User Manual
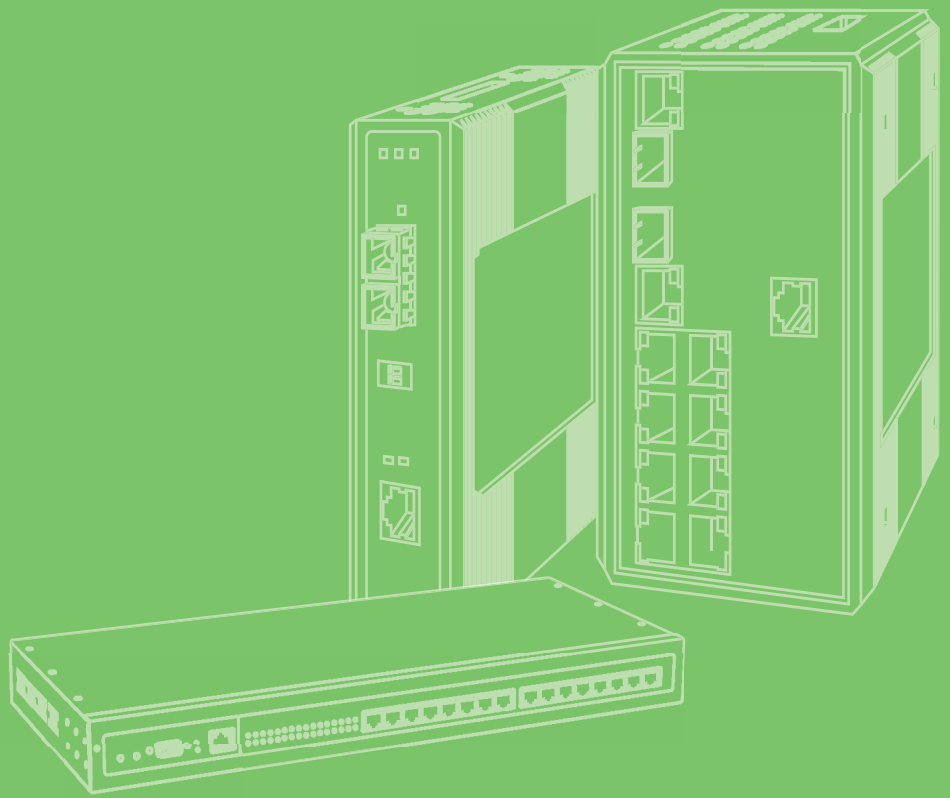
WISE-6610 Series

Industrial LoRaWAN Gateway

ADVANTECH

Enabling an Intelligent Planet

Copyright

Acknowledgements

Intel and Pentium are trademarks of Intel Corporation.

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.

All other product names or trademarks are properties of their respective owners.

Product Warranty (3 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for three years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For out of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any on screen messages you get when the problem occurs.

2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.

3. If your product is diagnosed as defective, obtain an RMA (return merchandize authorization) number from your dealer. This allows us to process your return more quickly.

4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.

5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class A

Note: 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.

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.

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.

NCC

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。

減少電磁波影響，請妥適使用

此為甲類資訊技術設備，於居住環境中使用時，可能會造成射頻擾動，在此種情況下使用者會被要求採取某些適當的對策。

Technical Support and Assistance

1. Visit the Advantech web site at www.advantech.com/support where you can find the latest information about the product.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
   - Product name and serial number
   - Description of your peripheral attachments

– Description of your software (operating system, version, application software, etc.)
– A complete description of the problem
– The exact wording of any error messages

Warnings, Cautions and Notes

Warning! *Warnings indicate conditions, which if not observed, can cause personal injury!*

Caution! *Cautions are included to help you avoid damaging hardware or losing data. e.g.*

There is a danger of a new battery exploding if it is incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Note! *Notes provide optional additional information.*

Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to: support@advant-ech.com

Packing List

Before setting up the system, check that the items listed below are included and in good condition. If any item does not accord with the table, please contact your dealer immediately.

■ 1 x Indsutrial LoRaWAN gateway
■ 1 x DIN-Rail mounting bracket and screws

Safety Instructions

- Read these safety instructions carefully.
- Keep this User Manual for later reference.
- Disconnect this equipment from any DC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
- For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
- Keep this equipment away from humidity.
- Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
- The openings on the enclosure are for air convection. Protect the equipment from overheating. DO NOT COVER THE OPENINGS.
- Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
- Position the power cord so that people cannot step on it. Do not place anything over the power cord.
- All cautions and warnings on the equipment should be noted.
- If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.
- Never pour any liquid into an opening. This may cause fire or electrical shock.
- Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
- If one of the following situations arises, get the equipment checked by service personnel:
  – The power cord or plug is damaged.
  – Liquid has penetrated into the equipment.
  – The equipment has been exposed to moisture.
  – The equipment does not work well, or you cannot get it to work according to the user's manual.
  – The equipment has been dropped and damaged.
  – The equipment has obvious signs of breakage.
- DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO -40°C (-40°F) ~ 85°C (185°F). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.
- The sound pressure level at the operator's position according to IEC 704-1:1982 is no more than 70 dB (A).
  DISCLAIMER: This set of instructions is given according to IEC 704-1. Advantech disclaims all responsibility for the accuracy of any statements contained herein.
- The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Wichtige Sicherheishinweise

- Bitte lesen sie Sich diese Hinweise sorgfältig durch.
- Heben Sie diese Anleitung für den späteren Gebrauch auf.
- Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie Keine Flüssig-oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
- Die NetzanschluBsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
- Das Gerät ist vor Feuchtigkeit zu schützen.
- Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen.
- Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor über-hitzung schützt. Sorgen Sie dafür, daB diese Öffnungen nicht abgedeckt werden.
- Beachten Sie beim. AnschluB an das Stromnetz die AnschluBwerte.
- Verlegen Sie die NetzanschluBleitung so, daB niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
- Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
- Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
- Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag aus-lösen.
- Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
- Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
  – Netzkabel oder Netzstecker sind beschädigt.
  – Flüssigkeit ist in das Gerät eingedrungen.
  – Das Gerät war Feuchtigkeit ausgesetzt.
  – Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
  – Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
  – Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
- Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70dB(A) oder weiger.

  Haftungsausschluss: Die Bedienungsanleitungen wurden entsprechend der IEC-704-1 erstellt. Advantech lehnt jegliche Verantwortung für die Richtigkeit der in diesem Zusammenhang getätigten Aussagen ab.

Safety Precaution - Static Electricity

Static electricity can cause bodily harm or damage electronic devices. To avoid damage, keep static-sensitive devices in the static-protective packaging until the installation period. The following guidelines are also recommended:

■ Wear a grounded wrist or ankle strap and use gloves to prevent direct contact to the device before servicing the device. Avoid nylon gloves or work clothes, which tend to build up a charge.

■ Always disconnect the power from the device before servicing it.

■ Before plugging a cable into any port, discharge the voltage stored on the cable by touching the electrical contacts to the ground surface.

Safety Precaution - Battery Installation

Danger of explosion if battery is incorrectly replaced.

■ Replace only with the same or equivalent type recommended by the manufacturer, discard used batteries according to the manufacturer's instructions.

Restricted Access - Installation Requirement

The equipment should only be installed in a Restricted Access Area.

Contents

Chapter   4   Configuration in Typical Situations .75

List of Figures

Chapter 1

Product Overview

1.1 Specifications

Specifications	Description	
WSN Support		
	Standard	LoRaWAN
	Frequency	WISE-6610-NXXX-A 915Mhz WISE-6610-EXXX-A 868Mhz WISE-6610-AXXX-A 923Mhz
	ANT Connector	SMA Male Reverse connector x 1
LAN Interface		
	Ethernet	10/100 Mbps, auto MDI/MDIX
	Connector	RJ45 x 1
	Protection	1.5-kV built-in magnetic isolation protection
Digital I/O		
	Port Type	Digital input on voltage: 2.7 ~ 36 V_{DC}
	Port Connector	4-way Molex mini-fit connector
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 tunneling	Open VPN client and server and P2P, L2TP, PPTP, GRE, EasyVPN, IPSec with IKEv1 and IKEv2
Cellular Interface (WISE-6610-EXXXC-A/WISE-6610-AXXXC-A only)		
	LTE Bit rate	150 Mbps (DL), 50 Mbps (UL)
	LTE Bands	B20 (800 MHz), B8 (900 MHz), B3 (1800 MHz), B1 (2100 MHz), B7 (2600 MHz)
	3G Bit rate	42.0 Mbps (DL), 5.76 Mbps (UL)
	3G Bands	900, 2100 MHz
	No. of SIM Slots	2 x Mini SIMs (2FF)
	ANT Connector	2 x RP-SMA female connectors
Cellular Interface (WISE-6610-NXXXC-A Only)		

Specifications	Description
	LTE	Cat M1
	LTE Bit rate	375 Kbps (DL), 375 Kbps (UL)
	LTE FDD	B12, B13, B28 (700 MHz), B20 (800 MHz), B5, B18, B19, B26 (850 MHz), B8 (900 MHz), B4 (1700 MHz), B3 (1800 MHz), B2 (1900 MHz), B1 (2100MHz)
	LTE TDD	B39 (1900 MHz)
Physical		
	Protection Class	IP30
	Mounting	DIN rail, wall
	Dimensions (W x H x D)	150 x 37.5 x 83 mm (5.9" x 1.48" x 3.27")
	Weight	500 g (17.63 oz)
Environment		
	Operating Temperature	-40 ~ 75°C (-40 ~ 167°F)
	Storage Temperature	-40 ~ 85°C (-40 ~ 185°F)
	Operating Humidity	10 ~ 95% (non-condensing)
Power		
	Power Input	9 ~ 36 V_{DC}
	Power Connector	4-way Molex moni-fit connector
	Power Consumption	3.1/6.6/40 mW (average/peak/sleep mode)
Certifications		
	EMC	■ EN61000-4-2, Level 3 ■ EN61000-4-3, Level 3 ■ EN61000-4-4, Level 3 ■ EN61000-4-5, Level 3 ■ EN61000-4-6, Level 3 ■ EN61000-4-12, Level 3 ■ EN61000-4-11, voltage dip: 70%
	Shock	IEC60068-2-27
	Free Fall	IEC60068-2-32
	Vibration	IEC60068-2-6

1.2 Hardware Views

1.2.1 Front View
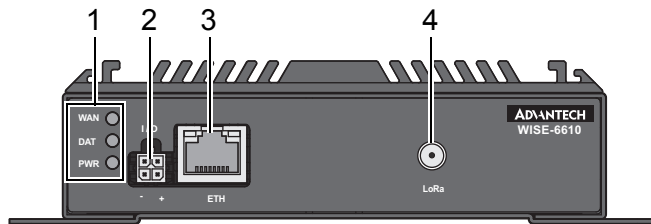
Figure 1.1 WISE-6610-XXXX-A Front View

No.	Item	Description
1	System LED panel	See "System LED Panel" on page 5 for further details.
2	I/O (Power socket)	Connect cabling for power.
3	ETH port	RJ45 x 1
4	Antenna connector	Connector for LoRa antenna.
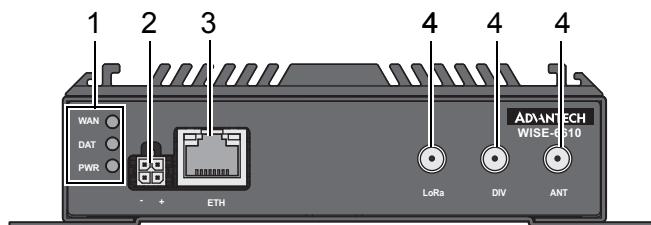
Figure 1.2 WISE-6610-XXXXC-A Front View

No.	Item	Description
1	System LED panel	See "System LED Panel" on page 5 for further details.
2	I/O (Power socket)	Connect cabling for power.
3	ETH port	RJ45 x 1
4	Antenna connector	Connector for antenna, from left to right: LoRa, DIV, ANT

1.2.2 Rear View
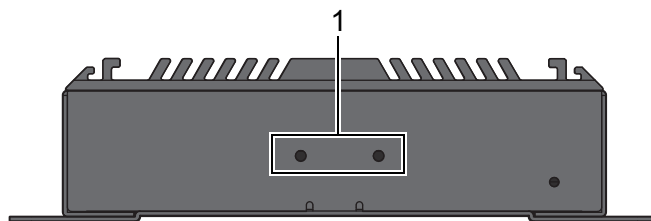
Figure 1.3 WISE-6610-XXXX-A Rear View

No.	Item	Description
1	DIN-Rail holes	Screw holes (2) used in the installation of a DIN rail clip.
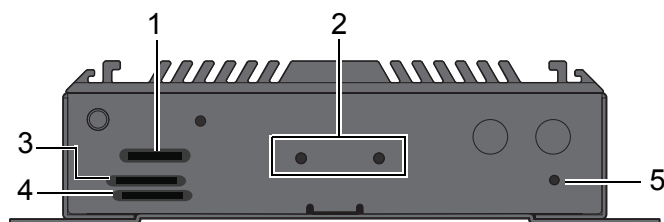
Figure 1.4 WISE-6610-XXXXC-A Rear View

No.	Item	Description
1	SD Card	Slot for SIM multimedia card.
2	DIN-Rail holes	Screw holes (2) used in the installation of a DIN rail clip.
3	SIM 2	Slot for SIM 2 smart card.
4	SIM 1	Slot for SIM 1 smart card.
5	RST	Reset button.

1.2.3 Top View
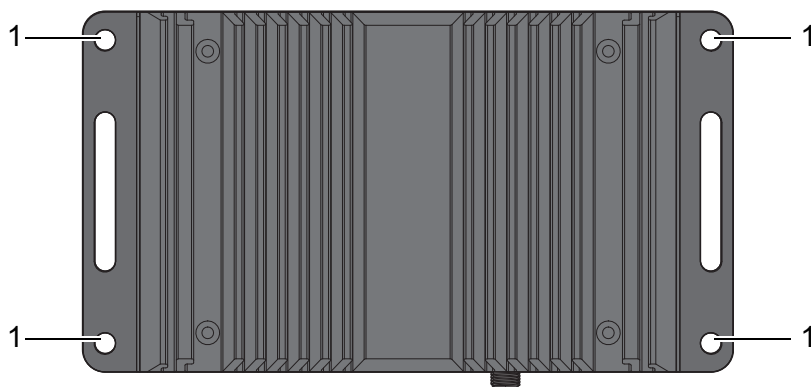
Figure 1.5 Top View

No.	Item	Description
1	Wall mounting holes	Screw holes (4) used in the installation on wall.

1.2.4 System LED Panel

LED Name	LED Color	Description
WAN*	Yellow, blinking	PPP connection established. Signal strength is from -50 dBm to -69 dBm (1x flash per sec.) Signal strength is from -70 dBm to -89 dBm or the difference between neighboring cells is exactly 3 dBm (2x flash per sec.) Signal strength is from -90 dBm to -113 dBm or difference the between neighboring cells is smaller than 3 dBm (3x flash per sec.)
DAT	Red, blinking	Communication in progress on radio channel.
PWR	Green, blinking	Device is ready.
	Green, on	Device is booting.

(*) This LED indication only functions on WISE-6610-XXXXC-A series models.

1.3 Dimensions

mm [inch]
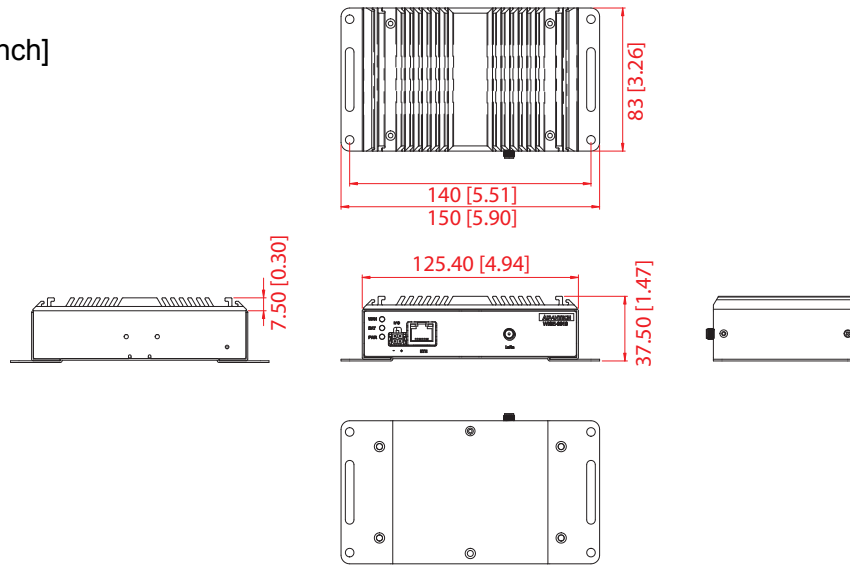
Figure 1.6 WISE-6610-XXXX-A Dimensions

mm [inch]
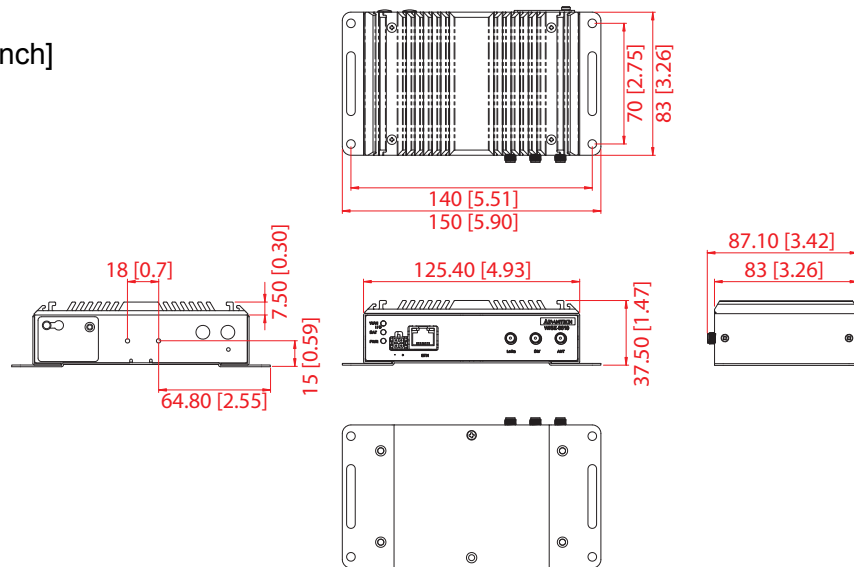
Figure 1.7 WISE-6610-XXXXC-A Dimensions

Chapter 2

Gateway Installation

2.1 Warning

Warning: Before working on equipment that is connected to power lines, remove any jewelry (including rings, necklaces, and watches). Metal objects can heat up when connected to power and ground, which can cause serious burns or weld the metal object to the terminals.

Caution! *Exposure to chemicals can degrade the sealing properties of materials used in the sealed relay device.*

Caution! *It is not recommended to work on the system or connect or disconnect cables during periods of lightning activity.*

Caution! *Before performing any of the following procedures, disconnect the power source from the DC circuit.*

Caution! *Read the installation instructions before connecting the system to its power source.*

Caution! *The device must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor.*

Caution! *The installation, replacement, or service of the device must be Only be performed by trained and qualified personnel.*

Caution! *Ultimate disposal of this product should be handled according to local and national regulations*

Caution! To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 70°C (158°F).

Caution! If the switch is to be installed in a hazardous location, ensure that the DC power source is located away from the vicinity of the switch.

Caution! The installation of the equipment must comply with all national and local electrical codes.

Caution! Explosion Hazard-The area must be known to be nonhazardous before servicing or replacing any components.

Warning! Airflow around the switch must be unrestricted. To prevent the switch from overheating, there must be the following minimum clearances:
- Top and bottom: 2.0 in. (50.8 mm)
- Sides: 2.0 in. (50.8 mm)
- Front: 2.0 in. (50.8 mm)

2.2 Installation Guideline

The following guidelines are provided to optimize the device performance. Review the guidelines before installing the device.

- Make sure cabling is away from sources of electrical noise. Radios, power lines, and fluorescent lighting fixtures can interference with the device performance.
- Make sure the cabling is positioned away from equipment that can damage the cables.
- Operating environment is within the listed range, see "Specifications" on page 2.
- Relative humidity around the switch does not exceed 95% (non-condensing).
- Altitude at the installation site is not higher than 10,000 feet.
- In 10/100 and 10/100/1000 fixed port devices, the cable length from the switch to connected devices can not exceed 100 meters (328 feet).
- Make sure airflow around the switch and respective vents is unrestricted. Without proper airflow the switch can overheat. To prevent performance degradation and damage to the switch, make sure there is clearance at the top and bottom and around the exhaust vents. Installing the Gateway.

2.2.1 Installing Antenna

Note!   *For the purpose of instructions, wherever the physical variance of the device is pertinent to the hardware installation process, a reference was provided to indicate the specific device series used. Otherwise, the illustration applies to all models.*

1. Connect the antenna by screwing the antenna connectors in a clockwise direction.
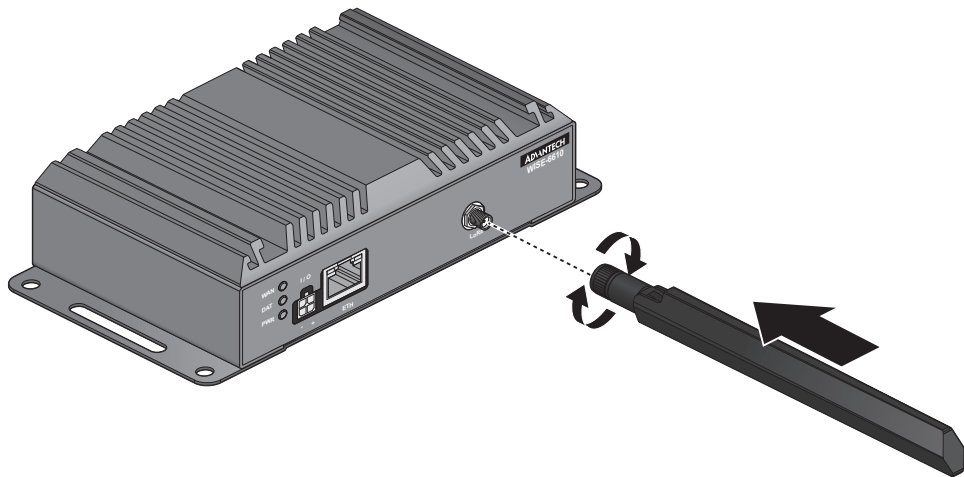
Figure 2.1 Installing the WISE-6610 Antenna
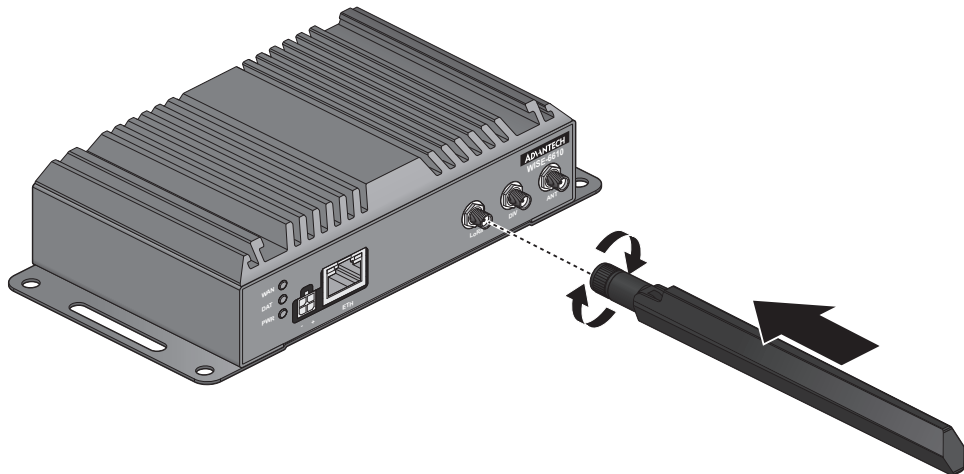
Figure 2.2 Installing the WISE-6610 LTE Antenna

2. Position the antenna for optimal signal strength.

Note! *The location and position of the antenna is crucial for effective wireless connectivity*
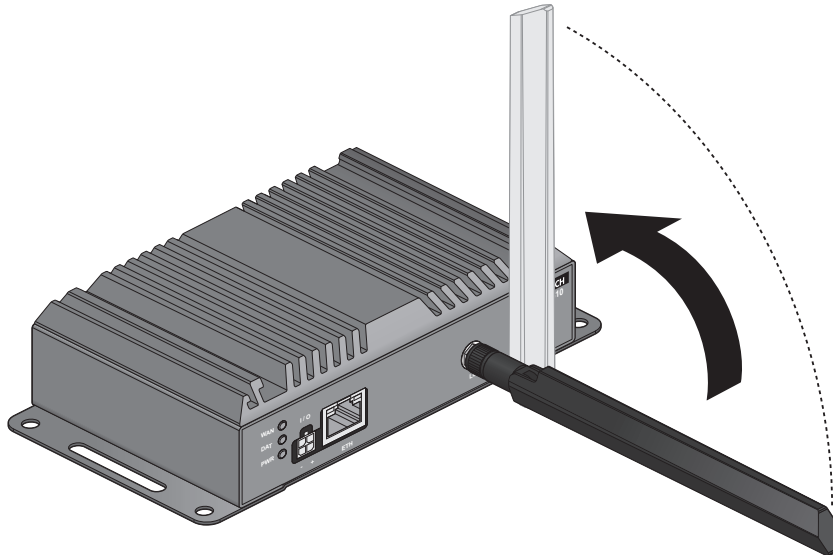
Figure 2.3 Positioning the WISE-6610 Antenna
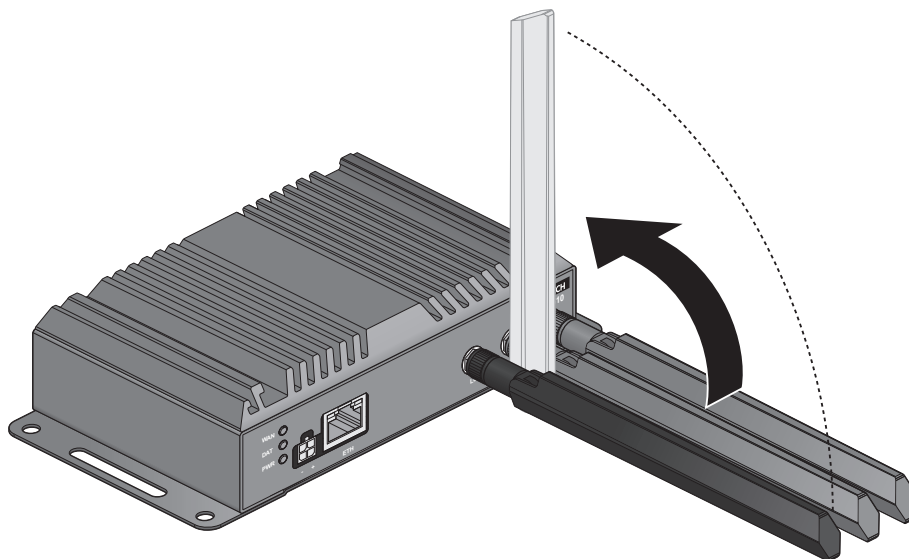
Figure 2.4 Positioning the WISE-6610 LTE Antenna

2.2.2 Wall Mounting

> **Note!**
>
> *For the purpose of instructions, wherever the physical variance of the device is pertinent to the hardware installation process, a reference was provided to indicate the specific device series used. Otherwise, the illustration applies to all models.*

1. Locate the area to install and mark the four screw locations. It is suggested to place the device on the installation location and use the mounting locations to mark the location of the screw holes).
2. If necessary first drill pilot holes. Drill four holes over the four marked locations on the wall. On concrete, it is recommended to install wall sinks
3. Align the SmartSwarm over the installation location on the wall.
4. Secure the SmartSwarm with screws (Ø 5.0 mm).
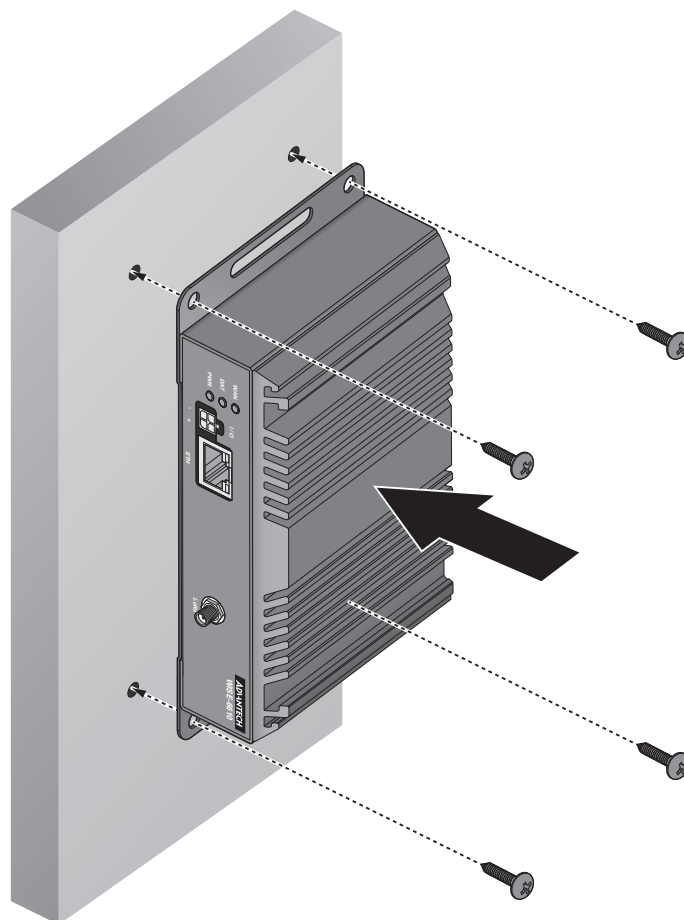
Figure 2.5 Wall Mount Installation

2.2.3 DIN Rain Mounting

2.2.3.1 Installing the DIN Rail Mounting Kit

1. Align the DIN rail clip with the rear of SmartSwarm.
2. Secure the DIN rail clip and the SmartSwarm with screws.
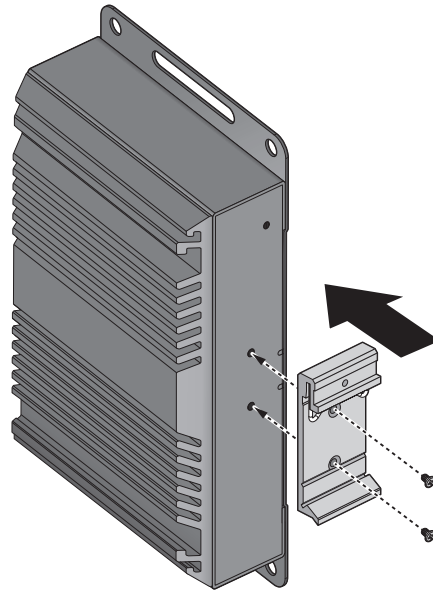
Figure 2.6 Wall Mount Installation

3. Position the rear panel of the SmartSwarm directly in front of the DIN rail, making sure that the top of the DIN rail clip hooks over the top of the DIN rail, as shown in the following illustration.

   Make sure the DIN rail is inserted behind the spring mechanism.

4. Once the DIN rail is seated correctly in the DIN rail clip, press the front of the SmartSwarm to rotate the SmartSwarm down and into the release tab on the DIN rail clip. If seated correctly, the bottom of the DIN rail should be fully inserted in the release tab.

DIN rail clip

DIN rail

DIN rail clip release tab
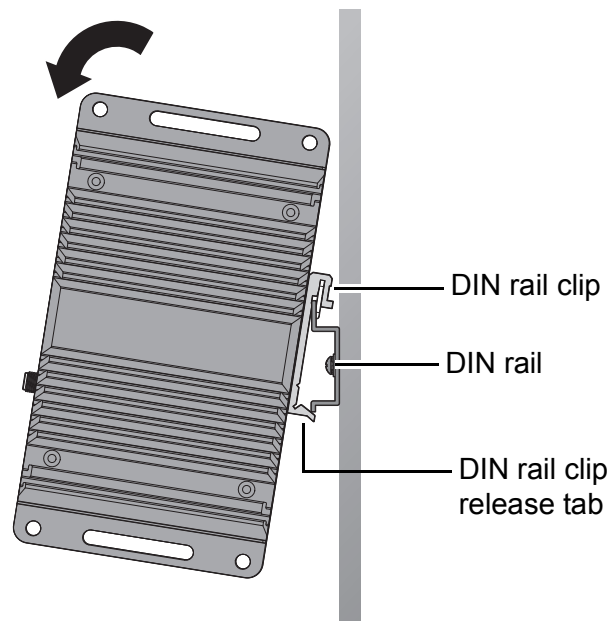
Figure 2.7 Installing the DIN-Rail Mounting Kit

See the following figure demonstrating the correct position of a completed DIN installation.
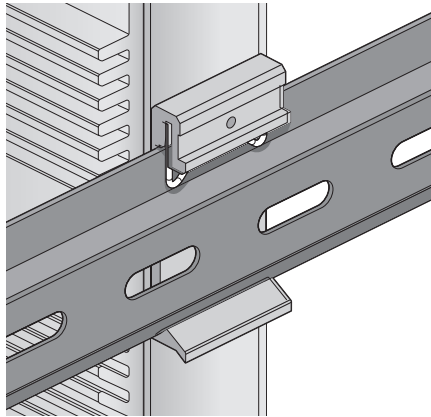
Figure 2.8 Correctly Installed DIN Rail Kit

2.2.3.2 Removing the DIN Rail Mounting Kit

1. Ensure that power is removed from the SmartSwarm, and disconnect all cables and connectors from the front panel of the SmartSwarm.
2. Push down on the top of the DIN rail clip release tab with your finger. As the clip releases, lift the bottom of the SmartSwarm, as shown in the following illustration.
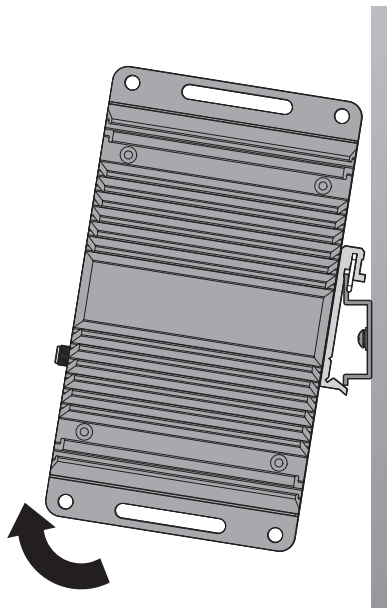
Figure 2.9 Removing the DIN-Rail

2.3 Connecting the Gateway to Ethernet Port

2.3.1 RJ45 Ethernet Cable Wiring

For RJ45 connectors, data-quality, twisted pair cabling (rated CAT5 or better) is recommended. The connector bodies on the RJ45 Ethernet ports are metallic and connected to the GND terminal. For best performance, use shielded cabling. Shielded cabling may be used to provide further protection.

Straight-thru Cable Wiring		Cross-over Cable Wiring	
Pin 1	Pin 1	Pin 1	Pin 3
Pin 2	Pin 2	Pin 2	Pin 6
Pin 3	Pin 3	Pin 3	Pin 1
Pin 6	Pin 6	Pin 6	Pin 2
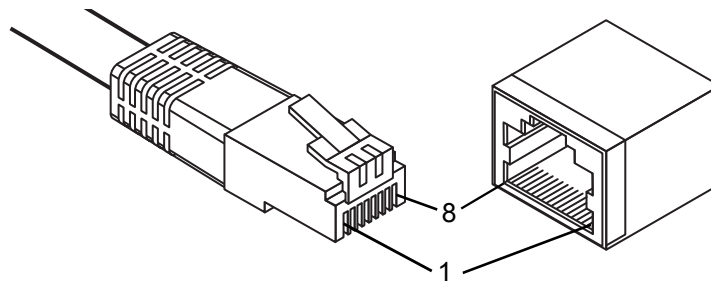
Figure 2.10 Ethernet Plug & Connector Pin Position

Maximum cable length: 100 meters (328 ft.) for 10/100BaseT.

2.4 Power Supply Installation

Note! For the purpose of instructions, wherever the physical variance of the device is pertinent to the hardware installation process, a reference was provided to indicate the specific device series used. Otherwise, the illustration applies to all models.

1. Insert the power cable into the power socket. The cable locks in place if installed correctly.
2. Connect the other end to a wall outlet.
   The LEDs light when the device is connected to the power source
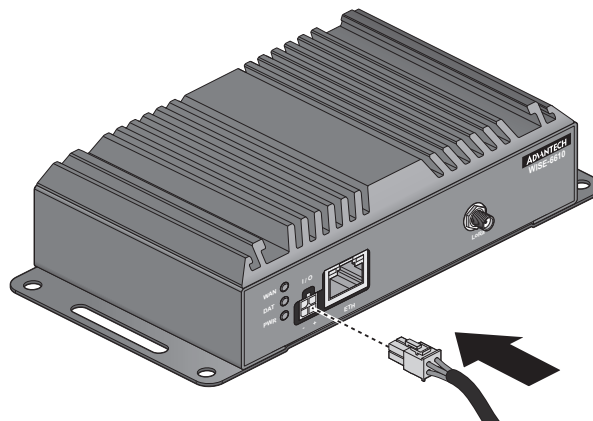
Figure 2.11 Installing the Power Cable

The following table show the color lines definition:

V+	DI	GND	D0
Red	Yellow	Black	Gray

Chapter   **3**

Managing Gateway

3.1 Access Interface

To access the login window, connect the device to the network, see "Connecting the Gateway to Ethernet Port" on page 12. When WISE-6610 Series is first installed, make sure the network environment is configured to enable access to the device. Your computer and the device must be on the same network subnet to allow them to establish a network connection.

> *Note!* *For the purpose of instructions, the user interface of a single model was used. The interface screens may not reflect your specific model.*

Before you begin, make sure the device is powered on, see "Power Supply Installation" on page 13 for further information.

1. Launch a web browser on a computer.
2. In the browser's address bar type in the default IP address (192.168.1.1). The login screen displays.
3. Enter the default user name and password (root/root) to log into the management interface. You can change the default password after a successfully log in. See "Changing Default Password" on page 19.
4. Click **Login** to enter the management interface.

Login	
Username	
Password	
	Login
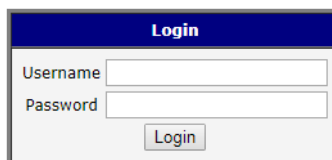
Figure 3.1 Login Screen

When you successfully enter login information on the login page, web interface will be displayed. The left side of the web interface contains a menu tree with sections for monitoring (Status), configuration (Configuration), customization (Customization) and administration (Administration) of the device.

Name and Location items in the right upper corner display the name and location of the device in the SNMP configuration (see "SNMP" on page 51). These fields are user-defined for each device.

After the green LED starts to blink you may restore the initial device settings by pressing the reset (RST) button on the back panel. If the reset button is pressed, all configuration will revert to factory defaults and the device will reboot (the green LED will be on during the reboot).

3.2 Recommended Practices

One of the easiest things to do to help increase the security posture of the network infrastructure is to implement a policy and standard for secure management. This practice is an easy way to maintain a healthy and secure network.
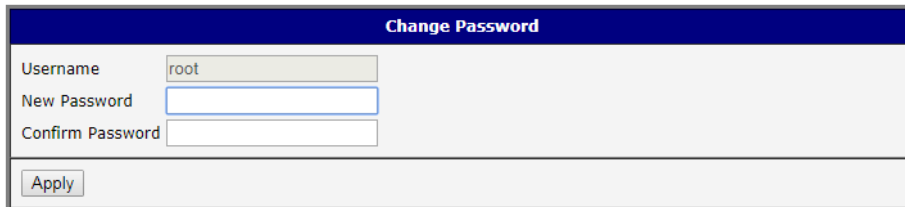
After you have performed the basic configurations on your switches, the following is a recommendation which is considered best practice policy.

3.2.1 Changing Default Password

In keeping with good management and security practices, it is recommended that you change the default password as soon as the WISE-6610 Series is functioning and setup correctly. The following details the necessary steps to change the default password.

To change the password:
1. Navigate to **Administration** > **Change Password**.
2. In the **New Password** field, type in the new password. Re-type the same password in the **Confirm Password** field.
3. Click **Apply** to change the current account settings.

Change Password	
Username	root
New Password	
Confirm Password	
Apply	

Figure 3.2 Changing a Default Password

Note!   *To change other user's password, go to **Administration** > **User**. From the **User Administration** menu, click **Change Password** behind the user's account*
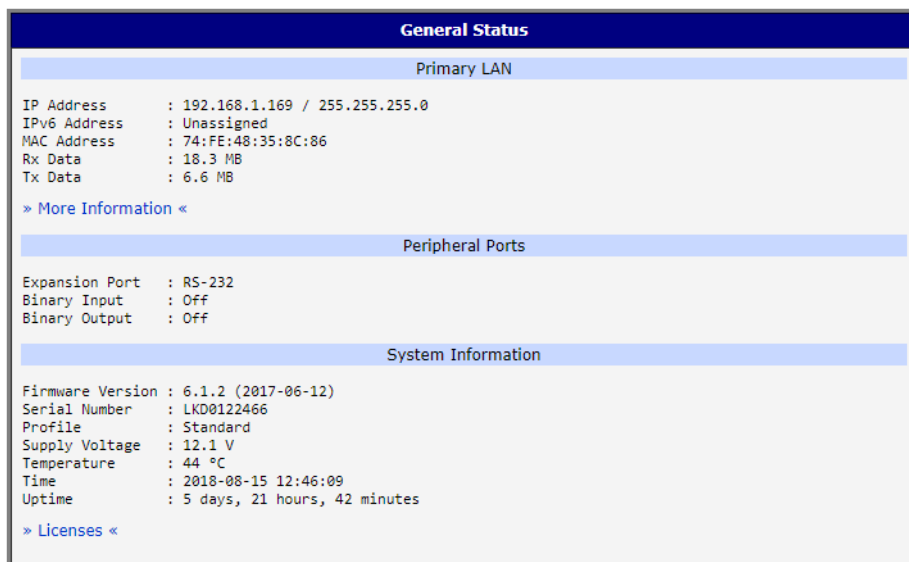
3.3 Status

3.3.1 General

Selecting the General item will open a screen displaying a summary of basic information about the device and its activities. This page is also displayed when you login to the web interface. Information is divided into several sections, based upon the type of device activity or the properties area: Mobile Connection, Primary LAN, Peripheral Ports and System Information. If the device is WiFi equipped, there will be a WiFi section.

IPv6 Address item can show multiple different addresses for one network interface. This is standard behavior since an IPv6 interface uses more addresses. The second IPv6 Address showed after pressing More Information is automatically generated EUI-64 format link local IPv6 address derived from MAC address of the interface. It is generated and assigned the first time the interface is used (e.g. cable is connected, Mobile WAN connecting, etc.).

To access this page, click **Status** > **General**.

General Status

Primary LAN

```
IP Address      : 192.168.1.169 / 255.255.255.0
IPv6 Address    : Unassigned
MAC Address     : 74:FE:48:35:8C:86
Rx Data         : 18.3 MB
Tx Data         : 6.6 MB

» More Information «
```

Peripheral Ports

```
Expansion Port  : RS-232
Binary Input    : Off
Binary Output   : Off
```

System Information

```
Firmware Version : 6.1.2 (2017-06-12)
Serial Number    : LKD0122466
Profile          : Standard
Supply Voltage   : 12.1 V
Temperature      : 44 °C
Time             : 2018-08-15 12:46:09
Uptime           : 5 days, 21 hours, 42 minutes

» Licenses «
```

Figure 3.3 Status > General

Note! *For the purpose of instructions, the user interface of a single model was used. The interface screens may not reflect your specific model.*

3.3.2 Network

To view information about the interfaces and the routing table, open the Network item in the Status menu.

To access this page, click **Status** > **Network**.

```
                            Network Status
                               Interfaces

eth0      Link encap:Ethernet  HWaddr 00:D0:C9:FA:82:03
          inet addr:192.168.1.169  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:247 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28988 (28.3 KB)  TX bytes:59673 (58.2 KB)
          Interrupt:56

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1048 (1.0 KB)  TX bytes:1048 (1.0 KB)

nat64     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet6 addr: 64:ff9b::/96 Scope:Global
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

                               Route Table

Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.1.1     0.0.0.0         255.255.255.255 UH    0      0        0 eth0

                              IPv6 Route Table

Destination                     Next Hop                Flags Metric Ref    Use Iface
64:ff9b::/96                     ::                      U     256    0        0 nat64
::1/128                         ::                      U     0      1        1 lo
64:ff9b::/128                   ::                      U     0      0        1 lo
ff00::/8                        ::                      U     256    0        0 nat64
```

Figure 3.4 Status > Network

3.3.3 DHCP

Information about the DHCP server activity is accessible via DHCP item. The DHCP server provides automatic configuration of the client devices connected to the device. The DHCP server assigns each device an IP address, subnet mask, default gateway (IP address of device) and DNS server (IP address of device). DHCPv6 server is supported.

To access this page, click **Status** > **DHCP**.

```
                            DHCP Status
                      Active DHCP Leases (LAN)

No active dynamic DHCP leases.

                     Active DHCPv6 Leases (LAN)

No active dynamic DHCPv6 leases.
```

Figure 3.5 Status > DHCP

3.3.4 IPsec

Selecting the IPsec option in the status menu of the web page will bring up the information for any IPsec Tunnels that have been established. If the tunnel has been built correctly, the screen will display IPsec SA established (highlighted in red in the figure below.) If there is no such text in log, the tunnel was not created.

To access this page, click **Status** > **IPsec**.

IPsec Status
IPsec Tunnels Information
IPsec is disabled.
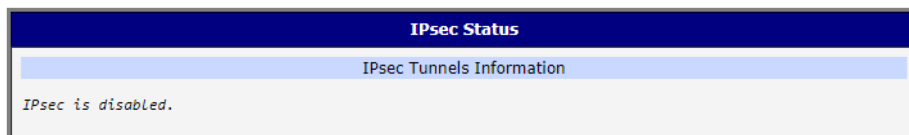
Figure 3.6 Status > IPsec

3.3.5 DynDNS

The device supports DynamicDNS using a DNS server on www.dyndns.org. If Dynamic DNS is configured, the status can be displayed by selecting menu option DynDNS. Refer to www.dyndns.org for more information on how to configure a Dynamic DNS client.

You can use the following listed servers for the Dynamic DNS service. It is possible to use the DynDNSv6 service with IP Mode switched to IPv6 on DynDNS Configuration page.

- www.dyndns.org
- www.spdns.de
- www.dnsdynamic.org
- www.noip.com

To access this page, click **Status** > **DynDNS**.

DynDNS Status
Last DynDNS Update Status
DynDNS client is disabled.
Last DynDNSv6 Update Status
DynDNSv6 client is disabled.
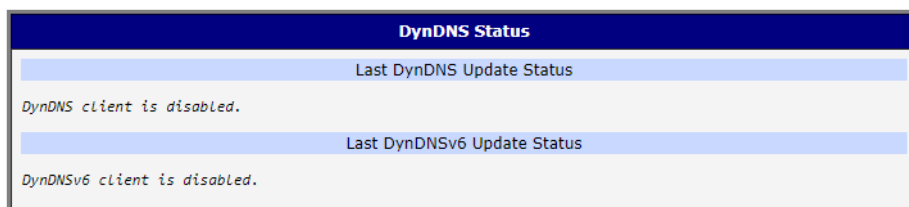
Figure 3.7 Status > DynDNS

When the device detects a DynDNS record update, the dialog displays one or more of the following messages:

- DynDNS client is disabled.
- Invalid username or password.
- Specified hostname doesn't exist.
- Invalid hostname format.
- Hostname exists, but not under specified username.
- No update performed yet.
- DynDNS record is already up to date.
- DynDNS record successfully update.
- DNS error encountered.
- DynDNS server failure.
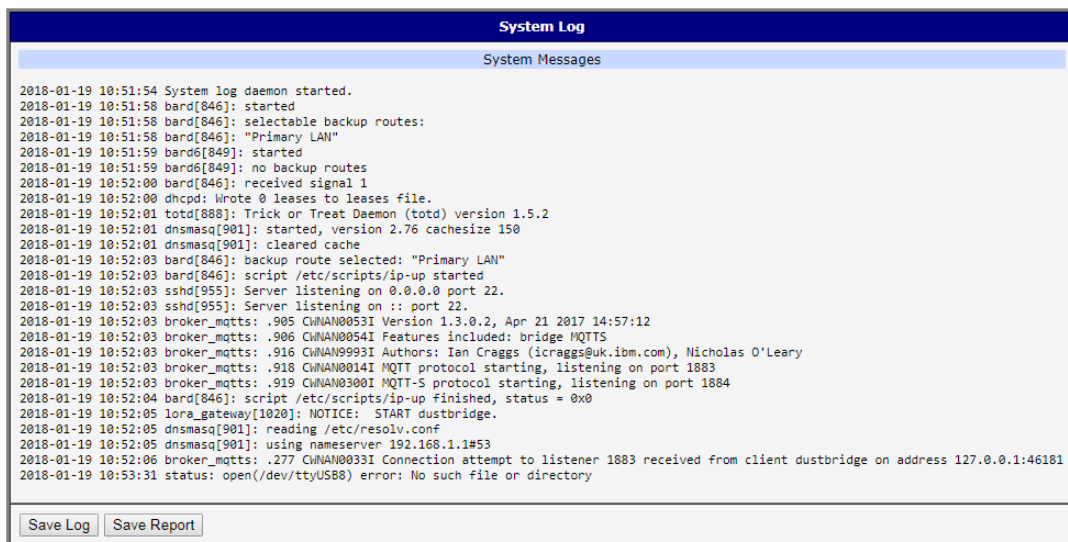
3.3.6 System Log

If there are any connection problems you may view the system log by selecting the System Log menu item. Detailed reports from individual applications running in the device will be displayed. Use the **Save Log** button to save the system log to a connected computer. (It will be saved as a text file with the .log extension.) The **Save Report** button is used for creating detailed reports. (It will be saved as a text file with the .txt extension. The file will include statistical data, routing and process tables, system log, and configuration.)

The default length of the system log is 1000 lines. After reaching 1000 lines a new file is created for storing the system log. After completion of 1000 lines in the second file, the first file is overwritten with a new file.

The Syslogd program will output the system log. It can be started with two options to modify its behavior. Option "-S" followed by decimal number sets the maximal number of lines in one log file. Option "-R" followed by hostname or IP address enables logging to a remote syslog daemon. (If the remote syslog daemon is Linux OS, there has to be remote logging enabled (typically running "syslogd -R"). If it's the Windows OS, there has to be syslog server installed, e.g. Syslog Watcher). To start syslogd with these options, the "/etc/init.d/syslog" script can be modified via SSH or lines can be added into Startup Script (accessible in Configuration section) according to Figure 3.9.

To access this page, click **Status** > **System Log**.

Figure 3.8 Status > System Log

The following example (figure) shows how to send syslog information to a remote server at 192.168.2.115 on startup.

Figure 3.9 Example Program Syslogd Start with the Parameter -R

3.4 Configuration

3.4.1 LAN

To enter the Local Area Network configuration, select the LAN menu item in the Configuration section.

LAN Configuration page is divided into IPv4 and IPv6 columns, see Figure 3.10. There is dual stack support of IPv4 and IPv6 protocols - they can run alongside, you can configure either one of them or both. If you configure both IPv4 and IPv6, other network devices will choose the communication protocol. Configuration items and IPv6 to IPv4 differences are described in the tables below.

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

Figure 3.10 Configuration > LAN

Item	Description
DHCP Client	Enables/disables the DHCP client function supporting both IPv4 and IPv6. ■ disabled - The device does not allow automatic allocation of an IP address from a DHCP server in LAN network. ■ enabled - The device allows automatic allocation of an IP address from a DHCP server in LAN network.
IP Address	A fixed IP address of the Ethernet interface. Use IPv4 notation in IPv4 column and IPv6 notation in IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IPv4 address. In the IPv6 column, fill in the Prefix for the IPv6 address - number in range 0 to 128.

Item	Description
Default Gateway	Specifies the IP address of a default gateway. If filled-in, every packet with the destination not found in the routing table is sent to this IP address. Use proper IP address notation in IPv4 and IPv6 column.
DNS Server	Specifies the IP address of the DNS server. When the IP address is not found in the Routing Table, the device forwards the request to DNS server specified here. Use proper IP address notation in IPv4 and IPv6 column.

The Default Gateway and DNS Server items are only used if the DHCP Client item is set to disabled and if the Primary or Secondary LAN is selected by the Backup Routes system as the default route. Since FW 5.3.0, Default Gateway and DNS Server are also supported on bridged interfaces.

The following items (in the table below) are global for the configured Ethernet interface. Only one bridge can be active on the device at a time. The DHCP Client, IP Address and Subnet Mask / Prefix parameters of the only one of the interfaces are used to for the bridge. Primary LAN has higher priority when other interfaces (wlan0) are added to the bridge. Other interfaces (wlan0 - wifi) can be added to or deleted from an existing bridge at any time. The bridge can be created on demand for such interfaces, but not if it is configured by their respective parameters.

Item	Description
Bridged	Activates/deactivates the bridging function on the device. ■ no - The bridging function is inactive (default). ■ yes - The bridging function is active.
Media Type	Specifies the type of duplex and speed used in the network. ■ Auto-negation - The device automatically sets the best speed and duplex mode of communication according to the network's possibilities. ■ 100 Mbps Full Duplex - The device communicates at 100 Mbps, in the full duplex mode. ■ 100 Mbps Half Duplex - The device communicates at 100 Mbps, in the half duplex mode. ■ 10 Mbps Full Duplex - The device communicates at 10 Mbps, in the full duplex mode. ■ 10 Mbps Half Duplex - The device communicates at 10 Mbps, in the half duplex mode.

3.4.1.1 DHCP Server

The DHCP server assigns the IP address, gateway IP address (IP address of the device) and IP address of the DNS server (IP address of the device) to the connected clients. If these values are filled in by the user in the configuration form, they will be preferred.

The DHCP server supports static and dynamic assignment of IP addresses. Dynamic DHCP assigns clients IP addresses from a defined address space. Static DHCP assigns IP addresses that correspond to the MAC addresses of connected clients.

If IPv6 column is filled in, the DHCPv6 server is used - it is dual stack IPv4 and IPv6.

> **Note!** *Do not to overlap ranges of static allocated IP addresses with addresses allocated by the dynamic DHCP server. IP address conflicts and incorrect network function can occur if you overlap the ranges.*

Configuration of Dynamic DHCP Server

Item	Description
Enable dynamic DHCP leases	Select this option to enable a dynamic DHCP server.
IP Pool Start	Starting IP addresses allocated to the DHCP clients. Use proper notation in IPv4 and IPv6 column.
IP Pool End	End of IP addresses allocated to the DHCP clients. Use proper IP address notation in IPv4 and IPv6 column.
Lease time	Time in seconds that the IP address is reserved before it can be re-used.

Configuration of Static DHCP Server

Item	Description
Enable static DHCP leases	Select this option to enable a static DHCP server.
MAC Address	MAC address of a DHCP client.
IPv4 Address	Assigned IPv4 address. Use proper notation.
IPv6 Address	Assigned IPv6 address. Use proper notation.

3.4.1.2 IPv6 Prefix Delegation

Note! *This is an advanced configuration option. IPv6 prefix delegation works automatically with DHCPv6 - use only if different configuration is desired and if you know the consequences.*

If you want to override the automatic IPv6 prefix delegation, you can configure it in this form. You have to know your Subnet ID Width (part of IPv6 address), see Figure 3.11 below for the calculation help - it is an example: 48 bits is Site Prefix, 16 bits is Subnet ID (Subnet ID Width) and 64 bits is Interface ID.
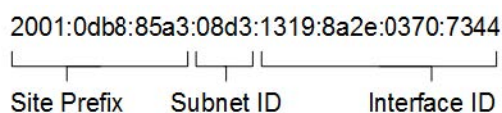
Figure 3.11 IPv6 Address with Prefix Example

Item	Description
Enable IPv6 prefix delegation	Enables prefix delegation configuration filled-in below.
Enable IPv6 prefix delegation	The decimal value of the Subnet ID of the Ethernet interface. Maximum value depends on the Subnet ID Width.
Subnet ID Width	The maximum Subnet ID Width depends on your Site Prefix - it is the remainder to 64 bits.

3.4.1.3 IEEE 802.1X Authentication
To prevent unauthorized radios from accessing data transmitting over wireless transmission, WISE-6610 Series provides rock solid security settings.

Navigate to **Configuration** > **LAN and locate Enable IEEE 802.1X Authentication**.

Item	Description
Enable IEEE 802.1X Authentication	Tick the radio button to enable the authentication function.
Authentication Method	Click the drop-down menu to select the method type. Range: EAP-PEAP/MSCHAPv2 or EAP-TLS.
CA Certificate	Enter the trusted digital certificate (required for EAP-PEAP).
Local Certificate	Enter the self-signed digital certificate (required for EAP-PEAP).
Local Private Key	Enter the secret key variable used to encrypt or decrypt the transmission.
Identity	Enter the Identity profile authorized to access the authentication server.
Password	Enter the string associated with the defined Identity profile in the previous frame.
Apply	Click **Apply** to accept the configuration changes.

The following are LAN configuration illustrations defining possible network topology.

Example 1: IPv4 Dynamic DHCP Server, Default Gateway and DNS Server

- The range of dynamic allocated IPv4 addresses is from 192.168.1.2 to 192.168.1.4.
- The address is allocated for 600 second (10 minutes).
- Default gateway IP address is 192.168.1.20
- DNS server IP address is 192.168.1.20
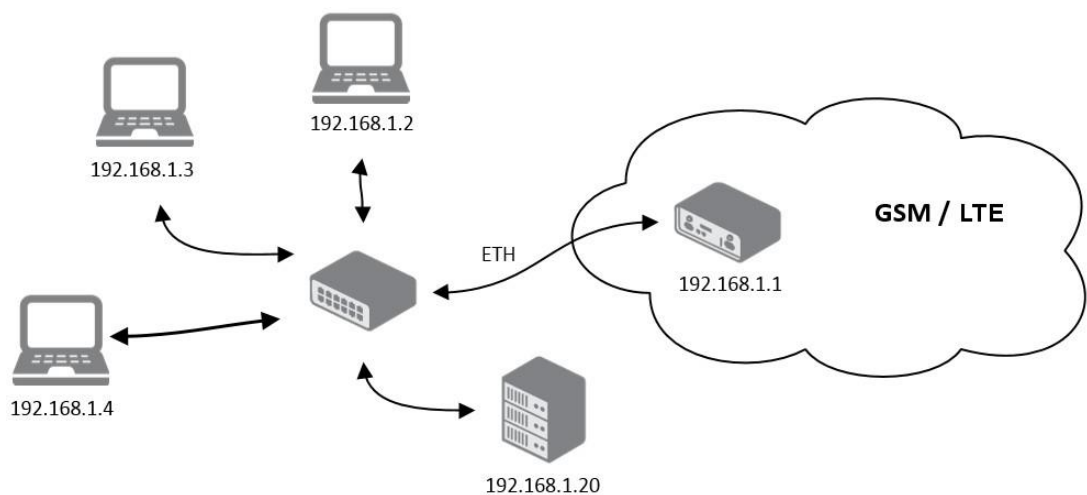
Figure 3.12 IPv4 Dynamic DHCP Network Topology

The settings required in the LAN configuration menu for an IPv4 Dynamic DHCP configuration are shown in the following figure.

Figure 3.13 LAN Configuration for a Dynamic Network Typology

Example 2: IPv4 Dynamic and Static DHCP server

■ The range of allocated addresses is from 192.168.1.2 to 192.168.1.4.

■ The address is allocated for 600 seconds (10 minutes).

■ The client with the MAC address 01:23:45:67:89:ab has the IP address 192.168.1.10.

■ The client with the MAC address 01:54:68:18:ba:7e has the IP address 192.168.1.11.
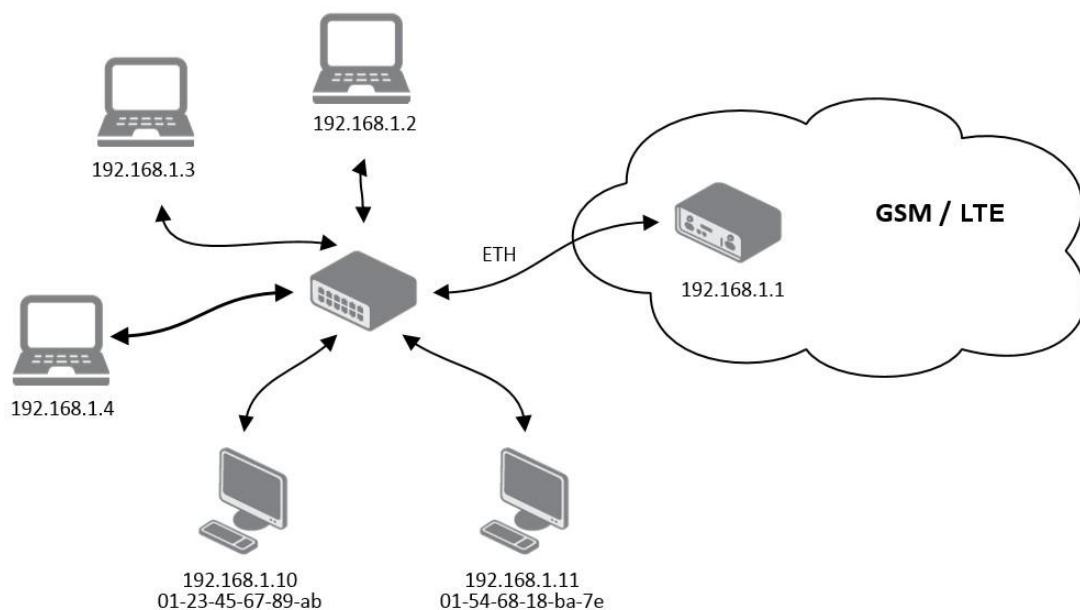
Figure 3.14 IPv4 Dynamic and Static DHCP Network Topology

The settings required in the LAN configuration menu for an IPv4 Dynamic and Static DHCP configuration are shown in the following figure.

Figure 3.15 LAN Configuration for an IPv4 Dynamic and Static DHCP Network Topology

Example 3: IPv6 Dynamic DHCP Server

■ The range of dynamic allocated IPv6 addresses is from 2001:db8::1 to 2001:db8::ffff.

■ The address is allocated for 600 second (10 minutes).

■ The device is still accessible via IPv4 (192.168.1.1).
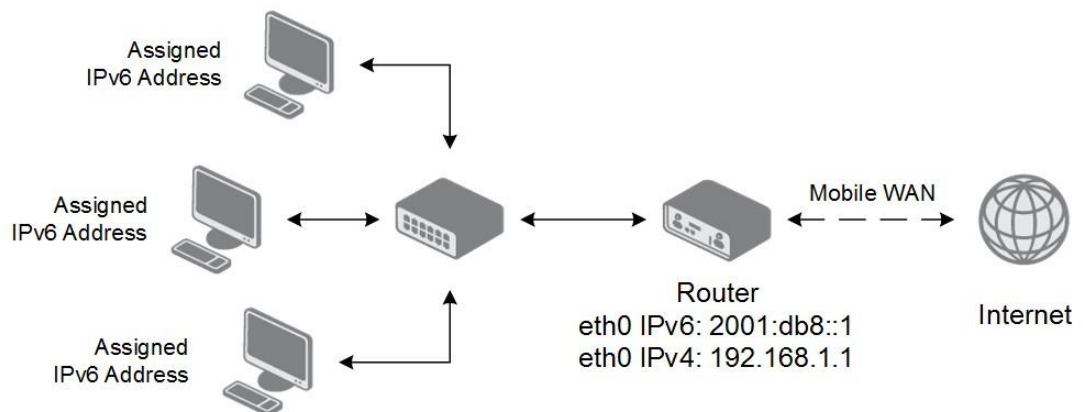
Figure 3.16 IPv6 Dynamic DHCP Server Network Topology

Figure 3.17 LAN Configuration for an IPv6 Dynamic DHCP Server Network Topology

3.4.2 NAT

To configure the address translation function, click on NAT in the Configuration section of the main menu. There is independent IPv4 and IPv6 NAT configuration since there is dual stack IPv4 and IPv6 implemented in the router. The NAT item in the menu on the left will expand to IPv4 and IPv6 options and you can click IPv6 to enable and configure the IPv6 NAT - see Figure below. The configuration fields have the same meaning in the IPv4 NAT Configuration and IPv6 NAT Configuration forms.

To access this page, click **Configuration** > **NAT**.

Figure 3.18 Configuration > NAT

The router actually uses Port Address Translation (PAT), which is a method of mapping a TCP/UDP port to another TCP/UDP port. The router modifies the information in the packet header as the packets traverse a router. This configuration form allows you to specify up to 16 PAT rules.

Item	Description
Public Port	Public port for the translation rule.
Private Port	Private port for the translation rule.
Type	Protocol type - TCP or UDP.
Server IP Address	IP address where the router forwards incoming data.

If you require more than sixteen NAT rules, insert the remaining rules into the Startup Script. The Startup Script dialog is located on Scripts page in the Configuration section of the menu. When creating your rules in the Startup Script, use this command for IPv4 NAT:

```
iptables -t nat -A napt -p tcp -dport [PORT_PUBLIC] -j DNAT
-to-destination [IPADDR]:[PORT_PRIVATE]
```

Enter the IP address [IPADDR], the public ports numbers [PORT_PUBLIC], and private [PORT_PRIVATE] in place of square brackets. For IPv6 NAT use ip6tables command with same options.

If you enable the following options and enter the port number, the router allows you to remotely access to the router from WAN (Mobile WAN) interface.

> **Caution!** *Enable remote HTTP access on port activates the redirect from HTTP to HTTPS protocol only. The router doesn't allow unsecured HTTP protocol to access the web configuration. To access the web configuration, always check the Enable re- mote HTTPS access on port item. Never enable the HTTP item only to access the web configuration from the Internet (configuration would not be accessible from the Internet). Always check the HTTPS item or HTTPS and HTTP items together (to set the redirect from HTTP).*

Item	Description
Enable remote HTTP access on port	This option sets the redirect from HTTP to HTTPS only (disabled in default configuration).
Enable remote HTTPS access on port	If field and port number are filled in, configuration of the router over web interface is allowed (disabled in default configuration).
Enable remote SSH access on port	Select this option to allow access to the router using SSH (disabled in default configuration).
Enable remote SNMP access on port	Select this option to allow access to the router using SNMP (disabled in default configuration).
Masquerade outgoing packets	Activates/deactivates the network address translation function.

Use the following parameters to set the routing of incoming data from the WAN (Mobile WAN) to a connected computer.

Item	Description
Send all remaining incoming packets to default server	Activates/deactivates forwarding unmatched incoming packets to the default server. The prerequisite for the function is that you specify a default server in the De- fault Server IPv4/IPv6 Address field. The router can for- ward incoming data from a GPRS to a computer with the assigned IP address.
Default Server IP Address	The IP address.

Example1: IPv4 NAT Configuration with Single Device Connected

Figure 3.19 Topology for NAT Configuration Example 1

It is important to mark the Send all remaining incoming packets to default server check box for this configuration. The IP address in this example is the address of the device behind the router. The default gateway of the devices in the subnetwork connected to router is the same IP address as displayed in the Default Server IPv4 Address field.

Figure 3.20 NAT Configuration for Example 1

Example 2: IPv4 NAT Configuration with More Equipment Connected

In this example, using the switch you can connect more devices behind the router. Every device connected behind the router has its own IP address. Enter the address in the Server IPv4 Address field in the NAT dialog. The devices are communicating on port 80, but you can set port forwarding using the Public Port and Private Port fields in the NAT dialog. You have now configured the router to access the 192.168.1.2:80 socket behind the router when accessing the IP address 10.0.0.1:81 from the Internet. If you send a ping request to the public IP address of the router (10.0.0.1), the router responds as usual (not forwarding). And since the Send all

remaining incoming packets to default server is inactive, the router denies connection attempts.
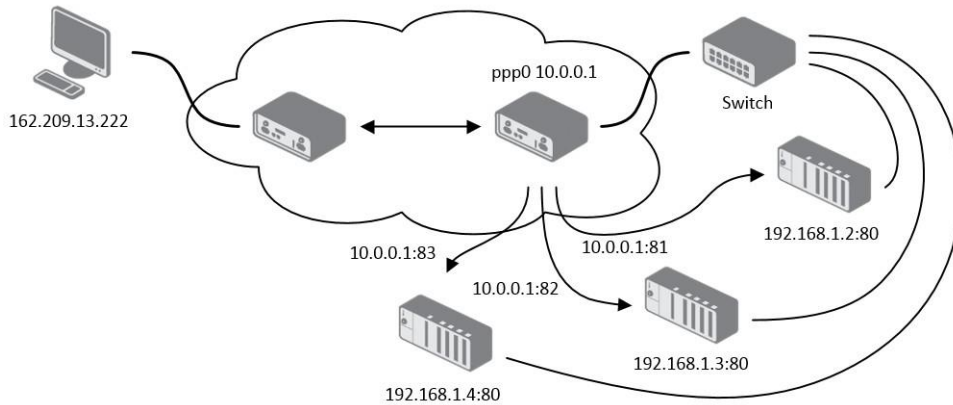
Figure 3.21 Topology for NAT Configuration Example 2

Figure 3.22 NAT Configuration for Example 2

3.4.3 OpenVPN

Select the OpenVPN item to configure an OpenVPN tunnel. The OpenVPN tunnel function allows you to create a secure connection between two separate LAN networks. The device allows you to create up to four OpenVPN tunnels. IPv4 and IPv6 dual stack is supported.

To access this page, click **Configuration** > **OpenVPN**.

Figure 3.23 Configuration > OpenVPN > 1st Tunnel

Item	Description
Description	Specifies the description or name of tunnel.

Item	Description
Protocol	Specifies the communication protocol. ■ UDP - The OpenVPN communicates using UDP. ■ TCP server - The OpenVPN communicates using TCP in server mode. ■ TCP client - The OpenVPN communicates using TCP in client mode. ■ UDPv6 - The OpenVPN communicates using UDP over IPv6. ■ TCPv6 server - The OpenVPN communicates using TCP over IPv6 in server mode. ■ TCPv6 client - The OpenVPN communicates using TCP over IPv6 in client mode.
UDP Port	Specifies the port of the relevant protocol (UDP or TCP).
Remote IP Address	Specifies the IPv4, IPv6 address or domain name of the opposite side of the tunnel.
Remote Subnet	IPv4 address of a network behind opposite side of the tunnel.
Remote Subnet Mask	IPv4 subnet mask of a network behind opposite tunnel's side.
Redirect Gateway	Activates/deactivates redirection of data on Layer 2.
Local Interface IP Address	Specifies the IPv4 address of a local interface. For proper routing it is recommended to fill-in any IPv4 address from local range even if you are using IPv6 tunnel only.
Remote Interface IP Address	Specifies the IPv4 address of the interface of opposite side of the tunnel. For proper routing it is recommended to fill-in any IPv4 address from local range even if you are using IPv6 tunnel only.
Remote IPv6 Subnet	Specify the subnet associated with the listed remote interface.
Remote IPv6 Subnet Prefix Length	IPv6 address and prefix of the remote IPv6 network. Equivalent of the Remote Subnet and Remote Subnet Mask in IPv4 section.
Local Interface IPv6 Address	Specifies the IPv6 address of a local interface.
Remote Interface IPv6 Address	Specifies the IPv6 address of the interface of opposite side of the tunnel.
Ping Interval	Specifies the IPv6 address of the interface of opposite side of the tunnel.
Ping Timeout	Specifies the time interval the device waits for a message sent by the opposite side. For proper verification of the OpenVPN tunnel, set the Ping Timeout to greater than the Ping Interval.
Renegotiate Interval	Specifies the renegotiate period (reauthorization) of the OpenVPN tunnel. You can only set this parameter when the Authenticate Mode is set to username/password or X.509 certificate. After this time period, the device changes the tunnel encryption to help provide the continues safety of the tunnel.
Max Fragment Size	Maximum size of a sent packet.
Compression	Compression of the data sent: ■ none - No compression is used. ■ LZO - A lossless compression is used, use the same setting on both sides of the tunnel.
NAT Rules	Activates/deactivates the NAT rules for the OpenVPN tunnel: ■ not applied - NAT rules are not applied to the tunnel. ■ applied - NAT rules are applied to the OpenVPN tunnel.

Item	Description
Authenticate Mode	Specifies the authentication mode: ■ none - No authentication is set. ■ Pre-shared secret - Specifies the shared key function for both sides of the tunnel. ■ Username/password - Specifies authentication using a CA Certificate, Username and Password. ■ X.509 Certificate (multiclient) - Activates the X.509 authentication in multi-client mode. ■ X.509 Certificate (client) - Activates the X.509 authentication in client mode. ■ X.509 Certificate (server) - Activates the X.509 authentication in server mode.
Pre-shared Secret	Specifies the pre-shared secret which you can use for every authentication mode.
CA Certificate	Specifies the CA Certificate which you can use for the username/ password and X.509 Certificate authentication modes.
DH Parameters	Specifies the protocol for the DH parameters key exchange which you can use for X.509 Certificate authentication in the server mode.
Local Certificate	Specifies the certificate used in the local device. You can use this authentication certificate for the X.509 Certificate authentication mode.
Local Private Key	Specifies the key used in the local device. You can use the key for the X.509 Certificate authentication mode.
Username	Specifies a login name which you can use for authentication in the username/password mode.
Password	Specifies a password which you can use for authentication in the username/password mode.
Extra Options	Specifies additional parameters for the OpenVPN tunnel, such as DHCP options. The parameters are proceeded by two dashes. For possible parameters see the help text in the device using SSH - run the openvpnd --help command.

Example: OpenVPN Tunnel Configuration in IPv4 Network
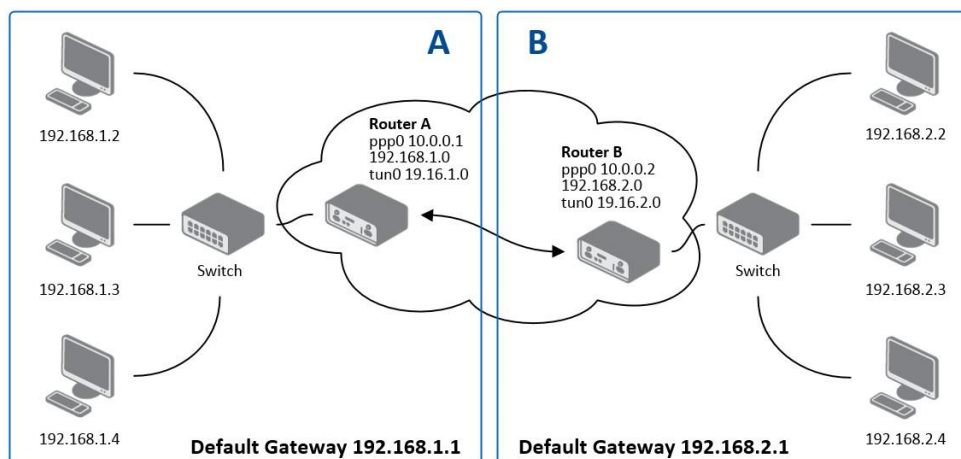
Figure 3.24 Topology of OpenVPN Configuration Example

OpenVPN tunnel configuration:

Configuration	A	B
Protocol	UDP	UDP
UDP Port	1194	1194

Configuration	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Interface IP Address	19.16.1.0	19.16.2.0
Remote Interface IP Address	19.16.2.0	19.16.1.0
Compression	LZO	LZO
Authenticate mode	none	none

Examples of different options for configuration and authentication of OpenVPN tunnel can be found in the application note OpenVPN Tunnel [5].

3.4.4 IPSec

To open the Tunnel Configuration page, click in the Configuration section of the main menu. The tunnel function allows you to create a secured connection between two separate LAN networks. The device allows you to create up to four tunnels. IPv4 and IPv6 tunnels are supported (dual stack), you can transport IPv6 traffic through IPv4 tunnel and vice versa.

To access this page, click **Configuration > IPSec**.

> *Note!* *To encrypt data between the local and remote subnets, specify the appropriate values in the subnet fields on both devices. To encrypt the data stream between the devices only, leave the local and remote subnets fields blank.*

> *Note!* *If you specify the protocol and port information in the Local Protocol/Port field, then the device encapsulates only the packets matching the settings.*

1st IPsec Tunnel Configuration

☐ Create 1st IPsec tunnel	
Description *	[ ]
Host IP Mode	IPv4 ▼
Remote IP Address *	[ ]
Tunnel IP Mode	IPv4 ▼
Remote ID *	[ ]
First Remote Subnet *	[ ]
First Remote Subnet Mask *	[ ]
Second Remote Subnet *	[ ]
Second Remote Subnet Mask *	[ ]
Remote Protocol/Port *	[ ]
Local ID *	[ ]
First Local Subnet *	[ ]
First Local Subnet Mask *	[ ]
Second Local Subnet *	[ ]
Second Local Subnet Mask *	[ ]
Local Protocol/Port *	[ ]
Encapsulation Mode	tunnel ▼
Force NAT Traversal	no ▼
IKE Protocol	IKEv1 ▼
IKE Mode	main ▼
IKE Algorithm	auto ▼
IKE Encryption	3DES ▼
IKE Hash	MD5 ▼
IKE DH Group	2 ▼
ESP Algorithm	auto ▼
ESP Encryption	DES ▼
ESP Hash	MD5 ▼
PFS	disabled ▼
PFS DH Group	2 ▼
Key Lifetime	3600 sec
IKE Lifetime	3600 sec
Rekey Margin	540 sec
Rekey Fuzz	100 %
DPD Delay *	[ ] sec
DPD Timeout *	[ ] sec
Authenticate Mode	pre-shared key ▼
Pre-shared Key	[ ]
CA Certificate	[ ]
Remote Certificate	[ ]
Local Certificate	[ ]
Local Private Key	[ ]
Local Passphrase *	[ ]
Debug	control ▼
* can be blank	

[Apply]

Figure 3.25 Configuration > 1st Tunnel

Item	Description
Description	Name or description of the tunnel.
Host IP Mode	■ IPv4 - The device communicates via IPv4 with the opposite side of the tunnel. ■ IPv6 - The device communicates via IPv4 with the opposite side of the tunnel.
Remote IP Address	IPv4, IPv6 address or domain name of the remote side of the tunnel, based in the Host IP Mode above.
Tunnel IP Mode	■ IPv4 - The IPv4 communication runs inside the tunnel. ■ IPv6 - The IPv6 communication runs inside the tunnel.
Remote ID	Identifier (ID) of remote side of the tunnel. It consists of two parts: a hostname and a domain-name.
Remote Subnet	IPv4 or IPv6 address of a network behind remote side of the tunnel, based on Tunnel IP Mode above.
Remote Subnet Mask	IPv4 subnet mask of a network behind remote side of the tunnel, or IPv6 prefix (single number 0 to 128).
Remote Protocol/ Port	Specifies Protocol/Port of remote side of the tunnel. The general form is protocol /port, for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Local ID	Identifier (ID) of local side of the tunnel. It consists of two parts: a hostname and a domain-name.
Local Subnet	IPv4 or IPv6 address of a local network, based on Tunnel IP Mode above.
First Local Subnet Mask	IPv4 subnet mask of a local network, or IPv6 prefix (single number 0 to 128).
Local Protocol/Port	Specifies Protocol/Port of a local network. The general form is protocol /port, for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Encapsulation Mode	Specifies the mode, according to the method of encapsulation. You can select the tunnel mode in which the entire IP datagram is encapsulated or the transport mode in which only IP header is encapsulated.
Force NAT Traversal	Enable/disables NAT address translation on the tunnel. Enable if you use NAT between the end points of the tunnel.
IKE Protocol	Click the drop-down menu to select to define a protocol (IKEv1/IKEv2, IKEv1, or IKEv2). IKE Phase 1 is ISAKMP (Internet Security Association and Key Management Protocol), which is used to create private tunnelling between peers for a secure communication.
IKE Mode	Specifies the mode for establishing a connection (main or aggressive). If you select the aggressive mode, then the device establishes the tunnel faster, but the encryption is permanently set to 3DES-MD5. We recommend that you not use the aggressive mode due to lower security!
IKE Algorithm	Specifies the means by which the device selects the algorithm: ■ auto - The encryption and hash algorithm are selected automatically. ■ manual - The encryption and hash algorithm are defined by the user.
IKE Encryption	Encryption algorithm - 3DES, AES128, AES192, AES256.
IKE Hash	Hash algorithm - MD5, SHA1, SHA256, SHA384 or SHA512.

Item	Description
IKE DH Group	Specifies the Diffie-Hellman groups which determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require more time to compute the key.
ESP Algorithm	Specifies the means by which the device selects the algorithm: ■ auto - The encryption and hash algorithm are selected automatically. ■ manual - The encryption and hash algorithm are defined by the user.
ESP Encryption	Encryption algorithm - DES, 3DES, AES128, AES192, AES256.
ESP Hash	Hash algorithm - MD5, SHA1, SHA256, SHA384 or SHA512.
PFS	Enables/disables the Perfect Forward Secrecy function. The function ensures that derived session keys are not compromised if one of the private keys is compromised in the future.
PFS DH Group	Specifies the Diffie-Hellman group number (see IKE DH Group).
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
Rekey Margin	Specifies how long before a connection expires that the device attempts to negotiate a replacement. Specify a maximum value that is less than half of IKE and Key Lifetime parameters.
Rekey Fuzz	Percentage of time for the Rekey Margin extension.
DPD Delay	Time after which the tunnel functionality is tested.
DPD Timeout	The period during which device waits for a response.
Authenticate Mode	Specifies the means by which the device authenticates: ■ Pre-shared key - Sets the shared key for both sides of the tunnel. ■ X.509 Certificate - Allows X.509 authentication in multiclient mode.
Pre-shared Key	Specifies the shared key for both sides of the tunnel. The prerequisite for entering a key is that you select pre-shared key as the authentication mode.
CA Certificate	Certificate for X.509 authentication.
Remote Certificate	Certificate for X.509 authentication.
Local Certificate	Certificate for X.509 authentication.
Local Private Key	Private key for X.509 authentication.
Local Passphrase	Passphrase used during private key generation.
Debug	Choose the level of verbosity to System Log. Silent (default), audit, control, control-more, raw, private (most verbose including the private keys). See strongSwan documentation for more details.

The function supports the following types of identifiers (ID) for both sides of the tunnel, Remote ID and Local ID parameters:

■ IP address (for example, 192.168.1.1)

■ DN (for example, C=CZ, O=CompanyName, OU=TP, CN=A)

■ FQDN (for example, @director.companyname.cz) - the @ symbol proceeds the FQDN.

■ User FQDN (for example, director@companyname.cz)

The certificates and private keys have to be in the PEM format. Use only certificates containing start and stop tags.

The random time, after which the device re-exchanges new keys is defined as follows:

Lifetime - (Rekey margin + random value in range (from 0 to Rekey margin * Rekey Fuzz/100))

The default exchange of keys is in the following time range:

- Minimal time: 1h - (9m + 9m) = 42m
- Maximal time: 1h - (9m + 0m) = 51m

We recommend that you maintain the default settings. When you set key exchange times higher, the tunnel produces lower operating costs, but the setting also provides less security. Conversely, when you reducing the time, the tunnel produces higher operating costs, but provides for higher security.

The changes in settings will apply after clicking the **Apply** button.

Example: Tunnel Configuration in IPv4 Network
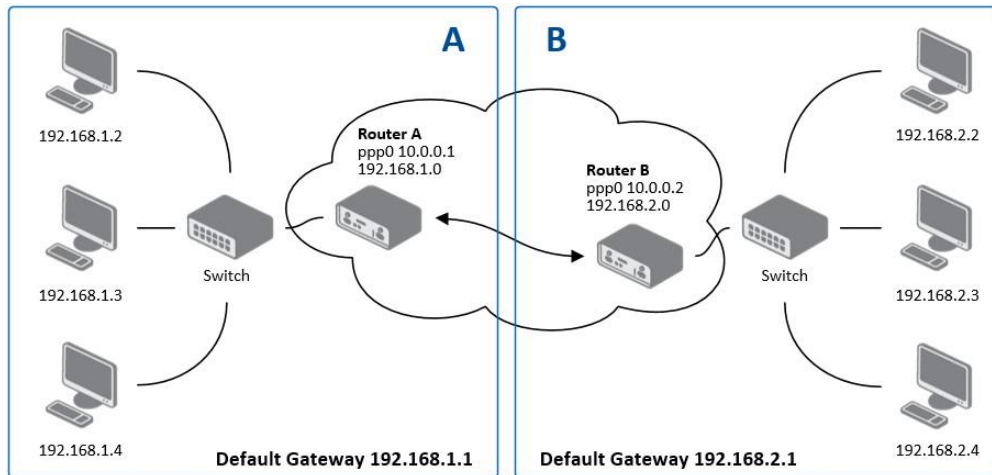
Figure 3.26 Topology of Configuration Example

tunnel configuration:

Configuration	A	B
Host IP Mode	IPv4	IPv4
Remote IP Address	10.0.0.2	10.0.0.1
Tunnel IP Mode	IPv4	IPv4
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Subnet	192.168.1.0	192.168.2.0
Local Subnet Mask	255.255.255.0	255.255.255.0
Authenticate mode	pre-shared key	pre-shared key
Pre-shared key	test	test

Examples of different options for configuration and authentication of tunnel can be found in the application note Tunnel [6].

3.4.5 GRE

> *Note!* *GRE is an unencrypted protocol. GRE via IPv6 is not supported.*

To open the GRE Tunnel Configuration page, click GRE in the Configuration section of the main menu. The GRE tunnel function allows you to create an unencrypted

connection between two separate LAN networks. The device allows you to create four GRE tunnels.

To access this page, click **Configuration** > **GRE**.

1st GRE Tunnel Configuration

☐ Create 1st GRE tunnel
Description *
Remote IP Address
Remote Subnet *
Remote Subnet Mask *
Local Interface IP Address *
Remote Interface IP Address *
Multicasts   disabled   ▼
Pre-shared Key *
* can be blank

Apply

Figure 3.27 Configuration > GRE > 1st Tunnel

Item	Description
Description	Description of the GRE tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	IP address of the network behind the remote side of the tunnel.
Remote Subnet Mask	Specifies the mask of the network behind the remote side of the tunnel.
Local Interface IP Address	IP address of the local side of the tunnel.
Remote Interface IP Address	IP address of the remote side of the tunnel.
Multicasts	Activates/deactivates sending multicast into the GRE tunnel: ■ disabled - Sending multicast into the tunnel is inactive. ■ enabled - Sending multicast into the tunnel is active.
Pre-shared Key	Specifies an optional value for the 32 bit shared key in numeric format, with this key the device sends the filtered data through the tunnel. Specify the same key on both devices, otherwise the device drops received packets.

Note!   *The GRE tunnel does not pass through NAT.*

The changes in settings will apply after pressing the **Apply** button.

Example: GRE Tunnel Configuration
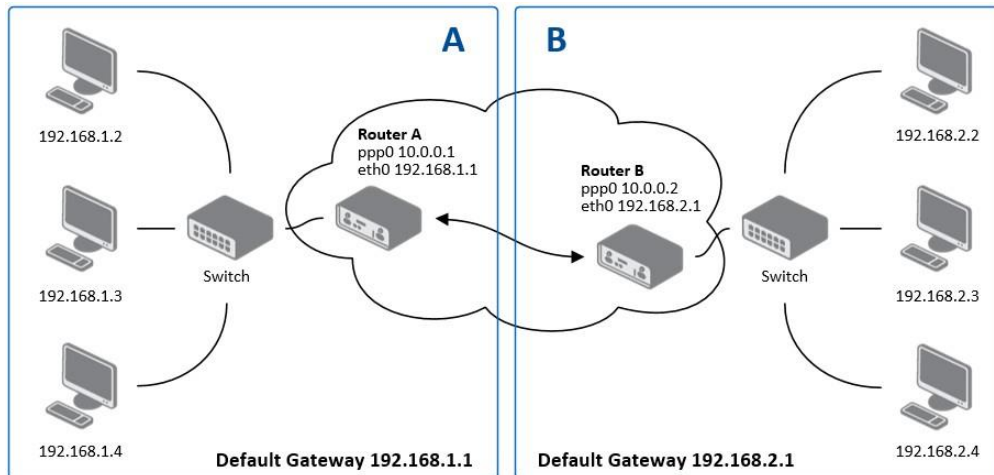
Figure 3.28 Topology of GRE Tunnel Configuration Example

GRE tunnel configuration:

Configuration	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0

Examples of different options for configuration of GRE tunnel can be found in the application note GRE Tunnel [7].

3.4.6 L2TP

> **Note!** *L2TP is an unencrypted protocol. L2TP via IPv6 is not supported.*

To open the L2TP Tunnel Configuration page, click L2TP in the Configuration section of the main menu. The L2TP tunnel function allows you to create a password protected connection between 2 LAN networks. The device activates the tunnels after you mark the Create L2TP tunnel check box.

To access this page, click **Configuration** > **L2TP**.

Figure 3.29 Configuration > L2TP

Item	Description
Mode	Specifies the L2TP tunnel mode on the device side: ■ L2TP server - Specify an IP address range offered by the server. ■ L2TP client - Specify the IP address of the server.
Server IP Address	IP address of the server.
Client Start IP Address	IP address to start with in the address range. The range is offered by the server to the clients.
Client End IP Address	The last IP address in the address range. The range is offered by the server to the clients.
Local IP Address	IP address of the local side of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	Address of the network behind the remote side of the tunnel.
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel.
Username	Username for the L2TP tunnel login.
Password	Password for the L2TP tunnel login.

Example: L2TP Tunnel Configuration
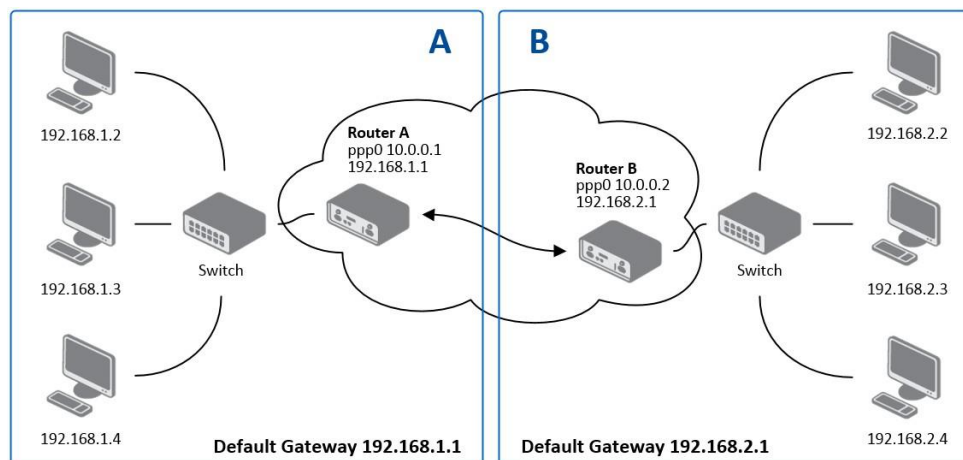
Figure 3.30 Topology of L2TP Tunnel Configuration Example

Configuration of the L2TP tunnel:

Configuration	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	N/A	10.0.0.1
Client Start IP Address	192.168.2.5	N/A
Client End IP Address	192.168.2.254	N/A
Local IP Address	192.168.1.1	N/A
Remote IP Address	N/A	N/A
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

3.4.7 PPTP

Note! *PPTP is an unencrypted protocol. PPTP via IPv6 is not supported.*

Select the PPTP item in the menu to configure a PPTP tunnel. PPTP tunnel allows password protected connections between two LANs. It is similar to L2TP. The tunnels are active after selecting Create PPTP tunnel.

To access this page, click **Configuration** > **PPTP**.

Figure 3.31 Configuration > PPTP

Item	Description
Mode	Specifies the L2TP tunnel mode on the device side: ■ PPTP server - Specify an IP address range offered by the server. ■ PPTP client - Specify the IP address of the server.
Server IP Address	IP address of the server.
Local IP Address	IP address of the local side of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	Address of the network behind the remote side of the tunnel.
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel.

Item	Description
Username	Username for the PPTP tunnel login.
Password	Password for the PPTP tunnel login.

The changes in settings will apply after pressing the **Apply** button.

The firmware also supports PPTP pass through, which means that it is possible to create a tunnel through the device.

Example: PPTP Tunnel Configuration
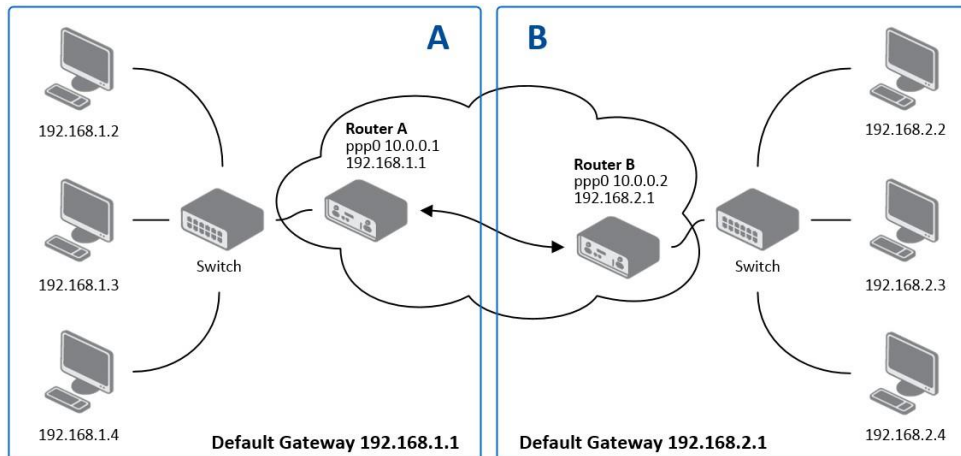
Figure 3.32 Topology of PPTP Tunnel Configuration Example

Configuration of the PPTP tunnel:

Configuration	A	B
Mode	PPTP Server	PPTP Client
Server IP Address	N/A	10.0.0.1
Local IP Address	192.168.1.1	N/A
Remote IP Address	192.168.2.1	N/A
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

3.4.8 Services

3.4.8.1 DynDNS

The DynDNS function allows you to access the device remotely using an easy to remember custom hostname. This DynDNS client monitors the IP address of the device and updates the address whenever it changes. In order for DynDNS to function, you require a public IP address, either static or dynamic, and an active Remote Access service account at www.dyndns.org. Register the custom domain (third-level) and account information specified in the configuration form. You can use other services, too - see the table below, Server item. To open the DynDNS Configuration page, click DynDNS in the main menu.

To access this page, click **Configuration** > **Services** > **DynDNS**.

Figure 3.33 Configuration > Services > DynDNS

Item	Description
Hostname	The third order domain registered on the www.dyndns.org server.
Username	Username for logging into the DynDNS server.
Password	Password for logging into the DynDNS server.
IP Mode	Specifies a DynDNS service other than the www.dyndns.org. Possible other services: www.spdns.de, www.dnsdynamic.org, www.noip.com. Enter the update server service information in this field. If you leave this field blank, the default server members.dyndns.org will be used.
Server	Specifies the version of IP protocol: ■ IPv4 - IPv4 protocol is used only (default). ■ IPv6 - IPv6 protocol is used only. ■ IPv4/IPv6 - IPv4 and IPv6 dual stack is enabled.

Example: DynDNS client configuration with the domain company.dyndns.org:

Figure 3.34 DynDNS Configuration Example

3.4.8.2 HTTP

To access this page, click **Configuration** > **Services** > **HTTP**.

HTTP Configuration

☐ Enable HTTP service
☑ Enable HTTPS service

Session Timeout 600   sec

[Apply]

Figure 3.35 Configuration > Services > HTTP

Item	Description
Enable HTTP service	Click the check box to set up Ethernet encapsulation (remote access) through HTTP function.
Enable HTTPS service	Click the check box to set up Ethernet encapsulation over HTTPS.
Session Timeout	Enter the variable in minutes to define the timeout period for the session.
Apply	Click **Apply** to save the values.

3.4.8.3 NTP

The NTP configuration form allows you to configure the NTP client. To open the NTP page, click NTP in the Configuration section of the main menu. NTP (Network Time Protocol) allows you to periodically set the internal clock of the device. The time is set from servers that provide the exact time to network devices. IPv6 Time Servers are supported.

■ If you mark the Enable local NTP service check box, then the device acts as a NTP server for other devices in the local network (LAN).

■ If you mark the Synchronize clock with NTP server check box, then the device acts as a NTP client. This means that the device automatically adjusts the internal clock every 24 hours.

To access this page, click **Configuration** > **Services** > **NTP**.

NTP Configuration

☐ Enable local NTP service

☐ Synchronize clock with NTP server
Primary NTP Server   [   ]
Secondary NTP Server [   ]

Timezone   [GMT+08:00   ▼]
Daylight Saving Time [no   ▼]

[Apply]

Figure 3.36 Configuration > Services > NTP

Item	Description
Primary NTP Server	IPv4 address, IPv6 address or domain name of primary NTP server.
Secondary NTP Server	IPv4 address, IPv6 address or domain name of secondary NTP server.
Timezone	Specifies the time zone where you installed the device.
Daylight Saving Time	Activates/deactivates the DST shift. ■ No - The time shift is inactive. ■ Yes - The time shift is active.

The figure below displays an example of a NTP configuration with the primary server set to ntp.cesnet.cz and the secondary server set to tik.cesnet.cz and with the automatic change for daylight saving time enabled.

NTP Configuration

- [ ] Enable local NTP service

- [x] Synchronize clock with NTP server
  - Primary NTP Server: ntp.cesnet.cz
  - Secondary NTP Server: tik.cesnet.cz

  - Timezone: GMT+01:00
  - Daylight Saving Time: yes

[Apply]

Figure 3.37 Example of NTP Configuration

3.4.8.4 SNMP

The SNMP page allows you to configure the SNMP v1/v2 or v3 agent which sends information about the device (and its expansion ports) to a management station. To open the SNMP page, click SNMP in the Configuration section of the main menu. SNMP (Simple Network Management Protocol) provides status information about the network elements such as devices or endpoint computers. In the version v3, the communication is secured (encrypted). To enable the SNMP service, mark the Enable the SNMP agent check box. Sending SNMP traps to IPv6 address is supported.

To access this page, click **Configuration** > **Services** > **SNMP**.

SNMP Configuration

- [x] Enable SNMP agent
  - Name *
  - Location *
  - Contact *
  - (*Configuration via SNMP is not possible.*)

- [x] Enable SNMPv1/v2 access

	Read	Write
Community	public	private

- [ ] Enable SNMPv3 access

	Read	Write
Username		
Authentication	MD5	MD5
Authentication Password		
Privacy	DES	DES
Privacy Password		

- [ ] Enable I/O extension

- [ ] Enable M-BUS extension
  - Baudrate: 300
  - Parity: even
  - Stop Bits: 1

- [ ] Enable reporting to supervisory system
  - IP Address
  - Period: min

  * can be blank

[Apply]

Figure 3.38 Configuration > Services > SNMP

Item	Description
Name	Designation of the device.

Item	Description
Location	Location of where you installed the device.
Contact	Person who manages the device together with information how to contact this person.

To enable the SNMPv1/v2 function, mark the Enable SNMPv1/v2 access check box. It is also necessary to specify a password for access to the Community SNMP agent. The default setting is public.

You can define a different password for the Read community (read only) and the Write community (read and write) for SNMPv1/v2. You can also define 2 SNMP users for SNMPv3. You can define a user as read only (Read), and another as read and write (Write). The device allows you to configure the parameters in the following table for every user separately. The device uses the parameters for SNMP access only.

To enable the SNMPv3 function, mark the Enable SNMPv3 access check box, then specify the following parameters:

Item	Description
Username	User name
Authentication	Encryption algorithm on the Authentication Protocol that is used to verify the identity of the users.
Authentication Password	Password used to generate the key used for authentication.
Privacy	Encryption algorithm on the Privacy Protocol that is used to ensure confidentiality of data.
Privacy Password	Password for encryption on the Privacy Protocol.

Activating the Enable I/O extension function allows you monitor the binary I/O inputs on the device.

Selecting Enable M-BUS extension and entering the Baudrate, Parity and Stop Bits lets you monitor the meter status connected to the expansion port MBUS status.

Selecting Enable reporting to supervisory system and entering the IP Address and Period lets you send statistical information to the monitoring system, R-SeeNet.

Item	Description
IP Address	IPv4 or IPv6 address.
Period	Period of sending statistical information (in minutes).

Each monitored value is uniquely identified using a numerical identifier OID - Object Identifier. This identifier consists of a progression of numbers separated by a point. The shape of each OID is determined by the identifier value of the parent element and then this value is complemented by a point and current number. So it is obvious

that there is a tree structure. The following figure displays the basic tree structure that is used for creating the OIDs.
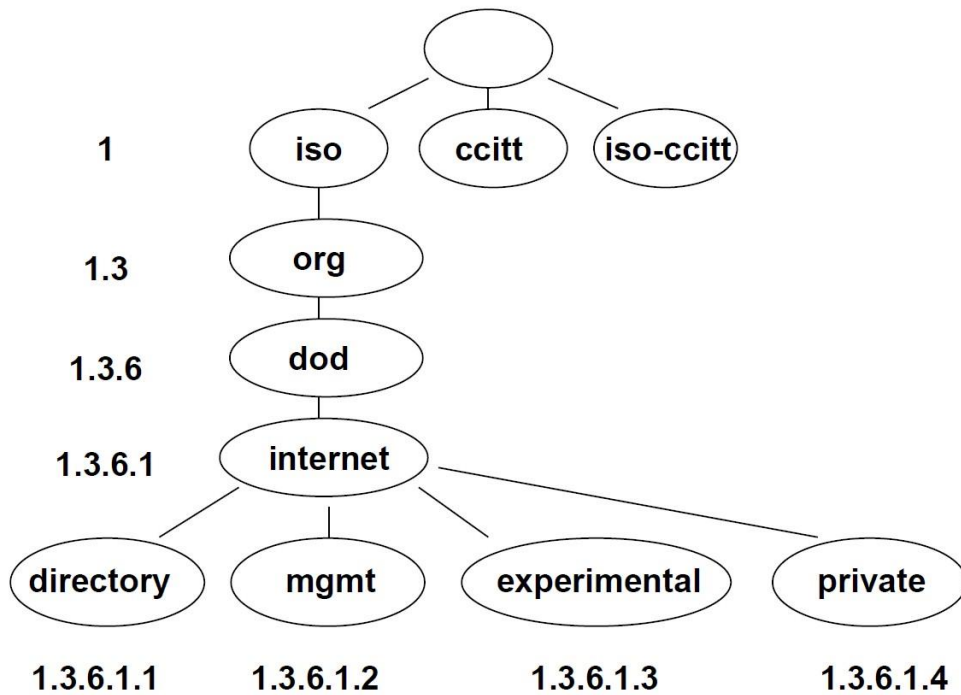
Figure 3.39 OID Basic Structure

The SNMP values that are specific for Conel devices create the tree starting at OID = .1.3.6.1.4.1.30140. You interpret the OID in the following manner:

iso.org.dod.internet.private.enterprises.conel

This means that the device provides for example, information about the internal temperature (OID 1.3.6.1.4.1.248.40.1.3.3) or about the power voltage (OID 1.3.6.1.4.1.248.40.1.3.4). For binary inputs and output, the following range of OID is used:

OID	Description
.1.3.6.1.4.1.30140.2.3.1.0	Binary input BIN0 (values 0,1)
.1.3.6.1.4.1.30140.2.3.2.0	Binary output OUT0 (values 0,1)
.1.3.6.1.4.1.30140.2.3.3.0	Binary input BIN1 (values 0,1)

The list of available and supported OIDs and other details can be found in the application note SNMP Object Identifier [8].

Figure 3.40 SNMP Configuration Example

Figure 3.41 MIB Browser Example

In order to access a particular device enter the IP address of the SNMP agent which is the device, in the Remote SNMP agent field. The dialog displayed the internal variables in the MIB tree after entering the IP address. Furthermore, you can find the status of the internal variables by entering their OID.

The path to the objects is:

iso ? org ? dod ? internet ? private ? enterprises ? conel ? protocols

The path to information about the device is:

iso ? org ? dod ? internet ? mgmt ? mib-2 ? system

3.4.8.5 SMTP

Use the SMTP form to configure the Simple Mail Transfer Protocol client (SMTP) for sending e-mails. IPv6 e-mail servers are supported.

To access this page, click **Configuration** > **Services** > **SMTP**.

Figure 3.42 Configuration > Services > SMTP

Item	Description
SMTP Server Address	IPv4 address, IPv6 address or domain name of the mail server.
SMTP Port	Port the SMTP server is listening on.
Secure Method	None, SSL/TLS, or STARTTLS. Secure method has to be supported by the SMTP server.
Username	Name for the e-mail account.
Password	Password for the e-mail account. The password can contain the following special characters * + , - . / : = ? ! # % [ ] _ { } ~ The following special characters are not allowed: " $ & ' ( ) ; < >
Own Email Address	Address of the sender.

The mobile service provider can block other SMTP servers, then you can only use the SMTP server of the service provider.

Figure 3.43 SMTP Client Configuration Example

You can send e-mails from the Startup script. The Startup Script dialog is located in Scripts in the Configuration section of the main menu. The device also allows you to send e-mails using an SSH connection. Use the email command with the following parameters:

- -t: e-mail address of the receiver
- -s: subject, enter the subject in quotation marks
- -m: message, enter the subject in quotation marks
- -a: attachment file
- -r: number of attempts to send e-mail (default setting: 2)

Note! *Commands and parameters can be entered only in lowercase.*

Example: Sending an e-mail:

email -t john@doe.com -s "System Log" -m "Attached" -a /var/log/messages

The command above sends an e-mail to address john@doe.com with the subject "System Log", body message "Attached" and attachment messages file with System Log of the device directly from the directory /var/log/.

3.4.8.6 SSH

To access this page, click **Configuration** > **Services** > **SSH**.

SSH Configuration

☑ Enable SSH service

Session Timeout 600   sec

Apply

Figure 3.44 Configuration > Services > SSH

Item	Description
Enable SSH service	Click the check box to set up Ethernet encapsulation (remote access) through the Secure Shell (SSH) function.
Session Timeout	Enter the variable in minutes to define the timeout period for the session.
Apply	Click **Apply** to save the values.

3.4.9 Scripts

There is possibility to create your own shell scripts executed in the specific situations. Go to the Scripts page in the Configuration section in the menu. The menu item will expand and there are Startup Script, Up/Down IPv4 and Up/Down IPv6 scripts you can use - there is IPv4 and IPv6 independent dual stack. For more examples of Scripts and possible commands see the Application Note Commands and Scripts [1].

To access this page, click **Configuration** > **Scripts**.

3.4.9.1 Startup Script
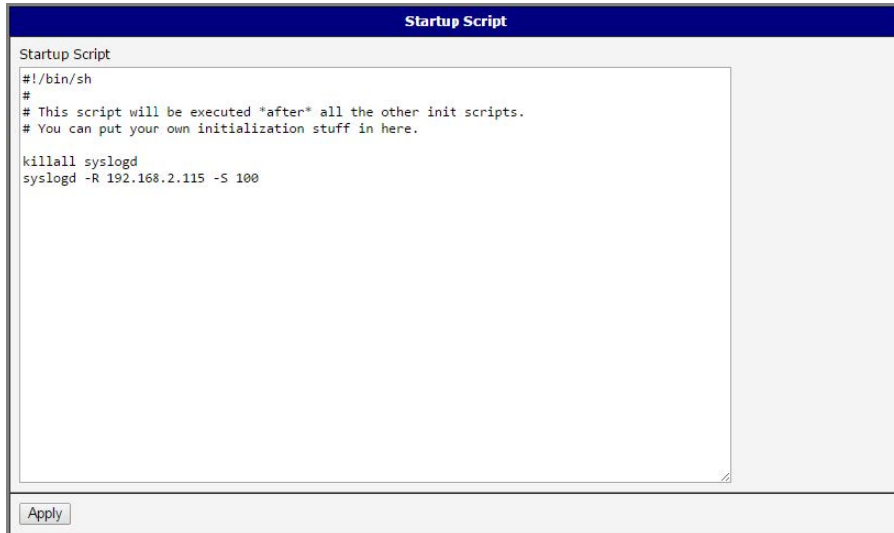
Use the Startup Script window to create your own scripts which will be executed after all of the initialization scripts are run - right after the device is turned on or rebooted. The changes in settings will apply after pressing the **Apply** button.

To access this page, click **Configuration** > **Scripts** > **Startup Script**.

> **Note!** *Any changes to the Startup Script will take effect the next time the device is power cycled or rebooted. This can be done with the Reboot button in the Administration section, or by SMS message.*

Example: Startup Script

Figure 3.45 Example of a Startup Script

When the device starts up, stop syslogd program and start syslogd with remote logging on address 192.168.2.115 and limited to 100 entries. Add these lines to the Startup Script:

    killall syslogd

    syslogd -R 192.168.2.115 -S 100

3.4.9.2 Up/Down Scripts

Use the Up/Down IPv4 and Up/Down IPv6 page to create scripts executed when the Mobile WAN connection is established (up) or lost (down). There is independent IPv4 and IPv6 dual stack implemented in the device, so there is independent IPv4 and IPv6 Up/Down script. IPv4 Up/Down Script runs only on the IPv4 WAN connection established/lost, IPv6 Up/Down Script runs only on the IPv6 WAN connection established/lost. Any scripts entered into the Up Script window will run after a WAN connection is established. Script commands entered into the Down Script window will run when the WAN connection is lost.

The changes in settings will apply after pressing the **Apply** button. Also you need to reboot the device to make Up/Down Script work.

To access this page, click **Configuration** > **Scripts** > **Up/Down IPv4** or **Up/Down IPv6**.

Example: IPv6 Up/Down Script

Figure 3.46 Example of IPv6 Up/Down Script

After establishing or losing an IPv6 WAN connection (connection to mobile network), the device sends an email with information about the connection state. It is necessary to configure SMTP before.

Add this line to the Up Script field:

email -t name@domain.com -s "Router" -m "Connection up."

Add this line to the Down Script field:

email -t name@domain.com -s "Router" -m "Connection down."

3.4.10 Automatic Update

Use the Automatic Update menu to configure the automatic update settings. The device can be configured to automatically check for firmware and configuration updates from a HTTP(S) or FTP(S) server. IPv6 sites/servers are supported. Used protocol is specified by an address in Base URL field: HTTP, HTTPS, FTP or FTPS. To prevent possible unwanted manipulation of the files, the device verifies that the downloaded file is in the tar.gz format. At first, the format of the downloaded file is checked. Then the type of architecture and each file in the archive (tar.gz file) is checked.

If the Enable automatic update of configuration option is selected, the device will check if there is a configuration file on the remote server, and if the configuration in the file is different than its current configuration, it will update its configuration to the new settings and reboot.

If the Enable automatic update of firmware option is checked, the device will look for a new firmware file and update its firmware if necessary.

To access this page, click **Configuration** > **Automatic Update**.

Figure 3.47 Configuration > Automatic Update

Item	Description
Base URL	Base URL, IPv4 or IPv6 address from which the configuration file will be downloaded. This option also specifies the communication protocol (HTTP, HTTPS, FTP or FTPS), see examples below.
Unit ID	Name of configuration (name of the file without extension). If the Unit ID is not filled, the MAC address of the device is used as the filename (the delimiter colon is used instead of a dot.)
Update Hour	Use this item to set the hour (range 1-24) when the automatic update will be performed every day. If the time is not specified, automatic update is performed five minutes after turning on the device and then every 24 hours. If the detected configuration file is different from the running one, it is downloaded and the device is restarted automatically.

The configuration file name consists of Base URL, hardware MAC address of ETH0 interface and cfg extension. Hardware MAC address and cfg extension are added to the file name automatically and it isn't necessary to enter them. When the parameter Unit ID is enabled, it defines the concrete configuration name which will be downloaded to the device, and the hardware MAC address in the configuration name will not be used.

The firmware file name consists of Base URL, type of device and bin extension. For the proper firmware filename, see the Update Firmware page in Administration section - it us written out there. See "Update Firmware" on page 74.

Note! *It is necessary to load two files (.bin and .ver) to the HTTP/FTP server. If only the .bin file is uploaded and the HTTP server sends the incorrect answer of 200 OK (instead of the expected 404 Not Found) when the device tries to download the nonexistent .ver file, then there is a risk that the device will download the .bin file over and over again.*

Note! *Firmware update can cause incompatibility with the user modules. It is recommended that you update user modules to the most recent version. Information about the user modules and the firmware compatibility is at the beginning of the user module's Application Note.*

Example 1: Automatic Update

In the following example the device checks for new firmware or configuration file each day at 1:00 a.m. An example is given for the WISE-6610 Series device.

- Firmware file: http://example.com/SPECTRE-v3L-LTE.bin
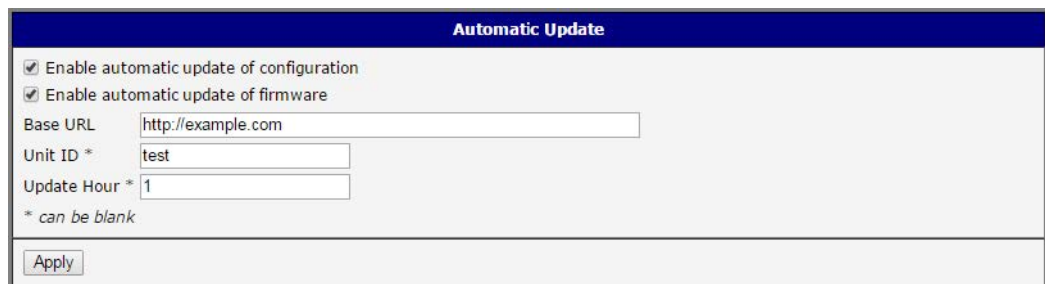- Configuration file:http://example.com/test.cfg

Figure 3.48 Example of Automatic Update 1

Example 2: Automatic Update Based on MAC

In the following example the device checks for new firmware or configuration each day at 1:00 a.m. An example is given for the WISE-6610 Series device with MAC address 00:11:22:33:44:55.

- Firmware file: http://example.com/SPECTRE-v3L-LTE.bin
- Configuration file: http://example.com/00.11.22.33.44.55.cfg
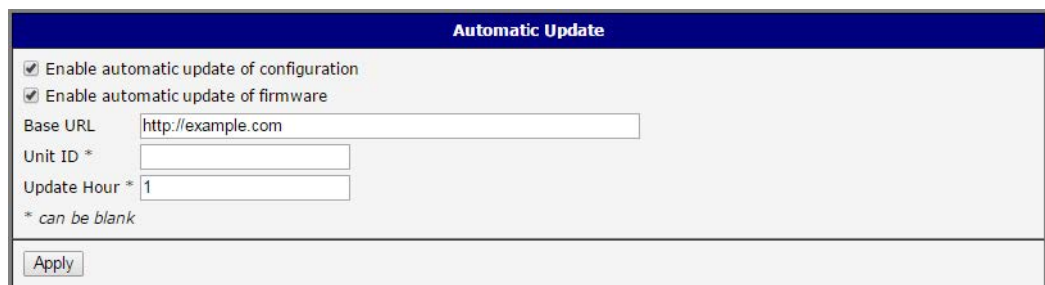
Figure 3.49 Example of Automatic Update 2

3.5 Customization

3.5.1 Adding a Module

You may run custom software programs in the device to enhance the features of the device. Use the User Modules menu item to add new software modules to the device, to remove them, or to change their configuration. Use the **Browse** button to select the user module (compiled module has tgz extension). Use the **Add** button to add a user module.

To access this page, click **User Modules** (located under Customization).

The new module appears in the list of modules on the same page. If the module contains an index.html or index.cgi page, the module name serves as a link to this page. The module can be deleted using the **Delete** button.

Updating a module is done the same way. Click the **Add** button and the module with the higher (newer) version will replace the existing module.

Programming and compiling of modules is described in the Application Note Programming of User Modules [10].
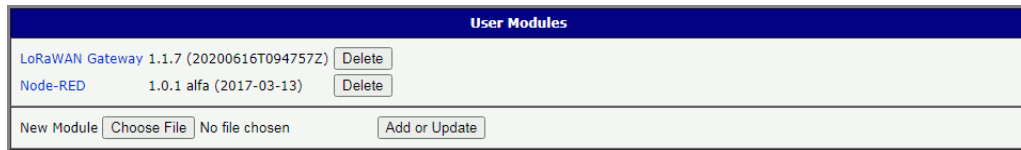

Figure 3.50 User Modules

Note! In some cases the firmware update can cause incompatibility with installed user modules. Some of them are dependent on the version of the Linux kernel (for example SmsBE and PoS Configuration). It is best to update user modules to the most recent version.

Information about the user module and the firmware compatibility is at the beginning of the user module's Application Note.

3.5.2 LoRaWAN Radio

3.5.2.1 Packet Forward

To access the LoRaWAN packet forwarding settings, navigate to Customization and click **User Modules** > **LoRaWAN Gateway** > **LoRaWAN Radio**.
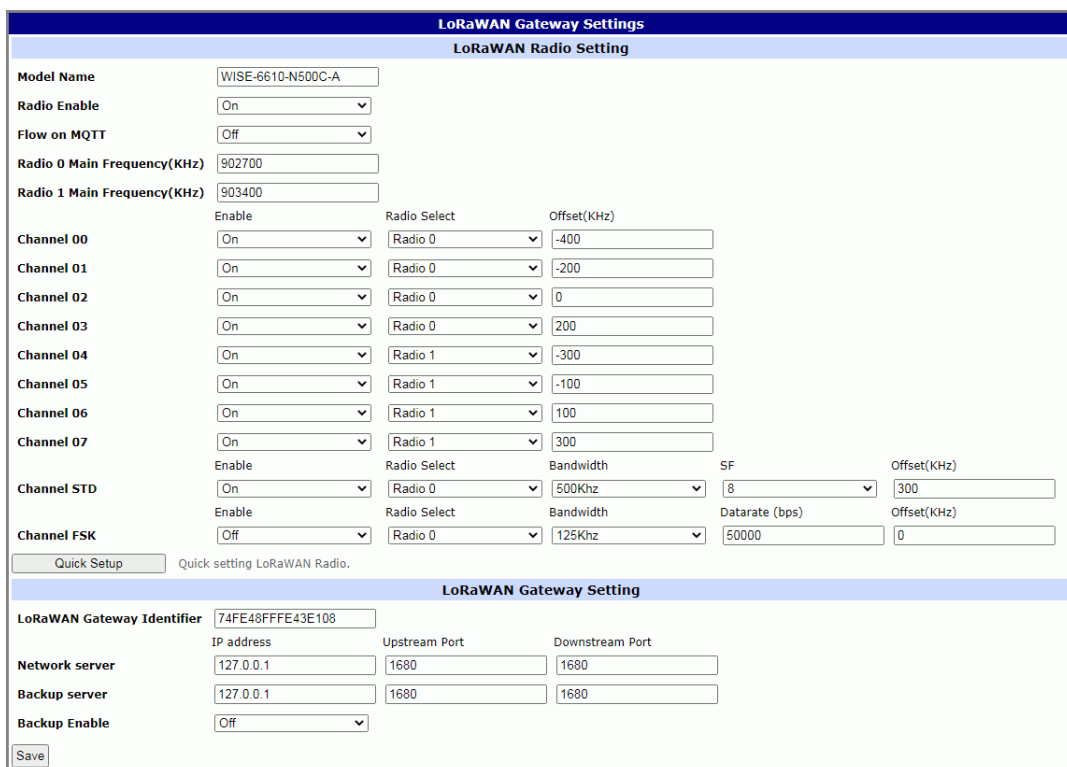
Figure 3.51 User Modules > LoRaWAN Gateway > LoRaWAN Radio

Item	Description
LoRaWAN Radio Setting	
Model Name	Enter the model name.
Radio Enable	Click the drop-down menu to enable the radio channel and corresponding settings.
Flow on MQTT	Click to enable or disable the data flow through the MQTT plugin.

Item	Description
Radio 0 Main Frequency (KHz)	Enter the frequency setting for the interface.
Radio 1 Main Frequency (KHz)	Enter the frequency setting for the interface.
Channel 00 ~ 07	■ Click drop-down menu to enable or disable the channel. ■ Click the Radio Select drop-down menu to select the radio to listen for packets. ■ Enter the frequency offset in KHz between transmitter and receiver.
Channel STD	■ Click drop-down menu to enable or disable the channel. ■ Click the Radio Select drop-down menu to select the radio to listen for packets. ■ Click the Bandwidth drop-down menu to select the channel bandwidth (250 / 500Khz) ■ Click the drop down menu to select the channel spreading factor (7-12). ■ Enter the intermediate frequency offset applied to the selected radio setting.
Channel FSK	■ Click drop-down menu to enable or disable the channel. ■ Click the Radio Select drop-down menu to select the radio to listen for packets. ■ Click the Bandwidth drop-down menu to select the channel bandwidth (125 / 250Khz). ■ Enter the channel data rate in bps. ■ Enter the intermediate frequency offset applied to the selected radio setting.
Quick Setup	Click to enter the Quick Setup menu enabling the selection of pre-configured region-specific, radio frequency settings.
LoRaWAN Gateway Setting	
LoRaWAN Gateway Identifier	Displays the gateway identifier for the remote LoRa network server.
Network Server	Enter the IP address of the network server. Enter the upstream port number. Enter the downstream port number.
Backup server	Enter the IP address of the backup server. Enter the upstream port number. Enter the downstream port number.
Backup Enable	Click the drop-down menu to enable (default: Off) the LoRaWAN backup feature.
Save	Click **Save** to save the values.

3.5.2.2 LoRaWAN Status

To access the gateway configuration page, navigate to Customization and click **User Modules** > **LoRaWAN Gateway** > **LoRaWAN Radio** > **LoRaWAN Status**.

LoRaWAN Gateway Settings							
Basic Status							

Data Record Time : 2020-09-18T07:09:39Z
Total Up Stream : 0 Bytes
CRC OK packet   : 0
CRC Bad packet   : 62
NO CRC packet   : 0

Channel Status

Channel	Radio Index	Enabled	Frequency(Hz)	Received(Bytes)
0	0	Enabled	902300000	0
1	0	Enabled	902500000	0
2	0	Enabled	902700000	0
3	0	Enabled	902900000	0
4	1	Enabled	903100000	0
5	1	Enabled	903300000	0
6	1	Enabled	903500000	0
7	1	Enabled	903700000	0
STD	0	Enabled	903000000	0
FSK	0	Disabled		0

Uplink Frame

UTC Time	Type	Devaddr/EUI	Freq	DR	RSSI	Fcnt	Data

Download Frame

Type	Devaddr/EUI	Freq	DR	Fcnt	Data

Refresh

Figure 3.52 User Modules > LoRaWAN Gateway > LoRaWAN Radio > LoRaWAN Status

Item	Description
Basic Status	
Basic Status	Displays basic gateway status.
Channel Status	Displays channel status.
Uplink Frame	Displays uplink information.
Download Frame	Displays download frame information
Refresh	Click **Refresh** to update the display.

3.5.3 Network Server

3.5.3.1 Settings

To access the gateway configuration page, navigate to Customization and click **User Modules** > **LoRaWAN Gateway** > **Network Server > Settings**.

Figure 3.53 User Modules > LoRaWAN Gateway > Network Server > Settings

Item	Description
LoRaWAN Network Server Setting	
LoRaWAN Network Server Enable	Click the drop-down menu to disable the LoRaWAN network server (default: On).
LoRaWAN Server Listen Port	Enter a variable (1 to 65535) to designate the listening port.
LoRaWAN Network Server HTTPS Port	Click the drop-down menu to enable the HTTPS service (default: Off).
LoRaWAN Web Username	Enter an identifier used to access the Web user interface for the LoRaWAN network server.
LoRaWAN Web Password	Enter the corresponding password to the set LoRaWAN Web username.
Auto ADR Count	Enter the number of rows to return (5 to 50) by the function.
LoRaWAN Network Server HTTPS Enable	Click the drop-down menu to enable the HTTPS service (default: Off).
Google Map API Key	Enter the unique identifier to authenticate for the Google Cloud Platform Console.
Refresh	Click **Refresh** to update the display.

3.5.3.2 Network Server (http)

To access the Network Server (http) page, navigate to Customization and click **User Modules** > **LoRaWAN Gateway** > **Network Server > Network Server (http)**.

The Dashboard interface open through the default browser as seen in the following:

Figure 3.54 User Modules > LoRaWAN Gateway > Network Server > Network Server (http)

3.5.3.3 Network Server (https)

Enable the **LoRaWAN Network Server HTTPS Enable** function under **MQTT and LoRaWAN** to access the website through https.

To access the Network Server (http) page, navigate to Customization and click **User Modules** > **LoRaWAN Gateway** > **Network Server > Network Server (https)**.

The Dashboard interface open through the default browser as seen in the following:
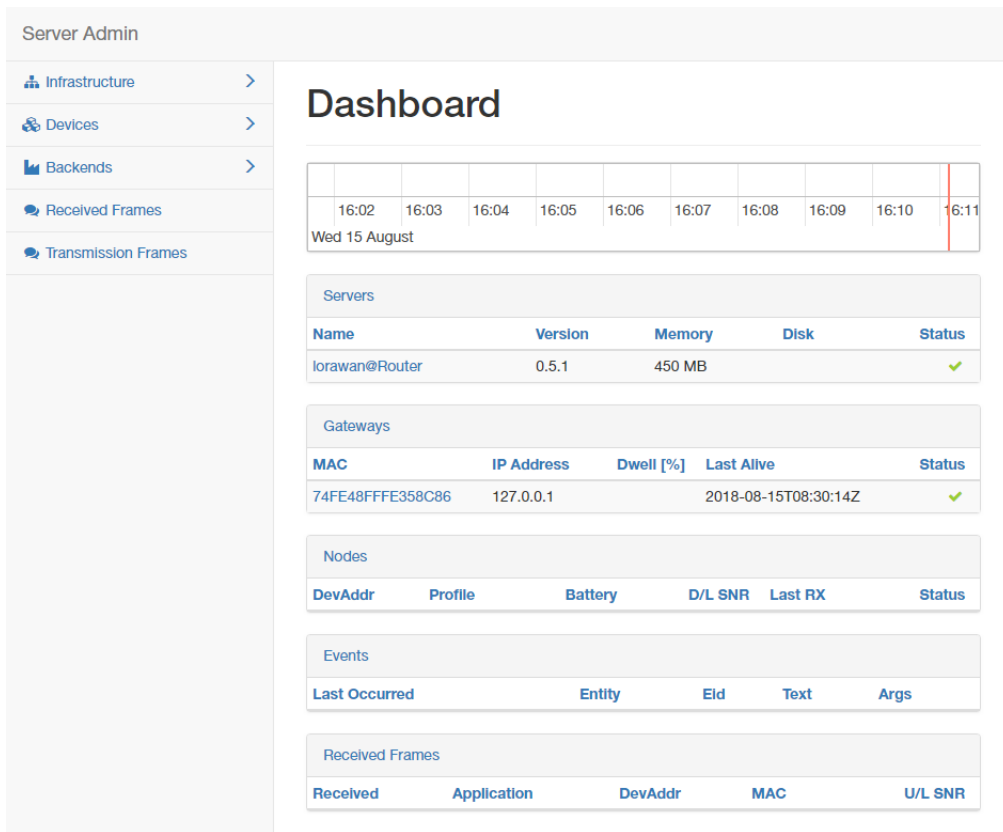

Figure 3.55 User Modules > LoRaWAN Gateway > Network Server > Network Server (https)

3.5.3.4 Database management

To access the Network Server (http) page, navigate to Customization and click **User Modules** > **LoRaWAN Gateway** > **Network Server > Database Management**.

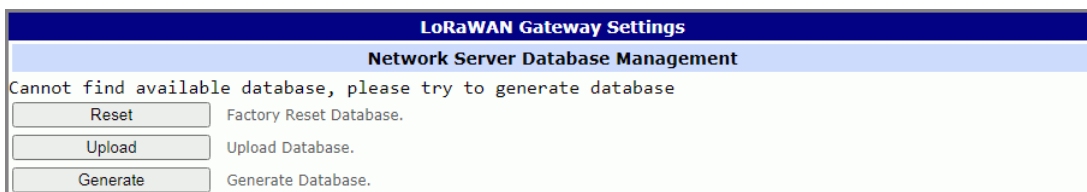The Dashboard interface open through the default browser as seen in the following:

Figure 3.56 User Modules > LoRaWAN Gateway > Network Server > Database Management

Item	Description
Network Server Database Management	
Reset	Click to reset the database to the initial factory settings.
Upload	Click to select a database file to upload. ■ Click the **Choose File** button to select a file. ■ Click **Upload** to confirm the file. ■ Click **Return** to go back to the previous page.
Generate	Click to generate the selected database file. If no file is selected, a notification is displayed to return to the DataBase Management page to download the network server database. Click **Return** to go back to the previous menu.

3.5.3.5 MQTT

To access the gateway configuration page, navigate to Customization and click **User Modules** > **LoRaWAN Gateway** > **MQTT**.

Figure 3.57 User Modules > LoRaWAN Gateway > MQTT

Item	Description
MQTT Broker	
MQTT Broker Enable	Click the drop-down menu to enable or disable local MQTT broker.
MQTT Broker Port	Enter a value to specify the port of MQTT broker (default: 1883).
MQTT Bridge	
MQTT Bridge Enable	Click the drop-down menu to enable or disable bridging to a remote MQTT broker.
MQTT Bridge Port	Enter a value to specify the port of MQTT bridge (default: 1883).
MQTT Bridge Address	Enter a value to specify the bridge address of the MQTT bridge.
MQTT Bridge User	Enter the name of the MQTT bridge user.
MQTT Bridge Password	Enter the character set for the define password type.u
MQTT Bridge Client Identifier	With MQTT and LoRa configured, pair and modify the node settings, see Node Control.
Save	Click **Save** to save the values.

3.5.4 Application Server

3.5.4.1 Settings

To access the gateway configuration page, navigate to Customization and click **User Modules** > **LoRaWAN Gateway** > **Application Server**.

Due to the length of the Application Server UI screen, the screen image was divided into two sections to allow for the description of all the settings. However, the menu is a single screen.

Figure 3.58 User Modules > LoRaWAN Gateway > Application Server

Item	Description
Advantech Application Server Setting	
Application Server Enable	Click the drop-down menu to enable the local Application server (default: Off).
Application Server Connect MQTT Address	Enter the private network address to allow bidirectional sending and receiving of messages.
Application Server Connect MQTT Port	Enter a port designation to associate with the previously defined network address.
MQTT Username	Enter an identifier used to access the remote MQTT broker.
MQTT Password	Enter the password associated with the MQTT user listed previously.
Uplink Topic	Enter a string identifier to describe the MQTT broker, uplink, subscription topic.
Downlink Topic	Enter a string identifier to describe the MQTT broker, downlink, subscription topic.
MQTT Publish Retain	Click the drop-down menu to enable or disable the publish retain function.
MQTT Publish QoS	Enter the internal publish quality of service level (0-2).
Modbus TCP Server	Click the drop-down menu to enable or disable the Modbus TCP server.
Modbus TCP Server Port	Enter the access port for the defined TCP server (1 - 65535).
Modbus Timeout	Enter the variable to define the timeout number (2 - 30).
SD Card Logging	Click the drop-down menu to enable or disable the function allowing the saving of log files to an SD card. Function only supported by the WISE 6610 v2.
Time Sync	Click the drop-down menu to enable or disable the Time synchronization for the WISE 2410/4610 series.

RESTful Server and Advantech WISE-PaaS Settings

Figure 3.59 User Modules > LoRaWAN Gateway > Application Server

Item	Description
RESTful Server Setting	
RESTful HTTP Enable	Click the drop-down menu to enable or disable the RESTful HTTP port 81.
RESTful HTTPS Enable	Click the drop-down menu to enable or disable the RESTful HTTPS port 8445.
Username	Enter the username to allow access to the defined RESTful API.
Password	Enter the password for the define username.
Advantech WISE-PaaS Setting	
WISE-PaaS Enable	Click the drop-down menu to disable or enable the WISE-PaaS connection.
WISE-PaaS Status	Displays the status of the WISE-PaaS connection.
WISE-PaaS Cerdential URL	Enter the credential URL to the WISE-PaaS setting.
WISE-PaaS Iotkey	Enter the Iotkey to the WISE-PaaS setting.
Save	Click **Save** to save the values.

3.5.4.2 Status

To access the gateway configuration page, navigate to Customization and click **User Modules** > **LoRaWAN Gateway** > **Application Server** > **Status**.

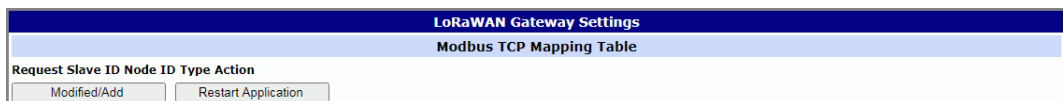Figure 3.60 User Modules > LoRaWAN Gateway > Application Server > Status

Item	Description
Application Server Setting	
Status	Displays the MQTT Status and Node number.
Advantech LoRaWAN Node	

Item	Description
Node Settings	Displays the following Node information: ■ Index ■ DevAddr ■ Battery ■ Model ■ Received ■ Fcnt ■ Packet Loss ■ Rssi ■ Action

Item	Description
Application Log	
Refresh	Click to synchronize the status screen.
Clear log	Click Clear log to delete the log history.

3.5.4.3 Modbus Mapping Table

To access the gateway configuration page, navigate to Customization and click **User Modules** > **LoRaWAN Gateway** > **Application Server** > **Modbus Mapping Table**.

Figure 3.61 User Modules > LoRaWAN Gateway > Application Server > Modbus Mapping Table

Item	Description
Modbus TCP Mapping Table	
Modified / Add	Click to **Modify** or **Add** a slave ID node.
Restart Application	Click to **Restart** the application.

3.5.4.4 Payload Engine

To access the gateway configuration page, navigate to Customization and click **User Modules** > **LoRaWAN Gateway** > **Application Server** > **Payload Engine**.
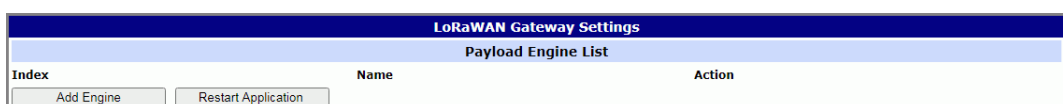
Figure 3.62 User Modules > LoRaWAN Gateway > Application Server > Payload Engine

Item	Description
Modbus TCP Mapping Table	
Add Engine	Click to **Add** a payload engine.
Restart Application	Click to **Restart** the application.

3.5.5 Licenses

To download a LoRaWAN license, navigate to the following: **User Modules** > **LoRaWAN Gateway > Licenses.**

Click Licenses to download.

3.5.6 Return to Router

The main menu is accessible through the Return to Router function. To return the WISE-6610 Series to the main menu, click **Customization > User Modules > LoRaWAN Gateway > Return to Router**.

3.6 Administration

3.6.1 Users

Note! *This configuration function is only available for users assigned the admin role!*

To assign roles and manage user accounts open the Users form in the Administration section of the main menu. The first frame of this configuration form contains an overview of available users. The table below describes the meaning of the buttons in this frame.

To access this page, click **Administration** > **Users**.

User Administration

| root | Admin | Lock | Change Password |

Role	User ▼
Username	
Password	
Confirm Password	
Add User

Figure 3.63 Administration > Users

Item	Description
Lock	Locks the user account. This user is not allowed to log in to the device, neither web interface nor SSH.
Change Password	Allows you to change the password for the corresponding user.
Delete	Deletes the corresponding user account.

Warning! *If you lock every account with the permission role Admin, you can not unlock these accounts. This also means that the Users dialog is unavailable for every user, because every admin account is locked and the users do not have sufficient permissions.*

The second block contains configuration form which allows you to add new user. All items are described in the table below.

Item	Description
Role	Specifies the type of user account: ■ User: User with basic permissions. ■ Admin: User with full permissions.
Username	Specifies the name of the user allowed to log in the device.
Password	Specifies the password for the corresponding user.
Confirm Password	Confirms the password you specified above.

> **Note!** *Ordinary users are not able to access device via Telnet, SSH or SFTP. Read only FTP access is allowed for these users.*

3.6.2 Change Profile

In addition to the standard profile, up to three alternate device configurations or profiles can be stored in device's non-volatile memory. You can save the current configuration to a device profile through the Change Profile menu item. Select the alternate profile to store the settings to and ensure that the Copy settings from current profile to selected profile box is checked. The current settings will be stored in the alternate profile after the **Apply** button is pressed. Any changes will take effect after restarting device through the Reboot menu in the web administrator or using an SMS message.

To access this page, click **Administration** > **Change Profile**.

Example: Using Profiles

Profiles can be used to switch between different modes of operation of the device such as PPP connection, VPN tunnels, etc. It is then possible to switch between these settings using the front panel binary input, an SMS message, or Web interface of the device.

Figure 3.64 Administration > Change Profile

3.6.3 Change Password

Use the Change Password configuration form in the Administration section of the main menu for changing your password used to log on the device. Enter the new password in the New Password field, confirm the password using the Confirm Password field, and press the **Apply** button.

To access this page, click **Administration** > **Change Password**.

Warning! *The default password of the device is root for the root user. To maintain the security of your network change the default password. You can not enable remote access to the device for example, in NAT, until you change the password.*

Change Password	
Username	root
New Password	
Confirm Password	
Apply	

Figure 3.65 Administration > Change Password

3.6.4 Set Real Time Clock

You can set the internal clock directly using the Set Real Time Clock dialog in the Administration section of in the main menu. You can set the Date and Time manually. When entering the values manually use the format yyyy-mm-dd as seen in the figure below. You can also adjust the clock using the specified NTP server. IPv4, IPv6 address or domain name is supported. After you enter the appropriate values, click the **Apply** button.

To access this page, click **Administration** > **Set Real Time Clock**.

Set Real Time Clock	
Date	2018 - 01 - 17
Time	15 : 18 : 01
NTP Server Address	
Apply	

Figure 3.66 Administration > Set Real Time Clock

3.6.5 Backup Configuration

You can save the configuration of the device using the Backup Configuration function. If you click on Backup Configuration in the Administration section of the main menu, then the device allows you to select a directory in which the device saves the configuration file.

3.6.6 Restore Configuration

You can restore a configuration of the device using the Restore Configuration form. To navigate to the directory containing the configuration file (.cfg) you wish to load on the device, use the **Browse** button.

To access this page, click **Administration** > **Restore Configuration**.

Restore Configuration	
Configuration File	Browse...
Apply	

Figure 3.67 Administration > Restore Configuration

3.6.7 Update Firmware

Select the Update Firmware menu item to view the current device firmware version and load new firmware into the device. There is current firmware version and firmware filename written out. When loading the new firmware, it has to have this name. To load new firmware, browse to the new firmware file and press the **Update** button to begin the update.

Warning! *Do not turn off the device during the firmware update. The firmware update can take up to five minutes to complete. Always use the filename written out as Firmware Name when updating the firmware.*

To access this page, click **Administration** > **Update Firmware**.

Figure 3.68 Administration > Update Firmware

During the firmware update, the device will show the following messages. The progress is shown in the form of adding dots ('.').

After the firmware update, the device will automatically reboot.

Note! *Uploading firmware intended for a different device can cause damage to the device.*

Starting with FW 5.1.0, a mechanism to prevent multiple startups of the firmware update is included. Firmware update can cause incompatibility with the user modules. It is recommended to update user modules to the most recent version. Information about user module and firmware compatibility is at the beginning of the user module's Application Note.

3.6.8 Reboot

To reboot the device select the Reboot menu item and then press the **Reboot** button.

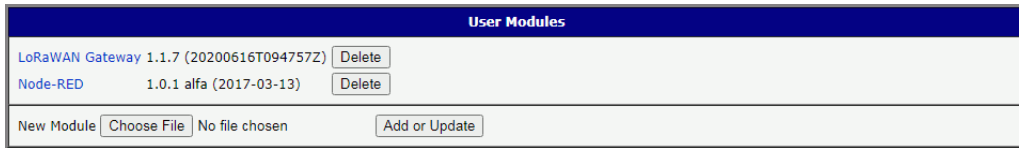To access this page, click **Administration** > **Reboot**.

Figure 3.69 Administration > Reboot

Chapter 4

Configuration in Typical Situations

4.1 Enabling the LoRaWAN and Network Server

1. Login WISE-6610 Series. See "Access Interface" on page 18.
2. Go to **Customization** > **User Modules**.
3. A list of available devices display. Click on the target **LoRaWAN Gateway**.

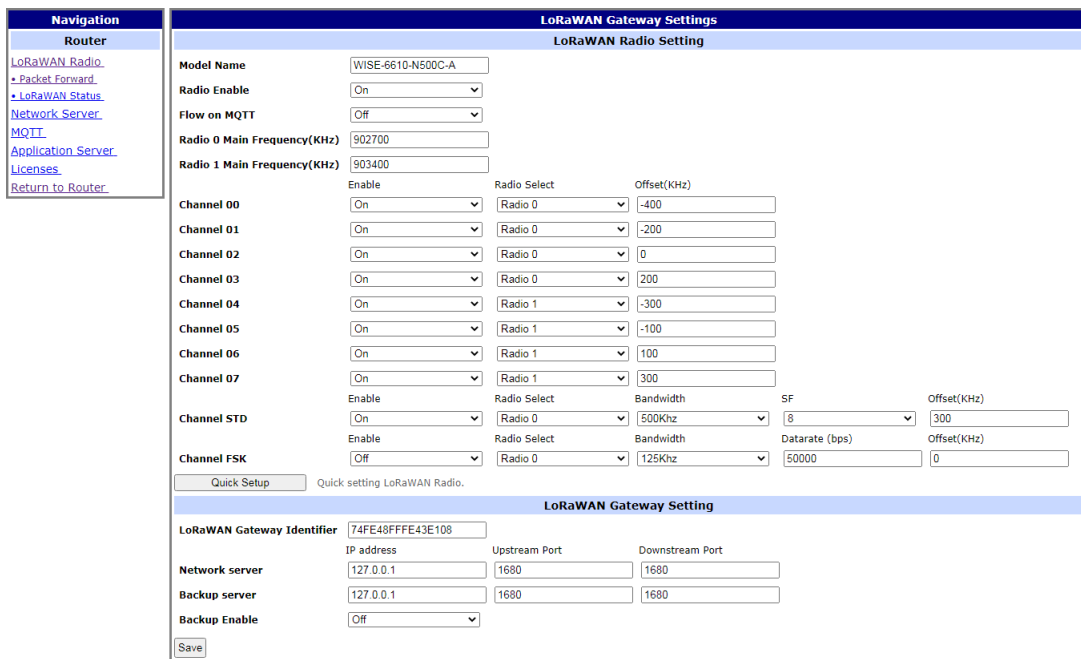| User Modules		
LoRaWAN Gateway 1.1.7 (20200616T094757Z)	Delete	
Node-RED 1.0.1 alfa (2017-03-13)	Delete	
New Module Choose File No file chosen	Add or Update	

Figure 4.1 Customization > User Modules

4. The Settings menu displays. In **LoRaWAN Radio Enable**, click the drop-down menu to enable LoRaWAN function.
5. Configure the main frequency for radio 0 and radio 1. For radio 1, there are eight channels and one standard channel.

Note!
1. *The offset setting for the eight channels must be +/-500KHz.*
2. *Use Quick Setup to define the main frequency for receiving the data from the LoRaWAN node.*

3. In **LoRaWAN Gateway Identifier**, copy the gateway ID and set on LoRaWAN network server.

Navigation		LoRaWAN Gateway Settings			
Router		LoRaWAN Radio Setting			
LoRaWAN Radio	Model Name	WISE-6610-N500C-A			
• Packet Forward	Radio Enable	On			
• LoRaWAN Status	Flow on MQTT	Off			
Network Server	Radio 0 Main Frequency(KHz)	902700			
MQTT	Radio 1 Main Frequency(KHz)	903400			
Application Server		Enable	Radio Select	Offset(KHz)	
Licenses	Channel 00	On	Radio 0	-400	
Return to Router	Channel 01	On	Radio 0	-200	
	Channel 02	On	Radio 0	0	
	Channel 03	On	Radio 0	200	
	Channel 04	On	Radio 1	-300	
	Channel 05	On	Radio 1	-100	
	Channel 06	On	Radio 1	100	
	Channel 07	On	Radio 1	300	

	Enable	Radio Select	Bandwidth	SF	Offset(KHz)
Channel STD	On	Radio 0	500Khz	8	300

	Enable	Radio Select	Bandwidth	Datarate (bps)	Offset(KHz)
Channel FSK	Off	Radio 0	125Khz	50000	0

Quick Setup	Quick setting LoRaWAN Radio.

	LoRaWAN Gateway Setting		
LoRaWAN Gateway Identifier	74FE48FFFE43E108		
	IP address	Upstream Port	Downstream Port
Network server	127.0.0.1	1680	1680
Backup server	127.0.0.1	1680	1680
Backup Enable	Off		
Save			

Figure 4.2 LoRaWAN Gateway > MQTT and LoRaWAN

4. In **LoRaWAN Network Server Setting**, click the drop-down menu to enable LoRaWAN network server.

5. In **MQTT Broker Enable**, click the drop-down menu to enable MQTT broker.

LoRaWAN Network Server Setting

LoRaWAN Network Server Enable
On ▼   Enable LoRaWAN network server.

LoRaWAN Server Listen Port
1680   The LoRa network server listen port number (1 - 65535).

LoRaWAN Network Server HTTP Port
8080   The LoRaWAN network server HTTP port number (1 - 65535).

LoRaWAN Network Server HTTPS Port
8443   The LoRaWAN network server HTTPS port number (1 - 65535).

LoRaWAN Web Username
root   The user name for the LoRaWAN network server.

LoRaWAN Web Password
root   The password for the LoRaWAN network server.

LoRaWAN Network Server HTTPS Enable
On ▼   Enable HTTPS service.
Upload Database   Upload LoRaWAN network server database.
Download Database   Download LoRaWAN network server database.
Factory Reset   Reset LoRaWAN network server database.

MQTT Broker

MQTT Broker Enable
On ▼   Enable the local MQTT broker.

MQTT Broker Port
1883   The local MQTT broker TCP port number (1 - 65535).

MQTT Bridge

MQTT Bridge Enable
On ▼   Enable bridging to a remote MQTT broker.

Figure 4.3 LoRaWAN Gateway > MQTT and LoRaWAN

6. Click **Save** to save the configuration.
7. Click **LoRaWAN Server** and enter the default user name and password (root/root) to log into the LoRaWAN Network Server page.

Note!   *The LoRaWAN Network Server does not support IE or EDGE browser.*

Figure 4.4 LoRaWAN Gateway > LoRaWAN Server

8. Click **Infrastructure** > **Gateways** to enter the Gateways List page.
9. Click **Create** to add a new gateway.

Figure 4.5 LoRaWAN Server > Infrastructure > Gateways

10. In the Create new gateway page, configure the new gateway settings. Input the MAC which is the LoRaWAN gateway ID shows on the LoRaWAN setting Page.

Figure 4.6 LoRaWAN Server > Infrastructure > Gateways > Create

Item	Description
MAC	Enter the LoRaWAN gateway ID shown on **MQTT and LoRaWAN** menu.
Group	Enter the opaque string with application-specific settings.
TX Chain	Enter a value to identify the radio chain used for downlinks (default: 0). It shall correspond to a `radio_x` (e.g. `radio_0`) with `tx_enable: true` in gateway's `global_conf.json`.
Antenna Gain (dBi)	Enter a value to ensure the TX Power + Antenna Gain is below the maximal allowed Equivalent Isotropic Radiated Power (EIRP) for the given Network.
Description	Enter the description for the gateway.
Submit	Click **Submit** to save the values and update the screen.

11. Click **Infrastructure** > **Networks** to enter the Networks List page.
By default, the WISE-6610 Series pre-configures the network to support EU868, AU915, AS923 and US902.

Figure 4.7 LoRaWAN Server > Infrastructure > Networks

12. Click **Create** to create your own network frequency.

Figure 4.8 LoRaWAN Server > Infrastructure > Network > Create > General

Item	Description
Name	Enter the name of the network.
NetID	Enter the NetID of the network. Use 000000 or 000001 for private networks.
SubID	Enter the SubID of the network in the format of HexValue:Length which specifies the fixed bits in the DevAddr of the active node. (optional)
Region	Enter a value to determine the regional characteristics of LoRaWAN.
Coding Rate	Enter a value to define the coding rate. It is regularly set on 4/5.
RX1 Join Delay (s)	Enter a value to define the JOIN_ACCEPT_DELAY1.
RX2 Join Delay (s)	Enter a value to define the JOIN_ACCEPT_DELAY2.
RX1 Delay (s)	Enter a value to define the RECEIVE_DELAY1.
RX2 Delay (s)	Enter a value to define the RECEIVE_DELAY2.
Gateway Power (dBm)	Enter a value to define the default transmission power for downlinks.
Submit	Click **Submit** to save the values and update the screen.

In the General tab, follow the table below when configuring a new network:

Parameter	EU868	US902	CN779	EU433	AU915	CN580	AS923	KR920	IN865	RU864
Coding Rate	4/5	4/5	4/5	4/5	4/5	4/5	4/5	4/5	4/5	4/5
RX1 Join Delay(s)	5	5	5	5	5	5	5	5	5	5

Parameter	EU868	US902	CN779	EU433	AU915	CN580	AS923	KR920	IN865	RU864
RX2 Join Delay(s)	6	6	6	6	6	6	6	6	6	6
RX1 Delays	1	1	1	1	1	1	1	1	1	1
RX2 Delays	2	2	2	2	2	2	2	2	2	2
Gateway Power	16	26	12	12	30	19	16	23	30	16
Max EIRP (dBm)	16	30	12.15	12.15	30	19.15	16	14	30	16
Max Power	Max	Max	Max	Max	Max	Max	Max	Max	Max	Max
Min Power	Max - 14 dB	Max - 20 dB	Max - 10 dB	Max - 10 dB	Max - 20 dB	Max - 14 dB	Max - 14 dB	Max - 14 dB	Max - 20 dB	Max - 14 dB
Max Data Rate	SF7 125 kHz	SF8 500 kHz	SF7 125 kHz	SF7 125 kHz	SF8 500 kHz	SF7 125 kHz	SF7 125 kHz	SF7 125 kHz	SF7 125 kHz	SF7 125 kHz
Initial RX1 DR Offset	0	0	0	0	0	0	0	0	0	0
Initial RX2 DR	SF12 125 kHz	SF12 500 kHz	SF12 125 kHz	SF12 125 kHz	SF12 500 kHz	SF12 125 kHz	SF10 125 kHz	SF12 125 kHz	SF10 125 kHz	SF10 125 kHz
Initial RX2 Freq (MHz)	869.525	923.3	786	434.665	923.3	505.3	923.2	921.9	866.550	869.1
Initial Channels	0-2	0-71	0-2	0-2	0-71	0-95	0-x*	0-2	0-2	0-1

13. Click the **ADR** tab to configure the ADR settings for a specified parameter.

Figure 4.9 LoRaWAN Server > Infrastructure > Network > Create > ADR

| Item	Description
Max EIRP (dBm)	Enter a value to specify the EIRP used in your region.
Max Power	Enter a value to define the first TX Power item.
Min Power	Enter a value to define the last TX Power item.

Item	Description
Max Data Rate	Enter a value to define the highest DR (lowest SF) supported by the channels in this network. Additional channels may need to be given a different value.
	Note: The Max Data Rate is not always the last item (lowest SF) in the TX data rate table. Not all channels (frequencies) are allowed to use all data rates. For example, in EU868, the default channels use SF12/125 to SF7/125 only. The SF7/250 is allowed for the 867.3 MHz channel only and FSK for 867.7 MHz only.
Initial RX1 DR Offset	Enter a value to define the offset between the uplink and downlink data rates used to communicate with the end-device on the first reception slot (RX1).
Initial RX2 DR	Enter a value to define the data rate for the second reception slot (RX2).
Initial RX2 Freq (MHz)	Enter a value to define the default frequency in the RX2 receive window.
Submit	Click **Submit** to save the values and update the screen.

14. Click the **Channel** tab to configure the channel settings following the frequency rule.

Figure 4.10 LoRaWAN Server > Infrastructure > Network > Create > Channel

Item	Description
Initial Channels	Enter a range of values to define the initial channels including a comma-separated list of intervals, e.g. `0-2` for EU and `0-71` for US.
Channels	Click **Add new channels** to define a list of additional channels sent to the device during Join (CFList).
	■ Frequency (MHz): Enter a value to define the channel frequency.
	■ Min Data Rate: Enter a value to define the lowest data rate allowed in this channel. Enter 0 if it's not specified.
	■ Max Data Rate: Enter a value to define the highest data rate allowed in this channel. Enter the global value of the **ADR** tab if it's not specified.
Submit	Click **Submit** to save the values and update the screen.

15. Click **Backends** > **Handlers** to enter the Handlers List page.

The WISE-6610 Series handler is created by default. The LoRaWAN data comes with the item with the Field in the handler settings.
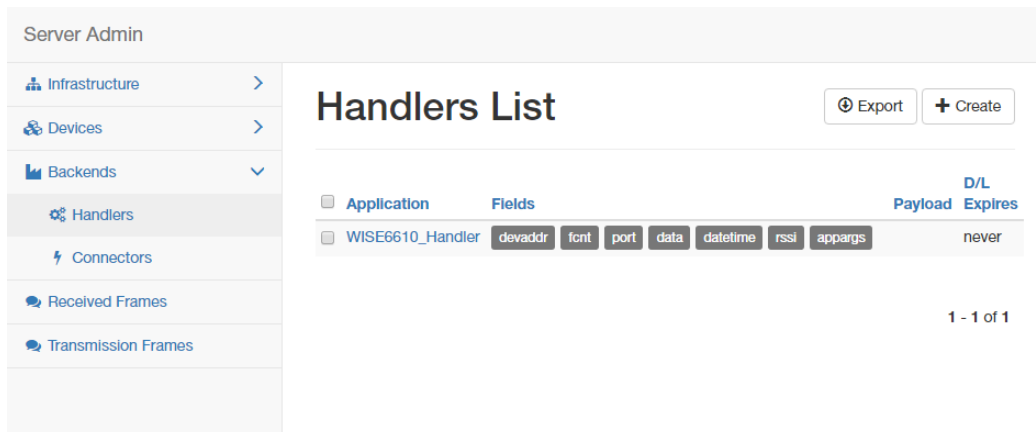
Figure 4.11 LoRaWAN Server > Backends > Handlers

Field	Type	Definition
app	String	Application (Handler) name
devaddr	Hex String	DevAddr of the active node
deveui	Hex String	DevEUI of the device
appargs	Any	Application arguments for the node
battery	Integer	Most recent battery level reported by the device
fcnt	Integer	Received frame sequence number
port	Integer	LoRaWAN port number
data	Hex String	Raw application payload encoded as a hexadecimal string
datetime	ISO 8601	Timestamp using the server clock
freq	Number	RX central frequency in MHz (unsigned float/ Hz precision)
datr	String	LoRa data rate identifier (e.g. SF12BW500)
codr	String	LoRa ECC coding rate identifier (default: 4/5)
best_gw	Object	Gateway with the strongest reception
mac	Hex String	MAC address of the gateway with the strongest reception
lsnr	Number	LoRa uplink SNR ratio in dB (signed float/ 0.1 dB precision) (same as `rxq.lsnr` for `best_gw`)
rssi	Number	RSSI in dBm (signed integer/ 1 dB precision) (same as `rxq.rssi` for `best_gw`)
all_gw	Object	List of all gateways that received the frame

16. Click **Create** to add a new handler rule. This function allows you to choose the desired uplink fields and supports the parse script option that helps you parse the raw data received from the sensor node as shown in Figure 4.13.

Figure 4.12 LoRaWAN Server > Backends > Handlers > Create

Item	Description
Application	Enter the name of the handler.
Uplink Fields	Enter the filter values to be forwarded to the backend connector.
Payload	Enter the filter values as the format for automatic decoding.
Parse Uplink	Enter the string to extract additional data fields from the uplink frame. See Figure 4.13 for references.
Parse Event	Enter the string to be forwarded to the backend connector.
Build Downlink	Enter the string to create a downlink frame based on backend data fields.

Item	Description
D/L Expires	Click the drop-down menu to define when the downlinks may be dropped. ■ Never: 　– All class A downlinks for a device will be queued and eventually delivered. 　– All confirmed downlinks will be retransmitted until acknowledged even when a new downlink is sent. ■ When Superseded: 　– Only the most recent class A downlinks will be scheduled for delivery. Superseded downlinks will be dropped. 　– Unacknowledged downlinks will be dropped when a new downlink (either class A or C) is sent.
Submit	Click **Submit** to save the values and update the screen.

```
fun(Fields,Port, <<DEV, Temp:16, Hum:16, Sensor:16>>) ->
if
  DEV==1 ->
    Fields#(device => co2, temp => Temp/100, hum => Hum/100, sensor => Sensor);
  DEV==2 ->
    Fields#(device => co, temp => Temp/100, hum => Hum/100, sensor => Sensor);
  DEV==3 ->
    Fields#(device => pm25, temp => Temp/100, hum => Hum/100, sensor => Sensor);
true ->
    false
end
end.
```

Figure 4.13 Parse Uplink Sample

17. Click **Backends** > **Connectors** to enter the Connectors List page.

The connector settings define the data flow which is the rule for processing the LoRaWAN data. For example, data comes with the handler rule should be saved to the MQTT broker or websocket.

The broker and websocket on the WISE-6610 Series is enabled by default. The uplink from the sensor node comes with the MQTT topic is uplink/{devaddr} and the downlink topic is downlink/{devaddr}.
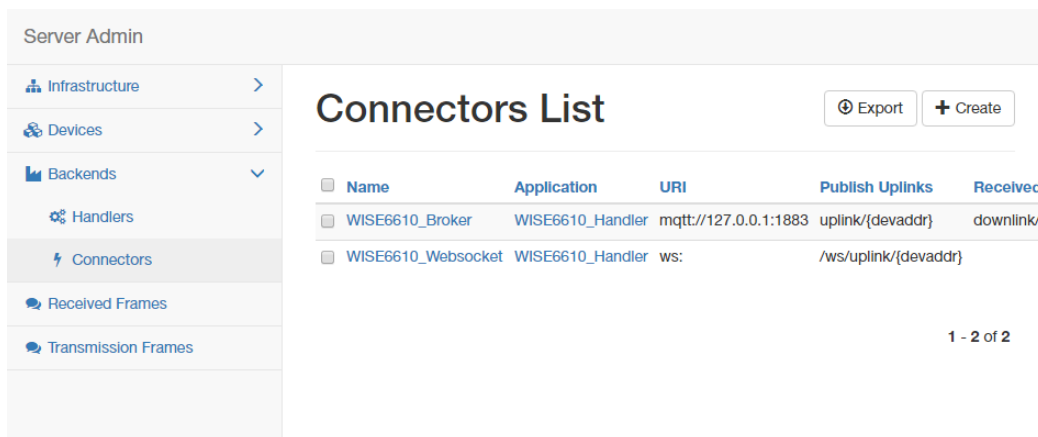
Figure 4.14 LoRaWAN Server > Backends > Connectors

18. Click **Create** to create your own connector rule.

Figure 4.15 LoRaWAN Server > Backends > Connectors > Create

Item	Description
Connector Name	Enter the name of the connector.
Application	Click the drop-down menu to select the application to reference a specific backend handler.
Format	Click the drop-down menu to select the format. ■ JSON: Encode data fields as Json structures such as `{"NameOne":ValueOne, "NameTwo":ValueTwo}`. ■ Raw Data: Send only the binary content of the data field without ant port numbers nor flags. ■ Web Form: Encode fields in query strings such as `NameOne=ValueOne&NameTwo=ValueTwo`.
URI	Enter a string to define the target host which can be `mqtt://` for MQTT or `mqtts://` for MQTT/SSL.
Publish Uplinks	Enter a string to define a server pattern for constructing the publication topic for uplink messages, including the actual DevEUI, DevAddr or other data fields in the message topic. e.g. `out/{devaddr}`.
Publish Events	Enter a string to define a server pattern for constructing the publication topic for event messages.
Subscribe	Enter a string to define a topic for subscription. It may include broker specific wilcards, e.g. `in/#`. The MQTT broker will then send messages with a matching topic to this connector.
Received Topic	Enter a string to define the template for parsing the topic of received messages, e.g. `in/{devaddr}`. This can be used to obtain a DevEUI, DevAddr or a device group that receives a given downlink.
Enabled	Check to allow a temporarily disable on an existing connector.

Item	Description
Failed	Click the drop-down menu to select the flag indicates the failure items.
	■ badarg: Some connector parameters are bad.
	■ network: The destination server cannot be reached.
	■ topic: The target broker configuration is wrong.
Submit	Click **Submit** to save the values and update the screen.

19. Click **Devices** > **Profiles** to enter the Profiles List page.

Define the profile rule for the LoRa node and assign the handler rule to each profile. The default profiles are listed in the figure below:
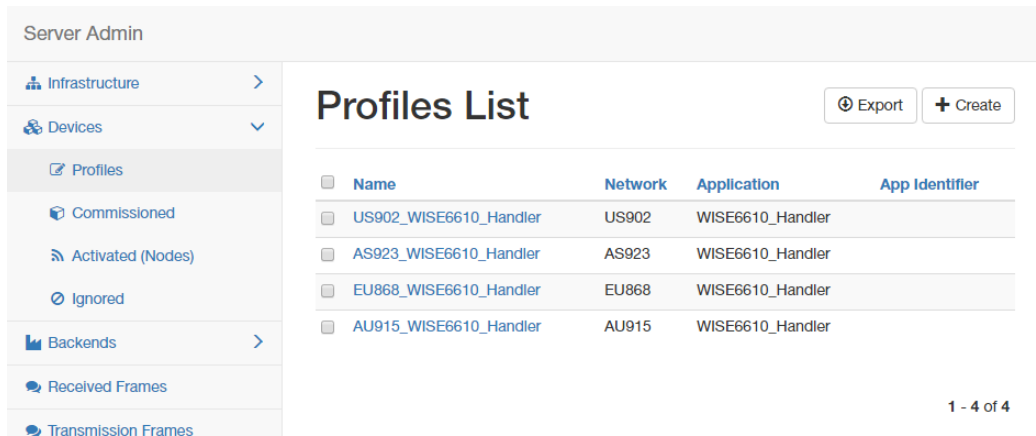
Figure 4.16 LoRaWAN Server > Devices > Profiles

20. Click **Create** to add a new profile.
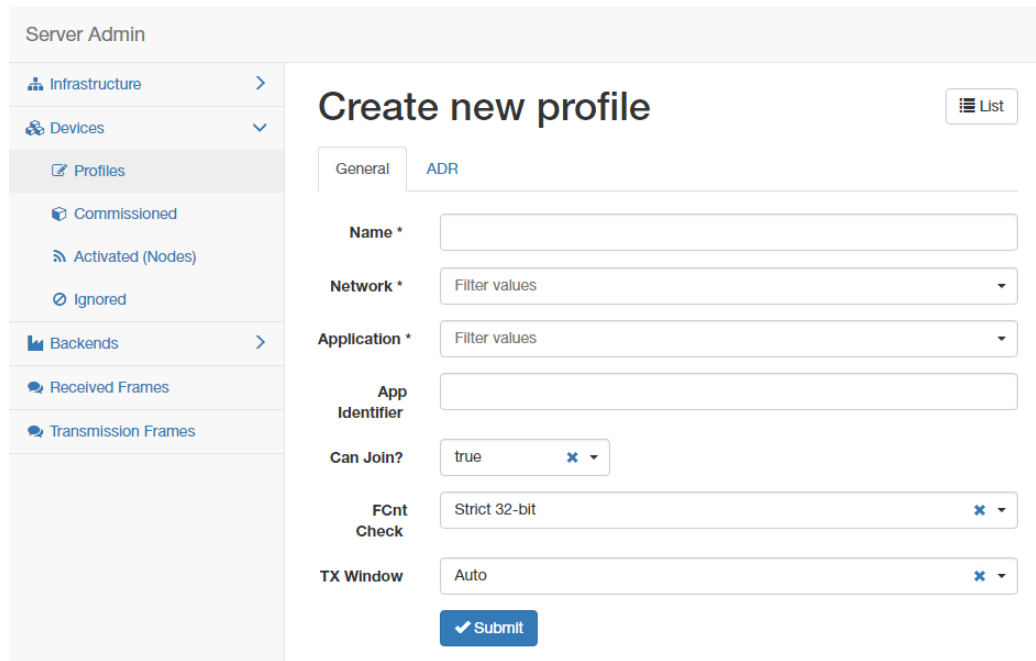
Figure 4.17 LoRaWAN Server > Devices > Profiles > Create > General

Item	Description
Name	Enter the name of the profile.
Network	Click the drop-down menu to select the network.
Application	Click the drop-down menu to select the application in use.
App Identifier	Enter the name of the application ID.

Item	Description
Can Join?	Click the drop-down menu to select a flag to prevent the device from joining.
FCnt Check	Click the drop-down menu to select the FCnt check for the device. ■ Strict 16-bit (default) or Strict 32-bit: Indicates a standard compliant counter. ■ Reset on zero: Behaves as a "less strict 16-bit" which allows personalised (ABP) devices to reset the counter. This weakens the device security a bit as more reply attacks are possible. ■ Disabled: Disables the check for faulty devices and destroys the device security.
TX Window	Click the drop-down menu to select the TX window for downlinks to the device. ■ Auto: Choose the earliest feasible option: RX1 or RX2. ■ RX1: Always use the first RX window. ■ RX2: Always use the second RX window.
Submit	Click **Submit** to save the values and update the screen.

21. Click the **ADR** tab to configure further settings for the node.

Figure 4.18 LoRaWAN Server > Devices > Profiles > Create > ADR

Item	Description
ADR Mode	Click the drop-down menu to determine the adaptive data rate (ADR) mechanism for the device: Disabled, Auto-Adjust or Maintain.
Set Power	Enter a value to define the power (in dBm).
Set Data Rate	Enter a value to define the data rate.
Max Data Rate	Enter a value to define the maximal data rate supported by the devices.
Set Channels	Enter a value to define the set of channels. The channels are given as a comma-separated list of interfaces, e.g. `0-2` for EU, `0-71` for the whole US band, or `0-7,64` for the first US sub-band.

Item	Description
Set RX1 DR Offset	Enter a value to define the offset between the uplink and the RX1 slot downlink data rates.
Set RX2 DR	Enter a value to define the data rate for the second reception slot (RX2).
Set RX2 Freq (MHz)	Enter a value to define the default frequency in the RX2 receive window.
Request Status?	Click the drop-down menu to select the flag used to disable the status requests for simple devices that do not support the function (default: true).
Submit	Click **Submit** to save the values and update the screen.

22. Click **Devices** > **Activated (Nodes)** to enter the Nodes List page.

    Activated (Nodes) is the setting for ABP type nodes and **Commissioned** is for OTAA type nodes. The LRPv2 nodes only supports ABP so the info can only be created in the ABP options.
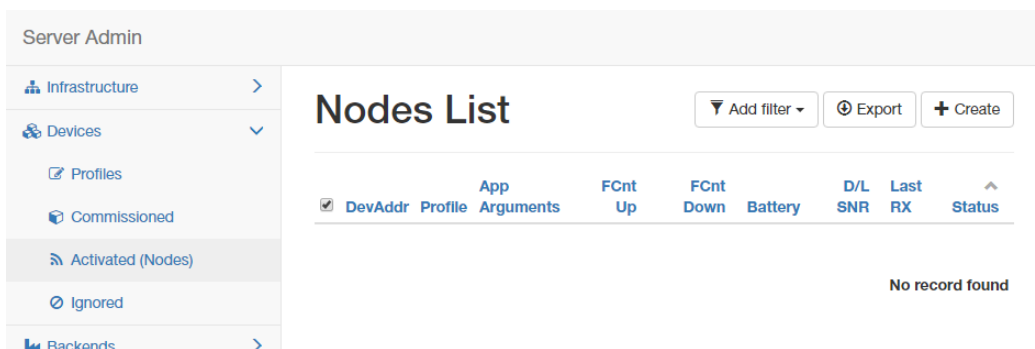
Figure 4.19 LoRaWAN Server > Devices > Activated (Nodes)

23. Click **Create** to add a new LoRaWAN node (ABP) along with its Devaddr, APPkey and NwkKey.
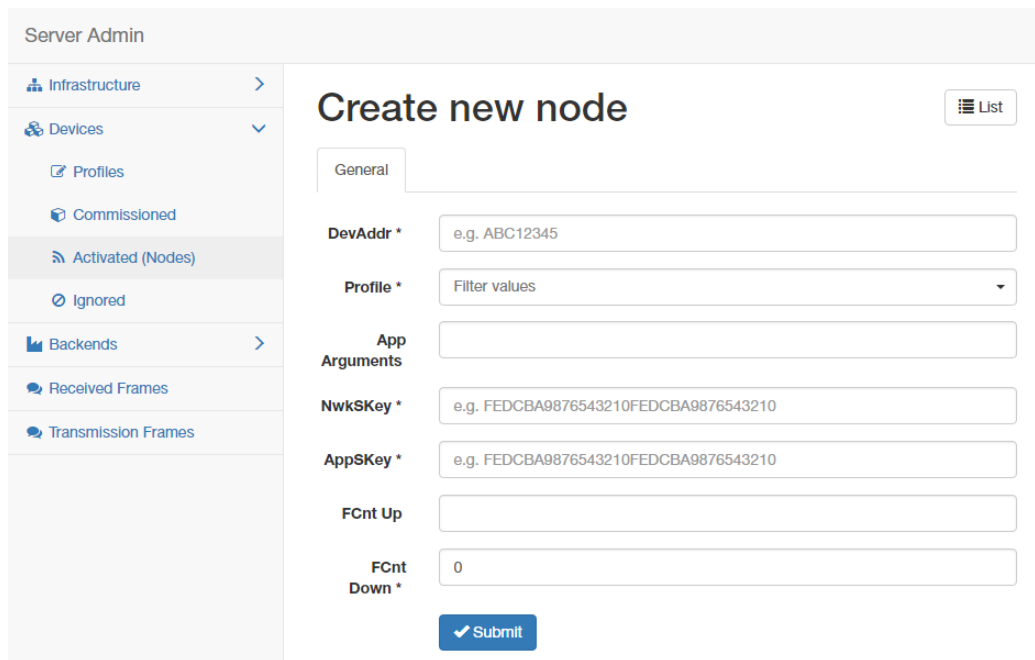
Figure 4.20 LoRaWAN Server > Devices > Activated (Nodes) > Create

Item	Description
DevAddr	Enter the name of the node.
Profile	Click the drop-down menu to select the profile for the node.

Item	Description
App Arguments	Enter the opaque string with application-specific settings.
NwkSKey	Enter the NwkSKey for the node.
AppSKey	Enter the AppSKey for the node.
FCnt Up	Enter a value to define the frame counter.
FCnt Down	Enter a value to define the frame counter.
Submit	Click **Submit** to save the values and update the screen.

24. Click **Devices** > **Commissioned** to enter the Devices List page.
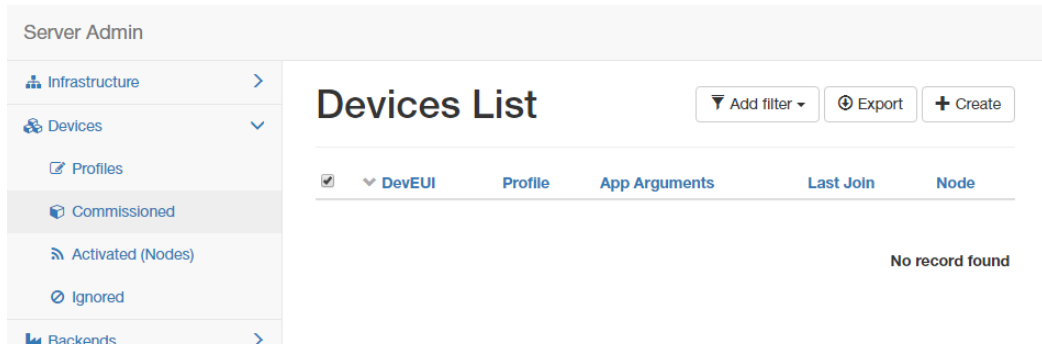
Figure 4.21 LoRaWAN Server > Devices > Commissioned

25. Click **Create** to add a new LoRaWAN node (OTAA).
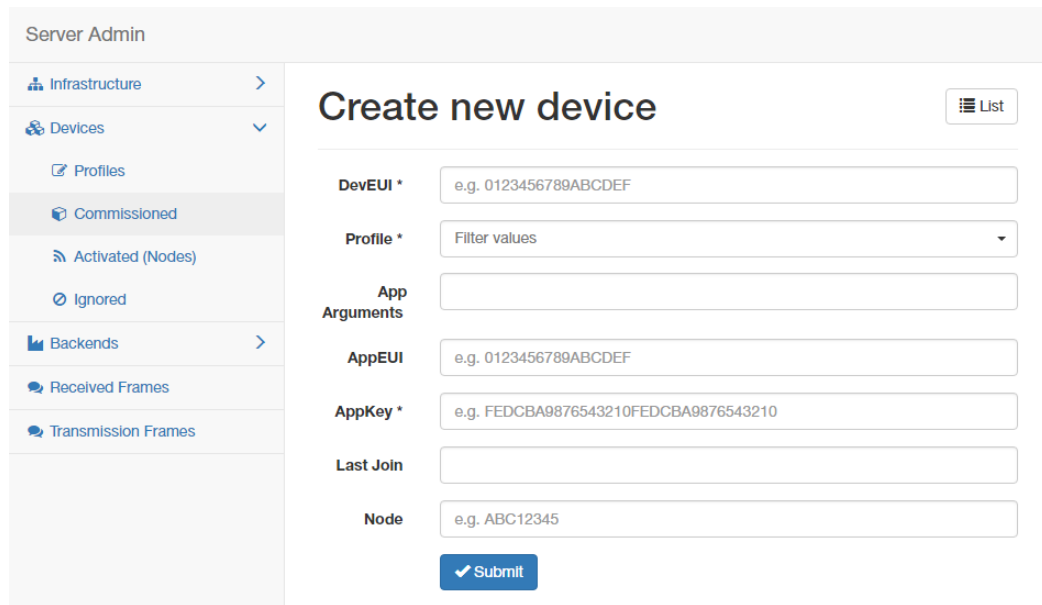
Figure 4.22 LoRaWAN Server > Devices > Commissioned > Create

Item	Description
DevEUI	Enter the DevEUI for the device.
Profile	Click the drop-down menu to select the profile for the device.
App Arguments	Enter the opaque string with application-specific settings.
AppEUI	Enter the AppEUI for the device.
AppKey	Enter the AppKey for the device.
Last Join	Enter a value to define the timestamp of the last successful Join request.
Node	Enter the corresponding node.
Submit	Click **Submit** to save the values and update the screen.

26. After the LoRaWAN network, gateway, node, handler and connector funcitons are enabled. Click **Received Frames** to enter the Received Frames page and check the received messages.

Received	Application	DevAddr	MAC	U/L RSSI	U/L SNR	FCnt	Confirm	Port	Data
2018-03-02T14:02:41Z	WISE6610_Handler	00220009	000A1FFFEDEF0A1	-37	7	4	✔	15	0109010E5002E8
2018-03-02T13:55:00Z	WISE6610_Handler	00220009	000A1FFFEDEF0A1	-47	14	2	✔	15	0109010E5002E8
2018-03-02T13:54:34Z	WISE6610_Handler	00220009	000A1FFFEDEF0A1	-41	10	1	✔	15	0109010E5002E8
2018-02-27T14:36:55Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-77	7	9	✖	2	030A4414610009
2018-02-27T14:34:25Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-77	9.8	8	✖	2	030A47140C000A
2018-02-27T14:31:55Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-72	7.8	7	✖	2	030A481414000B
2018-02-27T14:29:25Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-81	9.2	6	✖	2	030A4E142A000A
2018-02-27T14:26:55Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-74	6.5	5	✖	2	030A551400000C
2018-02-27T14:24:25Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-79	9.2	4	✖	2	030A581406000A
2018-02-27T14:21:55Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-77	9	3	✖	2	030A531429000C
2018-02-27T14:19:26Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-78	9.8	2	✖	2	030A4F13E9000B
2018-02-27T14:16:56Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-76	9.5	1	✖	2	030A35148E000F
2018-02-27T14:15:22Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-76	10.2	1	✖	2	030A1214BE000B
2018-02-27T14:12:48Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-63	8.5	4	✖	2	0309C415510008
2018-02-27T14:09:49Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-60	10.5	3	✖	2	0309B615AB000A
2018-02-27T14:06:49Z	WISE6610_Handler	0A6A3668	000A1FFFEDEF0A1	-63	8.5	2	✖	2	03099C160A0008
2018-02-27T10:43:03Z	WISE6610_Handler	067D3663	000A1FFFEDEF0A1	-74	6.5	7	✖	2	01093016820477
2018-02-27T10:37:10Z	WISE6610_Handler	067D3663	000A1FFFEDEF0A1	-109	8	5	✖	2	010937169B04F0
2018-02-27T10:34:14Z	WISE6610_Handler	067D3663	000A1FFFEDEF0A1	-115	5.8	4	✖	2	01092916BE0533

Figure 4.23 LoRaWAN Server > Received Frames

27. Since the MQTT broker on the WISE-6610 series is enabled by default, you can subscribe the MQTT "#" on 192.168.1.1 to receive the LoRaWAN node messages.

david@david-VirtualBox:~/WORK_PATH/LORA/LoRaWAN_USER_MODULE/LoRa_gateway_1_0_0/usermodule-adv-lora$ mosquitto_sub -t '#' -h 192.168.1.1 -v
out/FE050872 {"data":"030A5D15130004","datetime":"2017-11-28T11:33:12Z","devaddr":"FE050872","fcnt":10,"gateway":{"mac":"000A14FFFEDEF0B1"},"group":"Local","port":15,"rxq":{"codr":"4/5","datr":"SF10BW125","freq":923.8,"lsnr":12.2,"rssi":-35,"time":"2017-11-28T11:33:12.160972Z","tmst":2190760940},"shall_reply":true}
out/FE050872 {"data":"030A6615310003","datetime":"2017-11-28T11:34:10Z","devaddr":"FE050872","fcnt":11,"gateway":{"mac":"000A14FFFEDEF0B1"},"group":"Local","port":15,"rxq":{"codr":"4/5","datr":"SF10BW125","freq":924.0,"lsnr":9.2,"rssi":-30,"time":"2017-11-28T11:34:10.343071Z","tmst":2248948636},"shall_reply":true}
out/FE050872 {"data":"030A6615100003","datetime":"2017-11-28T11:35:08Z","devaddr":"FE050872","fcnt":12,"gateway":{"mac":"000A14FFFEDEF0B1"},"group":"Local","port":15,"rxq":{"codr":"4/5","datr":"SF10BW125","freq":923.2,"lsnr":12.2,"rssi":-37,"time":"2017-11-28T11:35:08.540106Z","tmst":2307136124},"shall_reply":true}
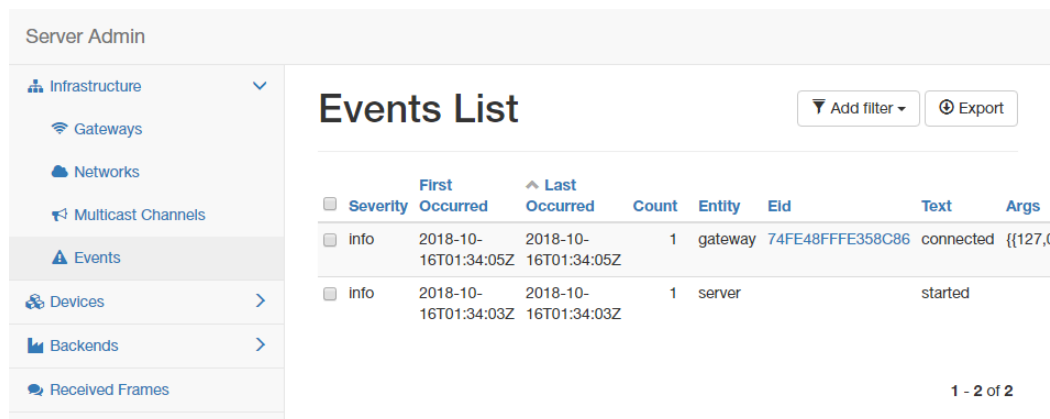
Figure 4.24 MQTT Subscription
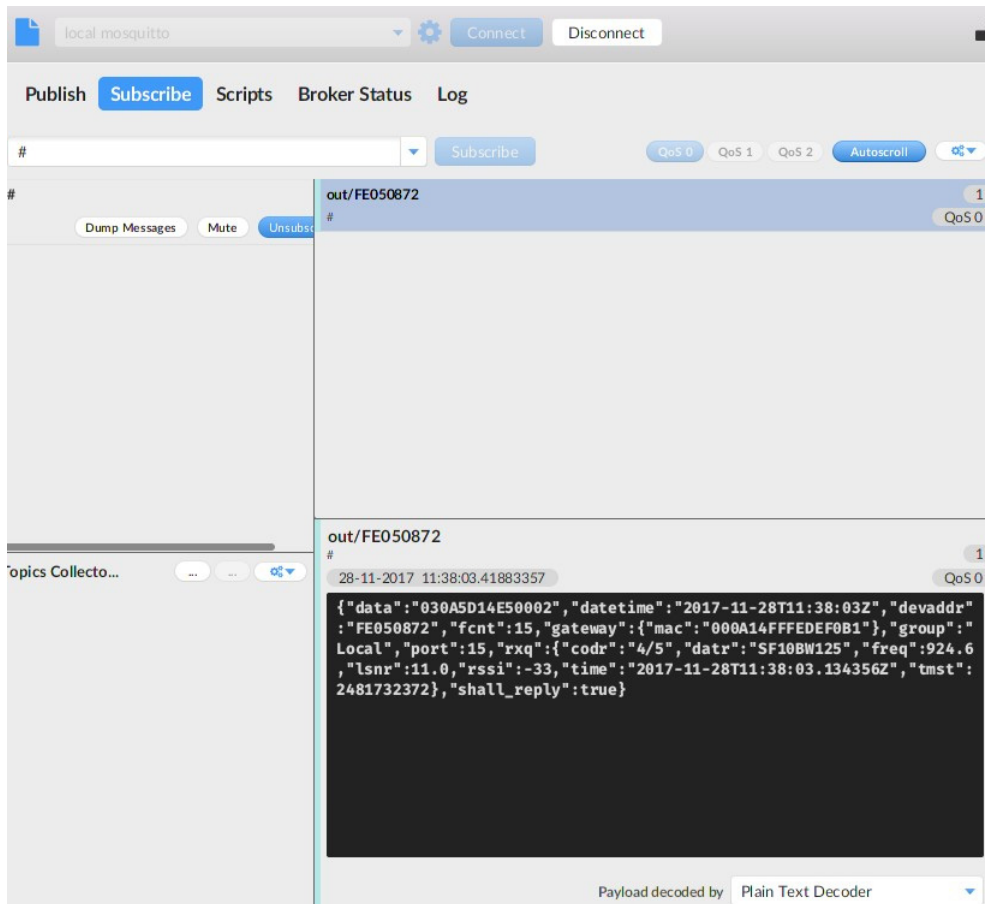
Figure 4.25 MQTT Subscription

28. Click **Infrastructure** > **Events** to enter the Events List page to view the events.

Figure 4.26 LoRaWAN Server > Infrastructure > Events

Item	Description
rxwin_setup_failed	Network server get RXParamSetup failed.
uplinks_lost	Gateway lost uplink frame.
ack_lost	Gateway lost ack frame.
downlinks_lost	Gateway lost downlink frame.
uplinks_missed	Network server lost uplink frame.
uplinks_duplicate	Network server get duplicate frame and more than the 200ms
downlink_missed	Network server lost downlink frame.
repeated_reset	node reset and network server get join request

4.2 Changing the Raw LoRa Data Format

This function parses and shows the raw data from an Advantech LRPv2 LoRa node.

Note!	**WISE-6610 series** *models does not parse data from a non-Advantech LoRa node through the Advantech Application function.*

Note!	*All the foregoing settings must be configured before using this function.*

1. To access this page, click **User Modules > LoRaWAN Gateway** > **Advantech Application**.

Figure 4.27 User Modules > LoRaWAN Gateway > Advantech Application

2. Click **Detail** to list the real data and status detail of the node.

Figure 4.28 Data and Status

3. To get the sensor node data, the application server needs to be enabled first. After the application server is enabled, the Advantech application server will parse the data subscribed from the MQTT broker (WISE-6610 and WISE-6610 LTE with topic uplink/#) as shown in the figure below.

Figure 4.29 User Modules > LoRaWAN Gateway > MQTT and LoRaWAN

4. Click **LoRaWAN Server** > **Devices** > **Activated (Nodes)** to enter the Nodes List page.

Figure 4.30 LoRaWAN Server > Activated (Nodes)

5. Edit the LoRa Node and enter **Advantech** in the **App Arguments** field. The Advantech application server will deal with the raw data based on the info and list the real data on the **Advantech Application** page.

Figure 4.31 LoRaWAN Server > Activated (Nodes) > Edit > General

6. Not only the data will be shown on the Advantech Application page, if you would like to apply the data to other software applications, you can also subscribe Topic "#" or direct Topic "Advantech/+/data" from the WISE-6610 MQTT server.

Edit mqtt in node

Cancel   Done

🌐 Server   127.0.0.1:1883   ▼   ✎

☰ Topic   Advantech/+/data

⚙ QoS   2   ▼

🏷 Name   Name

Figure 4.32 Applying Data to Other Software Applications

4.3 Node-RED Setup

1. Go to **Customization** > **User Modules**.
2. A list of available devices display. Click on the target **Node-RED**.

User Modules

LoRaWAN Gateway 1.1.7 (20200616T094757Z) Delete
Node-RED   1.0.1 alfa (2017-03-13)   Delete

New Module Choose File No file chosen   Add or Update

Figure 4.33 Customization > User Modules

3. The Settings menu displays. Click **Node-RED** and check the box to enable the Node-RED and enter the port number (default: 1880).

Configuration module

☑ Enable Automatic Start
Port 1880   the port used to serve the editor UI. Default: 1880.

Apply Node-RED will start immediately.

Figure 4.34 Node-RED

4. Go to Node-RED page (http://192.168.1.1:1880/) and log in using the default user name and password (root/root) for further configuration.

Username:

Password:

Node-RED   Login

Figure 4.35 Node-RED

ADVANTECH

Enabling an Intelligent Planet