JetWave2212S/X

Industrial Dual 802.11n 2.4G/5G 2T2R MIMO Wireless AP

User Manual

V1.0 Oct, 2018

Copyright

About This Manual

This user manual provides the following notes:

1. The Declaration of Conformity policy and manufacturer information.
2. The Safety Precaution and important notification.
3. The technical specification of the product.
4. The instruction on how to install and configure your product.

Please read this document carefully and only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Conventions

For your attention on important parts, special characters and patterns are used in this manual:

Note:

This indicates an important note that you must pay attention to.

The Blue Wording is important note that you must pay attention to.

The Blue Wording with Big Case is very important note you must pay more attention to.

Warning:

This indicates a warning or caution that you have to abide.

The Red wording is very important you must avoid.

Bold: Indicates the function, important words, and so on.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

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

This device is restricted to indoor use.

IMPORTANT NOTE:

FCC 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 20cm between the radiator & your body.

Korenix Technology Co., Ltd.

14F., No.213, Beixin Rd., Xindian Dist., New Taipei City 23143, Taiwan (R.O.C.)

TEL: +886-2-8911-1000

Safety Precautions – JetWave Wireless Product

General Notification
● Only operate the device according to the technical specification. You can find the information from the product datasheet, user manual…etc. ● Read the installation instructions before connecting the system to the power source. ● If you don't get exact info you need, you can contact Korenix technical people, korecare@korenix.com. Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
● The devices are designed for operation with extra-low voltage (SELV). Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC/EN 60950 based safety standards. (Not included 110V input model)
Solely connect the power supply that corresponds to the type of your device. For power connection, make sure the following requirement are met: ● The DC power circuit of the product is isolated design circuit. In practical, it is suggested to use isolated DC power design PSU for field installation. Besides the PSU selection, well digital/earth grounding is also important before power on the system. ● The Power Supply conforms to the overvoltage category I or II. ● The output voltage of the AC/DC to DC Power Supply conforms to the range of the input voltage of the equipment. ● The connection cables used are permitted for the specified electronic voltage, current, wire diameter and temperature range. (Wire Diameter of AC voltage is at least 0.75mm, AWG18. For DC voltage, it is at least 1.0mm, AWG16.) ● Follow the power installing instruction of the user manual, it indicates the input voltage, pin assignment, connection circuit and notice. ● The Power Supply must be well installed, includes grounded and other notices which are defined in its instruction guide. ● Only switch on the supply voltage to the device if the housing is closed, the terminal blocks are wired up correctly and the terminal blocks are connected.

- The equipment must be grounded. Ground the device before connecting the cables, antennas and power supply. The grounding of the equipment and DC Power Supply may be different in some applications, then, you must ground them separately.
- Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Environment & Housing

- **Hot surface.** Avoid touching the device while it is operating.
- Only operate the device at the specified ambient temperature and humidity. The temperature of the surrounding air means a distance of up to 5cm from the device. While installing multiple devices within the cabinet, remains suitable width between the devices is MUST for better heat dispersing.
- Better install the device in the vertical position, with the upper antenna connections pointing upward, lower antenna pointing downward.
- Install the device in a cabinet or in an operating site with limited access, the metal cabinet will filter the radio signals, use the extended antenna cable and install the external antenna in free space helps to get better Radio signal.
- Only technicians authorized by the manufacturer are permitted to open the housing. Without the manufacturer permitted, open the housing means the product is not warrantied and no responsible for any unexpected risk.

Installation

If you are installing the wireless equipment in the field box or outdoor area, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.

Please note the following things as well:

- Do not use a metal ladder;
- Do not work on a wet or windy day;
- Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.

- If you are installing the equipment in the indoor office or factory, be aware of the power source and grounding must be well installed. The professional Wireless IT Engineer can provide service for AP location, channel and field plan to get better performance and coverage.
- Connect the equipment which meets the IP degree of protection requirements for the application case.

- Read the Radio output power, receiver sensitivity, antenna gain specification before installing. The shipped products and antenna comforts to the R&TTE and allowed to be used in all European countries. You can read the related technical specification from the product datasheet or user manual.
- When installing external antennas, the Radio Output power and antenna gain value must be allowed according to the regulations of the country.
- When the system is operational with high gain antenna, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.
- When the system is operational with high gain antenna in short distance, adjust the radio output lower. Strong output power plus high gain antenna is not good installation for short distance transmission.

- You are responsible for undertaking suitable lightning protection.
- Install over voltage protector devices on every outdoor Ethernet cable.
- Protect each antenna installed outside with lightening protection devices, ex: lightening arrester.

Note that Field EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.

Content

Chapter 1

Introduction

Chapter 1 Introduction

1.1 Introduction

The user manual is applied to Korenix JetWave 2212S/X Industrial Wireless Access Point. JetWave 2212S/X provide perfect solution to manage serial devices via Ethernet/Wireless in flexible ways, such as TCP server, TCP client, UDP. JetWave 2212S/X creates a transparent gateway for the serial communication to Ethernet/Wireless. The Wireless LAN solution is 802.11a/b/g/n with up to 300Mbps data rate. Give you an easy way and high bandwidth connection to the hard-to-wire or moved serial devices, ease your network cabling problem in the field.

Model List

JetWave2212X-E: 2 x Fast Ethernet Ports EU version

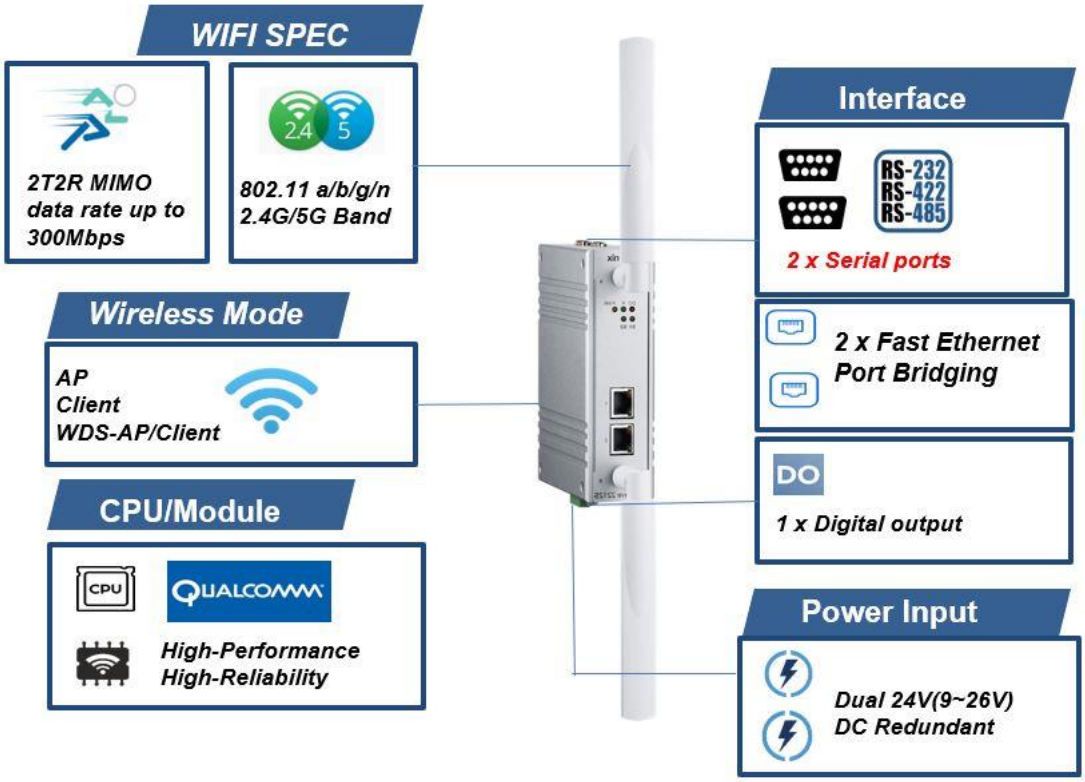
JetWave2212X-U: 2 x Fast Ethernet Ports US version

JetWave2212S-E: 2 x Fast Ethernet Ports + 2 Serial Ports EU version

JetWave2212S-U: 2 x Fast Ethernet Ports + 2 Serial Ports US version

1.2 JetWave 2212S/X Appearance

JetWave2212S



JetWave2212X

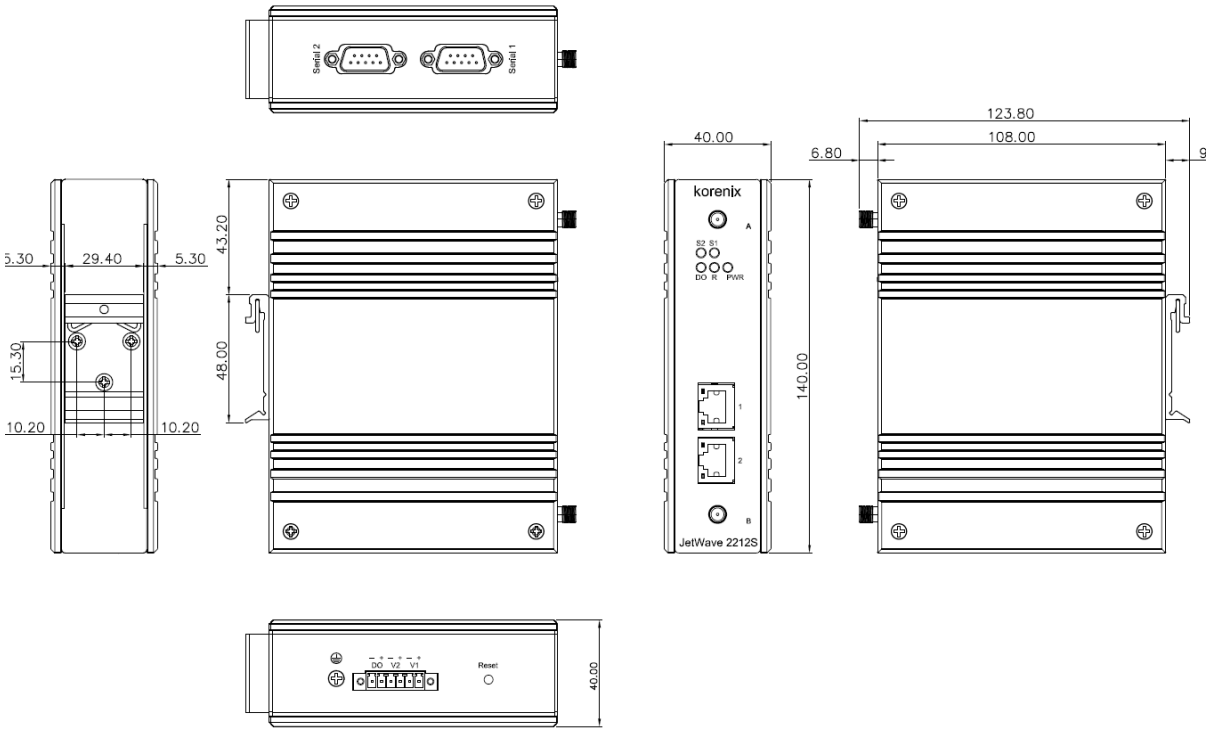
1.3 JetWave 2212S/X Major Features

Features:

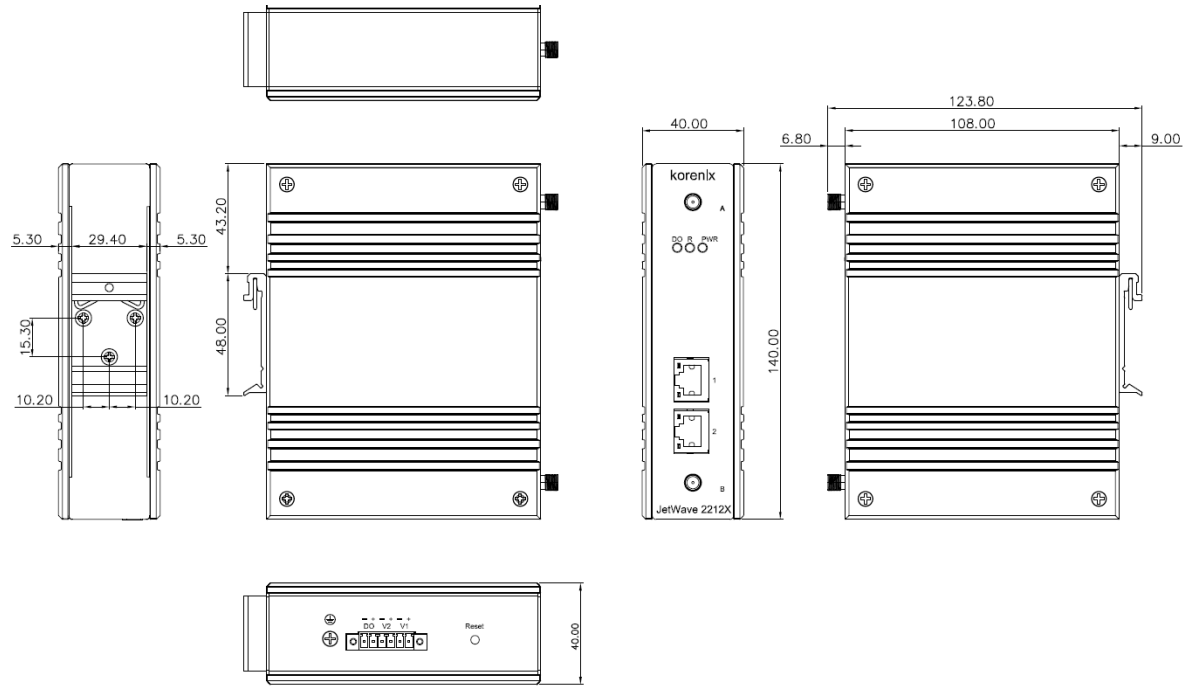
- Industrial Slim Size Wireless AP
- 2-port RS-232/422/485 to Wireless Network(JetWave 2212S ONLY)
- IEEE 802.11a/b/g/n 2.4G & 5G Wi-Fi, up to 2T2R MIMO, 300Mbps
- 2-port Fast Ethernet Port
- Versatile Serial Application: TCP Server, TCP Client and UDP listening
- Management by Web GUI and Korenix View Commander
- Event Warning by Syslog, Email and SNMP trap
- Heavy Industrial Grade design
- Operating Temperature: -40~75°C
- Triple Power Inputs by 9~26VDC Terminal Block

1.4 JetWave 2212S/X Product Dimension

JetWave 2212S



JetWave 2212X



1.5 Product Package

The product package you have received should contain the following items.

Package
JetWave 2212S or 2212X unit
2x Wi-Fi 2.4G+5Ghz Antenna
Din-Rail Mounting Kit
6-pin terminal connector
Quick Installation Guide
Note: Please download the utility and user manual from Korenix Web site.

Chapter 2
Hardware Installation

Chapter 2 Hardware Installation

This chapter describes safety precautions and product information before installing JetWave 2212S/X.

2.1 Professional Installation Required

- Please seek assistance from a professional installer for field installation or professional IT Engineer for indoor installation. These engineers must be well trained in the RF installation and knowledgeable for the Wireless AP setup and field plan.
- The JetWave 2212S/X series is distributed through distributors and system installers with professional technicians and will not be sold directly through retail stores.

2.1.1 Safety Precautions

To keep you safe and install the hardware properly, please refer to the safety precautions in the front pages of this manual. **The Safety Precautions described in the front pages include General Notification, Power Source & Grounding Notification, Environment & Housing Notification and Installation Notification.**

Additional Notification for the product:

1. The DC power circuit of the product is isolated design circuit. In practical, it is suggested to use isolated DC power design PSU for field installation. Besides the PSU selection, well digital/earth grounding is also important before power on the system. Connect the Ethernet Cables, Antennas or Antenna RF Cables, Ground and Power Terminal Block well before powering on.

2. If you are installing the product in the field box, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines. Please note the following things as well:

- Do not use a metal ladder
- Do not work on a wet or windy day
- Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.

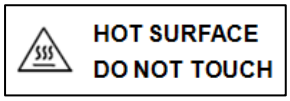
3. If you are installing the product in the indoor office or factory, be aware of the power source and grounding must be well installed. The professional Wireless IT Engineer can provide service for location, antenna and field plan to get better performance and coverage.

4. When you exchange to high gain antenna on JetWave 2212S/X, please notice that the Radio Output power and antenna gain value must be allowed according to the regulations of the country. And avoid standing directly in front of high gain antenna. Strong RF fields are present when the transmitter is on.

5. You are responsible for undertaking suitable lightning protection. Install over voltage protector devices on every outdoor Ethernet cable. Protect antennas installed outside with lightening protection devices, ex: lightening arrester.

Note that Field EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.

6. The operating temperature of JetWave 2212S/X series is from -40 to 75℃, please MUST installed the device in a restricted access location to avoid the hot surface of housing, and make more aware of potential hazards and reduce the risk.



2.2 Power Installation

The system provides dual DC power input.

2.2.1 DC Input

1. There is one 6-pin terminal block within the package, which is applied for screwing the DC wires. It is a good practice to turn off the system power, and to unplug power terminal block before making wire connections

2. Insert the positive and negative wires into the V+ and V- contact on the terminal block connector. Tighten the wire-clamp screws to prevent DC wires from being loosened. The range of the suitable electric wire is from 12 to 24 AWG.

3. The typical and suggest power source is DC 24V, the acceptable range is range from 9~26V. The dual DC power can be redundant. You can connect one power to typical power source and the other to battery/UPS as backup.

4. If you connect the wrong positive/negative wires, the system would not be power on or cause unexpected error. Please avoid this in field installation.

2.2.2 Connect both DC input

The 2 power sources DC input are redundant power design. When you connect 2 power sources, for example you connect the DC Power 1. While you power on the DC power 1 as the 1st power source, the DC power 2 port will not power from DC power 2. In this condition, while the DC power source failure, the other power source can seamlessly redundant.

I/O Configuration

2.3.1 Wiring your Ethernet Port

T There are two Fast Ethernet ports. The 2 ports are standard RJ-45 form factor. They can support 10Base-TX and 100Base-TX. All the Ethernet ports will auto-detect the signal from connected devices to negotiate the link speed and duplex mode. Auto MDI/MDIX allows users to connect another switch, hub or workstation without changing straight through or crossover cables. In some cases, the MDI/MDI-X may requests the connected device support auto-negotiation.

Available Cable Type:

10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable (100m)

100 Base-TX: 2/4-pair UTP/STP Cat. 5 cable (100m)

Cable Request in Harsh environment: CAT 5E/CAT 6 is preferred for Data transmission.

Wiring STP Cable: STP (Shielded Twisted Pair) cable is preferred. The device is a heavy Industrial EMC certificated product and usually install in harsh environment, part of the EMS protection are based on STP cable, for example the surge protection of front Ethernet ports. STP cable can provide better field protection. It is MUST for the device installation in harsh environment.

Reset

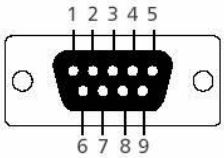
There is one reset button located on the top of the device. The reset button provides users with a quick and easy way to restore the default settings of JetWave 2212S/X. Press reset button for 7 seconds.

JetWave 2212S/X unit will restore to default value including default IP address (192.168.10.1), and no password. When the Power LED turns green, the device is ready to function.

2.3.2 Serial

Connect the serial device to the unit DB9 male port by the pin assignment table.

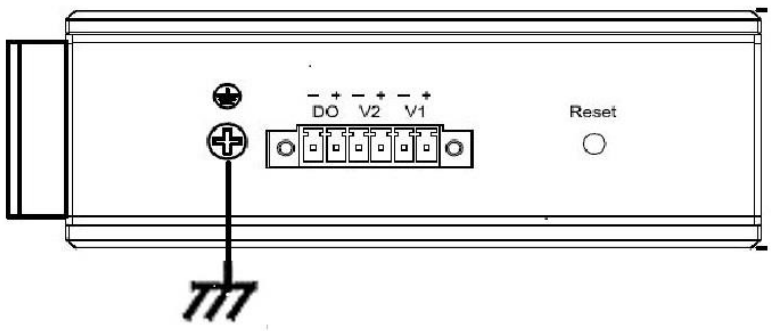
Pin Assignment



Pin #	RS232	RS422	RS485 (4 wire)	RS485(2 wire)
1	DCD	TX-	TX-	DATA-
2	RXD	TX+	TX+	DATA+
3	TXD	RX+	RX+	-
4	DTR	RX-	RX-	-
5	GND	GND	GND	GND
6	DSR	-	-	-
7	RTS	-	-	-
8	CTS	-	-	-
9	RI	-	-	-

2.3.3 Ground

To ensure the system will not be damaged by noise or any electrical shock, we suggest you to make exact connection with the Earth Ground. There is one Earth Ground screw on the bottom side of the device. Loosen the earth ground screw then tighten the screw after earth ground wire is connected.



2.3 WIFI Antenna

The JetWave 2212S equips two antenna sockets for Wireless 2T2R MIMO. The product attaches the Wi-Fi antennas inside the package.

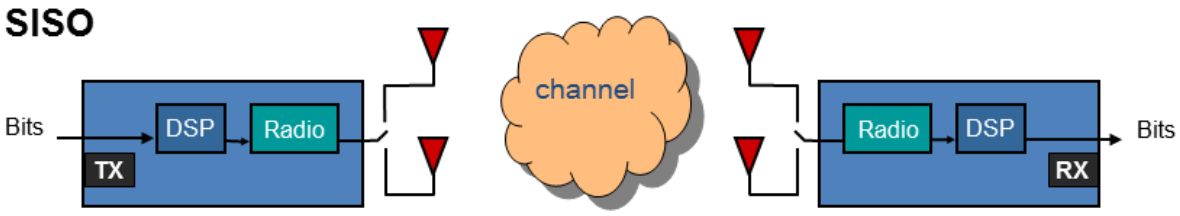
Model Name/ Type	JetWave 2212S/X
Radio	802.11n 2.4GHz/5G
Antenna (Wifi Dual Band)	2dBi for 2.4G 4dBi for 5G

2.4.1 MIMO & Dual Polarization

- **What is MIMO:**

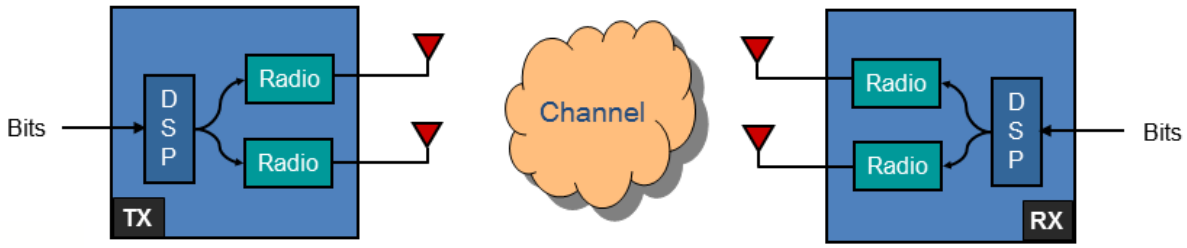
With the rising data rates and signal congestion, the MIMO is the proposed radio technology in IEEE 802.11n and accepted popularly. MIMO is short of the Multiple-Input and Multiple-Output, is the use of multiple antennas at both the transmitter and receiver to increase the wireless communication bandwidth, for example the 2T2R means 2 Transmitter and 2 receiver, then the bandwidth is double than SISO. MIMO technology offers significant increases in data throughput without additional bandwidth or increased transmit radio power.

The below figure shows the SISO technology, each transmitter and receiver has single radio.



The below figure shows the MIMO technology, the transmitter and receiver spread the total transmit power to 2 (or more) different radio antenna for communication.

MIMO

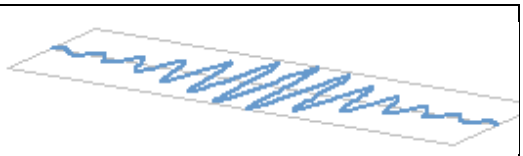
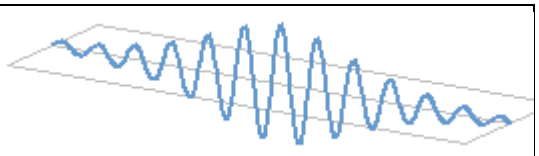


➢ **What is Polarization:**

Polarization is a property of wireless antenna, the polarization determines the antennas that can pick up the signal, for example you can set up two antennas in close and pointing to the same direction, but with different polarization. The result is only antennas with the same polarization will be able to communicate with each other, this is important especially in point-to-pint wireless communication.

There are two major polarizations, Vertical and Horizontal. The antenna may support either one, you can choose Vertical or Horizontal polarization for the antenna installation. The result would be that antenna which is vertically polarized would only receive the signal from the vertically transmitting antenna, horizontally polarized antenna would only receive horizontally transmitting antenna.

The below figures show the typical Horizontal / Vertical polarization:

Horizontal Polarization	Vertical Polarization
	

2.4.2 Antenna Socket

The JetWave 2212S/X supports IEEE 802.11n and 802.11ac 2T2R MIMO technology. JetWave 2212S/X series is embedded antenna that you don't need to mount external antennas. JetWave 2212S/X is external antenna model, it equips SMA Type antenna sockets for two WIFI radio (2x sockets by option), you can connect 2 WIFI antennas based on your need.

Antenna termial side

RP-SMA Male

JetWave 2212S/X Antenna terminal side

RP-SMA Female

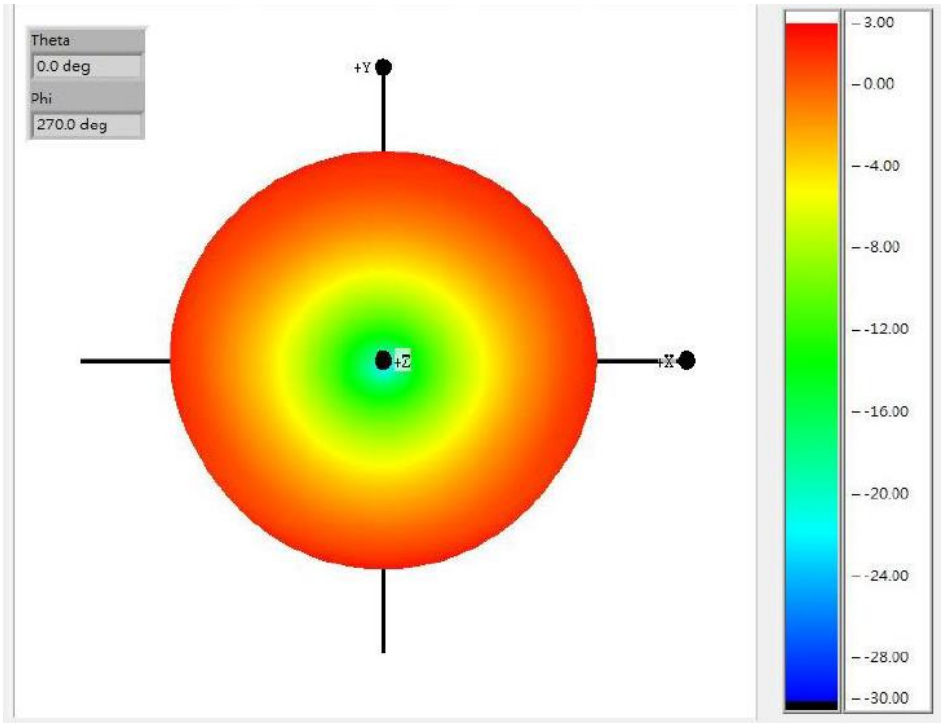
2.4.3 Default External WIFI Antenna Specification:

The following information applied to the default WIFI antenna.

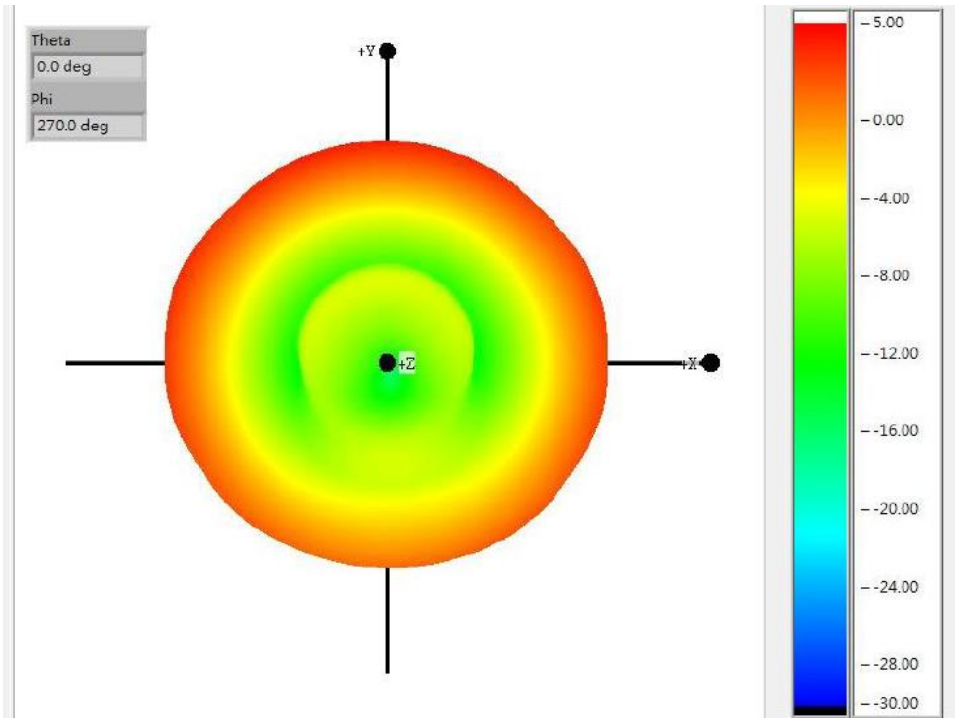
External SMA type 2.4G/5G 2T2R Antenna			
Frequency (MHz)	2400-2500	5150-5350	5475-5875
Peak gain(dBi)	2.44	4.41	4.73
VSWR	1.8：1 Max.		
Polarization	Linear, vertical		
Impedance	50 Ω		

Reference Distance: The suggested distance of the embedded WIFI antenna is from 150 to 300 meters wide in public space. (However, the free space lost may affect the transmitting distance, so that the device may have different performance in different environment.)

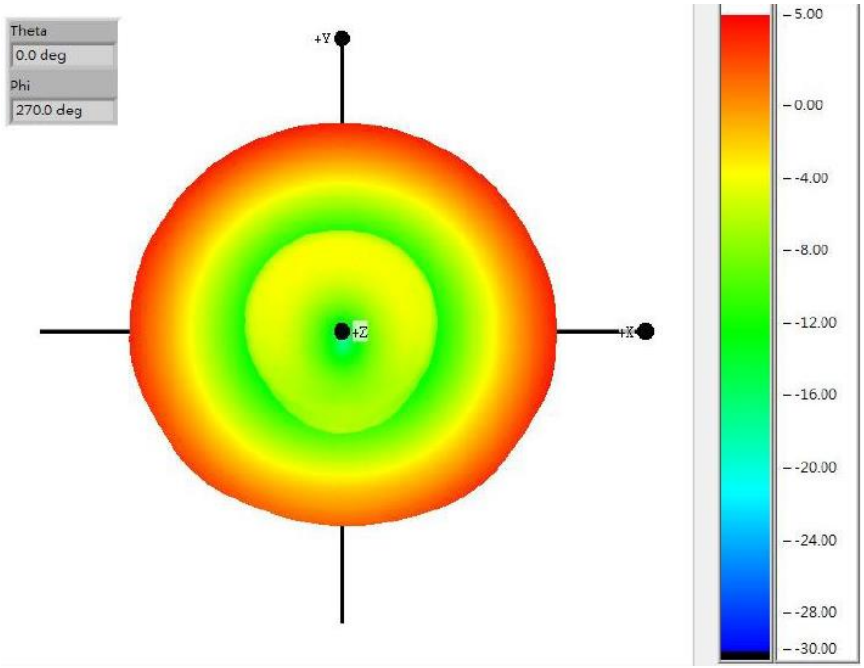
➢ **2.5G Antenna Radiation Pattern**



➢ **5.15G Antenna Radiation Pattern**



➢ **5.55G Antenna Radiation Pattern**



2.4 Mounting

2.5.1 Din-Rail Mounting Installation

The DIN-Rail clip is already attached to the JetWave 2212S/X when packaged. If the DIN-Rail clip is not screwed on the Switch, follow the instructions and the figure below to attach DIN-Rail clip to the Switch.

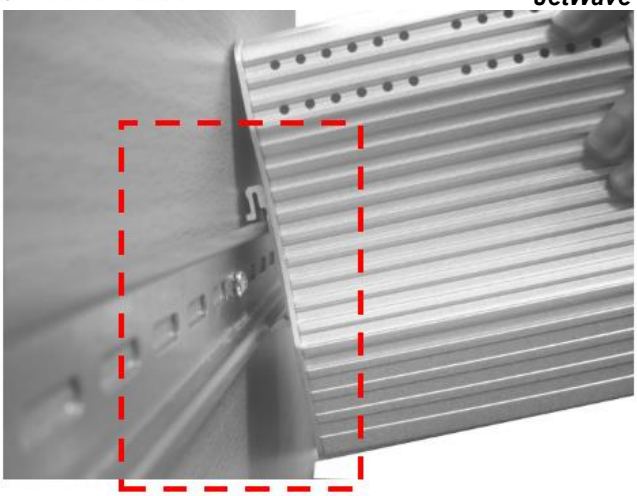
Use the screws to attach DIN-Rail clip to the real panel of Switch.

1. Use the screws to attach DIN-Rail clip to the real panel of Switch.

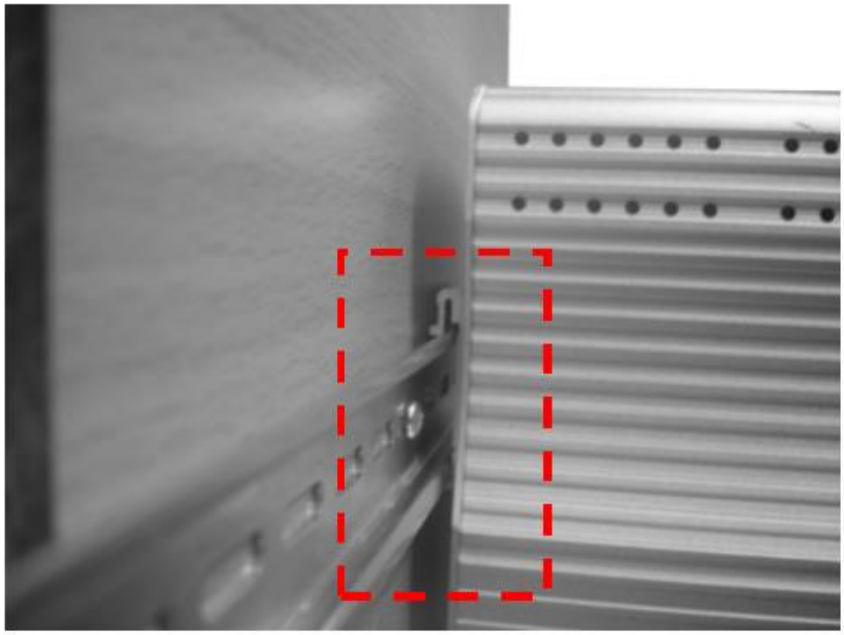
2. To remove DIN-Rail clip, reverse step 1.

Follow the steps below to mount the Ethernet Switch to the DIN-Rail track:

1. First, insert the upper end of DIN-Rail clip into the back of DIN-Rail track from its upper side.



2. Lightly push the bottom of DIN-Rail clip into the track.



3. Check if DIN-Rail clip is tightly attached on the track.

4. To remove it from the track, reverse the steps above.

Notes: The DIN Rail should compliance with DIN EN50022 standard. Using wrong DIN rail may cause system install unsafe.

2.5.2 Mounting the SMA external antenna:

While selecting the SMA external antenna, you must use SMA type, please notice that the antenna should support Vertical Polarization for 2T2R MIMO radio transmission.

2.5 Using the External Antenna

Consult your system integrator or our technical support engineer to choose the suitable external antenna with SMA-type for your application.

Select the External Antenna:

Gain: It affects the system performance.

Polarization: Vertical Polarization is MUST for this 2T2R MIMO product.

Connector: SMA-Type.

Note:

- When prepare the external antenna, make sure the antenna can support Vertical Polarization.
- Most of high gain external antenna is installed in higher place than AP, get low power lost antenna cable in advance.
- While installing the AP within metal field box, connect the extended antenna cable to outside the box is must to avoid the Radio lost.

Chapter 3

Prepare for Management

Chapter 3 Prepare for Management

The JetWave 2212S/X Series supports Web GUI Configuration, Simple Network Management Protocol (SNMP), Telnet and Diagnostic Command Line Interface for management and Window Utility helps you discover the device cross network, basic IP setting, firmware management…etc.

This chapter describes the preparation for management. In your first time access the device, you can refer to the Basic Factory Default Settings to know the default settings and the default IP of the device.

The chapter also tells you how to login the Web-based interface, Diagnostic Console. If you forget IP address you changed, you can use Korenix View Utility to discover the devices' IP address and then access it.

3.1 Basic Factory Default Settings

We elaborated the JetWave 2212S/X Series basic factory default settings. You can re-acquire these parameters by default. This info is easier for you to find the device and access the switch's configuration interface. For further info, please refer to configuration guide of the feature set.

Table 1 JetWave 2212S/X Basic Factory Default Settings

Features	Factory Default Settings
Username	admin
Password	admin
Model Name	JetWave2212S (/2212X depends on which model you access)
Device Name	korenixXXXXXX (X represents the last 6 digits of Ethernet MAC address)
Country/Region	By model: JetWave2212S/X-E: European Union JetWave2212S/X-U: United States JetWave2212S/X: All Country

Default IP (Lan Settings)		
IP Address		192.168.10.1
Subnet Mask		255.255.255.0
Default Gateway		0.0.0.0
Default IP		
IP Setup	Access Type	Static IP
	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DNS1	8.8.8.8 (Google IP)
	DNS2	0.0.0.0
	(Refer to the System – IP Settings for further information)	
Wireless Settings		
Wireless Basic Setting	Wireless Mode	AP
	Wireless Network Name (SSID)	JetWave_1 (WLAN 1)
	Broadcast SSID	Enabled
	802.11 Mode	802.11G/N
	Frequency/ Channel	2437MHz(6)
	Channel Mode	20 MHz
	Data Rate	Auto
	(Refer to the Wireless – WLAN – Basic Settings)	
Wireless Advanced Settings	A-MPDU aggregation	Enabled
	A-MSDU aggregation	Disabled
	Short GI	Disabled
	RTS Threshold	2347
	Fragment Threshold	2346
	Beacon Interval	100
	DTIM Interval	1
	Preamble Type	Auto
	Ap Roaming	Disabled
Other Settings		
Remote Settings	Remote Management Privacy	Telnet, SNMP
	Server Port:	161

SNMP	Get Community	Public
	Set Community	Private
	Trap Destination	0.0.0.0
	Trap Community	Public
Korenix View Utility	Device Search, IP Assign, Basic Tool, Wireless Panel	**Note:** While using Korenix View Utility to search the device, please connect to the LAN.

Warning:

It is Important to change all the default settings of the Wireless AP, includes the User Name, Password, Default IP Address, Default SSID, SNMP Community Name and configure Wireless Security to secure your network.

3.2 System Requirements

Before configuration, please make sure your system meets the following requirements:

- A computer coupled with 10/100/1000 Base-T(X) adapter;
- Configure the computer with a static IP address of 192.168.10.X (X cannot be 0, 1, nor 255), as the default IP address of JetWave 2212S/X Series is 192.168.10.1
- A Web browser on PC for configuration such as Microsoft Internet Explorer 6.0 or above, Google Chrome or Firefox.

Note: If you want to do throughput test, not just configure the switch, please notice that the throughput of the high performance and low performance CPU must be different.

3.3 How to Login the Web-based Interface

The system provides you with user-friendly Web-based management tool.

Open Web browser and enter the IP address (Default: **192.168.10.1**) into the address field. You will see the WELCOME page as below.

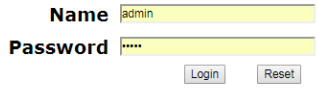


Figure – Web GUI Login Page

Enter the name of Account (Default: **admin**) and password (Default: **admin**) respectively and click "**Login**" to login the main page of the device. As you can see, this management interface provides main options in the above, which are **Status**, **System Wireless, Serial, Tools, Save, Logout** and **Reboot.**

(Note: Routing page appears when Network Mode set Route ETH WAN)

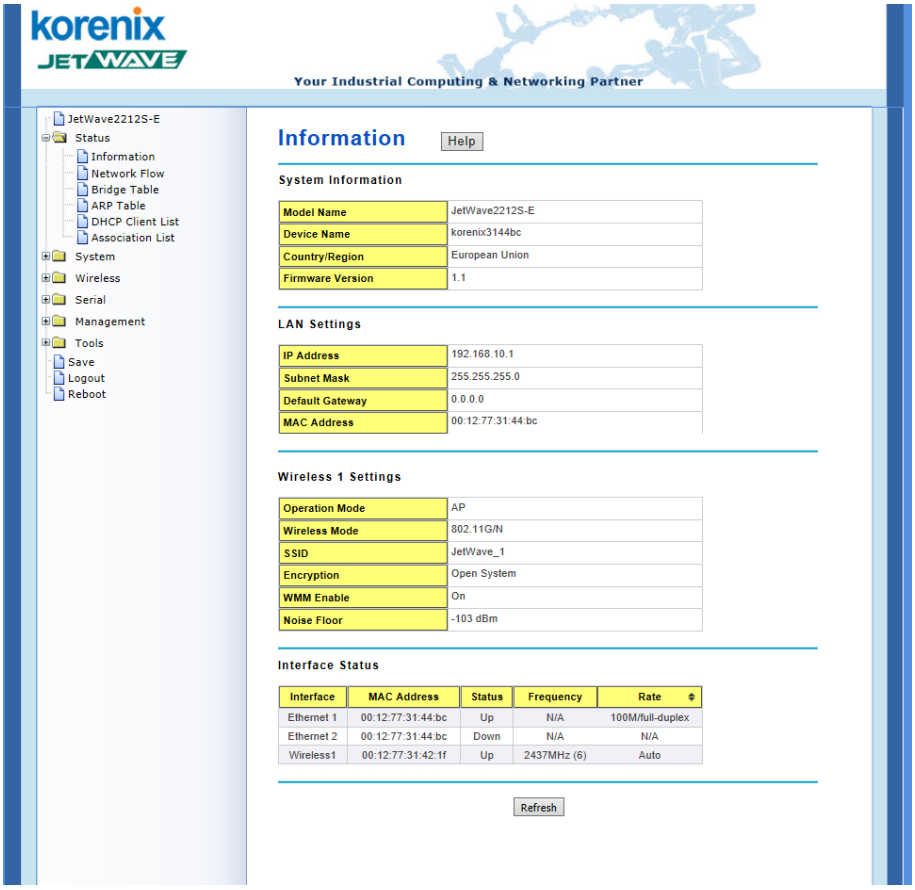


Figure - Main Page

3.4 Fail to login the Web GUI

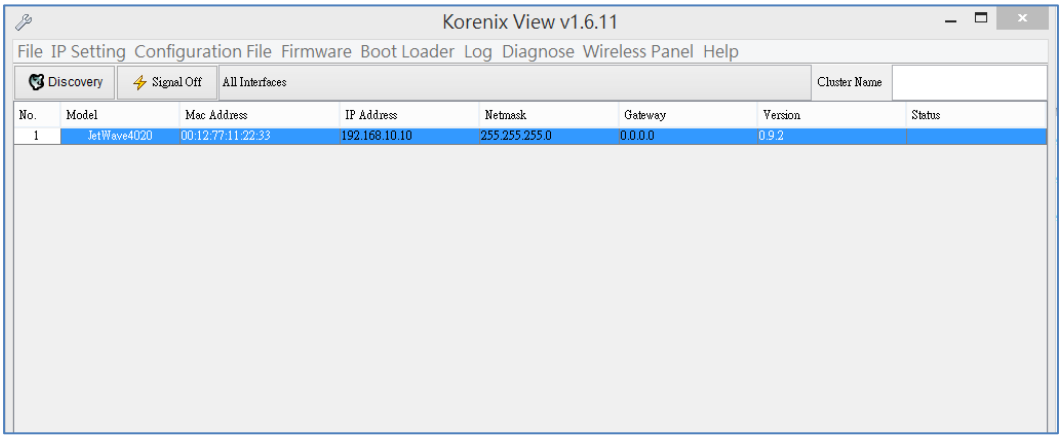
If you failed to login the web GUI, there are something you can do for troubleshooting.

1. Normally, you can access the device by using any kind of Window based Web browser, such as Microsoft Internet Explorer, Google Chrome, Firefox…, to configure and interrogate the product from anywhere on the network. If you failed access in either of the above Web browser, this might be the interoperability issue among your PC, OS version, Web browser and our product. You can try another Web browser as first self-aid, it usually works.
2. Please disable the firewall setting of your browser. The firewall setting may block the connection from your PC to the device. Note that after finished the setting, re-enable your firewall to protect your PC.
3. Check the IP Setting, your PC and managed device must be located within the same subnet.
4. Check the connected port, the default GT1 and GT2 equipped with different IP Address in Router mode.
5. The Web UI connection session of the device will be logged out automatically if you don't give any input after 30 seconds. After logged out, you should re-login and key in correct user name and password again.
6. Please contact Korenix engineer (Korecare@korenix.com) once you have problem for login.

3.5 Discovery Utility – Korenix View Utility

Korenix View is client/server architecture. Users use the client application to issue the operations and there is a server on the device to do these operations. The major difference between the Korenix View and other management tools, ex. Web, CLI, and SNMP, is that the Korenix View can configure several devices at the same time.

The PC with Korenix View Utility can discover the AP cross the IP subnet. But, if you want to do further configuration, the PC must be located in the same subnet with your AP. Change the IP address of your PC or change the IP address of the AP.



- Please download the latest Korenix View Utility from Korenix Web Support page.
- The chapter 5.3 introduces how to use Korenix View Utility.

Chapter 4

Web GUI Configuration

Chapter 4 Web GUI Configuration

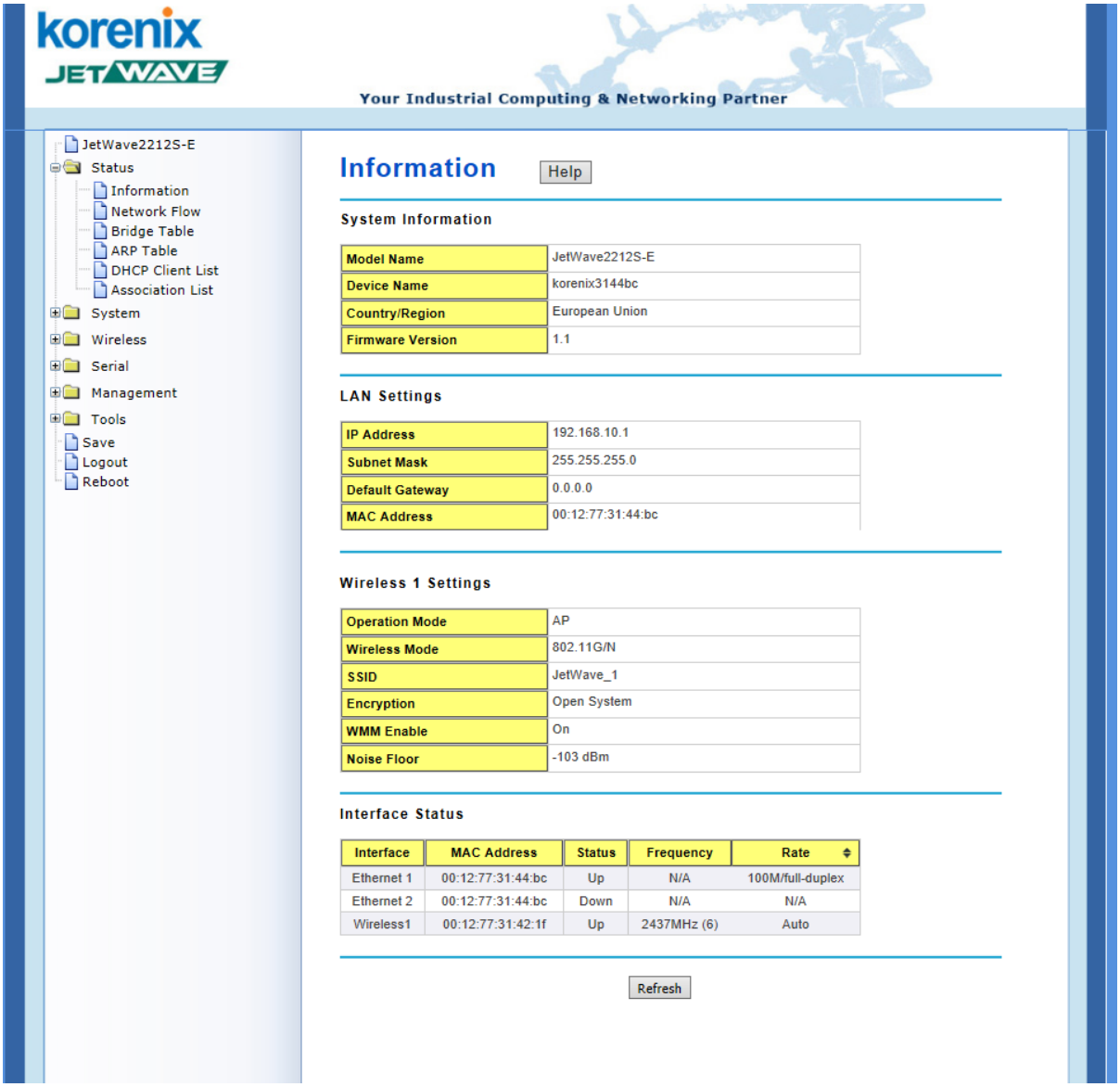
This chapter describes the Web GUI for Software Configuration.

4.1 Status

The Status feature set includes Information, Network Flow, Bridge Table, ARP Table , DHCP Client List and Association List. The information allows you to see the information of the device.

4.1.1 Information

This page shows the current status and some basic setting of the device.



System Information: The Model Name, Device Name, Country/Region you selected and Firmware version.

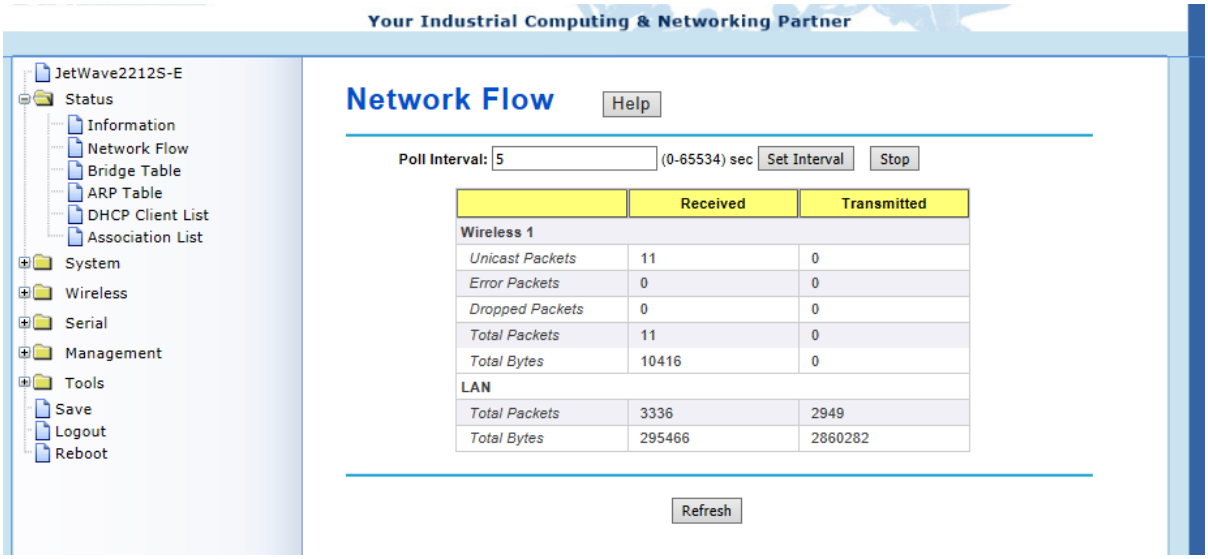
LAN Settings: It shows the IP Address, Subnet Mask and Default Geteway of the MAC Address.

Wireless Settings: It shows the Operation Mode, Wireless Mode, SSID, Encryption, A, WMM State, Noise Floor.

Interface Status: This table shows the Interface Name, MAC Address, Status, Frequency and Rate.

4.1.2 Network Flow

This page shows the packet counters for transmission and reception regarding to Wireless 1, Ethernet.



Poll Interval: The poll interval time setting, range from 0~65534 seconds. If you want to change the poll interval time, press “Stop” and then enter new value, press “Set Interval” to activate.

Set Interval: Set new Interval time after enter new poll interval time.

Stop: Stop polling the associated clients.

4.1.3 Bridge Table

The table shows the Bridge table.

MAC Address: The MAC Address of the connected device.

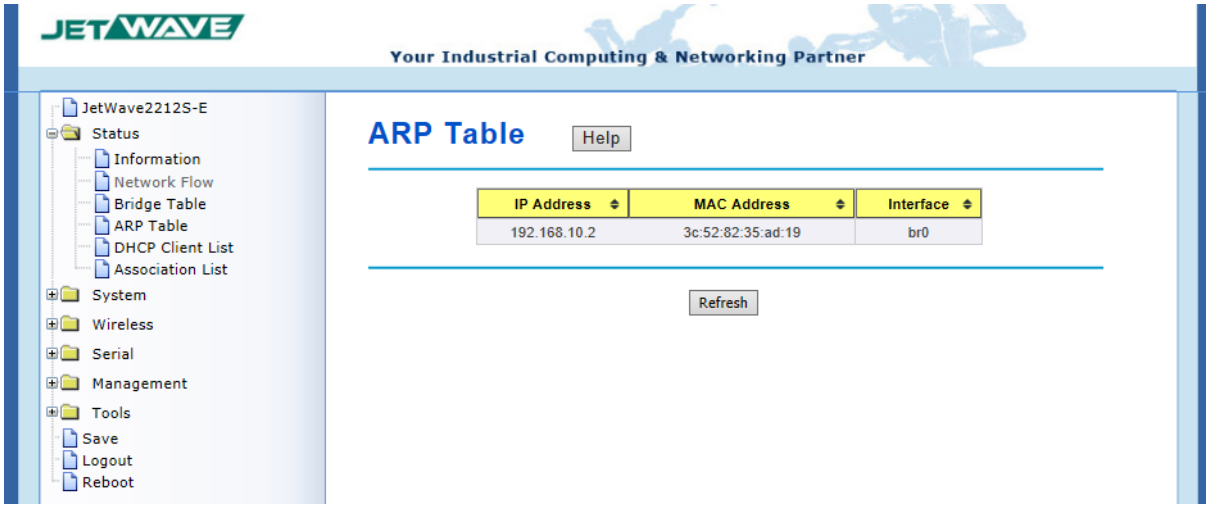
Interface: The field shows the interface which learnt the MAC Address.

Ageing Timers(s): The aging time of the this entry. If the MAC didn't transmit any packet, the aging time will start counting, and delete the entry after aging timeout.

Refresh: Refresh the table.

4.1.4 ARP Table

This table shows the ARP table.



IP Address: The IP Address leant from the interface.

MAC Address: The MAC Address leant from the interface.

Interface: The interface which learnt the ARP packet (IP and MAC Address).

Refresh: Refresh the table.

4.1.5 DHCP Client List

This table shows the assigned IP address, MAC address and Time Expired of the connected DHCP client devices.

IP Address: The assigned IP address of the connected DHCP client device.

MAC Address: The MAC Address of the connected DHCP client device.

Time Expired(s): The DHCP expire timer connected DHCP client device. Time unit is second. The number can be changed in DHCP Server Lease Time setting.

Refresh: Refresh the table.

4.1.6 Association List

This table shows the MAC Address, IP Address, RSSI and Connection Time for each associated devices.

Poll Interval: The poll interval time setting, range from 0~65534 seconds. If you want to change

the poll interval time, press “Stop” and then enter new value, press “Set Interval” to activate new setting.

Set Interval: Set new Interval time after enter new poll interval time.

Stop: Stop polling the associated clients.

====Entry Info==========

SSID: The SSID of wireless interface that associated with wireless client device.

MAC Address: The MAC Address of the associated device.

Signal Strength: The signal strength of the associated device. The value can help you to see the connection quality of AP/WDS-AP and Client/WDS-Client.

Noise Floor: The Noise Floor of the associated device.

Connection Time: The time when the device connected to the AP.

Last IP: The last IP address it had.

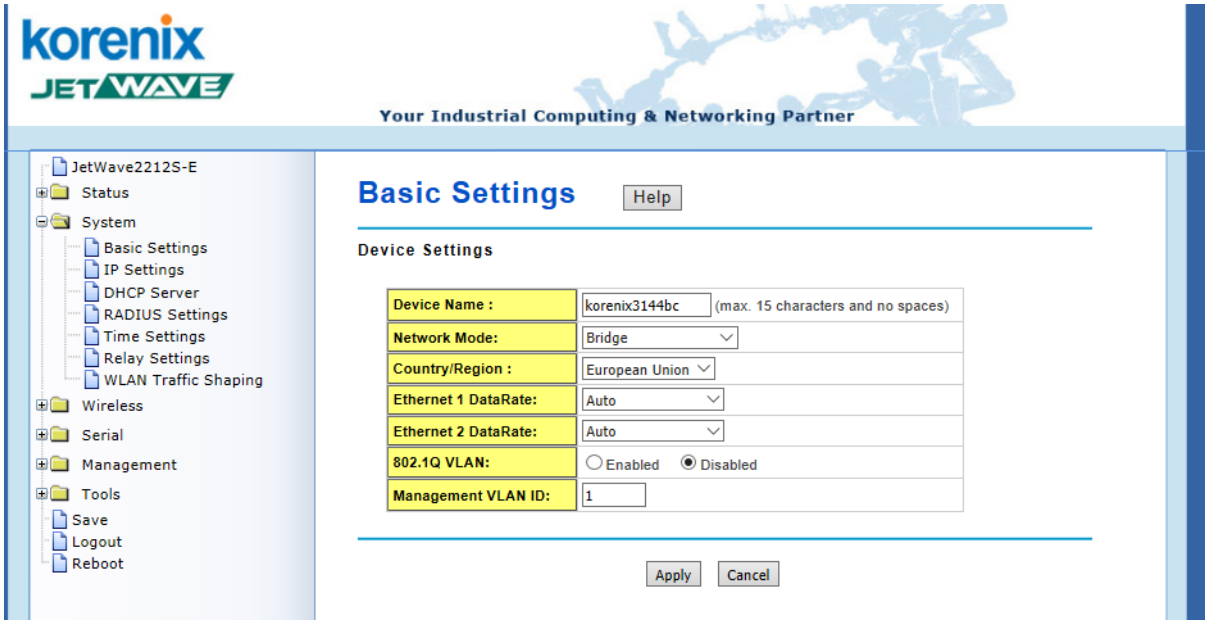
Action – Kick: This command allows you force kick the associated client.

Refresh: The item helps you refresh the table manually.

4.2 System

For users who use the JetWave 2212S/X for the first time, it is recommended that you begin configuration from the "**System**" feature set pages shown below:

In System pages, there are some configuration pages for the system settings. These setups include Basic Settings, IP Settings, RADIUS Settings, Time Settings, Relay Settings and WLAN Traffic Shaping, these features are introduced in below pages.



4.2.1 Basic Settings

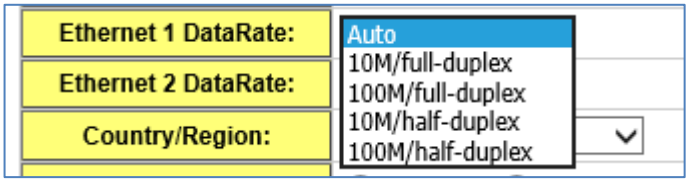
Use this page to configure the basic parameters of the device.

Device Name: User could give a name for identifying a particular access point here. It allows maximum 15 characters and no spaces.

NetWork Mode: There are 2 modes, Bridge and Route WLAN1 WAN modes. The default setting of JetWave 2212S/X is Bridge mode. It means only one UP address (LAN) interface is available.

Country/Region: Select the country you are installed. The channel number may be different based on your country.

Ethernet 1 Data Rate: Configure the Speed/Duplex of the WAN port. The default value, Auto means Auto-Negotiation. Force speed/duplex is available to setup here.



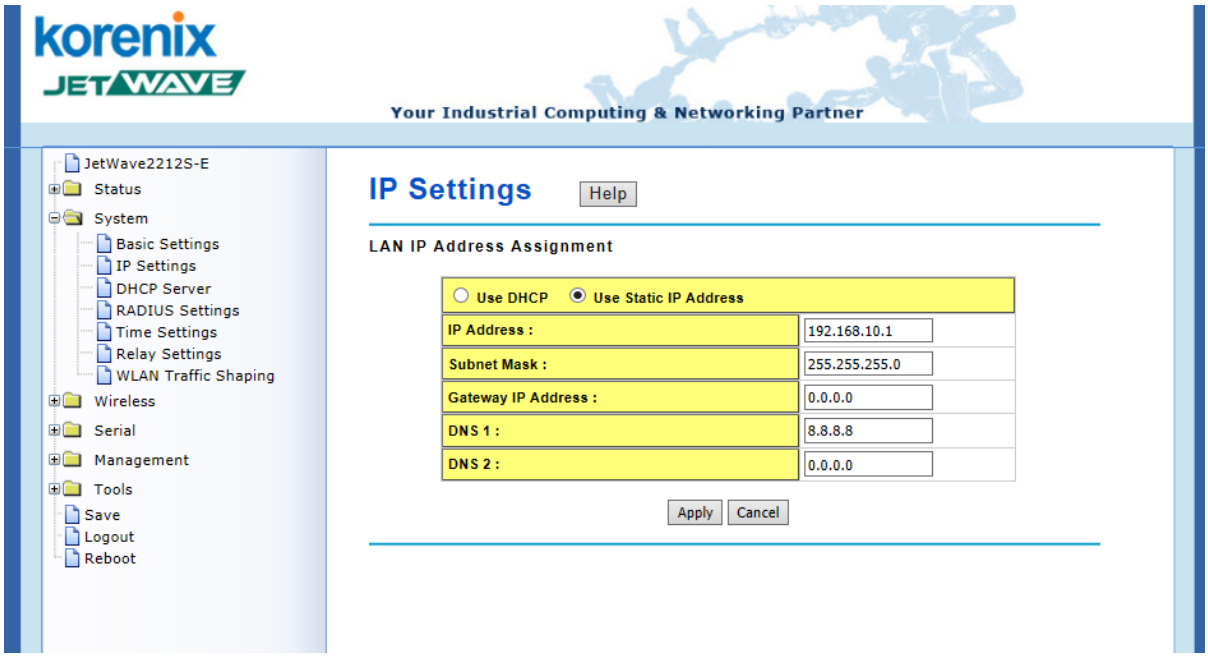
Ethernet 2 Data Rate: Configure the Speed/Duplex of the LAN port. The default value is Auto, it means Auto-Negotiation. Force speed/duplex is available to setup here.

802.1Q VLAN: Enable or Disable 802.1Q VLAN. With 802.1Q enabled, the packet will attach the 1Q VLAN tag inside. To assign the VLAN ID for each AP profile, you should enable 802.1Q VLAN first. Here is the global VLAN Enable setup.

Management VLAN ID: This is the management VLAN ID of the device. Only the client within the same management VLAN can access the device's management interface. To enable Management VLAN ID, you must enable "802.1Q VLAN" and assign "VLAN ID" for each AP profile first.

4.2.2 IP Settings

Use this page to configure the IP related parameters for LAN interfaces. Here you may change the setting for IP address, subnet mask, Gateway IP Address, DNS.



Use DHCP: User could give domain name system for the device.

Use Static IP address: .

IP Address: The IP Address field allows you to set the device's IP address manually.

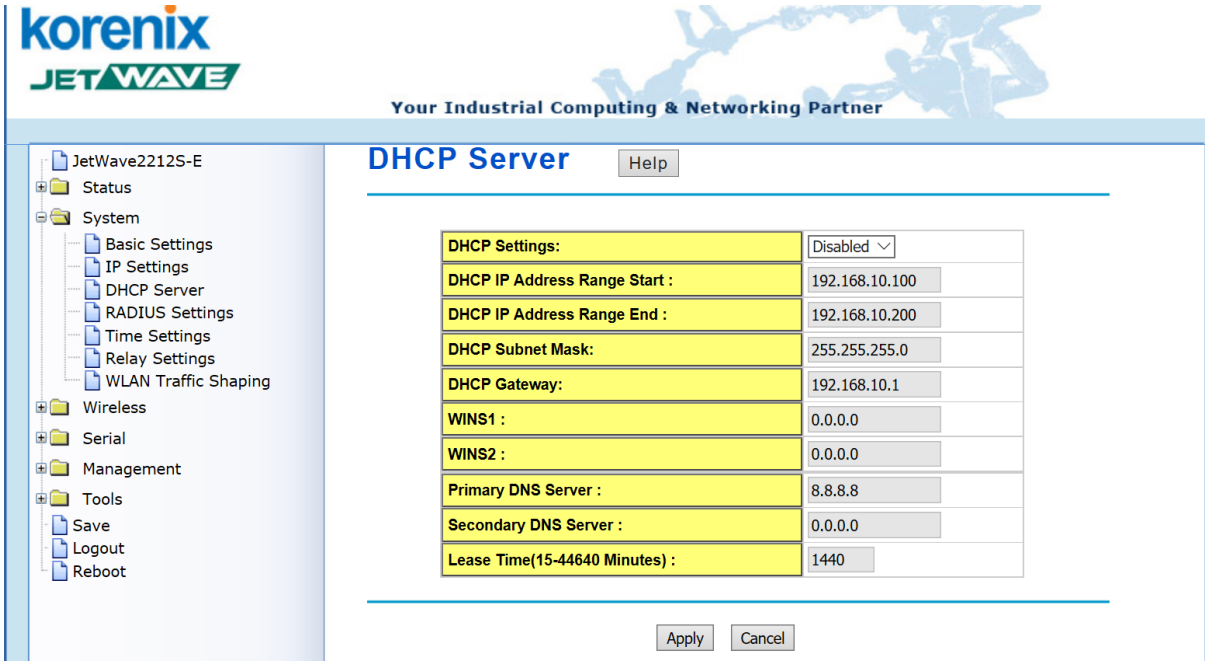
Subnet Mask: You can change the subnet mask address for the LAN interface. The default subnet mask is a Class C address: 255.255.255.0

Gateway IP Address: This is the system gateway IP address.

DNS: The DNS (Domain name system) servers for this device. DNS is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide

4.2.3 DHCP Server

Use this page to configure the **DHCP** Server Setting.



DHCP Settings: Enable / Disable the local DHCP Server. After the DHCP Server option is enabled, you can then assign the starting and ending IP of the DHCP IP address range. The device allows you to assign up to one Class C range which is 255 IP addresses. The maximum connections per session is 64.

DHCP IP Address Range Start: The starting address of the IP lease block.

DHCP IP Address Range End: The ending address of the IP lease block.

DHCP Subnet Mask: The subnet mask of the network.

DHCP Gateway: The default gateway IP address that you want the DHCP server to distribute.

WINS: The WINS server (NetBIOS name server) address that you want the DHCP server to distribute.

Primary/Secondary DNS Server: The DNS server address that you want the DHCP server to distribute.

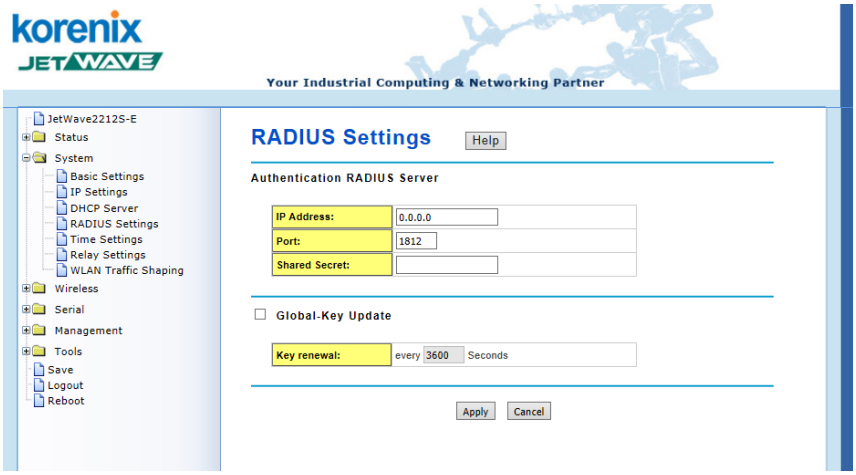
Lease Time: The time in minutes a DHCP lease is valid for.

Press "**Apply**" to activate the settings.

4.2.4 RADIUS Settings

Use this page to configure the **RADIUS** Server Setting.

RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; it plays a central role in the network in providing the capabilities of authenticating, authorizing, accounting, alarming and etc. It allows an organization to maintain user profiles in a central database that all remote servers can share.



Authentication RADIUS Server

IP Address: Enter the IP address of the Radius Server;

Port: Enter the TCP port number of the Radius Server; the default port number is 1812.

Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the device and RADIUS server during authentication.

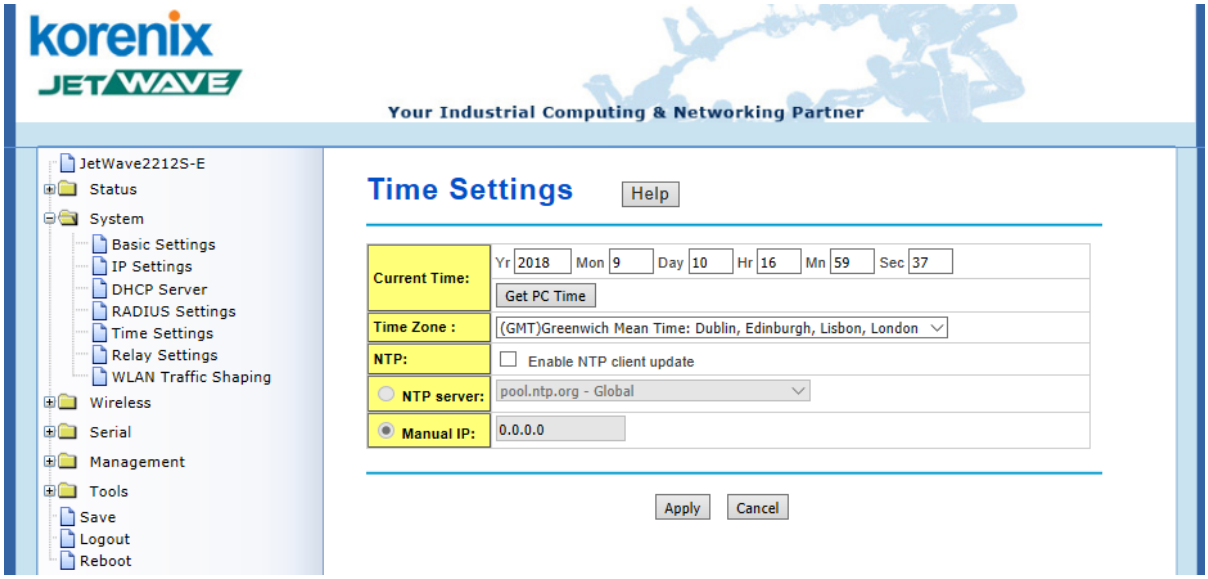
Global-Key Update: Check this option and specify the time interval between two global-key updates.

Key renewal: Set the time interval between two authentications.

For User Security, please go to Wireless Security Setting page (Refer to the chapter 4.4.2)

4.2.5 Time Settings

Use this page to configure the **Time Settings**. You can configure current time, time zone and configure NTP protocol to synchronize system time with a public time server over the internet.



Current Time: You can manually type the current time or get the time from you PC. Click **"Get PC time"**, the current time will be updated according to your PC's time.

Time Zone Select: Select the time zone of your country from the dropdown list.

NTP: You can select **"Enable NTP client update"** in this page, then the NTP feature will be activated and synchronize from the remote time server.

NTP Server: Select the time server from the "**NTP Server**" dropdown list or manually input the IP address of available time server into "**Manual IP**".

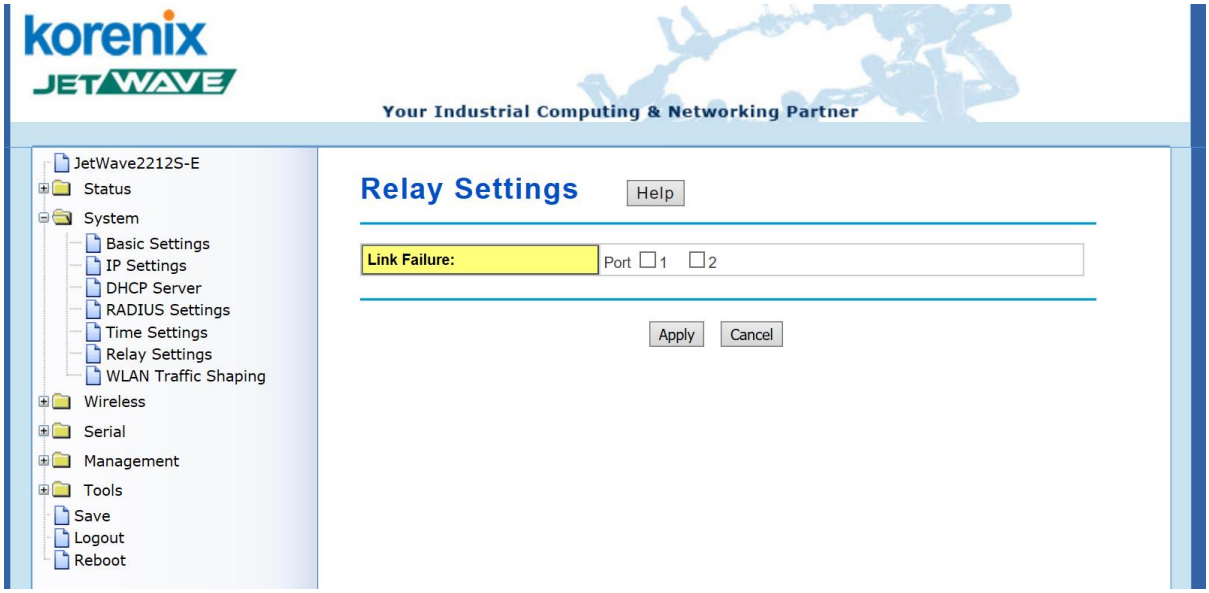
Press "**Apply**" to activate the settings.

4.2.6 Relay Setting

Use this page to configure the Link Failure Relay

Link Failure: You can Select the port number for which you want to monitor the link status. If a link failure occurs on the selected ports, the system relay is triggered

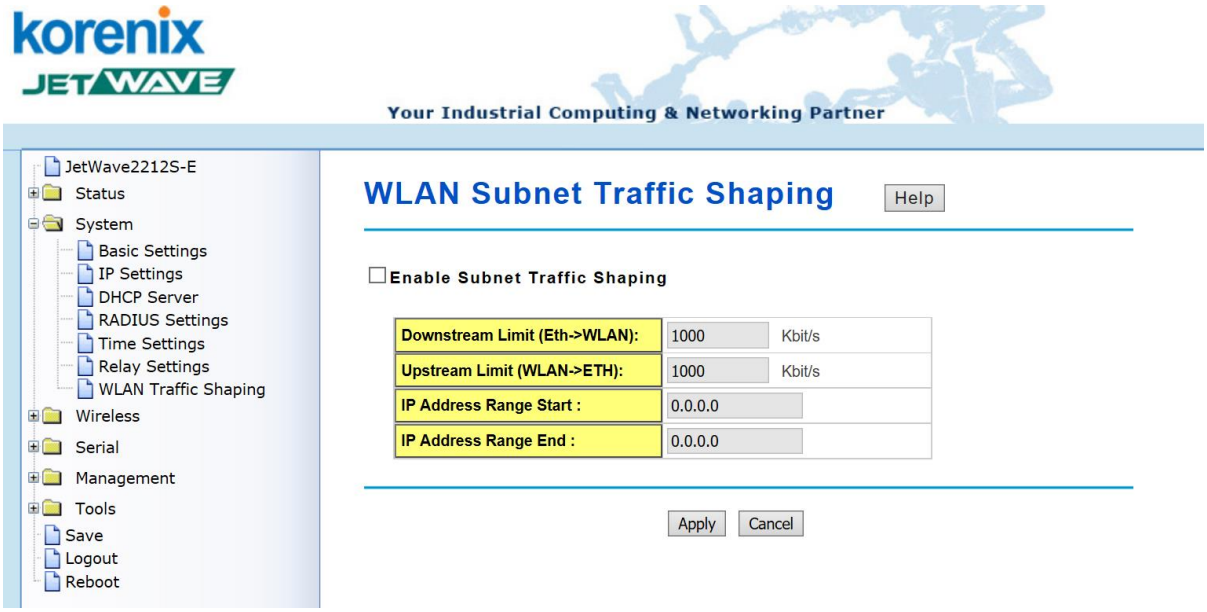
Press "**Apply**" to activate the settings.



4.2.7 WLAN Traffic shaping

Use this page to specify the IP based Downstream and Upstream traffic limit.

Note: Only class B,C network address support



Enable traffic shaping: Use this check box to enable or disable traffic shaping

Downstream Limit: Maximum Downstream rate guaranteed. The range is 1000 to 1024000.

Upstream limit: Maximum Upstream rate guaranteed. The range is 1000 to 1024000.

IP address Range start: The begin IP address to limit.

IP address Range End: The end IP address to limit

Press "**Apply**" to activate the settings.

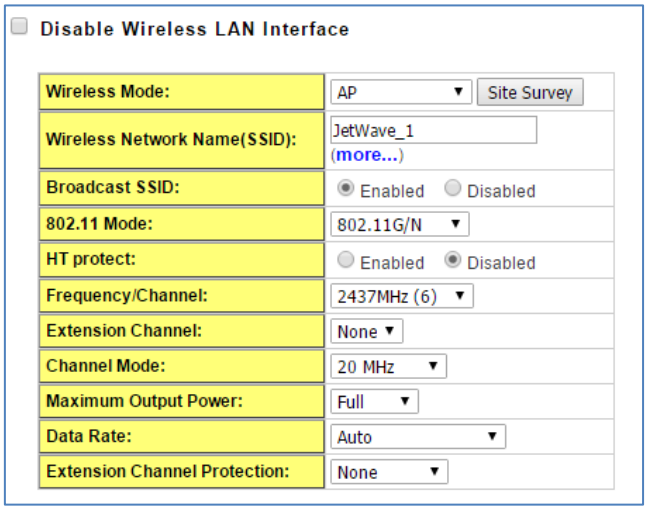
4.3 Wireless

The "**Wireless**" feature set pages allow users to configure the Wireless LAN configuration. The Wireless means the WIFI radio of the device. JetWave 2212S/X equip one-radio interface and it includes Basic Settings, Security Settings, Advanced Settings and Access Control can be configured in the WLAN Settings.

4.3.1 Basic Settings

Use this page to configure the parameters for Wireless LAN Interface of the device. Here you may change wireless interface modes and related parameters.

- **WLAN 1- Factory default setting**



Disable Wireless LAN Interface: Check this option to disable WLAN interface, then the wireless module of the AP will stop working and no wireless device can connect to it.

Wireless Mode: The below operating modes are available on JetWave 2212S/X series.

AP: The AP works as the Access Point mode, it establishes a wireless coverage and receives connectivity from other wireless client devices, the clients can search and connect to it. In Wireless AP mode, you can configure the Wireless Network Name (SSID), Enable/Disable Broadcast SSID, select the 802.11 mode, HT Protect Enabled/Disabled, Frequency/Channel, Extension Channel, Channel Mode, Maximum Output Power (per chain), Data Rate and Extension Channel Protection. When the Wireless Client connected to the AP, the client must follow AP settings for communicating.

Wireless Client: The JetWave 2212S/X is able to connect to the AP and thus join the wireless network around it. In Wireless Client mode, you can click "**Site Survey**" to find the best signal connected AP per your need. In Wireless Client mode, you can configure the Wireless Network Name (SSID) that you want to connect, 802.11 mode, Channel Mode, Maximum Output Power (per chain), Data Rate and Extension Channel Protection. While in wireless client, please note that all the rest of Wireless Client settings must be the same as your AP settings.

WDS-AP: WDS mode is usually implemented in Point to Point (P2P) connection. When configuring P2P, one end should be WDS-AP and the other end should be WDS-Client. WDS-AP can also provide network access to general clients to act as an AP repeater.

WDS-Client: In WDS-Client mode, you must type the target WDS-AP's SSID and MAC address. With the setting, the traffic from the WDS-Client can only transmit to the WDS-AP. Please note that the rest of other wireless/security settings must the same as the WDS-AP as well.

Wireless Network Name (SSID): This wireless network name is shared among all associated devices in your wireless network. Keep it identical on all those devices. Note that the SSID is case-sensitive and can not exceed 32 characters

Factory default SSID on WLAN 1: JetWave_1

Broadcast SSID: Enable or disable Broadcast SSID. Under AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the clients can not scan and find the AP, so that malicious attack by some illegal clients could be avoided.

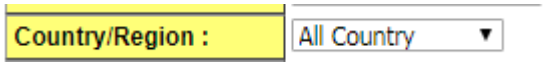
802.11 Mode: The AP can communicate with wireless devices of 802.11a/b/g/n. You can select 802.11 Mode and it will work under an appropriate wireless mode automatically. WLAN 1 support 2.4G band, and 5G band. Different band has different settings.

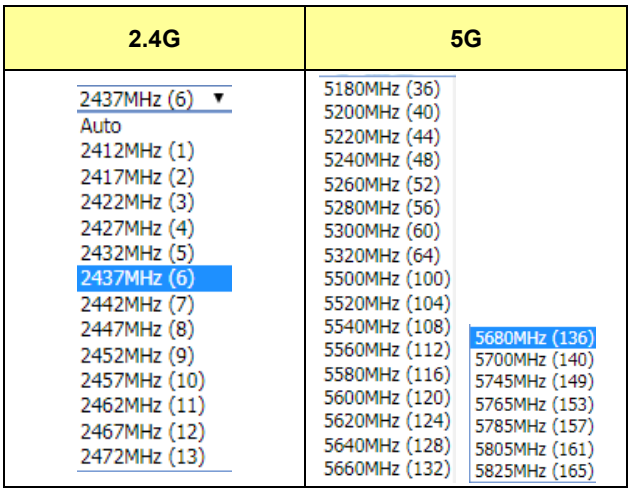
802.11 Supported Mode
WLAN 1
802.11A Only
802.11B Only
802.11G Only
802.11 G/N
802.11 A/N

HT Protect: Enable HT (High Throughput) Protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.

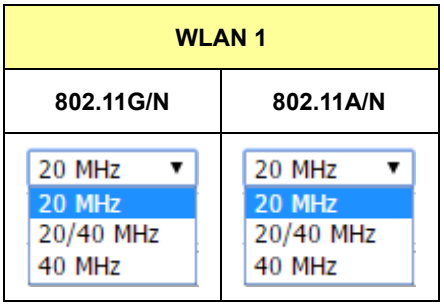
Frequency/Channel: Channel varies much as the available band differs from country to country.

Select a proper operating channel in the drop-down list according to your situation. By Our design, FCC support channel1~11,and CE support channel1~13 in 2.4G. In 5G, FCC support band1 and band4,and CE support only band1. And user will can choice the country code- All Country to open channel 1~13 in 2.4G,and band1~band4 channel in 5G.

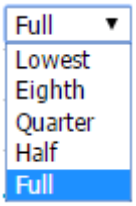




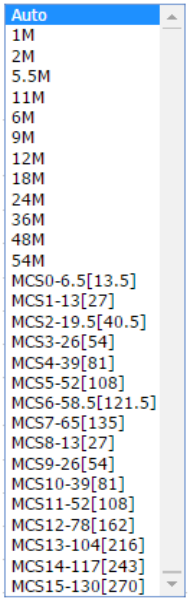
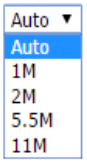
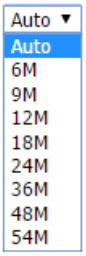
Channel Mode: Two levels are available: 20MHz and 20/40MHz. The latter one can enhance the data rate more effectively, but takes more bandwidth, thus cause potential interference.



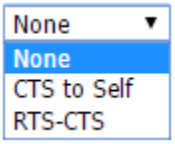
Maximum Output Power: Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly. Usually "**Full**" with proper antenna is preferred. **Half**: 1/2 of Full (Full -3dBm), **Quarter**: 1/4 of Full (Full -6dBm), **Eighth**: 1/8 of Full (Full –9dBm).



Date Rate: Usually “Auto” is preferred. Under this rate, the AP will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

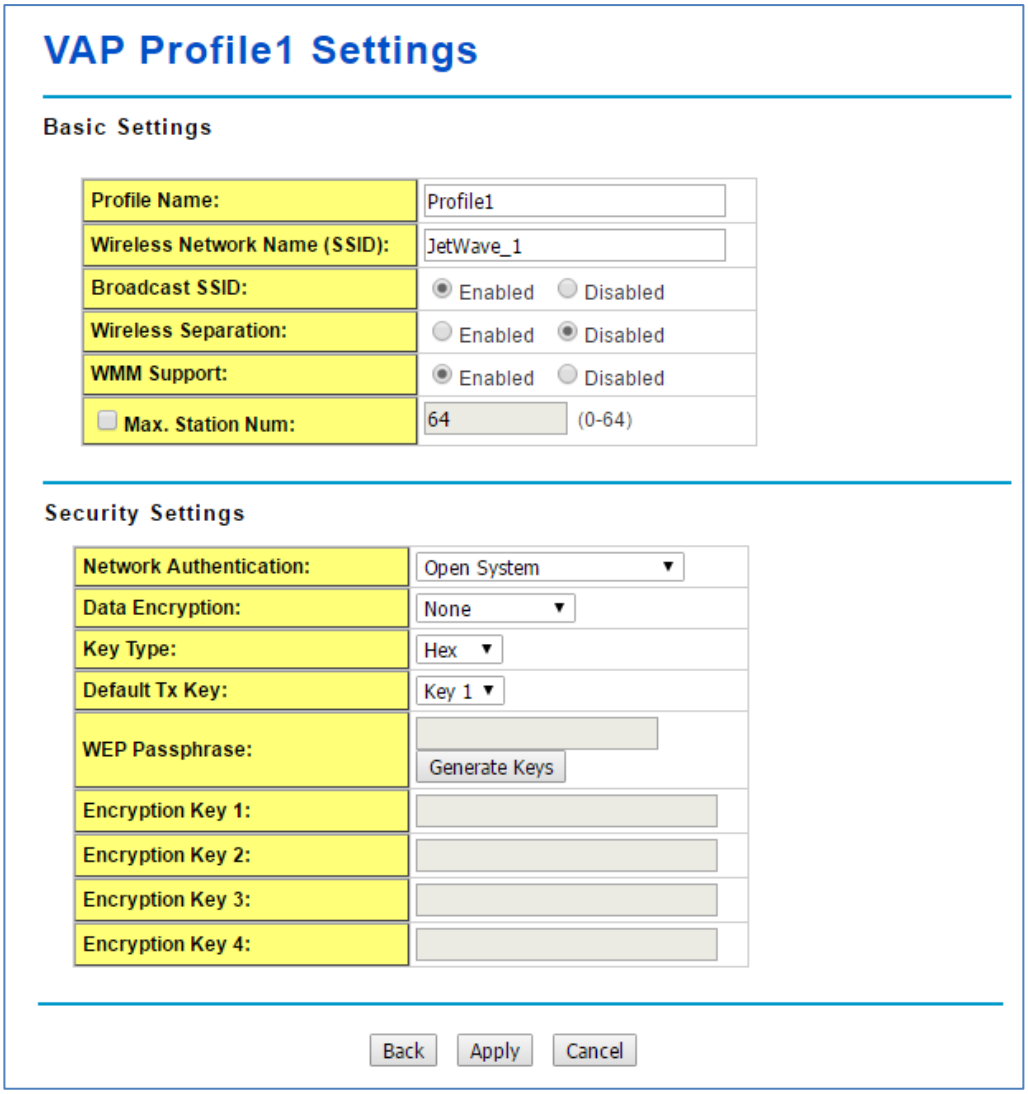
802.11G/N, 802.11A/N	802.11B Only	802.11G Only, 802.11A Only
		

Extension Channel Protection: This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to **CTS to Self**, the transmission amount of **RTS-CTS** is much lower. Press “**Apply**” to activate the settings.



4.3.2 Security Settings

The page allows you configure the Security Settings



➢ **Basic Settings**

Profile Name: The profile name of the settings.

Wireless Network Name(SSID): This is the same SSID of the AP.

Broadcast SSID: Normally, the SSID is broadcast and all the clients can search the SSID. For security concern, you can disable the Broadcast SSID function, then the clients can't search it and the client must type the correct AP's SSID to connect the AP. This is a simple security setting.

Wireless Separation: Wireless separation is an ideal way to enhance the security of network transmission. Under the AP mode, enable "Wireless Separation" can prevent the communication among associated wireless clients.

WMM Support: WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication

to define a priority limit on the basis of data type, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. In AP mode, you will have more settings as below.

Max. Station Num: In Wireless AP mode, you can define the maximum amount of wireless clients allowed to be connected. The maximum client of the system is 64. The most user access at the same time may cause system busy and the performance becomes lower. It is suggested to assign the value depends on how much bandwidth your client generally need, and totally bandwidth suggest is under 250Mbps for TCP based data transmission.

- **Security Settings**

Network Authentication: Select Network Authentication type.

Open System: It allows any device to join the network without performing any security check.

Shared Key: Data encryption and key are required for wireless authentication.

WPA with RADIUS: With warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. This is the common way to be adopted in large enterprise network.

WPA2 with RADIUS: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, AES encryption and RADIUS server is required.

WPA & WPA2 with RADIUS: If it is selected, AES & TKIP encryption and RADIUS server is required.

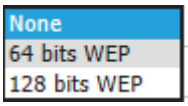
WPA-PSK: It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.

WPA2-PSK: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.

WPA-PSK & WPA2-PSK: If it is selected, the data encryption will be AES & TKIP and the passphrase is required.

Data Encryption: If data encryption is enabled, the key is required and only sharing the same key

with other wireless devices can the communication be established.



None: Available only when the authentication type is open system.

64 bits WEP: It is made up of 10 hexadecimal numbers.

128 bits WEP: It is made up of 26 hexadecimal numbers.

TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK

AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK.

EAP Type: For WPA/WPA2 with Radius. The system supports **TTLS**, **LEAP**, **TLS**, **PEAP** and **FAST Eap types.** Select the Eap type and type the User Name, Password for the WAP/WPA2 with Radius.

Group Key update Period: Time internal for rekeying GTK (Broadcast/multicast encryption keys) in seconds. This defaults to 86400 seconds (once per day) when using CCMP/GCMP as the group chpher and 0 seconds means no update

Press "**Apply**" to activate the settings, and you can also press "Back" to check the **VAP Profile Settings** for each Profile.

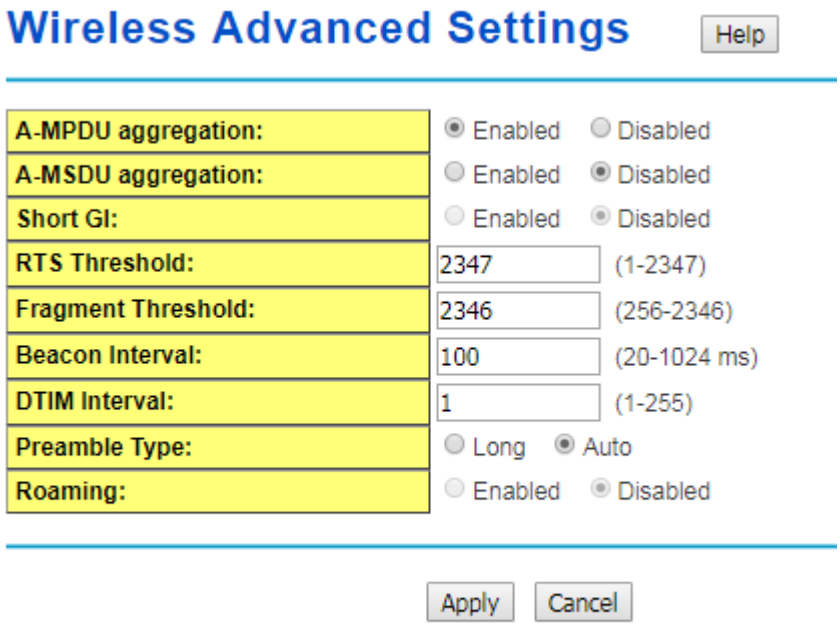
Note:

(1) We strongly recommend you enable wireless security on your network!

(2) Only setting the same Authentication, Data Encryption and Key in the JetWave and other associated wireless devices, can the communication be established!

4.3.3 Advanced Settings

The page allows you to configure advanced wireless setting. These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. **Some of these settings should not be changed unless you know what effect the changes will take. And some of the modification on them may negatively impact the performance of your wireless network.**



A-MPDU/A-MSDU Aggregation: Under AP mode, the data rate of your AP could be enhanced greatly with this option enabled; however, if your wireless clients don't support A-MPDU/A-MSDU aggregation, it is recommended not to enable it.

Short GI: Under 802.11n mode, enable it (Short Guard Interval) to obtain better data rate if there is no negative compatibility issue.

Short GI: Under 802.11n mode, enable it (Short Guard Interval) to obtain better data rate if there is no negative compatibility issue.

RTS Threshold: The AP/Gateway sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2347 in byte. The default value is 2347.

Fragment Threshold: Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

Beacon Interval: Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024. The default value is 100ms.

DTIM Interval: DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter

a value between 1 and 255.

Preamble Type: It defines some details on the 802.11 physical layer. "**Long**" and "**Auto**" are available.

Roaming: Under Client mode, STA will roaming to better AP if the RSSI of client is lower than setting of Roaming Threshold.

4.3.4 Access Control

This page allows you configure the Wireless Access Control list. You can configure Allow list or Deny list for your wireless network on the JetWave2212S/X.

Access Control Mode: Allow Listed or Deny Listed.

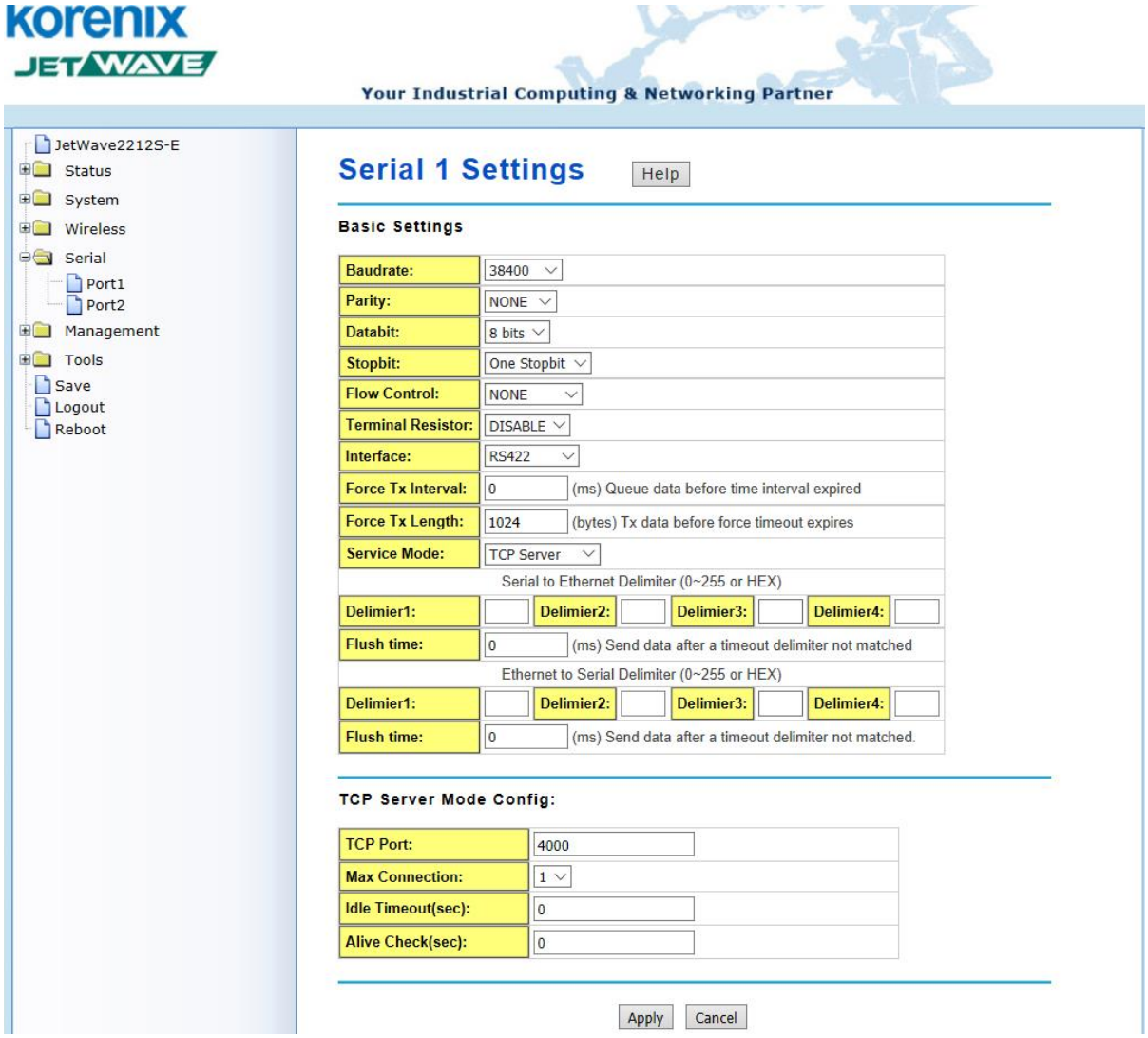
MAC Address: Type the MAC address of the client which you want to Allow or Deny.

Press "**Apply**" to activate the new settings.

The lower screen shows the Wireless Access Control list you configured. Press "**Delete Selected**" or '**Delete All**" to delete part of or all of the entries. Press "**Refresh**" to refresh the table.

4.4 Serial (JetWave 2212S ONLY)

JetWave 2212S is equipped with RS-232/422/485 3-in-1 serial port. It supports TCP Server/Client and UDP for remote connection. This page could configure the Serial interface's parameters.



➢ **Basic Settings**

Serial port settings: Select the **Baudrate, Parity**, **Databit, Stopbit Flow Control** and **Flow Control** settings from the dropdown list.

Interface: Manually choose and change the interface type. The serial port supports the **RS232**, **RS422**, **RS485-2w** and **RS485-4w**

TX Internal: Configure the Tx Internal time, the system will queue the transmit data before time interval expired. The time unit is millisecond.

Tx Length: Configure the Tx length, the system will queue the transmit data before time force

timeout expired

Service Mode: Select **TCP Server**, **TCP Client**, and **UDP Listening** from the dropdown list.

Serial to Ethernet/Ethernet to Serial Delimiter: Configure the **Delimiter** and **Flush time** (a timeout that the delimiter not matched) setting for Serial to Ethernet or Ethernet to Serial transmission. There are up to 4 delimiters and be configured here. After the Delimiter is configured, the data will be stored in the buffer until hit the Delimiter or the Flush time timeout. After the Delimiter is configured, the data will be stored in the buffer until hit the Delimiter or the Flush time timeout

- **TCP server Mode Cnofig:**

In TCP server mode, the serial port on the JetWave 2212S is assigned a port number which must not conflict with any other serial port on the JetWave 2212S. The host computer initiates contact with the JetWave 2212S, establishes the connection, This operation mode also supports up to 5 simultaneous connections, enabling multiple hosts to collect data from the same serial device at the same time. and receives data from the serial device.

TCP port: Select the TCP server listening port (4002 by defaylt),

Max Connection: Specific the maximum number of connections that will be accepted by the serial port.

Idle Timeout(sec): configure a service with a timeout value to terminate any idle server connections when the configured time (in seconds) elapses. If the server is idle for the configured amount of time, the JetWave 2212S closes the server connection.

Active Check (sec): Configure how long the JetWave 2212S will wait for a pesponse to " keep alive" packets before closing the TCP connection. JetWave 2212S checks connection status by setting periodic "keep alive" packets.

4.5 Management

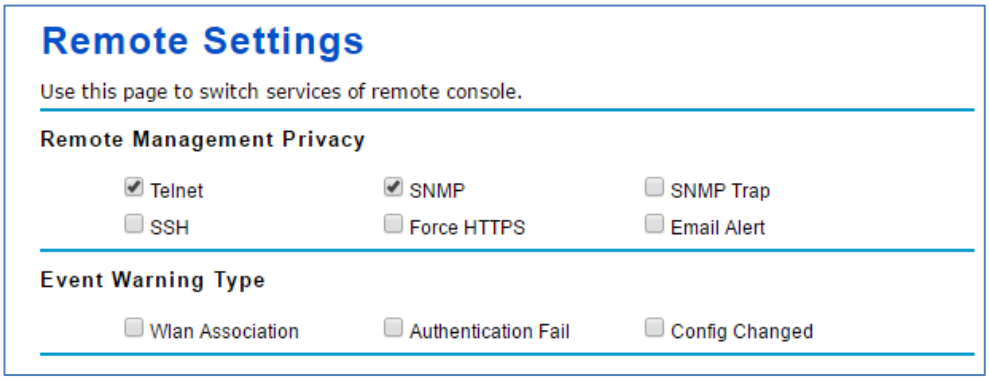
The "**Management**" feature set pages allow users to configure the Remote Setting, SMTP Configuration, Login Settings, Firmware Update, Configuration File, Certification File, Controller, Remote IP Scan and Topology Discovery.

4.5.1 Remote Setting

Use this page to set the Remote Management Privacy with selected Event Warning Type.

And this page also includes the configuration of SNMP settings V2c and V3.

Please make sure the configuration of SNMP should match between the device and SNMP server.



➢ **Remote Settings**

Remote Management Privacy: You can select which kinds of remote service should be opened in your environment. The services include **Telnet, SNMP, SNMP Trap, SSH, Force HTTPS** and **Email Alert.** Select the service and press "**Apply**" to activate the settings.

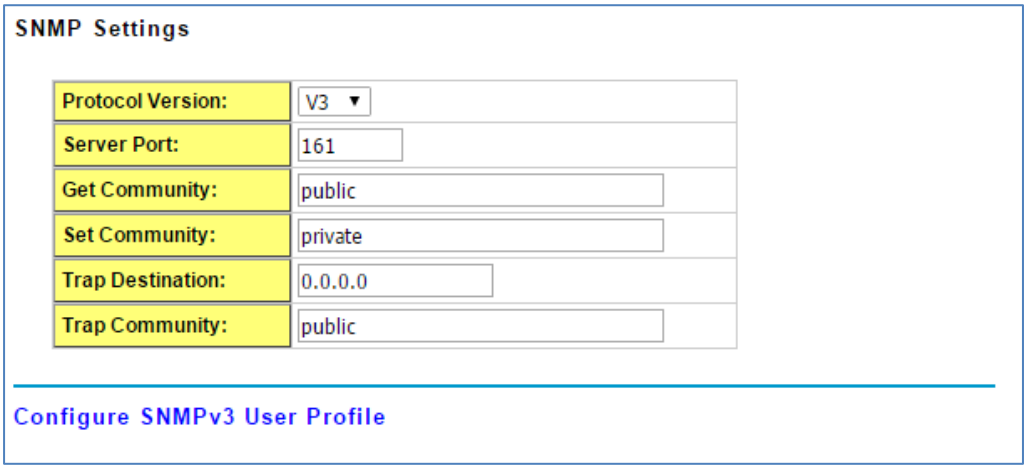
Event Warning Type: The event warning type selection.

Wlan Association: The client associated to the AP event.

Authentication Fail: The client failure of authentication event.

Config Changed: The configuration of the AP/Gateway is changed event.

➢ **SNMP Settings**



Protocol Version: Select the SNMP version, and keep it identical on the device and the SNMP manager. While you chose SNMPv3 and applied, you must configure the SNMPv3 User Name, Password and their Access type, Authentication and Privacy Protocol in below SNMPv3 User Profile.

Server Port: Change the server port for a service if needed; however you have to use the same port to use that service for remote management.

Get Community: Specify the password for the incoming Get and GetNext requests from the management station. By default, it is set to public and allows all requests.

Set Community: Specify the password for the incoming Set requests from the management station. By default, it is set to private.

Trap Destination: Specify the IP address of the station to send the SNMP traps to.

Trap Community: Specify the password sent with each trap to the manager. By default, it is set to public and allows all requests.

Note:

For security concern, it is recommended change the Community Name before you connect the AP to the network. The experience engineer who familiar with SNMP protocol can easily discovery and change the configuration of the AP/Gateway through SNMP once you use the default communication name.

4.5.2 SMTP Configuration

The AP supports E-mail Warning feature. The AP will send the occurred events to remote E-mail

server. The receiver can then receive notification by E-mail. The E-mail warning is conformed to SMTP standard. This page allows you to enable E-mail Alert, assign the SMTP Server IP, Sender E-mail, and Receiver E-mail. If SMTP server requests you to authorize first, you can also set up the username and password in this page.

SMTP Server IP: The IP Address of the SMTP server.

E-mail Account: The Sender's Email Account.

Authentication Protocol: If the SMTP server requires authentication, select the Authentication Protocol and enter User Name and Password.

User Name: The User Name of the sender E-mail account.

Password: The password of the Sender e-mail account.

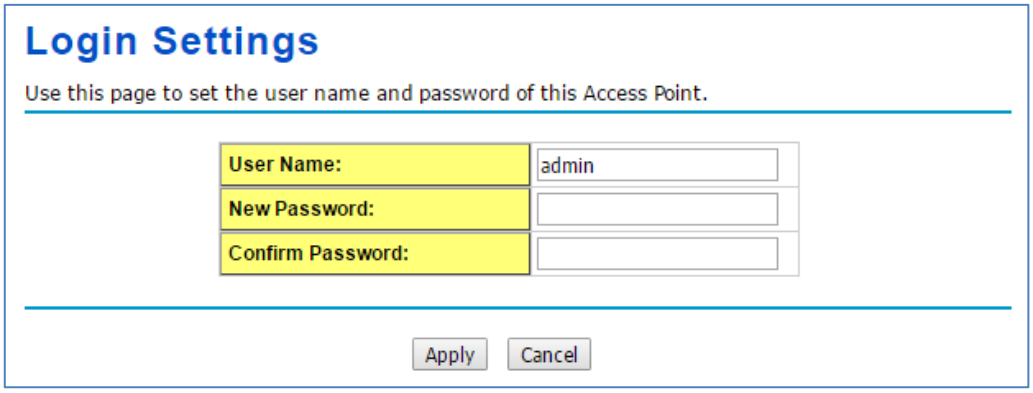
Rcpt Email Address: The Receiver's e-mail address.

Press **"Apply"** to activate the change.

4.5.3 Login Settings

Use this page to set the user name and password of the AP. Type the **User Name**, **New Password** and **Confirm Password** again.

Press **"Apply"** to activate the new password.

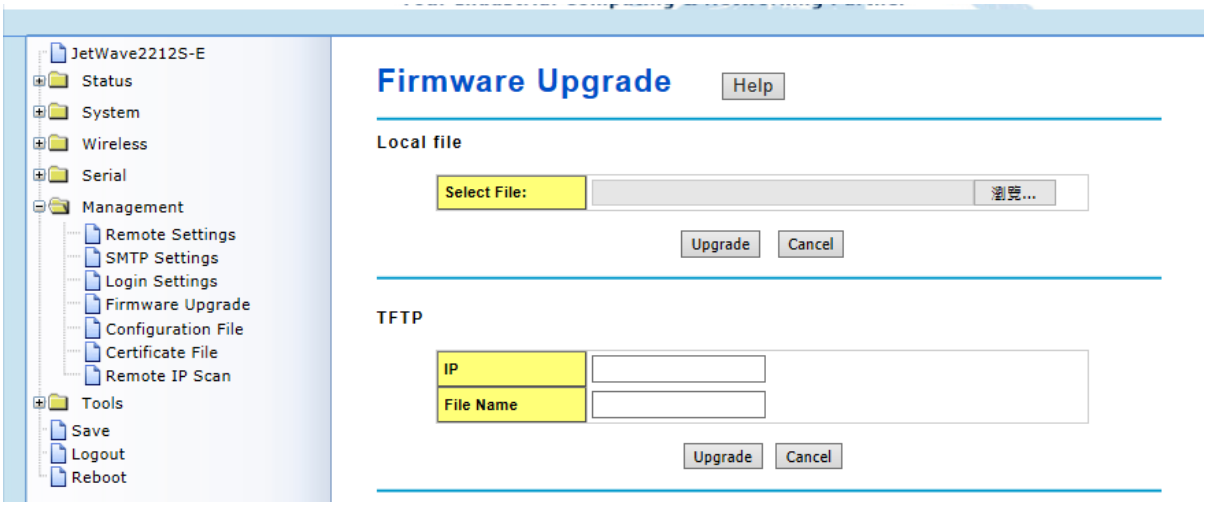


4.5.4 Firmware Upgrade

In this section, you can update the latest firmware for your AP. Korenix provides the latest firmware in Korenix Web site. The new firmware may include new features, bug fixes or other software changes. We'll also provide the release notes for the update as well. From technical viewpoint, we suggest you use the latest firmware before installing the AP to the customer site.

Note: The system will be automatically rebooted after you finished upgrading new firmware. Please

remind the attached users before you do this.



➢ **Local File:**

Type the path of the firmware in **Select File** field, or click "**Browse…**" to browse the firmware file.

Press "**Upgrade**" to upload the firmware file to the AP. After finishing transmitting the firmware, the system will copy the firmware file and replace the firmware in the flash.

➢ **TFTP :**

IP: Thisis the IP address of the TFTP server where the firmware image resides.

File Name: This is the file name of the firmware image.

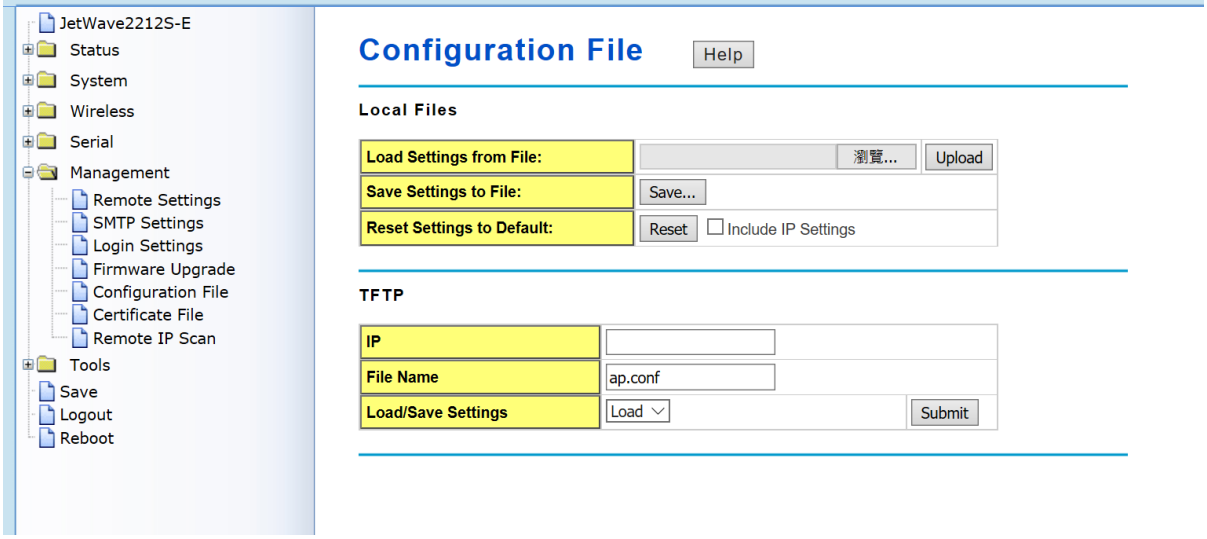
Press **"Upgrade"** to activate the new password

Press **"Cancel"** to clear the entered IP address and firmware file name.

After the firmware has upgraded, the device reboots automatically.

4.5.5 Configuration File

In this Page, you can backup and restore a system configuration file by two methods, local file or TFTP server.



➢ **Local File:**

Local setting from file: Click "**Browse…**" to select the previously saved backup configuration file.

After locating the configuration file, click "**Upload** :button

Save setting to file: Click the" **Save"** button to save the configuration file.

Reset setting to Default: Click the**" Reset"** button to reset all the configuration settings, but not the default IP address to default settings unless you select the **Include IP setting** option when you click the Reset Button.

➢ **TFTP :**

IP: This is the IP address of the TFTP server where your configuration file has been previously saved or can be saved.

File Name: This is the file name of the configuration file to be saved.

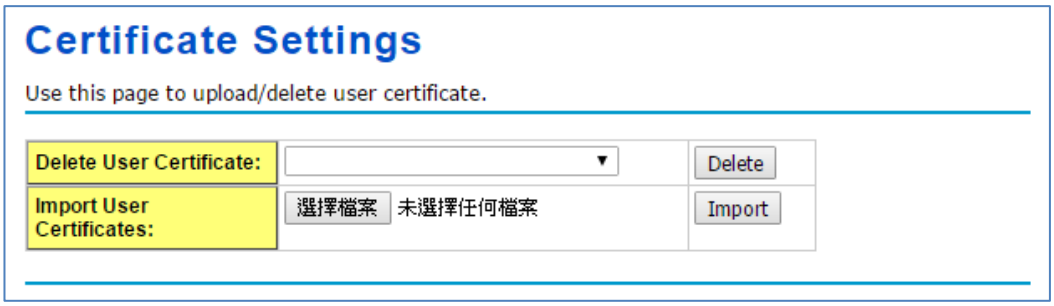
Locad/Save Settings:

Select the **"Load"** option to load the configuration from the TFTP server onto the router.

Select the **"Save"** option to save the configuration on the router to the TFTP server.

4.5.6 Certificate File

Use this page to manage the user certificate file. You can import user certificate file, select "**Browse…**" to select the certificate file and press "**Import**". You can generate the file by 3rd party tool, web site or get from the IT administrator. Select the user certificate, and then use the **Delete** to remove it.



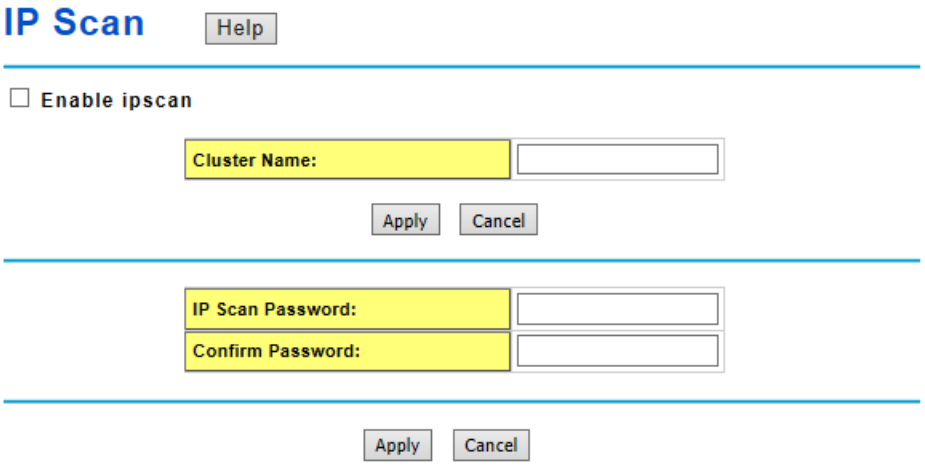
In **Wireless/Security Settings**, following is the security setting under "**WPA with Radius**" Authentication mode, the Eap type is **"TLS"**. You can see the "User Certificate file" is assigned. The AP must use the same certificate file as your Radius Server under this setting.

4.5.7 Remote IP Scan

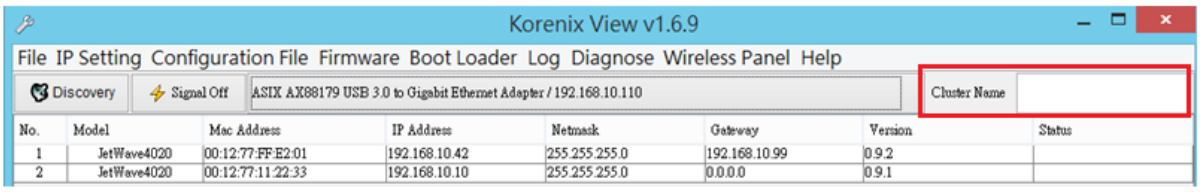
The page allow user to set remote IP Scan, it include **Cluster Name** and **IP Scan Password.** With **Remote IP Scan,** it provide higher wireless security when use Korenix View management tool.

Note: Must use Korenix View V1.6.9 or higher version

After set **Cluster Name**, Korenix View will not list JetWave device in Model filed unless user type the same Cluster name at Korenix View interface.



If set **Cluster Name** with **Password**, Korenix View will not list JetWave device in Model filed unless user type the same Cluster name at Korenix View interface, if user already type the same Cluster Name at Korenix View, it will list JetWave device but need to key in password if user want to modify configuration, such as Reboot, Load factory default, Change Cluster Name and Wireless panel settings.

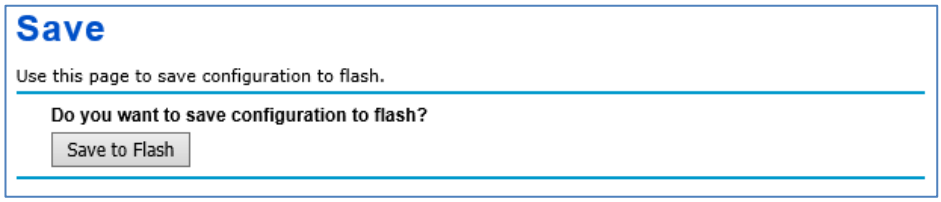


4.6 Tools

The tools provides the system tools, for example: Save the configuration, Logout and Reboot the system.

4.6.1 Save

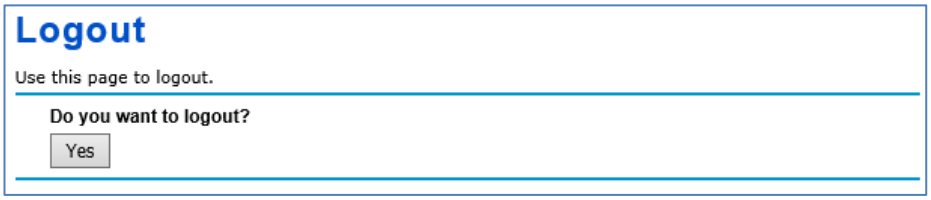
Use this page to save configuration to flash. Every time while you finished the configuring the device, please remember to save the configuration to flash. Otherwise, the configuration will lost after reboot the system.



Press "**Save to Flash**" to save the configuration to flash.

4.6.2 Logout

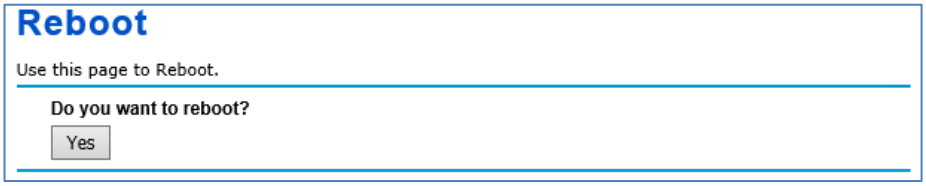
After finished configuring and leave, please remember to Logout the system. Without Logout the system, the login session will not timeout for couple minutes, it is a risk that other user may login your system without password checking before timeout. Another affect is that the user can NOT access at the same time if someone already login the system.



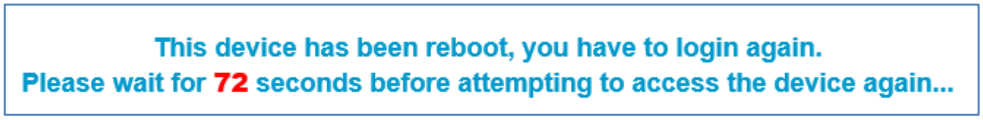
Use this page to logout. Press "**Yes**" to logout.

4.6.3 Reboot

Use this page to reboot the system. Press "**Yes**" to reboot system.

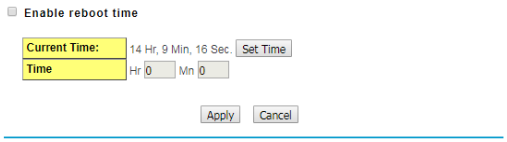


The below warming message will appear after you reboot the system.



- **Enable reboot time:**

Enable the reboot time and set the Time, when the Current Time ran to the value that you set, the system will reboot the device automatically. Press Apply to activate the settings.



Chapter 5

Configuration – SNMP, CLI, View Utility

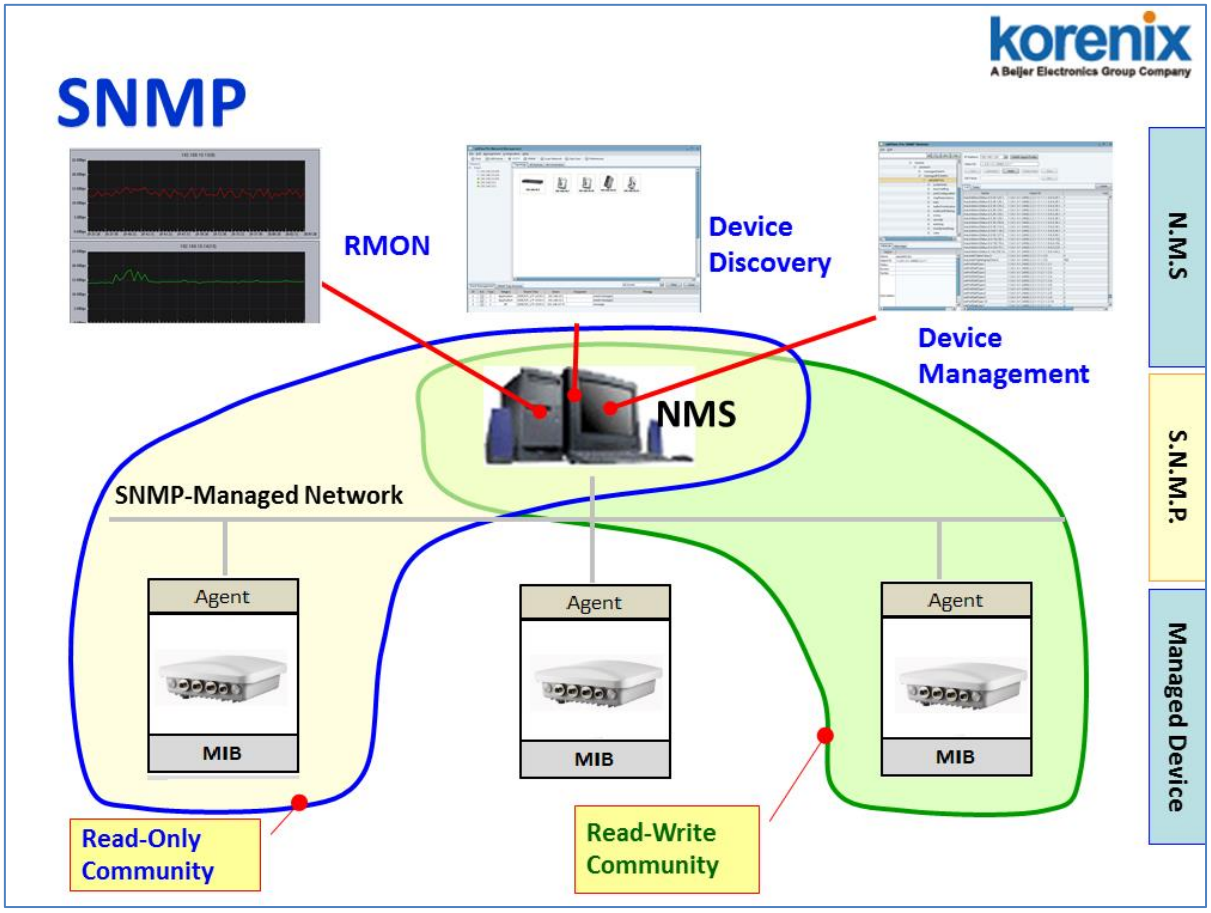
Chapter 5 Configuration – SNMP, CLI, View Utility

5.1 SNMP

5.1.1 What is SNMP?

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. This product series supports SNMP v1, v2c and V3.

Typical SNMP Architecture:



An SNMP managed network consists of two main components: Agent of the Managed Device and Manager (Network Management System, NMS).

Agent of the Managed Device: An agent is a management software module that resides in AP. An agent translates the local management information (Management Information Base, MIB) from the managed device into a SNMP compatible format. In MIB, all the status and settings of the

AP/Gateway has its own specific object ID (OID), the manager can read or write the value of the OID.

Manager (Network Management System, NMS): The manager is the console through the network. Network Management System (NMS) is the typical management system to manage the SNMP compatible devices. It normally provides device discovery, management, remote monitoring on network (RMON), trap server…etc.

Community:

The community is similar to the password of SNMP, while the manager wants to manage the target device, they must have the same community name. The community includes 2 privileges, Read Only and Read and Write. With Read Only privilege, you only have the ability to read the values of MIB tables. Default community string is Public. With Read and Write privilege, you have the ability to read and set the values of MIB tables. Default community string is Private.

SNMP Setup:

Please refer to the **4.6.1 Remote Setting.**

5.1.2 Management Information Base (MIB):

Before you want to manage the JetWave 2212S/X AP through SNMP, please go to download the MIB files from Korenix web site and compile all of them to the NMS. The AP supports function based MIB, the same function/parameters in all the models have the same object ID (OID). The benefit is you just need to compile the MIB file one time even you purchase different models. While you purchase our new released models in the future, the MIB file can be applied as well. Once we provide new features for the MIB, you just need one time effort to update the MIB table for all the models.

There are some MIB files which are:

a. JETWAVE-ACL-MIB.my: This is the JetWave ACL object MIB.

b. JETWAVE-DEVICE-MIB.my: This is the JetWave Device Management object MIB.

c. JETWAVE-EVENT-MIB.my: This is the JetWave Event/Trap MIB.

d. JETWAVE-ROOT-MIB.my: This is the JetWave top level object MIB.

e. JETWAVE-STATISTICS-MIB.my: This is the JetWave Serial Port object MIB.

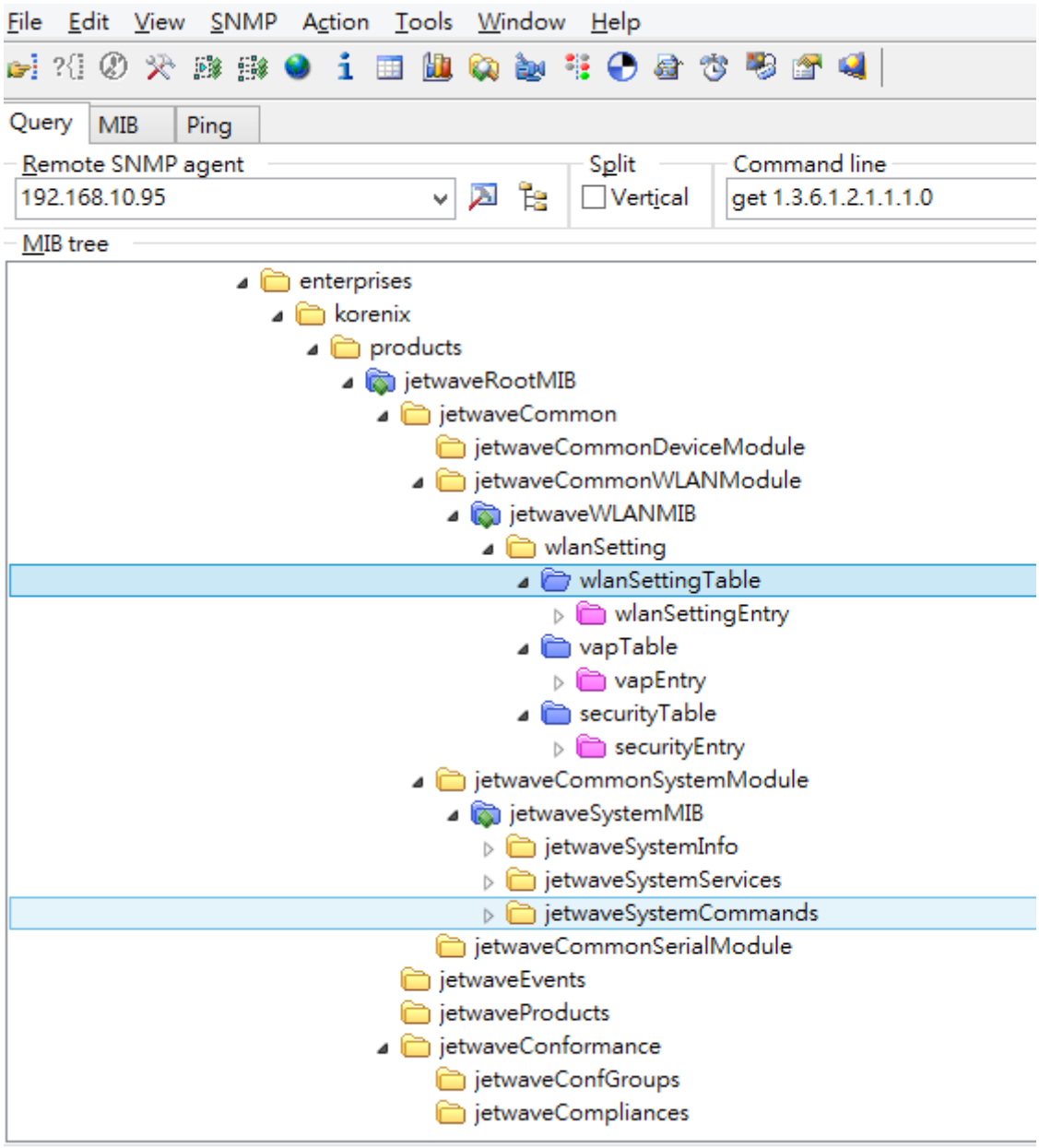
f. JETWAVE-SYSTEM-MIB.my: This is the JetWave System objects MIB.

g. JETWAVE-WLAN-MIB.my: This is the JetWave Wireless LAN Setting object MIB.

(Please download the latest MIB file from Korenix web site.)

5.1.3 MIB Tree in NMS

.The below figure shows the MIB tree after compiled in the NMS.



Example: wlanSetting **wlanSettingEntry:**

- wlanSettingTable
  - wlanSettingEntry
- vapTable
  - vapEntry
- securityTable
  - securityEntry
- associationListTable
  - associationListEntry

- wlanSettingEntry
  - operatemode
  - wirelessmode
  - radioEnable
  - ssid
  - hidenetworkname
  - frequency
  - datarate
  - beaconinterval
  - rtsthreshold
  - fraglength
  - dtiminterval
  - preamble
  - txpower
  - htprotect
  - channelmode
  - channeloffset
  - extchprote
  - shortgi
  - ampdu
  - amsdu
  - igmp
  - wmmSupport
  - wlanseparator
  - rifs
  - lintegration
  - maxStaNum
  - maxStaNumLimit
  - spaceinmeter
  - antennaNum
  - wdsAPMacAddress
  - wifiRedundancyPrimaryInterface
  - wifiRedundancyThreshold
  - roamingEnable
  - roamingThreshold
  - roamingDiff
  - roamingScanChannel1
  - roamingScanChannel2
  - roamingScanChannel3
  - autoOffloadEnable
  - offloadLowerSignal
  - offloadUpperSignal
  - onetimeOffloadEnable
  - offloadReconnectWIFI
  - offloadActivePath

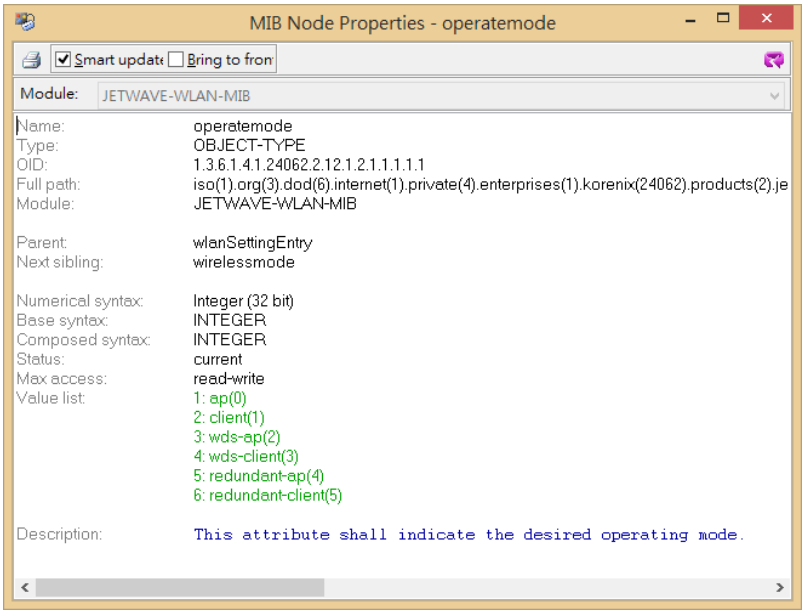
Example of Object in wlanSettingEntry

Operatemode: (Operation Mode)

The OID: .1.3.6.1.4.1.24062.2.12.1.2.1.1.1.1.1.

Max Access: read-write (Read and Write)

Value list: you can read the value or set a new value according to the value list. This is the same as web GUI and CLI.



Select the OID and press the Right key of the mouse. You can see the tool set to read or write new value.

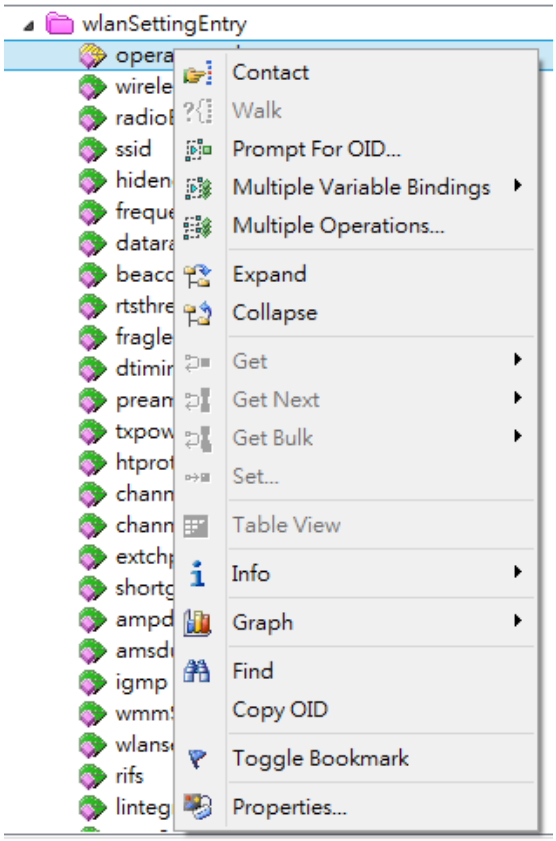
Get: Read the value of the selected OID.

GetNext: Read the value of the next OID.

GetBulk: Read the value of the next 10 OID.

Set: Set new value for the selected OID.

Property: See the MIB Node information.



5.2 Command Line Interface (CLI)

The AP provides the Command Line Interface (CLI), you can access it through the Telnet or Console. The Command Line Interface (CLI) is the user interface to the AP's embedded software system. You can view the system information, show the status, configure the switch and receive a response back from the system by keying in a command.

The below screen is the login screen of the AP. The default username/password is admin/admin, it is the same as Web GUI. Once you modified it from other configuration interface, please type the new name/password to login.

There are some different command sets. Each command sets has its own access ability and available command lines. These command sets are:

SHOW: This is Read Only command to show the current setting and status of the AP/Gateway.

SET: This is Write command to change the current setting.

LIST: This is Help command to show the usage information of the command.

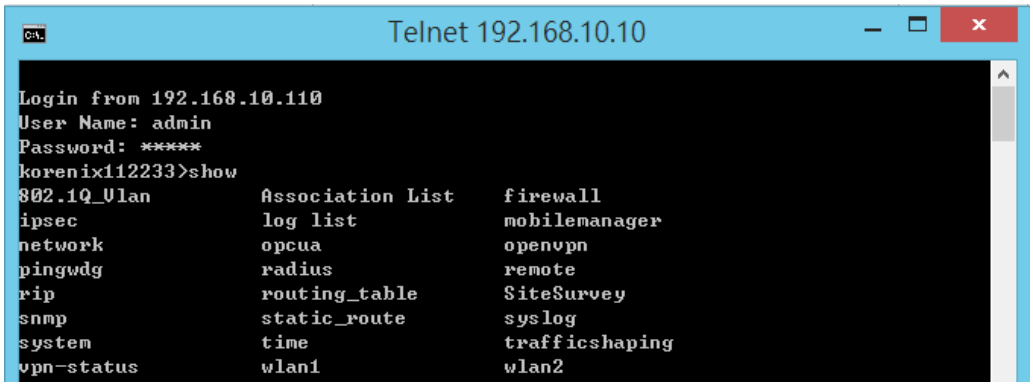
Del: This is Delete command to delete the applied settings.

Exit: To exit the CLI. It is logout command.

Note: Use **"Tab⇆"** key can help you find the correct command and complete the command no matter you want to Read or Write easier.

5.2.1 SHOW Command Set:

Type **Show** + **"Tab⇆"** to see all the show command sets. The following command lines are available.



Type **show wlan1** + **"Enter"** to see all the wlan information. The console print all the information for reference.

Type show **wlan1 ra + "Tab"** to complete the commands, and then you can see the result.

korenixffffff>show wlan1 ra (+Tab)

radio rate

korenixffffff>show wlan1 rad (+Tab)

radio rate

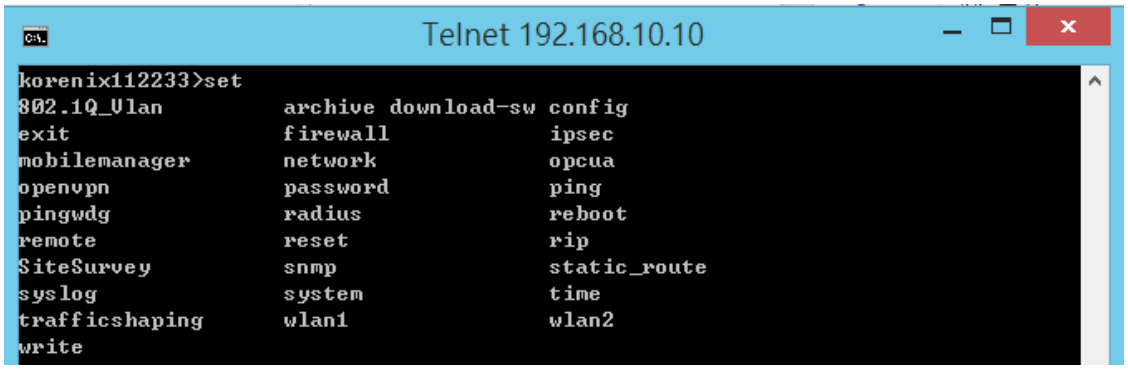
korenixffffff>show wlan1 radio (+ Enter)

wlan1 radio : Enabled (This is the result.)

Please check the List command set to know the usage of all commands.

5.2.2 Set Command Set:

Type **Set** + **"Tab⇆"** to see all the write command sets. The following command lines are available.

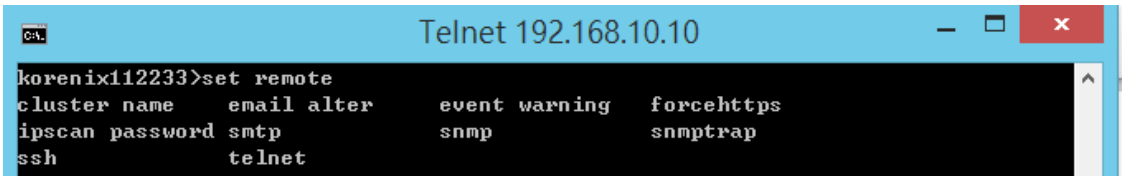


The most Set comment lines have the same functionality as the the Web GUI configuration we

introduce in chapter 4. Please read chapter 4 to know all the features our AP supported. And the CLI is a different way for you to complete the setting.

Example: Set the remote configuration (Refer to the 4.6.1 – Remote Setting)

Type **set remote + "Tab⇆"** to see all the remote settings.



Example: SNMP Enable/Disable:

```
korenixffffff>set remote snmp
Disabled      Enabled
korenixffffff>set remote snmp Disabled
remote snmp                    : Disabled
korenixffffff>set remote snmp Enabled
remote snmp                    : Enabled
korenixffffff>
```

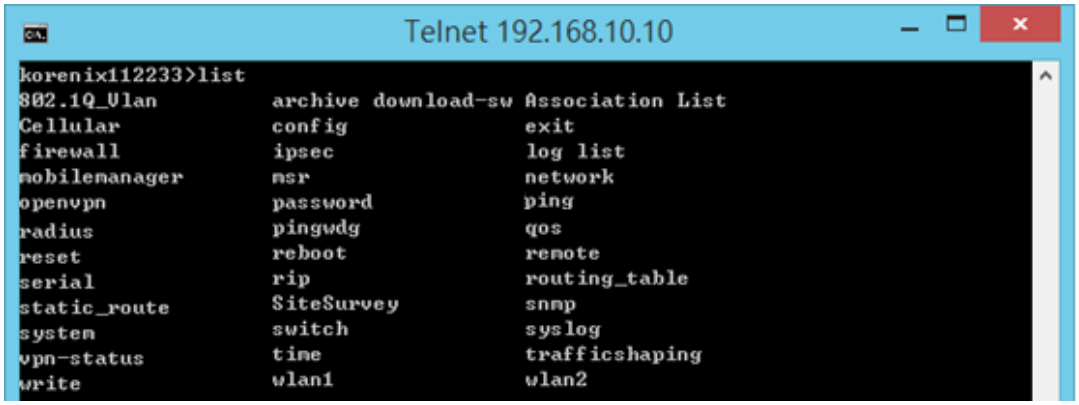
====SNMP Setting=========

The SNMP command lines and how to set SNMP version, community name, trap server.

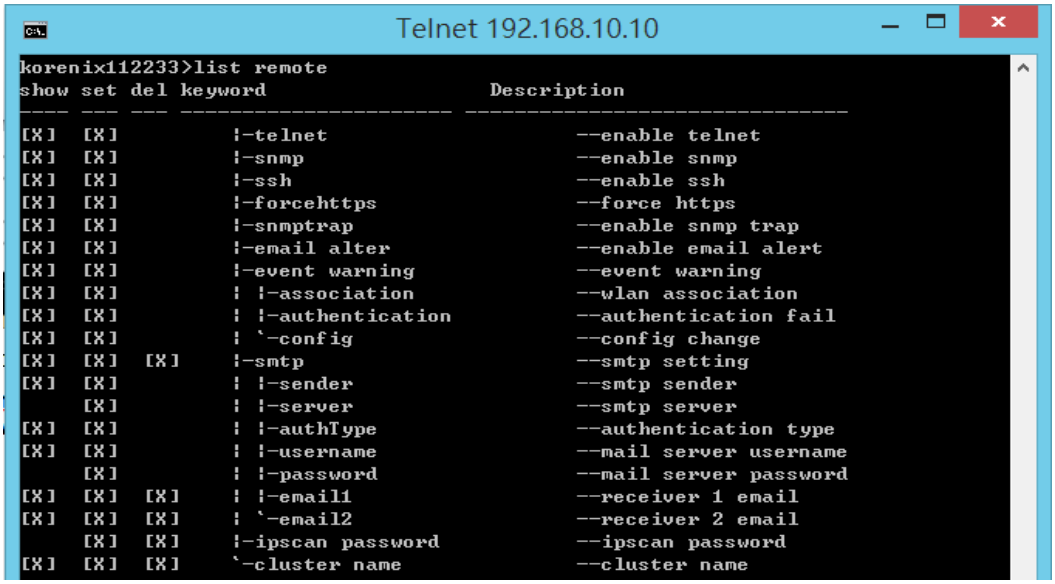
```
korenixffffff>set snmp (+Tab)
getCommunity      port              setCommunity      trapcommunity
trapdestination v3Admin             v3User            version

korenixffffff>set snmp version V2
snmp version                   : V2

korenixffffff>set snmp getCommunity orwell
snmp getCommunity              : orwell

korenixffffff>set snmp setCommunity orwell
snmp setCommunity              : orwell

korenixffffff>set snmp trapdestination 192.168.10.95
snmp trapdestination           : 192.168.10.95

korenixffffff>set snmp trapcommunity orwell
snmp trapcommunity             : orwell
```

5.2.3 List Command Set:

Type **List + "Tab⇆"** to see all the command usage. This is similar to the Help command.



Below command is to list the remote configuration command line and its description.



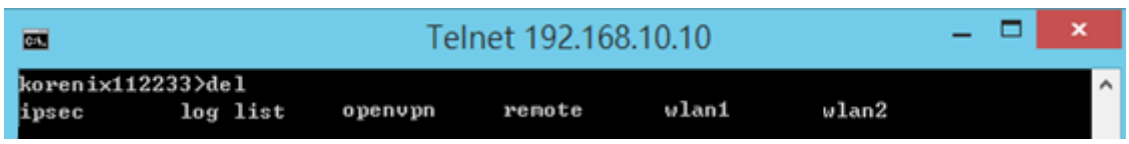
show, set and del: Which privilege the command has? [X] means Yes.

Keyword: The command you should enter in the CLI.

Description: Short description of the usage of the command.

5.2.4 Delete Command Set:

Type **del + "Tab⇆"** to see all the delete command sets. The following command lines are available.



The log list can be delete through CLI.

korenixffffff>del log list

The configured smtp email addresses can be delete through CLI.

korenixffffff>del remote smtp

email1 email2

The below wlan 1 settings can be delete through CLI. (JetWave 2212S/X 1st Radio)

korenixffffff>del wlan1

acl eap key wpa

5.3 Korenix View Utility

The Korenix View Utility (Rename from the JetView) provides you convenient tool to scan the network and configure the AP. Please connect your PC to JetWave 2212X/S Ethernet port and start below steps to scan and configure.

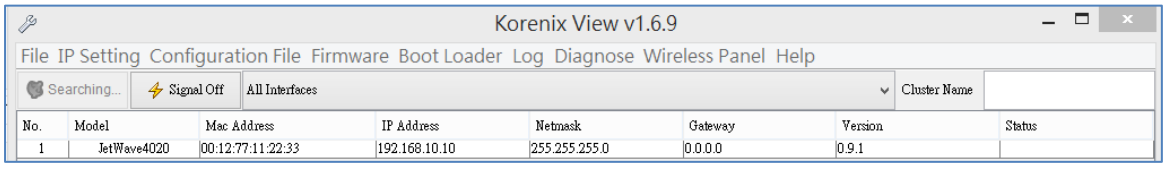
5.3.1 Device Discovery:

Step 1: Open the Korenix View Utility. (Must later than V1.6.11)

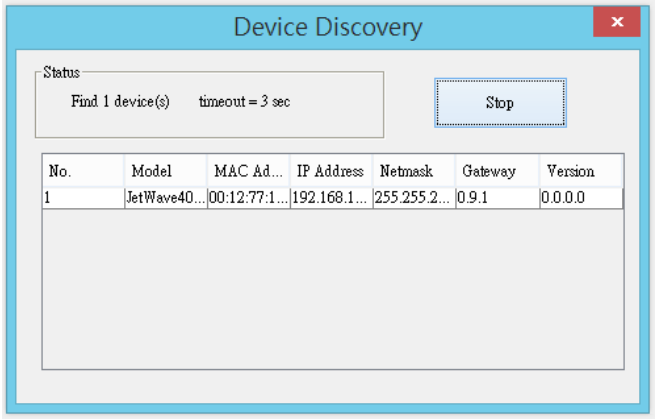
Step 2: Select the correct NIC (Network Interface Card) from the NIC list or remains the “All Interfaces”.

Step 3: Click **“Discovery”**, and then the Nodes and its IP address can be found and listed in Node list.

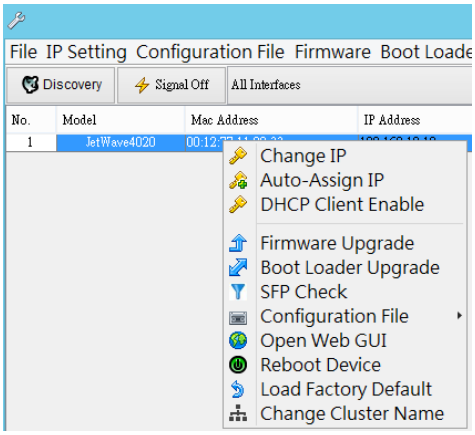
- Figure: The main screen of the Korenix View Utility



- Figure: The Device Discovery Screen, please wait couple seconds.



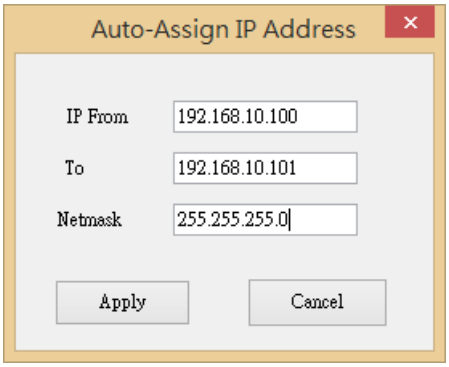
5.3.2 Basic Tools Shortcut:



After you scan the network, select the AP and click Right key of mouse, you can see some tools.

a. You can modify the IP address/Netmask directly on the field and then click "**Change IP**" to change the IP settings.

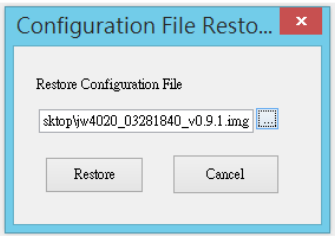
b. Select multiple devices and click "**Auto-Assign IP**", the popup screen will ask you type the IP Address range. You can assign new IP address for the selected devices.

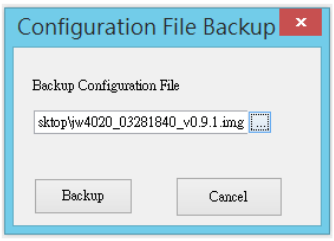


c. You can enable DHCP client by "DHCP Client Enable".

d. You can upgrade firmware for single or multiple units by **"Firmware Upgrade"**. A popup screen will ask you select the target firmware file you'd like to upgrade.

e. You can Backup/Restore the configuration file by "**Configuration File -> Backup/Restore"**. A popup screen will ask you select target configuration/target folder you'd like to backup or restore.

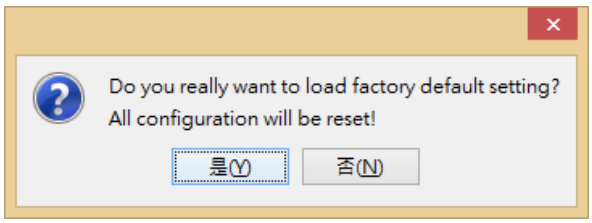




f. Click "**Open Web GUI**" to access the web management interface.

g. You can reboot the device by "**Reboot Device**". A popup screen will ask you confirm again.

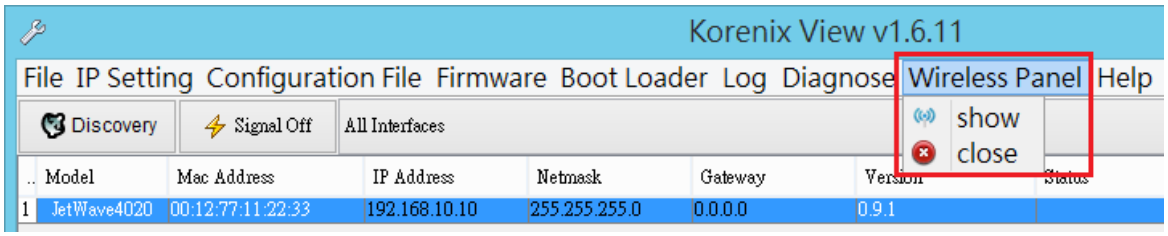
h. You can restore to default configuration by "**Load Factory Default**". A popup screen will ask you confirm again.



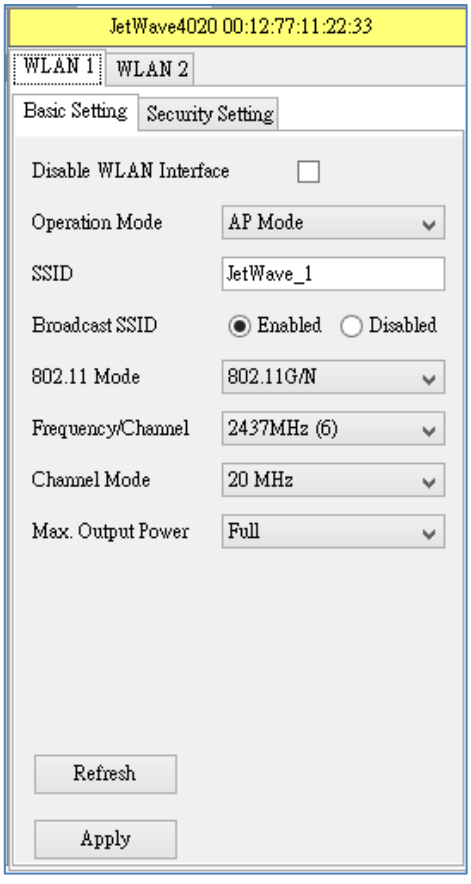
Note: You can also find these commands in the upper menu of the Korenix View Utility.

5.3.3 Wireless Panel

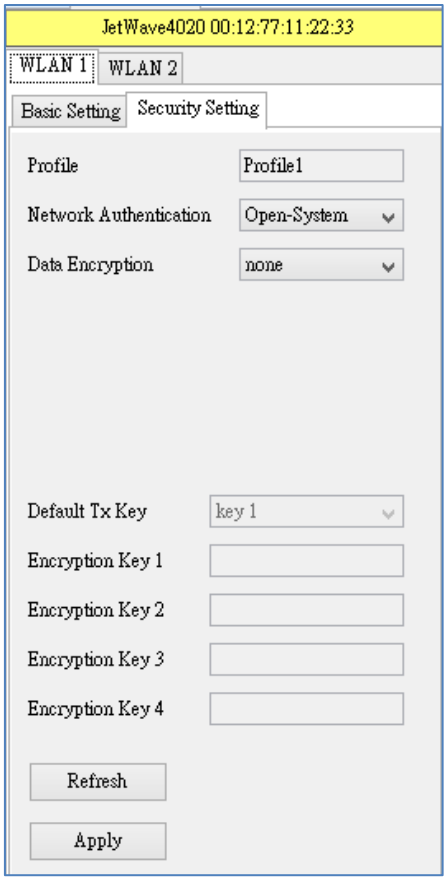
Korenix View Utility provides Wireless panel to configure some **Basic Setting** and **Security setting** for Wireless LAN Interfaces. You can use the tool to configure settings for single device or a group of devices. Select the target device/devices for further configuration.



Basic Setting



Security Setting



Basic Setting

The Basic Setting panel allows you Disable WLAN Interface, configure the Operating Mode, SSID, Broadcast SSID, Enable/Disable, 802.11 Mode, Frequency/Channel, Channel Mode and Max. output power.

Press “**Apply**” to activate the new settings.

Security Setting

The Security Setting panel allows you to configure the Network Authentication type and the encryption keys for the AP profile.

Press “**Apply**” to activate the new settings.

Note:

Must click **“Refresh”** to load the current configuration of the selected AP

Chapter 6

Troubleshooting

Chapter 6 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the JetWave 2212S/X. For warranty assistance, contact your service provider or distributor for the process.

6.1 General Question

6.1.1 How to know the MAC address of the AP?

MAC Address distinguishes itself by the unique identity among network devices. There are two ways available to know it.

Each device has a label posted on the side of the AP. There are MAC addresses for Ethernet and Radio interfaces. On the Web-based management interface, you can view the MAC Address from "**Status**" -> "**Information**". You can also see this in CLI or SNMP OID.

6.1.2 What if I would like to reset the unit to default settings?

You can reset the unit to default setting in Web GUI. You can reserve the IP address setting.

6.1.3 Why can not access the Web-based management interface?

Please check the followings:

- Check whether the IP address of PC is correct (In the same network segment as the unit)
- Login the unit via other browsers such as Firefox, Google Chrome.
- Use Korenix View Utility to scan the AP and check/modify the IP address.
- If everything is correct, but, you still can't access the web GUI, we suggest you connect the console cable to do further checking. Please refer to the pin assignment in hardware installation chapter.
- Check whether the power supply is OK; Try to power on the unit again. If the web GUI can't be accessed issue occurred again, please contact our technical service engineer. We may ask you connect console cable and provide us more information.

6.2 Wireless

6.2.1 What if the wireless connection is not stable after associating with an AP under wireless client mode?

- In addition, you can start "**Site Survey**" to check the signal strength. If it is weak or unstable (The smaller the number is, the weaker the signal strength is.), please join other available AP for better connection.
- If you install the directional antenna for point to point/multi-point connection, adjust the antenna and tune the signal strength/performance by Antenna Alignment Tool again. After antenna alignment, the data rate test can help you check the current performance.
- In Wireless client mode, type the connected AP' MAC address to fix the AP for your client. It avoid your wireless client not to connect other AP.

6.2.2 What if the wireless connection performance is not good, how to improve it?

- Once the signal strength RSSI is always under **-65dbm** in long distance transmission, it is suggest you to change antenna's direction or replace antenna with higher gain.
- If the distance between the wireless client and target AP is short, but, the antenna gain is very high. Reduce the RF power is also an option.

6.3 Appendix

6.3.1 ASCII

WEP can be configured with a 64-bit or 128-bit Shared Key (hexadecimal number or ACSII). As defined, hexadecimal number is represented by 0-9, A-F or a-f; ACSII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.

ASCII Table

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
‘	27	?	3F	W	57	o	6F
(	28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[	5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45	]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64	|	7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

Revision History

Version	Description	Date	Editor
V1.0	1st release for JetWave 2212S/X	Oct. 2018	Shelly Tsai