

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 screenshot displays the Kura system's status page. The left sidebar contains navigation menus for 'System' and 'Services'. The 'System' menu includes Status, Device, Network, Firewall, Cloud Connections, Drivers and Assets, Wire Graph, Packages, and Settings. The 'Services' menu includes a search bar and several service entries: Simple Artemis MQTT Broker, ActiveMQ Artemis Broker, ClockService, DeploymentService, CommandService, WebConsole, H2DbService, PositionService, RestService, WatchdogService, and Wirepas Data Configuration. The main content area shows the 'Status' page with a 'Refresh' button and a table of system settings.

| Status | |
|--------------------------|--|
| Refresh | |
| Cloud Services | |
| Connection Name | org.eclipse.kura.cloud.CloudService |
| Account | SOLIDSENSE-TEST |
| Broker URL | tcp://vps610213.ovh.net:1883 |
| Client ID | BS191400585 |
| Service Status | CONNECTED |
| Username | solidrun-internal |
| Cellular Settings | |
| 2-1.2 | Disabled |
| Ethernet Settings | |
| eth0 | 192.168.1.51 Subnet Mask: 255.255.255.0 Mode: WAN IP Acquisition: DHCP Router Mode: |
| Wireless Settings | |
| wlan0 | 172.16.1.1 Subnet Mask: 255.255.255.0 Mode: LAN IP Acquisition: Manual Router Mode: DHCP & NAT Wireless Mode: Access Point SSID: BS181300110 |
| Position Status | |
| Longitude | 0.0 |
| Latitude | 0.0 |
| Altitude | 0.0 m |

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

System

- Status
- Device
- Network**
- Firewall
- Cloud Connections
- Drivers and Assets
- Wire Graph
- Packages
- Settings

Services

Search +

- Simple Artemis MQTT Broker
- ActiveMQ Artemis Broker
- ClockService
- DeploymentService
- CommandService
- WebConsole
- H2DbService
- PositionService
- RestService
- WatchdogService
- Wirepas Data Configuration

Network

Select a Network Interface and configure it. DHCP Server and NAT can be configured only for interfaces enabled for LAN usage. When applying your changes, your connection to the gateway on your network configuration changes.

Interface Name

- lo
- eth0**
- wlan0
- 2-1.2

Apply **Refresh**

TCP/IP DHCP & NAT Hardware

Status

Enabled for WAN

Configure

Using DHCP

IP Address

192.168.1.51

Subnet Mask

255.255.255.0

Gateway

192.168.1.1

Renew DHCP Lease

DNS Servers

192.168.1.1

Information

Mouse over enabled items on the left to see help text.

Copyright © 2011-2019 Eurotech and others. EPL v1.0 KURA_4.0.0

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

kura

System

- Status
- Device
- Network
- Firewall
- Cloud Connections
- Drivers and Assets
- Wire Graph
- Packages
- Settings

Services

Search +

- Simple Artemis MQTT Broker
- ActiveMQ Artemis Broker
- ClockService
- DeploymentService
- CommandService
- WebConsole
- H2DbService
- PositionService
- RestService
- WatchdogService

Network

Select a Network Interface and configure it. DHCP Server and NAT can be configured only for interfaces enabled for LAN usage. When applying your changes, your connection to the gateway on your network configuration changes.

Interface Name

- lo
- eth0
- wlan0
- 2-1-2

Apply Refresh

TCP/IP Wireless DHCP & NAT Hardware

Status

Enabled for LAN

Configure

Manually

IP Address

172.16.1.1

Subnet Mask

255.255.255.0

Gateway

Renew DHCP Lease

DNS Servers

Information
Mouse over enabled items on the left to see help text.

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.

System

- Status
- Device
- Network
- Firewall
- Cloud Connections
- Drivers and Assets
- Wire Graph
- Packages
- Settings

Services

Search +

- Simple Artemis MQTT Broker
- ActiveMQ Artemis Broker
- ClockService
- DeploymentService
- CommandService

Network

Select a Network Interface and configure it. DHCP Server and NAT can be configured only for interfaces enabled for LAN usage. W on your network configuration changes.

Interface Name

- lo
- eth0
- wlan0
- 2-1.2

Apply **Refresh**

TCP/IP Wireless **DHCP & NAT** Hardware

Router Mode

DHCP and NAT

DHCP Beginning Address

172.16.1.100

DHCP Ending Address

172.16.1.110

DHCP Subnet Mask

255.255.255.0

DHCP Default Lease Time (s)

7200

DHCP Max Lease Time (s)

7200

Pass DNS Servers through DHCP

true false

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)

The screenshot shows the Kura Network configuration page. On the left, a sidebar lists system components like Status, Device, Network (selected), Firewall, Cloud Connections, Drivers and Assets, Wire Graph, Packages, Settings, and Services. The main content area is titled 'Network' and includes a note: 'Select a Network Interface and configure it. DHCP Server and NAT can be configured only for interfaces enabled for LAN usage. When applying your changes, your connection to the gateway may be'. Below this, there's a table of interface names: lo, eth0, wlan0, ppp0 (highlighted), and docker0. To the right, the configuration for 'ppp0' is shown, with tabs for TCP/IP, Cellular (selected), GPS, and Hardware. The configuration includes:

- Buttons: Apply, Refresh
- Model: Android-EC25
- Network Technology: LTE (dropdown)
- Connection Type: PPP
- Modem Identifier: Android
- Interface #: 0
- Dial String*: at*99**#
- APN*: orange
- Auth Type: Auto (dropdown)
- Username: orange
- Password: masked with asterisks
- Modem Reset Timeout*: 5
- Reopen connection on termination: true false
- Connection Attempts*: 5

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.solidrun.io:8080/> Or better using https (available since January 2020): <https://kapua.solidrun.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

The screenshot shows the Kura web interface. On the left is a navigation sidebar with sections for System (Status, Device, Network, Firewall), Cloud Connections (highlighted), Drivers and Assets, Wire Graph, Packages, Settings, and Services (with a search bar and a list of services like Simple Artemis MQTT Broker, ActiveMQ Artemis Broker, etc.). The main content area is titled 'Cloud Connections' and contains a table of existing connections. Below the table are tabs for 'CloudService', 'DataService', and 'MqttDataTransport' (which is selected). Under the 'MqttDataTransport' tab, there are several configuration fields: 'Broker-uri*' (with a help text and a text input containing 'mqtt://vps610213.ovh.net:1883'), 'Topic Context Account-Name' (with a help text and a text input containing 'SOLIDSENSE-TEST'), 'Username' (with a help text and a text input containing 'solidrun-internal'), 'Password' (with a help text and a masked text input), 'Client-id' (with a help text and a text input containing 'BS191400587'), and 'Keep-alive*' (with a help text).

| Service PID | Type | Status | Factory PID |
|-------------------------------------|------------------|-----------|-------------------------------------|
| org.eclipse.kura.cloud.CloudService | Cloud connection | Connected | org.eclipse.kura.cloud.CloudService |

Broker-uri*
URL of the mqtt broker to connect to. Everyware Cloud: mqtt://broker-sandbox.everyware-cloud.com:1883/, mqtt://broker-sandbox.everyware-cloud.com:8883/, ws://broker-sandbox.everyware-cloud.com:8080/ or wss://broker-sandbox.everyware-cloud.com:443/; Eclipse IoT: mqtt://iot.eclipse.org:1883/, mqtt://iot.eclipse.org:8883/, ws://iot.eclipse.org:80/ws or wss://iot.eclipse.org:443/ws.
mqtt://vps610213.ovh.net:1883

Topic Context Account-Name
The value of this attribute will replace the '#account-name' token found in publishing topics. For connections to remote management servers, this is generally the name of the server side account.
SOLIDSENSE-TEST

Username
Username to be used when connecting to the MQTT broker.
solidrun-internal

Password
Password to be used when connecting to the MQTT broker.

Client-id
Client identifier to be used when connecting to the MQTT broker. The identifier has to be unique within your account. Characters '/', '+', '#' and '.' are invalid and they will be replaced by '_'. If left empty, this is automatically determined by the client software as the MAC address of the main network interface (in general uppercase and without ':').
BS191400587

Keep-alive*
Frequency in seconds for the periodic MQTT PING message.

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
```

The screenshot shows the Kura Settings interface. On the left is a navigation menu with 'System' and 'Services' sections. The 'System' section includes Status, Device, Network, Firewall, Cloud Connections, Drivers and Assets, Wire Graph, and Packages. The 'Services' section includes a search bar and a list of services: Simple Artemis MQTT Broker, ActiveMQ Artemis Broker, ClockService, DeploymentService, CommandService, WebConsole, H2DbService, PositionService, RestService, WatchdogService, Wirepas Data Configuration, and Wirepas Sink Configuration. The main content area is titled 'Settings' and contains the 'SSL Configuration' tab. Below the tab are 'Apply' and 'Reset' buttons. The configuration items are:

- ssl.default.protocol**: The protocol to use to initialize the SSLContext. If not specified, TLSv1 will be used. Value: TLSv1.2
- ssl.hostname.verification**: Enable or disable hostname verification. Radio buttons for true (selected) and false.
- ssl.default.trustStore**: Location of the Java keystore file containing the collection of CA certificates trusted by this application process (trust store). Key store type is expected to be JKS. If not specified or the specified file does not exist, the default Java VM trust store will be used. Value: /usr/lib/jvm/openjdk-8/jre/lib/security/cacerts
- ssl.keystore.password**: Keystore access password. Value: *****
- ssl.default.cipherSuites**: Comma-separated list of allowed ciphers. If not specified, all Java VM ciphers will be allowed. Value: (empty)

Step 2: re-configuring the MQTT Data Transport

The broker URL needs to be updated to: `mqttps://kapua.solid sense.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.