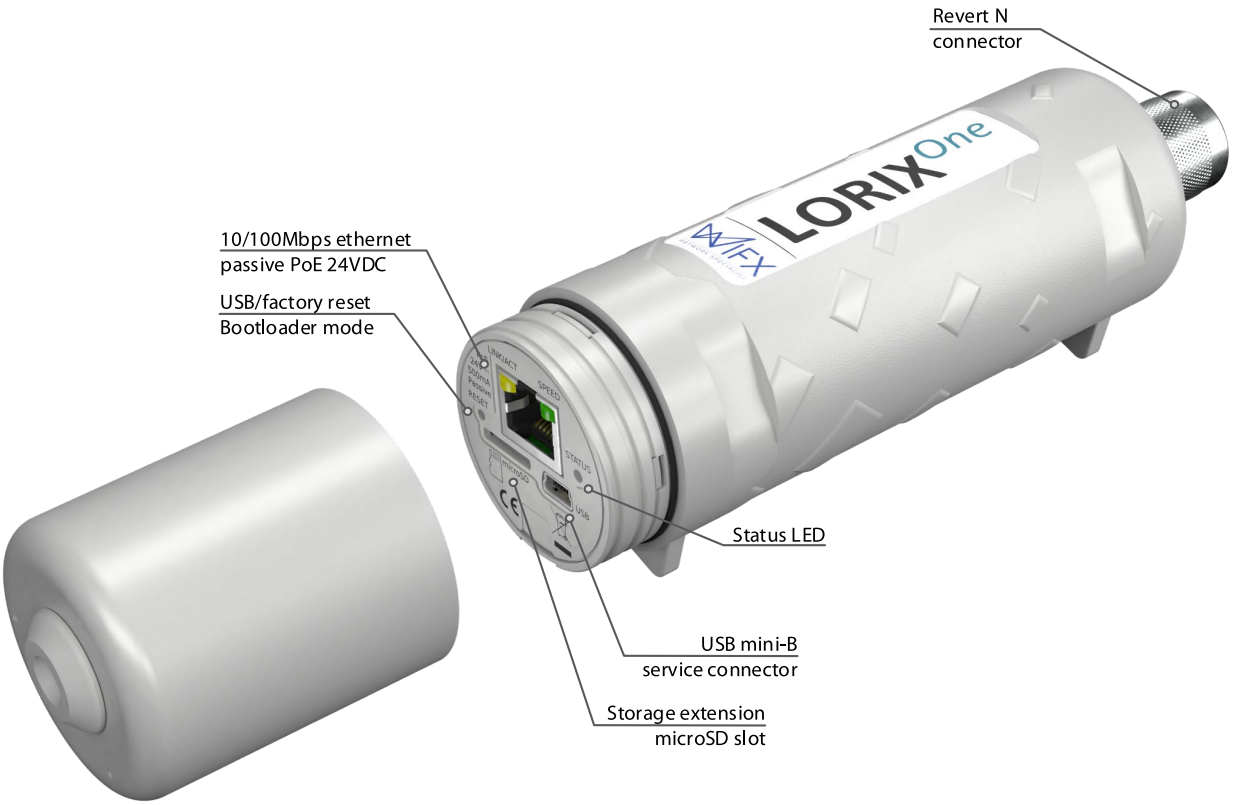
LORIX One

WIFX IP65 GATEWAY WITH EMBEDDED LORAWAN® CONCENTRATOR CHIP

User manual



Versions:

Revision	Note	Date
1.0	Added TTN cloud application Added system update	03/05/2017
1.1	Updated operating temperature and power supply following safety certification requirements	30/07/2017
1.2	Added Kersing packet-forwarder and updated others packet-forwarders and clouds-manager with manual forwarder option	21/04/2018
1.3	Added US version	08/05/2018
1.4	Updated FCC and IC legal texts and added installation description	06/07/2018
1.5	Updated NAND memory based on HW version	03/09/2018
1.6	Updated graphics with latest Wifx logo and added RF specifications table	14/02/2019
1.7	Updated Table 4 (ERC 70-3 Band)	28/11/2019
1.8	Added specification to comply with Peruvian regulation and update general documentation based on LORIX OS.	05/12/2021
1.9	Fix typo	21/06/2022

1 SUMMARY

2 PRODUCT SPECIFICATIONS

Version	IP64 (Waterproof)
Physical specifications	
Dimensions	See 9.1 LORIX One
Weight	< 230 grams
Connectors	
	1 RJ45 Ethernet 10/100 Mbps port Max 100 m length, use shielded cable for outdoor use
	1 USB mini-B service connector (service access only)
	1 N type RF antenna connector
	1 microSD SD Memory Card Specification v2.0 slot
Power specifications	
Input supply	24 VDC 500 mA (through passive PoE)
Power supply	See 5.1 Power through passive PoE
Consumption	See 8.1 Power consumption
Climatic specifications	
Operating temperature	-30 °C to +55 °C -5 °C to +40 °C for the power supply (S-)HNP12-240L6, indoor use only
Storage temperature	-20 °C to +70 °C
Operating humidity	10% to 90% RH Non-condensing
Storage humidity	5% to 90% RH Non-condensing
System	
CPU	ARM Cortex-A5 @ 600 MHz
RAM	128 MB DDR2 @ 200 MHz
Internal memory	Up to **1.0d** HW version: 256 MB NAND FLASH with 4bits hardware ECC (Micron MT29F2G08ABAEAH4) From **1.0d2** HW version: 512 MB NAND FLASH with 8bits hardware ECC (Micron MT29F4G08ABAEAH4)
External memory	microSD card slot, SDHC compatible, can be used as boot source

TABLE 1: PRODUCTS SPECIFICATIONS

Version	8XX	9XX	
RF specification			
LoRaWAN region	EU868	US915	AU915
LoRa modulation (Chirp spread spectrum modulation)	863-873 MHz Following Table 3: Certification compliance Version 8XX for Europe	902-928 MHz	915-928 MHz
FSK Modulation	863-873 MHz Following Table 3: Certification compliance Version 8XX for Europe	Not applicable	Not applicable
Power of transmission	Following Table 4: Duty cycles and maximum EIRP Version 8XX for Europe	Max radiated power of 30 dBm. Conducted power must be adapted to antenna gain.	Following Table 7: RF Specifications Version 9XX for Australia/New Zealand
TX frequency tolerance	±4 ppm including ageing, temperature compensated		
RX min sensitivity (10% PER)	-136.5 dB (SF12BW125)	-136.5 dB (SF12BW125)	
Antenna impedance	50 Ohm		

TABLE 2: PRODUCTS RF SPECIFICATIONS

3 REGULATIONS

3.1 VERSION 8XX (863-870 MHZ BAND)

3.1.1 EUROPE / CE

The LORIX One 8XX version complies with requirements listed in article 3 of the RED 2014/53/EU directive:

Certification compliance	
Radio & EMC	RED 2014/53/EU (European Radio Equipment Directive)
	ETSI EN 300 220-2
	EN 61000-6-1:2007 IEC 61000-6-1:2005 (ed2.0)
	ETSI EN 301 489-3 V1.6.1:2013
Human safety	EN 62209-2 IEC/EN 62479-1
Electrical safety	IEC/EN 62368-1

TABLE 3: CERTIFICATION COMPLIANCE VERSION 8XX FOR EUROPE

For use in Europe, the LORIX One must comply with the ERC 70-3 requirements regarding duty cycle and maximum EIRP. These parameters are summarized in the following table:

Duty cycle and maximum EIRP			
ERC 70-3 Band	**Frequency (MHz)**	**Power**	**Duty cycle**
h1.3	863 – 865	14dBm ERP	0.1%
h1.4	865 – 868	14dBm ERP	1%
h1.5	868 – 868.6	14dBm ERP	1%
h1.6	868.7 – 869.2	14dBm ERP	0.1%
h1.7	869.4 – 869.65	27dBm ERP	10%
h1.8	869.7 – 870	7dBm ERP	No requirement
h1.9	869.7 – 870	14dBm ERP	1%

TABLE 4: DUTY CYCLES AND MAXIMUM EIRP VERSION 8XX FOR EUROPE

If the antenna is changed, the output power must be adjusted to consider the gain of the antenna and avoid exceeding the values defined by the ERC 70-3 regulation.

Warning: some countries in Europe may have a specific frequency range, a maximum EIRP and duty cycle regulation. Please check the local regulations before installing and using the LORIX One 8XX version.

For countries outside Europe, please check that the frequency range, the maximum allowed EIRP and duty cycle are authorized.

3.2 VERSION 9XX (902-928 MHZ BAND)

The LORIX One (IP43 & IP65) 9XX version complies with both FCC and IC regulation:

Certification compliance	
CFR 47 FCC Part 15	FCC 47 CFR Part 15: 2014 - Part 15- Radio frequency devices
RSS 247	RSS-Gen – Issue 5, Avril 2018 – General requirements and Information for the Certification of radio Apparatus
	RSS-247 Issue 2, February 2017 – Digital Transmission Systems (DTSS), Frequency Hopping Systems (FHSS) and License-Exempt Local Area Network (LE-LAN) Devices

TABLE 5: CERTIFICATION COMPLIANCE VERSION 9XX FOR USA/CANADA

The associated FCC and IC identifiers of the LORIX One 9XX version are:

FCC ID: 2APAZ-LORIXONE
IC: 23715-LORIXONE
Model: LORIX One

Some conditions must be met to maintain the FCC and IC compliance of the devices in the USA and Canada. These conditions are detailed in the following paragraphs. For other countries, please check the specific regulations regarding maximum allowed EIRP and duty cycle.

3.2.1 USA / FCC

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.

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

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 personal expense.

This device must be professionally installed.

Also, some specific recommendations for exposure to magnetic fields must be followed: This equipment complies with FCC's radiation exposure limits set forth for an uncontrolled environment under the following conditions:

1. This equipment should be installed and operated such that a minimum separation distance of 20 cm is maintained between the radiator (antenna) and user's/nearby person's body at all times.
2. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

3.2.2 CANADA / IC

This device complies with Industry Canada's license-exempt RSS standards. 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 of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. L'appareil ne doit pas produire de brouillage ;
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, that antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that necessary for successful communication.

This radio transmitter has been approved by Industry Canada to operate with the antenna types listed as accessories with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with the device.

This equipment should be installed and operated such that a minimum separation distance of 20 cm is maintained between the radiator (antenna) and user's/nearby person's body at all times.

3.2.3 AUSTRALIA/NEW ZEALAND

This device complies with the section 134 (1) (g) of the New Zealand Radiocommunication Act 1989 and belongs on the following applicable standards:

Certification compliance	
Safety	IEC/EN 62368-1
EMC	EN 61000-6-1:2007 IEC 61000-6-1:2005 (ed2.0)
	ETSI EN 301 489-3 V1.6.1:2013
Radio Spectrum	FCC 47 CFR Part 15: 2014 - Part 15- Radio frequency devices
	RSS-247 Issue 2, February 2017 – Digital Transmission Systems (DTSS), Frequency Hopping Systems (FHSS) and License-Exempt Local Area Network (LE-LAN) Devices
	RSS-Gen Issue 4, November 2014 – General Requirements for Compliance of Radio Apparatus

TABLE 6: CERTIFICATION COMPLIANCE VERSION 9XX FOR AUSTRALIA/NEW ZEALAND

This device must be professionally installed and used only in industrial context. In addition, the network server must respect RF specifications defined in the following table.

RF Specifications	
Frequency range	915-928 MHz
Max EIRP	30 dBm
Max conducted power (2 dBi antenna)	28 dBm
Max conducted power (3 dBi antenna)	27 dBm
Max conducted power (4 dBi antenna)	26 dBm
Max conducted power (5 dBi antenna)	25 dBm

TABLE 7: RF SPECIFICATIONS VERSION 9XX FOR AUSTRALIA/NEW ZEALAND

4 General information

4.1 Online documentation

The online documentation is available at iot.wifx.net/docs and contains information about technical use of the product including its operating system, the LORIX OS.

Complete documentation

The documentation in this user manual is minimal and more information, especially regarding LORIX OS, is available online. Please consult it if you can't find the information in this document.

4.1.1 Update information

The modifications made between each new release of LORIX OS are described under the online documentation changelog page available at https://iot.wifx.net/docs/lorix-os/latest/release-notes.

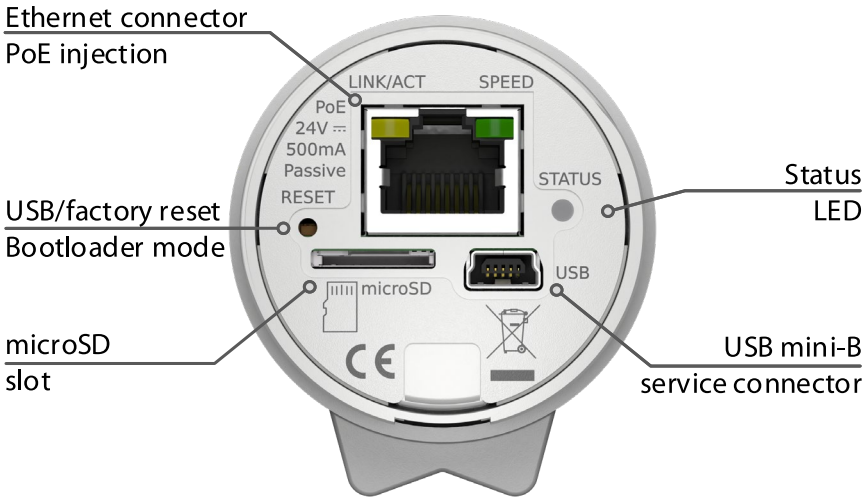
4.1.2 Troubleshooting

Frequent encountered problems are summarized under the online documentation troubleshooting page, with suggested solutions available at https://iot.wifx.net/docs/lorix-os/latest/troubleshooting.

4.1.3 Open source licenses

All the licenses of the open source softwares used or available in the package repository of the LORIX OS are available at https://download.wifx.net/lorix-os/<LORIX OS release version>/licenses/, for example for the version 1.3.4, the licenses are available at https://download.wifx.net/lorix-os/1.3.4/licenses/.

4.2 Connectivity/Interface



4.3 Start/Reset

The gateway automatically boots when connected to a power supply through passive PoE on the Ethernet cable. After start-up, the status LED should blink briefly and turn off. Once the Linux OS starts, the status LED will start blinking in "heartbeat" mode.

The reset button can be used to:

- reset normally the gateway and start in normal operating mode
- restore the gateway close to its original factory settings
- enter in programming mode.

To press the button, use a thin tool such as a paper clip. Upon release, the status LED will briefly flash and then stop to signal the reset action.

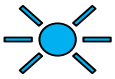
4.3.1 PROCEDURES

Short-press

Press briefly, for less than 1 second. The blue LED will briefly blink upon release

Long-press

Press and hold for several seconds. The blue LED will briefly blink after the delay specified below

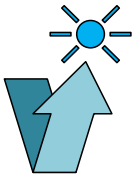


Status LED

A short flash of the blue LED

Normal reset procedure

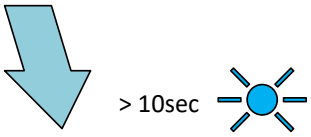
1. Short-press
2. The status LED will flash upon release and the gateway will reboot



Factory reset procedure

The factory reset procedure can be used to reset the initial default configuration and thus restore the device to its original settings. This procedure is useful to solve a network misconfiguration or to recover a forgotten password.

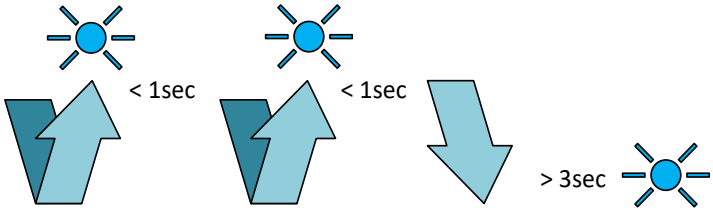
1. Wait at least 1 second after another reset pressure.
2. Long-press for at least 10 seconds
3. After the LED starts blinking, release the reset button.
4. The gateway will boot in factory reset mode. When Linux has started, a script will copy the default files.



Programming mode procedure

This procedure is used to enter in programming mode. It enables the possibility to reprogram the gateway using the Wifx Programming Tool (previously called LORIX Programming Tool) through the USB port as summarized on the online documentation page https://iot.wifx.net/docs/go/wifx-programming-tool/help.

1. Remove the microSD card from the device
2. Wait at least 1 second for another reset pressure
3. Perform 2 short presses with less than 1 second between each press
4. Perform a third long press for more than 3 seconds (but less than 5 seconds)



5 ETHERNET/POE

Connector details:

RJ45 Pin number	Wire color	Function	
1	Green	TX+	
2	Green/white	TX-	
3	Orange	RX+	
4	Blue	VPOE1	Voltage 1 for PoE powering (must be connected with pin 5)
5	Blue/white	VPOE1	Voltage 1 for PoE powering (must be connected with pin 4)
6	Orange/white	RX-	
7	Brown	VPOE2	Voltage 2 for PoE powering (must be connected with pin 8)
8	Brown/white	VPOE2	Voltage 2 for PoE powering (must be connected with pin 7)

TABLE 8 ETHERNET/POE CONNECTION

The yellow LED shows the LINK and the ACTIVITY on the Ethernet connection:

OFF No link
ON Link
Blink Link and activity

The green LED shows the actual SPEED of the Ethernet connection:

OFF 10Base-T
ON 100Base-TX

5.1 POWER THROUGH PASSIVE POE

The LORIX One gateway is exclusively powered through passive PoE using the Ethernet connector. The power is injected through a PoE injector as shown below:

V_{POE1} and V_{POE2} (in Table 8) represent both power lines of the gateway. Power must be injected in the power input connector using the switching power supply provided with the LORIX One only:

Reference HNP12-240L6
Output voltage 24VDC
Output courant 500mA

6 SERVICE ACCESS

The embedded Linux can be accessed and configured either through the service USB Type-C connector or through SSH or web interface with a working Ethernet connection.

> **Default user and password**
>
> The default user is **admin** and the password is **lorix4u**. This is useful and easy to remember during the initial configuration time but we strongly advise changing the password as soon as possible as explained in 7.2.1 Password.

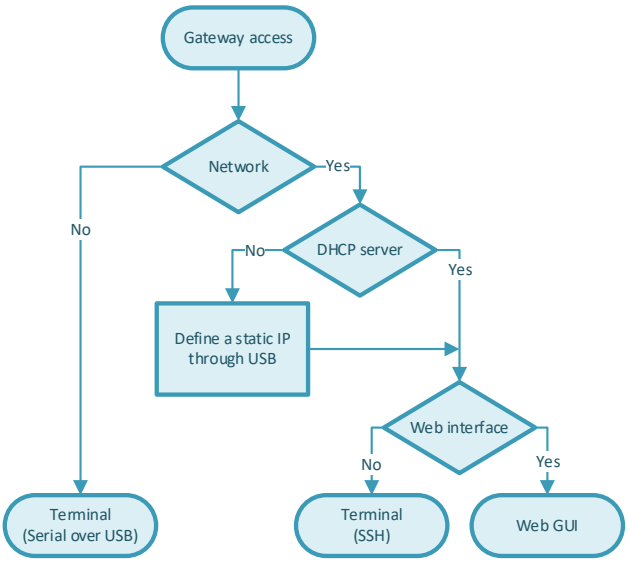
6.1 ACCESS METHODS

6.1.1 OVERVIEW

This diagram gives an overview of the methods you can use to access the gateway. If you have only USB or if network is not configured (or IP is not known), you have always terminal access through the USB service connector.

As soon as the network is configured and working, you can decide either to use terminal through network (SSH) or the more user-friendly web interface through your favourite web browser.

If your network doesn't have a DHCP server, you need to configure a static IP address using the USB access.



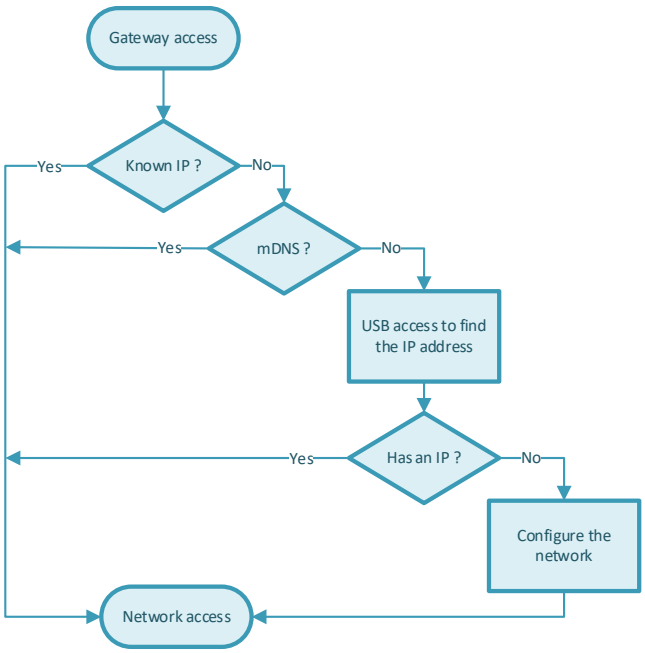
6.1.2 NETWORK ACCESS

To reach the gateway through the web interface or through SSH if you prefer using a terminal, you need a working network with a DHCP server (which will provide a dynamic IP address) or define a static IP address for your gateway.

If your gateway has an IP and you know it, you can simply reach it as explained at 6.3 Network.

If you don't know the IP but probably have a DHCP server, you can't try to reach it using mDNS as explained at 6.3.1 mDNS or find the IP from the router's admin interface.

Finally, you can find the IP or configure it as static through the USB interface.



6.2 USB

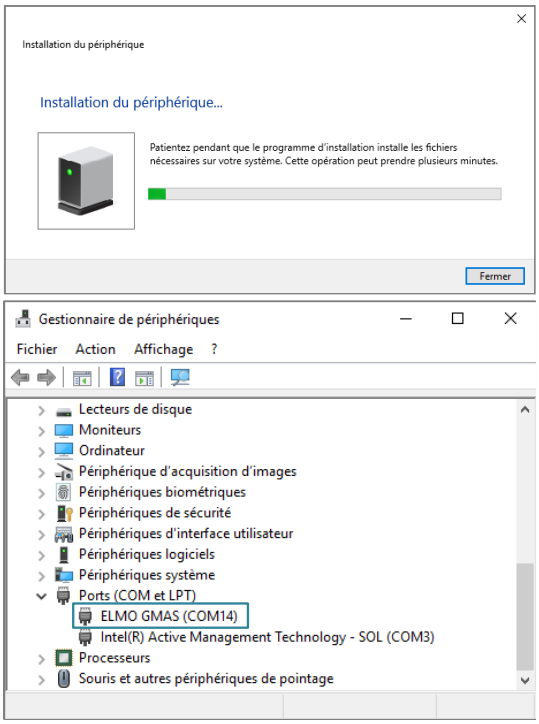
The gateway has a USB Type-C connector which provides a virtual COM port as soon as the service LED (white) turns on. Accessing the gateway this way allows you to debug and configure the system. This is also the only way to reach the service terminal when the network is not accessible or not yet configured.

USB Connection consideration

The USB connection should be used exclusively for service administration/configuration and should not be left connected during normal use. The IP65 level is also not guaranteed during USB service connector use.

To access the gateway through USB:

1. Power up the gateway with passive PoE through the Ethernet connector or through the USB directly
2. Connect a PC to the gateway with a A ⇔ C cable
3. The virtual COM port is automatically detected by the PC
    a. On Windows a new virtual COM port will appear in the device manager under the name **ELMO GMAS (COMxx)**



    b. On Linux a new virtual COM port will appear in the folder **/dev/ttyACMxx**
4. A terminal program like PuTTY or minicom can be used with the following parameters:

baudrate	**921600**
data bits	**8**
stop bits	**1**
parity	**none**
flow control	**none**

6.3 NETWORK

6.3.1 MDNS

The gateway will announce itself through the mDNS protocol (aka Zeroconf, Bonjour) with its default hostname on the '.local' domain. The default hostname is composed of the prefix `lorix-one-` and the last 6 characters of the MAC address as lowercase: `lorix-one-xxxxxx`.

This means that you can reach your gateway with the following address: `lorix-one-xxxxxx.local`.

> **Example**
>
> The gateway MAC address show on the sticker is FC:C2:3D:AA:BB:CC
> This hostname is therefore lorix-one-aabbcc
>
> You can reach the gateway at lorix-one-aabbcc.local

To contact the gateway through mDNS, your network must support this feature (with IGMP snooping disabled) and you must be on the same subnetwork than the gateway to contact.

6.3.2 SSH

The gateway provides an SSH server and be accessed through SSH as soon as configured and connected to a working network using an SSH client program like PuTTY or ssh on Linux.

To access the gateway with SSH:

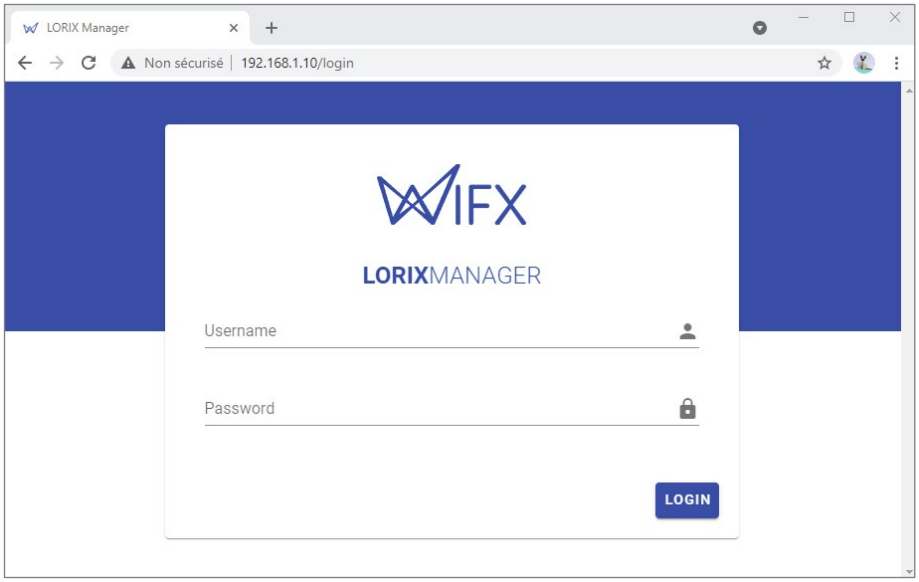
1. Power up the gateway
2. A terminal program like PuTTY or ssh can be used with the following parameters:
   address **IP address or mDNS hostname**
   port **22**
3. Accept the RSA key fingerprint if asked

6.3.3 WEB INTERFACE

The gateway provides a web graphical interface and can be accessed through your favorite web explorer.

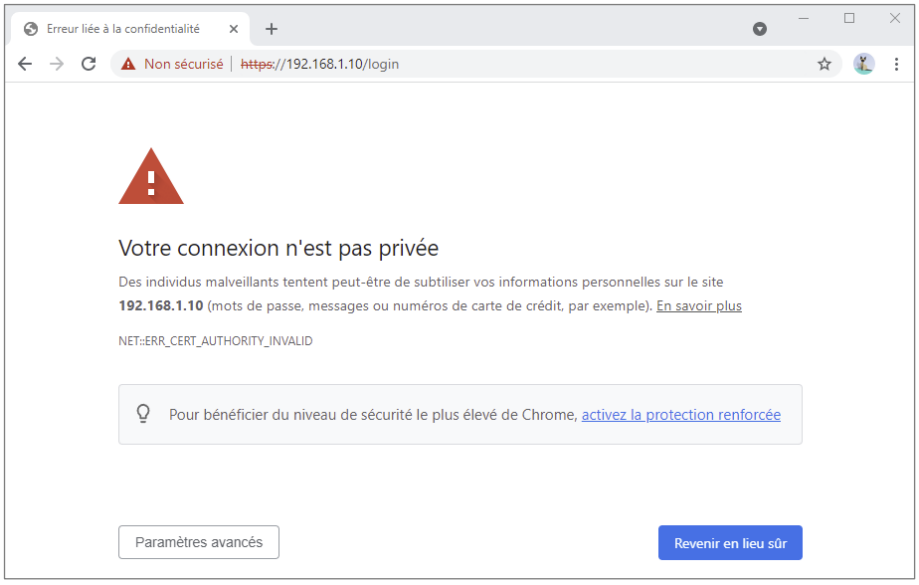
As explained previously, you can reach the gateway through its IP address or through mDNS. Also, you can choose between HTTP (not secure) and HTTPs (SSL secured) by prefixing the address with `http://` respectively `https://`.

> **Example**
>
> For the IP address 192.168.1.148, you can reach the gateway using http://192.168.1.148 or https://192.168.1.148. This is also correct with mDNS as you could reach the gateway with http://lorix-one-aabbcc.local or https://lorix-one-aabbcc.local.



6.3.3.1 SECURITY WARNING

If you access the gateway with SSL support (HTTPs), you will get a security warning. The form can differ from one web browser to another but the concept stays the same. You receive this error because the SSL certificate of the gateway is self-signed as we don't know the address at the certificate creation time.



You can always accept this security warning but it depends on your browser so please consult its documentation to know how to accept the risk and move forward.

Security consideration

This security warning is important to let you know that the certificate is not trust by a global certification issuer. If you know the IP address is correct as long as it is in your local network, it still secures your connection and avoid anyone to see data exchange (like user/password) between your computer and the gateway.

We suggest then to use HTTPs when possible.

7 BASIC SETUP

This chapter is made to help you to easily configure your gateway during the initial configuration process. It follows chronological configuration when possible so you should read it like a step by step configuration procedure and pass some steps when they are not required for your setup.

7.1 CONFIGURE THE NETWORK

The USB access is made for service only usage since the gateway is primarily made to be reached through an IP network. The first step is then to configure the network aspects through the USB service access.

7.1.1 CHECK THE CURRENT STATUS

7.1.1.1 IP ADDRESS

You can see the current IP address (v4 and v6) by using the command ifconfig:

```
$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr fc:c2:3d:aa:bb:cc
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::fec2:3dff:fe2d:56f1/64 Scope:Link
          inet6 addr: aaaa:bbbb:1:0:bbbb:3dff:fe2d:56f1/64 Scope:Global
          inet6 addr: aaaa:bbbb:1:0:dddd:ca08:6889:a36b/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10219756 errors:3 dropped:30251 overruns:0 frame:3
          TX packets:58541 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:493144710 (470.2 MiB)  TX bytes:14043284 (13.3 MiB)
          Interrupt:27
```

The field `inet addr` returns the IPv4 addresses, `inet6 addr` fields return the IPv6 addresses.

7.1.1.2 CONNECTIVITY

You can test the current connectivity to see if the gateway has access to local, global or no access at all:

```
$ nmcli networking connectivity check
full
```

The possible result values are:

- **none**
  the host is not connected to any network.
- **portal**
  the host is behind a captive portal and cannot reach the full Internet.
- **limited**
  the host is connected to a network, but it has no access to the Internet.
- **full**
  the host is connected to a network and has full access to the Internet.
- **unknown**
  the connectivity status cannot be found out.

7.1.1.3 CONNECTION INFORMATION

The main connection provided by the system is called **backhaul** in LORIX OS and represents the connection established on the eth0 device (main and only Ethernet connector of the product).

You can display its various parameters using the nmcli utils as follow:

```
$ nmcli connection show backhaul
connection.id:                          backhaul
connection.uuid:                        390e5c2b-7312-415e-80e6-7b94a5c24fc3
connection.stable-id:                   --
connection.type:                        802-3-ethernet
connection.interface-name:              eth0
connection.autoconnect:                 yes
connection.autoconnect-priority:        1
connection.autoconnect-retries:         0 (forever)
connection.multi-connect:               0 (default)
connection.auth-retries:                -1
connection.timestamp:                   1637144771
connection.read-only:                   no
connection.permissions:                 --
connection.zone:                        --
connection.master:                      --
connection.slave-type:                  --
connection.autoconnect-slaves:          -1 (default)
connection.secondaries:                 --
connection.gateway-ping-timeout:        0
connection.metered:                     unknown
connection.lldp:                        default
connection.mdns:                        -1 (default)
connection.llmnr:                       -1 (default)
connection.wait-device-timeout:         -1
802-3-ethernet.port:                    --
802-3-ethernet.speed:                   0
802-3-ethernet.duplex:                  --
802-3-ethernet.auto-negotiate:          no
802-3-ethernet.mac-address:             --
802-3-ethernet.cloned-mac-address:      --
802-3-ethernet.generate-mac-address-mask:--
802-3-ethernet.mac-address-blacklist:   --
802-3-ethernet.mtu:                     auto
802-3-ethernet.s390-subchannels:        --
802-3-ethernet.s390-nettype:            --
802-3-ethernet.s390-options:            --
802-3-ethernet.wake-on-lan:             default
802-3-ethernet.wake-on-lan-password:    --
lines 1-38
```

There is a lot more parameters which are not displayed here and that you can display using the up/down keyboard keys to move through the parameters list.

Lower case parameters are configuration, upper case ones are related to the resulting situation (connection) and give you information about the current status.

For example, the value IP4.ADDRESS[1] is interesting and returns in this case 192.168.1.10/24. Note the /24 at the end which represent the netmask.

7.1.2 DHCP

By default, the gateway has a DHCP client waiting for an IP address and other configuration from a DHCP server. This is the most standard and simple way to manage it. If you have found an IP address at the previous step, it means you have a DHCP server which is configured correctly.

You can then either use the IP address or the mDNS hostname if you are in the same sub-network.

Additional configuration

Additional DHCP configuration is often not required but if you need to modify parameters or add route for example, you can either use the web interface (Network → Ethernet → Settings) or consult nmcli's documentation[1] if you prefer the terminal access (USB or SSH).

7.1.3 STATIC

From connection display described at 7.1.1.3 Connection information, you can modify connection parameters like setting the method to manual and the IP address, netmask, etc.

7.1.3.1 DEFINE A STATIC IPV4 ADDRESS WITH CUSTOM DNS

The following commands will define a fixe IPv4 address, the gateway and DNS addresses and finally set the method to manual (use auto to come back to DHCP):

```
$ nmcli connection modify backhaul ipv4.address 192.168.1.11/24
$ nmcli connection modify backhaul ipv4.gateway 192.168.1.1
$ nmcli connection modify backhaul ipv4.dns 8.8.8.8
$ nmcli connection modify backhaul ipv4.method manual
```

Apply the new parameters with the following command:

```
$ nmcli connection up backhaul
```

The nmcli show connection command returns now the following:

```
$ nmcli connection show backhaul
[…]
ipv4.method:                            manual
ipv4.dns:                               8.8.8.8
[…]
ipv4.addresses:                         192.168.1.11/24
ipv4.gateway:                           192.168.1.1
[…]
IP4.ADDRESS[1]:                         192.168.1.11/24
IP4.GATEWAY:                            192.168.1.1
IP4.ROUTE[1]:                           dst = 192.168.1.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                           dst = 0.0.0.0/0, nh = 192.168.1.1, mt = 100
IP4.DNS[1]:                             8.8.8.8
[…]
```

From the web interface, you can observe the graphical equivalent:

[1] nmcli — command-line tool for controlling NetworkManager
https://developer.gnome.org/NetworkManager/stable/nmcli.html

7.1.4 NETWORK VERIFICATION AND TROUBLESHOOTING

You should have a working network configuration at this time and the following chapter will help you to verify it.

The first things to do is to test again the network connectivity as described in chapter 7.1.1.2 Connectivity, you should get the result “full”.

If it’s not the case, your configuration is not right or your network block outgoing connection. In all case, you must be able to reach your main gateway, this can be verified using the command ping (with our example gateway):

```
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=6.43 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=6.43 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=6.45 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 6.425/6.434/6.453/0.013 ms
```

Or traceroute:

```
traceroute 192.168.1.1
traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 38 byte packets
 1  192.168.1.1 (192.168.1.1)  6.357 ms  6.380 ms  6.324 ms
```

If you don’t have access to the gateway, verify your network parameters and be sure you have reloaded your connection.

If you have access to the gateway, contact your IT support to verify for example outgoing connection are authorized for your device.

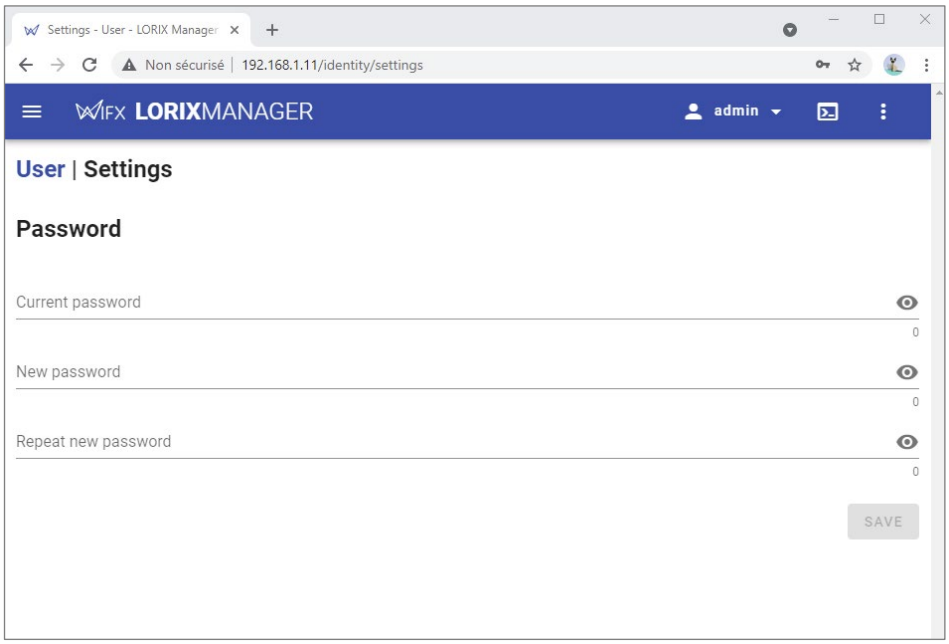
If all is working, you can now reach your gateway using SSH and the web interface which will be used by default for the next chapters.

7.2 SECURITY

7.2.1 PASSWORD

One of the first step to do once logged in the web interface is to change the admin password. Unless you use your gateway for development in a controlled network, this is a basic security advice which can prevents obviously easy attack to be done.

To change it, click on the user (Top right corner of the web interface) → Settings:



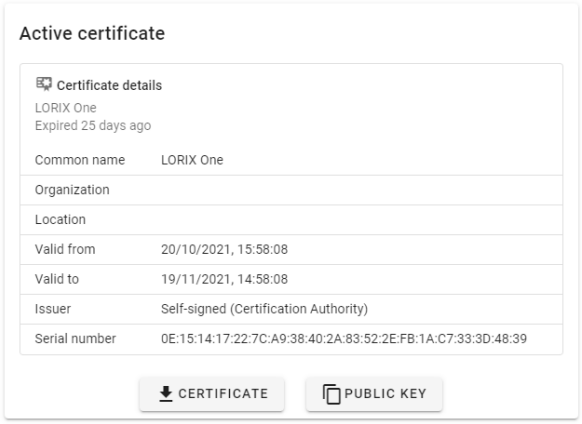
Enter the current password and the new one twice and click on Save button. You then get a notification which confirms the password has been changed.

7.2.2 SSL CERTIFICATE

From the web interface, you can read, define or generate a certificate from general preferences. On the top right corner, press on the 3 points button -> Preferences.

7.2.2.1 READ/DOWNLOAD THE CURRENT CERTIFICATE

You can find on this page, on the left the current certificate:



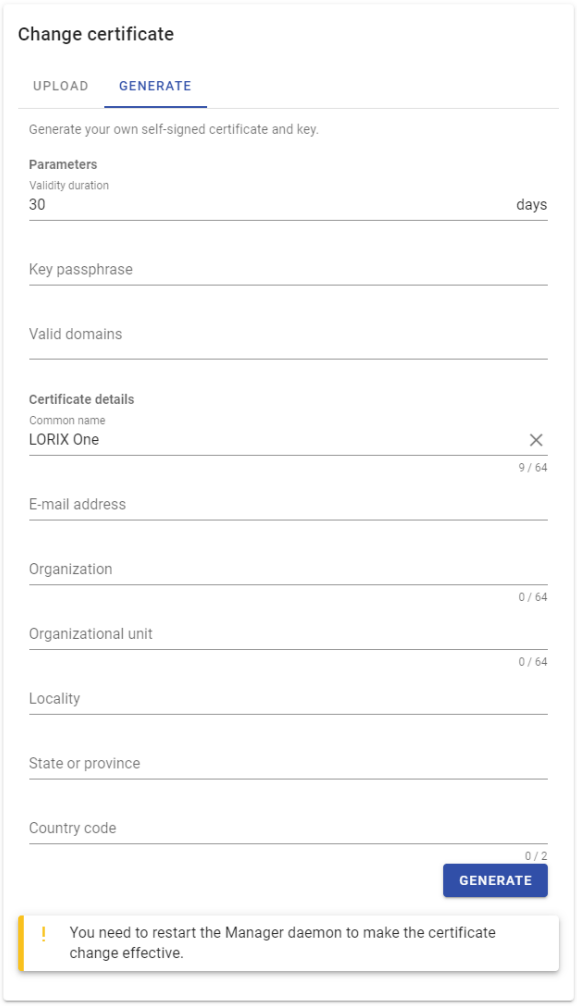
You can for example add this certificate to your web browser to explicitly recognize this device as known and avoid having the security warning.

Please consult directly your browser's documentation for that.

Initial certificate validity

By default, the initial certificate generated during first boot is valid only 30 days. To increase this validity, you need to generate yourself a new certificate from the web interface or import one from your own PKI.

7.2.2.2 GENERATE A CERTIFICATE



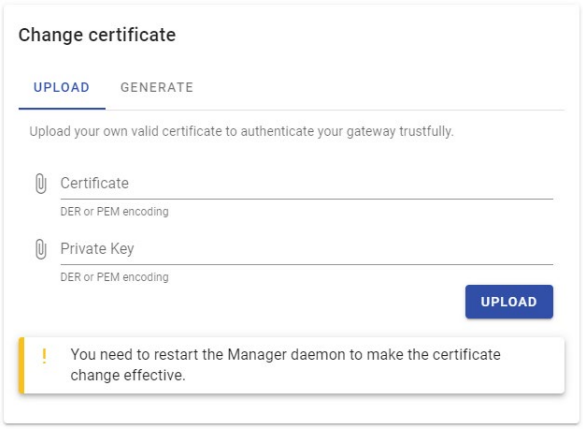
The certificate generator offers the possibility to create your own certificate with a custom validity for example.

If you don't have a root CA from which you can create and derive a device certificate, this is a good solution to create a custom certificate than you can immediately add to your browser's certificates store and which will ensure later the device is known and trusted.

Intermediate solution

This solution doesn't require a PKI nor a root CA on your side but you will need to add the device's certificate in every computer that will access the device to avoid the security warning and any potential security issue.

7.2.2.3 UPLOAD AN EXISTING CERTIFICATE



This is the best option but also the most advanced. If you want to ensure all your devices can be trusted while keeping configuration of your collaborators at the simplest, you can create a different certificate for each device and derived from your root CA.

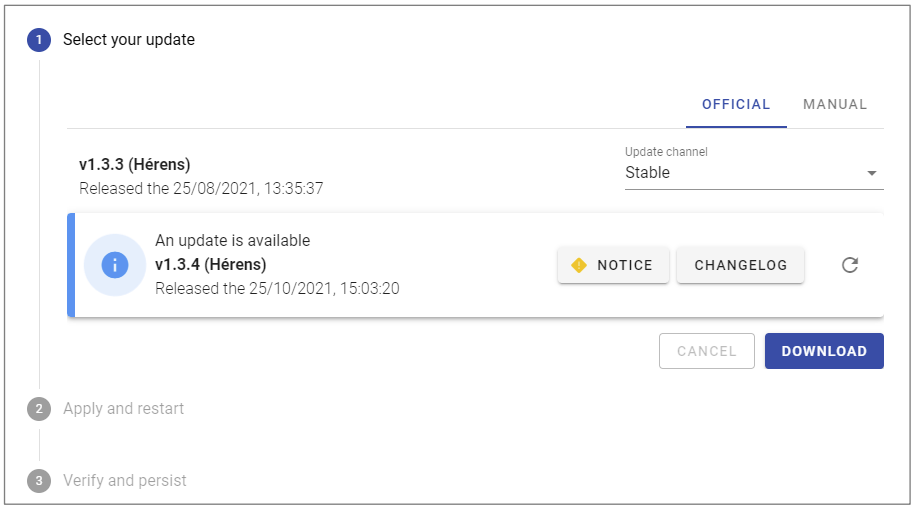
You can then add your public root certificate into the browser's certificates store and upload each device certificate into the device using the web interface on first configuration.

This way, you are sure the device you are accessing is known and trusted but also for your collaborators and using a chain of trust.

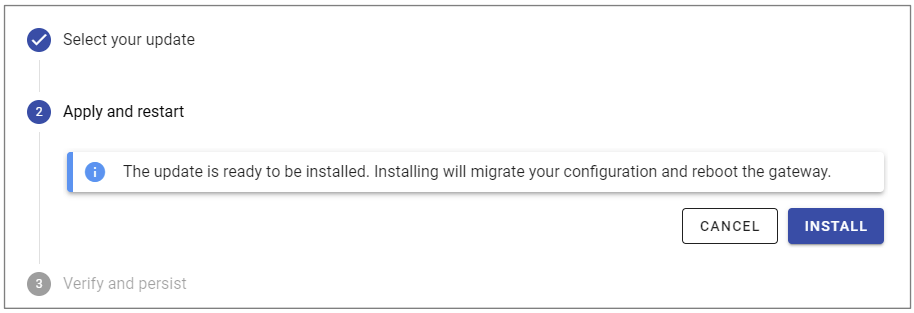
7.3 SYSTEM UPDATE

The network and security aspects have been defined. Prior to concrete usage of the product, we advise to update it to the latest available system version.

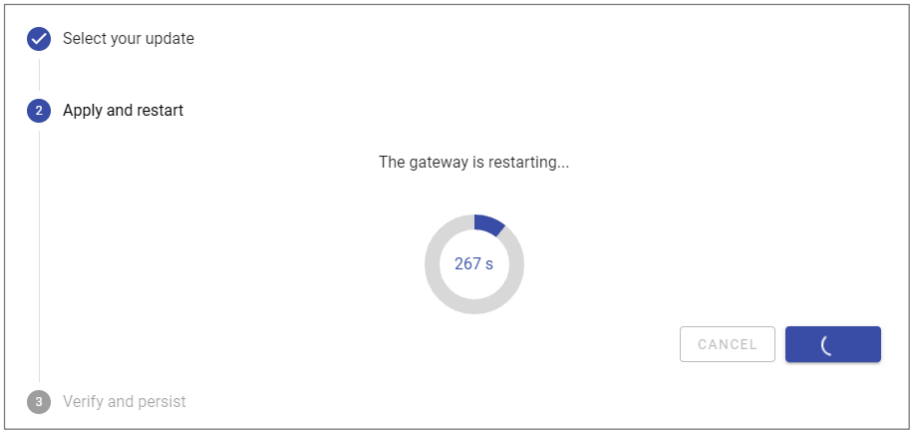
For that, go into System → Update and verify if a new version is available:



Downloaded image screen:

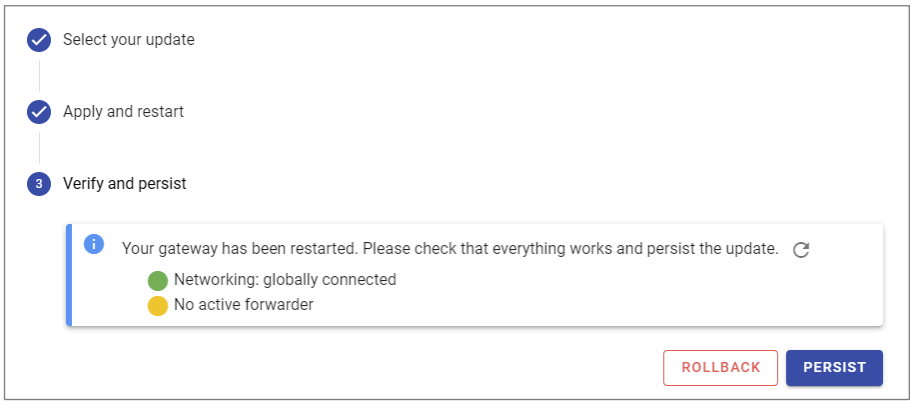


The image is ready to be flash into the gateway. Click on install then wait for the update to be complete:



During the reboot, you will be disconnected.

> **Interface reconnection**
>
> The connection should be enabled again automatically after 3-4 minutes. If it's not the case, you can try to refresh the page and removing the cache using the command CTRL+F5.



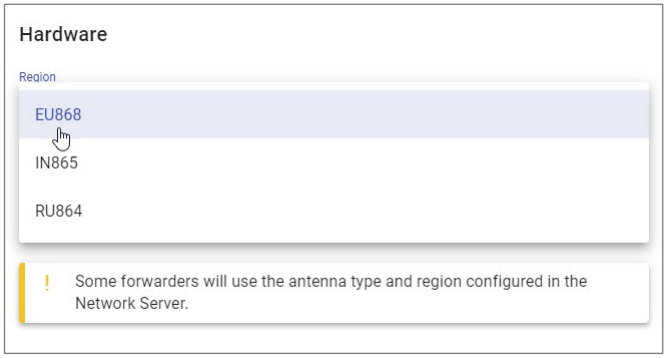
You are done and the system has successfully been updated. To confirm this new version, click on Persist button.

7.4 LoRa/LoRaWAN configuration

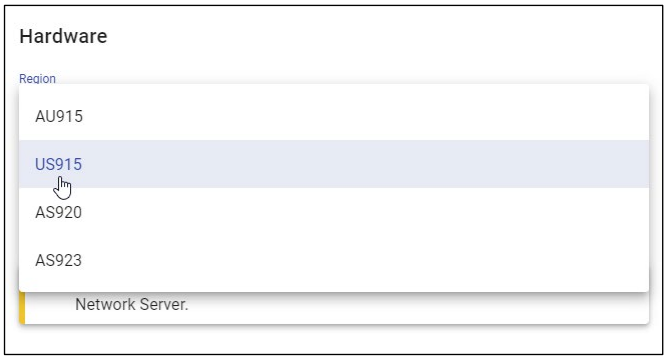
7.4.1 LoRa (RF)

Prior to any usage of LoRaWAN forwarder, you need to configure the region and the antenna. To do so, go into LoRa → Settings and define the region and antenna.

7.4.1.1 8XX Region



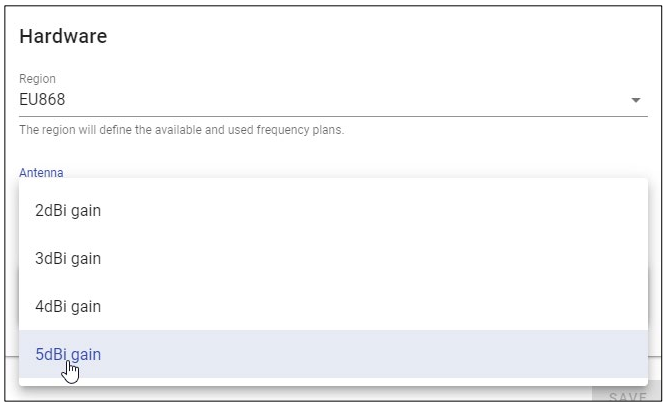
7.4.1.2 9XX REGION



Specific regions regulation

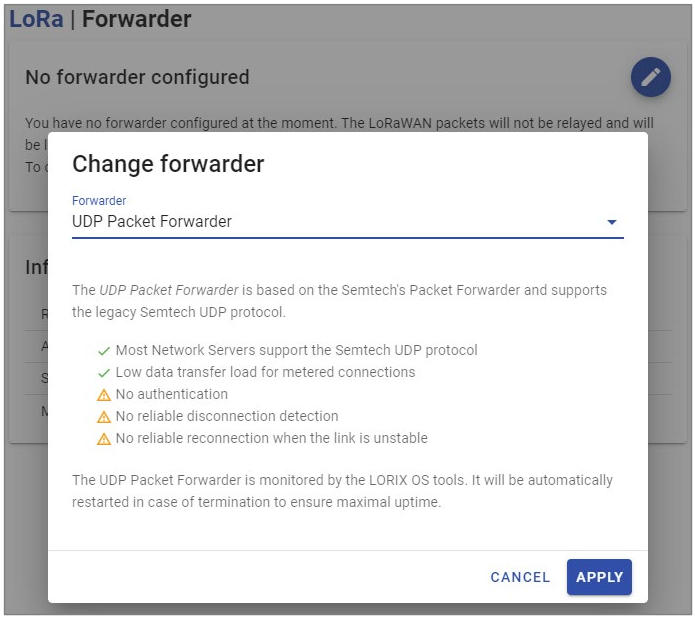
Be careful to not configure the region with doesn't correspond to your local regulation. For example, US915 uses frequency band 902-928MHz while only 915-928MHz is authorized in Australia.

7.4.1.3 ANTENNAS



7.4.2 LoRaWAN

Once the RF base is correctly configured, you can select your favourite forwarder under LoRa → Forwarder:



Clicking on the right blue button opens a modal window which displays the various forwarders and describes briefly the pros and cons of each solution.

Configuration of each forwarder will not be described here but can be found at https://iot.wifx.net/docs/go/forwarding.

7.4.3 GWID Format

The gateway ID is a 64 bits unique ID based on the 48 bits unique MAC address. The extended 64 bits address is simply created by removing the ":" of the MAC address and by adding the 2 Bytes 0xFF and 0xFE between the 3rd and 4th Bytes.

The format of the gateway ID (GWID) is the following:

Following this process, the MAC address **01:00:5E:22:BB:33** becomes the gateway ID **01005EFFFE22BB33**.

The gateway ID is also, on some clouds, under the form eui-<gateway ID>. In this case **eui-01005efffe22bb33**.

8 ELECTRICAL

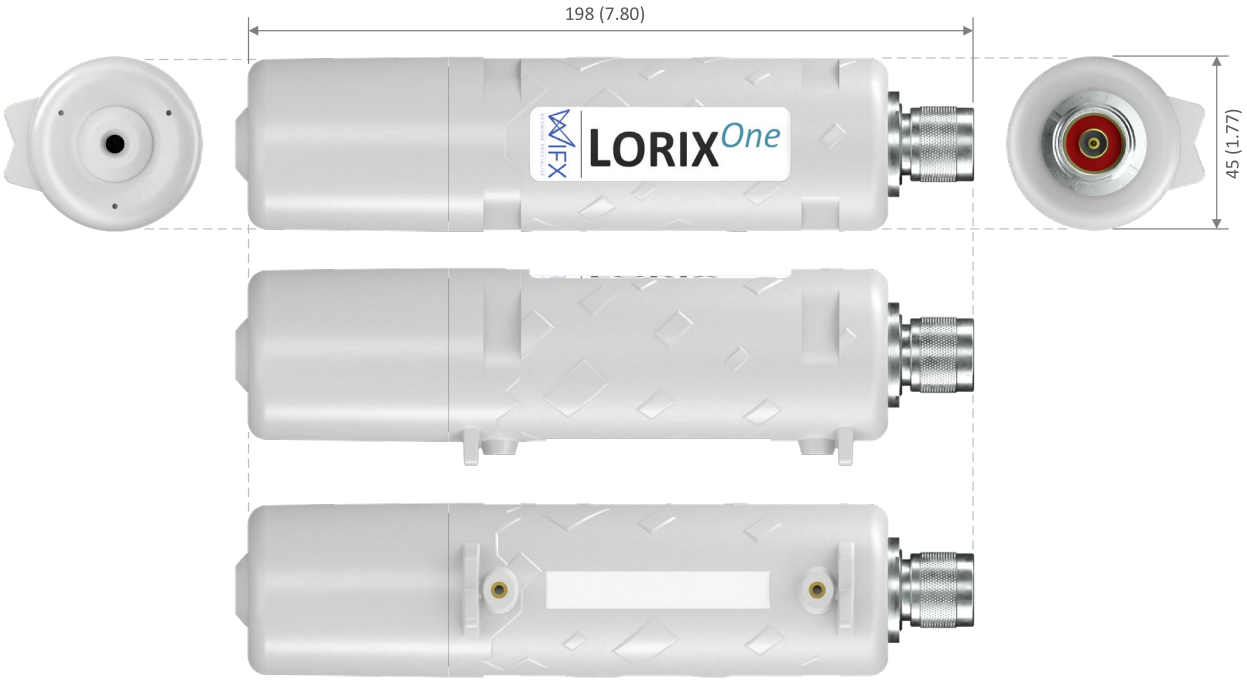
8.1 POWER CONSUMPTION

Task (@ 20°C ambient)	Voltage [V]	Current [mA]	Power [W]
Linux only running RF part disabled	24	42	1,01
LoRa gateway with util_pkt_logger 6 channels for RX	24	105	2,52
LoRa gateway with util_pkt_logger 8 channels for RX	24	117	2,81

9 MECHANICAL

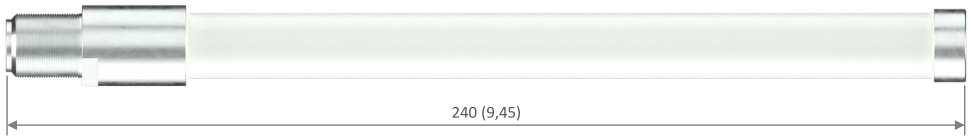
9.1 LORIX ONE

Dimensions in mm (inch)



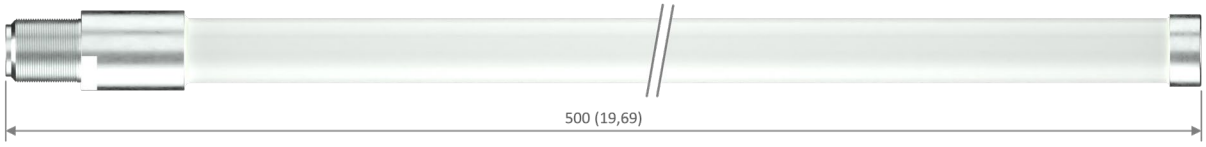
9.2 ANTENNA 3 dBi (8XX & 9XX VERSIONS)

Dimensions in mm (inch)



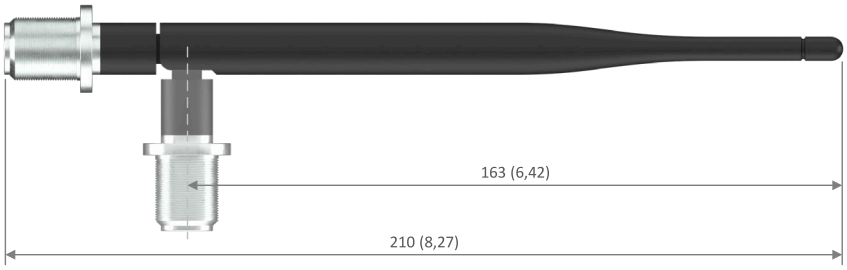
9.3 ANTENNA 5 dBi (8XX & 9XX VERSIONS)

Dimensions in mm (inch)



9.4 ANTENNA 2.15 dBi (8XX VERSIONS)

Dimensions in mm (inch)



10 SETUP GUIDE

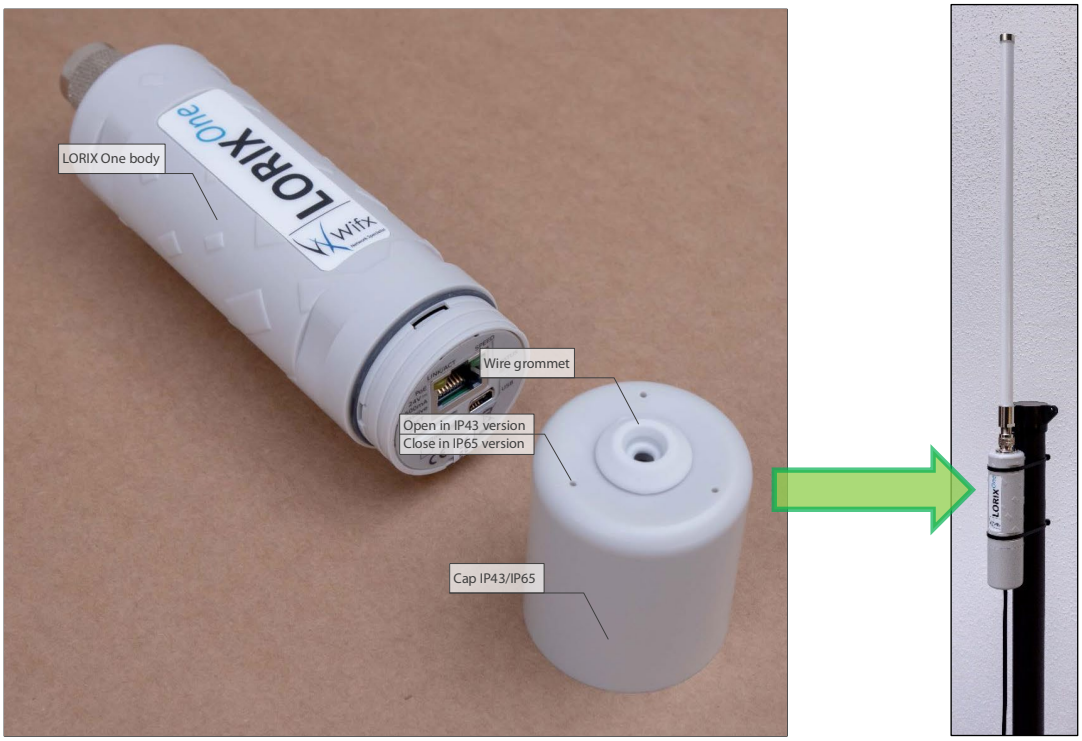
10.1 GENERAL RECOMMENDATIONS

The LORIX One gateway is designed to be placed **vertically** with the antenna pointing **upwards**.

If you wish to attach the LORIX One to a pole, it is strongly recommended to use the plastic mounting loops provided with the gateway which are UV-resistant. Guide the loops around the LORIX One through the edge markings, and attach the gateway around the pole where it will be mounted.

It is strongly recommended to not connect a loose Ethernet cable to the Ethernet port while attaching the gateway to a pole, to avoid adding weight to the port. Ideally, the Ethernet cable should be attached within 2 meters from the gateway device.

10.2 STANDARD MOUNTING USING A POLE



Remove the wire grommet from the cap.

Once the Ethernet cable passed through the cap hole, open the silicon grommet and put it around the cable as showed on the picture.

Be careful with the orientation of the grommet

Press the grommet with your finger from inside the cap (left picture) until take it final position (right picture).

Connect the Ethernet cable.

Move the cap in direction of the body while maintaining the cable with the other hand to keep the cable as straight as possible.

Screw the cap on the body to guarantee as good as possible water and dust protection.

Once fixed, be sure the cable is well placed and verify that the grommet is correctly positioned.

Use only appropriate antenna provided as accessory for the LORIX One.

Engage the antenna connector into the LORIX One RF connector as showed on the picture.

While maintaining the antenna into the LORIX One, start screwing with the other hand the RF LORIX One connector tightening ring.

Never turn or use directly the antenna body to screw it on the LORIX One, it could damage or break the antenna.

Once the cable and the antenna correctly connected and the LORIX One correctly closed, you can install it on a pole using the 2 provided cable tie.

The provided cable tie are black because they are specifically made to support UV.

You should use always the provided one or UV protected specifically.

Once the LORIX One well oriented and the cable tie well tight, use a cutting pliers to cut the exceeding plastic part of the cable tie.

The LORIX One is now installed on a pole using the provided elements (excluding Ethernet cable).

It is strongly recommended to not connect a loose Ethernet cable to the Ethernet port while attaching the gateway to a pole, to avoid adding weight to the port. Ideally, the Ethernet cable should be attached within 2 meters from the gateway device.

On the other side of the cable, use the PoE passive injector provided with the LORIX One as explained in the chapter 5.1 Power through passive PoE.

Once the LORIX One is correctly installed, consult the chapter 6 Service access to access and do the initial configuration.