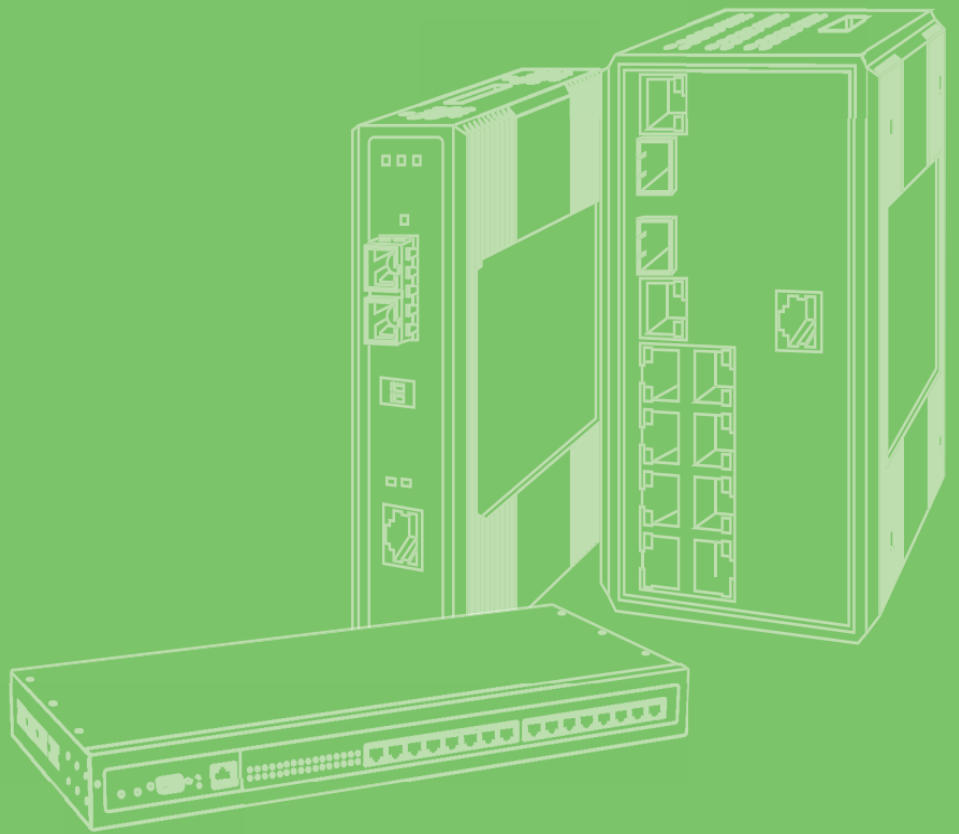


User Manual



WISE-6610

Industrial LoRaWAN Gateway

ADVANTECH

Enabling an Intelligent Planet

Contest

1.1 Overview	3
1.2 Device Features.....	4
1.3 Statement.....	4
1.4 Specifications.....	7
1.4.1 Dimensions (mm).....	7
1.4.2 Specifications.....	8
1.4.3 Mounting Specification and Process.....	8
1.4.4 Hardware Rear View	9
2.1 Login.....	10
2.1.1 Changing Default Password.....	11
2.2 Overview.....	12
2.3 Interface	14
2.3.1 LAN	14
2.3.2 ETHWAN.....	16
2.4 LoRaWAN.....	17
2.4.1 Advantech LoRaWAN Service	17
2.4.2 BasicStation	18
2.5 Networking	19
2.5.1 Static Route.....	19
2.5.2 Forwarding.....	20
2.5.3 Security	22
2.5.4 OpenVPN.....	23
2.5.5 GRE.....	26
2.5.6 QoS Settings.....	27
2.5.7 VRRP	29
2.5.8 IPSEC VPN.....	30
2.6 System Management.....	34
2.6.1 Password Manager.....	34
2.6.2 Syslog.....	34
2.6.3 NTP/Time.....	35
2.6.4 SNMP.....	36
2.6.5 Network Access	37
2.6.6 Configuration Manager.....	38
2.6.7 Firmware Upgrade	39
2.6.8 Reset System.....	39
2.6.9 Reboot Device.....	40
2.6.10 Apply Configuration	40
2.7 Application Tools	41
2.7.1 Custom Script.....	41

2.7.2 MQTT	42
2.7.2 Node-RED.....	44
2.7 Diagnostics Tools.....	45
2.8 IPK Management	46

Chapter 1

Introduction

1.1 Overview

WISE-6610-XB Serial is an Industrial Internet of Things (IIoT) LoRaWAN Gateway designed for industrial automation and data collection applications. It offers various connectivity options and features for monitoring, control, and data collection in industrial environments.

The WISE-6610-XB series offers reliable LoRaWAN transmission services, supporting all LoRaWAN Nodes. It also provides compatibility with cloud services such as Actility ThinkPark Enterprise, AWS IoT Core and The Things Network.

1.2 Device Features

- WISE-6610-XB comes with an industrial-grade design, including a durable enclosure and the ability to withstand various harsh environmental conditions.
- WISE-6610-XB is specifically designed for LoRaWAN connectivity, enabling long-range, low-power IoT communication suitable for applications in various domains, such as smart cities, agriculture, and industrial automation.
- It supports remote monitoring and management, allowing users to access the device from remote locations, view real-time data, and perform remote management tasks.
- Supports wide temperature range: -40 ~ 70°C
- Support Advantech LoRaWAN Service
- Supports GRE, OpenVPN secured tunnel

1.3 Statement

Industry Canada statement

This device complies with ISED's licence-exempt RSSs. 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.

Le présent appareil est conforme aux CNR d'ISED applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes : (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

FOR MOBILE DEVICE USAGE (>20cm/low power)

Radiation Exposure Statement:

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with greater than 20cm between the radiator & your

body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à plus de 20cm entre le radiateur et votre corps.

DETACHABLE ANTENNA USAGE

This radio transmitter [IC: 9404A-WISE6610V2] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio [IC: 9404A-WISE6610V2] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Manufacturer	Model	Antenna Type	Max Gain (dBi)	Impedance (Ω)
Advantech	WISE-6610	Dipole	2.9	50

Federal Communication Commission Interference Statement

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

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

- Reorient or relocate the receiving antenna.

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

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FOR MOBILE DEVICE USAGE (>20cm/low power)

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.

NCC 電信管制射頻器材警語

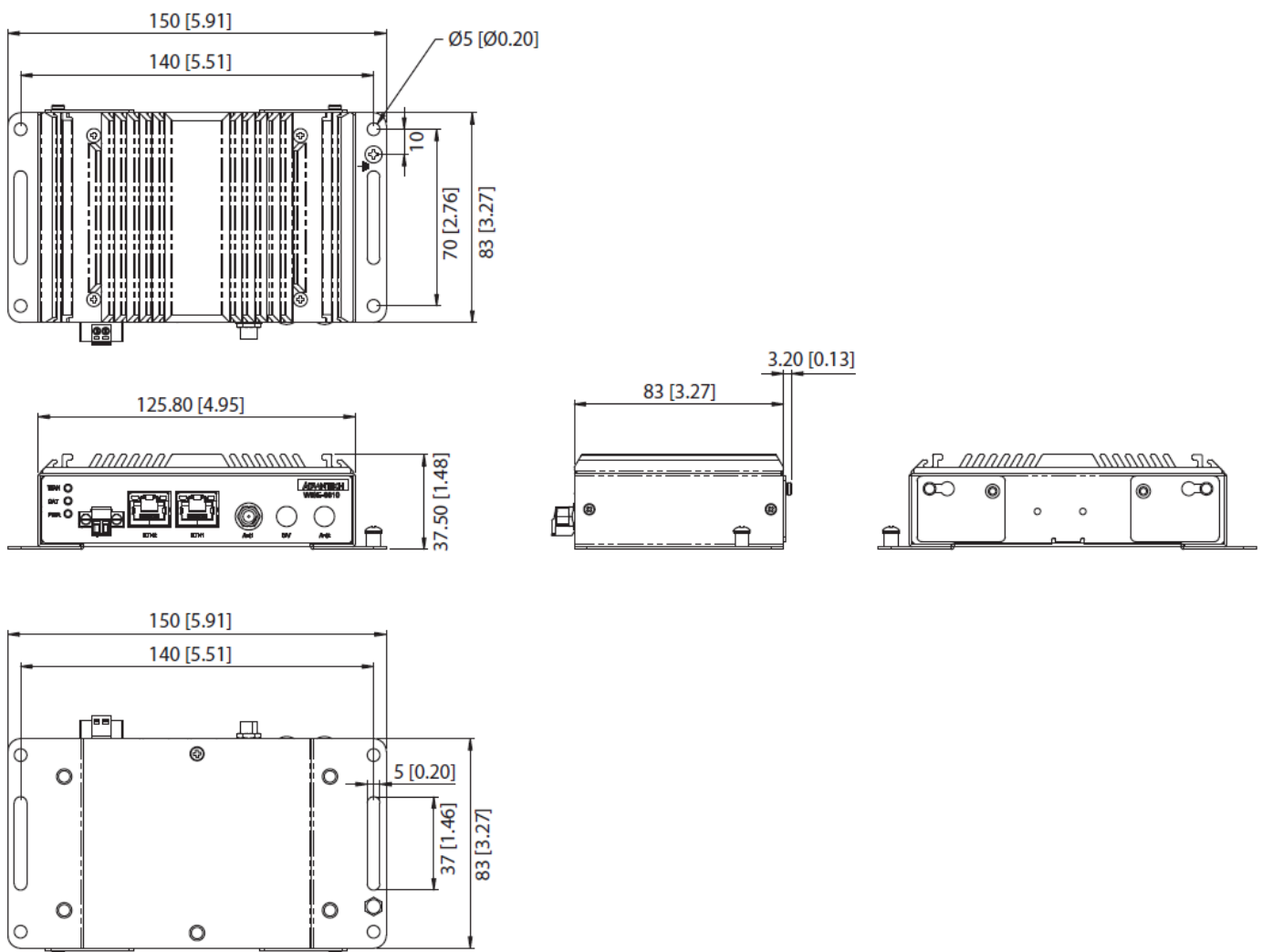
取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

1.4 Specifications

The WISE-6610v2 is the next generation of Industrial LoRaWAN Gateway. It has high-performance that offers reliable connectivity for industrial environments. It supports the LoRaWAN protocol for building LoRaWAN private and public networks, as well as various industrial protocols including Modbus, OPCUA, Backnet/IP, MQTT, etc. The hardware and software flexibility of the WISE-6610 provides rich features for edge intelligence systems, and also supports VPN tunneling with various protocols ensures safe communications. The WISE-6610 also runs an embedded LoRaWAN network server (LNS) that can decode the LoRaWAN data directly in our device.

1.4.1 Dimensions (mm)



1.4.2 Specifications

System

- CPU ARM Cortex-A8, 1000 MHz
- RF Chip Semtech SX1302
- Memory 4GB DDR3
- Internal Storage 16GB EMMC

WSN Support

- Standard LoRaWAN
- Frequency IN865/EU868/AU915/US915/KR920/AS923
- ANT Connector RP-SMA Male connector x 1

LAN Interface

- Ethernet 10/100 Mbps, auto MDI/MDIX
- Connector 2 x RJ45
- Protection 1.5-kV built-in magnetic isolation protection

General

- LED Indicators PWR, DAT, WAN, ETH
- Reboot Trigger Reset button

Software

- Network and Routing DHCP server, NAT/PAT, VRRP, dynamic DNS client, DNS proxy, VLAN, QoS, DMVPN, NTP client/server, IGMP, BGP, OSPF, RIP, SMTP, SMTPS, SNMP v1/v2c/v3, backup routers, PPP, PPPoE, SSL, port forwarding, host port routing, Ethernet bridging, network server
- Configuration SSH, Web Browser
- Network Security HTTPS, SSH, VPN tunnels, SFTP, DMZ, firewall (IP filtering, MAC address filtering, inbound/outbound port filtering)
- VPN tunnelling Open VPN client and server and P2P, L2TP, PPTP, GRE, EasyVPN, IPSec with IKEv1 and IKEv2
- Software package Node-Red, LoRaWAN Network Server, Edgeling (only in -EL P/N)

Mechanics

- Dimensions (W x H x D) 150 x 37.5 x 83 mm (5.9" x 1.48" x 3.27")
- Mounting DIN rail, wall
- Weight 500g
- Enclosure Rating IP30
- SD Card 1 x Micro SD Card Slot
- SIM Card 2 x Nano SIM Card Slot

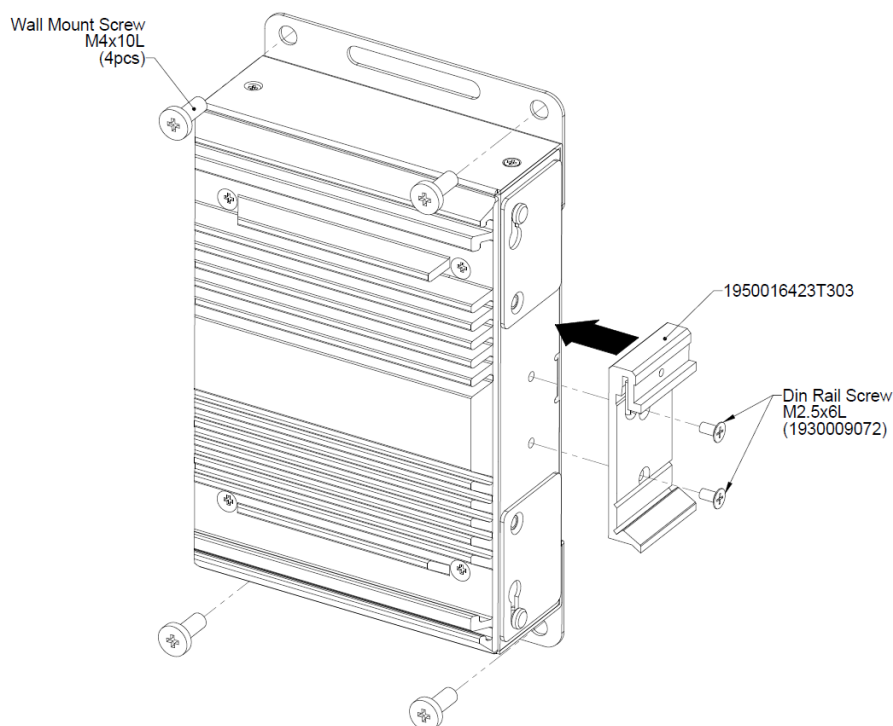
Power Requirements

- Power Input 9 – 36 V_{DC}
- Power Consumption Typ. 3W@24V (Max.3.2W)
Typ. 3W@12V (Max.4W)

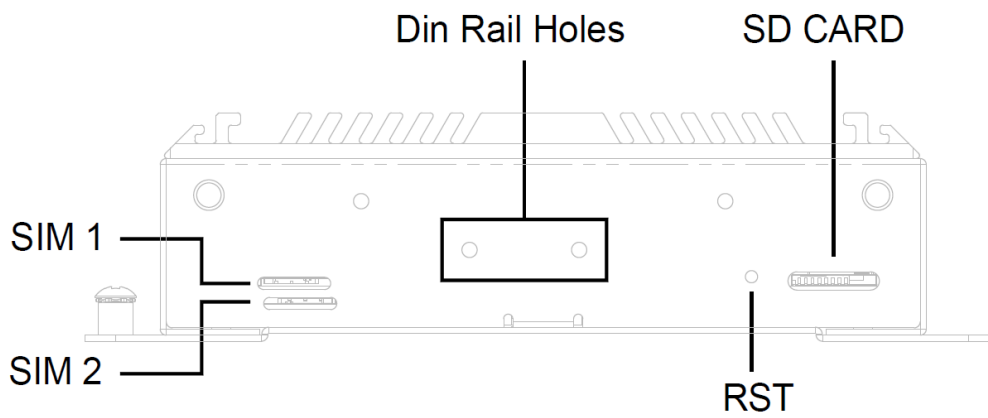
Environment

- Operating Temperature -40 – 75°C
- Storage Temperature -40 – 85°C
- Operating Humidity 10 – 95% RH

1.4.3 Mounting Specification and Process



1.4.4 Hardware Rear View



Chapter 2

Web Interface

2.1 Login

When the device is first installed, the default IP is 192.168.1.1. You will need to make sure your network environment supports the device setup before connecting it to the network.

1. Launch your web browser on a computer.
2. In the browser's address bar type in the device's default IP address (192.168.1.1). The login screen displays.
3. Enter the default user name and password (admin/admin) to log into the management interface. You can change the default password after you have successfully logged in.
4. Click Login to enter the management interface.

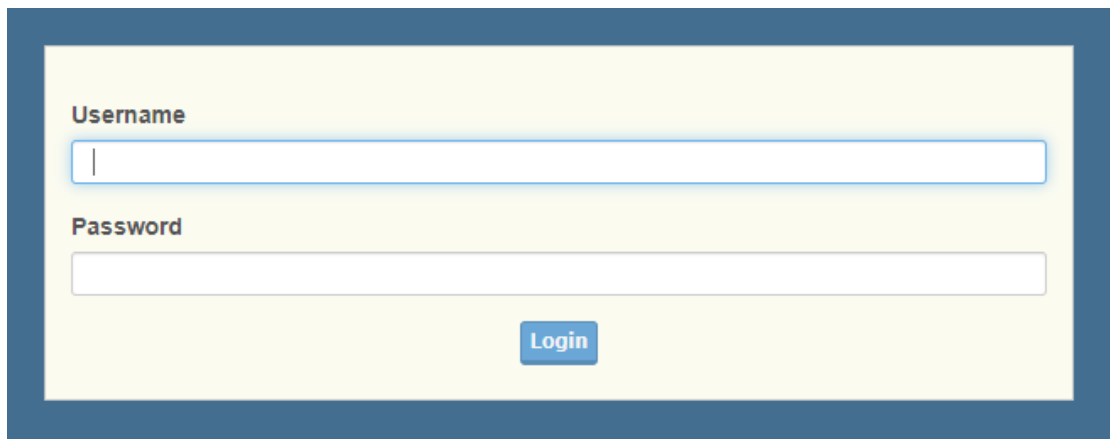
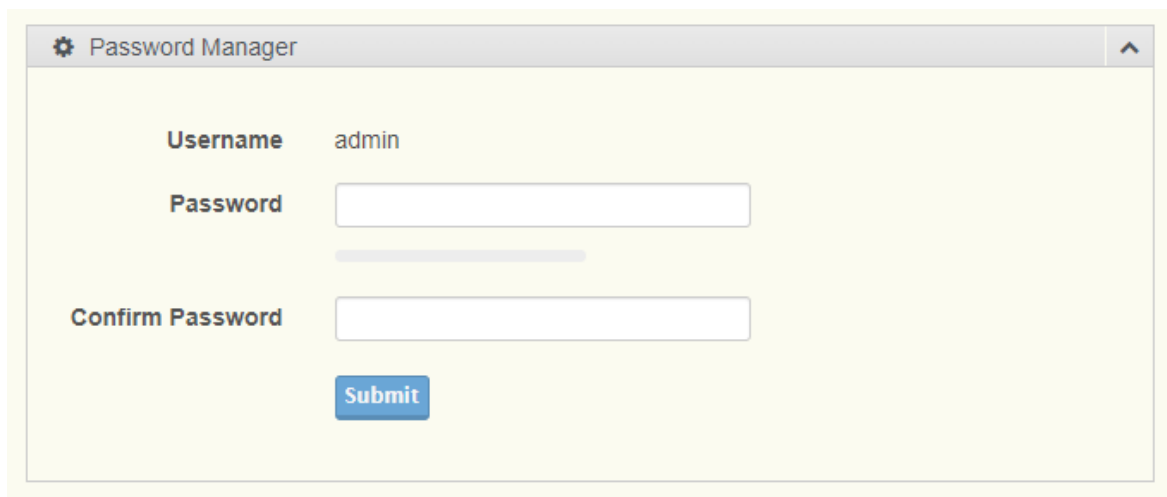
The image shows a login screen with a light yellow background and a dark blue border. It features two input fields: "Username" and "Password". The "Username" field contains a vertical cursor. Below the fields is a blue "Login" button.

Figure 2.1 Login Screen

2.1.1 Changing Default Password


1. Navigate to **System Management > Password Manager**. The HTTP configuration page displays.
2. Enter the username of the profile to change (currently logged in user displays), then enter the new password under the Password field.
3. Re-type the same password in the Confirm Password field.
4. Click Submit to change the current account settings.

The image shows the "Password Manager" configuration page. The title bar includes a gear icon and the text "Password Manager". The page has a light yellow background. It displays the "Username" field with the value "admin". Below it are the "Password" and "Confirm Password" fields, both empty. A blue "Submit" button is located at the bottom.

2.2 Overview

To access this page, click **Overview**.

System Info	
Information Name	Information Value
Firmware Version	1.0.5
LoRaWAN Service Version	1.00.09
SX1302 Chip Version	V01.00.05
Serial Number	1234568899
Local Hostname	Advantech
System Time	Thu Oct 26 01:12:52 2023
System Up Time	0 day 18 hr 30 min 42 sec
Model Name	WISE-6610-NB

LAN Interface	
Information Name	Information Value
LAN Status	 Address: 192.168.1.1 Netmask: 255.255.255.0 Gateway: 0.0.0.0 DNS Server: RX: 2.48 MB (13143 Pkts.) TX: 2.91 MB (6686 Pkts.) MAC-Address: 74:11:22:33:44:66


WAN Interface	
Information Name	Information Value
ETHWAN	 Address: 172.16.12.108 Netmask: 255.255.254.0 Gateway: 172.16.13.254 DNS Server: 172.20.1.100, 172.20.1.99 RX: 1.10 GB (3718218 Pkts.) TX: 101.99 KB (1000 Pkts.) MAC-Address: 74:11:22:33:44:55

Figure 2.3 Overview

If device has LTE module, also see the Cellular Status


WAN Interface	
Information Name	Information Value
Cellular Status	 Type: Current SIM: SIM doesn't exist Network Provider: Signal Level: dBm Internet Status: Disconnected IP Address: Netmask: Default Gateway: Connection Time: 0 day 0 hr 0 min 0 sec

Figure 2.4 Cellular Status

DHCP Leases			
Hostname	IPv4-Address	MAC-Address	Lease Time Remaining
There are no active leases.			




System Status	
Information Name	Information Value
Storage Utilization	 2% (170.2M/9.5G)
Memory Utilization	 16% (82584KB/505044KB)
CPU Utilization	 10%

Figure 2.5 Cellular Status

The following table describes the items in the previous figure

Item	Description
System Info	
Firmware Version	Displays the current firmware version of the device
LoRaWAN Service Version	Displays the current version of Advantech LoRaWAN Service
SX1302 Chip Version	Displays the current firmware version of the SX1302 LoRaWAN Module
Serial Number	Displays the serial number of the device
Local Hostname	Displays the current local hostname of the device.
System Up Time	Displays the time since the last device reboot
Model Name	Displays the model name of the device.
LAN Interface	
LAN Status	<ul style="list-style-type: none"> ■ Local IP Address: Displays the assigned IP address of the LAN interface. ■ Local Netmask: Displays the assigned netmask of the LAN interface. ■ Gateway: Displays the assigned gateway for the LAN interface. ■ DNS Server: Displays the IP address of the

	<ul style="list-style-type: none"> ■ RX: Displays the receiving volume of data in bytes. ■ TX: Displays the transmission volume of data in bytes. ■ MAC Address: Displays the MAC address of the device
WAN Interface	
WAN Status	<ul style="list-style-type: none"> ■ Local IP Address: Displays the assigned IP address of the LAN interface. ■ Local Netmask: Displays the assigned netmask of the LAN interface. ■ Gateway: Displays the assigned gateway for the LAN interface. ■ DNS Server: Displays the IP address of the ■ RX: Displays the receiving volume of data in bytes. ■ TX: Displays the transmission volume of data in bytes. ■ MAC Address: Displays the MAC address of the device
Cellular Status	<ul style="list-style-type: none"> ■ Type: Displays the LTE type. ■ Current SIM: Displays the status of the SIM slot. ■ Network Provider: Displays the name of the provider of the LTE carrier. ■ Signal Level: Displays the signal level in dBm. ■ Internet Status: Displays the status of the Internet connection. ■ IP Address: Displays the IP address of the current connection. ■ Netmask: Displays the netmask of the current connection. ■ Default Gateway: Displays the gateway of the current connection. ■ Connection Time: Displays the uptime of the connection.
DHCP Leases	
Active Leases	Displays the active DHCP leases.
System Status	
Storage Utilization	Displays the total storage utilization in terms of percentage.
Memory Utilization	Displays the total memory utilization in terms of percentage.
CPU Utilization	Displays the total CPU utilization in terms of percentage.

2.3 Interface

2.3.1 LAN

To access this page, click **Interface > LAN**.

LAN Interface Setup

Local Hostname: Advantech

Domain Name: lan

Mode: Static

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP Server

DHCP Server: Enabled Disabled

Start IP Address: 192.168.1.100

Pool Size: 150

Lease Time: Day: 0 (0 - 365), Hour: 12 (0 - 23), Minute: 0 (0 - 59), Second: 0 (0 - 59)

Static DNS 1: [Empty]

Static DNS 2: [Empty]

Static Hosts

IP Address	Identified by	Delete
<input type="button" value="Add"/>		
<input type="button" value="Submit"/>		

Figure 2.6 Interface > LAN

The following table describes the items in the previous figure.

Item	Description
LAN Interface Setup	
Local Hostname	Enter the device name: up to 31 alphanumeric characters.
Domain Name	Enter the name to be assigned for the interface domain.
Protocol	Click the drop-down menu to assign the type of protocol to the interface: DHCP Client or Static
IP Address	Static Protocol Only: Enter a value to specify the IP address of the interface. The default is

	192.168.1.1.
Subnet Mask	Static Protocol Only: Enter a value to specify the IP subnet mask for the interface. The default is 255.255.255.0.
DHCP Server	
DHCP Server	Click to enable or disable the DHCP server function.
Start IP Address	Enter the starting IP address of the DHCP pool.
Pool Size	Enter the value to define the number of allowed DHCP leases.
Lease Time	Enter the lease time duration in Days (0-365), Hours, (0-23), Minutes (0-59), and Seconds (0-59).
Static DNS 1	Enter the IP address of the primary DNS
Static DNS 2	Enter the IP address of the secondary DNS.
Static Hosts	
IP Address	IP Address of this static host
Identified by	Identified name of this static host
Delete	Delete button of this static host
Submit	Click Submit to save the values and update the screen.

Note! All new configurations will take effect after rebooting. To reboot the device, click **System Management > Reboot Device.**

2.3.2 ETHWAN

To access this page, click **Interface > ETHWAN.**

Figure 2.7 Interface > ETHWAN

The following table describes the items in the previous figure.

Item	Description
Ethernet WAN	Click the drop-down menu to select the WAN interface: Disable or ETH 1.
Protocol	Click the drop-down menu to assign the type of protocol to the ETHWAN: DHCP Client , Static , PPPoE , PPTP or L2TP.
IP Address	Static , PPTP or L2TP: Enter a value to specify the IP address of the interface
Subnet Mask	Static , PPTP or L2TP: Enter a value to specify the IP subnet mask for the interface
Default Gateway	Static , PPTP or L2TP: Enter a value to specify the default gateway for the interface.
DNS Server 1	Static Protocol Only: Enter a value to specify the primary DNS server for the interface.
DNS Server 2	Static Protocol Only: Enter a value to specify the secondary DNS server for the interface.
Server IP Address	PPTP or L2TP: Enter PPTP or L2TP server IP address.
Username	PPPoE , PPTP or L2TP: Enter username for this session.
Password	PPPoE , PPTP or L2TP: Enter password for this session.
Service	PPPoE Only: Specifies the Service Name to connect to, If unset, pppd uses the first discovered one
MTU	PPPoE Only: MTU on this PPPoE session
Keep Alive	PPPoE Only: Number of connection failures before reconnect

2.4 LoRaWAN

2.4.1 Advantech LoRaWAN Service

To access this page, click **LoRaWAN > Advantech LoRaWAN Service**.

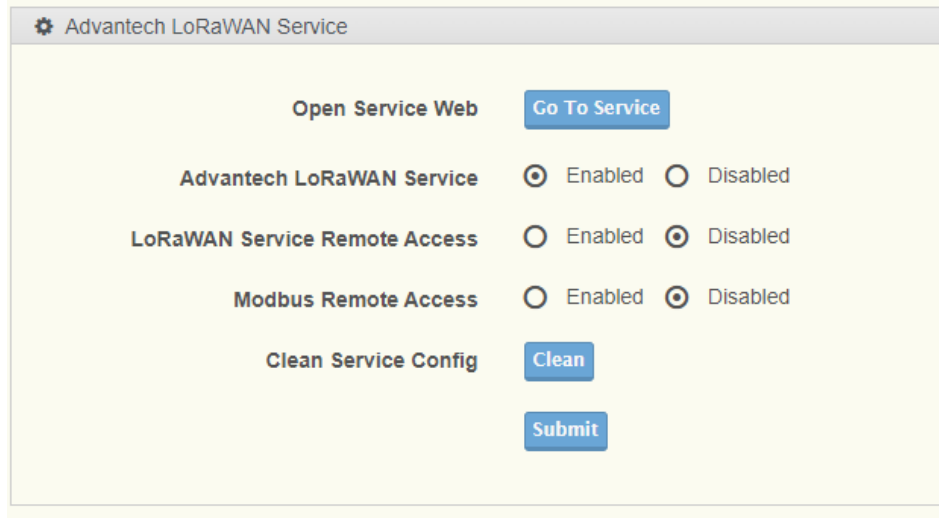


Figure 2.11 LoRaWAN > Advantech LoRaWAN Service.

The following table describes the items in the previous figure.

Item	Description
Open Service Web	Direct to Advantech LoRaWAN Network Server
Advantech LoRaWAN Service	Click to enable or disable the LoRaWAN Network Server function.
LorRaWAN Service Remote Access	Click to enable or disable the LoRaWAN Network Server access from WAN side.
Modbus Remote Access	Click to enable or disable the Advantech Application Modbus service access from WAN side.
Clean Service Config	Reset Advantech LoRaWAN Service configuration.
Submit	Click Submit to save the values and update the screen.

2.4.2 BasicStation

2.4.2.1 Setting

To access this page, click **LoRaWAN > BasicStation > Setting**.

Figure 2.12 LoRaWAN > BasicStation > Setting

The following table describes the items in the previous figure.

Item	Description
BasicStation	Click to enable or disable the BasicStation function.
LoRaWAN Gateway EUI	EUI of SX1302 chip on this WISE-6610v2
Server IP Address	Enter server IP address or URL
Port	Enter server port
Back-end Protocol	Click the drop-down menu to assign the type of protocol to the BasicStation: LoRaWAN Network Server(LNS) or Configuration and Update Service(CUPS).
Authentication Mode	Click the drop-down menu to assign the type of authentication mode to the BasicStation: No Authentication , Turst Server CA Only , Server and Client Authentication or Server and Client Token
Trusted Server CA	Upload server trust file
Client CA	Upload client certificate file
Private Key	Upload private key file
Submit	Click Submit to save the values and update the screen.

2.5 Networking

2.5.1 Static Route

A static route provide fixed routing path through the network. It is manually configured on the router and must be updated if the network topology was changed recently. Static routes are private routers unless they are redistributed by a routing protocol.

To access this page, click **Networking > Static Route**.

Target IP Address	Netmask	Gateway	Interface	Metric	MTU	Delete
192.168.1.10	255.255.0.0	192.168.1.1	LAN	3	1500	Delete
			LAN			Delete

Add Submit

Figure 2.13 Networking > Static Route

The following table describes the items in the previous figure.

Item	Description
Target IP Address	Enter an IP address (static route) for this static route.
Netmask	Enter a netmask setting (static route) for this static route.
Gateway	Enter a gateway setting (static route) for this static route.
Interface	Enter an interface for this static route, options: LAN, WAN, or Cellular
Metric	Enter the administrative distance (default: 1) used by the ap to choose the best path for two or more routes to the same destination.
MTU	Enter the maximum transmission value for the data packets if applicable.
Delete	Click Delete to remove the route from the available list
Add	Click Add to include the route in the static routing policy
Submit	Click Submit to save the values and update the screen.

2.5.2 Forwarding

2.5.2.1 Port Forwarding

Port forwarding, also known as port mapping, allows for the application of network addresses (NAT) the redirection of a communication request from an address and port to a specified address while the packets traverse the firewall. The function are designed for networks hosting a specific server, such as a web server or mail server, on the private local network and behind the NAT firewall.

To access this page, click **Networking > Forwarding > Port Forwarding**.

To access this page, click **Networking > Forwarding > Port Forwarding**.

Enabled	Name	Start Port	End Port	Local IP	Local Port	Protocol	Delete
<input checked="" type="checkbox"/>	http_server	80	82	192.168.1.10	80	TCP	Delete
<input checked="" type="checkbox"/>	ftp_server	21	21	192.168.1.20	21	Both	Delete
<input checked="" type="checkbox"/>	ssh	22	22	192.168.1.30	22	Both	Delete
<input type="checkbox"/>						TCP	Delete

Add Apply

Figure 2.14 Networking > Forwarding > Port Forwarding.

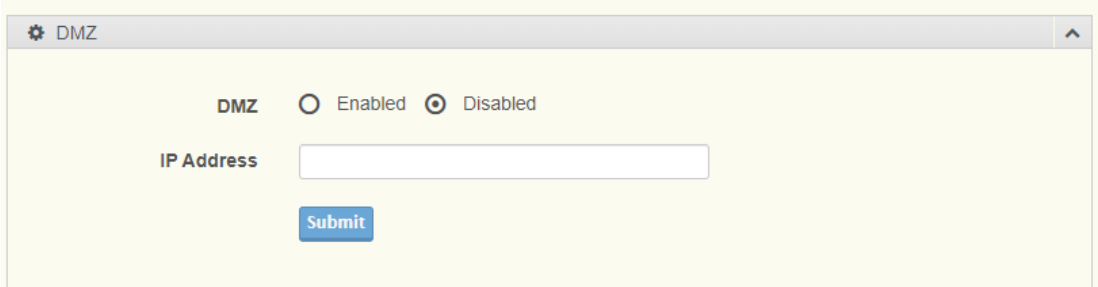
The following table describes the items in the previous figure.

Item	Description
Enabled	Select to enable the defined port forwarding entry
Name	Enter a text string to identify the port forwarding entry
Start Port	Enter the value of the starting port for this entry.
End Port	Enter the value of the ending port for this entry
Local IP	Enter the IP address defining the static address of the local IP.
Local Port	Enter the value defining the local port.
Protocol	Click the drop-down menu to select the protocol setting, options: TCP, UDP, Both.
Delete	Click Delete to remove the selected entry from the port forwarding policy.
Add	Click Add to include the entry in the port forwarding policy.
Submit	Click Submit to save the values and update the screen.

2.5.2.2 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to the Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

To access this page, click **Networking > Forwarding > DMZ**



The screenshot shows a web-based configuration window titled "DMZ". At the top left, there is a gear icon and the text "DMZ". Below this, the label "DMZ" is followed by two radio buttons: "Enabled" (which is unselected) and "Disabled" (which is selected). Underneath, the label "IP Address" is followed by a text input field. At the bottom center, there is a blue "Submit" button.

Figure 2.14 Networking > Forwarding > DMZ.

The following table describes the items in the previous figure.

Item	Description
DMZ	Click the radio button to enable or disable the DMZ function.
IP Address	Enter the IP address to designate a static IP address as the DMZ target.
Submit	Click Submit to save the values and update the screen.

2.5.3 Security

2.5.3.1 Filter

The firewall is a system or group of systems that enforce an access control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. The device has capabilities of Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding as well as DMZ. Source IP Filtering: The source IP filtering gives users the ability to restrict certain types of data packets from users local network to Internet through the device. Use of such filters can be helpful in securing or restricting users local network.

To access this page, click **Networking > Security > Filter**.

Enabled	Direction	Source IP	Destination IP	Protocol	Source Port	Destination Port	Delete
<input checked="" type="checkbox"/>	LAN -> WAN	192.168.1.100	8.8.8.8	TCP	8080	8080	Delete

Figure 2.15 Networking > Security > Filter.

The following table describes the items in the previous figure.

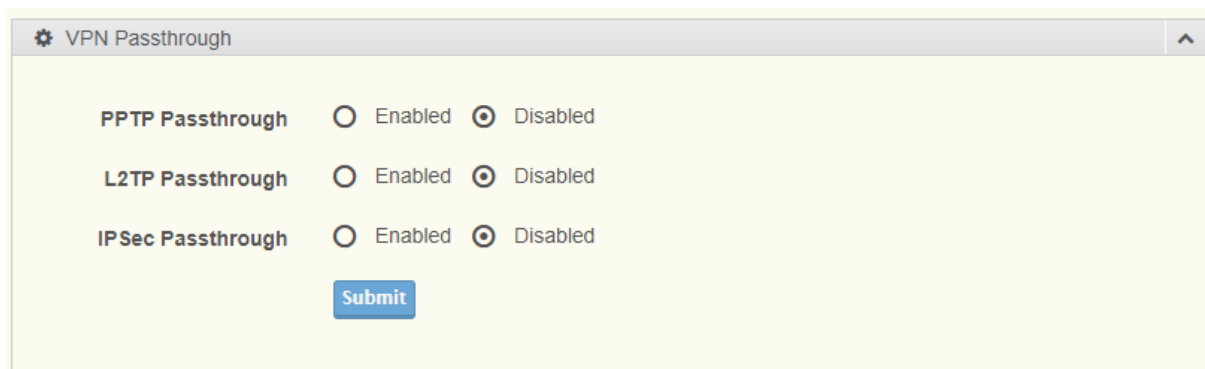
Item	Description
Filter	Click the radio button to enable or disable the Filter policy
Enabled	Select to enable the defined filter entry.
Direction	Click the drop-down menu to select the direction of the data packet traffic for the entry: LAN to WAN, WAN to LAN.
Source IP	Enter the IP address of the sender address.
Destination IP	Enter the IP address of the destination address.
Protocol	Click the drop-down menu to select the protocol type for the entry: TCP, UDP, ICMP.
Source port	Enter the port number of the sender IP address
Destination port	Enter the port number of the destination IP address.
Delete	Click Delete to remove the entry from the Filter policy.
Add	Click Add to include the entry in the Filter policy
Submit	Click Submit to save the values and update the policy.

2.5.3.1 VPN Passthrough

VPN pass-through is a function of the router, which provides outbound VPN function. VPN pass-

through does not provide inbound VPN function. You can enable VPN passthrough without the need to open any ports, and it will run automatically

To access this page, click **Networking > Security > VPN Passthrough**



VPN Passthrough

PPTP Passthrough Enabled Disabled

L2TP Passthrough Enabled Disabled

IPSec Passthrough Enabled Disabled

Submit

Figure 2.16 Networking > Security > VPN Passthrough.

The following table describes the items in the previous figure.

Item	Description
PPTP Passthrough	Click the radio button to enable or disable PPTP packets to pass through.
L2TP Passthrough	Click the radio button to enable or disable L2TP packets to pass through.
IPSec Passthrough	Click the radio button to enable or disable IPSEC packets to pass through.
Submit	Click Submit to save the values and update the policy

2.5.4 OpenVPN

2.5.4.1 Tunnel 1

VPN pass-through is a function of the router, which provides outbound VPN function. VPN pass-through does not provide inbound VPN function. You can enable VPN passthrough without the need to open any ports, and it will run automatically.

To access this page, click **Networking > OpenVPN > Tunnel 1**

Figure 2.17 Networking > OpenVPN > Tunnel 1.

The following table describes the items in the previous figure.

Item	Description
Status	Displays the current status of the OpenVPN
Tunnel 1	Click to enable or disable the tunnel.
Protocol	Click to define the protocol for the tunnel. Settings: UDP, TCP Server, or TCP Client.
Port	Enter the variable to define the tunnel port.
Remote IP Address	Enter the IP address of the remote endpoint.
Remote Subnet	Enter the subnet address of the remote endpoint.
Remote Subnet Mask	Enter the remote subnet mask of the remote endpoint.
Server Network	If Authenticate mode is selected under Server Mode, you need to assign a server IP address.
Server Netmask	If Authenticate mode is selected under Server Mode, you need to assign

	a server network mask.
Redirect Gateway	Adds (rewrites) the default gateway. All packets are then sent to this gateway via tunnel, if there is no other specified default gateway inside them.
Local Interface IP Address	Specifies the IPv4 address of a local interface
Remote Interface IP Address	Specifies the IPv4 address of the interface of opposite side of the tunnel.
Ping Interval	Enter the variable to define the frequency of the ping activity. Variable: 1 to 86400.
Ping Timeout	Enter the variable to define the timeout period for a failed ping.
Renegotiate Interval	Enter the variable to define the period of time before initiating a renegotiation. Variable: 0 to 86400.
Max Fragment Size	Maximum size of a sent packet.
Compression	Click the drop-down menu to select the type of compression. Setting: None or LZO.
NAT Rules Applied	Activates/deactivates the NAT rules for the OpenVPN tunnel.
Authenticate Mode	Click the drop-down menu to select the authentication mode: Setting: None, Server Mode, Secret, Password, TLS MClient, TLS Server, TCL Client.
Pre-Shared Secret	Click Choose File to browse and select a file containing the preshared secret.
CA Certificate	Click Choose File to browse and select a certificate.
DH Parameters	Click Choose File to browse and select a file containing key exchange protocol.
Local Certificate	Click Choose File to browse and select a file containing the local certificate.
Local Private Key	Click Choose File to browse and select a file containing a designated private key.
Username	Enter the string to define a user name.
Password	Enter a string to bind to the defined user name
Extra Options	Specifies additional parameters for the OpenVPN tunnel, such as DHCP options. The parameters are preceded by two dashes.
Submit	Click Submit to save the values and update the policy.

2.5.4.2 Tunnel 2

For further information regarding the configuration of the OpenVPN Tunnel function see “Tunnel 1” on page 23.

2.5.4.3 Tunnel 3

For further information regarding the configuration of the OpenVPN Tunnel function see “Tunnel 1” on page 23.

2.5.4.4 Tunnel 4

For further information regarding the configuration of the OpenVPN Tunnel function see “Tunnel 1” on page 23.

2.5.5 GRE

The Generic Routing Encapsulation (GRE) protocol encapsulates data packets one routing protocol inside the packet of another protocol. GRE enables the support of protocols not normally supported by a network.

2.5.5.1 Tunnel 1

To access this page, click **Networking > GRE > Tunnel 1**.

GRE Tunnel 1

GRE Enabled Disabled

Description

Remote IP Address

Remote Subnet

Remote Subnet Mask

Local Interface IP Address

Remote Interface IP Address

Multicasts Enabled Disabled

Pre-shared Key (1 - 4294967295)

Submit

Figure 2.18 Networking > GRE > Tunnel 1.

The following table describes the items in the previous figure.

Item	Description
------	-------------

GRE	Click to enable or disable the GRE function.
Description	Enter a string to describe the tunnel entry
Remote IP Address	Enter the IP address of the remote network to establish the tunnel with the device.
Remote Subnet	Enter the subnet of the assigned remote IP address endpoint.
Remote Subnet Mask	Enter the subnet mask of the assigned remote IP address endpoint.
Local Interface IP Address	Enter the IP address of the local IP address to designate as the tunnel endpoint.
Remote Interface IP Address	Enter the IP address of the remote IP address to designate as the tunnel endpoint.
Multicasts	Click to enable or disable the multicast function.
Pre-Shared Key	Enter a value to define the security key. Value: 1 to 4294967295.
Submit	Click Submit to save the values and update the screen.

2.5.5.2 Tunnel 2

For further information regarding the configuration of the GRE Tunnel function see “Tunnel 1” on page 26.

2.5.5.3 Tunnel 3

For further information regarding the configuration of the GRE Tunnel function see “Tunnel 1” on page 26.

2.5.5.4 Tunnel 4

For further information regarding the configuration of the GRE Tunnel function see “Tunnel 1” on page 26.

2.5.6 QoS Settings

2.5.6.1 QoS Settings

To access this page, click **Networking > QoS Settings > QoS Settings**

Figure 2.19 Networking > QoS Settings> QoS Settings.

The following table describes the items in the previous figure.

Item	Description
QoS	Click the radio button to enable or disable the QoS policy on the selected interface.
Download Speed (kbit/s)	Enter the value (kbit/s) to define the download speed of the policy: 1024 to 102400, default: 85000).
Upload Speed (kbit/s)	Enter the value (kbit/s) to define the upload speed of the policy: 1024 to 102400, default: 10000).
Submit	Click Submit to save the values and update the screen.

2.5.6.2 QoS IP Base Rules

To access this page, click **Networking > QoS Settings> QoS IP Base Rules.**

Figure 2.20 Networking > QoS Settings> QoS IP Base Rules.

The following table describes the items in the previous figure.

Item	Description
Field	Click the drop-down menu to classify the traffic type for the rule.
IP Address	Enter the IP address to bind to the rule.
Priority	Click the drop-down menu to set the priority for the rule. Value: Low, Normal, Medium, or High.
Delete	Click Delete to remove the selected rule.
Add	Click Add to include the selected rule.
Submit	Click Submit to save the values and update the screen.

2.5.6.3 QoS Protocol Base Rules

To access this page, click **Networking > QoS Settings> QoS Protocol Base Rules**.

Protocol	Source Port	Destination Port	Priority	Delete
UDP	80	5000	Medium	Delete
TCP			High	Delete

Add Submit

Figure 2.21 Networking > QoS Settings> QoS Protocol Base Rules.

The following table describes the items in the previous figure.

Item	Description
Protocol	Click the drop-down menu to select the protocol type. Value: UDP, TCP.
Source Port	Enter the port value for the source endpoint.
Destination Port	Enter the port value for the destination endpoint.
Priority	Click the drop-down menu to set the priority for the rule. Value: Low, Normal, Medium, or High.
Delete	Click Delete to remove the selected rule.
Add	Click Add to include the selected rule.
Submit	Click Submit to save the values and update the screen.

2.5.7 VRRP

VRRP is an abbreviation for "Virtual Router Redundancy Protocol", the primary goal of VRRP is to ensure high network availability. If the active router fails or becomes unavailable, VRRP automatically switches over to a standby router to ensure uninterrupted network connectivity. This is achieved by sharing a virtual IP address and virtual MAC address, making it appear as if there is only one router to external devices during the switchover.

To access this page, click **Networking > VRRP**

Figure 2.21 Networking > VRRP.

The following table describes the items in the previous figure.

Item	Description
VRRP	Click the radio button to enable or disable the VRRP
Protocol Version	Click the drop-down menu to set version for VRRP. Value VRRPv2 or VRRPv3
Virtual Server IP Address	Enter the IP address of the virtual server IP to establish the VRRP with the device.
Virtual Server ID	Enter the Virtual Server ID for VRRP . Value 1-255
Host Priority	Enter the Host Priority for VRRP . Value 1-255

2.5.8 IPSEC VPN

An IPsec (Internet Protocol Security) VPN is a network protocol and technology used to establish secure, encrypted Virtual Private Networks (VPNs). Its primary purpose is to protect data transmitted over the Internet or public networks through encryption and authentication mechanisms.

2.5.8.1 Tunnel 1

To access this page, click **Networking > IPSEC VPN > Tunnel 1**

IPSEC VPN 1

Tunnel 1 Enabled Disabled

Description

Host IP Mode

Remote IP Address

Tunnel IP Mode

Remote ID

Remote Subnet

Remote Subnet Mask

Protocol/Port

Local ID

Local Subnet

Local Subnet Mask

Local Protocol/Port

Encapsulation Mode

Force NAT Traversal

IKE Protocol

IKE Mode

IKE Algorithm

IKE Encryption

IKE Hash

IKE DH Group

IKE Reauthentication

XAUTH Enabled

XAUTH Mode

XAUTH Username

XAUTH Password

ESP Algorithm

ESP Encryption

ESP Hash

PFS Enabled Disabled

PFS DH Group	<input type="text" value="2"/>	
Key Lifetime	<input type="text"/>	sec (1 - 86400)
IKE Lifetime	<input type="text"/>	sec (1 - 86400)
Rekey Margin	<input type="text"/>	sec (1 - 86400)
Rekey Fuzz	<input type="text" value="100"/>	% (0 - 200)
DPD Delay	<input type="text"/>	sec (1 - 3600)
DPD Timeout	<input type="text"/>	sec (1 - 3600)
Authenticate Mode	<input type="text" value="Pre-shared Key"/>	
Pre-shared Key	<input type="text"/>	
CA Certificate	<input type="button" value="Choose File"/> No fil...osen	
Remote Certificate / PubKey	<input type="button" value="Choose File"/> No fil...osen	
Local Certificate / PubKey	<input type="button" value="Choose File"/> No fil...osen	
Local Private Key	<input type="button" value="Choose File"/> No fil...osen	
Local Passphrase	<input type="text"/>	
Debug	<input type="text" value="Control"/>	
	<input type="button" value="Submit"/>	

Figure 2.22 Networking > IPSEC VPN > Tunnel 1

The following table describes the items in the previous figure.

Item	Description
Tunnel 1	Click to enable or disable the tunnel.
Description	
Host IP Mode	
Remote IP Address	
Tunnel IP Mode	
Remote ID	
Remote Subnet	
Remote Subnet Mask	
Protocol/Port	
Local ID	
Local Subnet	
Local Subnet Mask	
Local Protocol/Port	
Encapsulation Mode	
Force NAT Traversal	
IKE Protocol	

IKE Mode	
IKE Algorithm	
IKE Encryption	
IKE Hash	
IKE DH Group	
IKE Reauthentication	
XAUTH Enabled	
XAUTH Mode	
XAUTH Username	
XAUTH Password	
ESP Algorithm	
ESP Encryption	
ESP Hash	
PFS	
PFS DH Group	
Key Lifetime	
IKE Lifetime	
Rekey Margin	
Rekey Fuzz	
DPD Delay	
DPD Timeout	
Authenticate Mode	
Pre-shared Key	
CA Certificate	Click Choose File to browse and select a certificate.
Remote Certificate / PubKey	Click Choose File to browse and select a file containing the remote certificate.
Local Certificate / PubKey	Click Choose File to browse and select a file containing the local certificate.
Local Private Key	Click Choose File to browse and select a file containing a designated private key.
Local Passphrase	
Debug	

2.5.8.2 Tunnel 2

For further information regarding the configuration of the IPSEC VPN Tunnel function see “Tunnel 1” on page 30.

2.5.8.3 Tunnel 3

For further information regarding the configuration of the IPSEC VPN Tunnel function see “Tunnel 1”

on page 30.

2.5.8.4 Tunnel 4

For further information regarding the configuration of the IPSEC VPN Tunnel function see “Tunnel 1” on page 30.

2.6 System Management

2.6.1 Password Manager

To access this page, click **System Management > Password Manage**

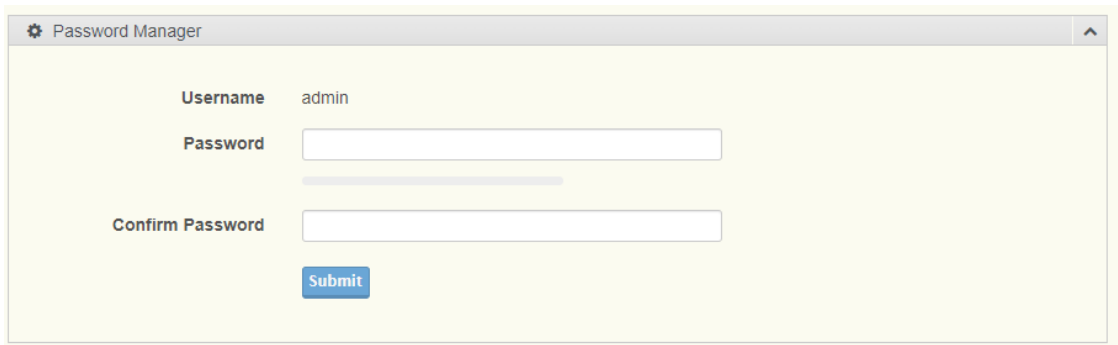


Figure 2.23 System Management > Password Manage

The following table describes the items in the previous figure.

Item	Description
Password Manager	
Username	Displays the current user name.
Password	Enter the character set for the define password type.
Confirm Password	Retype the password entry to confirm the profile password.
Submit	Click Submit to save the values and update the screen

2.6.2 Syslog

Users can enable the syslog function to record log events or messages locally or on a remote syslog server.

To access this page, click **System Management > Syslog**.

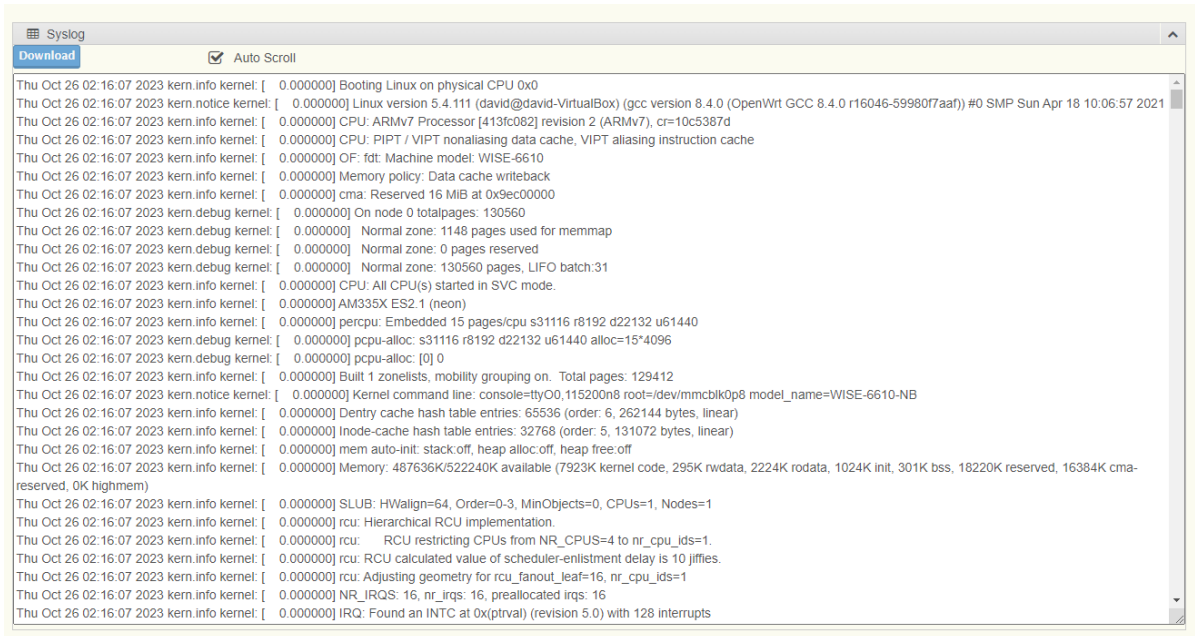


Figure 2.23 System Management > Syslog

The following table describes the items in the previous figure.

Item	Description
Download	Click Download to download the log file.
Auto Scroll	Click the checkbox to enable the Auto Scroll function.

2.6.3 NTP/Time

To access this page, click **System Management > NTP/Time**

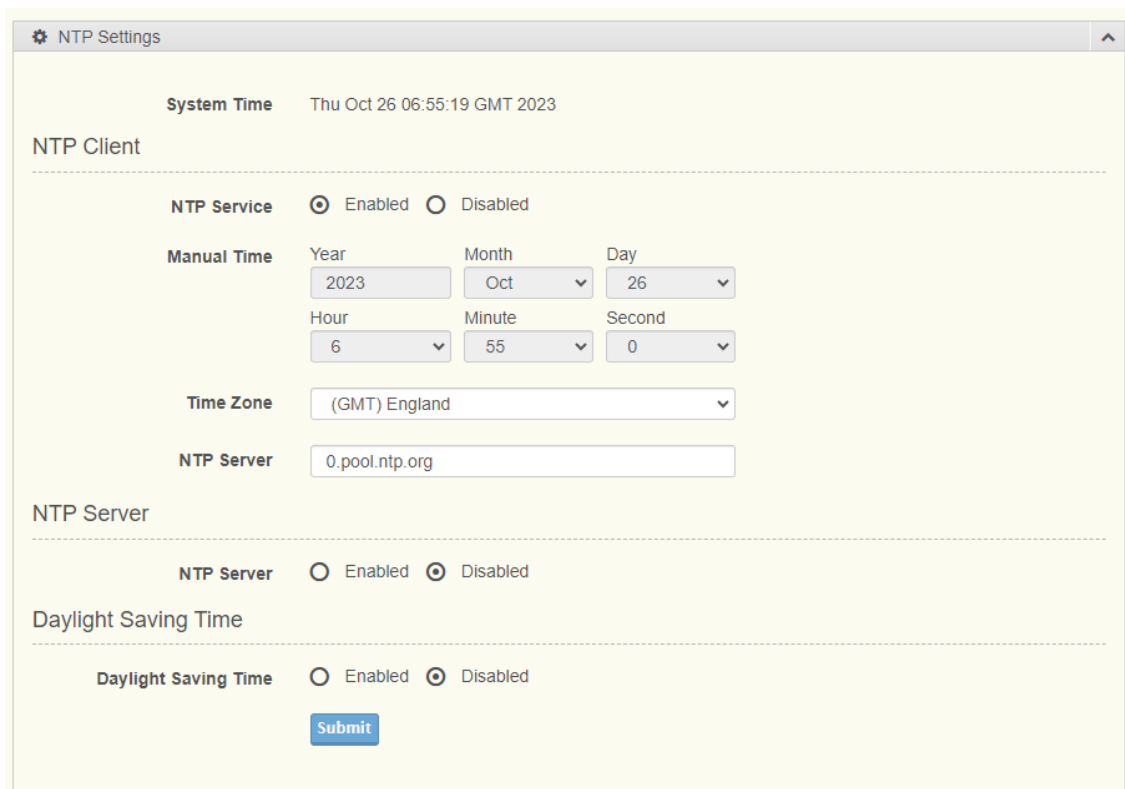


Figure 2.23 System Management > NTP/Time

The following table describes the items in the previous figure.

Item	Description
System Time	Displays the system date and time.
NTP Client	
NTP Service	Click to enable or disable the NTP Service , include NTP Server.
Manual Time	Set the system date and time.
Time Zone	Click the drop-down menu to select a system time zone.
NTP Server	Enter the address of the NTP server.
NTP Server	
NTP Server	Click to enable or disable the NTP Server.
Daylight Saving Time	
Daylight Saving Time	Click to enable or disable the Daylight Saving Time.

2.6.4 SNMP

To access this page, click **System Management > SNMP**

The screenshot displays the configuration interface for SNMP, organized into three sections:

- SNMP System Settings:**
 - SNMP: Enabled Disabled
 - Contact:
 - Name:
 - Location:
 - Description:
- SNMP Daemon Settings:**
 - Version:
 - Server Port:
 - Read Community:
 - Write Community:
- SNMP Trap Settings:**
 - Version:
 - Trap Server IP:
 - Trap Server Port:
 - Trap Community:

A **Submit** button is located at the bottom of the form.

Figure 2.24 System Management > SNMP

The following table describes the items in the previous figure.

Item	Description
SNMP System	
Settings	
SNMP	Click to enable or disable the SNMP Service.
Contact	Enter the string to define the sysContact for SNMP. The default is Advantech@advantech.com.tw.
Name	Enter the string to define the sysName for SNMP. The default is Advantech.
Location	Enter the string to define the sysLocation for SNMP. The default is tw.
SNMP Daemon	
Settings	
Version	Click the drop-down menu to select the version for SNMP Service: V1, V2 or V3 .
Server Port	Enter the port address of the SNMP server
Read Community	Enter the string to define the Read Community for SNMP. The default is public.
Write Community	Enter the string to define the Write Community for SNMP. The default is private.
SNMP Trap Settings	
Version	Click the drop-down menu to select the version for SNMP trap: V1 or V2 .
Trap Server IP	Enter the IP address of the SNMP Trap server
Trap Server Port	Enter the port address of the SNMP Trap server.
Trap Community	Enter the string to define the Trap Community for SNMP Trap. The default is public.

2.6.5 Network Access

To access this page, click **System Management > Network Access**

Figure 2.25 System Management > Network Access

The following table describes the items in the previous figure.

Item	Description
HTTP	
Redirect HTTP Requests to HTTPS	Click to enable or disable the redirect to HTTP function
HTTPS Port	Enter the port number for the assigned remote HTTPS address.
HTTP Port	Enter the port number for the assigned remote HTTP address
SSH	
SSH	Click to enable or disable the SSH function.
Telnet	
Telnet	Click to enable or disable the Telnet function.
Submit	Click Submit to save the values and update the screen.

2.6.6 Configuration Manager

To access this page, click **System Management > Configuration Manager**.

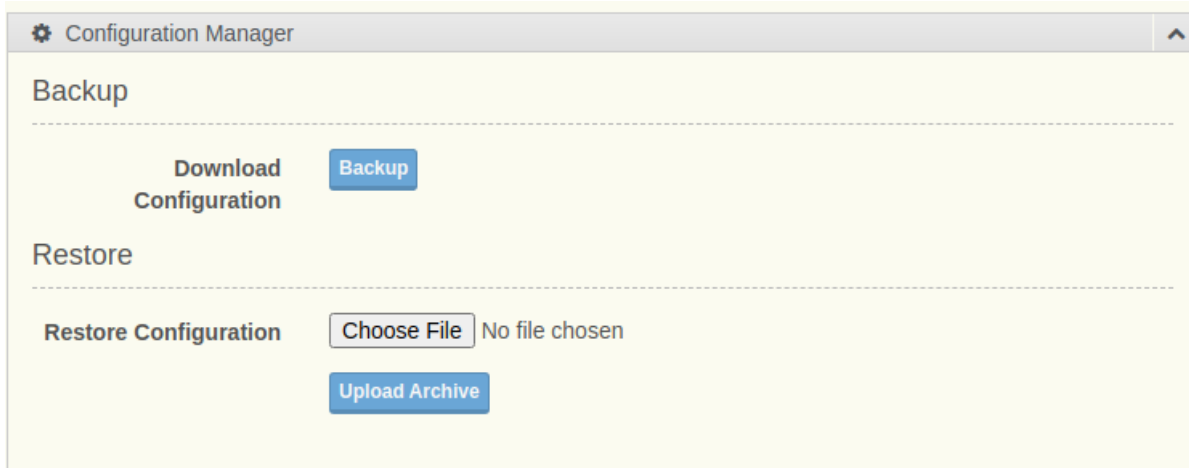


Figure 2.26 System Management > Configuration Manager.

The following table describes the items in the previous figure.

Item	Description
Backup	
Download Configuration	Click Backup to backup the device settings
Restore	
Choose File	Click Choose File to select the configuration file
Upload Archive	Click Upload Archive to restore the configuration to the device.

2.6.7 Firmware Upgrade

To access this page, click **System Management > Firmware Upgrade**.

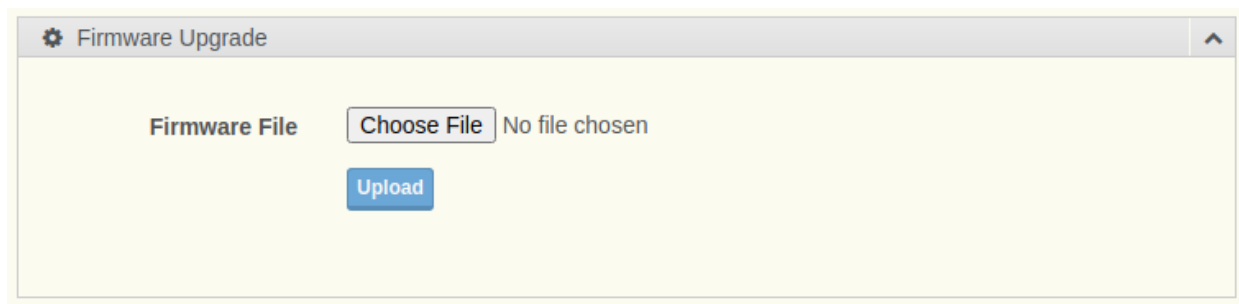


Figure 2.27 System Management > Firmware Upgrade.

The following table describes the items in the previous figure.

Item	Description
Upgrade Manager	Click Choose File to select the configuration file
Upload	Click Upload to upload to the current version.

2.6.8 Reset System

To access this page, click **System Management > Reset System**.



Figure 2.28 System Management > Reset System.

The following table describes the items in the previous figure.

Item	Description
Reset to Defaults	Click Reset of Reset to Defaults to have all configuration parameters reset to their factory default values. All changes that have been made will be lost, even if you have issued a save.
Factory Reset	"Click 'Reset to Factory' to reset all configuration parameters, including LoRaWAN Service configuration, node-red, and IPK Management , to their factory default values. All changes that have been made will be lost, even if you have saved them."

2.6.9 Reboot Device

To access this page, click **System Management > Reboot Device**.



Figure 2.29 System Management > Reboot Device.

The following table describes the items in the previous figure.

Item	Description
Reboot	Click Reboot to reboot device.

2.6.10 Apply Configuration

To access this page, click **System Management > Apply Configuration**.

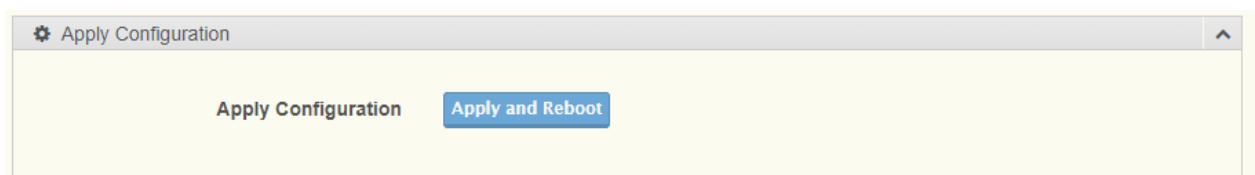


Figure 2.30 System Management > Apply Configuration.

The following table describes the items in the previous figure.

Item	Description
Apply Configuration	Click Apply and Reboot to have configuration changes you have made to be saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.

2.7 Application Tools

2.7.1 Custom Script

To access this page, click **Application Tools > Custom Script**.

The screenshot displays the 'Custom Script' configuration interface. At the top, there is a title bar with a gear icon and the text 'Custom Script'. Below this is a table with five columns: 'File', 'Description', 'Edit', 'Test', and 'Startup'. The table contains five rows, each representing a script. The first row, 'Script 1', has a description of 'test'. The other four rows, 'Script 2' through 'Script 5', have a description of 'write description here'. Each row has an 'Edit' button, a 'Test' button, and a checkbox in the 'Startup' column. Below the table, there is a section titled 'Script Edit Box : Script 1' which contains a text area with the content 'echo "test script"'. The interface has a light yellow background and a thin border.

File	Description	Edit	Test	Startup
Script 1	test	Edit	Test	<input type="checkbox"/>
Script 2	write description here	Edit	Test	<input type="checkbox"/>
Script 3	write description here	Edit	Test	<input type="checkbox"/>
Script 4	write description here	Edit	Test	<input type="checkbox"/>
Script 5	write description here	Edit	Test	<input type="checkbox"/>

Script Edit Box : Script 1

```
echo "test script"
```



Figure 2.31 Application Tools> Custom Script.

The following table describes the items in the previous figure.

Item	Description
File	Index of custom script.
Description	Description of this custom script.
Edit	Click Edit to edit custom script on Script Edit Box.
Test	Click Test to test custom script , result will show on Script Output Box.
Startup	Run custom script on system boot

2.7.2 MQTT

To access this page, click **Application Tools> MQTT**.

Figure 2.32 Application Tools> MQTT.

The following table describes the items in the previous figure.

Item	Description
MQTT Broker	
Broker	Click to enable or disable the MQTT Broker.
Broker Port	Enter the port number of the MQTT Broke.
MQTT Bridge	
Bridge	Click to enable or disable the MQTT Bridge.
Bridge Port	Enter the port number of the MQTT Bridge server.
Bridge TLS	Click to enable or disable the TLS for MQTT Bridge server.
Try Private	Click to enable or disable the Try Private. If Try Private is set to enabled, the bridge will attempt to indicate to the remote broker that it is a bridge not an ordinary client. If successful, this means that loop detection will be more effective and that retained messages will be propagated correctly. Not all brokers support this

	feature so it may be necessary to set Try Private to false if your bridge does not connect properly.
Bridge Address	Enter the IP address or URL of the MQTT Bridge server.
Bridge User	Enter the string to define a username for MQTT Bridge server.
Bridge Password	Enter the string to define a password for MQTT Bridge server.
Bridge Client ID	Enter the string to define a MQTT Client ID for MQTT Bridge session.
CA Certificate	Click Choose File to browse and select a CA certificate.
Certificate	Click Choose File to browse and select a certificate.
Key	Click Choose File to browse and select a file containing a designated private key.

2.7.2 Node-RED

2.7.2.1 Settings

To access this page, click **Application Tools> Node-RED >Setting**.

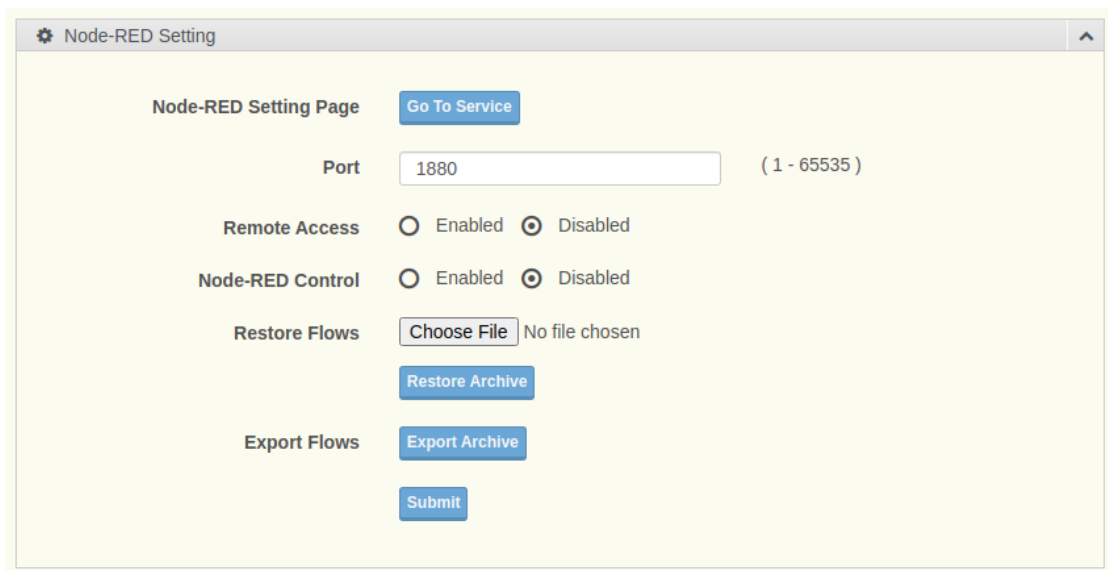


Figure 2.33 Application Tools> Node-RED >Setting.

The following table describes the items in the previous figure.

Item	Description
Node-RED	Click Go To Service to redirect Node-RED WEB
Port	Enter the port number of the Node-RED.
Remote Access	Click to enable or disable the Node-RED access from WAN side.
Node-RED Control	Click to enable or disable the Node-RED.
Restore Flows	Click Choose File to browse and select a Node-RED Flows file.
Restore Archive	Click Restore Archive to upload Node-RED Flows file to Node-RED service.
Export Flows	Click Export Archive to download Node-RED Flows file.

2.7.2.1 Library

To access this page, click **Application Tools > Node-RED > Library**.

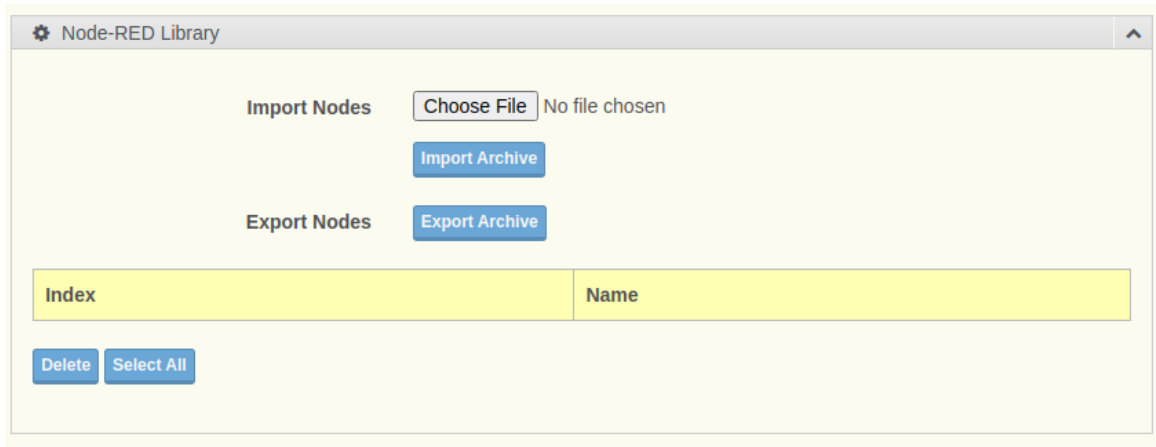


Figure 2.34 Application Tools > Node-RED > Library.

The following table describes the items in the previous figure.

Item	Description
Import Nodes	Click Choose File to browse and select a nodes file.
Import Archive	Click Import Archive to upload nodes library to Node-RED service.
Export Nodes	Click Export Archive to download nodes library.
Delete	Delete selected nodes library.
Select All	Select all imported nodes library.

2.7 Diagnostics Tools

To access this page, click **Diagnostics Tools**.

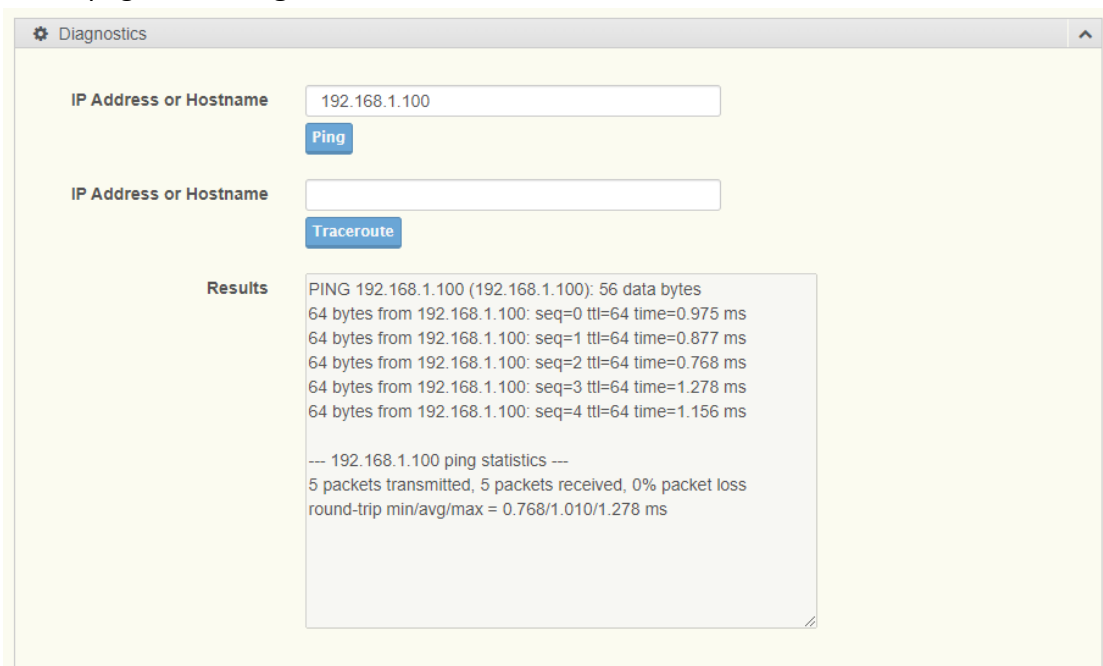


Figure 2.35 Diagnostics Tools.

The following table describes the items in the previous figure.

Item	Description
IP Address or Hostname	Enter the IP address or hostname of a device on the network to execute a ping test. Click Ping to initiate and display the ping result for the device.
IP Address or Hostname	Enter the IP address or hostname of the host to initiate a trace route from the switch to the defined host. Click Traceroute to initiate and display the trace results.
Results	Displays the results of the Ping or Traceroute test.

2.8 IPK Management

To access this page, click **IPK Mangement**.

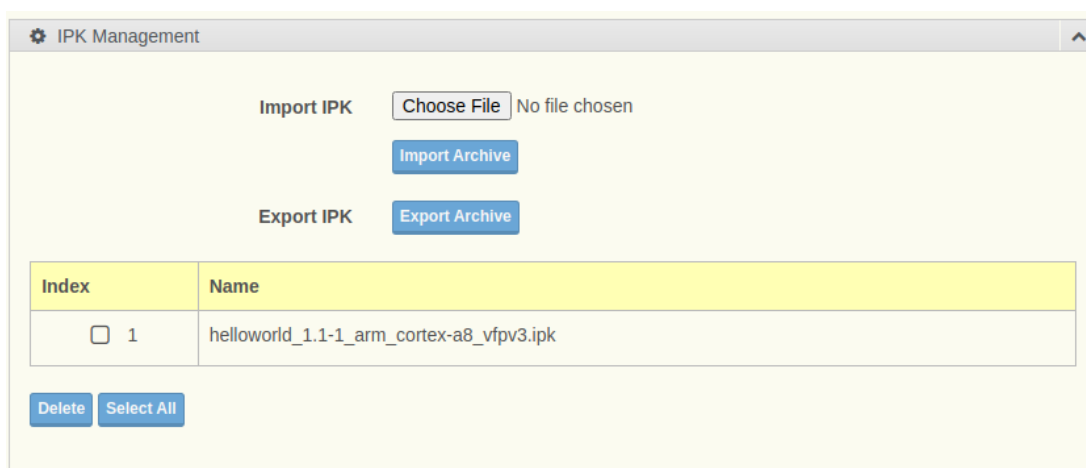


Figure 2.36 IPK Mangement.

The following table describes the items in the previous figure.

Item	Description
Import IPK	Click Choose File to browse and select a IPK file.
Import Archive	Click Import Archive to upload IPK.
Export IPK	Click Export Archive to IPK.
Delete	Delete selected IPK.
Select All	Select all imported IPK.