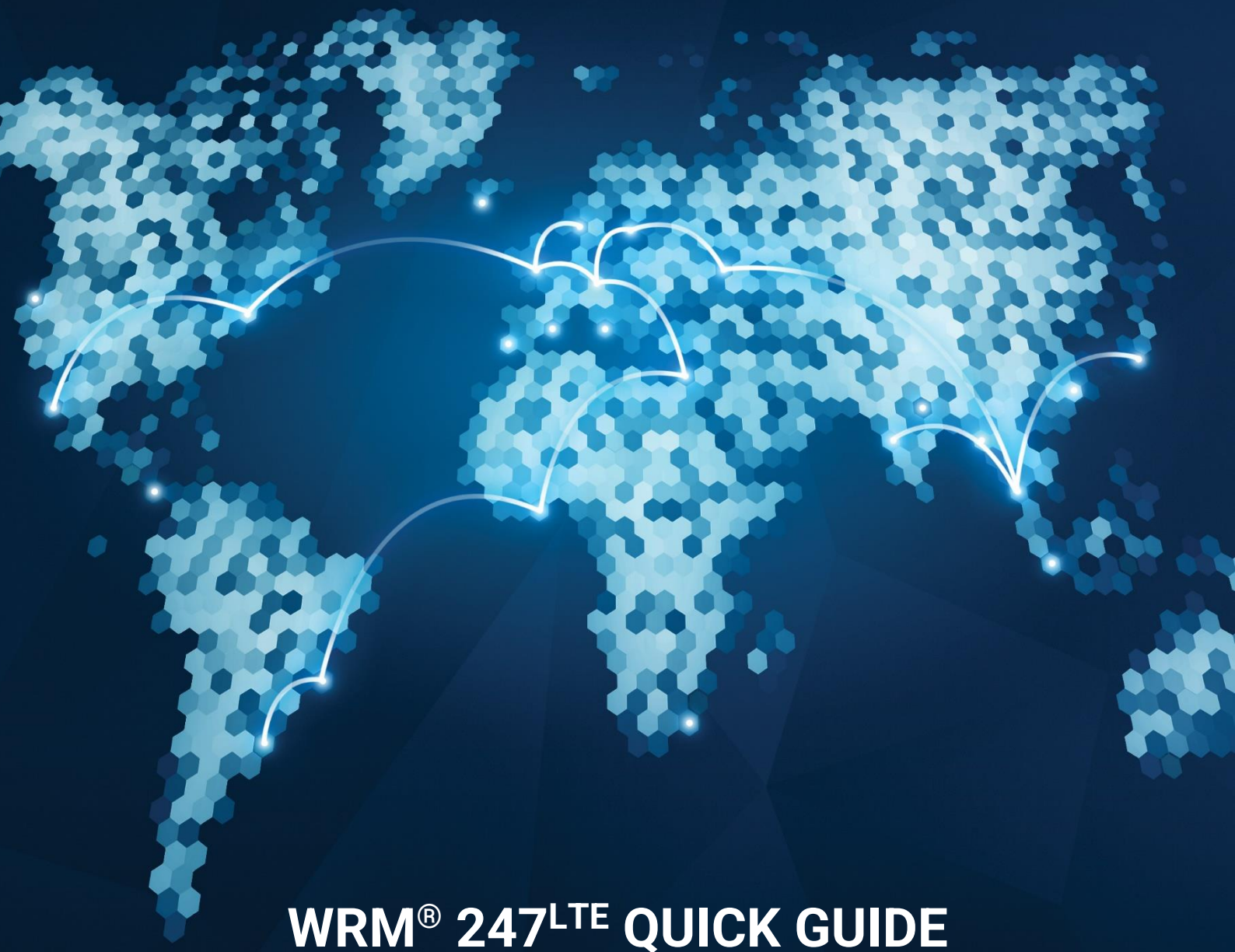
IoT-TICKET®

YOUR TICKET TO INTERNET OF THINGS AND BEYOND



WRM® 247LTE QUICK GUIDE

Copyright

Disclaimer of liability

To the extent that the document and the information in this document are provided free-of-charge, we will not be liable for any loss or damage of any nature.

You accept that we have an interest in limiting the personal liability of Wapice's employees. Having regard to that interest, you accept that we are a limited liability entity and agree that you will not bring any claim personally against Wapice's individual members or employees in respect of any losses you suffer in connection with this document, the products described in this document or these terms and conditions.

Nothing in the terms and conditions will limit or exclude our or your liability for fraud or fraudulent misrepresentation or limit any of our or your liabilities in any way that is not permitted under the applicable law.

Regulatory notices

Note:

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

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

NOTICE:

Changes or modifications made to this equipment not expressly approved by Wapice Ltd. may void the FCC authorization to operate this equipment.

Radiofrequency radiation exposure information:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Safety notes

Warning:

Make sure that all conducting systems entering from outdoors are sufficiently protected and antennas installed withing the area covered by a lightning protection system. When implementing lightning protection concept, adhere to IEC 62305 standard.

Notice:

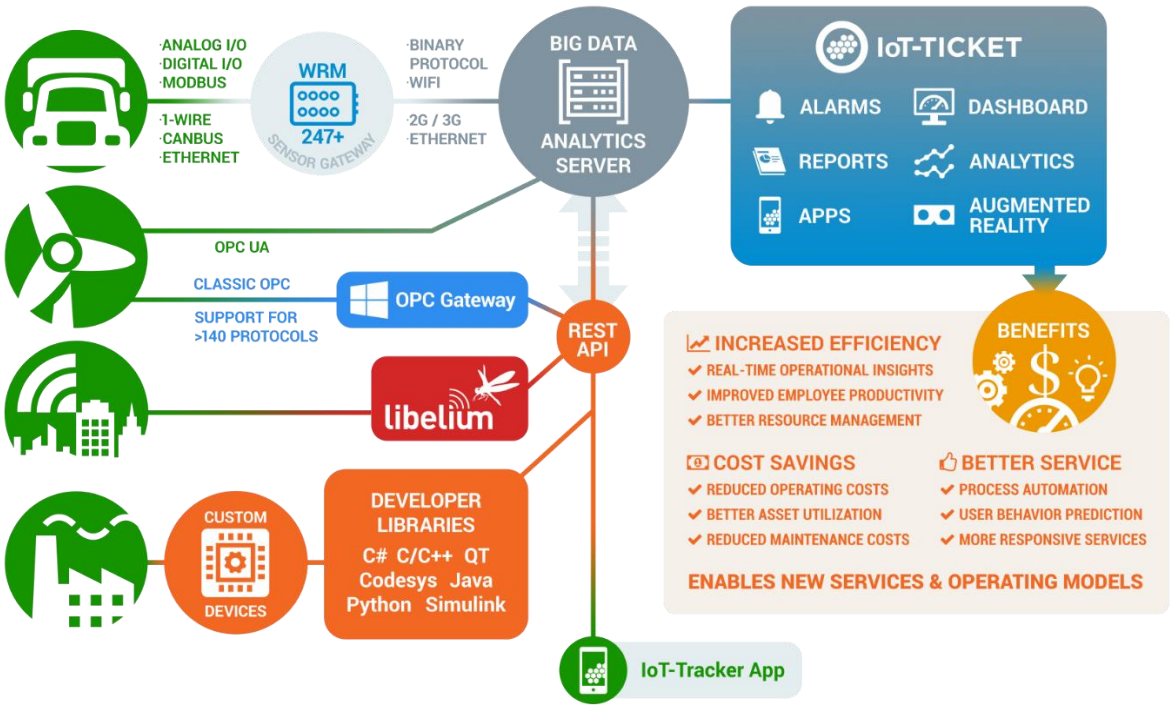
The device (and its components) may only be used for the application described in the instructions. Correct and safe operation of the device is only guaranteed only when it is set up, installed, and used according to the instructions.

Contents

About IoT-TICKET®

IoT-TICKET® is a complete Internet of Things (IoT) tool suite and platform allowing you to build web, mobile, cloud and reporting applications in minutes with big data analytics and easy to use tools.

IoT-TICKET covers versatile data-acquisition needs, Big-Data and analytics enabled servers, web-based Dashboards and Reports. With IoT-TICKET, one can create and deploy fully fledged IoT applications in minutes.



1. Introduction

WRM® 247LTE is a robust device for remote management, measurement, and control. The device can be used independently or as a part of Internet of Things platform such as **IoT-TICKET®**.

Designed by Wapice, it has complete customization opportunities to meet the requirements of industrial conditions. Wapice also provides complete software development services for the target system.

1.1 Technical specification

TECHNICAL DATA		
	Processor	ARM® Cortex™-A5, 536MHz
	RAM	512MB DDR2
	Flash	256MB NAND Flash
	Multimedia Card	1 Micro SD slot
	SIM Card	Nano-SIM
	Wireless Connectivity	GSM/GPRS/3G/4G, WLAN and WPAN external antennas
	GNSS	GPS L1, GLONASS, BeiDou & Galileo Tracking sensitivity GPS: -159dBm, GLONASS: -158dBm Acquisition sensitivity GPS: -147dBm, GLONASS: -146dBm
	Ethernet 10/100 Mbps	2 (4 pin M12 industrial Ethernet connectors)
	CAN	2
	RS-485	1
	RS-485 5V output	Max 100mA
	RS-232	1
	1-Wire	1, Max 10mA
	USB	1 x host, Max 500mA
	5V output	Max 500mA
	Digital output	4 x 0-1, level 1 configurable 5-30 V, max 200 mA current output
	Digital input	4 x 0-1, level 1 any between 5-30 V
	Analog input	2 x 0-22 mA and 2 x 0-30 V, compatible with 4-20 mA current loop
	DC supply voltage range	7 – 56 Vdc
	LED	1 programmable red/green LED, GSM LED and 2 x Ethernet LED
	Accelerometer	Digital, triaxial, 16 bit, ±2g/±4g/±8g/±16g
	Supported OS	Real Time Linux
	RTC Back-up capacitor	Yes
	IP Class	IP 65
	Operating temperature	-30°C to +60°C
	Weight	615g
	Dimensions	173mm x 95mm x 67mm (without antennas), cast aluminum casing
	GSM Bands	GSM850, GSM-900, GSM-1800, GSM-1900 Max. transmitted power: 33dBm, 27dBm on GSM-900
	3G Bands	WCDMA FDD Band 1, WCDMA FDD Band 2, WCDMA FDD Band 3, WCDMA FDD Band 4, WCDMA FDD Band 5, WCDMA FDD Band 6, WCDMA FDD Band 8, WCDMA FDD Band 19 Max. transmitted power: 24dBm
	LTE bands	LTE 1, LTE 2, LTE 3, LTE 4, LTE 5, LTE 7, LTE 8, LTE 12, LTE 13, LTE 18, LTE 19, LTE 20, LTE 26, LTE 38, LTE 40, LTE 41, LTE 66 Max. transmitted power: 24dBm
	WLAN & WPAN	2.4-2.48GHz Max. transmitted power: WLAN 17.5dBm / WPAN 8.5dBm

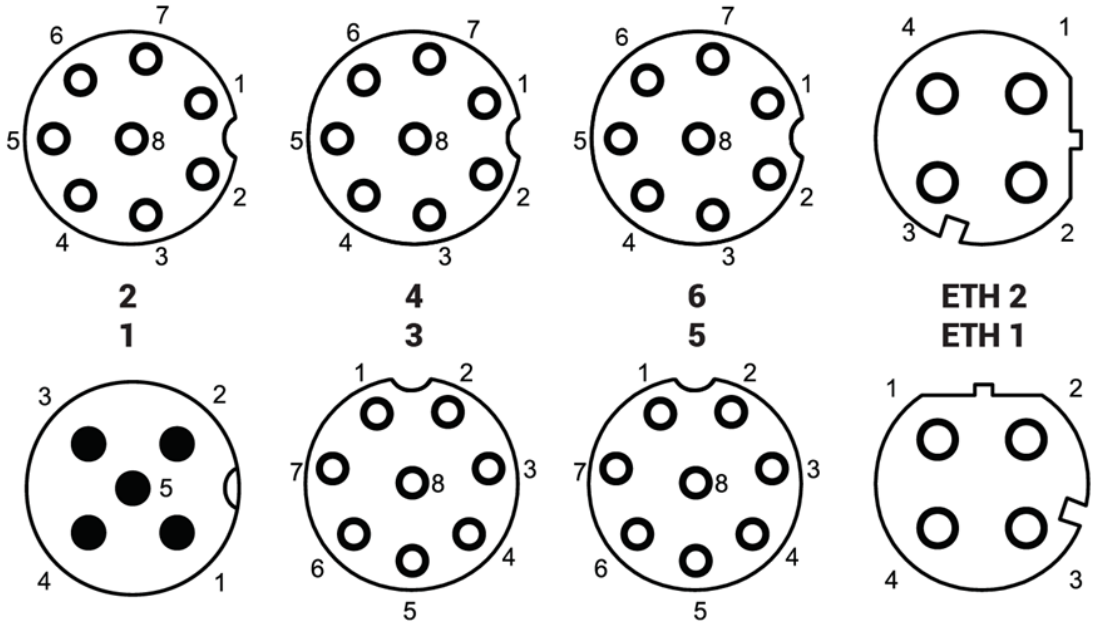
1.2 Connecting the device

Upon configuration, the user must connect the WRM® 247LTE module via the power cable to a power source, connect the WLAN antenna to the module by screwing it in and connect the module to the computer via the Ethernet cable. Details on the recommended cables and antenna are offered in the sections below. The equipment must be powered by a PS2 source in compliance with the IEC 62368-1 standard.

1.3 Pin connectors (top)

The arrangement and functionality of the eight pin correctors of WRM® 247LTE device is listed below.

> ***Note:*** The tables are arranged in the same way the connectors are arranged on the WRM® 247LTE device.



Connector 2
1. Analog voltage input 2
2. 4-20mA current input 2
3. 4-20mA input 2 return
4. 4-20mA input 1 return
5. Analog voltage input 1
6. 4-20mA current input 1
7. Analog GND
8. Analog GND

Connector 4
1. RS-485 +5V output
2. RS-485 D+
3. RS-485 D-
4. Digital input 2
5. Digital input 3
6. Digital input 4
7. RS-485 GND
8. GND

Connector 6
1. Debug serial RXD
2. CAN 2 H
3. CAN 2 L
4. Debug serial TXD
5. 1-Wire Vcc
6. CAN GND
7. GND
8. 1-Wire DQ

Ethernet 2
1. Ethernet 2 TX+
2. Ethernet 2 RX+
3. Ethernet 2 TX-
4. Ethernet 2 RX-

Connector 1
1. Digital output supply+
2. Power supply +
3. Digital output 1
4. Digital input 1
5. Power ground

Connector 3
1. USB Host Power
2. USB Host D-
3. USB Host D+
4. Digital output 2
5. Digital output 3
6. Digital output 4
7. USB Host GND
8. GND

Connector 5
1. RS-232 RXD
2. CAN 1 H
3. CAN 1 L
4. RS-232 TXD
5. +5V output
6. CAN GND
7. GND
8. GND

Ethernet 1
1. Ethernet 1 TX+
2. Ethernet 1 RX+
3. Ethernet 1 TX-
4. Ethernet 1 RX-

All the device pin connectors are manufactured by Phoenix Contact. Their exact types as well as the recommended corresponding cable connectors from Phoenix are presented in the table below.

Connector	Connector type on the device	Recommended connector for cable assemblies
Connector 1	SACC-CI-M12MS- 5CON-SH TOR 32 with SACC-BP-M-M12/M15-6-THR	SACC-M12FS-5CON-PG 7-SH
Connectors 2 - 6	SACC-CI-M12FS-8CON-SH TOR 32 with SACC-BP-F-M12/M15-6-THR	SACC-M12MS-8CON-PG 9-SH
Connectors 7 & 8	SACC-CI-M12FSD-4CON-L180-THR with SACC-BP-F-M12/M15-6-THR	SACC-M12MSD-4CON-PG 9-SH

All the cable connectors at the table above have knurled thumb screw fasteners, whose recommended fastening torque is 0,4 Nm. Exceeding this recommended value when tightening the connectors may damage the device. There are torque tools available e.g. from Phoenix Contact for fastening the thumb screw fasteners with accurate torque.

1.4 Antenna connectors (side)

In addition to the connectors on top of the WRM® 247LTE device, there are also 4 SMA antenna connectors at ends of the device, one for each of the following:

- 4G (main)
- 4G DIV (diversity)
- GPS/GNSS
- WLAN/WPAN

In case the device needs to be connected via one of the above wireless interfaces, the specific antennas must be connected to the device. Wapice may offer them upon request. No warranty is given, and no responsibility taken for defects of the third-party items offered by Wapice. The recommended tightening torque for the SMA connectors of the device is 0,4 Nm. Unused antenna connectors shall be fitted with a protective cap to ensure IP65 water protection.

1.4.1 Supported antennas and antennae requirements

European Economic Area compliance testing of the WRM® 247LTE has been carried out using the WLAN 001-0001 antenna from Laird Connectivity and 3G/LTE GNSS 2J6941MGFa antenna from 2J Antennas. Use of any other antenna than mentioned above is not permitted, without re-certification.

The FCC compliance testing of the WRM® 247LTE has been carried out using the WLAN 001-0001 antenna from Laird Connectivity and 3G/LTE GNSS 2J6941MGFa antenna from 2J Antennas. Antennas with same radiation pattern and peak gain that is less than or equal to certified antennas is allowed without re-certification.

The 001-0001 WLAN antenna has an omnidirectional radiation pattern at a maximum antenna peak gain of 2 dBi. To use alternative WLAN antennas in FCC regions on WRM® 247LTE without re-certification, an antenna with an omnidirectional radiation pattern and a peak gain being less than or equal to 2 dBi is required.

The 2J6941MGFa 3G/LTE GNSSS antenna has an omnidirectional radiation pattern at a maximum antenna peak gain of 8 dBi. To use alternative 3G/LTE antennas in FCC regions on WRM® 247LTE without re-certification, an antenna with an omnidirectional radiation pattern and a peak gain being less than or equal to 8 dBi is required.

1.5 Installing WRM® 247LTE device

WRM® 247LTE device can be installed on a wall or ceiling or used on a surface horizontally. A screw mounting is recommended, if the device is installed to a height exceeding two (2) meters. All connectors that are not in use should be sealed with plugs that the device is delivered with.

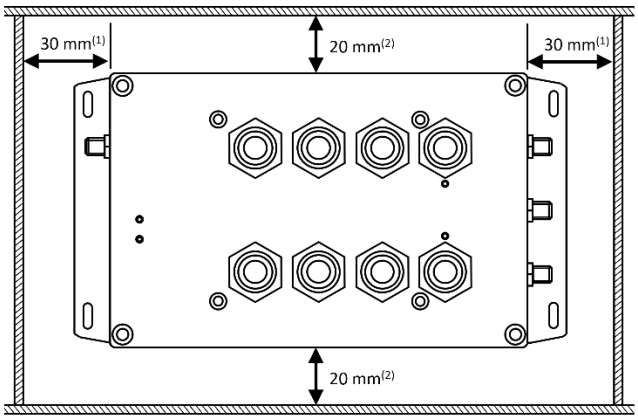
1.5.1 Wall or ceiling mounting WRM® 247LTE device.

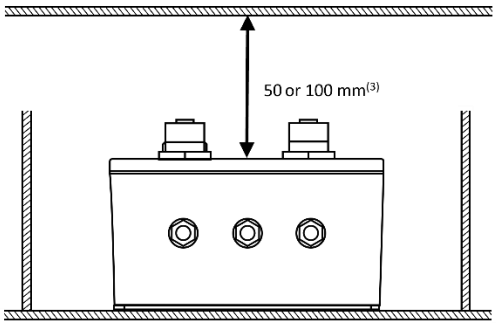
The device should be mounted on a vertical surface or on a ceiling from flanges at both ends of the housing, applying 2 screws per flange. The screws should be 3.0 - 3.5 mm in diameter. The most appropriate choice of mounting screw type depends on the material of surface the device is attached to, which is why no precise recommendations on the screw type are given in this guide. The person mounting WRM® 247LTE should however ensure that the screws can

hold up the device against the installation surface with at least 20 N force, i.e., firmly enough for keeping a 2 kg object attached to a ceiling.

1.5.2 Installation angle and dimensions

In the case of vertical surface installation, it is recommended that the device is aligned horizontally, as in the figure below. The figure also demonstrates the minimum clearances needed for different wire harness types.





(1) Clearance is mandatory with one or more antennas or antenna cables attached to SMA connectors.
(2) 20 mm clearance is required on the side of the device, if any cables with 90° angle connectors are attached to the device top connectors on the same side. If merely cables with straight M12 connectors are used, no clearance on the sides is needed.
(3) 100 mm clearance is needed if any cables with straight M12 connector are attached. If only connectors with 90° angle are used, 50 mm clearance will suffice.

1.6 LEDs and the meaning of their colors or statuses

There are four LEDs on the WRM® 247LTE device, each of them displaying statuses for the following functions:

STATUS LED	
LED off	Powered off
Orange	Working normally

ETHERNET 2 LED (GREEN)	
LED off	No link
Blinking	Network activity
LED on	Link active

MODEM LED (GREEN)	
LED off	Not connected
Blinking	Trying to connect
LED on	Connected

ETHERNET 1 LED (GREEN)	
LED off	No link
Blinking	Network activity
LED on	Link active

1.7 Opening the enclosure cover

Opening the WRM247 enclosure is not advised unless internal components such as SIM-card or SD-card needs to be changed. The device must be powered off and opening the enclosure must be done using considerable caution and care. Repeated opening and closing of the enclosure may degrade the ingress protection. For more details on SIM-card installation refer to Section 3.1.2.1.

Enclosure cover is mounted with four (4) 6-32 x 1/2" O-ring sealed threaded screws visible on top of the case. Make sure not to lose or damage the O-ring seals on the screws as well as the seal ring on the outer edges of the enclosure. The enclosure cover screw's must be tightened to a torque of 25-30cN.m to meet the specified enclosure ingress protection rating.

2. Configuration settings for the WRM® 247LTE

By default, the WRM® 247LTE device's DHCP client is enabled on both Ethernets. Upon connecting WRM® 247LTE to a network, device will attempt to request an IP-address trough DHCP process and connect to IoT-TICKET® server without any action needed from the user's side. The default networks settings of the WRM® 247LTE device are presented in the table below:

Interface	Settings
Ethernet 1 (ETH1)	**Status:** Enabled (always enabled) **DHCP (dynamic):** Enabled
Ethernet 2 (ETH2)	**Status:** Enabled (always enabled) **DHCP (dynamic):** Enabled
WLAN	**Status:** Disabled **DHCP (dynamic):** Enabled
Modem (4G)	**Status:** Disabled **APN server:** internet **PIN code:** -

If the interface and DHCP are enabled, but WRM® 247LTE device fails to get DHCP lease (i.e. there is no DHCP server available), then the WRM® 247LTE device will use the IP settings presented in the table below:

Interface	Settings
Ethernet 1 (ETH1)	**Status:** Enabled **IP:** 192.168.100.100 **Subnet mask:** 255.255.255.0
Ethernet 2 (ETH2)	**Status:** Enabled **IP:** 169.254.255.240 **Subnet mask:** 255.255.0.0
WLAN	**Status:** Enabled **IP:** 192.168.101.100 **Subnet mask:** 255.255.255.0

Note: Usually the operating system tries to identify the network for a while before falling to the DHCP lease fail IP. During this period, the WRM® 247LTE device is not accessible.

2.1 Setting up communication to local user interface

2.1.1 Direct connection from WRM to PC

Connect an M12 ethernet cable between WRM® 247LTE and PC. Device's Local UI can be accessed from lease fail address of Ethernet 2 interface (https://169.254.255.240). By default, Windows operating system will assign itself fallback IP address from the same 169.254.0.0/16 address pool as ETH 2

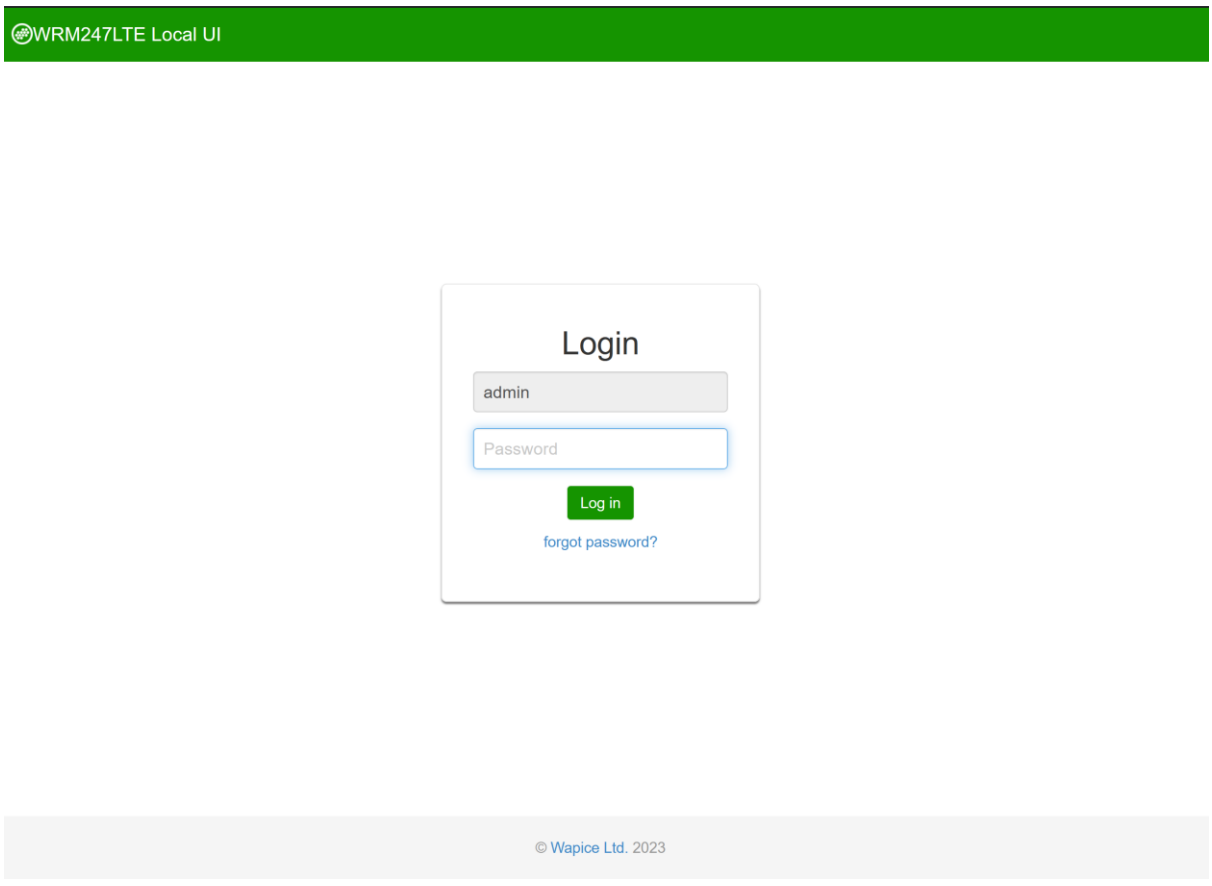
2.1.2 How to find out the WRM® 247LTE device's IP when DHCP is enabled?

Access the network administration interface and inspect the assigned IP addresses, the MAC address of WRM® 247LTE is printed out on the device.

If the WRM® 247LTE device has received an IP address trough the DHCP service and is connected to internet, then the user may get the IP address from the network settings data node of the corresponding device in the IoT-TICKET®.

2.2 Starting the web connection

After the IP configuration, the user may access the local user interface for the WRM® 247LTE by just typing https://<WRM_DEVICE_IP> in any browser, where WRM_DEVICE_IP is the IP address of the WRM® 247LTE device. The device uses self-signed certificate for the HTTPS traffic, user must accept the self-signed certificate when connecting to the device.

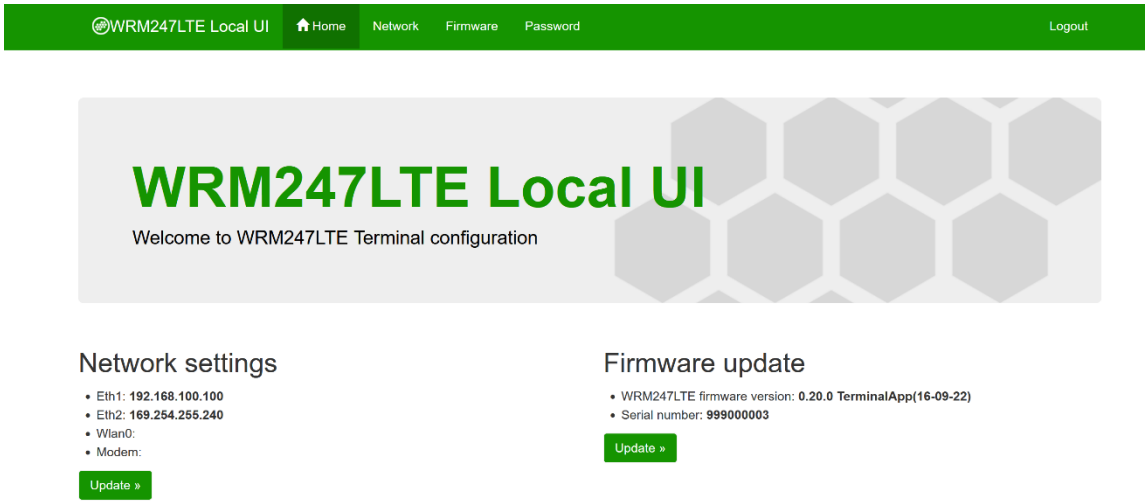


The Username is always **admin,** and it cannot be changed. By default, the password is **device serial number**.

Note: It is recommended to change password after the first login!

3. Local UI

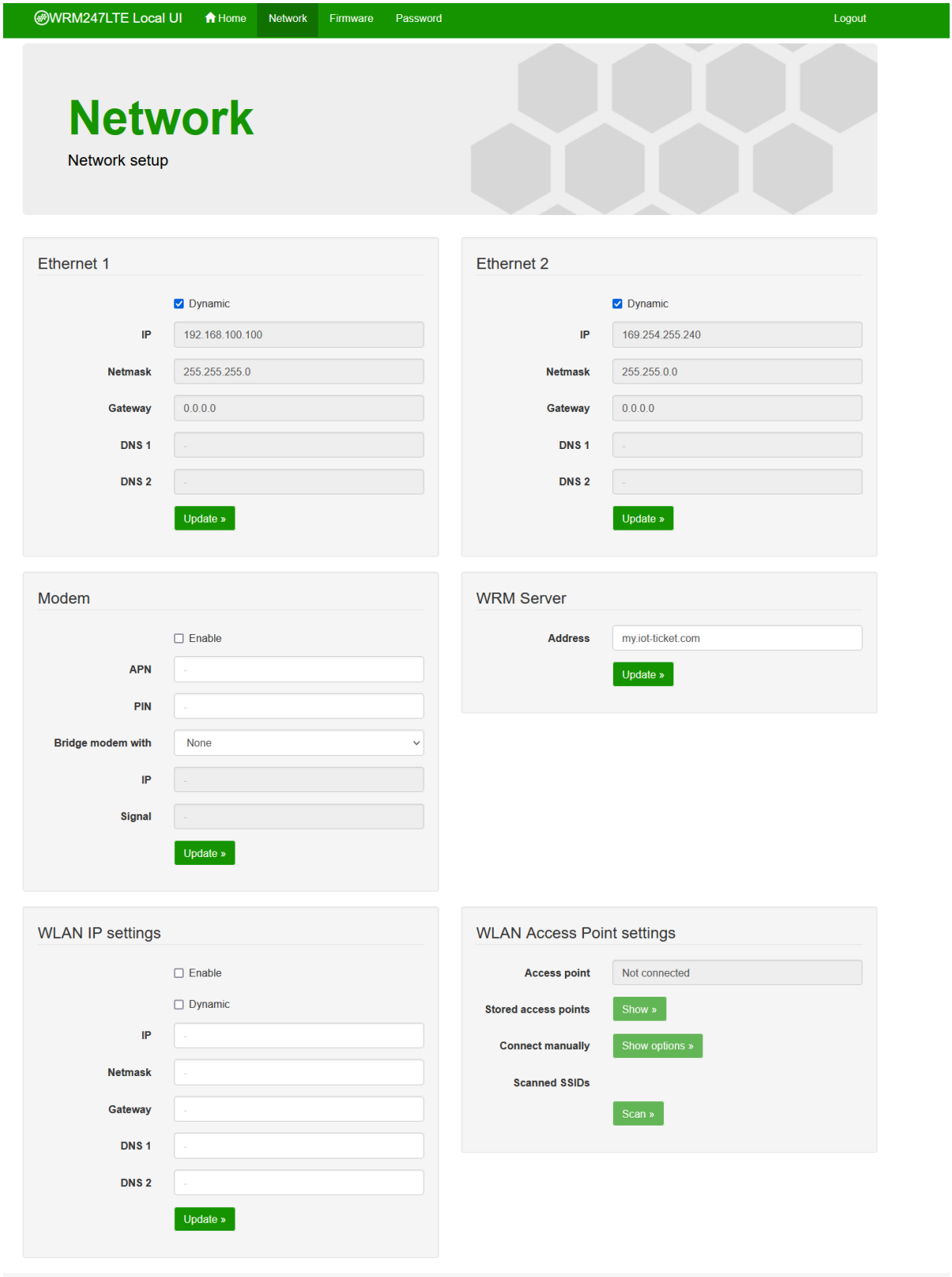
Once the IP configuration for the WRM® 247LTE device is done and the user logs in to homepage of the local user interface, the main view is displayed.



Next to the name of the page, in the navigation bar, the user may access all the pages available for the local UI: **Home**, **Network**, **Firmware** and **Password**. At the same time, the navigation bar includes the **Logout** button that disconnects the user from the homepage.
The main pane of the homepage includes information related to the **Network settings** and the **Firmware update**, together with the buttons that are linked to the respective pages.

3.1 Network settings

Either by selecting **Network** on the navigation bar or by clicking on the **Update** button under **Network settings** in the main pane of the homepage, the user may open the **Network settings** page of the device.


WRM247LTE Local UI
Home
Network
Firmware
Password
Logout
Network
Network setup
Ethernet 1
Dynamic
IP
192.168.100.100
Netmask
255.255.255.0
Gateway
0.0.0.0
DNS 1
DNS 2
Update »
Ethernet 2
Dynamic
IP
169.254.255.240
Netmask
255.255.0.0
Gateway
0.0.0.0
DNS 1
DNS 2
Update »
Modem
Enable
APN
PIN
Bridge modem with
None
IP
Signal
Update »
WRM Server
Address
my.iot-ticket.com
Update »
WLAN IP settings
Enable
Dynamic
IP
Netmask
Gateway
DNS 1
DNS 2
Update »
WLAN Access Point settings
Access point
Not connected
Stored access points
Show »
Connect manually
Show options »
Scanned SSIDs
Scan »

The Network settings include the settings for the four network interfaces: Ethernet 1, Ethernet 2, Modem and WLAN. The UI always shows the current active settings the WRM® 247LTE device has.

To take edited settings into use, the **Update** button must be pressed, otherwise the changes in settings made by the user will not be saved.

3.1.1 Ethernet

The available settings for the Ethernet that can be modified according to the user's desires are the following:

- **Dynamic** – If set, the DHCP client is enabled, and all the static fields are disabled so that they cannot be modified.
- **IP address**
- **Netmask**
- **Gateway**
- **DNS 1 server**
- **DNS 2 server**

If the user decides to use static IP settings, user may do so by unmarking the box in front of **Dynamic**. Once done, the user must at least give an **IP address** and a **Netmask** for the device. All the other fields are optional.

3.1.2 Modem (mobile data)

The available settings for the modem (mobile data) that can be modified according to the user's desires are the following:

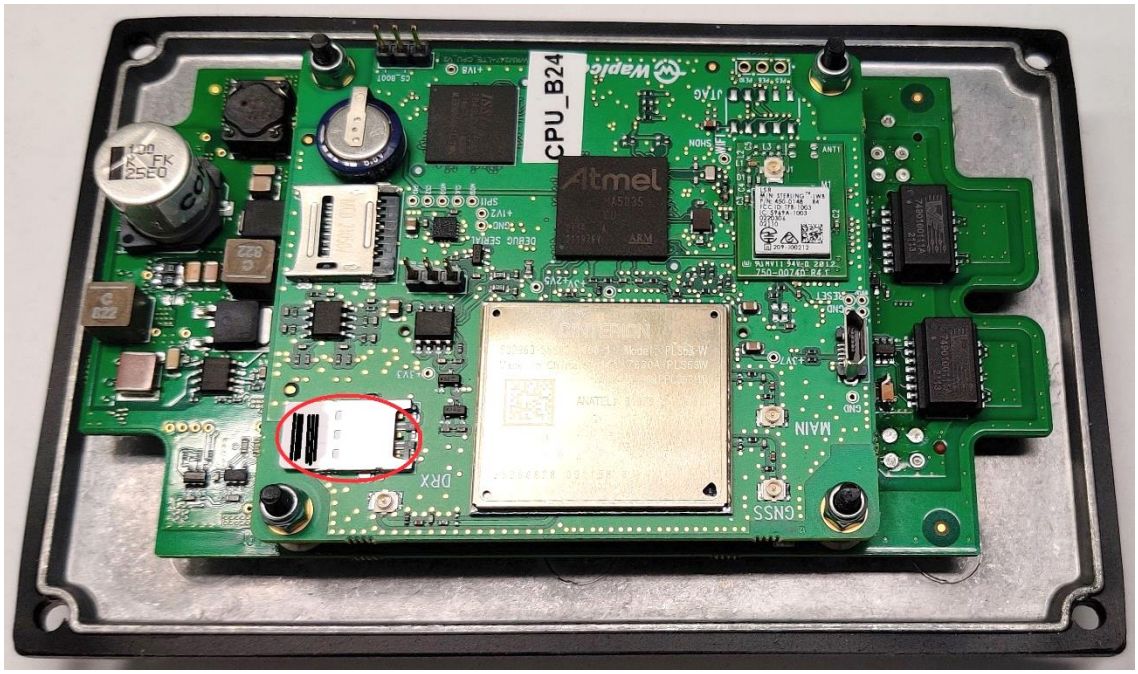
- **Bridge modem with** – Interface(s) which the Modem interface is bridged with. Using bridge, Modem's internet connection can be shared with selected interface(s). If WLAN is selected, WLAN hotspot is created based on settings defined for WLAN interface.
- **DHCP server in bridge** – Whether to use DHCP server in bridge. DHCP lease parameters are determined based on settings on corresponding interface.
- **Enable** – Activate Modem interface and enable mobile data communication.
- **APN** – Access point name for the SIM card used for mobile data communication.
- **PIN** – PIN code for the SIM card used for mobile data communication.

By default, the modem interface is disabled. If the user decides to enable the mobile interface, then the APN server of the mobile operator is required to be set. Most operators in Finland use *internet* as the APN server address.

If the SIM card used in the WRM® 247LTE device does not have a PIN code set, then the PIN field under the modem settings may be left empty.

3.1.2.1 Inserting the SIM card

The WRM® 247LTE device uses a standard nano SIM card. The card may be inserted in the slot available side as shown in the images below. Read instructions on *1.7 Opening the enclosure cover*, before opening the cover.



3.1.3 IoT-TICKET® server

The local user interface enables the user to set up the server address of IoT-TICKET® server that the WRM® 247LTE device will connect to.

> ***Note:*** By default, the IoT-TICKET® server address is: my.iot-ticket.com. This address should not be changed unless the user has a private installation of an IoT-TICKET® server.

3.1.4 WLAN

The available settings for WLAN that can be modified according to the user's needs are the following:

- **Enable** – Activate WLAN interface.
- **Dynamic** – If set, the DHCP client is enabled, and all the static fields are disabled so that they cannot be modified. The cursor will change into a forbidden icon in order to show the user that the WLAN settings are not editable when the box in front of Dynamic setting is marked.
- **IP address**
- **Netmask**
- **Gateway**
- **DNS 1 server**
- **DNS 2 server**

> ***Note:*** The WLAN access point scan and (802.1X) enterprise authentication features are currently only available in the device's local user interface and not in the IoT-TICKET® server.

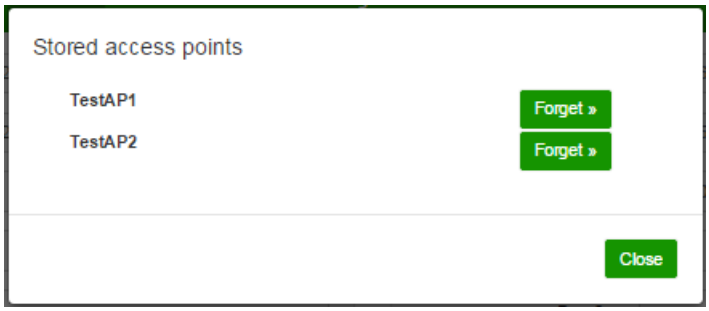
The WLAN interface supports the following authentication methods:

Method	Description
Open	The access point requires no authentication.
Pre-shared key (PSK)	The access point uses pre-shared passphrase for authentication: WPE-PSK, WPA-PSK, WPA2-PSK.
Enterprise	IEEE 802.1X based enterprise authentication which uses a separate authentication server.

By default, the WLAN interface is disabled. The WLAN interface needs to be enabled for the user to be able to configure both the WLAN IP settings and the WLAN access point settings.

The **Access point** field under WLAN access point settings shows if the WLAN has connected to the access point by showing the access point name or “Not connected” text. The time required to connect to an access point depends on the authentication method as well as on the access point itself. After establishing the connection, the user might need to refresh the page manually to show the correct connection status, if the connection takes longer than normally.

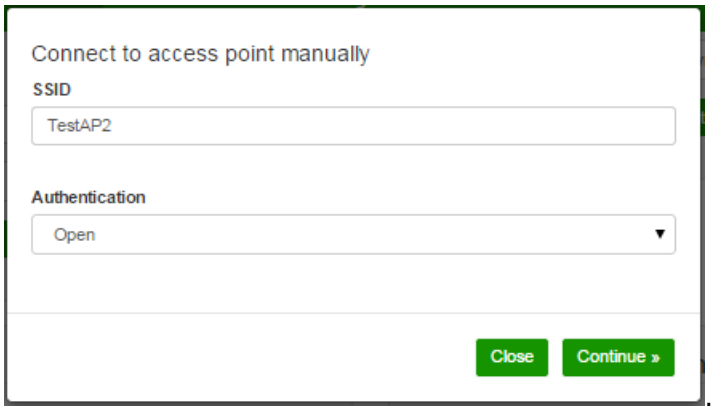
Clicking the **Show** button under **Stored access points** opens the list of access points which have previously been configured in the device. In the newly pop-up list of stored access points, it is possible to **Forget** access points, in case the user wants to delete the previously saved access points no longer valid. If WLAN is enabled and there are access points stored, the device will automatically try to connect to these saved access points.



The user may configure a new access point either manually or by scanning the wireless network. The manual setup can be used off-site or if the access point uses hidden SSID (not visible by scanning). The scanning method allows to connect to access points which are currently broadcasting their SSID to the wireless network.

3.1.4.1 Connecting to an access point manually

If the user wants to manually connect to an access point, the user must select the **Show options** button next to the Connect manually setting. The action opens a pop-up window where the user may input the SSID manually and may select the authentication method.

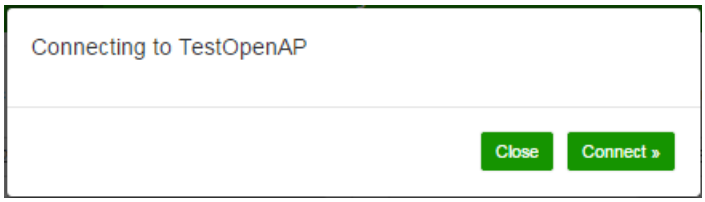


Upon selecting **Continue**, the user it taken to the next dialog window. The content of the next window depends on the selected authentication method. These dialogs are similar to the ones used when connecting to a scanned access point and they are described in the following section.

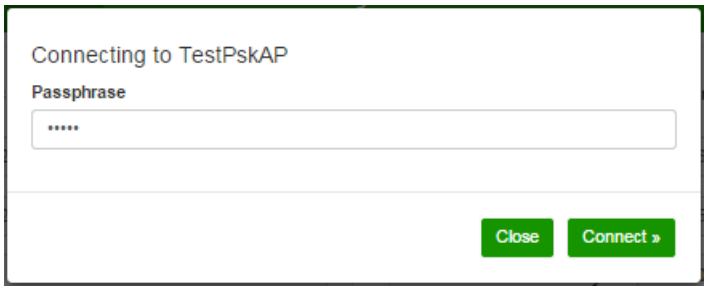
3.1.4.2 Connecting to a scanned access point

When the WLAN is enabled, the wireless network is scanned automatically once. The user may also scan the network by selecting the **Scan** button.

The WLAN automatically detects the authentication method which the scanned access points are using and opens a correct connection dialog accordingly. When connecting to an open access point, since the access point does not need any authentication information, the user does not need to input anything. When the user selects the **Connect** button, the access point's information is stored on the device, and the device tries to connect to the network.

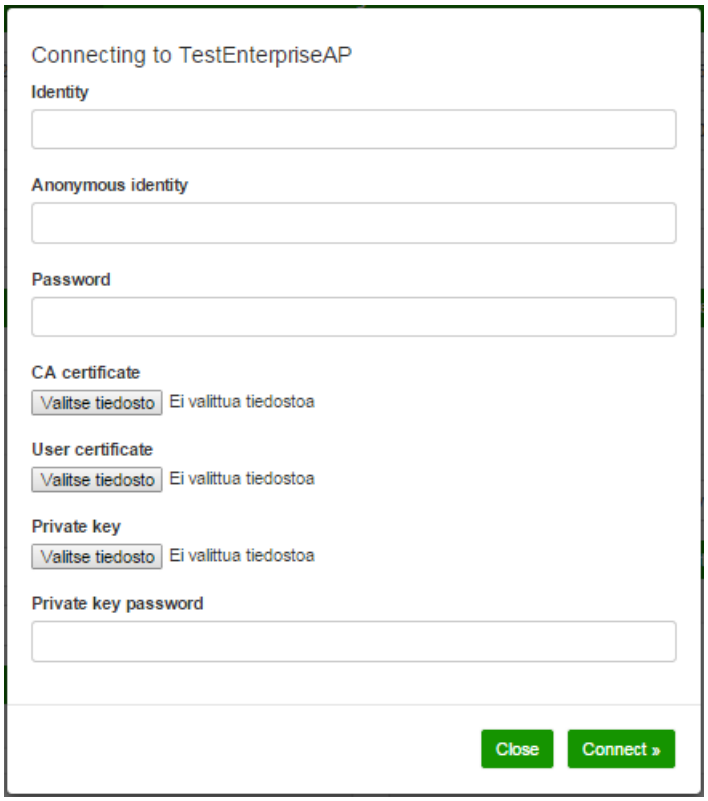


When connecting to an access point which uses pre-shared key, the user needs to provide the passphrase for the access point.



The third possible authentication method is IEEE 802.1X enterprise authentication. The following parameters are to be defined in order for the connection to be established:

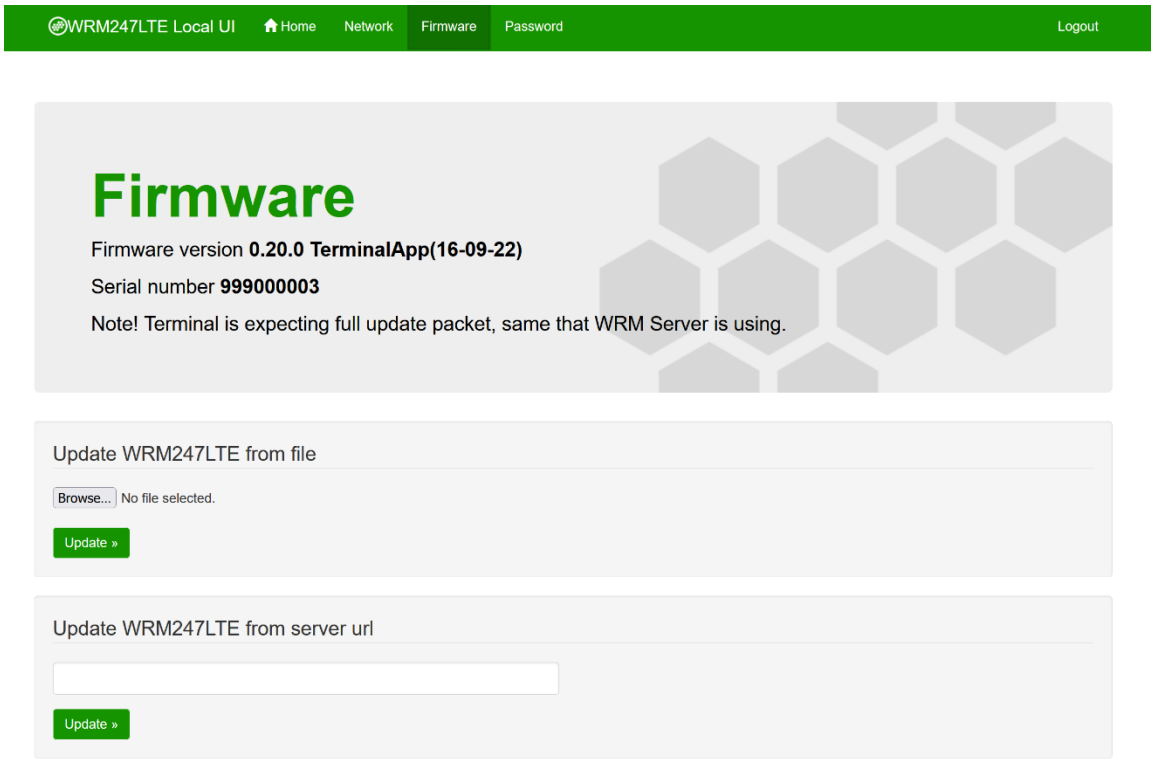
Parameter	Description
Identity	User identity, e.g., username or email address.
Anonymous identity	Anonymous identity for the unencrypted use. Real identity is sent only within an encrypted TLS tunnel.
Password	The identity's password.
CA certificate	The certificate authority which is used to validate the access point's certificate. If this is omitted, the access point certificate will not be validated.
User certificate	The certificate which is used by the access point to validate the user.
Private key	The private key which is used for encryption.
Private key password	The password for the private key file.



The WRM® 247LTE device cannot automatically detect which fields are required by the access point. Therefore, the user needs to obtain this information from the maintainer/administrator of the wireless network.

3.2 Firmware

Either by selecting Firmware on the navigation bar or by clicking on the **Update** button under **Firmware update** in the main pane of the homepage, the user may open the **Firmware** page of the device.



The Firmware page allows the user to update the WRM® 247LTE device software locally.

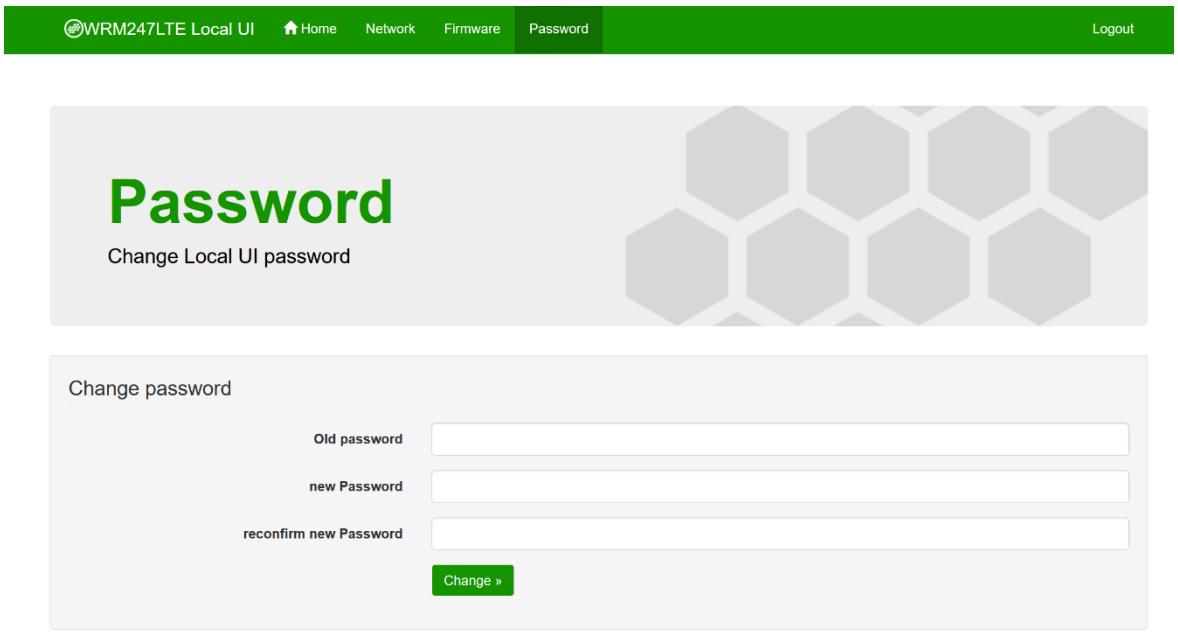
> ***Note:*** The user should use the firmware update from the IoT-TICKET® server. The user should not use the update from a file, unless there is some specific reason for the local update.

The user must give the server address from where the device can download the software package if the update from the server is used. The given address must include the entire path to the firmware package, including the file extensions, for example: *ftp://myserver/WRM247_firmware_package.tar.gz*.

When the **Update** button is selected, the firmware update starts. The UI informs the user when the firmware update is ready. At this point, the user must log in again.

3.3 Password

By selecting **Password** on the navigation bar, the user may open the Password page that allows for the change of the **admin** user's password.



The user must type in:

- The Old password
- The New password
- The Reconfirmation of new password

When **Change** button is selected, the new password is taken into use and the UI logs out automatically. The user must log in again with the new password.

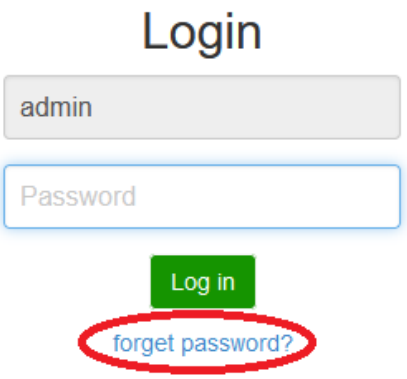
Reminder:

It is recommended to change the default password the first time you log in!

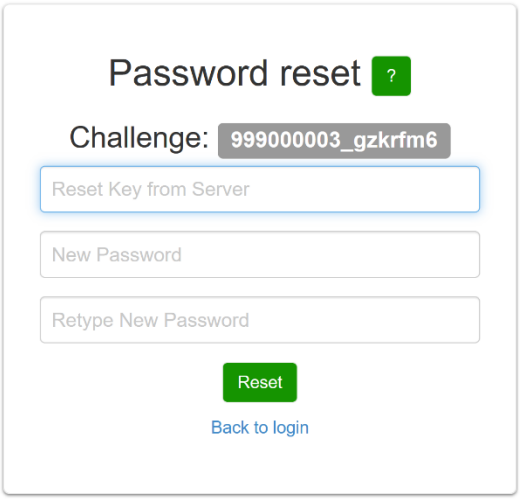
3.3.1 Retrieving the lost Local UI password

In case the Local UI password is lost, the user can request a new password by following the below steps:

1. Go to the local UI log in page and select the **forgot password?** link.



2. In the new pop-up window, copy the value displayed next to **Challenge** and paste it to *Reset Terminal Password* utility located on IoT-TICKET® server to generate the reset key for the WRM® 247LTE device.



3. Fill in the generated **Reset Key from Server**.
4. Type in a new password and retype it.
5. Select the **Reset** button.

The Local UI redirects the user to the log in page. The user may log in with the new password.

Wapice Ltd.

Yliopistonranta 5
65200 Vaasa, Finland
Phone +358 10 277 5000

Support@iot-ticket.com
IoT-TICKET.com