Configuring SolidSense networking with Kura

Foreword on Kura versions

The SolidSense software includes the version Kura 4.0 until release 1.1a. From release 1.2 onward (available in May 2021), SolidSense will be delivered with Kura 5, in sync with the official release of the framework by the Eclipse foundation.

For this steps, there are not a lot of differences, but one is very noticeable: Kura Web console access is now done **https instead of http**. So don't be surprised if some browser are reacting to that.If there is no reaction using the direct http access try https if you are not sure about the installed version.

First steps

You can start this step after the gateway has received its firmware. Either after it has been flashed by the user or the gateway has been delivered with the firmware loaded.

To perform the configuration steps described here:

1. The gateway shall be equipped with an antenna installed on the WiFi port
2. Gateway powered up with no USB disk inserted
3. Optionally a Ethernet cable can inserted in the RJ45 connector to connected the gateway directly to your local network
4. To setup a connection over cellular networks, the adapted antenna shall be installed the LTE port and a SIM card inserted in the SIM card holder accessible via door on the bottom of the device

To verify that the system is running, the simplest way is to check WiFi available networks and when the gateway is ready, the SSID <Serial Number> is broadcasted. The serial number is found on the system label.

Accessing the gateway Kura web interface

Default network configuration

Ethernet (eth0) => DHCP client. WAN interface

WiFi (wlan0) => Access point and DHCP server. LAN interface. IP 172.16.1.1

SSID = Gateway serial number

Password: 'testKEYS'

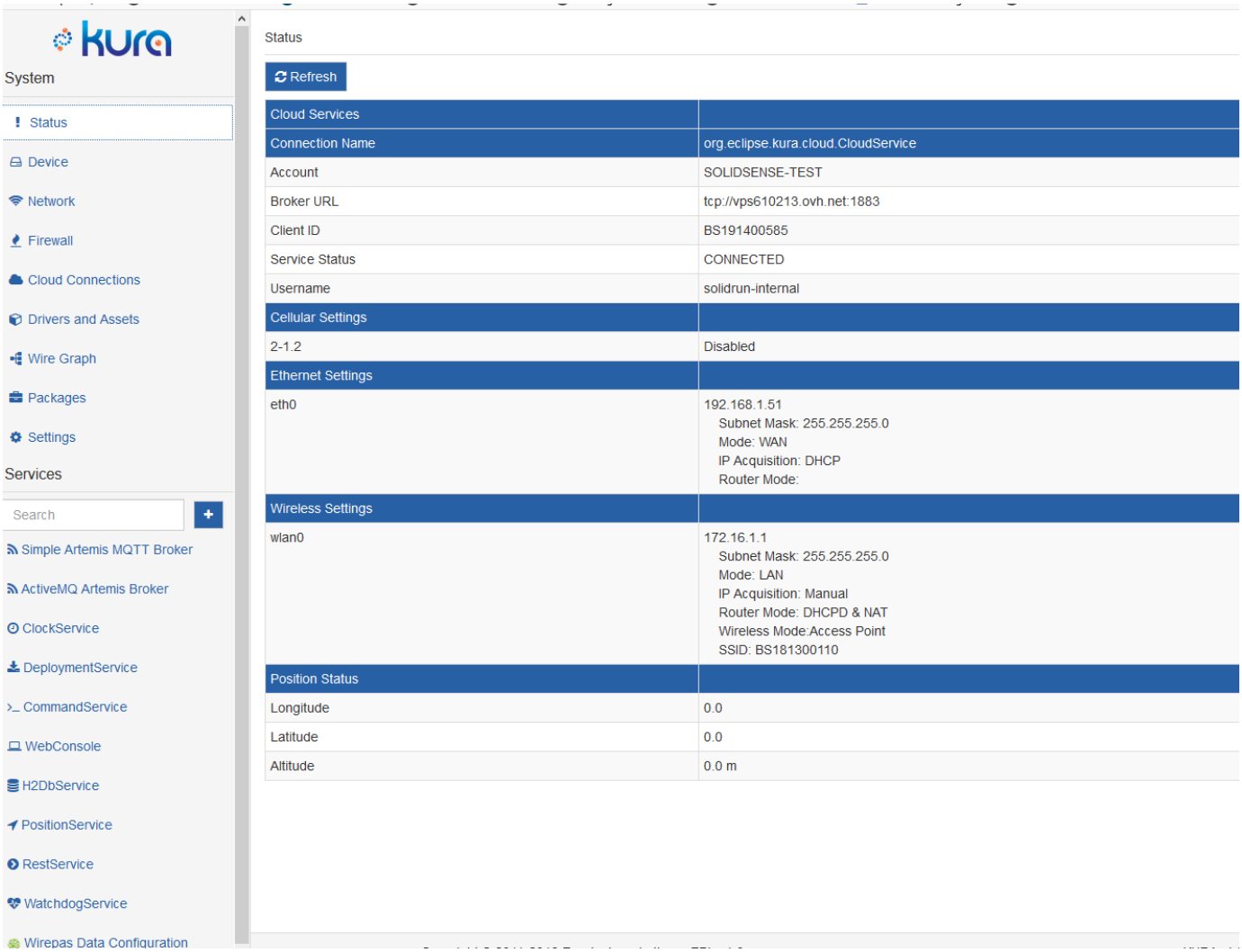
To access Kura you need a computer that is on a network that can reach the gateway directly (no NAT) then type in your browser:

for **Kura4**: http://<IP address or name>/kura

for **Kura5**: https://<IP address or hostname> or https://<IP address or hostname>/admin/auth

Default credential to access Kura: admin/admin

And the Kura welcome screen shall show



The important pages for configuration on the left are

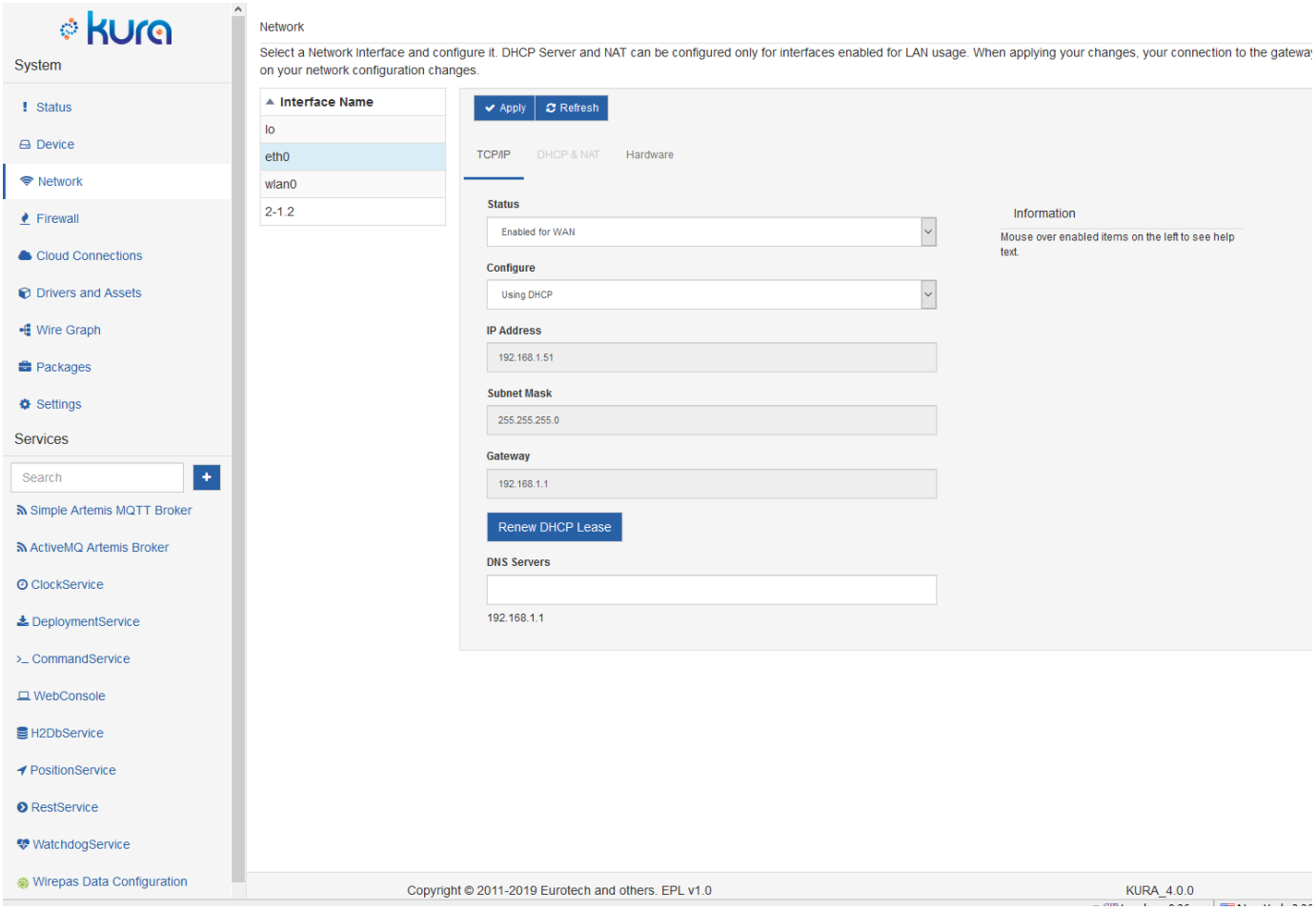
Network

Cloud Connections

> **Please Note**
>
> By default during installation, the gateway is initialized with Kapua credential on an internal SolidRun account (SOLIDSENSE-NURSERY). If the gateway is connected to the Internet you can see the status “connected”. See the relevant section below to configure your own access

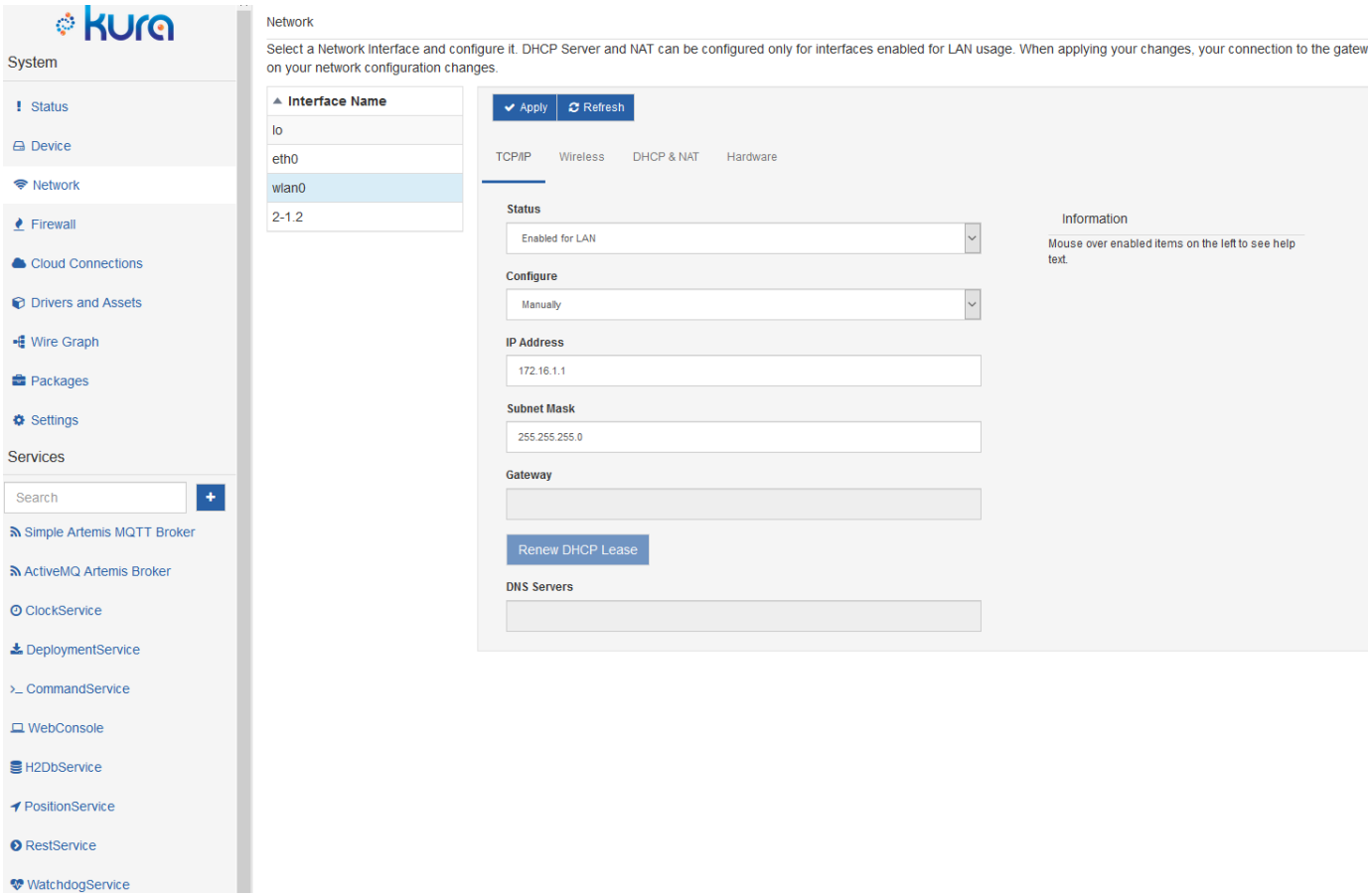
Cellular (ppp0) => disabled. When never configured appears as ‘2-1.2’

Connection to Ethernet

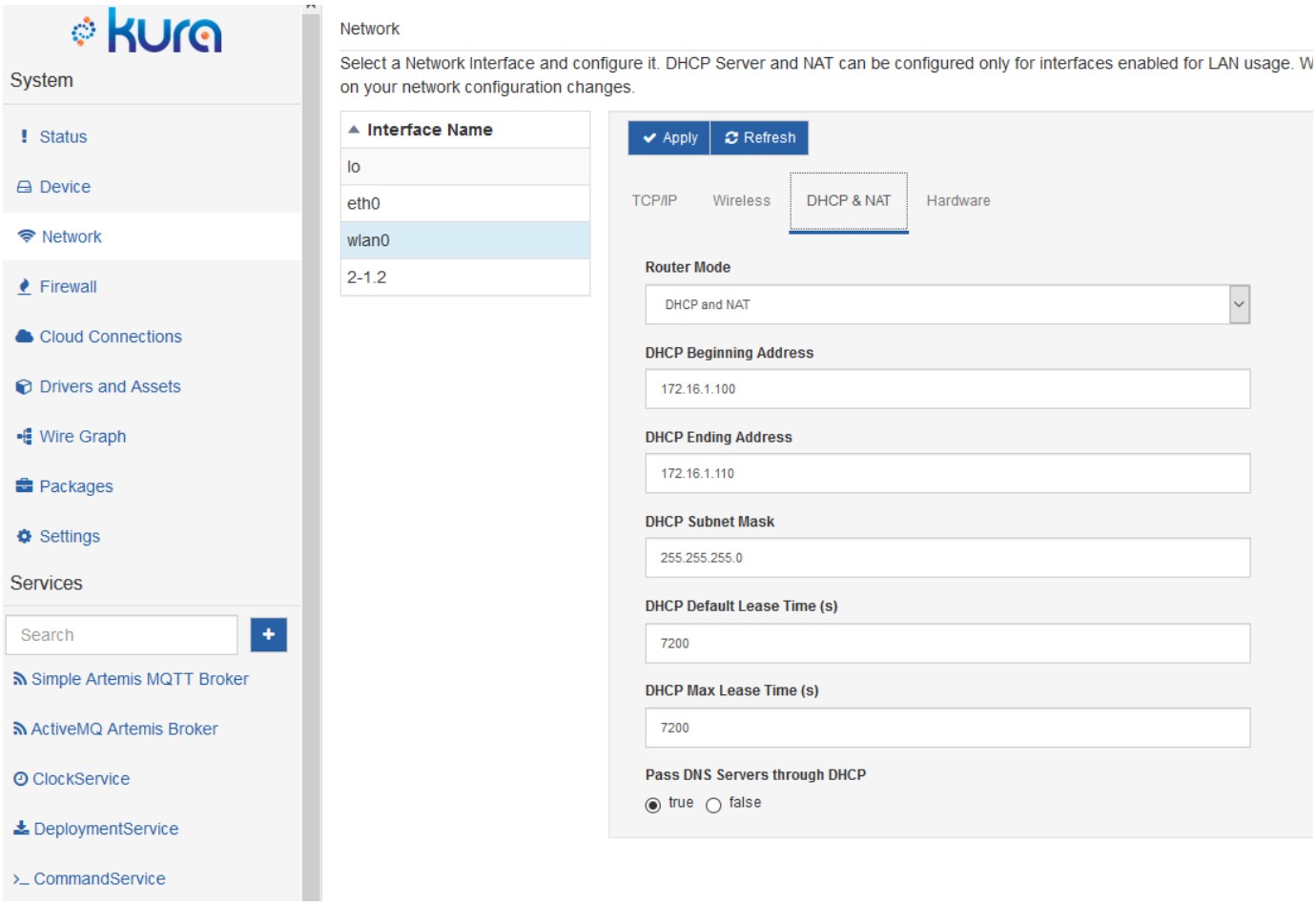


The Ethernet port can be set as DHCP server or DHCP client (default). If the Ethernet port is used for LAN access, it can be configured as a router for other device connected to this port.

Connection to WiFi



The WiFi interface can be set as Access Point (default) or Station. All parameters can be configured through this pages and sub-pages. Access Point is providing routing for all devices connected through it. To allow full routing don’t forget to select the feature pass DNS Servers through DHCP.



Connection to cellular network

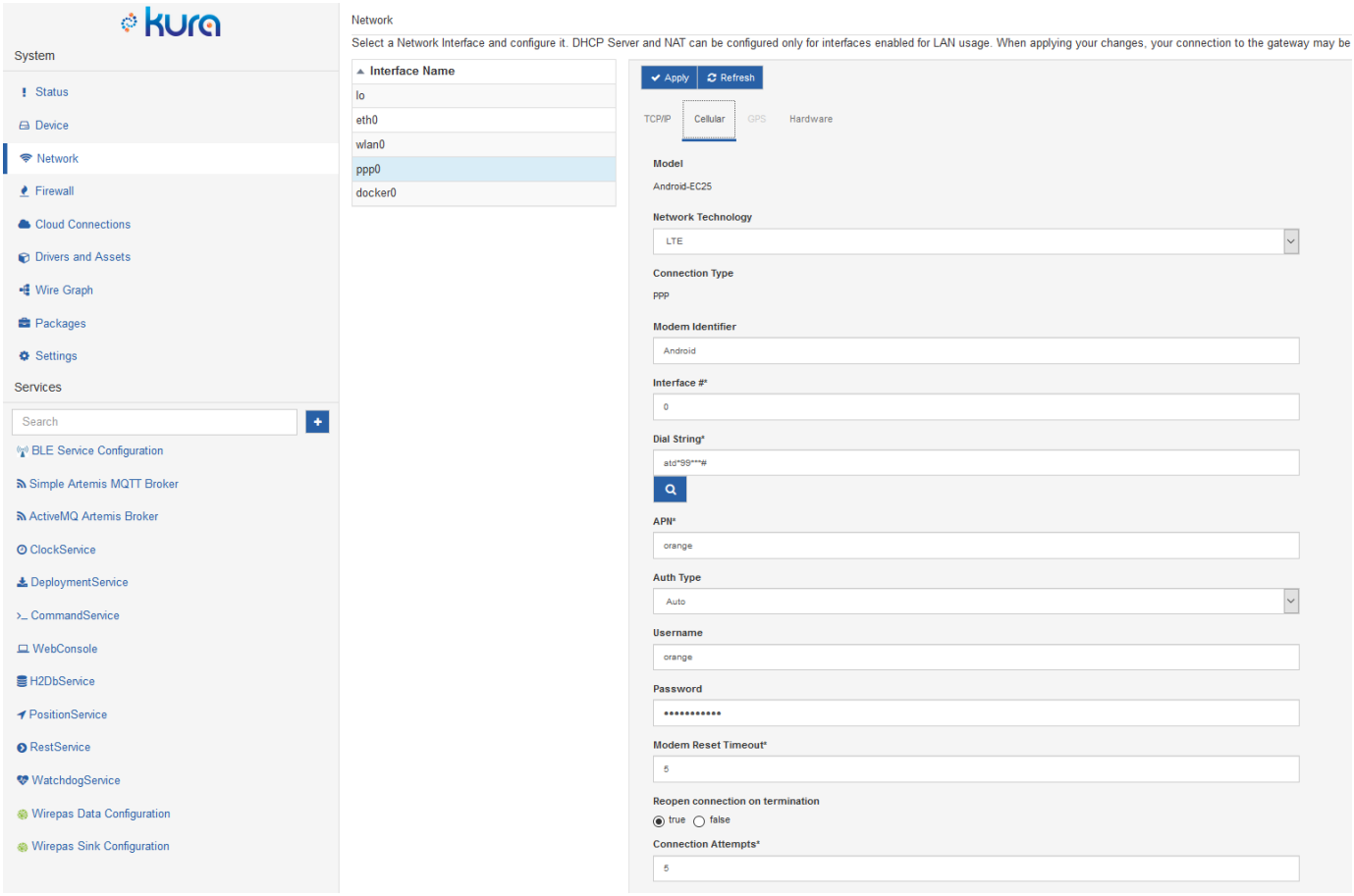
The following actions are needed

1. Insert a SIM with NO PIN in the system and reboot. The automatic SIM detection feature is not enabled. If your SIM card is protected by a PIN code, see how to unlock it via the Controlling and accessing the modem and GPS . You can then configure the PIN code in the service configuration file.
2. Set the eth0 as a LAN interface instead of WAN. Only 1 WAN interface can exist
3. On the ppp0 (or 2-2.1) page
    a. Set the Status as Enabled for WAN
    b. Configure the Cellular with the APN info corresponding to the info given by your operator. Here are the fields that must be configured (see screenshot below)
        i. Dial string that shall be: atd*99**<pdp context num># ex: '**atd*99**1#**'

By default <pdp context num> shall be set to 1. With Kura 5, if the pdp context digit is NOT present, the ppp setup will fail.

1. APN name as per your operator instructions
    - APN Authentication type
    - If authentication is not none (CHAP, PAP or Auto) then the username and password must be entered otherwise they needs to be left blank
    - All other fields can be left as default
    - Apply and wait a few seconds and your system is connected to the Internet via the mobile network

Routing between WiFi and LTE shall work. If any routing problem, check the DHCP & NAT tab in wlan0 page and verify at the bottom that the pass DNS Servers through DHCP is well selected and apply (in any case make apply)



Modem troubleshooting: if the connection via cellular is not coming up, more explanations and troubleshooting tips in Controlling and accessing the modem and GPS .

SIM Format

Here are the format supported by the gateway models

N6 Indoor: Standard SIM 2FF (25x15mm)

N6 Outdoor: Standard SIM 2FF (25x15mm)

N6 Industrial: Micro SIM 3FF (15x12mm)

N8 Compact: Micro SIM 3FF (15x12mm)

Gateway connection to Kapua

Kapua is providing several resources from the Cloud to supervise the gateways and collect the information via MQTT (https://www.eclipse.org/kapua/)

SolidRun is providing an instance for its customer to help the rapid setup of their systems and applications: http://kapua.solidsense.io:8080/ Or better using https (available since January 2020): https://kapua.solidsense.io

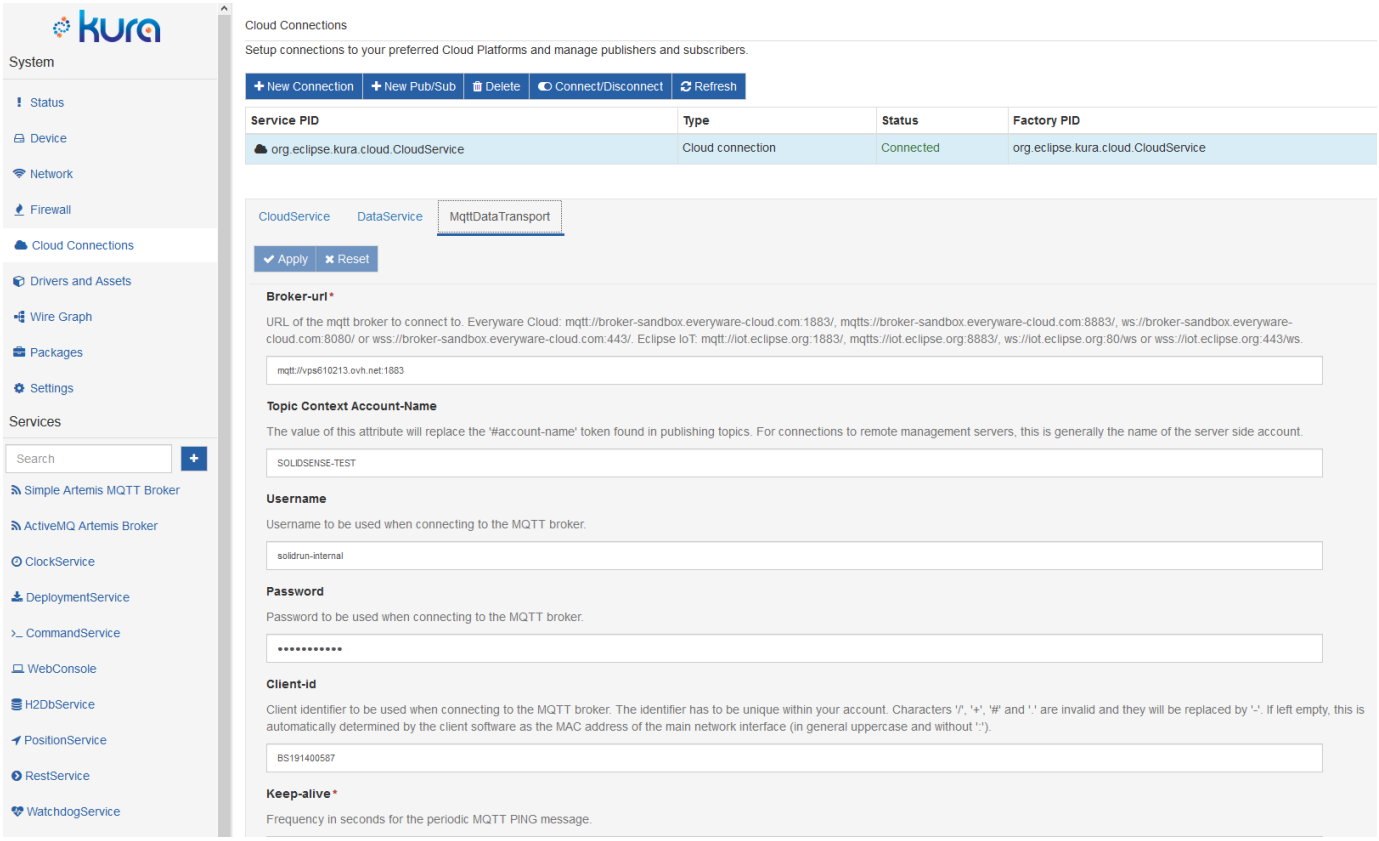
Contact your SolidRun representative to obtain your account and credentials for the gateways and users into Kapua. (SolidSense Support Overview **)**

More on the usage of Kapua

Please Note

The Kapua instance referred by the URL above is provided by SolidRun as a convenience during early test and development phases. It cannot be used for production. No warranty for availability of the service is provided by SolidRun for these services

The configuration of the connectivity is realized using the Cloud Service/MQTT Data Transport page



3 fields needs to be updated with the credentials sent by SolidRun:

Account: This the name your account shared by all the gateways and users

Username: This is the username for the gateway connections

Password: associated password

Another set of credentials is given for the direct user access to Kapua.

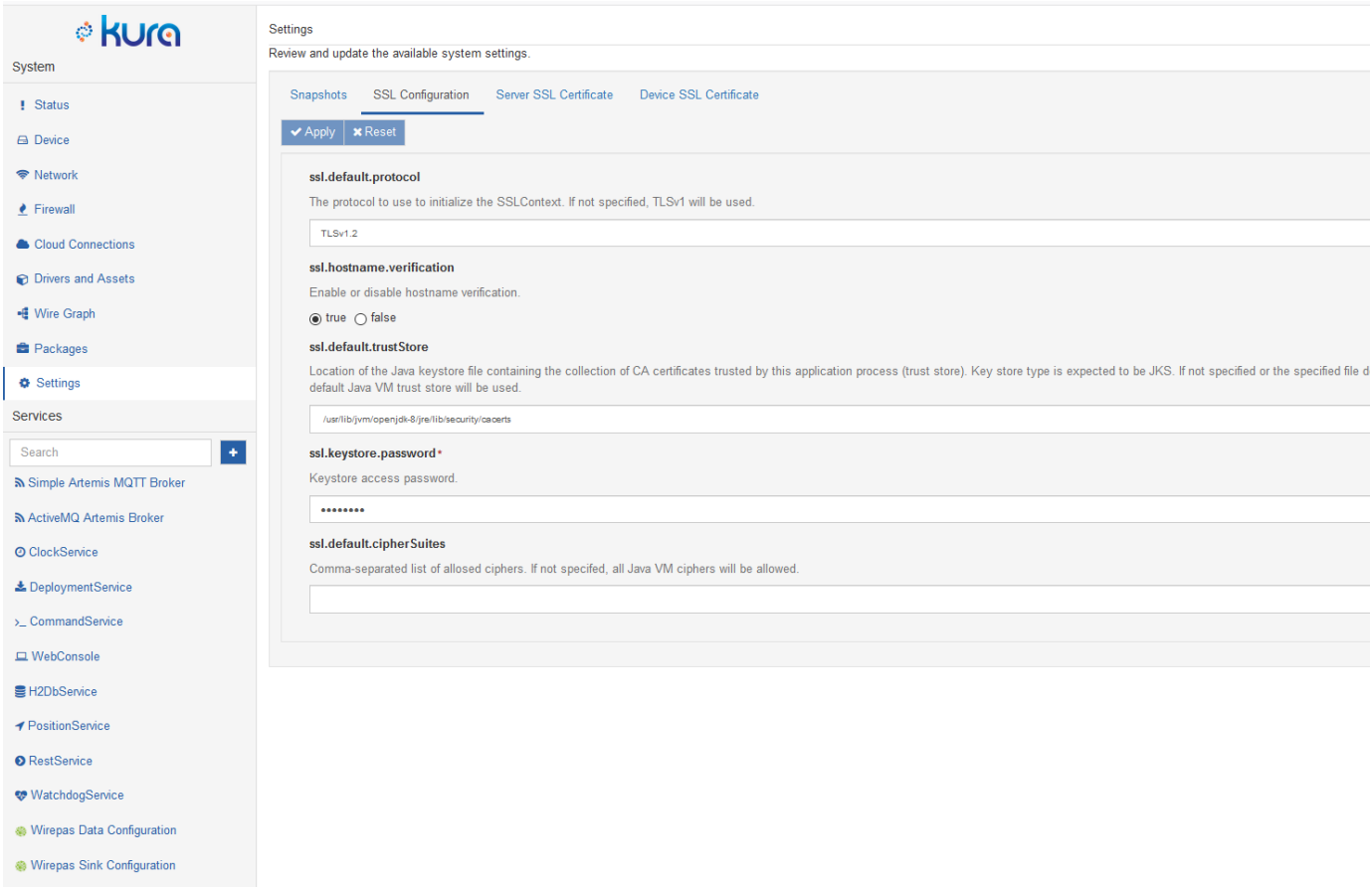
SSL connection between the gateway (Kura) and Kapua

For increased security, we recommend to have the MQTT connection between Kura and Kapua encrypted over SSL The SolidSense managed Kapua is able to handle secure communications. For customer hosted Kapua this shall be configured.

Step1 Configure the SSL manager

set ssl.default.trustStore to `/usr/lib/jvm/openjdk-8/jre/lib/security/cacerts`

set ssl.keystore.password to `changeit`



Step 2: re-configuring the MQTT Data Transport

The broker URL needs to be updated to: mqtts://kapua.solidsense.io:8883

SSH access

To perform specific configuration steps or troubleshooting you can gain ssh access to the gateway.

Please contact SolidRun customer support for the credentials.