613-002090 Rev.A 150206

IEEE 802.11a/b/g/n Wireless LAN Access Point

AT-MWS AP series

Reference Manual

Allied Telesis

Table of Contents

1 Before You Begin 5

1.1 Considerations for Wireless Installation 6

Computer Settings 6

Hardware Installation 9

2 Configuring Your Access Point 11

2.1 Configuring Your Access Point 12

Default Settings 12

Web Configuration 12

3 Overview 15

3.1 Overview 16

Device Status 16

Connections 18

4 Network 19

4.1 Basic 20

IPv4 Settings 20

IPv6 Settings 20

5 2.4GHz & 5GHz Wireless 21

5.1 Wireless Network 22

Wireless Settings 22

2.4GHz/5GHz SSID Profile 24

Wireless Security 25

Wireless MAC Filter 28

Traffic Shaping 28

Guest Network 29

Fast Handover 30

Management VLAN Settings 30

6 Management 31

6.1 SNMP Settings 32

6.2 CLI/SSH Settings 33

6.3 HTTPS Settings 34

6.4 Email Alert 35

6.5 Date and Time Settings 36

6.6 WiFi Scheduler 37

Auto Reboot Settings 37

WiFi Scheduler 37

6.7 Tools 38

Ping Test Parameters 38

Traceroute Parameters 38

Speed Test Parameters 39

6.8 LED Control 40

6.9 Device Discovery 41

7 System Manager 43

7.1 Account Setting 44

7.2 Firmware Upgrade 45

7.3 Backup/Restore 46

Factory Setting 46

User Setting 46

7.4 System Log 47

7.5 Reset 48

7.6 Logout 49

1

Before You Begin

1.1 Considerations for Wireless Installation

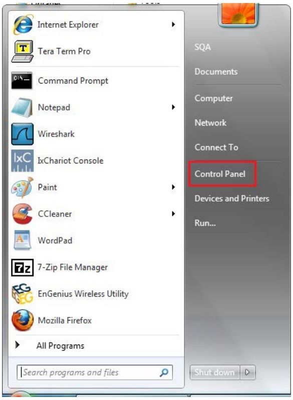
The operating distance of all wireless devices can often not be pre-determined due to a number of unknown obstacles in the environment in which the device is deployed. Obstacles such as the number, thickness, and location of walls, ceilings, or other objects that the AT-MWS600AP/AT-MWS900AP's wireless signals must pass through can weaken the signal. Here are some key guidelines for allowing the AT-MWS600AP/AT-MWS900AP to have an optimal wireless range during setup.

- Keep the number of walls and/or ceilings between the AT-MWS600AP/AT-MWS900AP and other network devices to a minimum. Each wall and/or ceiling can reduce the signal strength, resulting in a lower overall signal strength.
- Building materials make a difference. A solid metal door and/or aluminum stubs may have a significant negative effect on the signal strength of the AT-MWS600AP/AT-MWS900AP. Locate your wireless devices carefully so the signal can pass through drywall and/or open doorways. Materials such as glass, steel, metal, concrete, water (example: fish tanks), mirrors, file cabinets, and/or brick can also diminish wireless signal strength.
- Interference from your other electrical devices and/or appliances that generate RF noise can also diminish the AT-MWS600AP/AT-MWS900AP's signal strength. The most common types of devices are microwaves or cordless phones.

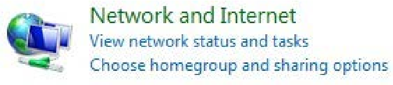
Computer Settings

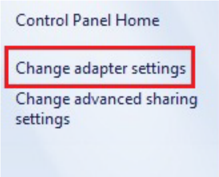
In order to use the AT-MWS600AP/AT-MWS900AP, you must first configure the TCP/IPv4 connection of your Windows 7/8 computer system.
The following shows the procedures for setting a Windows 7 PC.

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

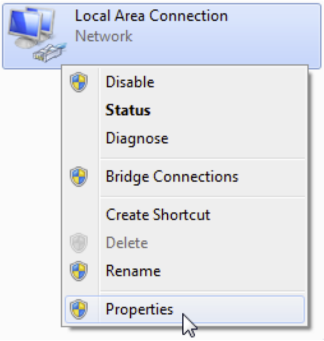


2 Click **View network status and tasks** in the **Network and Internet** section, then select **Change adapter settings**.

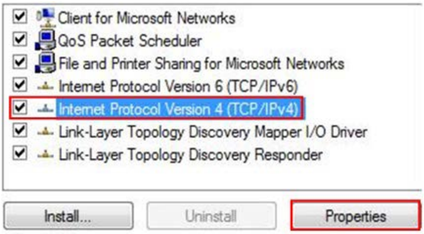

Network and Internet
View network status and tasks
Choose homegroup and sharing options



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

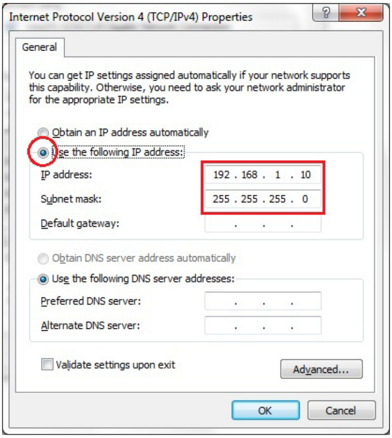


4 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.


☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

1.1 Considerations for Wireless Installation

5 Select **Use the following IP address** and enter an IP address that is different from the AT-MWS600AP/AT-MWS900AP and Subnet mask, then click **OK**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Tips

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

For example:

• AP IP address:	192.168.1.230 (default setting)
• PC IP address:	192.168.1.1 - 192.168.1.229
	192.168.1.231 - 192.168.1.254
• PC Subnet mask:	255.255.255.0

Hardware Installation

1. Ensure that the computer in use has an Ethernet Controller port (RJ-45 Ethernet Port). For more information, verify with your computer's user manual.

2. Connect one end of the Category 5e Ethernet cable into the RJ-45 port of the AT-MWS600AP/AT-MWS900AP and the other end to the RJ-45 port of the computer. Ensure that the cable is securely connected to both the AT-MWS600AP/AT-MWS900AP and the computer.

3. Connect the Power Adapter DC connector to the DC-IN port of the AT-MWS600AP/AT-MWS900AP and the Power Adapter to an available electrical outlet. Once both connections are secure, verify the following:

   a) Ensure that the **POWER** light is on (it will be **orange**).
   b) Ensure that the **2.4 GHz/5 GHz** WLAN light is off.
   c) Ensure that the **LAN** (Computer/AT-MWS600AP/AT-MWS900AP Connection) light is on (it will be **blue**).
   d) Once all three lights are on, proceed to set up the Access Point using the computer.

2

Configuring Your Access Point

2.1 Configuring Your Access Point

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

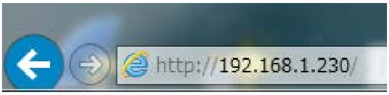
Default Settings

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

IP Address	192.168.1.230
Username	manager
Password	friend

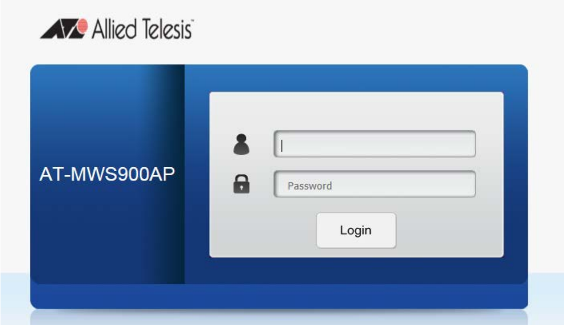
Web Configuration

1 Open a web browser (Microsoft Internet Explorer 9 or later) and enter the IP Address http://192.168.1.230.

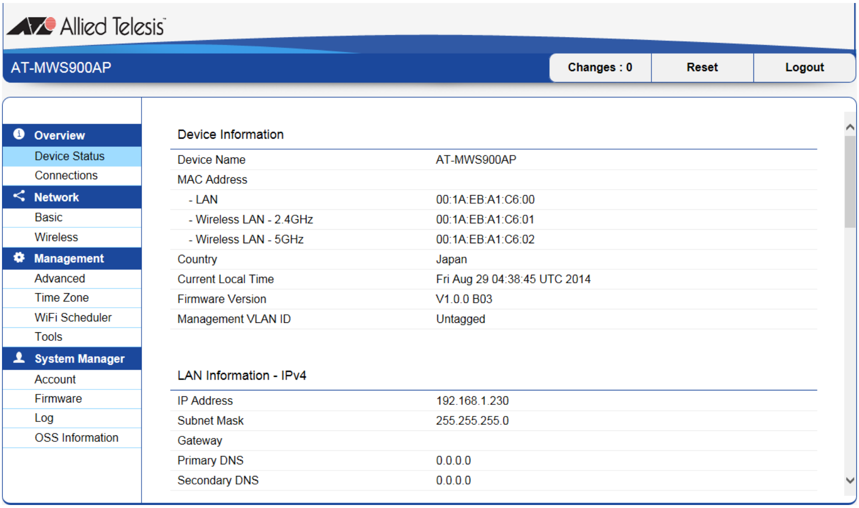

http://192.168.1.230/

Tips **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 is **manager** and the password is **friend**. 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 AT-MWS AP series User Menu.



Device Information

Device Name	AT-MWS900AP
MAC Address	
- LAN	00:1A:EB:A1:C6:00
- Wireless LAN - 2.4GHz	00:1A:EB:A1:C6:01
- Wireless LAN - 5GHz	00:1A:EB:A1:C6:02
Country	Japan
Current Local Time	Fri Aug 29 04:38:45 UTC 2014
Firmware Version	V1.0.0 B03
Management VLAN ID	Untagged

LAN Information - IPv4

IP Address	192.168.1.230
Subnet Mask	255.255.255.0
Gateway	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

3

Overview

3.1 Overview

The **Overview** section contains the following options:

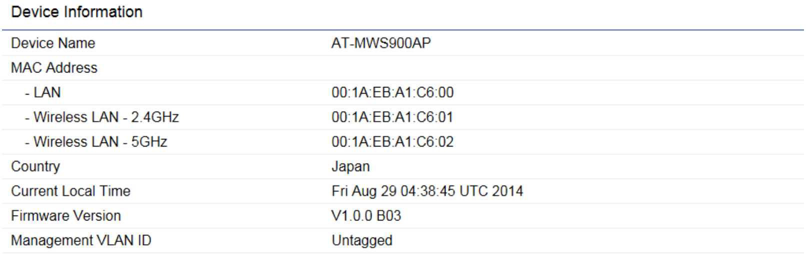
- Device Status
- Connections

The following sections describe these options.

Device Status

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

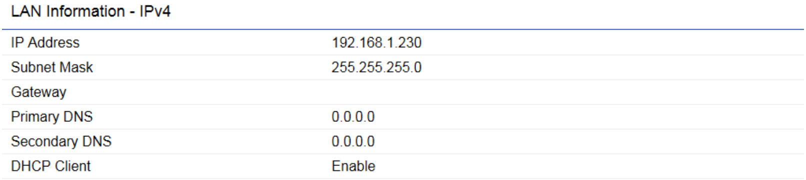
- The **Device Information** section shows general system information such as Device Name, MAC address, Current Time, Firmware Version, and Management VLAN ID



Device Information

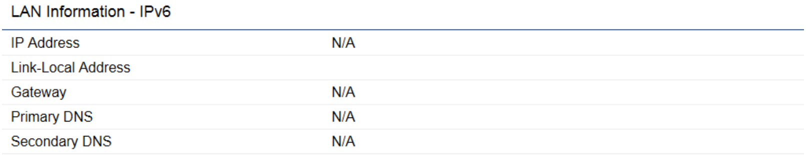
Device Name	AT-MWS900AP
MAC Address	
- LAN	00:1A:EB:A1:C6:00
- Wireless LAN - 2.4GHz	00:1A:EB:A1:C6:01
- Wireless LAN - 5GHz	00:1A:EB:A1:C6:02
Country	Japan
Current Local Time	Fri Aug 29 04:38:45 UTC 2014
Firmware Version	V1.0.0 B03
Management VLAN ID	Untagged

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



LAN Information - IPv4

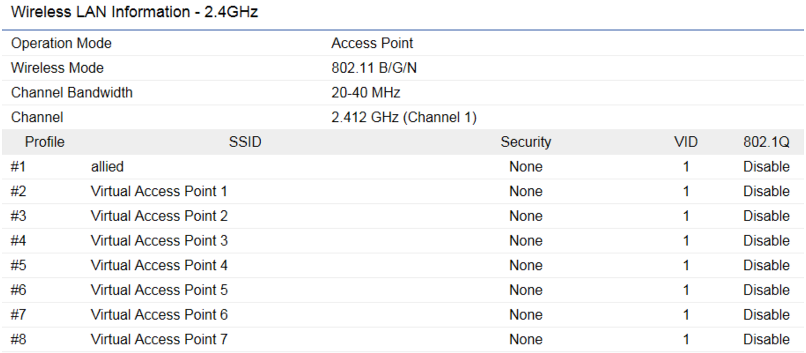
IP Address	192.168.1.230
Subnet Mask	255.255.255.0
Gateway	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
DHCP Client	Enable



LAN Information - IPv6

IP Address	N/A
Link-Local Address	
Gateway	N/A
Primary DNS	N/A
Secondary DNS	N/A

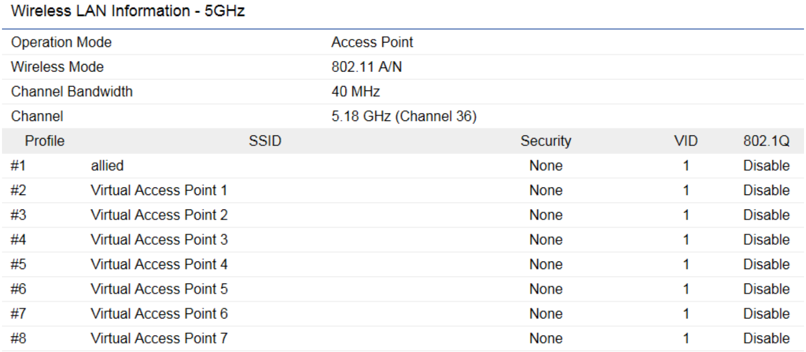
- The **Wireless LAN Information 2.4 GHz/5GHz** section shows wireless information such as Operating Mode, Frequency, and Channel. Since the AT-MWS AP supports multiple-SSIDs, information about each SSID and security settings are displayed.



Wireless LAN Information - 2.4GHz

Operation Mode	Access Point
Wireless Mode	802.11 B/G/N
Channel Bandwidth	20-40 MHz
Channel	2.412 GHz (Channel 1)

Profile	SSID	Security	VID	802.1Q
#1	allied	None	1	Disable
#2	Virtual Access Point 1	None	1	Disable
#3	Virtual Access Point 2	None	1	Disable
#4	Virtual Access Point 3	None	1	Disable
#5	Virtual Access Point 4	None	1	Disable
#6	Virtual Access Point 5	None	1	Disable
#7	Virtual Access Point 6	None	1	Disable
#8	Virtual Access Point 7	None	1	Disable



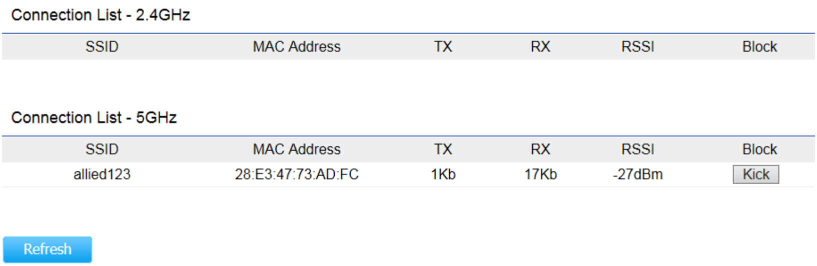
Wireless LAN Information - 5GHz

Operation Mode	Access Point
Wireless Mode	802.11 A/N
Channel Bandwidth	40 MHz
Channel	5.18 GHz (Channel 36)

Profile	SSID	Security	VID	802.1Q
#1	allied	None	1	Disable
#2	Virtual Access Point 1	None	1	Disable
#3	Virtual Access Point 2	None	1	Disable
#4	Virtual Access Point 3	None	1	Disable
#5	Virtual Access Point 4	None	1	Disable
#6	Virtual Access Point 5	None	1	Disable
#7	Virtual Access Point 6	None	1	Disable
#8	Virtual Access Point 7	None	1	Disable

Connections

Clicking the **Connections** link under the **Device Status** menu displays the list of clients associated to the AT-MWS AP's 2.4GHz/5GHz, along with the MAC address, TX, RX and signal strength for each client. Clicking **Kick** in the Block column removes this client.



Connection List - 2.4GHz

SSID	MAC Address	TX	RX	RSSI	Block

Connection List - 5GHz

SSID	MAC Address	TX	RX	RSSI	Block
allied123	28:E3:47:73:AD:FC	1Kb	17Kb	-27dBm	Kick

Click **Refresh** to refresh the Connection List page.

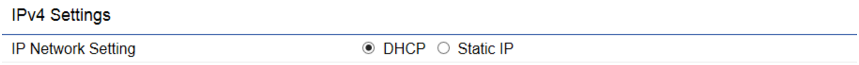
4

Network

4.1 Basic

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

IPv4 Settings

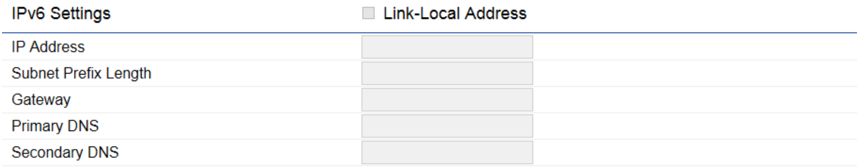


IPv4 Settings

IP Network Setting ● DHCP ○ Static IP

IP Network Setting:	Select whether the device IP address will use the static IP address specified in the IP Address field or be obtained automatically when the device connects to a DHCP server.
IP Address:	The IP Address of this device.
IP Subnet Mask:	The IP Subnet mask of this device.
Gateway:	The Default Gateway of this device. Leave it blank if you are unsure of this setting.
Primary/Secondary DNS:	The primary/secondary DNS address for this device.

IPv6 Settings



IPv6 Settings □ Link-Local Address

IP Address	
Subnet Prefix Length	
Gateway	
Primary DNS	
Secondary DNS	

Link-Local Address:	Check this if you want to use Link-Local Address.
IP Address:	The IPv6 IP Address of this device.
Subnet Prefix Length:	The IPv6 Subnet Prefix Length of this device.
Gateway:	The IPv6 Default Gateway of this device. Leave it blank if you are unsure of this setting.
Primary / Secondary DNS:	The primary / secondary DNS address for this device.

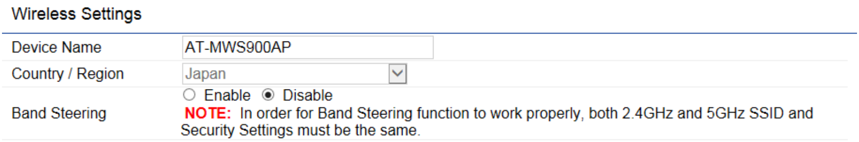
5

2.4GHz & 5GHz Wireless

5.1 Wireless Network

This page displays the current status of the Wireless settings of the AT-MWS AP.

Wireless Settings

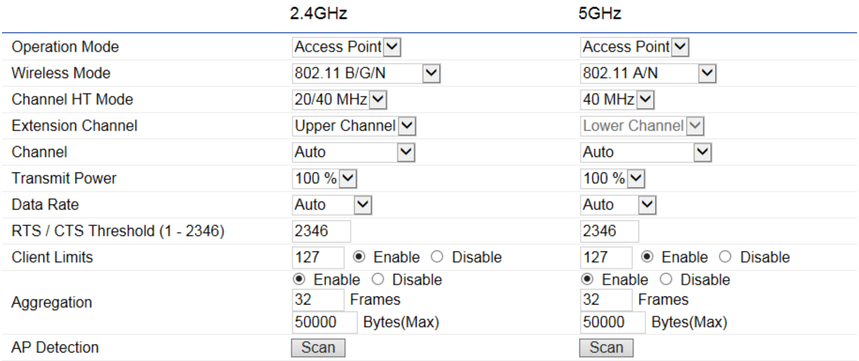


Wireless Settings

Device Name	AT-MWS900AP
Country / Region	Japan
Band Steering	○ Enable ● Disable **NOTE:** In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.

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 broadcast to other devices.
Country/Region:	Select a Country/Region to conform to local regulations. Japan only (not changeable).
Band Steering:	Enable Band Steering to sends 802.11n clients to the 5GHz band, where 802.11b/g clients cannot go, and leaves the 802.11b/g clients in 2.4GHz to operate at their slower rates. Band Steering works within the Access Point by directing 5GHz-capable clients to that band.

Tips **Note:** In order for the Band Steering function to work properly, both the 2.4GHz and the 5GHz SSID and security settings must be under the same selection settings.



	2.4GHz	5GHz
Operation Mode	Access Point	Access Point
Wireless Mode	802.11 B/G/N	802.11 A/N
Channel HT Mode	20/40 MHz	40 MHz
Extension Channel	Upper Channel	Lower Channel
Channel	Auto	Auto
Transmit Power	100 %	100 %
Data Rate	Auto	Auto
RTS / CTS Threshold (1 - 2346)	2346	2346
Client Limits	127 ● Enable ○ Disable	127 ● Enable ○ Disable
Aggregation	● Enable ○ Disable 32 Frames 50000 Bytes(Max)	● Enable ○ Disable 32 Frames 50000 Bytes(Max)
AP Detection	Scan	Scan

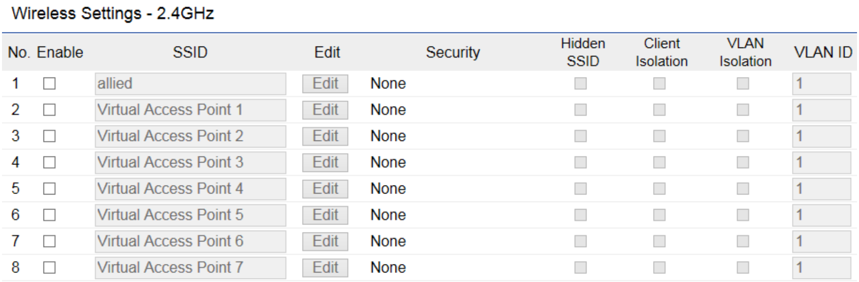
Wireless Mode:	Supports 802.11b/g/n mixed mode in 2.4GHz and 802.11a/n mixed mode in 5GHz.
Channel HT Mode:	The default channel bandwidth is 20/40MHz. The larger the channel bandwidth, the better the transmission quality and speed. This option is only available for 802.11n modes only.

Extension Channel:	Use the drop-down menu to set the Extension Channel as Upper or Lower channel. An extension channel is a secondary channel used to bond with the primary channel to increase this range to 40MHz allowing for greater bandwidth. The Extension Channel may be degraded into 20MHz bandwidth in 2.4GHz, when the secondary channel frequency is interfared by other 802.11 or non-802.11 devices. This option is only available when Wireless Mode is 802.11n and Channel HT Mode is 20/40 MHz or 40MHz.
Channel:	Select the channel appropriate for your country's regulation. Note that the Dynamic Frequency Selection (DFS) will work over channel ranges W53 (channels 52 to 64) and W56 (channels 100 to 140) in Japan.
Transmit Power:	Select the transmit power for the radio. Increasing the power improves performance, but if two or more access points are operating in the same area on the same channel, it may cause interference.
Data Rate:	Use the drop-down list to set the available transmit data rates permitted for wireless clients. The data rate affects the throughput of the access point. The lower the data rate, the lower the throughput, but the longer transmission distance.
RTS/CTS Threshold:	Specifies the threshold package size for RTC/CTS. A small 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:	AP Detection can select the best channel to use by scanning nearby areas for Access Points.

5.1 Wireless Network

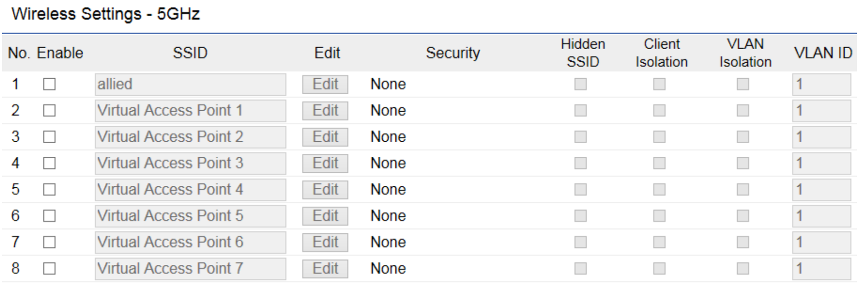
2.4GHz/5GHz SSID Profile

Under **Wireless Settings**, you can edit the SSID profile to fit your needs. Click **Edit** under the SSID you would like to make changes to.



Wireless Settings - 2.4GHz

No.	Enable	SSID	Edit	Security	Hidden SSID	Client Isolation	VLAN Isolation	VLAN ID
1	□	allied	Edit	None	□	□	□	1
2	□	Virtual Access Point 1	Edit	None	□	□	□	1
3	□	Virtual Access Point 2	Edit	None	□	□	□	1
4	□	Virtual Access Point 3	Edit	None	□	□	□	1
5	□	Virtual Access Point 4	Edit	None	□	□	□	1
6	□	Virtual Access Point 5	Edit	None	□	□	□	1
7	□	Virtual Access Point 6	Edit	None	□	□	□	1
8	□	Virtual Access Point 7	Edit	None	□	□	□	1



Wireless Settings - 5GHz

No.	Enable	SSID	Edit	Security	Hidden SSID	Client Isolation	VLAN Isolation	VLAN ID
1	□	allied	Edit	None	□	□	□	1
2	□	Virtual Access Point 1	Edit	None	□	□	□	1
3	□	Virtual Access Point 2	Edit	None	□	□	□	1
4	□	Virtual Access Point 3	Edit	None	□	□	□	1
5	□	Virtual Access Point 4	Edit	None	□	□	□	1
6	□	Virtual Access Point 5	Edit	None	□	□	□	1
7	□	Virtual Access Point 6	Edit	None	□	□	□	1
8	□	Virtual Access Point 7	Edit	None	□	□	□	1

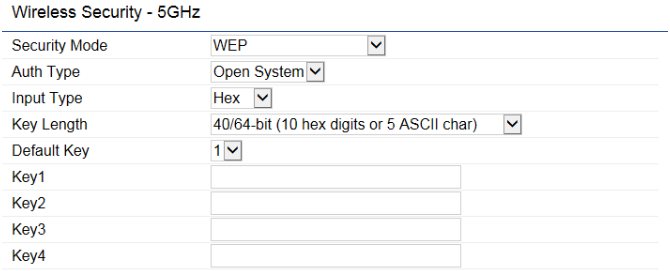
Enable:	Check this option to enable this profile.
SSID:	Specifies the SSID for the current profile. The SSID is a seuqence of case sensitive alphanumeric characters and symbols (_!@$%^*()-+=|<>,.? []{}~`#&V'").
Security:	Displays the Security Mode the SSID uses. You can click **Edit** to change the security mode. For more details, see the next section.
Hidden SSID:	Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.
Client Isolation:	Check this option to prevent communication between client devices.
VLAN Isolation:	Check this option to enable VLAN Isolation feature.
VLAN ID:	Specifies the VLAN ID for the SSID profile.

Wireless Security

The Wireless Security section lets you configure the AT-MWS AP's security modes: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA-Enterprise, WPA2-Enterprise and WPA Mixed Enterprise.

It is strongly recommended that you use **WPA2-PSK**. Click on the **Edit** button under Wireless Settings next to the SSID to change the security settings.

WEP

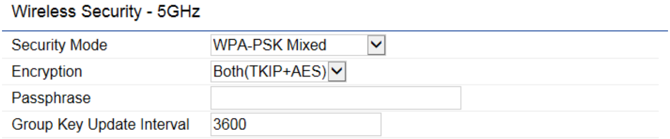


Wireless Security - 5GHz

Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	
Key2	
Key3	
Key4	

Auth Type:	Select **Open System** or **Shared Key**.
Input Type:	**ASCII**: Regular Text (Recommended) or **HEX**: Hexadecimal Numbers (For advanced users).
Key Length:	Select the desired option and ensure the wireless clients use the same setting. Your choices are: **64**, **128**, and **152-bit** password lengths.
Default Key:	Select the key you wish to be default. 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.
Key1-4:	Enter the Key Value or values you wish to use. The default is none.

WPA-PSK/WPA2-PSK (Pre-Shared Key)

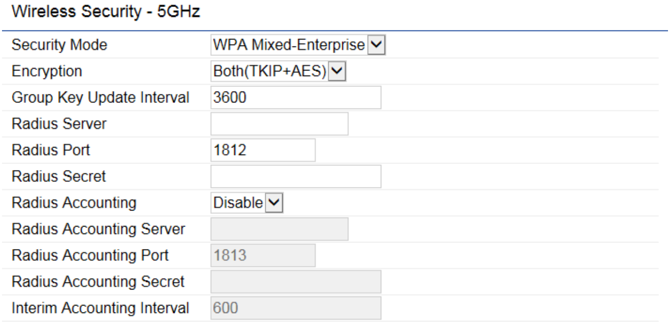


Wireless Security - 5GHz

Security Mode	WPA-PSK Mixed
Encryption	Both(TKIP+AES)
Passphrase	
Group Key Update Interval	3600

Encryption:	Select the WPA/WPA2 encryption type you would like to use. Available options are **Both**, **TKIP(Temporal Key Integrity Protocol)** and **AES(Advanced Encryption Standard)**. 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 to 63 characters in length. If using HEX format, the Key must be 64 HEX characters in length.
Group Key Update Interval:	Specify how often, in seconds, the Group Key changes.

WPA/WPA2-Enterprise



Wireless Security - 5GHz

Security Mode	WPA Mixed-Enterprise
Encryption	Both(TKIP+AES)
Group Key Update Interval	3600
Radius Server	
Radius Port	1812
Radius Secret	
Radius Accounting	Disable
Radius Accounting Server	
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600

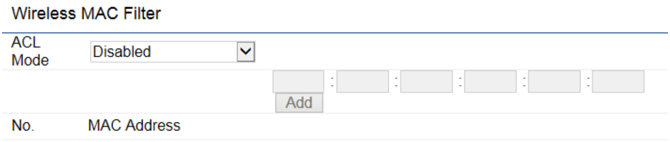
Encryption:	Select the WPA/WPA2 encryption type you would like to use. Available options are Both, TKIP(Temporal Key Integrity Protocol) and AES(Advanced Encryption Standard). Please ensure that your wireless clients use the same settings.
Group Key Update Interval:	Specify how often, in seconds, the group key changes.
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.
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:	Specify how often, in seconds, the accounting data sends.

Tips

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.

Wireless MAC Filter

Wireless MAC Filter is used to allow or deny network access to wireless clients (computers, tablet PCs, NAS, smart phones, etc.) according to their MAC addresses. You can manually add a MAC address to restrict permission to access AT-MWS AP. The default setting is: Disable Wireless MAC Filter.

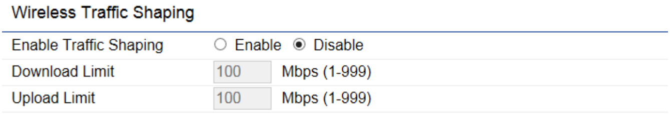

Wireless MAC Filter

ACL Mode: Disabled

ACL (Access Control List) Mode:	Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC address table on this page. Choices given 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.

Traffic Shaping

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


Wireless Traffic Shaping

Enable Traffic Shaping: ○ Enable ● Disable

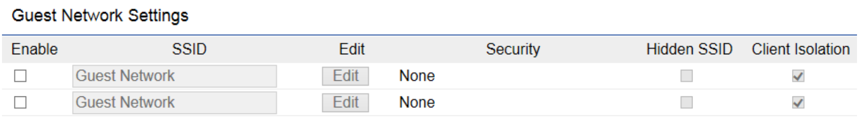
Download Limit: 100 Mbps (1-999)

Upload Limit: 100 Mbps (1-999)

Enable Traffic Shaping:	Select to Enable or Disable 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 apply the changes.

Guest Network

The Guest Network function allows administrators to grant Internet connectivity to visitors or guests while keeping other networked devices (computers and hard drives) and sensitive personal or company information private and secure.

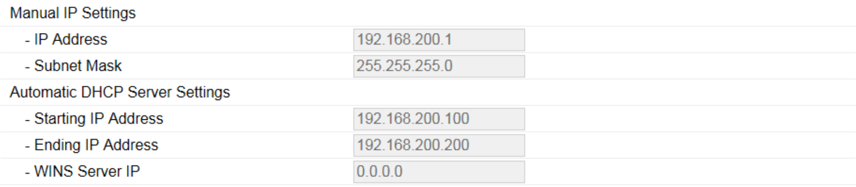


Guest Network Settings

Enable	SSID	Edit	Security	Hidden SSID	Client Isolation
□	Guest Network	Edit	None	□	☑
□	Guest Network	Edit	None	□	☑

Enable SSID:	Select to Enable or Disable SSID broadcasting.
SSID:	Specify the SSID for the current profile. This is the name visible on the network to wireless clients.
Security:	You can use None or WPA-PSK / WPA2-PSK security for this guest network.
Hidden SSID:	Check this option to hide the SSID from broadcasting to discourage wireless users from connecting to a particular SSID.
Client Isolation:	Check this option to prevent wireless clients associated with your access point to communicate with other wireless devices connected to the AP.

After enabling Guest Network in the SSID Config page, assign an IP Address, Subnet Mask and DHCP server IP address range for this Guest Network.



Manual IP Settings	
- IP Address	192.168.200.1
- Subnet Mask	255.255.255.0
Automatic DHCP Server Settings	
- Starting IP Address	192.168.200.100
- Ending IP Address	192.168.200.200
- WINS Server IP	0.0.0.0

Manual IP Settings

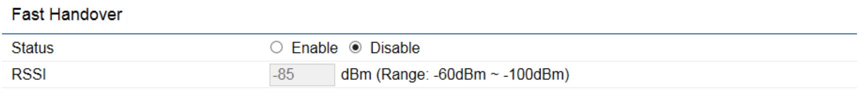
IP Address:	Specify an IP Address for the Guest Network
Subnet Mask:	Specify the Subnet Mask IP Address for the Guest Network

Automatic DHCP Server Settings

Starting IP Address:	Specify the starting IP Address range for the Guest Network.
Ending IP Address:	Specify the ending IP Address range for the Guest Network.
WINS Server IP:	Specify the WINS Server IP Address for the Guest Network. WINS means Windows Internet Name Service. It is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names.

Fast Handover

With Fast Handover enabled, the AP will send a disassociation request to the wireless client and let it find another AP to handover and associate upon detecting the wireless client's RSSI value lower than specified. The RSSI value can be adjusted to allow more clients to stay associated to this AP. Note that setting the RSSI value too low may cause wireless clients to reconnect frequently.



Fast Handover

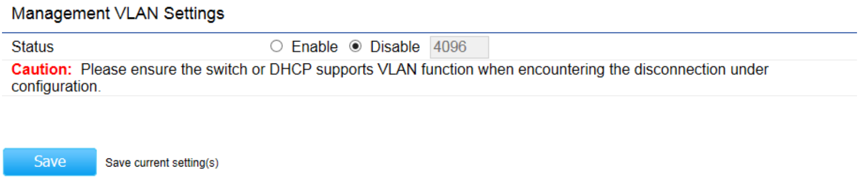
Status ○ Enable ● Disable

RSSI -85 dBm (Range: -60dBm ~ -100dBm)

Status:	Select to **Enable** or **Disable** Fast Handover.
RSSI:	Specify the RSSI value to send a disassociation request to the wireless client whose strength is detected lower than that. The range is from **-90**dBm to **-60**dBm.

Management VLAN Settings

This section allows you to assign a VLAN tag to the packets. 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.



Management VLAN Settings

Status ○ Enable ● Disable 4096

Caution: Please ensure the switch or DHCP supports VLAN function when encountering the disconnection under configuration.

Status:	If your network includes VLANs and if tagged packets need to pass through the Access Point, select **Enable** and enter the VLAN ID. Otherwise, click **Disable**.
Save:	Click **Save** to apply the changes.

Tips

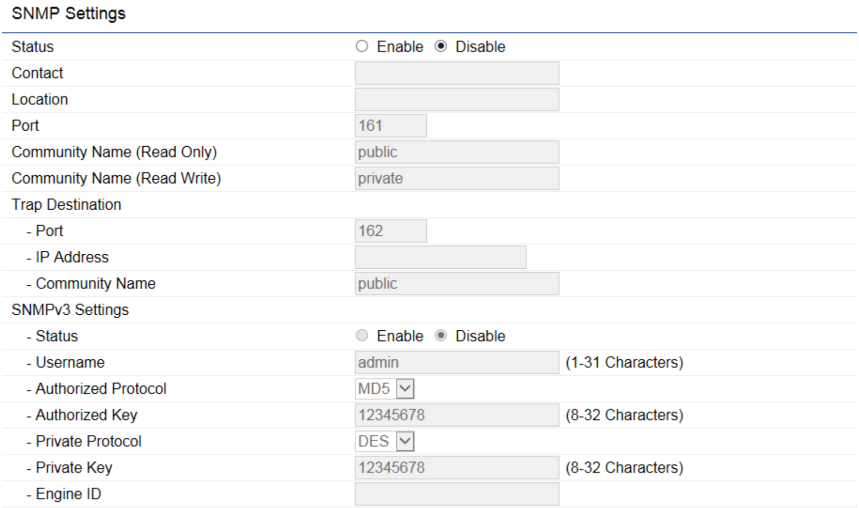
Note: If you reconfigure the Management VLAN ID, you may lose your connection to the AT-MWS AP. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the AT-MWS AP using the new IP address.

6

Management

6.1 SNMP Settings

This page allows you to assign the Contact Details, Location, Community Name, and Trap Settings for Simple Network Management Protocol (SNMP). This 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) returns the data stored in their Management Information Bases. To configure SNMP Settings, click under the **Advanced** tab on the side bar under **Management**.



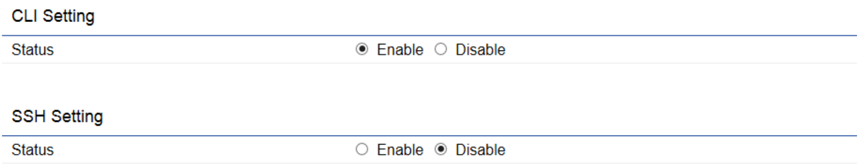
SNMP Settings

Status	○ Enable ● Disable	
Contact		
Location		
Port	161	
Community Name (Read Only)	public	
Community Name (Read Write)	private	
Trap Destination		
- Port	162	
- IP Address		
- Community Name	public	
SNMPv3 Settings		
- Status	○ Enable ● Disable	
- Username	admin	(1-31 Characters)
- Authorized Protocol	MD5	
- Authorized Key	12345678	(8-32 Characters)
- Private Protocol	DES	
- Private Key	12345678	(8-32 Characters)
- Engine ID		

Status:	Enables or Disables the SNMP feature.
Contact:	Specifies the contact details of the device.
Location:	Specifies the location of the device.
Port:	Displays the port number.
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 port and IP address of the computer that will receive the SNMP traps.
Trap Destination Community Name:	Specifies the password for the SNMP trap community.
SNMPv3 Status:	Enables or Disables the SNMPv3 feature.
User Name:	Specifies the username for the SNMPv3.feature
Auth Protocol:	Select the Authentication Protocol type: **MDS** or **SHA**.
Auth Key:	Specify the Authentication Key for authentication.
Priv Protocol:	Select the Privacy Protocol type: **DES**.
Priv Key:	Specifies the privacy key for privacy.
Engine ID:	Specifies the Engine ID for SNMPv3.

6.2 CLI/SSH Settings

Most users will configure the device through the graphical user interface (GUI). However, for those who prefer an alternative method there is the command line interface (CLI). The CLI can be access through a command console, modem or Telnet connection. For security's concern, you can enable SSH (Secure Shell) to establish a secure data communication.



CLI Setting

Status ● Enable ○ Disable

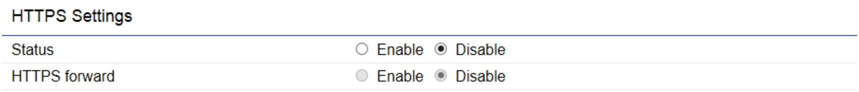
SSH Setting

Status ○ Enable ● Disable

CLI Status:	Select **Enable** or **Disable** to enable or disable the ability to modify the AT-MWS AP via a command line interface (CLI).
SSH Status:	Select **Enable** or **Disable** to enable or disable the ability to modify the AT-MWS AP via a command line interface (CLI) with a secure channel.

6.3 HTTPS Settings

Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.



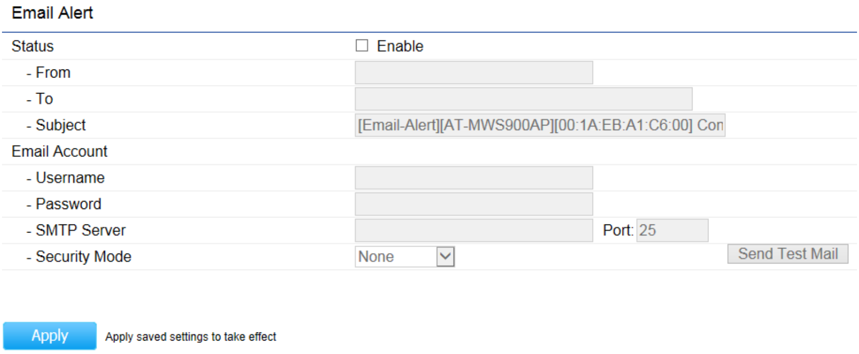
HTTPS Settings

Status	○ Enable ● Disable
HTTPS forward	○ Enable ● Disable

Status:	Select **Enable** or **Disable** to enable or disable the ability to modify the AT-MWS AP via a HTTPS.
HTTPS forward:	Enable this option; it will be forwarded to HTTPS if user uses HTTP to access AT-MWS AP.

6.4 Email Alert

AT-MWS AP will send email alerts when AT-MWS AP's configuration has been changed.



Email Alert

Status	□ Enable
- From	
- To	
- Subject	[Email-Alert][AT-MWS900AP][00:1A:EB:A1:C6:00] Con
Email Account	
- Username	
- Password	
- SMTP Server	Port: 25
- Security Mode	None

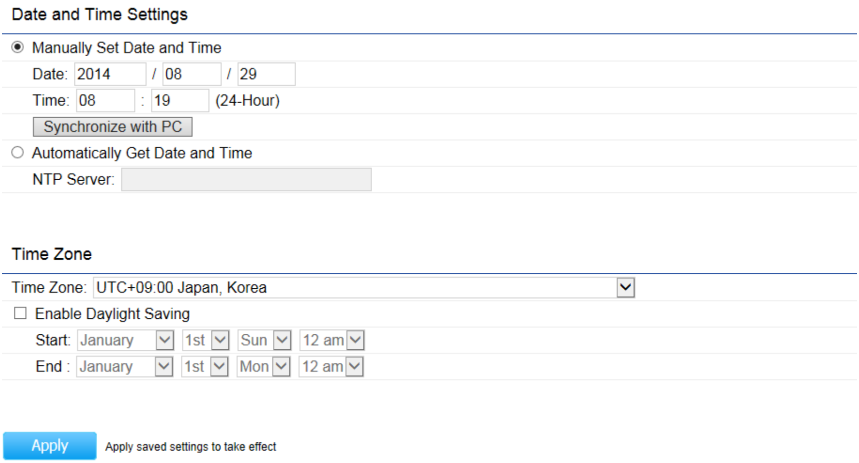
Status:	Check **Enable** to enable Email Alert feature.
From:	Enter the address to show as the sender of the email.
To:	Enter the address to show as the receiver of the email.
Subject:	Enter the subject to show as the subject of the email.

Email Account

Username/Password:	Enter the username and password required to connect to the SMTP server.
SMTP Server/Port:	Enter the IP address/domain name and port of the SMTP server. The default port of SMTP Server is port 25.
Security Mode:	Select the mode of security for the Email alert. The options are None, SSL/TLS and STARTTLS.
Send Test Mail:	Click **Send Test Mail** button to test the Email Alert setup.
Apply:	Click **Apply** to save the changes.

6.5 Date and Time Settings

This page allows you to set the internal clock of the AT-MWS AP. To access the Date and Time settings, click **Time Zone** under the **Management** tab on the side bar.



Date and Time Settings

● Manually Set Date and Time

Date: 2014 / 08 / 29

Time: 08 : 19 (24-Hour)

○ Automatically Get Date and Time

NTP Server:

Time Zone

Time Zone: UTC+09:00 Japan, Korea

□ Enable Daylight Saving

Start: January 1st Sun 12 am

End : January 1st Mon 12 am

Apply saved settings to take effect

Manually Set Date and Time:	Manually specify the date and time.
Synchronize with PC:	Click to Synchronize the AT-MWS AP with the computer's internal clock.
Automatically Get Date and Time:	Enter the IP address of an NTP server or use the default NTP server to have the internal clock set automatically.
Time Zone:	Choose the time zone you would like to use from the drop-down list.
Enable Daylight Savings:	Check the box to enable or disable daylight savings time for the AT-MWS AP. Next, enter the dates that correspond to the present year's daylight savings time.

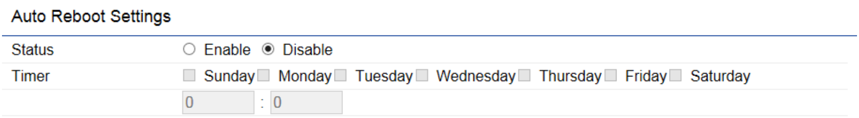
Click **Apply** to save the changes.

6.6 WiFi Scheduler

Use the schedule function to reboot AT-MWS AP or control the wireless availability on a routine basis. The Schedule function relies on the GMT time setting acquired from a network time protocol (NTP) server. For details on how to connect the AT-MWS AP to an NTP server, see Date and Time Settings.

Auto Reboot Settings

You can specify how often you would like to reboot the AT-MWS AP.

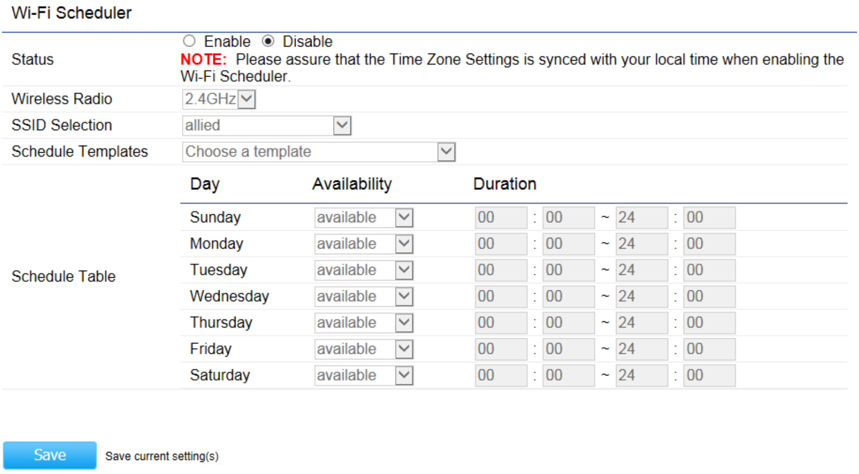


Auto Reboot Settings

Status	○ Enable ● Disable
Timer	□ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday
	0 : 0

Status:	Enables or disables the Auto Reboot function.
Timer:	Specifies the time and frequency in rebooting the AT-MWS AP by Min, Hour and Day.

WiFi Scheduler



Wi-Fi Scheduler

Status	○ Enable ● Disable NOTE: Please assure that the Time Zone Settings is synced with your local time when enabling the Wi-Fi Scheduler.
Wireless Radio	2.4GHz
SSID Selection	allied
Schedule Templates	Choose a template

Schedule Table

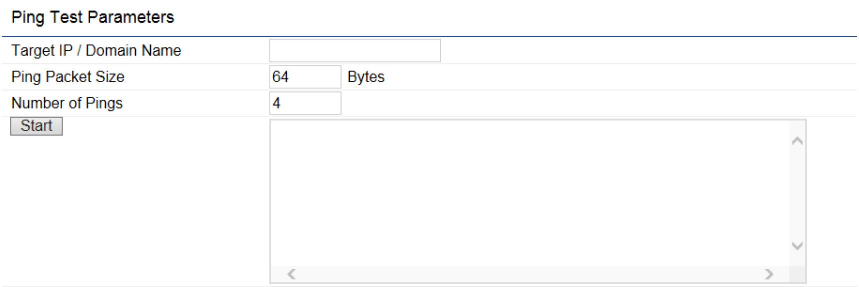
Day	Availability	Duration
Sunday	available	00 : 00 ~ 24 : 00
Monday	available	00 : 00 ~ 24 : 00
Tuesday	available	00 : 00 ~ 24 : 00
Wednesday	available	00 : 00 ~ 24 : 00
Thursday	available	00 : 00 ~ 24 : 00
Friday	available	00 : 00 ~ 24 : 00
Saturday	available	00 : 00 ~ 24 : 00

Status:	Enables or disables the WiFi Scheduler function.
Wireless Radio:	Select **2.4GHz** or **5GHz** to use WiFi Schedule.
SSID Selection:	Select a SSID to use WiFi Schedule.
Schedule Templates:	AT-MWS AP provides three templates: **Always available**, **Available 8-5 daily** and **Available 8-5 daily except weekends.** Select Custom schedule if you want to set the schedule manually.
Schedule Table:	Set the schedule manually.

6.7 Tools

This section allows you to analyze the connection quality of the AT-MWS AP and trace the routing table to a target in the network.

Ping Test Parameters

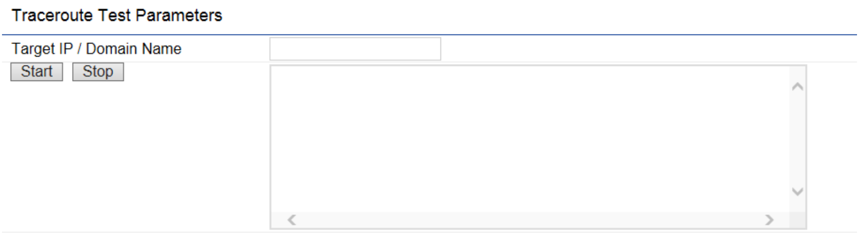


Ping Test Parameters

Target IP / Domain Name	
Ping Packet Size	64 Bytes
Number of Pings	4

Target IP/Domain Name:	Enter the IP address or Domain name you would like to search.
Ping Packet Size:	Enter the packet size of each ping.
Number of Pings:	Enter the number of times you wish to ping.
Start:	Click **Start** to begin pinging target device (via IP).

Traceroute Parameters

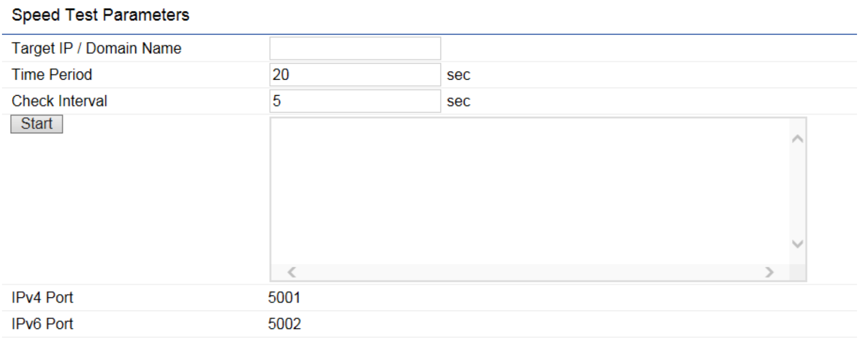


Traceroute Test Parameters

Target IP / Domain Name	

Target IP/Domain Name:	Enter an IP address or domain name you wish to trace.
Start:	Click **Start** to begin the trace route operation.
Stop:	Halts the traceroute test.

Speed Test Parameters



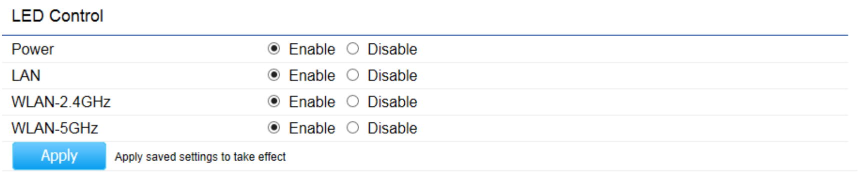
Speed Test Parameters

Target IP / Domain Name		
Time Period	20	sec
Check Interval	5	sec
IPv4 Port	5001	
IPv6 Port	5002	

Target IP/Domain Name:	Enter an IP address or domain name you wish to run a Speed Test for.
Time Period:	Enter the time in seconds that you would like the test to run.
Check Interval:	Enter the intervals in seconds at which you would like to run the test.
Start:	Starts the Speed Test.
IPv4 / IPv6 Port:	AT-MWS AP uses IPv4 port 5001 and IPv6 port 5002 for the speed test.

6.8 LED Control

This section allows you to control the LED control functions: Power status, LAN interface and 2.4GHz/5GHz WLAN interface.



LED Control

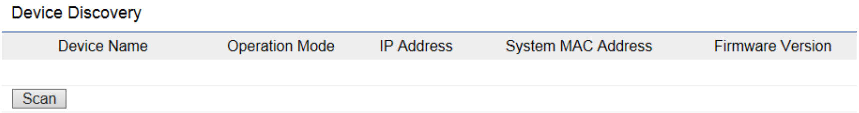
Power	● Enable ○ Disable
LAN	● Enable ○ Disable
WLAN-2.4GHz	● Enable ○ Disable
WLAN-5GHz	● Enable ○ Disable

Apply saved settings to take effect

Click **Apply** to save the settings after selecting your choices from the boxes.

6.9 Device Discovery

Under Device Discovery, you can choose for the AT-MWS AP to automatically scan for local devices to connect to. Click **Scan** to begin the process.



Device Discovery

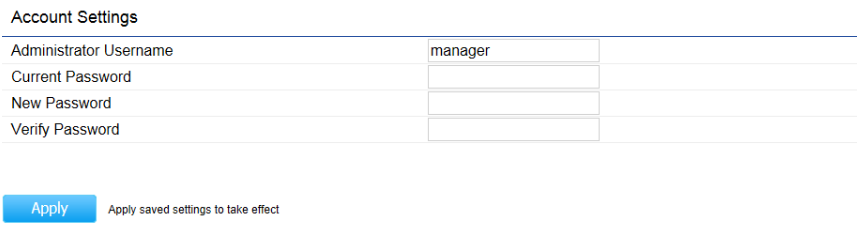
Device Name	Operation Mode	IP Address	System MAC Address	Firmware Version

7

System Manager

7.1 Account Setting

This page allows you to change the AT-MWS AP username and password. By default, the username is manager and the password is friend. The password can contain from 0 to 12 alphanumeric characters and is case sensitive.



Account Settings

Administrator Username	manager
Current Password	
New Password	
Verify Password	

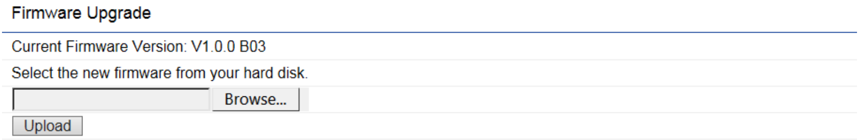
Apply saved settings to take effect

Administrator Username:	Enter a new username for logging in to the Administrator Username entry box.
Current Password:	Enter the old password for logging in to the Current Password entry box.
New Password:	Enter the new password for logging in to the New Password entry box.
Verify Password:	Re-enter the new password in the Verify Password entry box for confirmation.
Apply:	Click **Apply** to save the changes.

Tips **Note:** it is highly recommended that you change your password to something more unique for greater security.

7.2 Firmware Upgrade

This page allows you to upgrade the Firmware of the AT-MWS AP.



Firmware Upgrade

Current Firmware Version: V1.0.0 B03

Select the new firmware from your hard disk.

To Perform the Firmware Upgrade:

1 Click the **Browse...** button and navigate the OS File System to the location of the Firmware upgrade file.

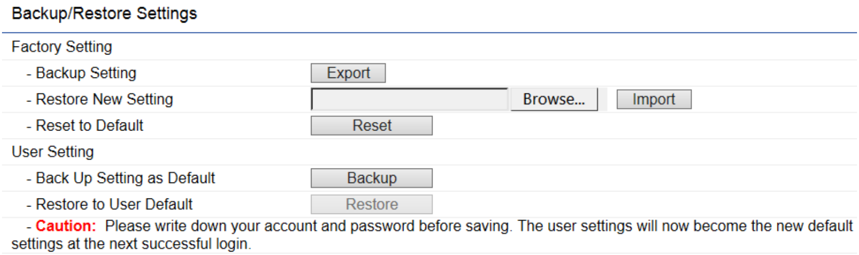
2 Select the upgrade file. The name of the file will appear in the Upgrade File field.

3 Click the **Upload** button to commence the Firmware upgrade.

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

7.3 Backup/Restore

This page allows you to save the current device configurations. When you save the configurations, you can also reload the saved configurations into the device through the **Restore New Settings** from a file folder. If extreme problems occur, or if you have set the AT-MWS AP incorrectly, you can use the **Reset** button in the **Reset to Default** section to restore all the configurations of the AT-MWS AP to the original default settings. To Configure the Backup/Restore Settings, click **Firmware** under the **Systems Manager** tab.



Backup/Restore Settings

Factory Setting	
- Backup Setting	Export
- Restore New Setting	Browse... Import
- Reset to Default	Reset
User Setting	
- Back Up Setting as Default	Backup
- Restore to User Default	Restore

- **Caution:** Please write down your account and password before saving. The user settings will now become the new default settings at the next successful login.

Tips **Important:** Do not edit or modify a backup configuration file.

Factory Setting

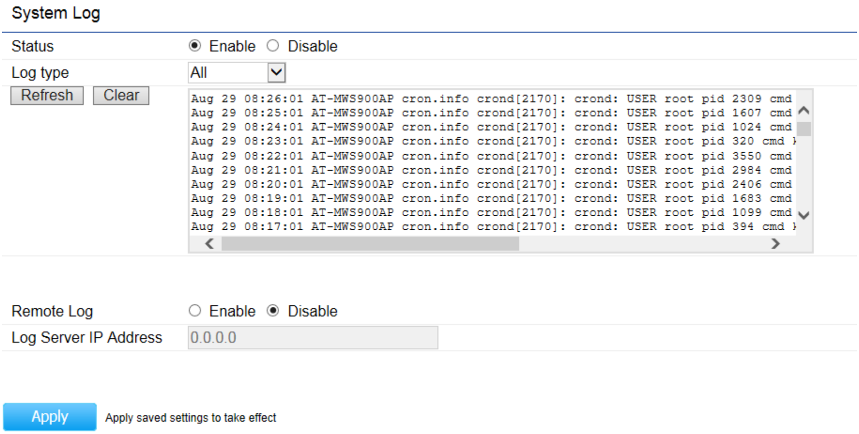
Backup Setting:	Click **Export** to save the current device configurations to a file.
Restore New Setting:	Choose the file you wish restore for settings and click **Import**.
Reset to Default:	Click the **Reset** button to restore the AT-MWS AP to its factory default settings.

User Setting

Back Up Setting as Default:	Click **Backup** to backup the user settings you would like to use as the default settings.
Restore to User Default:	Click **Restore** to restore the AT-MWS AP to user's default settings.

7.4 System Log

This page allows you to setup the System Log and local log functions of the AT-MWS AP. Click **Log** under the **Systems Manager** tab to open up the System Log page.



System Log

Status ● Enable ○ Disable

Log type: All

```
Aug 29 08:26:01 AT-MWS900AP cron.info crond[2170]: crond: USER root pid 2309 cmd
Aug 29 08:25:01 AT-MWS900AP cron.info crond[2170]: crond: USER root pid 1607 cmd
Aug 29 08:24:01 AT-MWS900AP cron.info crond[2170]: crond: USER root pid 1024 cmd
Aug 29 08:23:01 AT-MWS900AP cron.info crond[2170]: crond: USER root pid 320 cmd
Aug 29 08:22:01 AT-MWS900AP cron.info crond[2170]: crond: USER root pid 3550 cmd
Aug 29 08:21:01 AT-MWS900AP cron.info crond[2170]: crond: USER root pid 2984 cmd
Aug 29 08:20:01 AT-MWS900AP cron.info crond[2170]: crond: USER root pid 2406 cmd
Aug 29 08:19:01 AT-MWS900AP cron.info crond[2170]: crond: USER root pid 1683 cmd
Aug 29 08:18:01 AT-MWS900AP cron.info crond[2170]: crond: USER root pid 1099 cmd
Aug 29 08:17:01 AT-MWS900AP cron.info crond[2170]: crond: USER root pid 394 cmd
```

Remote Log ○ Enable ● Disable

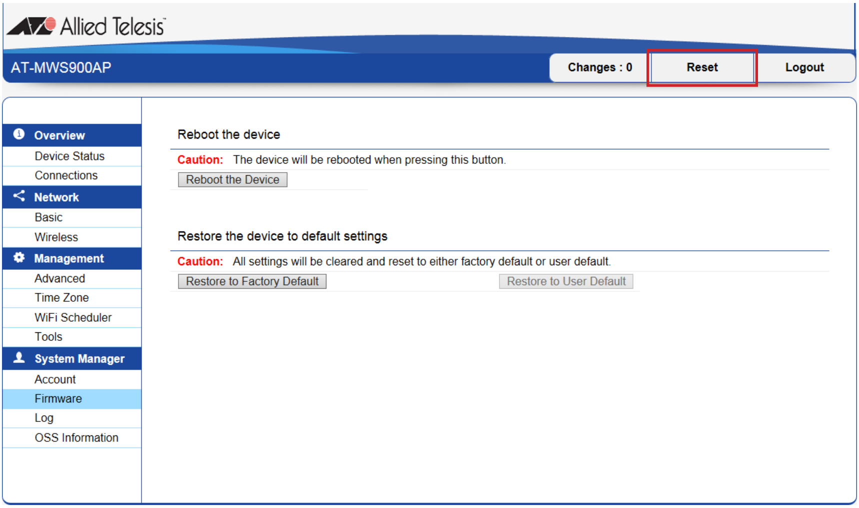
Log Server IP Address: 0.0.0.0

Apply saved settings to take effect

Status:	Enables or disables the System Log function.
Log Type:	Select the Log Type mode you would like to use.
Remote Log:	Enables or disables the Remote Log feature. If enabled, enter the IP address of the Log you would like to remote to.
Log Server IP Address:	Enter the IP address of the log server.
Apply:	Click **Apply** to save the changes.

7.5 Reset

In some circumstances, you may be required to force the device to reboot. Click on **Reboot the Device** to reboot the device.



Reboot the device

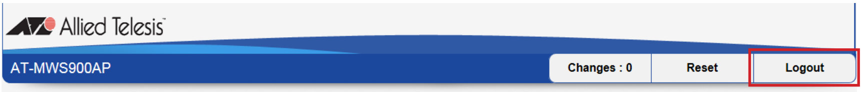
Caution: The device will be rebooted when pressing this button.

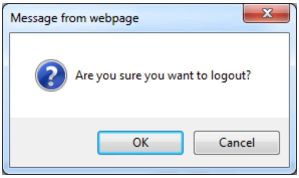
Restore the device to default settings

Caution: All settings will be cleared and reset to either factory default or user default.

7.6 Logout

Click **Logout**, it will pop up a warning window. Click **OK** to logout.





Are you sure you want to logout?

Copyright Notice

About Trademarks

Microsoft ®, Windows ® and Internet Explorer ® are trademarks of Microsoft corporation, registered in the U.S. and other countries.
All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.

Revision History

January 2015	Rev.A	Initial release

Allied Telesis K.K.