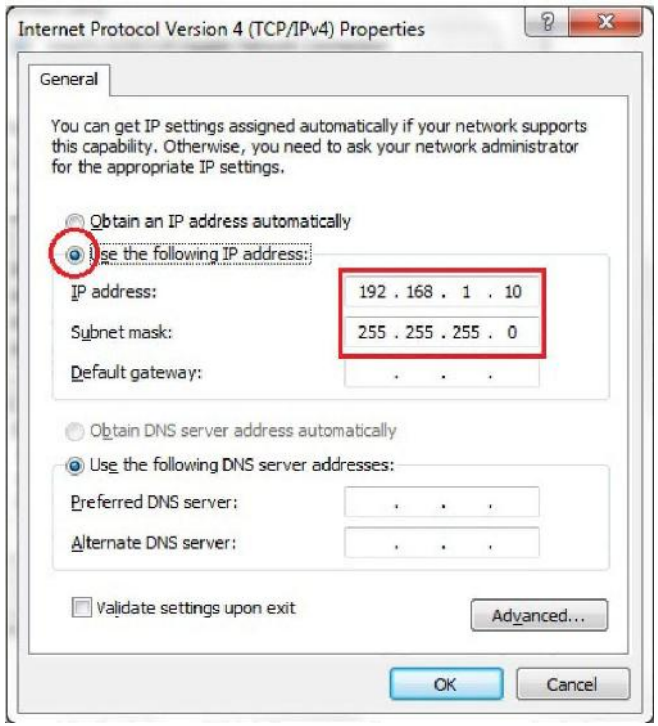
5. Select Use the following IP address and enteran IP address that is different from SWM 3530 and Subnet mask, then click ok.

Note: Ensure that the IP address and Subnet mask are on the same subnet as the device.

For example: SWM 3530 IP address:

192.168.1.1 IP adress: 192.168.1.2-192.168.1.255

PC Subnet mask: 255.255.255.0



Apple Mac OS X

1. Go to System Preferences (Which can be opened in the Applications folder or selecting it in the Apple Menu).

2. Select Network in the Internet & Network section.

3. Highlight Ethernet.

4. In Configure IPv4, select Manually.

5. Enter an IP address that is different from the SWM 3530 and Subnet mask then press OK.

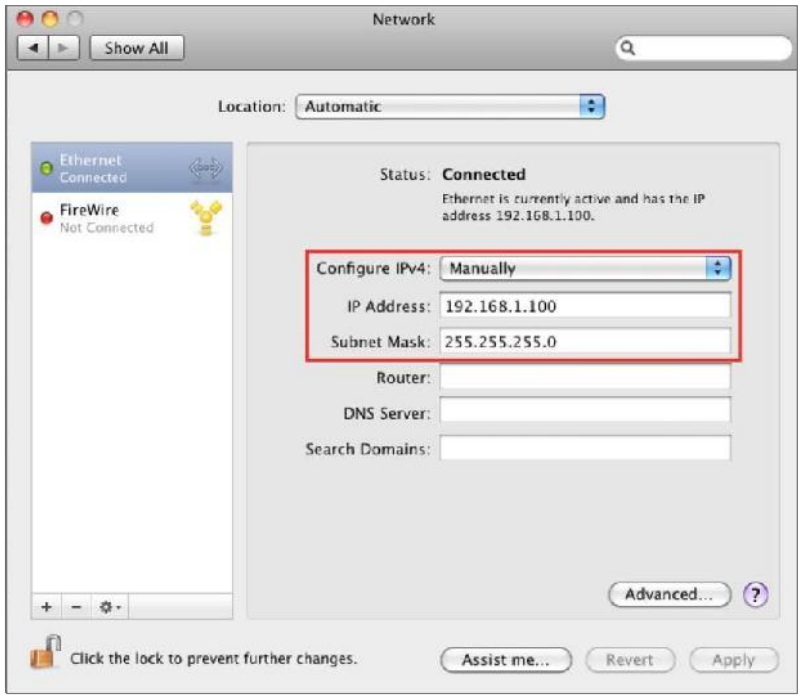
   Note: Ensure that the IP address and Subnet mask are on the same subnet as the device.

   For example: SWM 3530 IP address: 192.168.1.1

   PC IP address: 192.168.1.2–192.168.1.255

   PC Subnet mask: 255.255.255.0

6. Click Apply when done.



Hardware Installation

1. Connect one end of the Ethernet cable into the main LAN port (PoE) of the Access Point and the other end to the AP Ethernet port on the PoE injector.

2. Connect the Power Adapter to the DC-IN port of the PoE injector and plug the other end in to an electrical outlet.

3. Connect the second Ethernet cable into the LAN port of the PoE injector and the other end to the Ethernet port on the computer.

4. Screw on the provided antennas to the device. Once both connections are secure, verify the following:

   a) Ensure that the POWER light is on (it will be green).

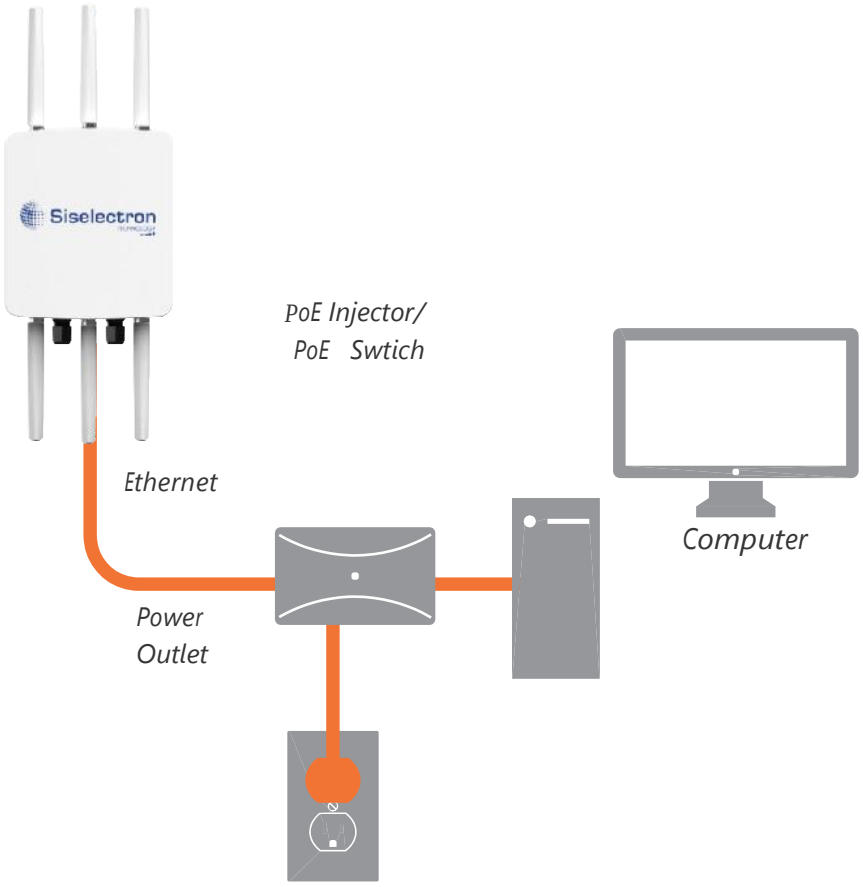
   b) Ensure that the 2.4 GHz/5 GHz WLAN light is on (it will be green for both 5 GHz and 2.4 GHz).

   c) Ensure that the LAN (Computer/SWM 3530 Connection) light is on (it will be green).

   d) Once all three lights are on, proceed to set up the Access Point using the computer.

Note: The Access Point supports both IEEE 802.3at PoE (Power over Ethernet) or the included power injector. You may use either one as the power source. Do NOT use both at the same time.

This diagram depicts the hardware configuration.



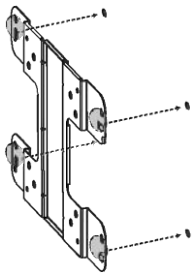
Mounting the SWM 3530

Using the provided hardware, the SWM 3530 can be attached to a wall or a pole.

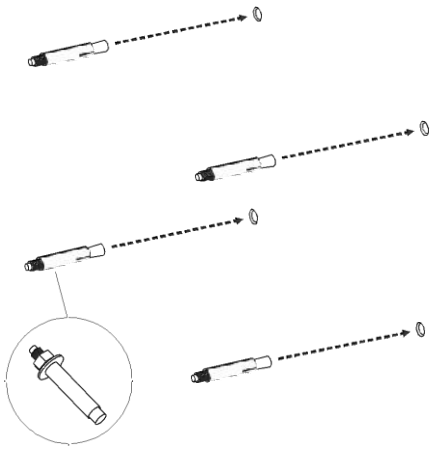
To attach the SWM 3530 to a wall using wall mounting kit:

1. Mark the four locations of the mounting holes on the flat mounting surface.
2. Drill a 37 mm deep 8 mm hole in the markings and hammer the bolts into the openings.
3. Place the lock and flat washers on the four hex cap screws and drive the screws to attach the bracket to the back of the Access Point.
4. Tighten the flat washers to secure the bracket to the mounting surface.

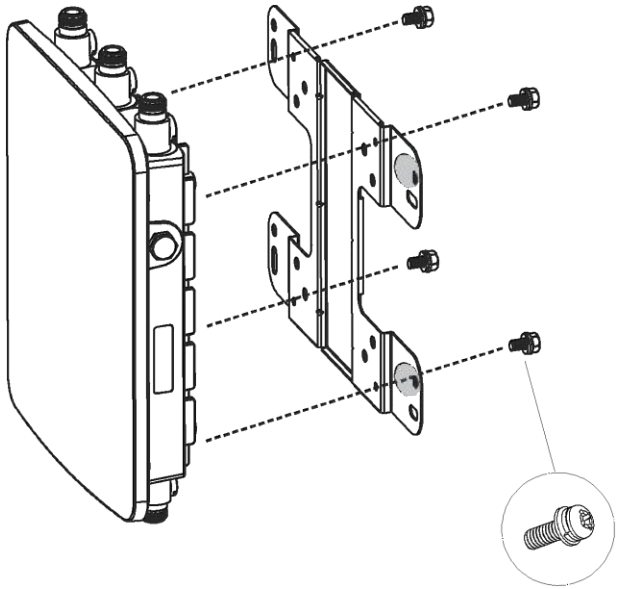
1.



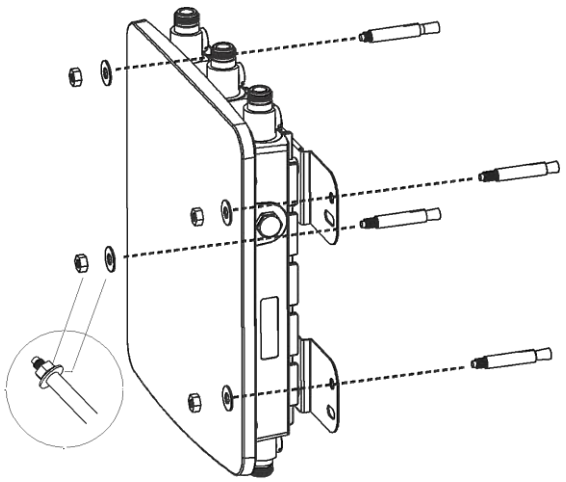
2.



3.



4.

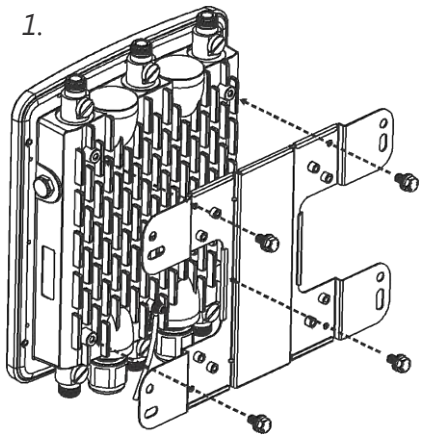


To attach the SWM 3530 to a pole using the provided pole mounting kit:

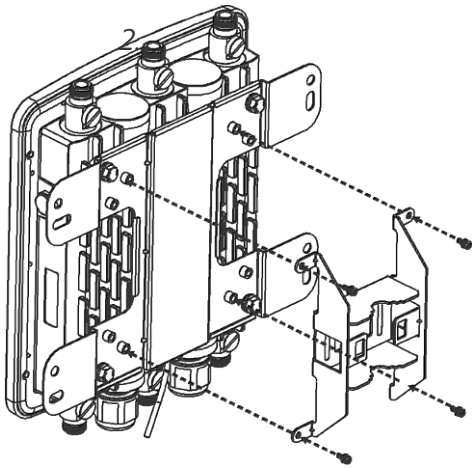
1. Place the lock and flat washers on the four hex cap screws and drive the screws to attach the bracket to the back of the Access Point.
2. Drive the four round head screws to attach the Pole Mount Bracket to the bracket.
3. Thread the open end of the Pole Strap through the two tabs on the Pole Mount Bracket .
4. Lock and tighten the Pole Strap to secure the Pole Mount Bracket to the pole.

Note: See diagram below for vertical and horizontal placements.

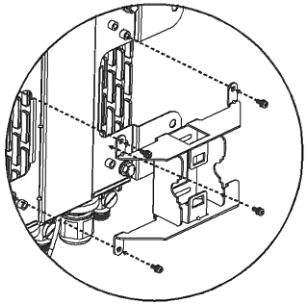
1.

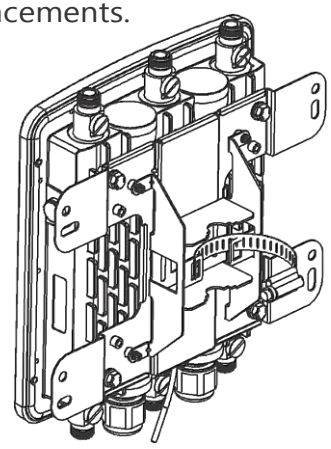


2

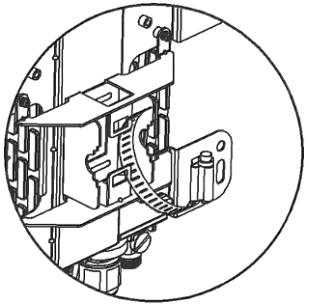


horizontal placement

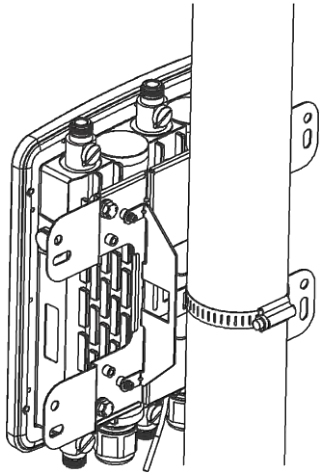




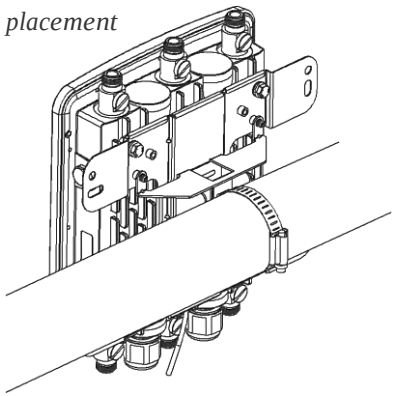
horizontal placement



4.



horizontal placement



Configuring Your Access Point

This section will show you how to configure the device using the web-based configuration interface.

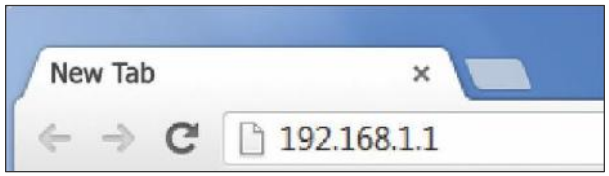
Default Settings

Please use your Ethernet port or wireless network adapter to connect the Access Point.

IP Address	192.168.1.1
Username / Password	admin / admin

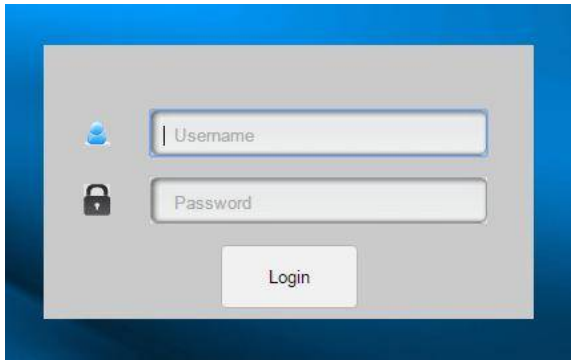
Web Configuration

1. Open a web browser (Internet Explorer/Firefox/Safari/ Chrome) and enter the IP Address http://192.168.1.1.



Note: If you have changed the default LAN IP Address of the Access Point, ensure you enter the correct IP Address.

2. The default username and password are admin. Once you have entered the correct username and password, click the Login button to open the web-based configuration page.

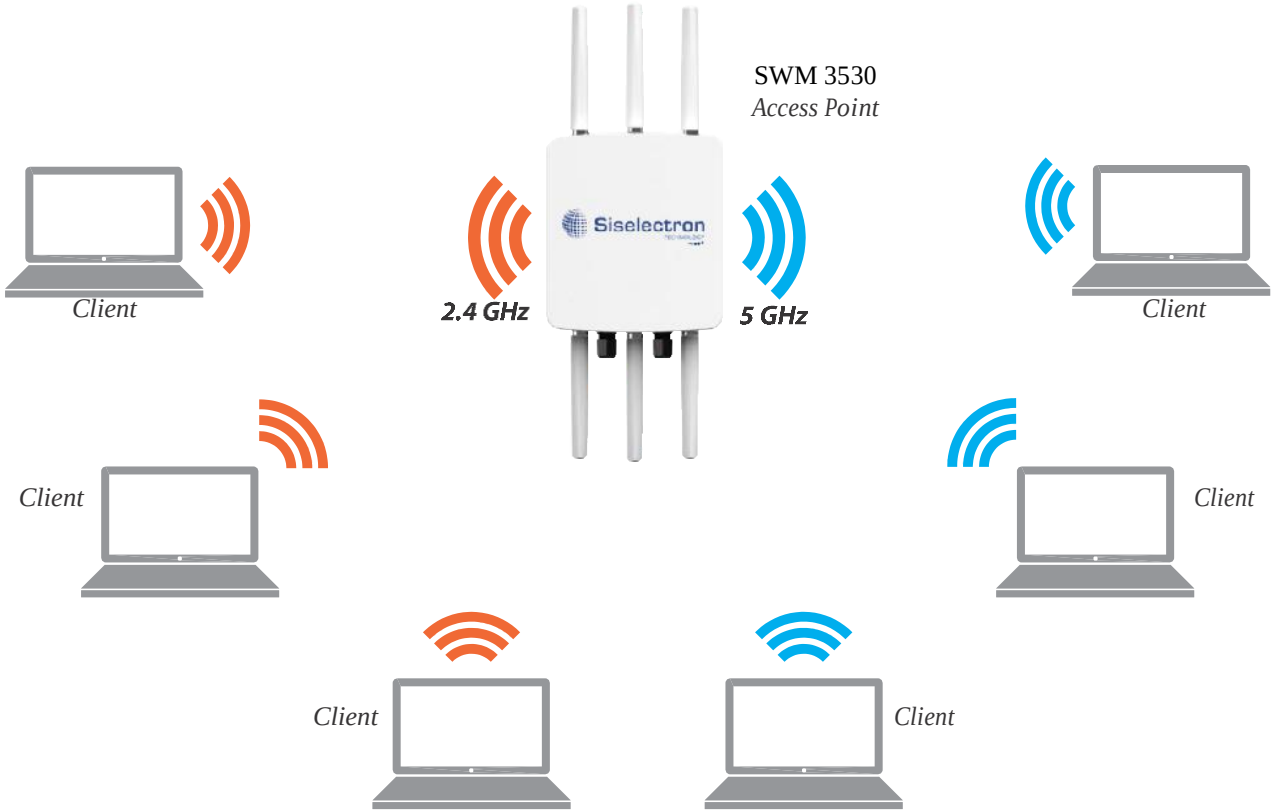


3. If successful, you will be logged in and see the SWM 3530 User Menu.

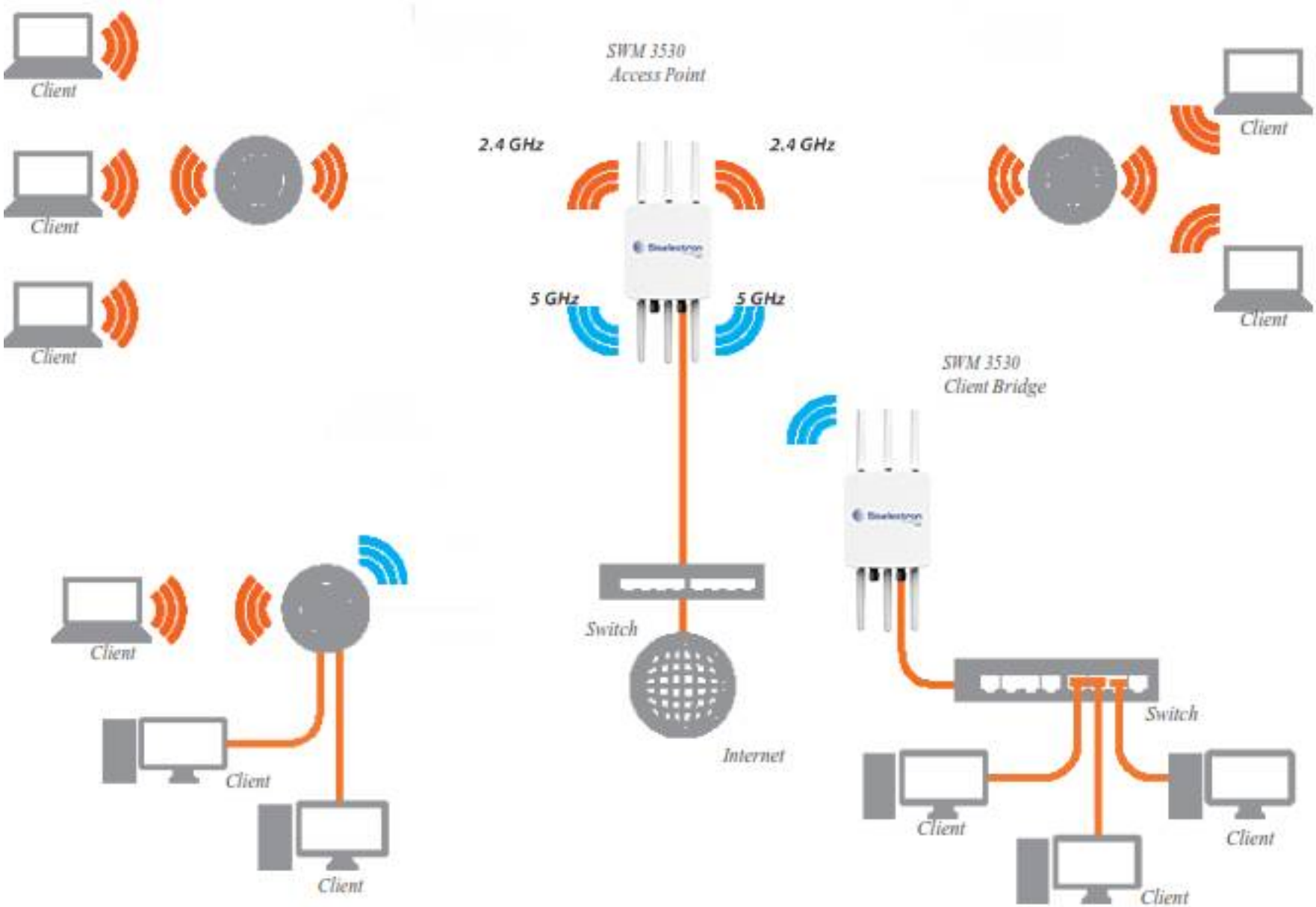
The SWM 3530 has the ability to operate in various modes. This chapter describes the operating modes of the SWM 3530.

Access Point Mode

In Access Point Mode, SWM 3530 behaves likes a central connection for stations or clients that support IEEE 802.11ac/a/b/ g/n networks. The stations and clients must be configured to use the same SSID (Service Set Identifier) and security password to associate with the SWM 3530. The SWM 3530 supports up to eight (8) SSIDs per band at the same time for secure access.

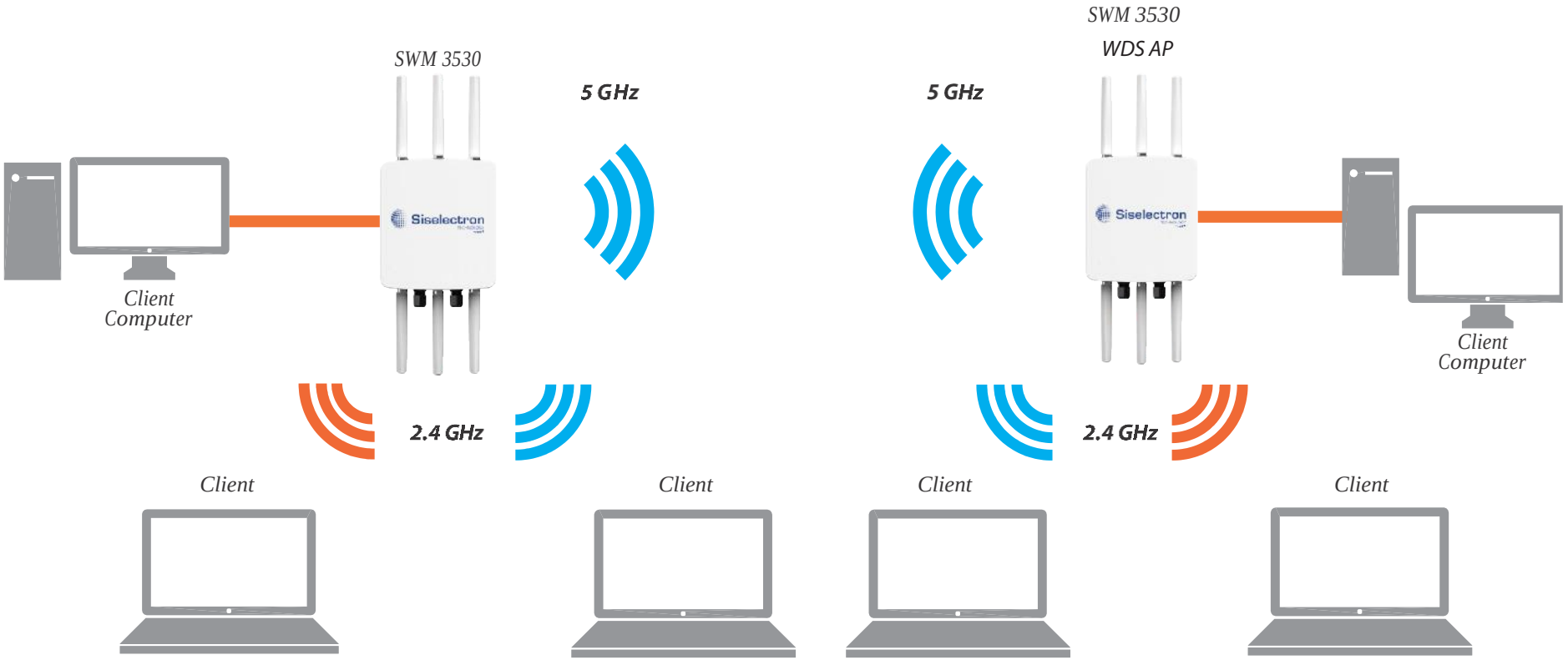


The SWM 3530 can be used as a centralized Outdoor Access Point with which other Siselectron Wireless N 2.4 or 5 GHz Outdoor Client Bridges can associate; leveraging the long-range capability of their internal high-gain directional antennas, resulting in a very cost-effective solution to expand a company network over a multiple building campus.



WDS AP Mode

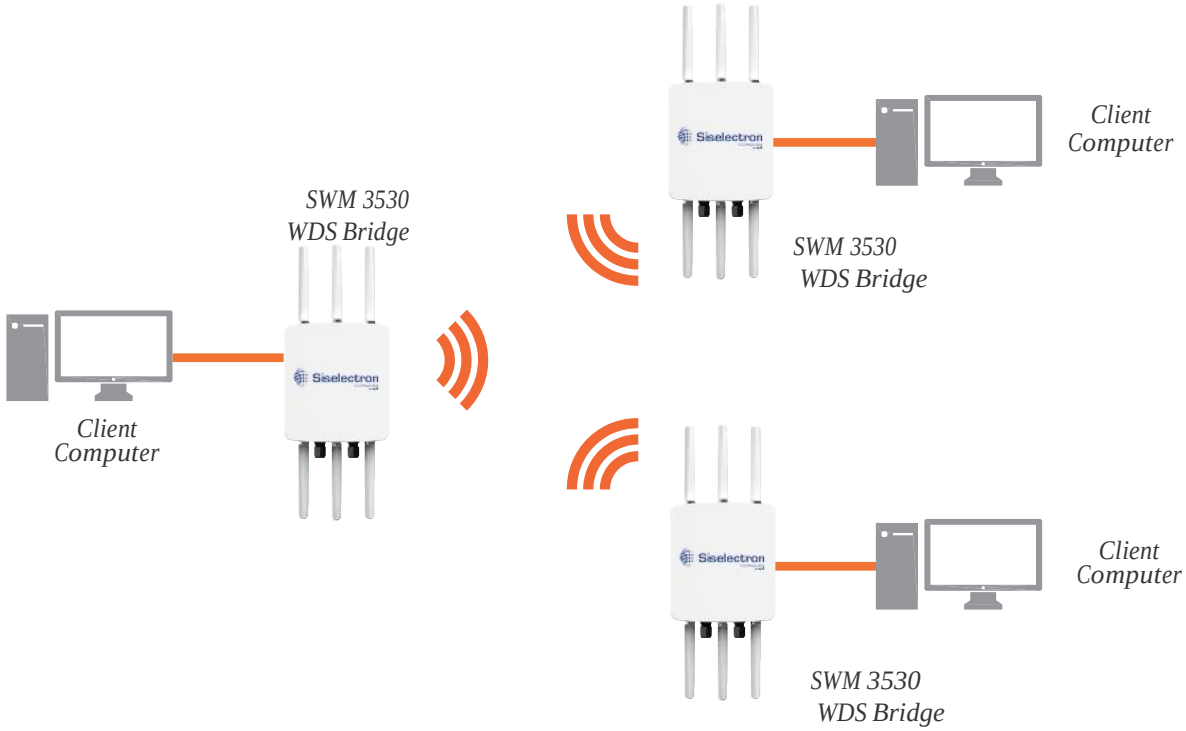
The SWM 3530 also supports WDS AP mode. This operating mode allows wireless connections to the SWM 3530 using WDS technology. In this mode, configure the MAC addresses in both Access Points to enlarge the wireless area by enabling WDS Link settings. WDS supports up to four (4) AP MAC addresses.



WDS Bridge Mode

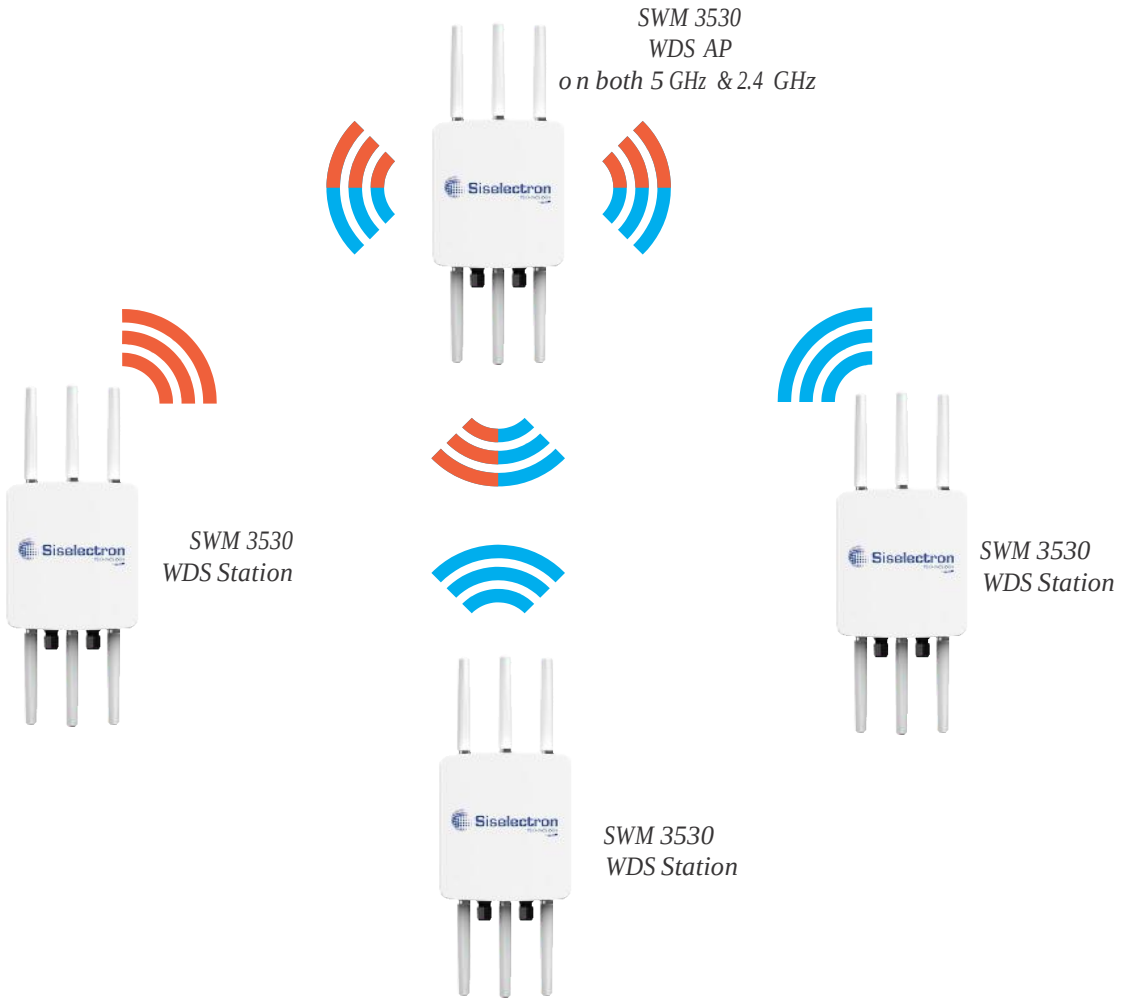
In WDS Bridge Mode, the SWM 3530 can wirelessly connect different LANs by configuring the MAC address and security settings of each SWM 3530 device. Use this mode when two wired LANs located a small distance apart want to communicate with each other. The best solution is to use the SWM 3530 to wirelessly connect two wired LANs, as shown in the following diagram. WDS Bridge Mode can establish up to four (4) WDS links, creating a star-like network.

Note: WDS Bridge Mode does not act as an Access Point. Access Points linked by WDS are using the same frequency channel. More Access Points connected together may lower throughput. This configuration can be susceptible to generate endless network loops in your network, so it is recommended to enable the Spanning Tree feature to prevent this from happening.



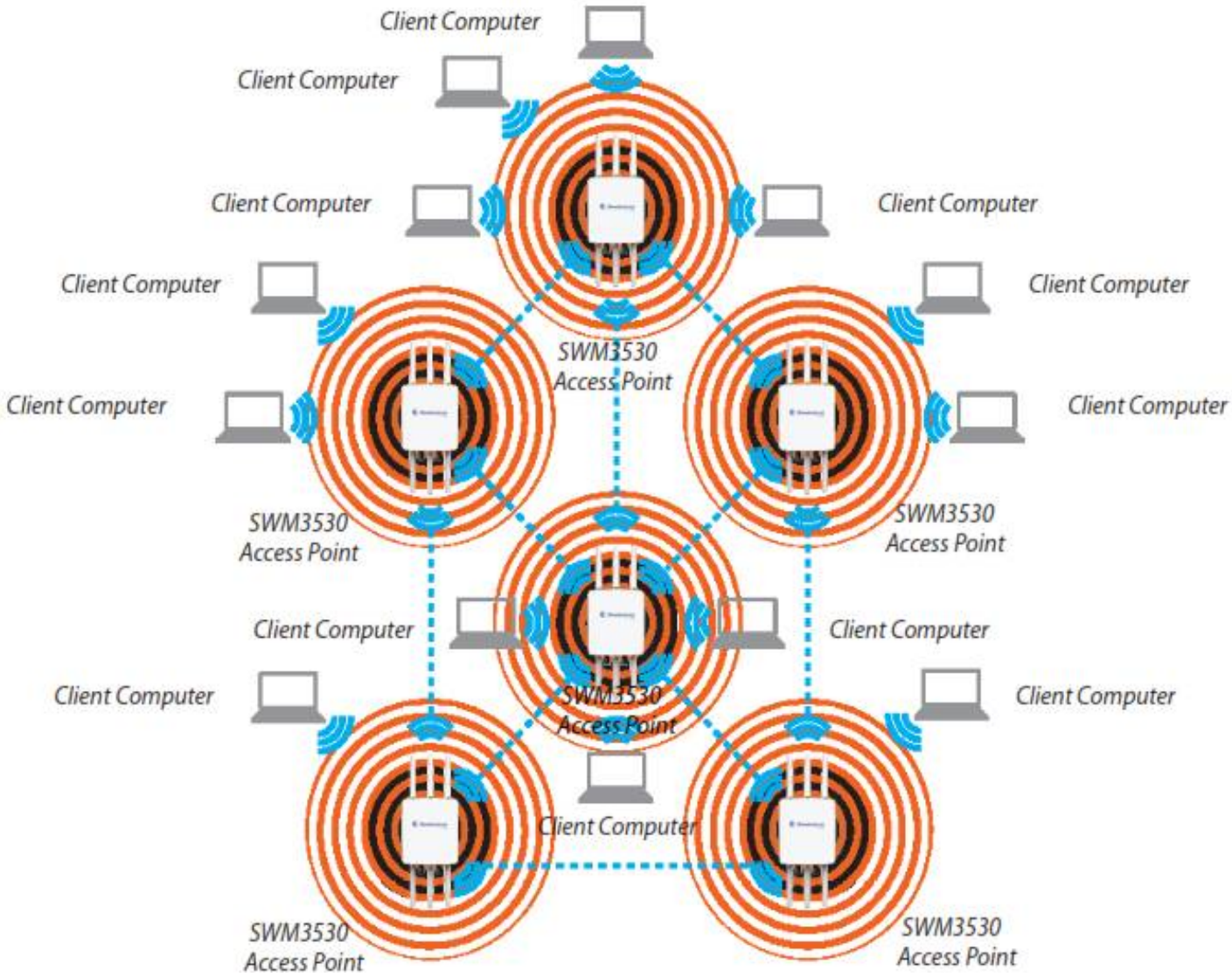
WDS Station Mode

Station mode expands the WDS by receiving a wireless signal/service and sharing it through the Ethernet port.



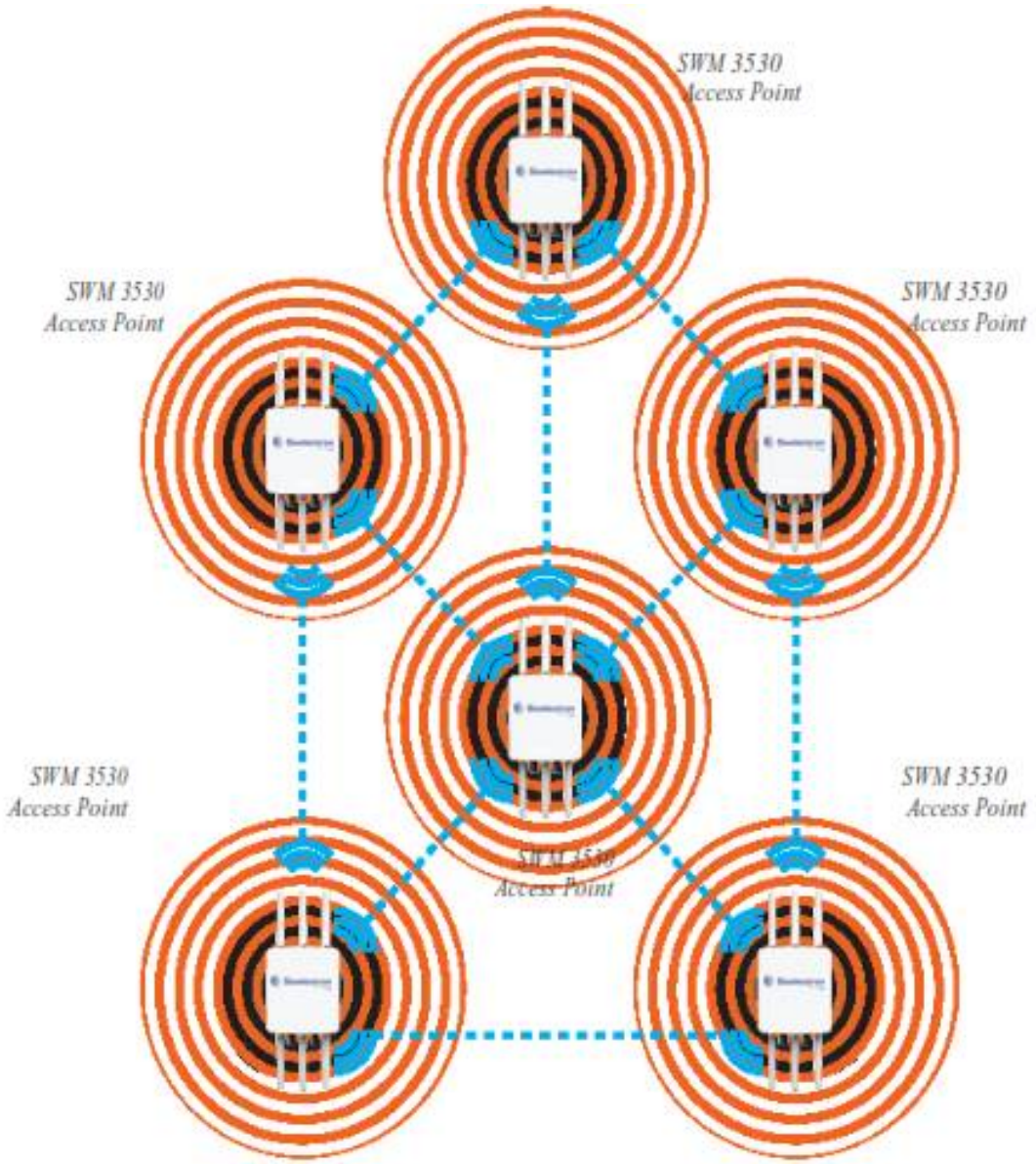
AP Mesh Mode

Under the AP Mesh mode, the SWM 3530 can be used as the central connection hub for station or clients that support IEEE 802.11 b/g/n network. Under this mode, the SWM 3530 can be configured with the same Mesh SSID and security password in order to associate with other SWM 3530s, as well as connect with clients under the same SSID and encryption signatures. For example, you would use one band to connect Access Points in range with Mesh mode and the other band to broadcast traffic on the network.



Mesh Only Mode

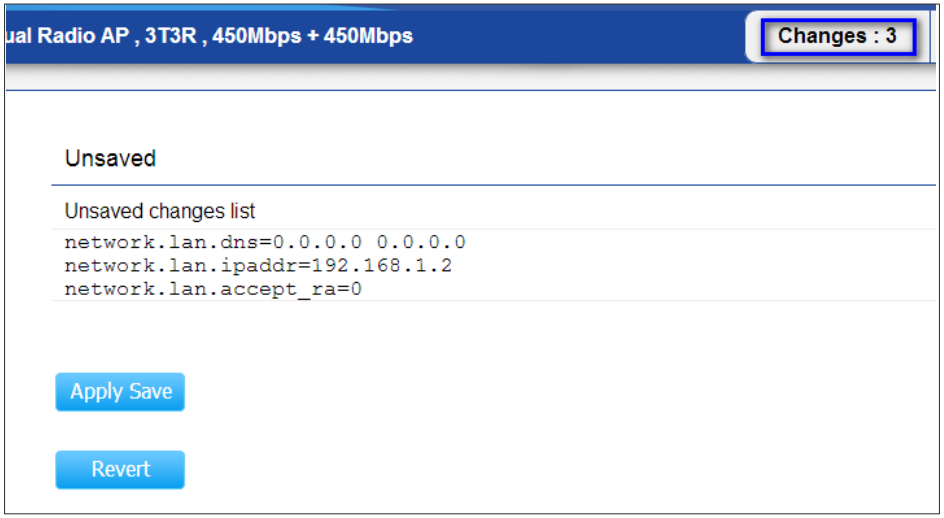
Under the Mesh-only mode, the SWM 3530 can be configured with the same Mesh SSID and security password in order to associate with other Mesh enable SWM 3530s, instead of connecting with clients.



Main Status

Save Changes

This page lets you save and apply the settings shown under Unsaved changes list, or cancel the unsaved changes and revert to the previous settings that were in effect.



Device Status

Clicking the Device Status link under the Overview menu shows the status information about the current operating mode.

- The Device Information section shows general system information such as Device Name, MAC Address, Current Time, Firmware Version, and Management VLAN ID.

  Note: VLAN ID is only applicable in Access Point or WDS AP mode.

Device Information	
Device Name	SWM 3530
MAC Address	
- LAN	88:DC:96:06:3C:94
- Wireless LAN - 2.4GHz	88:DC:96:06:3C:96
- Wireless LAN - 5GHz	88:DC:96:06:3C:97
Country	Default
Current Local Time	Wed Sep 25 03:04:37 UTC 2013
Firmware Version	2.0.0
Management VLAN ID	4096

- The LAN Information section shows the Local Area Network settings such as the LAN IP Address, Subnet mask, and DNS Address.

LAN Information - IPv4

IP Address	192.168.20.3
Subnet Mask	255.255.255.0
Gateway	192.168.20.254
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
DHCP Client	Disable
Spanning Tree Protocol (STP)	Disable

- The Wireless LAN Information 2.4 GHz/5 GHz section shows wireless information such as Operating Mode, Frequency, and Channel. Since the SWM 3530 supports multiple-SSIDs, information about each SSID, the ESSID, and security settings, are displayed

Note: Profile Settings are only applicable in Access Point and WDS AP modes.

Profile	SSID	Security	VID	802.1Q
#1	Siselectron26797E_1-2.4GHz	None	1	Disable
#2	Siselectron26797E_2-2.4GHz	None	2	Disable
#3	Siselectron26797E_3-2.4GHz	None	3	Disable
#4	Siselectron26797E_4-2.4GHz	None	4	Disable
#5	Siselectron26797E_5-2.4GHz	None	5	Disable
#6	Siselectron26797E_6-2.4GHz	None	6	Disable
#7	Siselectron26797E_7-2.4GHz	None	7	Disable
#8	Siselectron26797E_8-2.4GHz	None	8	Disable

Wireless Settings - 2.4GHz

No.	Enable	SSID	Edit	Security	Hidden SSID	Client Isolation	VLAN Isolation	VLAN ID
1		Siselectron26797E_1-5GHz	Edit	None				1
2		Siselectron26797E_2-5GHz	Edit	None				2
3		Siselectron26797E_3-5GHz	Edit	None				3
4		Siselectron26797E_4-5GHz	Edit	None				4
5		Siselectron26797E_5-5GHz	Edit	None				5
6		Siselectron26797E_6-5GHz	Edit	None				6
7		Siselectron26797E_7-5GHz	Edit	None				7
8		Siselectron26797E_8-5GHz	Edit	None				8

- The Statistics section shows Mac information such as SSID, MAC address, RX and TX.

Statistics

SSID	MAC	RX(Packets)	TX(Packets)
Ethernet	88:DC:96:26:79:7C	94879.436KB(1165000 PKts.)	9382.996KB(14841 PKts.)
sis	88:DC:96:26:79:7F	2455885.747KB(13410524 PKts.)	690713.584KB(10231486 PKts.)

- The Wireless Mesh Information-2.4 GHz section shows wireless information such as Operation Mode, Wireless Mode, Channel Bandwidth, Frequency/ Channel, Mesh SSID and Mesh Security.

Connection

2.4 GHz/5 GHz Connection List

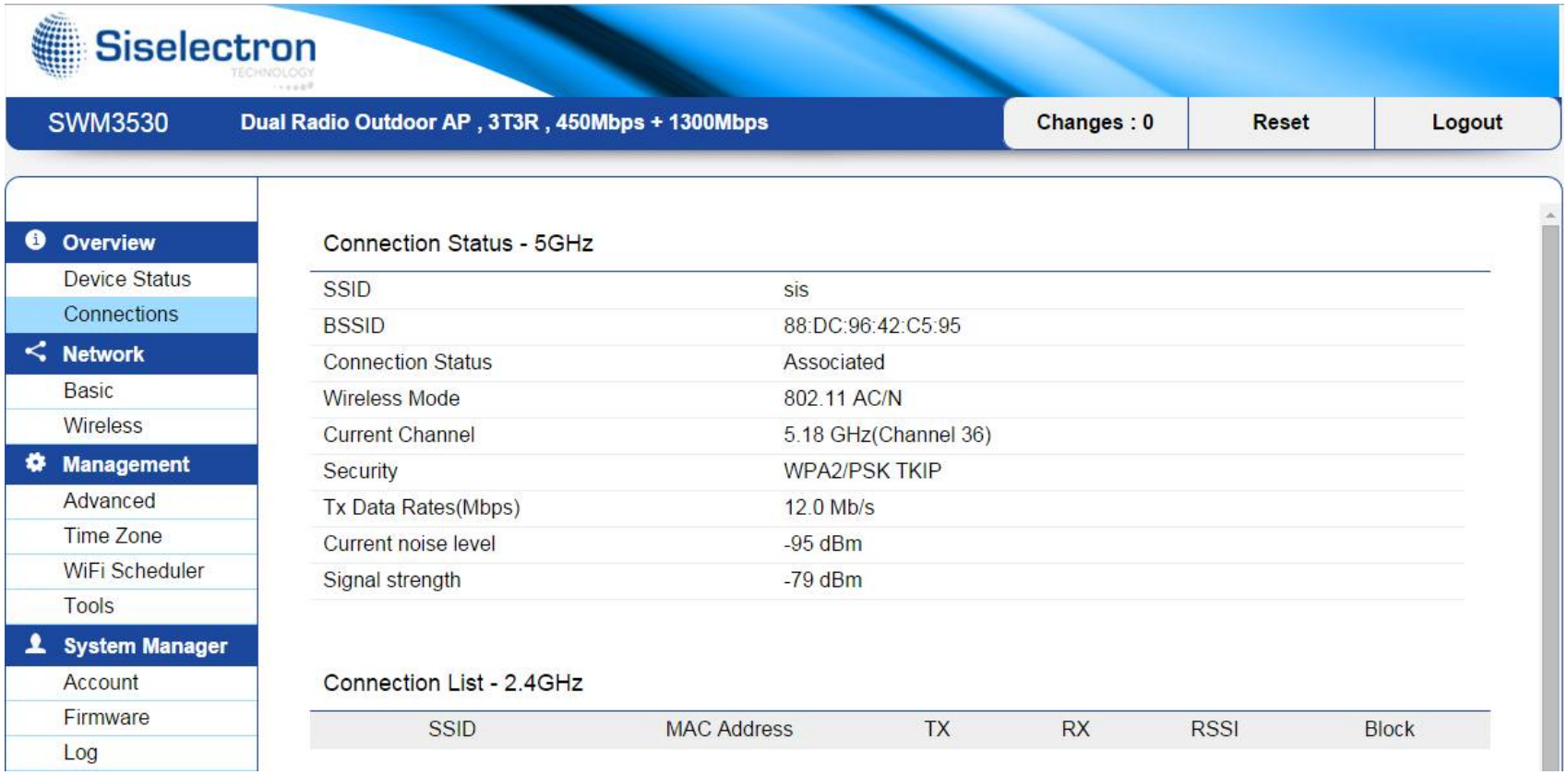
Click the Connection link under the Overview tab to display the connection list of clients associated to the SWM 3530's 2.4 GHz/5 GHz bands, along with the MAC addresses and signal strength for each client. Clicking Refresh updates the client list.

Note: Only applicable in Access Point and WDS AP modes.

2.4 GHz/5 GHz WDS Link List

Click the connection link under the Overview menu. This page displays the current status of the WDS link, including WDS Link ID, MAC Address, Link Status and RSSI.

Note: Only applicable in WDS AP and WDS Bridge modes.



The Mesh Link List

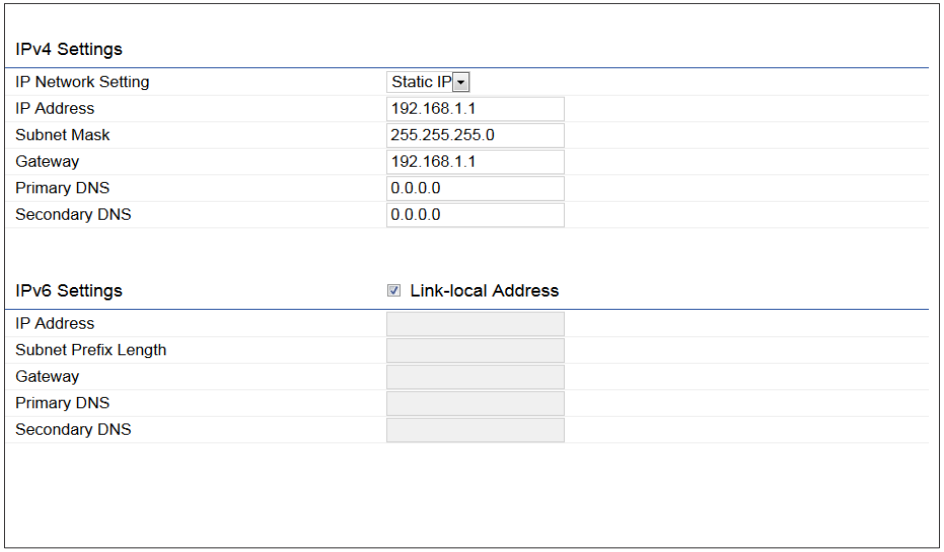
You can monitor the 2.4GHz Mesh Link List under the Status menu. The page will display the current status of the Mesh Links under Mesh AP mode and the Mesh nodes under Mesh Only mode.

Note: Only applicable in the Mesh AP and Mesh Only modes.

Basic IP Settings

IPv4/IPv6 Settings

This page allows you to modify the device's IP settings.



IP Network Settings: Select whether the device IP address will use a static IP address specified in the IP address field or be obtained automatically when the device connects to a DHCP server.

IP Address: Displays the IP address of this device.

Subnet Mask: Displays the IP Subnet mask of this device. Gateway:

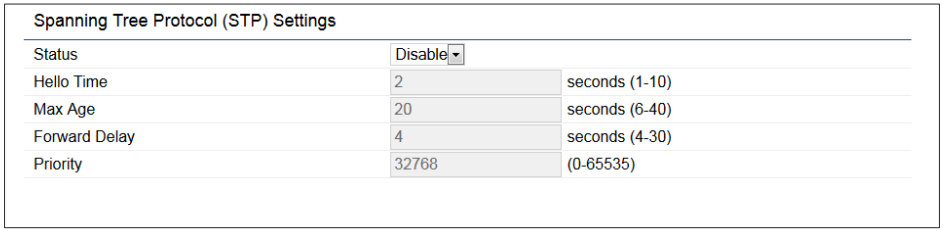
Displays the Default Gateway of this device.
Leave it blank if you are unsure of this setting.

Primary/Secondary DNS: Displays the primary/secondary DNS address for this device.

Save: Click Save to confirm the changes.

Spanning Tree Protocol (STP) Settings

This page allows you to modify the Spanning Tree settings. Enabling the Spanning Tree protocol will prevent network loops in your LAN network.



Spanning Tree Status: Enables or disables the Spanning Tree feature.

Hello Time: Specifies Bridge Hello Time in seconds. This value determines how often the device sends handshake packets to communicate information about the topology throughout the entire Bridged Local Area Network.

Max Age: Specifies Bridge Max Age in seconds. If another bridge in the spanning tree does not send a hello packet for a long period of time, it is assumed to be inactive.

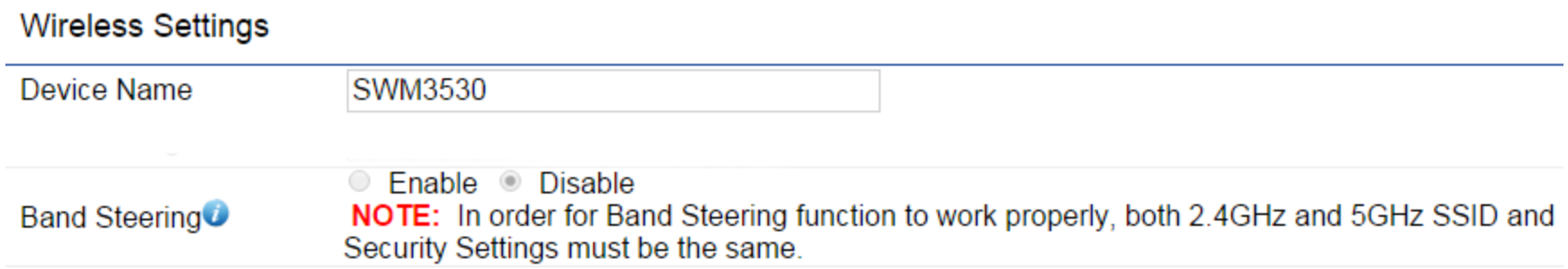
Forward Delay: Specifies Bridge Forward Delay in seconds. Forwarding delay time is the time spent in each of the Listening and Learning states before the Forwarding state is entered. This delay is provided so that when a new bridge comes onto a busy network, it analyzes data traffic before participating in the network.

Priority: Specifies the Priority Number. A smaller number has a greater priority than a larger number.

Save: Click Save to confirm the changes.

Wireless

Wireless Settings



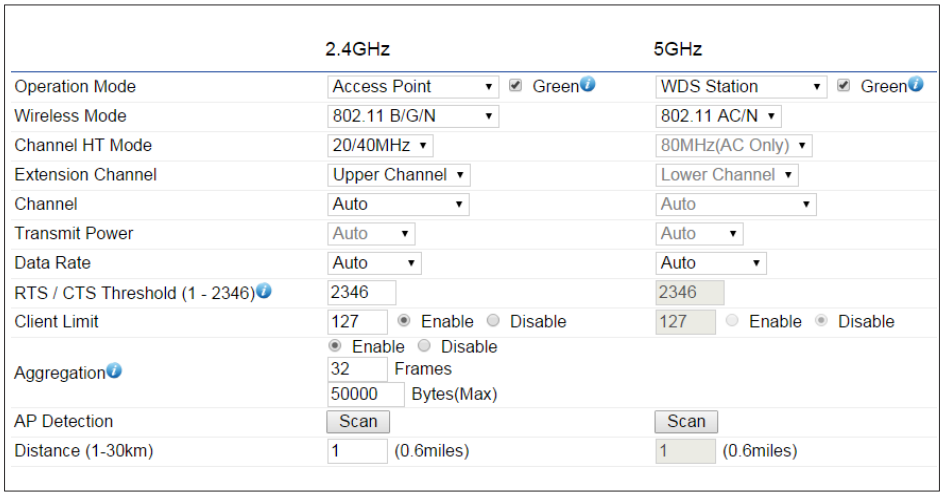
Device Name: Enter a name for the device. The name you type appears in SNMP management. This name is not the SSID and is not broadcasted to other devices.

Band Steering: Enable Band Steering to send 802.11n clients to the 5 GHz band, where 802.11b/g clients cannot go,and leave 802.11b/g clients in 2.4 GHz band to maintain optimal data traffic flow. Band Steering works within the Access Point by directing 5 GHz-capable clients to that band.

Save: Click Save to confirm the changes.

2.4 GHz/5 GHz Wireless Network

This page displays the current status of the Wireless settings of the SWM 3530.



	2.4GHz	5GHz
Operation Mode	Access Point ▾ ☑ Green	WDS Station ▾ ☑ Green
Wireless Mode	802.11 B/G/N ▾	802.11 AC/N ▾
Channel HT Mode	20/40MHz ▾	80MHz(AC Only) ▾
Extension Channel	Upper Channel ▾	Lower Channel ▾
Channel	Auto ▾	Auto ▾
Transmit Power	Auto ▾	Auto ▾
Data Rate	Auto ▾	Auto ▾
RTS / CTS Threshold (1 - 2346)	2346	2346
Client Limit	127 ◉ Enable ○ Disable	127 ○ Enable ◉ Disable
Aggregation	◉ Enable ○ Disable 32 Frames 50000 Bytes(Max)	
AP Detection	Scan	Scan
Distance (1-30km)	1 (0.6miles)	1 (0.6miles)

Operation Mode: Select Operation Mode. The SWM 3530 supports two different operation modes: Access Point, or WDS (WDS AP, WDS Bridge, and WDS Station).

Wireless Mode: Supports 802.11b/g/n mixed mode in 2.4 GHz and 802.11ac/a/n mixed mode in 5 GHz.

Channel HT Mode: The default channel bandwidth is 20 MHz/40 MHz. The larger the channel, the greater the transmission quality and speed.

Extension Channel: Select the upper or lower channel. Your selection may affect the Auto channel feature.

Transmit Power: Sets the power output of the wireless signal.

Data Rate: Select a data rate from the drop-down list. The data rate affects throughput of data in the SWM 3530. Select the best balance for you and your network but note that the lower the data rate, the lower the throughput, though transmission distance is also lowered.

RTS/CTS Threshold: Specifies the threshold package size for RTC/CTS. A smaller number causes RTS/CTS packets to be sent more often and consumes more bandwidth.

Client Limits: Limits the total number of clients.

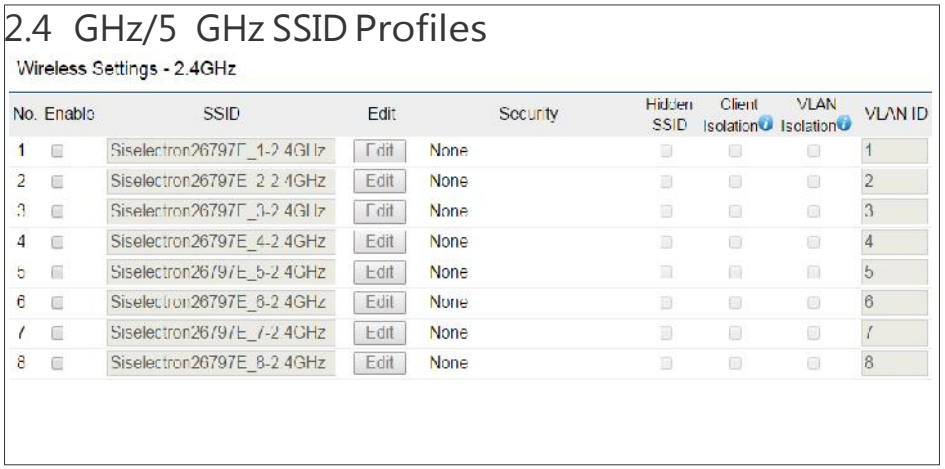
Aggregation: Merges data packets into one packet. This option reduces the number of packets, but also increases packet sizes.

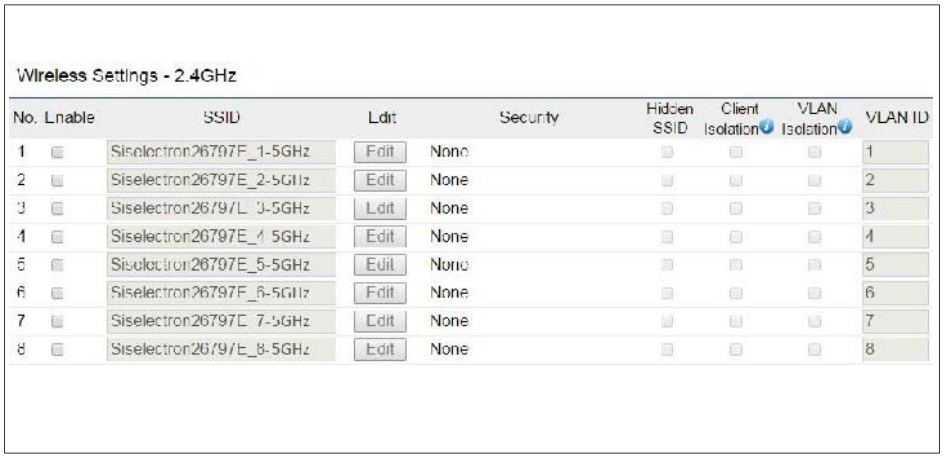
AP Detection: The AP Detection feature can select the best channel to use by scanning nearby areas for Access Points.

Distance: Specifies the distance between Access Points and clients. Note that longer distances may drop higher-speed connections.

Save: Click Save to confirm the changes or Cancel to cancel and return to previous settings.

2.4 GHz/5 GHz SSID Profiles





Current Profile: You can configure up to sixteen (16) different SSIDs (eight (8) per band). If multiple client devices will be accessing the network, you can arrange the devices into SSID groups. Click Edit to configure the profile and check whether you wish to enable extra SSIDs.

SSID: Specifies the SSID for the current profile.

Suppressed SSID: Check this option to hide a SSID from clients. If checked, the SSID will not appear in the site survey.

Station Separation: Check the box to allow or prevent communication between client devices.

VID: Specifies the VLAN tag for each profile. If your netowrk includes VLANs, you can specify a VLAN ID for packets to pass through the Access Point with a tag.

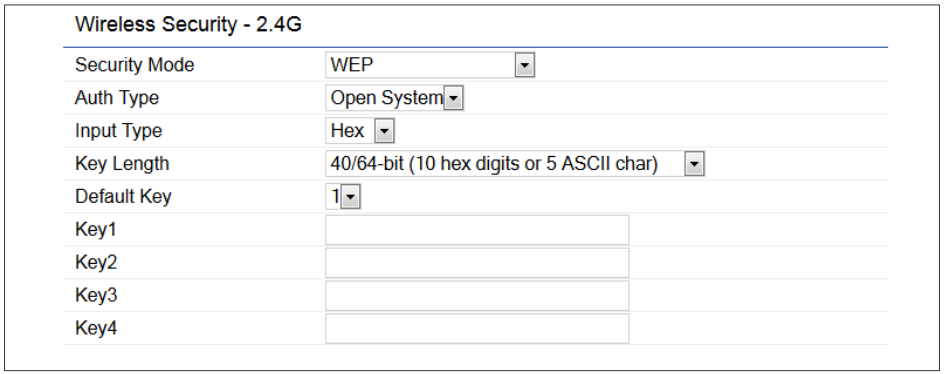
Wireless Security: See the Wireless Security section on page 42.

Isolation: Check the box to restrict clients from communicating with different VIDs.

Save: Click Save to accept the changes.

Wireless Security

The Wireless Security section lets you configure the SWM 3530's security modes: WEP, WPA-PSK, WPA2- PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed. It is strongly recommend that you use WPA2-PSK.



Auth Type: Select Open System or Shared Key. Input

Type:

ASCII: Regular Text (recommended) Hexadecimal Numbers (For advanced users)

Key Length: Select the desired option and ensure that wireless clients use the same setting. Your choices are 64, 128, and 152-bit password lenghts.

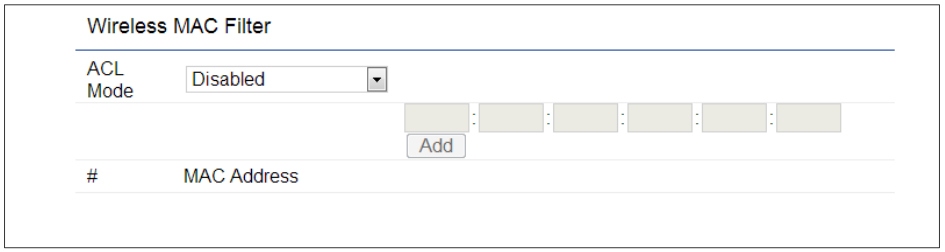
Default Key: Select the Key you wish to be the default value. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a Key Value for the Default Key.

Encryption Key Number: Enter the Key Value or values you wish to use. Only the Key selected as Default is required. The others are optional.

Wireless MAC Filtering

Wireless MAC Filtering is used to allow or deny network access to wireless clients (computers, tablet PCs, NAS, smartphones, etc.) according to their MAC addresses. You can manually add a MAC address to restrict permission to access the SWM 3530. The default setting is: Disable Wireless MAC Filter.

Note: Only applicable in Access Point and WDS AP modes.



ACL Mode: Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC address table on this page. Your choices are: Disabled, Deny MAC in the list, or Allow MAC in the list.

MAC Address: Enter the MAC address of the wireless client.

Add: Click Add to add the MAC address to the MAC address table.

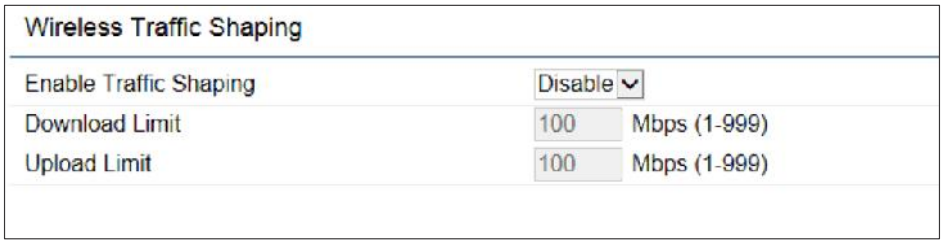
Delete: Deletes the selected entries. Save:

Click Save to apply the changes.

Wireless Advanced

Wireless Traffic Shaping

Traffic shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.



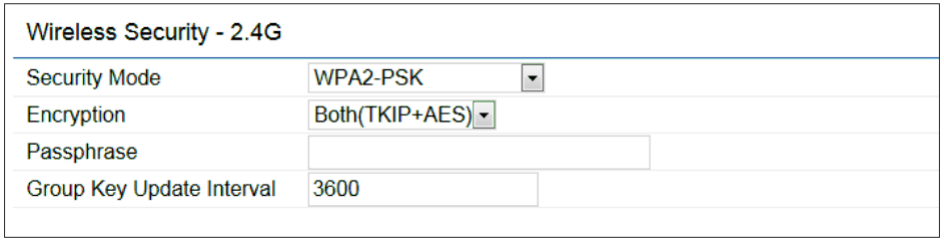
Enable Traffic Shaping: Check this option to enable Wireless Traffic Shaping.

Download Limit: Specifies the wireless transmission speed used for downloading.

Upload Limit: Specifies the wireless transmission speed used for uploading.

Save: Click Save to confirm the changes.

WPA-PSK (WPA Pre-Shared Key) Encryption:

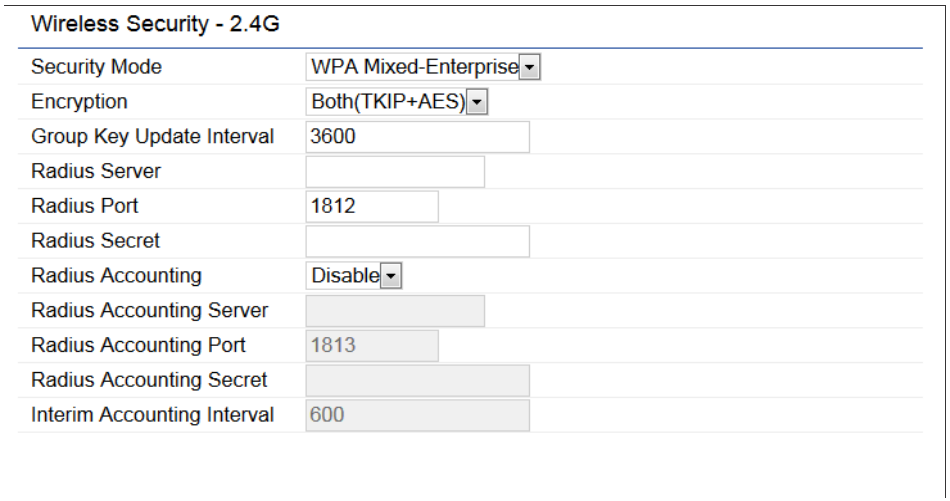


Encryption: Select the WPA encryption type you would like to use. Please ensure that your wireless clients use the same settings.

Passphrase: Wireless clients must use the same Key to associate the device. If using ASCII format, the Key must be from 8~63 characters in length. If using HEX format, the Key must be 64 HEX characters in length.

Group Key Update Interval: Specifies how often, in seconds, the Group Key Changes.

WPS Mixed-Enterprise: Access Point / WDS AP Mode



Encryption: Select the WPA encryption type you would like to use. Please ensure that your wireless clients use the same settings.

Radius Server: Enter the IP address of the Radius server.

Radius Port: Enter the port number used for connections to the Radius server.

Radius Secret: Enter the secret required to connect to the Radius server.

Group Key Update Interval: Specifies how often, in seconds, the Group Key changes.

Radius Accounting: Enables or disables the accounting feature.

Radius Accounting Server: Enter the IP address of the Radius accounting server.

Radius Accounting Port Enter the port number used for connections to the Radius accounting server.

Radius Accounting Secret: Enter the secret required to connect to the Radius accounting server.

Interim Accounting Interval: Specifies how often, in seconds, the accounting data sends.

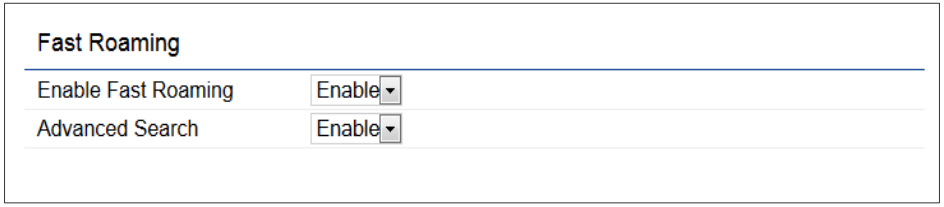
Note: 802.11n does not allow WEP/WPA-PSK TKIP/ WPA2-PSK TKIP security mode. The connection mode will automatically change from 802.11n to 802.11g.

Fast Roaming

Enable this feature to serve mobile client devices that roam from Access Point to Access Point. Some applications running on client devices require fast re-association when they roam to a different Access Point

Please enter the settings of the SSID and initialize the Security mode to WPA Enterprise, as well as setting the Radius Server. Users can then enable Fast Roaming and implement the advanced search feature.

Next, set the same Enterprise Encryption with the same SSID on other Access Points in the network and enable Fast Roaming. When the configuration is set on all the Access Points on the network, mobile client devices can run voice services that require fast roaming to prevent delay in conversation from Access Point to Access Point.



Enable Fast Roaming: Enables or disables the Fast Roaming feature.

Enable Advanced Search: Enables or disables the Advanced Search feature.

WDS Link Settings

Using the WDS (Wireless Distribution System) feature will allow a network administrator or installer to connect to Access Points wirelessly. Doing so will extend the wired infrastructure to locations where cabling is not possible or inefficient to implement.

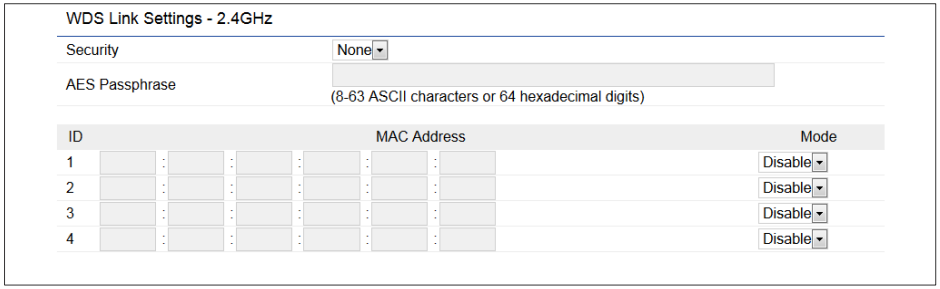
Note: Compatibility between different brands and models of Access Points is not guaranteed. It is recommended that the WDS network be created using the same models for maximum compatibility.

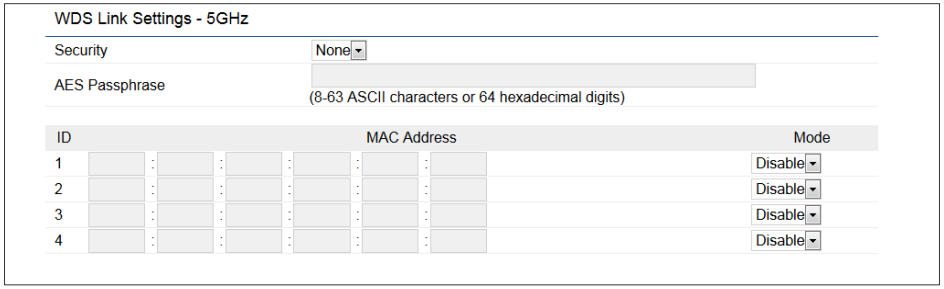
Also note: All Access Points in the WDS network need to use the same Channel and Security settings.

To create a WDS network, please enter the MAC addresses of the Access Points that you want included in the WDS. There can be a maximum of four (4) Access Points.

Note: Only applicable in WDS AP and WDS Bridge modes.

2.4 GHz/5 GHz WDS Link Settings





Security: Select None or AES from the drop-down list.

AES Passphrase: Enter the Key Values you wish to use. Other Access Points must use the same Key to establish a WDS link.

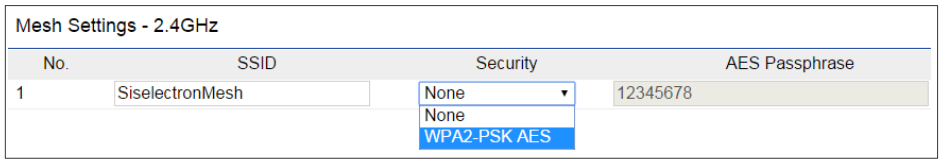
MAC Address: Enter the Access Point's MAC address to where you want to extend the wireless area.

Mode: Select to disable or enable from the drop-down list. Save:

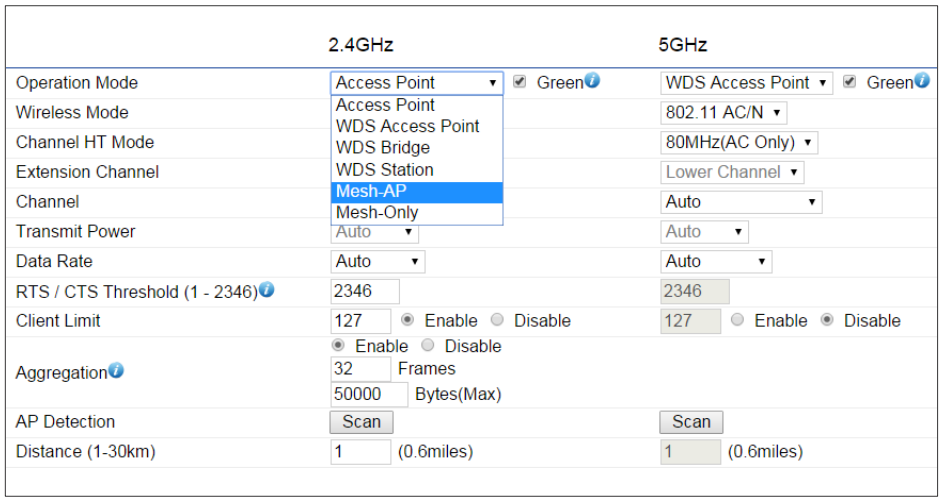
Click Save to confirm the changes.

2.4 GHz Mesh Link Settings

Users can choose the 2.4 GHz band for Mesh Mode.



Mesh Settings



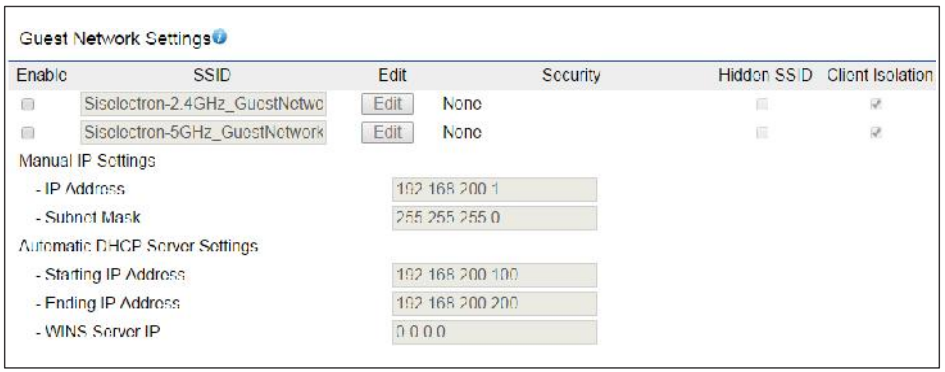
Mesh SSID: To create a Mesh network, please enter the Mesh SSID of the Access Point that you wish to include in the Mesh network.

Security: Select None or WPA2-PSK AES from drop-down list.

AES Passphrase: Enter the Key Values you wish to use. Other Access Points must use the same Key to establish a Mesh Link.

Guest Network Settings

Adding a guest network allows visitors to use the Internet without giving out your office or company wireless security key. You can add a guest network to each wireless network for both the 2.4 GHz and 5 GHz frequency bands.



SSID: Specifies the SSID for the current profile.

Suppressed SSID: Check this option to hide the selected SSID from clients. If checked, the SSID will not appear in the site survey.

Station Separation: Check the box to allow or prevent communication between client devices.

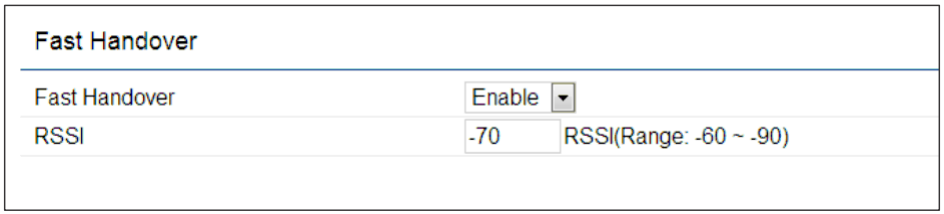
IP Address: Displays the IP address of this device.

Subnet Mask: Displays the IP Subnet mask of this device.

Starting IP Address: The first IP Address in the range of the addresses used by the DHCP server.

Ending IP Address: The last IP Address in the range of addresses assigned by the DHCP server.

Fast Handover



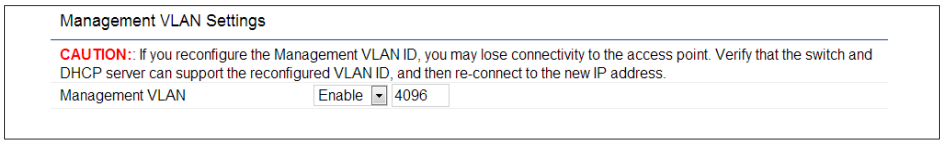
Fast Handover: Enable the Fast Handover feature by ensuring that each client is served by at least one Access Point at any time. Access Points continuously monitor the connectivity quality of any client in their range and efficiently share this information with other Access Points in the vincinity of that client to coordinate which of them should serve the client best.

RSSI: Enter the RSSI (Received Signal Strength Index) in order to determine the handover procedure which the current wireless link will terminate. RSSI is an indication of the power level being received by the antenna. Therefore,the higher the RSSI number, the stronger the signal.

Management VLAN Settings

This page allows you to assign a VLAN tag to packets sent over the network. A VLAN is a group of computers on a network whose software has been configured so that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN.

Note: Only applicable in Access Point and WDS AP modes.



Management VLAN: If your network includes VLANs, you can enable the Management VLAN ID setting for packets passing through the Access Point with a tag.

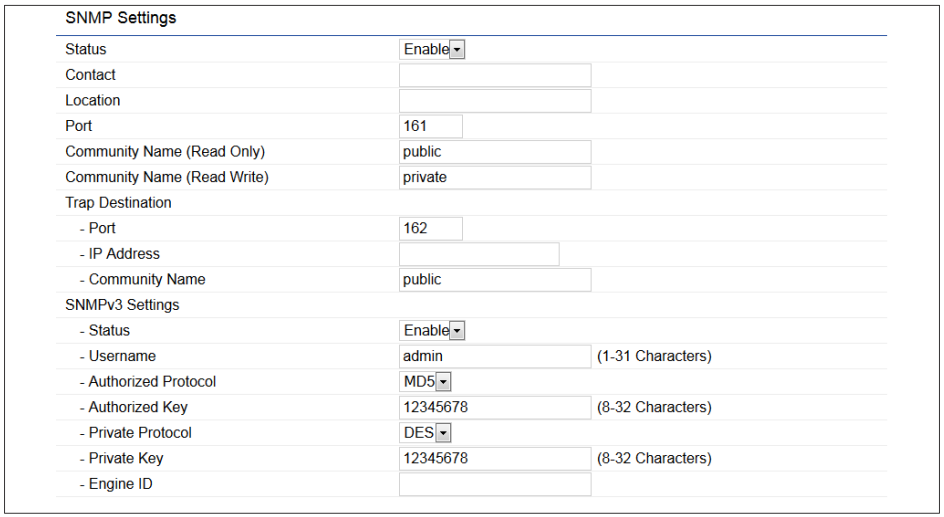
Save: Click Save to confirm the changes or Cancel to cancel and return to previous settings.

Note: If you reconfigure the Management VLAN ID, you may lose your connection to the SWM 3530. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the SWM 3530 using the new IP address.

Advanced Settings

SNMP Settings

This page allows you to assign the Contact Details, Location, Community Name, and Trap Settings for a Simple Network Management Protocol (SNMP). SNMP is a networking management protocol used to monitor network attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of the network. Upon receiving these messages, SNMP compatible devices (called agents) return the data stored in their Management Information Bases.



SNMP Enable/Disable: Enables or disables the SNMP feature.

Contact: Specifies the contact details of the device.

Location: Specifies the location of the device. Community Name

(Read Only): Specifies the password
for the SNMP community for read only access.

Community Name (Read/Write): Specifies the password for the SNMP community with read/write access.

Trap Destination Address: Specifies the IP address of the computer that will receive the SNMP traps.

Trap Destination Community Name: Specifies the password for the SNMP trap community.

SNMPv3: Enables or disables the SNMPv3 feature. User

Name: Specifies the username for SNMPv3.

Auth Protocol: Selects the authentication protocol type: MDS or SHA.

Auth Key: Specifies the authentication key.

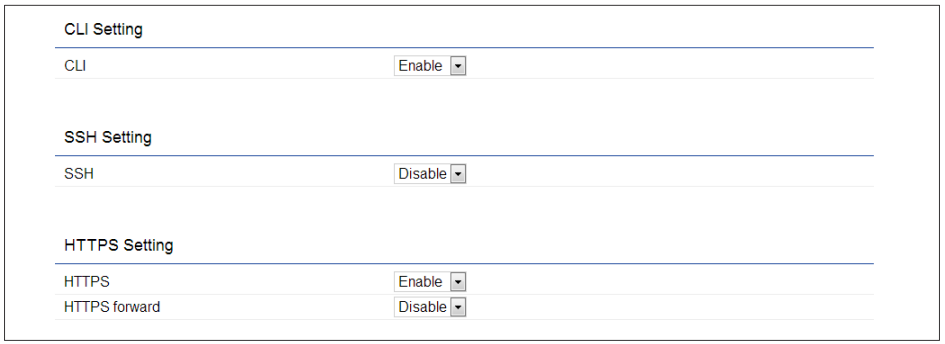
Priv Protocol: Selects the privacy protocol type: DES. Priv Key:

Specifies the privacy key.

Engine ID: Specifies the engine ID for SNMPv3.

Apply Save: Click Apply Save to apply the changes.

CLI Settings



CLI: The Command Line Interface (CLI) allows you to type commands instead of choosing them from a menu or selecting an icon to perform an action.

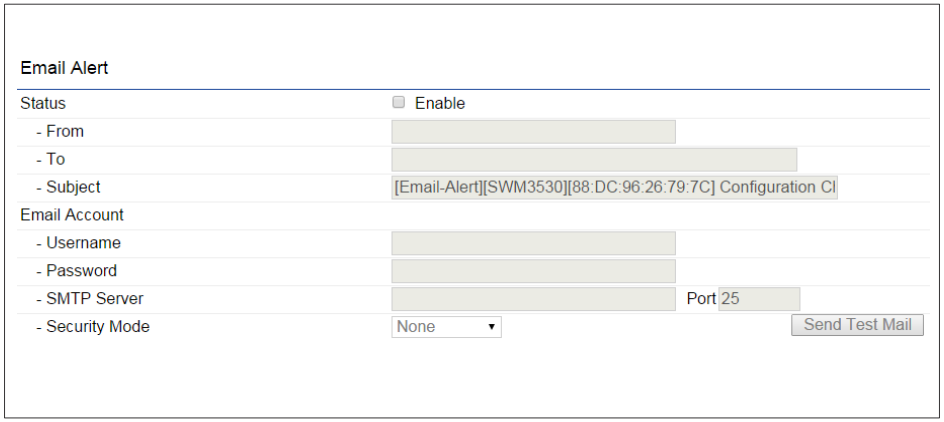
SSH: Enable Secure Shell (SSH) to make secure, encrypted connections in the network. Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two network devices.

HTTPS: Enable HTTPS to transfer and display web content securely. The Hypertext Transfer Protocol over SSL (Secure Socket Layer) is a TCP/IP protocol used by web servers to transfer and display web content securely.

Email Alerts

You can use the Email Alert feature to send messages to the configured email address when particular system events occur.

Note: Do NOT use your personal email address as it can unnecessarily expose your personal email login credentials. Use a separate email account made for this feature instead



From: Enter the email address to show the sender of the email.

To: Enter the address to receive email alerts.

Subject: Enter the text to appear in the email subject line.

Username: Enter the username for the email account that will be used to send emails.

Password: Enter the password for the email account that will be used to send emails.

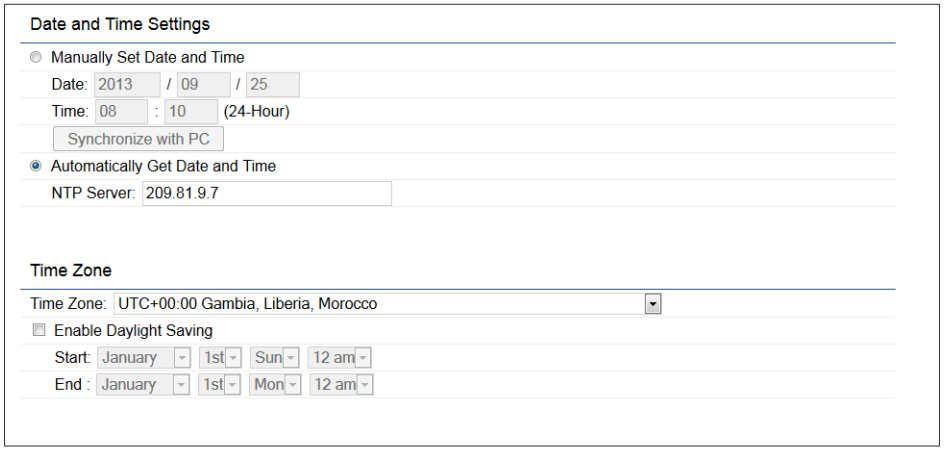
SMTP Server: Enter the IP address or hostname of the outgoing SMTP server.

Port: Enter the SMTP port number to use for outbound emails.

Time Zone

Time Setting

This page allows you to set the internal clock of the SWM 3530.



Manually Set Date and Time: Manually specify the date and time.

Automatically Get Date and Time: Select this option and enter the IP address of an NTP server or use the default NTP server to have the internal clock synch automatically.

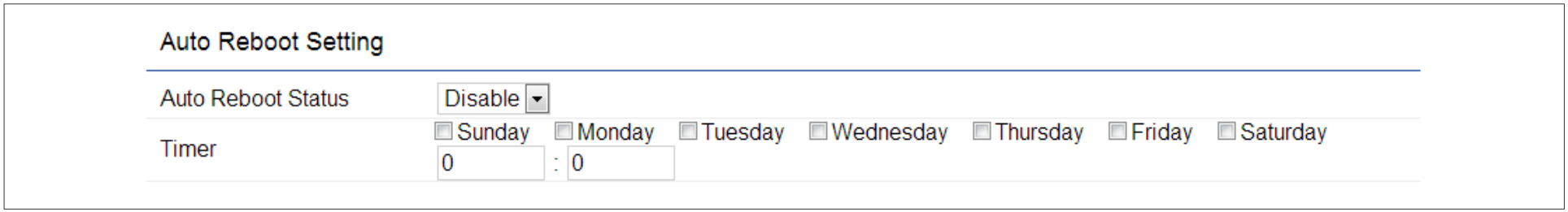
Enable Daylight Saving: Check whether daylight savings applies to your area. If you select this option, you will need to enter start and stop times.

Start: Select the day, month, and time when daylight savings time starts in your region.

End: Select the day, month, and time when daylight sav- ings times ends in your region.

Auto Reboot Settings

You can specify how often you wish to reboot the SWM 3530.



Auto Reboot Setting: Enables or disables the Auto Reboot feature.

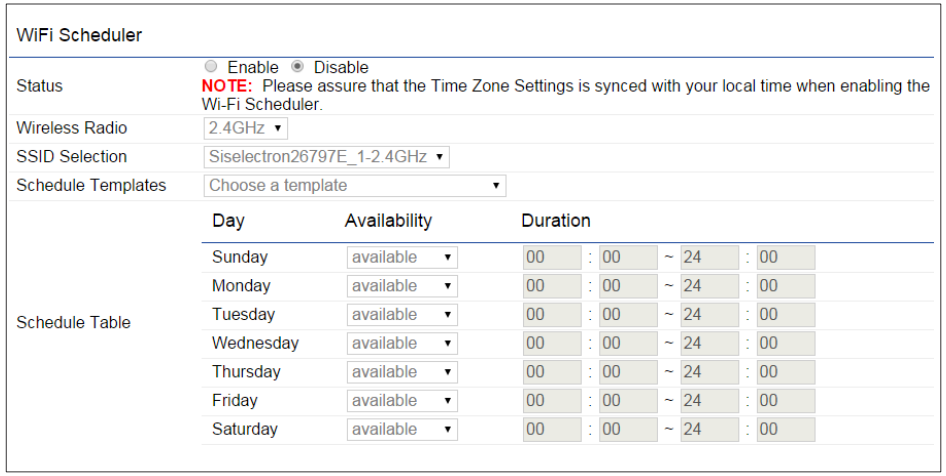
Frequency of Auto Reboot: Specifies how often you wish to reboot the SWM 3530 by Min, Hour, Day or Week.

Timer: Select the day and enter the time you would like to reboot automatically.

Save: Click Save to apply the changes.

Wi-Fi Scheduler

The Wi-Fi Scheduler can be created for use in enforcing rules. For example, if you wish to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu and Fri while entering a Start time of 3pm and an End Time of 8pm to limit access to these times.



Status: Enables or disables the Wi-Fi scheduler feature. Wireless

Radio: Select 2.4 GHz or 5 GHz from the drop-down list for the preferred band type that you wish to be regulated.

SSID Selection: Select a SSID from the drop-down list to be regulated.

Schedule Templates: Select a schedule template from the drop-down list.

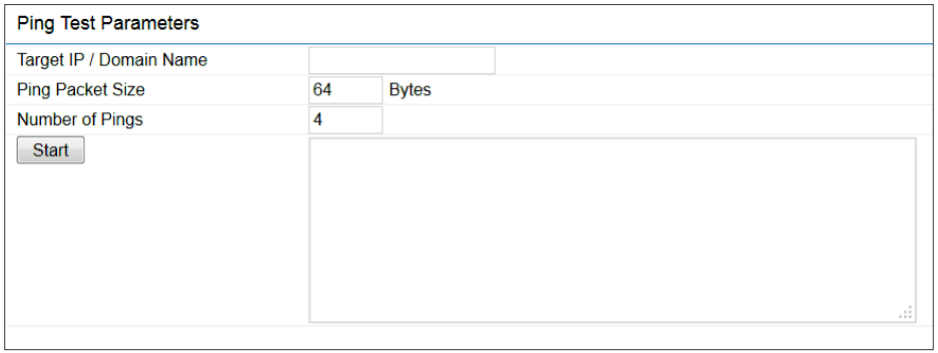
Day(s): Place a checkmark in the boxes for the desired days or select the All Week from the drop-down list to select all seven days of the week.

Duration: The Start Time is entered in two fields. The first box is for hours and the second box is for minutes. The End Time is entered in the same format as the Start time.

Tools

Ping Test Parameters

This page allows you to analyze the connection quality of the SWM 3530 and trace the routing table to a target in the network in the event of an issue.



Target IP: Enter the IP address you would like to test. Ping

Packet Size: Enter the packet size of each ping.

Number of Pings: Enter the number of times you wish to ping.

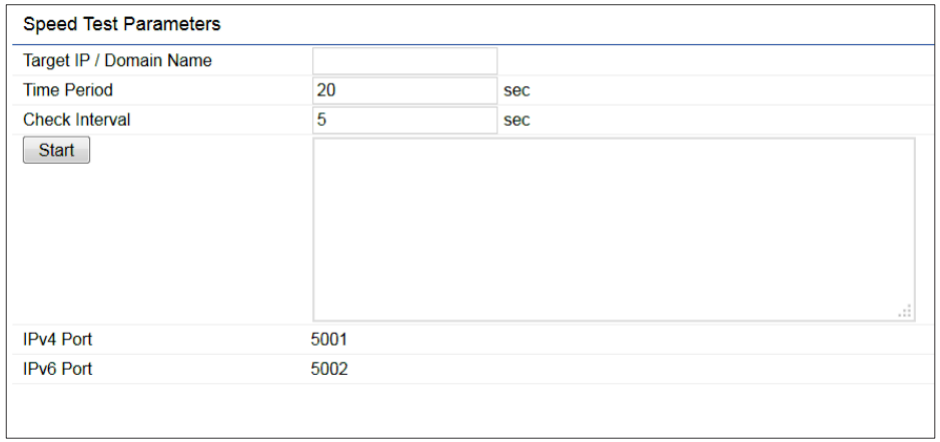
Start Ping: Click Start Ping to begin the ping test. Traceroute

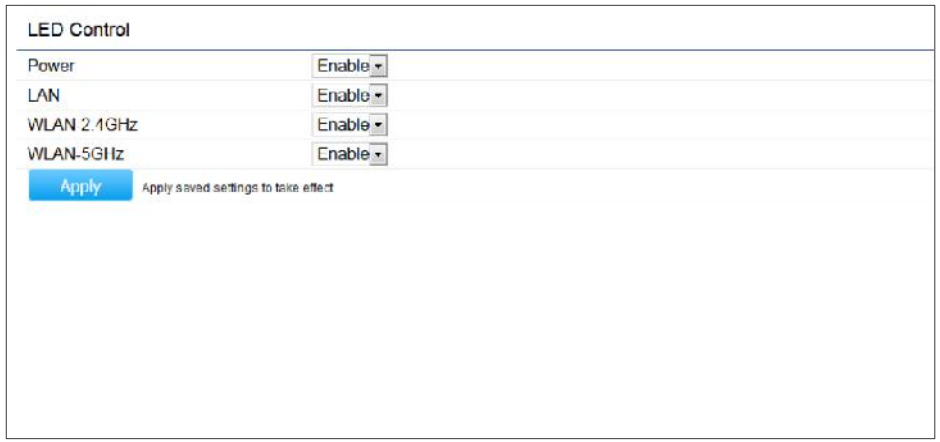
Target: Enter the IP address or domain name you wish to trace.

Start Traceroute: Click Start Traceroute to begin the trace route operation.

Speed Test Parameters/LED Control

This page allows you to power on/off the LEDs for Power, LAN interface, or 2.4 GHz/5 GHz WLAN interface for the SWM 3530.





LED Control

Power: Enables or disables the Power LED indicator. LAN:

Enables or disables the LAN LED indicator.

WLAN-2.4 GHz: Enables or disables the WLAN 2.4 GHz LED indicator.

WLAN-5 GHz: Enables or disables the WLAN 5 GHz LED indicator.

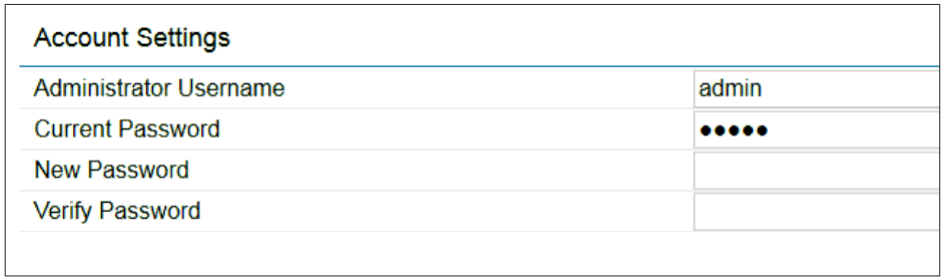
Device Discovery

This page allows you to discover devices on the network and displays their: Operation Mode, IP Address, System MAC Address and Firmware version.

Account

This page allows you to change the SWM 3530 username and password. By default, the username is: admin and the password is: admin. The password can contain from 0~12 alphanumeric characters and is case sensitive.

Account Settings



Administrator Username: Enter a new username for logging in into the New Name entry field.

Current Password: Enter the old password for logging in into the Old Password entry field.

New Password: Enter the new password for logging in into the New Password entry field.

Verify Password: Re-enter the new password in the Confirm Password entry field for confirmation. Apply:

Click Apply to apply the changes.

Firmware

Firmware Upgrade

This page allows you to upgrade the firmware of the SWM 3530.

To Perform the Firmware Upgrade:

1. Click the Choose File button and find the firmware file you downloaded from siselectron.com.tw
2. Select the upgrade file. The name of the file will appear in the Upgrade File field.
3. Click the Upload button to commence the firmware upgrade.

   Note: The device is unavailable during the Firmware upgrade process and must restart when the upgrade is completed. Any connections to or through the device will be lost.

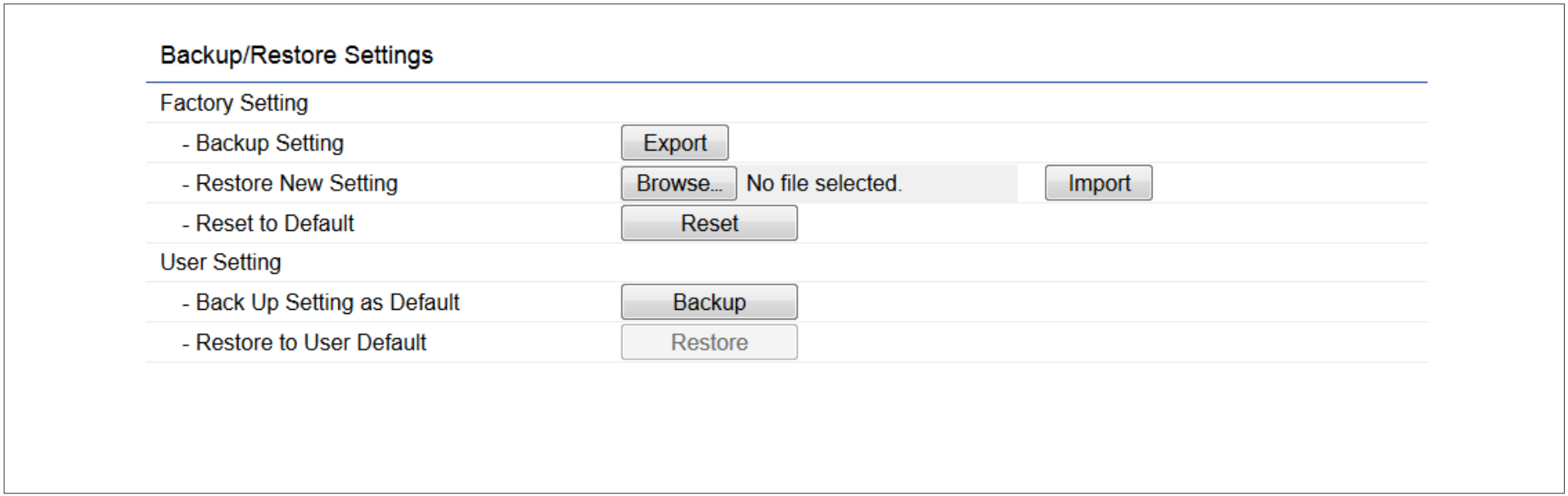
Backup/Restore

This page allows you to save the current device configurations. When you save your configurations, you also can reload the saved configurations into the device through the Restore Saved Settings from a file saved on your computer. If extreme problems occur, or if you have set the SWM 3530 incorrectly, you can use the Reset button in the Revert to Factory Default Settings section to restore all the configurations of the SWM 3530 to the original default settings.

Backup Setting: Click Export to save the current configured settings.

Restore New Setting: To restore settings that have been previously backed up, click Browse, select the file, and click Restore.

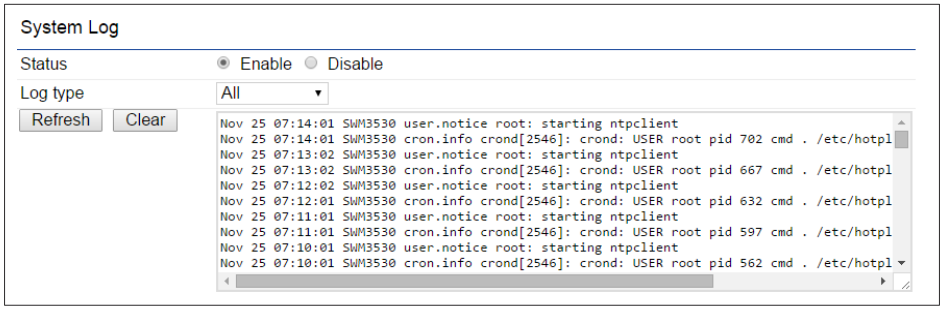
Restore to User Default: Click Reset button to restore the SWM 3530 to its factory default settings.



Log

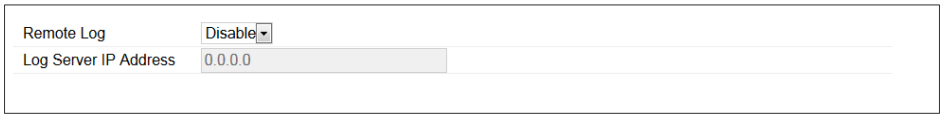
System Log

The SWM 3530 automatically logs (records) events of possible interest in its internal memory. To view the logged information, click the Log under the System Manager menu. If there is not enough internal memory to log all events, older events are deleted from the log. When powered down or rebooted, the log will be cleared.



Remote Log

This page allows you to setup the Remote Log service for the SWM 3530.



Syslog: Enables or disables the syslog function.

Log Server IP Address: Enter the IP address of the log server.

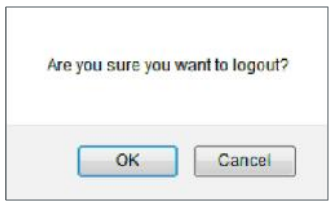
Remote Log: Enables or disables the Remote Log service

.

Apply: Click Apply to apply the changes.

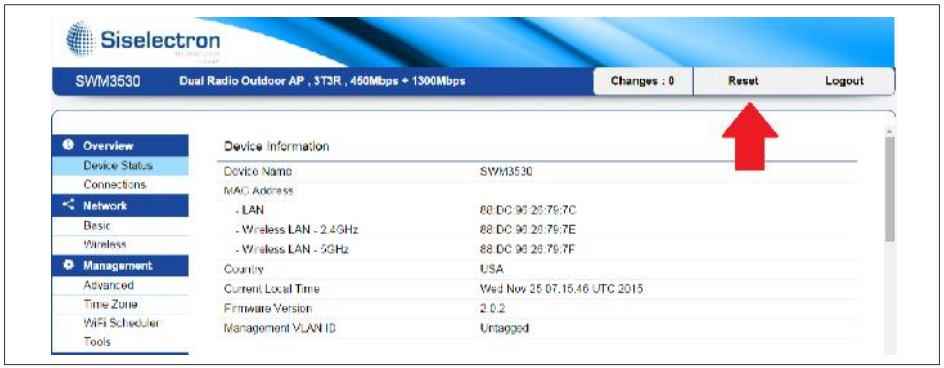
Logout

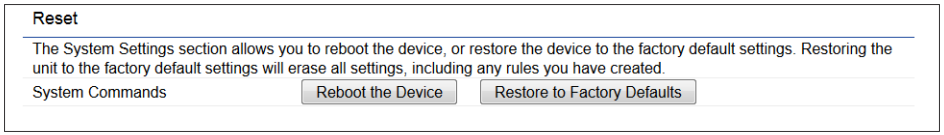
Click Logout in the Management menu to logout. Confirm by clicking OK.



Reset

In some circumstances, it may be required to force the device to reboot. Click on Reset to reboot the SWM 3530. Note that this will delete any configurations to their default settings. Please refer to page 61 to learn how to backup and save your customized configuration settings in the event of a Restore. Click Reboot the Device to confirm a reset or Restore to Factory Defaults to completely restore the device to its initial factory settings.





Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.

Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 41cm between the radiator & your body.

Professional installation instruction

1. Installation personal
This product is designed for specific application and needs to be installed by a qualified personal who has RF and related rule knowledge.
The general user shall not attempt to install or change the setting.

2. Installation location
The product shall be installed at a location where the radiating antenna can be kept 41cm from nearby person in normal operation condition to meet regulatory RF exposure requirement.

3. External antenna
Use only the antennas which have been approved by the applicant. The non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of FCC limit and is prohibited.

4. Installation procedure
Please refer to user's manual for the detail.

5. Warning
Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in relevant rules.
The violation of the rule could lead to serious federal penalty.

CE 0560 ⓘ

English	Hereby, Siselectron Technology Ltd. declarates that the SWM 3530 is in compliance with the essential requirementsand other relevants provisions of Directive 1999/5/EC.
Español (Spanish)	Por medio de la presente, Siselectron Technology Ltd. declara que el SWM 3530 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la directiva 1999/5/CE.