



nodeG5 Edge MQTT Gateway

Supporting



Deploy edge or FOG compute with an IIoT gateway that supports python, docker & services like AWS Sitewise & TensorFlow to manage CAN Bus J1939/OBD2, OPC UA, Serial RS485 Modbus TCP/RTU, WiFi & BLE data.

EDITION / November 2024 /
FIRMWARE VERSION 2.2

DESIGNED IN AUSTRALIA.
ASSEMBLED IN SINGAPORE.

REAL TIME DATA MODE

The addition of a Real Time data mode allow users to handle instantaneous status updates more effectively instead of queuing & storing data in a SQL buffer.

JSON CONFIGURATION FOR IOTASSET

We have changed the configuration of the iotasset set up from a .txt file to a .json format to improve flexibility & efficiency.

SAFETY OF USE 3

SECTION 1: ABOUT

nodeG5 Specifications 4
Hardware 5
Board Interface 6

SECTION 2: SETTING UP

SIM Installation 7
Logging In 8

SECTION 3: CONFIGURATIONS

Quickstart Guide 9
WAN & Cellular Settings 10
Dynamic DNS 11
Ethernet Settings 12
Wireless Settings 13
Serial & CAN Settings 14
IoT Hardware 16
IoT Client 18
IoT Data 20
Management 21
System Status 24

CONTACT US 25

SAFETY OF USE



ALL CONDITIONS

All specialist electronic devices must be operated with due care to avoid damage or injuries and should be installed and operated by a trained personnel.

DO NOT OPERATE THIS EQUIPMENT IN ENVIRONMENTS CONTAINING POTENTIALLY EXPLOSIVE GASES OR LIQUIDS, EXAMPLE, GAS STATIONS AND CHEMICAL PLANTS AND EXPLOSIVE STORES.

POWER SETUP

Inadequate current or dips in voltage may cause the device to fail to connect to data services even if the LEDs are lighted up. Supply over 30 VDC will damage the device.

SIM CARD

Never remove or insert SIM card when device has PWR switched in "ON" position. Damage caused to device or SIM in such case will not be warranted.

CONFIGURING THE ROUTER

Do not reboot/power-down the device until the writing process is acknowledged as completed.

ABOUT

1. 1 nodeG5 SPECIFICATIONS

CPU CORE

| | |
|------------------------|------------------------------------------------------------|
| CPU | NXP i.MX8M Plus QuadLite, quad-core ARM Cortex-A53, 1.8GHz |
| NPU | AI/ML Neural Processing Unit, up to 2.3 TOPS |
| REAL TIME CO-PROCESSOR | ARM Cortex-M7, 800Mhz |

STORAGE & MEMORY

| | |
|---------|------------------------------------|
| RAM | 2GB LPDDR4 |
| Storage | 32GB eMMC flash, soldered on-board |

NETWORK

| | |
|-----------|---------------------------------------------------------------|
| LAN | 2x 1000Mbps Ethernet ports, RJ45 |
| WIFI* | 802.11ax WiFi |
| BLE* | Bluetooth 5.3 BLE |
| CELLULAR* | 4G/LTE CAT4 cellular module, Quectel EC25-E/A (EU & US bands) |
| GNSS* | GPS |

I/O

| | |
|---------------|----------------------------------------------------------------|
| USB | 2x USB2.0, 1x USB3.0 type-A connectors |
| RS485/ RS232* | Up to 2x RS485 (half-duplex) |
| CAN BUS* | Up to 2x CAN bus port |
| Digital I/O | Optional 4IN + 4OUT digital I/O |
| Debug | 1x serial console via UART-to-USB bridge, micro-USB connector. |

MANAGEMENT

| | |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NETWORK ROBUSTNESS | <ul style="list-style-type: none">· Designed for maximum uptime from available network· NetMgr WWAN connect timeouts· End-to-End PING connectivity testing with reboot |
| NETWORKING | <ul style="list-style-type: none">· Dynamic DNS |
| CLOUD MANAGEMENT | <ul style="list-style-type: none">· Azure IoT Hub· AWS IoT Core / Sitewise Client· Ubidots Client· MQTT Client with TLS Security· On-board Real Time Clock |
| INTEGRATED DATA FEATURES | <ul style="list-style-type: none">· Real Time Data Mode· FIFO Data Mode |
| REMOTE MANAGEMENT | <ul style="list-style-type: none">· SSH for Remote LINUX Management |

USER CUSTOM PROGRAMMING

- Run Python (2.7.15 & 3.6.5)/ LUA/ BASH scripting
- Run containers on Debian Linux

WARRANTY

- 5 year manufacturer warranty

* denotes features that may be model specific

ABOUT

1.2 HARDWARE

PHYSICAL SPECIFICATIONS

| | |
|-----------|-------|
| DIMENSION | |
| - L | 132mm |
| - W | 84mm |
| - H | 25mm |
| WEIGHT | 550g |

POWER

- 8 to 26 VDC

PERIPHERALS INCLUDED

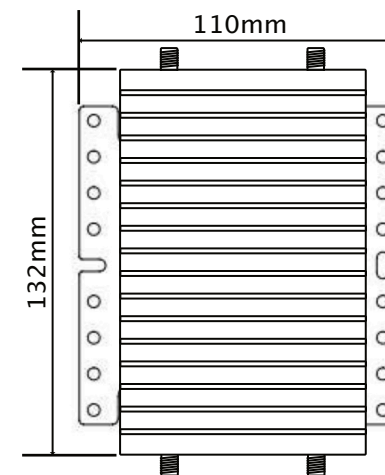
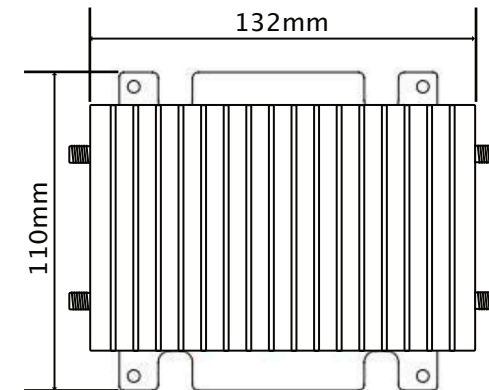
- Cellular rubber duck antenna with SMA connector
- CAT-5 LAN cable (3M)

OPTIONAL ACCESSORIES

- High-gain outdoor antenna (wall mounted)
- High-gain outdoor antenna (pole mounted)
- 2x 2.4GHz / 5GHz WiFi BLE Antennas
- 2x11-pin dual-row mating plug for industrial I/O

With the nodeG5 you have the option to install it using a mounting plate onto different surfaces.

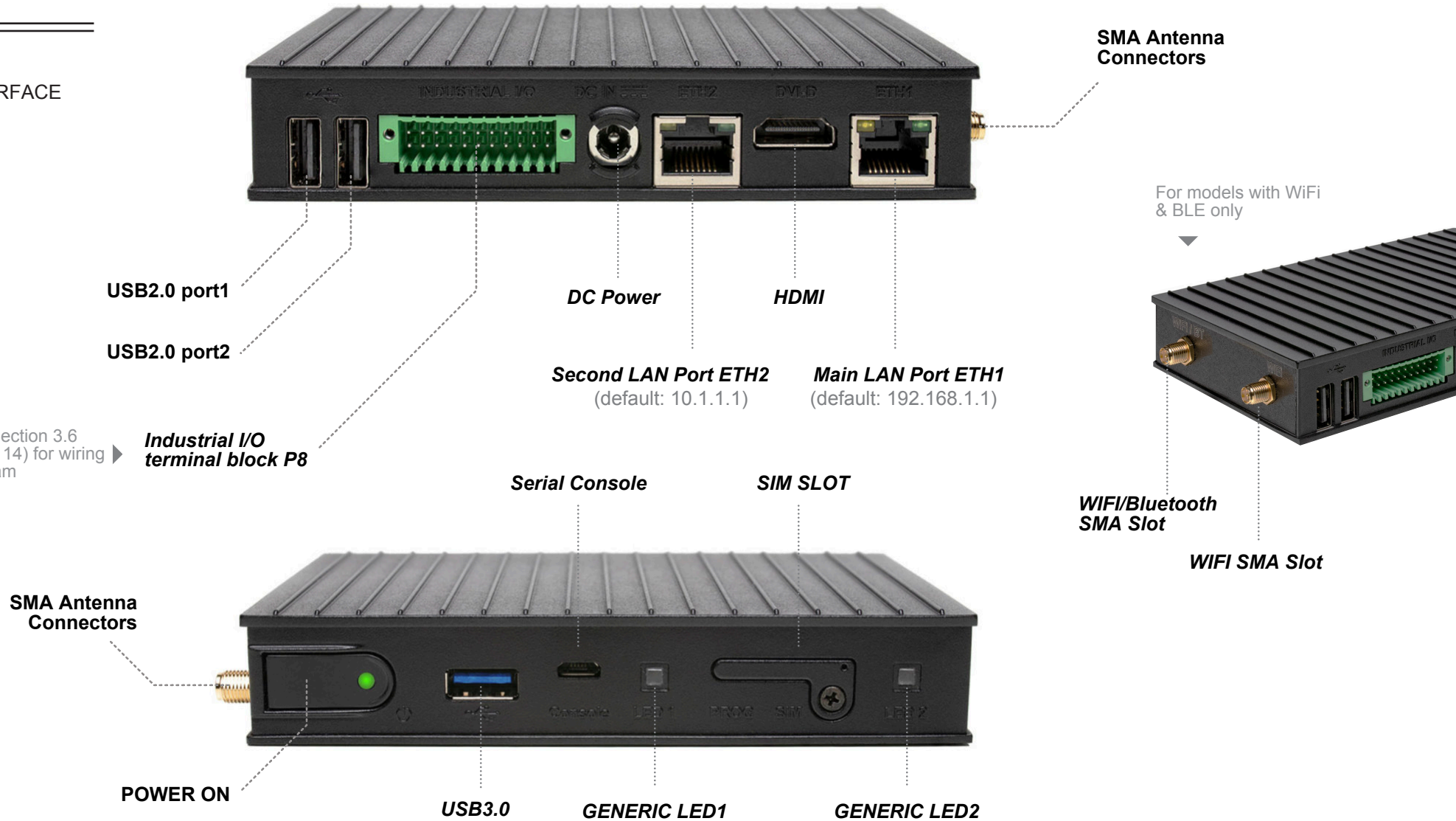
The orientation and dimensions are as below:



ABOUT

1.3 BOARD INTERFACE

See Section 3.6 (page 14) for wiring diagram



SETTING UP

2. 1 SIM INSTALLATION

INSERTING THE SIM CARD

STEP 1 of 5 - Unscrew the SIM cover and insert the micro SIM card into the slot.

WHAT YOU'LL NEED

1. 4G Data Enabled micro SIM Card
2. PC/Laptop with an Ethernet port
3. SIM card network details – APN/USERNAME/PASSWORD. You would need to get this information from your operator.



STEP 2 of 5 - Screw the cover back on and connect up the power adapter and the cellular antenna

SETTING UP

2. 2

LOGGING IN

When you have connected up the hardware to the box, the web console can be accessed at the address

192.168.1.1

For Security, after your first successful log in, you will be prompted to change your username & password.

Note: If you are using a SSH console:

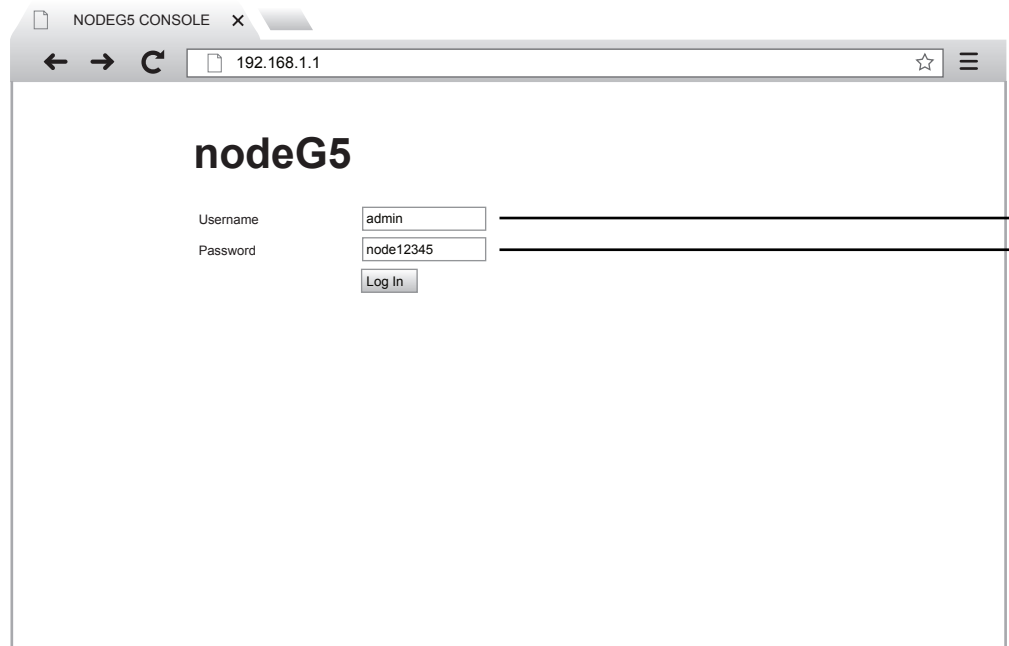
The login username is:
root

The default password remains as:
node12345

STEP 3 of 5 - Plug in the Ethernet cable from ETH1 to your pc and power up the nodeG5.

STEP 4 of 5 - Launch your browser and enter address as 192.168.1.1

STEP 5 of 5 - Log in.



The default username is:
admin

The default password is:
node12345

CONFIGURATION

nodeG5

3. 1 QUICK START

The Quick Start tab brings together all the settings you need to establish an immediate cellular connection in one page.

MENU OPTIONS Basic settings for nodeG5 Gateway for Cellular Internet Access

- Quick Start
- Cellular WAN**
- Dynamic DNS
- Ethernet
- Wireless
- Serial / CAN

[G5 Quick Start Guide.pdf](#)

- IoT Hardware
- IoT Client
- IoT Data

LAN (eth1) Port Settings

- LAN IP Address

 /

Cellular SIM Settings

APN

Dial Number

User Name (PAP/CHAP only)

Password (PAP/CHAP only)

SIM PIN Code (If required only)

You can find resource PDF links in our web config to help guide you through the different setups.

Key in the IP Address for your nodeG5 gateway here.

To connect the nodeG5 to a cellular network the following information is required. You will be able to get them from your internet service provider.

Click on UPDATE to save your settings.

Password Management

Current Password

New Password

Reconfirm New Password

For security, please ensure you change to a new password.

nodeG5

MENU OPTIONS **WAN & Cellular Settings**

- Quick Start
- Cellular WAN**
- Dynamic DNS
- Ethernet
- Wireless
- Serial / CAN

- IoT Hardware
- IoT Client
- IoT Data

- Management
- System Status
- Logout

Primary WAN Interface

Select your primary WAN interface from the options given. (Note that Wi-Fi is model dependent & you will need to complete the rest of your the settings in 'Wireless' tab.)

Cellular SIM Settings

APN

Dial Number

User Name (PAP/CHAP only)

Password (PAP/CHAP only)

SIM PIN Code (If required only)

Service

Assigned DNS

NetMgr WWAN Connect Timeout

To connect the nodeG5 to a cellular network the following information is required. You will be able to get them from your internet service provider.

If you will like to override your network assigned DNS, you can input your own address here. Otherwise leave it blank.

Set the amount of minutes before the system does a reboot (0 = never)

Advanced Settings

Enable Reboot on PING failure

To ensure reliable connectivity you can choose to PING an external IP address.

PING Remote Host

Add in a test IP address (i.e. Google at 8.8.8.8 T)

PING Interval

PING retries

Input the PING interval & number of retries made before the system reboots.

When you have completed your settings on this page, click 'Update' to save them.

CONFIGURATION

nodeG5

3. 3 DYNAMIC DNS

The Dynamic DNS feature helps to keep a standard domain name pointed to the nodeG5 even if it is assigned IP changes during a reboot/reconnection.

WHAT YOU'LL NEED

1. A data sim card with a public IP [You can check this with your operator.]
2. An account with a dynamic DNS service provider like dyndns2, easydns or changeip

MENU OPTIONS

- Quick Start
- Cellular WAN
- Dynamic DNS**
- Ethernet
- Wireless
- Serial / CAN

- IoT Hardware
- IoT Client
- IoT Data

- Management
- System Status
- Logout

Dynamic DNS Settings

- Enable DDNS Client
- Service Name [\[list\]](#)
- Device Hostname URL
- Username
- Password

ENABLED ▾

dyndns2

nodeg5.dyndns.org

your_username

UPDATE TEST

Enable or Disable the DYNDNS service.

Enter in the DYNDNS service you have registered with.

Enter in the FQDN (fully qualified domain name) of your host at DDNS provider.

Key in your DYNDNS Service Username & Password.

Click 'Update' to save your settings. The nodeG5 will connect to your account and point the domain after you reboot.

In the above example, you will be able to access your nodeG5 using the domain name "nodeG5.dyndns.org" on any regular browser.

Our new TEST feature allows you to quickly & easily verify that your dynamic domain assignment is working.

nodeG5

3. 4 ETHERNET SETTINGS

MENU OPTIONS

- Quick Start
- Cellular WAN
- Dynamic DNS
- Ethernet**
- Wireless
- Serial / CAN

- IoT Hardware
- IoT Client
- IoT Data

- Management
- System Status
- Logout

Ethernet Settings

| | |
|-----------------------|------------------------------------------------------------------------------|
| eth1 (LAN) IP Address | <input type="text" value="192.168.1.1"/> / <input type="text" value="24"/> |
| DHCP Enable | <input type="button" value="Cellular"/> |
| DHCP Start | <input type="text" value="10"/> e.g. xxx.xxx.xxx Start |
| DHCP Limit | <input type="text" value="10"/> Limit no. of IPs to assign |
| eth0 (WAN) IP Address | <input type="text" value="192.168.8.200"/> / <input type="text" value="24"/> |
| eth0 Gateway | <input type="text" value="192.168.8.254"/> |

Set up the IP Address of your LAN port.

Enable the nodeG5 to automatically assign IP addresses to your connected LAN devices.

This would be the starting address for connected devices. For the example here, the first connected device will be assigned the address of 192.168.1.10

This will limit the number of connected devices. For this example the last connected device will be assigned 192.168.1.20

Sets up the IP Address of your WAN port.

Sets up the IP Address of the nodeG5 gateway.

Once you have completed your settings click to save.

3. 5
WIRELESS
SETTINGS

nodeG5

MENU OPTIONS **Wireless Settings**

- Quick Start
- Cellular WAN
- Dynamic DNS
- Ethernet
- Wireless**
- Serial / CAN

- IoT Hardware
- IoT Client
- IoT Data

- Management
- System Status
- Logout

Wireless Mode

Settings for 'Infrastructure Mode' : connects to your wi-fi router for internet access

SSID

Security Type

Password

IP Address

 /

Router IP

Settings for 'Access Point Mode' : connection point for your wi-fi enabled devices

SSID

Security Type

Password

IP Address for AP mode

 /

Select to enable (Note that Wi-Fi is model dependent.)

Key in the SSID of your wi-fi router.

Input the security settings to connect to your router.

Key in the IP address for your nodeG5, or leave this blank to let it be assigned via DHCP.

Create a SSID for your nodeG5 access point.

Input the security settings to authenticate a connection with devices.

Key in the IP address for your nodeG5 as access point.

When you have completed your settings on this page, click 'Update' to save them.

CONFIGURATION

The industrial I/O signals are routed to terminal block P8. Pin-out is determined by the I/O modules configuration below:

3.6 SERIAL & CAN SETTINGS



Note: for RS485 2-wire, half-duplex cables are required.

| | |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Serial (RTU) Port A | <ul style="list-style-type: none"> · PIN 1 (RS485_POS) · PIN 3 (RS495_NEG) · PIN 5 (ISO_GND_1) |
| Serial (RTU) Port B | <ul style="list-style-type: none"> · PIN 7 (RS485_POS) · PIN 6 (RS495_NEG) · PIN 8 (ISO_GND_2) |
| CAN Port C | <ul style="list-style-type: none"> · PIN 12 (CAN_H) · PIN 14 (CAN_L) · PIN 21 (ISO_GND_3) |
| CAN Port E | <ul style="list-style-type: none"> · PIN 4 (CAN_H) · PIN 2 (CAN_L) · PIN 5 (ISO_GND_1) |

Connector Type:

22-pin dual-row plug with spring connections

Locking: screw flange

Pitch: 2.54mm

Wire cross-section: AWG20-AWG30

INDUSTRIAL I/O

| I/O module | Pin | Signal Name | Isolation Power Domain |
|------------|-----|-------------------------------|------------------------|
| A | 1 | RS232_TXD / RS485_POS | 1 |
| - | 2 | CAN_L | 1 |
| A | 3 | RS232_RXD / RS485_NEG | 1 |
| - | 4 | CAN_H | 1 |
| A | 5 | ISO_GND_1 | 1 |
| B | 6 | RS232_RXD / RS485_NEG | 2 |
| B | 7 | RS232_TXD / RS485_POS | 2 |
| B | 8 | ISO_GND_2 | 2 |
| D | 9 | IN0 | 3 |
| D | 10 | IN1 | 3 |
| D | 11 | IN2 | 3 |
| C | 12 | RS232_TXD / RS485_POS / CAN H | 3 |
| D | 13 | IN3 | 3 |
| C | 14 | RS232_RXD / RS485_NEG / CAN_L | 3 |
| D | 15 | OUT0 | 3 |
| D | 16 | OUT1 | 3 |
| D | 17 | OUT3 | 3 |
| D | 18 | OUT2 | 3 |
| D | 19 | 24V_IN | 3 |
| D | 20 | 24V_IN | 3 |
| C/D | 21 | ISO_GND_3 | 3 |
| C/D | 22 | ISO_GND_3 | 3 |

nodeG5

3.6 SERIAL & CAN SETTINGS

MENU OPTIONS

- Quick Start
- Cellular WAN
- Dynamic DNS
- Ethernet
- Wireless
- Serial / CAN**
- IoT Hardware
- IoT Client
- IoT Data
- Management
- System Status
- Logout

Serial / CAN Settings

Serial Port A Parameters

Speed E.g. 9600, 19200, 38400, 57600, 115200

Data Bits E.g. 7, 8

Parity

Stop Bits

Serial Port B Parameters

Speed E.g. 9600, 19200, 38400, 57600, 115200

Data Bits E.g. 7, 8

Parity

Stop Bits

Match the settings with your attached serial devices to the respective port (see wiring diagram on the previous page).

CAN Port Parameter

CAN Port C Baudrate (On-board) E.g. 50000, 100000, 125000, 250000, 500000, 1000000

CAN Port E Baudrate (FCCAN)

Match the settings with your attached CAN devices to the respective port (see wiring diagram on the previous page).

Click on 'Update' to save your settings.

nodeG5

3.7 IOT HARDWARE

| MENU OPTIONS | IOT Hardware Setup | |
|---------------------|------------------------------------------|---------------------------------------------------------------------------------|
| Quick Start | Modbus mode [modbus.pdf] | <input type="text" value="Enabled"/> |
| Cellular WAN | CAN bus mode [OBD2.pdf] | <input type="text" value="Disabled"/> OBD/C2Q: Query mode C2R: Read Mode |
| Dynamic DNS | COMeth mode [COMeth.pdf] | <input type="text" value="Disabled"/> ZBR: Query mode ZBQ: Read Mode |
| Ethernet | Event Drop Type | <input type="text" value="Disabled"/> |
| Wireless | Poll Period | <input type="text" value="15"/> secs |
| Serial / CAN | Poll Time Out | <input type="text" value="5"/> secs |
| IoT Hardware | Query Pause | <input type="text" value="0.1"/> secs (pause between query required for Modbus) |
| IoT Client | Time Stamp Offset | <input type="text" value="0"/> eg +8 or -6.5 (offset from UTC+0) |
| IoT Data | Bluetooth Radio | <input type="text" value="OFF"/> |
| Management | <input type="button" value="UPDATE"/> | |
| System Status | | |
| Logout | | |

Click to enable Modbus mode

Choose 'Query mode' to send request packet & read response values. Choose 'Read mode' when slaves auto report their status/values. J1939 users will also need to choose that CAN bus option here.

ComETH BOT supports query and reading of on-board digital input.

Select the time interval of reading data events of the iotasset listing. If you wish, have a different polling period for different assets, refer to our web FAQ to set your iotasset.txt configuration.

The timeout specifies the time period to accept responses after each network request. Ensure adequate spacing that takes into account network traffic and latency.

If you require a pause between separate poll queries, set it here.

Set your local timezone for event timestamp.

Enable the Bluetooth option here. Note that this feature is model dependant.

Update and reboot the nodeG5

nodeG5

3.7 IOT HARDWARE

MENU OPTIONS IOT Hardware Setup

- Quick Start
- Cellular WAN
- Dynamic DNS
- Ethernet
- Wireless
- Serial / CAN

IoT Hardware

- IoT Client
- IoT Data

- Management
- System Status
- Logout

DATA SNAPSHOT :: [Show Data](#) DELETE DATA Warning : Will delete all user sensor data

Check File :: [Check iotasset.txt](#) **UPLOAD IOTASSET.JSON FILE**

Show a snapshot of the current data

DELETE ALL JSON DATA

Ensure that the gateway HTTPS console must be accessible before proceeding with these steps.

1. Click on the 'UPDATE IOTASSET.JSON FILE' button.
2. In the new window, click on 'CHOOSE FILE' & select the updated file from your local folder.
3. Click 'UPLOAD FILE'
4. Close the page & log in again for security purposes.

If the update failed, check that the connection to the gateway is stable. Or else please contact support@amplified.com.au

Click to see the current configurations file in a new web page.

IMPORTANT ::

Please upload the following settings via the **Management tab**.

- **iotasset.json** with hardware device settings (e.g Modbus addresses)
- **connstr.txt** with Azure settings (e.g. Azure IoT device id token)

nodeG5

3.8
IOT CLIENT

MENU OPTIONS

- Quick Start
- Cellular WAN
- Dynamic DNS
- Ethernet
- Wireless
- Serial / CAN

- IoT Hardware
- IoT Client**
- IoT Data

- Management
- System Status
- Logout

IOT Client Setup

Client Setup :: Azure IoT

nodeG5 Azure IoT Quick Start Guide [web pdf](#)

Device ID

Client Type

Provisioning Host

ID Scope

SAS Private Key

Enable Client

Enter the Device ID you use to set up your Microsoft Azure IoT Account.

Select if you are connecting to Azure IoT Hub or IoT Central.

Enter the endpoint/host for sending the data. By default this is set to 'global.azure-devices-provisioning.net'

Enter in the ID scope assigned to your Azure device provisioning service.

Enter the SAS private key that is generated using your device connection string.

Select to Enable the Azure IoT Client

Client Setup :: AWS IoT

nodeG5 AWS IoT Quick Start Guide [web pdf](#)

Thing Name

Topic

AWS Endpoint

AWS Port

Enable Client

Enter the Thing Name, Topic, Endpoint & AWS Port as per the settings in your AWS account

Select to Enable the AWS IoT Client

nodeG5

3.8
IOT CLIENT

MENU OPTIONS

- Quick Start
- Cellular WAN
- Dynamic DNS
- Ethernet
- Wireless
- Serial / CAN

- IoT Hardware
- IoT Client**
- IoT Data

- Management
- System Status
- Logout

IOT Client Setup

Client Setup :: Ubidots

nodeG5 ubidots IoT Quick Start Guide [web pdf](#)

Device Token

Device Name

Enable Client

Enter the Device Token & Name as per the settings in your Ubidots account

Select to Enable the Ubidots IoT Client

Client Setup :: MQTT

nodeG5 MQTT IoT Quick Start Guide [web pdf](#)

Broker Host

Message Topic

Host Port

Username for port 1883

Password for port 1883

Enable Client

Enter the MQTT Broker IP that you want to connect to

And your Topic as per the settings in your Broker/ to describe your data set

And the Broker Port details as per the settings in your MQTT Broker

Enable the nodeG5 as a MQTT IoT Gateway

CONFIGURATION

3.9 IOT DATA

The industrial I/O signals are routed to terminal block P8. Pin-out is determined by the I/O modules configuration below:

Client Setup :: Ubidots

nodeG5 ubidots IoT Quick Start Guide [web pdf](#)

Device Token

Device Name

Enable Client

Enter the Device Token & Name as per the settings in your Ubidots account

Select to Enable the Ubidots IoT Client

Client Setup :: MQTT

nodeG5 MQTT IoT Quick Start Guide [web pdf](#)

Broker Host

Message Topic

Host Port

Username for port 1883

Password for port 1883

Enable Client

Enter the MQTT Broker IP that you want to connect to

And your Topic as per the settings in your Broker/ to describe your data set

And the Broker Port details as per the settings in your MQTT Broker

Enable the nodeG5 as a MQTT IoT Gateway

CONFIGURATION

3. 10 MANAGEMENT

Note that from the internet, the nodeG5 can only be accessed via HTTPS (secure) to ensure all data between user and nodeG5 web configuration page is encrypted.

We give our clients the choice to install their own signed certificate (e.g. Veri-sign or Digicert) via SSH to nodeG5 console. Since there is no packaged signed SSL certificate in each nodeG5, a complaint of error might be issued from the browser. Note that this does not affect the secure encryption of data to configure the nodeG5 via HTTPS.

nodeG5

MENU OPTIONS System Management

Quick Start
Cellular WAN
Dynamic DNS
Ethernet
Wireless
Serial / CAN

IoT Hardware
IoT Client
IoT Data

Management
System Status
Logout

Web Login Username
Enable https access from WAN
Enable Secure Shell (SSH)
Enable System Log
System Time reference
System Time reference

Set Up RTC (hardware clock)

Password Management

Current Password
New Password
Reconfirm New Password

admin

Enabled

Enabled

Disabled

Disabled

ntp

UPDATE

Set RTC using current system time

Change Password

This login name is only used for web. If you are using SSH, always log in as 'root'.

Click to enable remote https access via WAN port 443. Note that non secure https access via WAN is not allowed.

Disabled by default. If enabled it will provide root access using the default login details on page

If enabled you can download/view the log page from the 'System status page.

Choose a system time source reference as ntp (online time service) or rtc (on-board battery back hardware clock).

Click to update hardware clock using the current time system

For security, please do not use default password for your deployed unit.

Passwords are never stored directly but as a hash string to increase device security.

nodeG5

3. 10 MANAGEMENT

MENU OPTIONS System Management

- Quick Start
- Cellular WAN
- Dynamic DNS
- Ethernet
- Wireless
- Serial / CAN

- IoT Hardware
- IoT Client
- IoT Data

- Management**
- System Status
- Logout

Configuration Parameters Management

Please insert usb drive labelled 'nodeG5'.
Configuration file (config.db) backup & restore

Download config.db from nodeG5

Upload config.db to nodeG5

User Configuration and Scripts Management

Please insert usb drive labelled 'nodeG5'.
Files (e.g. iotasset.json, firewall.user, user.lua, user.py or connstr.txt) must be in the /user folder.

Download /user to nodeG5

Execute user.lua Script [nodeG5 Lua.pdf]

Delete User files

Execute user.py Script [nodeG5 Python.pdf]

To allow 'cloning' of parameter settings to multiple nodeG5 in deployment we utilise USB flash drives.

1. Format a USB thumb-drive (e.g. NODE32) and label it 'nodeG5'
2. After the nodeG5 is powered up insert the thumb-drive into an available USB port.
3. Click 'Download config.db from nodeG5', wait 5 seconds & remove thumb-drive
4. Insert the thumb-drive into new nodeG5 and click 'Upload config.db to nodeG5', wait 5 seconds and remove thumb-drive
5. Check in new nodeG5 that parameters from other nodeG5 has been copied over

To input your own LUA or Python program:

1. Write your LUA or Python program and name it as 'user.lua' or 'user.py'
2. Save the program in /user folder in your thumb-drive (drive labelled 'nodeG5')
3. Insert the thumb-drive into your nodeG5
4. Click 'Download /user to nodeG5', wait 5 seconds and remove the thumb-drive
5. You can click 'Execute Program' to test your program

Your program will automatically be executed after complete boot-up of the nodeG5.

nodeG5

MENU OPTIONS System Management

Quick Start
Cellular WAN
Dynamic DNS
Ethernet
Wireless
Serial / CAN

IoT Hardware
IoT Client
IoT Data

Management
System Status
Logout

Firmware Management

Update Firmware Patch [Patch Guide.pdf]

System Recovery Management

Factory Settings

Reboot System

Ensure that the gateway HTTPS console must be accessible before proceeding with this steps.

1. Click on the 'UPDATE FIRMWARE' button.
2. In the new window, click on 'CHOOSE FILE' and select from your local folder the specific firmware update .zip file. (Please check with support@amplified.com.au for any assistance).
3. Click 'UPLOAD FIRMWARE PATCH'. If the firmware has been successful you will get the following message:

"RESULT: The firmware update has been applied"

4. After closing the page, you will need to log in again for security purposes.

If the update failed, check that the connection to the gateway is stable. Or else please contact support@amplified.com.au

Click 'Reboot' to soft reset the nodeG5 device.

Click 'Factory Settings' to revert all parameters to factory default.

nodeG5

3. 11 SYSTEM STATUS

| | | |
|----------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| MENU OPTIONS | System Status | |
| Quick Start | Main | |
| Cellular WAN | | |
| Dynamic DNS | Firmware Version | 5.15.32+gb917e043c529 |
| Ethernet | System Date & Time | Thur Aug 10 02:41:16 UTC 2023 |
| Wireless | Upload and CPU Load (1,5,15m) | 02:41:16 up 16 min, 1 user, load average: 0.25, 0.22, 0.13 |
| Serial / CAN | Temperature | 39 * C |
| <hr/> | | |
| IoT Hardware | | |
| IoT Client | | |
| IoT Data | Cellular WAN | |
| Management | | |
| System Status | Modem firmware | EC25EUGAR06A07M4G |
| Logout | IMEI | 864303052713149 |
| | USIM IMSI | 502181121133668 |
| | USIM ICCID | 8960181171211336711 |
| | Modem State | connected |
| | Interface | wwan0 |
| | SIM APN | telstra.internet |
| | IP address | 21.173.254.22 |
| | Operator Name | U Mobile |
| | Roam Status: | home |
| | Service Mode: | lte |
| | Signal Strength: | 63% |
| | Cellular Data (since bootup) | RX packets 30 bytes 3286 (3.2 KIB) TX packets 42 bytes 3994 (3.9 KIB) |
| System Log : | System Log File | |
| Diagnostics : | <input type="button" value="Run Diagnostics"/> Diagnostics Output File | |
| Diagnostics : | <input type="button" value="Ping Test"/> | |

Run a system diagnostic test

Run a Ping test to check your connection

CONTACT US

.....
TECHNICAL
SUPPORT: SUPPORT@AMPLIFIED.COM.AU

SALES: SALES@AMPLIFIED.COM.AU

.....
WEBSITE AMPLIFIED.COM.AU

.....
ADDRESS Amplified Engineering Pty Ltd
 Unit 3, 2A Brodie Hall Drive
 Bentley WA 6102, Australia
 ABN 44127163035

