



NEXIS LX1 HARDWARE MANUAL



Contents

Version History	3
1 Initial Setup	4
1.1 Connections	4
1.2 LEDs & Buttons	5
1.3 Power.....	6
1.4 Temperature	7
1.5 Configuring	7
2. Web UI Overview	9
2.1 Home	9
2.3 Network Pages	10
Summary.....	10
Ethernet.....	11
Wi-Fi	14
Cloud.....	18
2.4 Hardware Pages	19
Summary.....	19
GNSS.....	21
Tilt Sensors	27
CAN.....	29
2.5 System Pages.....	30
Update.....	31
Recover	31
Name.....	32
Clock	33
Log	33
Tools	34
Auto Upgrade	34
2.6 Security Pages.....	34
Access	34
Firewall.....	35
NAT	39
QOS.....	41

DNS	41
DHCP	42
2.7 Routing Pages	44
Ethernet 2	44
Ethernet IP Alias	46
Static Routes	46
Client Routing	46
Mesh Routing	47
3. Compliance	48



Version History

The electronic version of this document is the approved and most current. Any printed version is uncontrolled and may not be current.

Version	Last Revision Date	Revision Owner	Changes
1	17/09/2025		

1 Initial Setup

Supporting documentation for the IV-SVC-TSG-02 Workflow

1.1 Connections

The LX1 has several connections, all located on the back panel of the device.

- **10 pin Milspec Bayonet style connector**
 1. I/O – Combines power, Ethernet, RS232 serial and two digital inputs.
- **8 pin M12 style connector**
 1. VEH – Provides CDL and Serial 2 connection.
- **5 Pin M12 connectors**
 1. CAN 1 – Primary CAN bus connection.
 2. CAN 2 – Secondary CAN bus connection.
- **8 soc M12 connectors**
 1. LAN – Provides an additional Ethernet connection and FPD link for the DS series slim screen connection.
- **Female N-Type connectors**
 1. WLAN 1 – Primary WIFI connection
 2. WLAN 2 – Secondary WIFI connection
- **Female TNC connectors**
 1. GNSS – GPS/GNSS connection
 2. LTE 1 – Primary LTE connection
 3. LTE 2 – Secondary LTE connection



1.2 LEDs & Buttons

The front panel of the LX1 has several LEDs to indicate different statuses and information.

1. Power
2. Interface
3. Network
4. Status



1.3 Power

The LX1 contains a highly-rated power supply suitable for use in most harsh industrial environments, including very large electro-magnetic fields and high temperatures.

The unit is capable of operating using an input voltage ranging from 6V DC to 38V DC.

At 24V DC, the LX1 will typically draw 160mA (~5W) during normal operation.

During startup, maximum operating currents at 24V DC is 250mA as the system initialises and tests several of the key components including the radio transmitters.

Recommended Power Supply: minimum 250mA 24V DC

The router contains several protection mechanisms designed to ensure excessive power variations do not cause any damage. These protection mechanisms include an internal 1.5 Amp fuse and an over-voltage protection circuit.

1.4 Temperature

The LX1 Nexis has been designed with an operating temperature range of -40°C to +85°C.

1.5 Configuring

When the Nexis is powered on, it will perform a series of configuration and initialisation tasks. This process can take up to one minute, during which time the Nexis configuration interface is not accessible.

Configuration of the device is done through its web interface and can be performed using any web browser. To access the configuration interface, perform the following steps.

Note: This explanation assumes the Nexis has a factory-default configured IP address of "192.168.1.254". Refer to the IP address details on the delivery documentation supplied with your Nexis for the device's IP address.

1. Ensure both the power and network connections have been correctly installed.
2. Connect the LX1 to a suitable network device – either a switch/hub using a standard (straight through) network cable, or directly to a PC.

If connecting directly to a PC, either an Ethernet cross-over adapter or a PC that supports auto-crossover must be used. If correctly installed, the attached device should detect the Ethernet link state less than 10 seconds after power is first applied to the LX1.

3. Modify (if necessary) the network properties for the PC that is to be used to configure the router, so that it uses an IP address in the range 192.168.1.1 to 192.168.1.253 inclusive, and a subnet mask of 255.255.255.0. If the IP address of the Nexis is not 192.168.1.254, an appropriate IP address for the PC should be chosen.
4. Using a web browser, navigate to this URL: <http://192.168.1.254:2000/>

At this point, the default Nexis web page (shown below) should appear, and configuration can be performed. The Configuration section below provides details of each feature that can be configured in the Nexis device. The status of various aspects can be viewed via the Information web pages (available in the upper-left column of each page, see Figure 1 below).

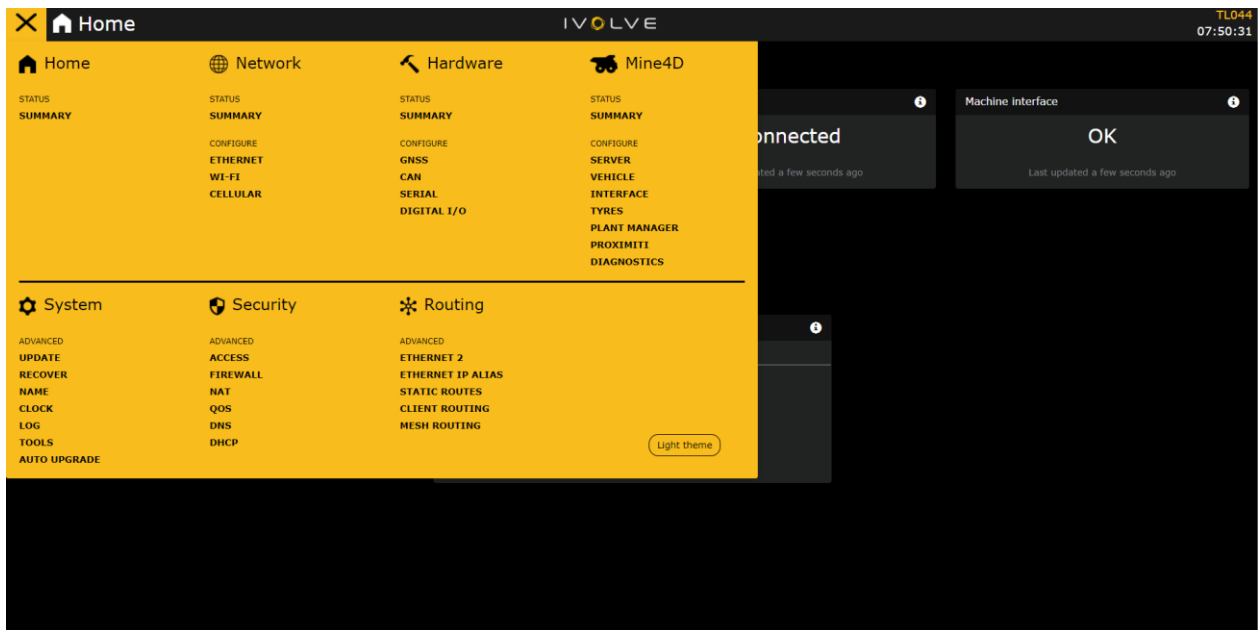
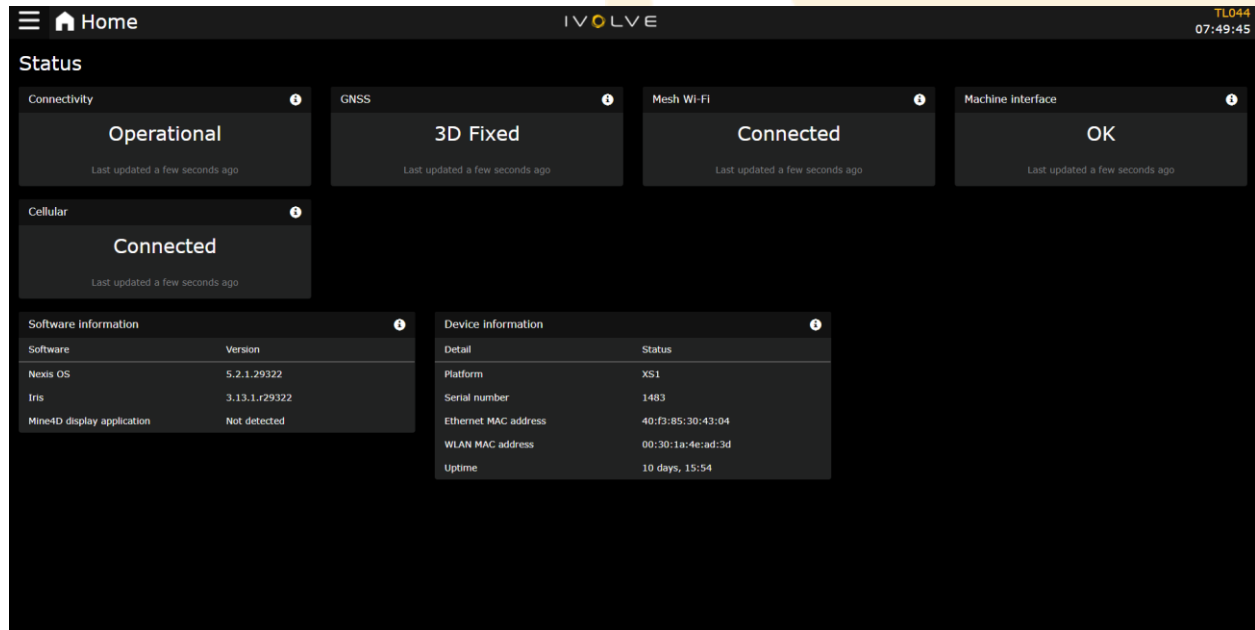


Figure 1 The upper left 'hamburger' menu, opened

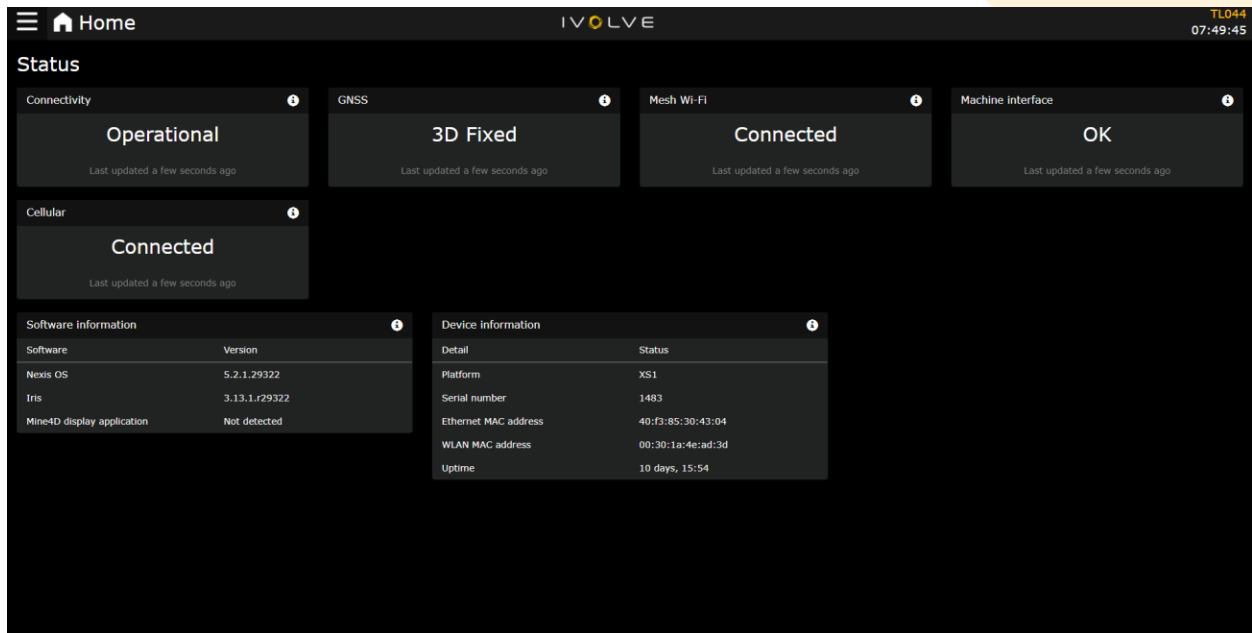
When prompted for a username and password, enter "root" as the username and "neX1s!" as the password. The Web UI section below gives more details about the pages that are of most interest.

Most pages are subdivided into various tabs, which can be accessed by clicking the tab's name. Changes are not saved unless the 'Update' button at the bottom of the page is clicked.

2. Web UI Overview

2.1 Home

The Summary web page provides details of the current firmware versions, current time, operating time, IP addresses, subnet masks and MAC addresses of the devices network interfaces, temperature, voltage and current.



The screenshot displays the iVOLVE Home web interface. The top navigation bar includes a menu icon, a home icon, the text 'Home', the iVOLVE logo, and the device identifier 'TL044' with the time '07:49:45'. The main content area is titled 'Status' and contains several status cards: 'Connectivity' (Operational), 'GNSS' (3D Fixed), 'Mesh Wi-Fi' (Connected), 'Machine interface' (OK), and 'Cellular' (Connected). Each card indicates it was 'Last updated a few seconds ago'. Below these cards are two tables: 'Software Information' and 'Device Information'.

Software	Version
Nexis OS	5.2.1.29322
Iris	3.13.1.r29322
Mine4D display application	Not detected

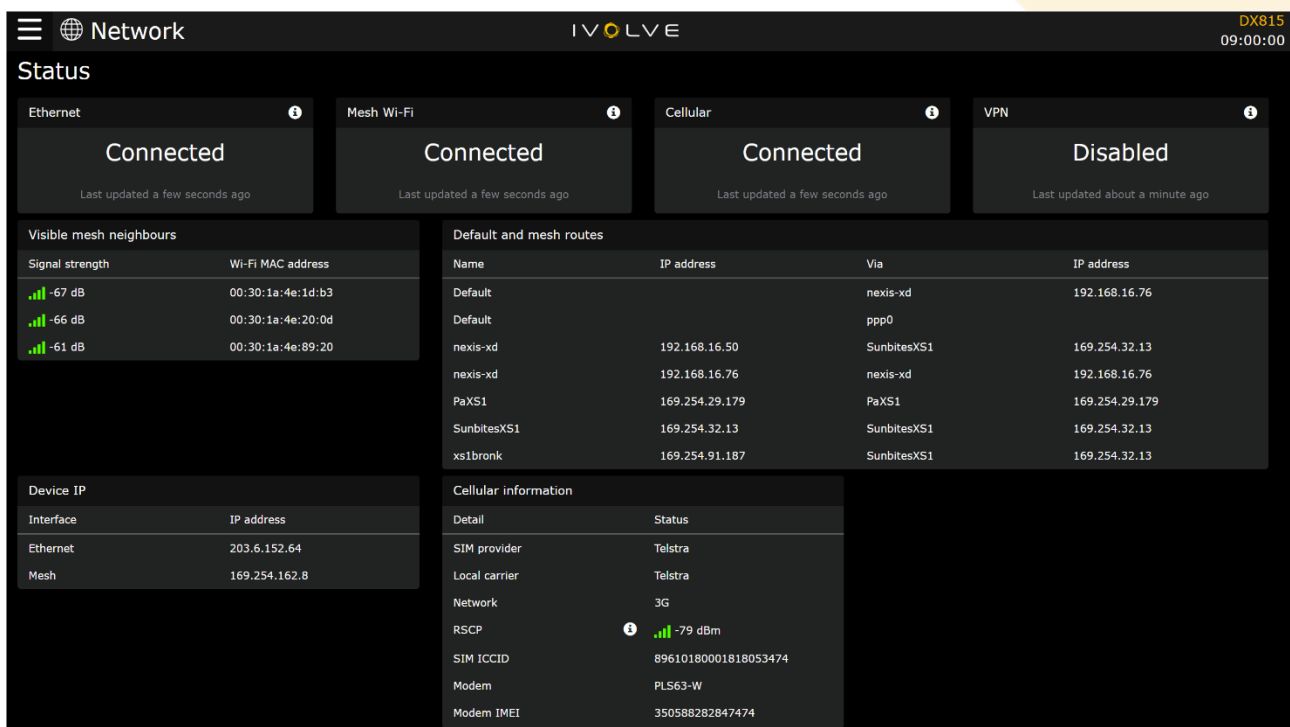
Detail	Status
Platform	XS1
Serial number	1483
Ethernet MAC address	40:f3:85:30:43:04
WLAN MAC address	00:30:1a:4e:ad:3d
Uptime	10 days, 15:54

2.3 Network Pages

The Network group of pages contains the configuration pages for the Ethernet, Mesh Wi-Fi and (if an LTE device) cloud, previously called cellular.

Summary

The summary page provides an overview of the status of the network connections, current mesh neighbours and routes, device IP addresses and cellular connection information.



The screenshot shows the 'Network' status page in the iVOLVE interface. The top bar indicates 'Network' and 'iVOLVE' with a user 'DX815' and time '09:00:00'. The main content is divided into several sections:

- Status:** Four cards showing connection status: Ethernet (Connected), Mesh Wi-Fi (Connected), Cellular (Connected), and VPN (Disabled). Each card has a timestamp indicating when it was last updated.
- Visible mesh neighbours:** A table with two columns: Signal strength and Wi-Fi MAC address. It lists three neighbours with signal strengths of -67 dB, -66 dB, and -61 dB.
- Default and mesh routes:** A table with four columns: Name, IP address, Via, and IP address. It lists routes for Default, nexis-xd, PaXS1, SunbitesXS1, and xs1brnck.
- Device IP:** A table with two columns: Interface and IP address. It shows the IP addresses for Ethernet (203.6.152.64) and Mesh (169.254.162.8).
- Cellular information:** A table with two columns: Detail and Status. It shows details for SIM provider (Telstra), Local carrier (Telstra), Network (3G), RSCP (-79 dBm), SIM ICCID (89610180001818053474), Modem (PLS63-W), and Modem IMEI (350588282847474).

Cellular information

The Cellular information card shows the status of the cellular network on the Nexis. This card is only displayed on iVolve's cellular platforms, the XS1D, XD8, and LX1.

SIM provider

The home provider of the SIM card. This field is always displayed for an XD8 screen and is only displayed for supported SIM cards for XS1D devices. If no SIM card is inserted, this field will display "SIM not detected".

Local carrier

Which service provider is providing internet access.

Network

Your device's mobile network (either 3G or 4G).

Your Network affects what is displayed in the following fields. If your device is on 3G, the RSCP field is displayed. If your device is on 4G, the RSRP and RSRQ fields are displayed instead.

- **RSRP (Reference Signal Received Power)**
The strength of your 4G signal in dBm; a higher value indicates a stronger signal.
(This field is 4G exclusive.)
- **RSRQ (Reference Signal Received Quality)**
The quality of the signal your device receives in dB; a lower value indicates potential noise or interference. (This field is 4G exclusive.)
- **RSCP (Received Signal Code Power)**
The strength of your 3G signal in dBm; a higher value indicates a stronger signal.
(This field is 3G exclusive.)

SIM ICCID

The unique identifier for your device's SIM card. If no SIM card is inserted, this field will display "SIM not detected".

Modem

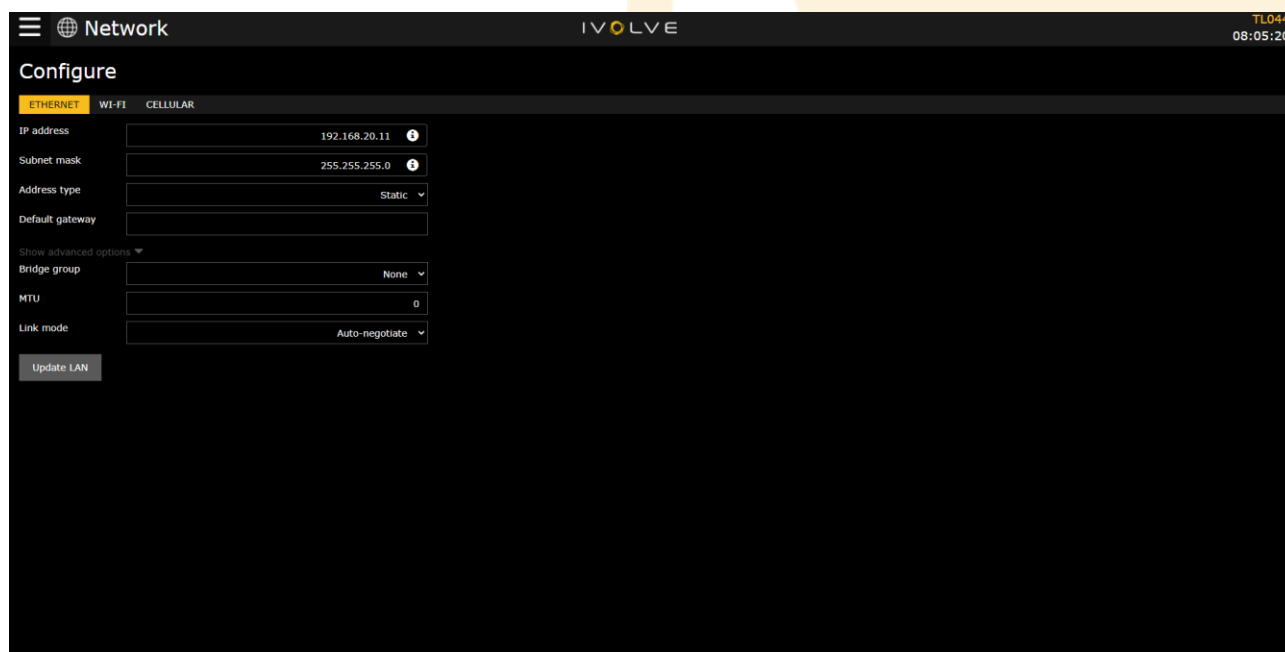
Your device's modem model.

Modem IMEI (International Mobile Equipment Identity)

The unique identifier for your device's modem.

Ethernet

The ethernet page contains configurations for the ethernet interface.



The screenshot shows the 'Configure' page for the Network section. The 'ETHERNET' tab is selected. The settings are as follows:

- IP address: 192.168.20.11
- Subnet mask: 255.255.255.0
- Address type: Static
- Default gateway: (blank)
- Bridge group: None
- MTU: 0
- Link mode: Auto-negotiate

There is an 'Update LAN' button at the bottom left of the configuration area.

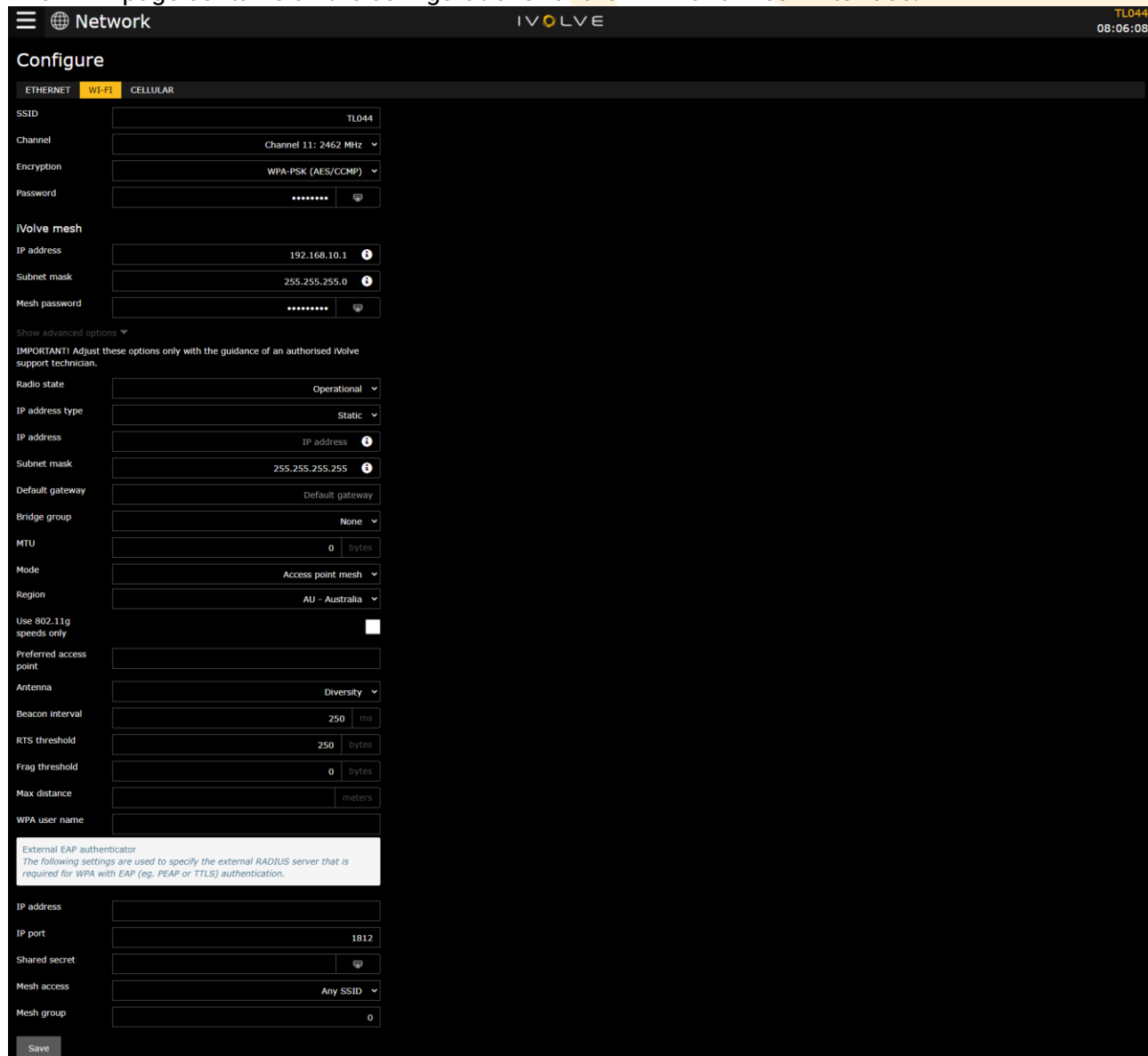
Setting	Options	Default value	Description
IP address	Any valid IP address	192.168.1.254	The IP address of the primary Ethernet (LAN) interface.
Subnet mask	Any valid subnet mask	255.255.255.0	The subnet mask to use to define the available IP addresses in the network.
Address type	Static, DHCP	Static	Whether the IP address is static or assigned using DHCP.
Default gateway	Any valid IP address.	Blank	Which address to route LAN traffic through to. For backbone devices this points toward the server but only needs to be set up on one backbone device as it broadcasts this to others.
Bridge group	0,1,2,3,4, None	None	Set the network interface bridge group. Mesh units should be set to zero and backbone devices should be set to None.
MTU	N/A	0	

Link mode	Auto-negotiate 10 Mbps half-duplex 10 Mbps full-duplex 100 Mbps half-duplex 100 Mbps full-duplex	Auto-negotiate	The mode by which the ethernet links.
-----------	--	----------------	---------------------------------------



Wi-Fi

The Wi-Fi page contains all the configurations for the Wi-Fi and mesh interface.



Network iVOLVE TL044 08:06:08

Configure

ETHERNET **WI-FI** CELLULAR

SSID: TL044

Channel: Channel 11: 2462 MHz

Encryption: WPA-PSK (AES/CCMP)

Password: *****

iVolve mesh

IP address: 192.168.10.1

Subnet mask: 255.255.255.0

Mesh password: *****

Show advanced options ▼

IMPORTANT! Adjust these options only with the guidance of an authorised iVolve support technician.

Radio state: Operational

IP address type: Static

IP address: IP address

Subnet mask: 255.255.255.255

Default gateway: Default gateway

Bridge group: None

MTU: 0 bytes

Mode: Access point mesh

Region: AU - Australia

Use 802.11g speeds only: ☐

Preferred access point:

Antenna: Diversity

Beacon interval: 250 ms

RTS threshold: 250 bytes

Frag threshold: 0 bytes

Max distance: meters

WPA user name:

External EAP authenticator
The following settings are used to specify the external RADIUS server that is required for WPA with EAP (eg. PEAP or TTLS) authentication.

IP address:

IP port: 1812

Shared secret: *****

Mesh access: Any SSID

Mesh group: 0

Save

Setting	Options	Default value	Description
SSID	Text	Nexis, or device serial e.g. LX10012	This is the 'Service Set Identifier' for the wireless interface.

Setting	Options	Default value	Description
Channel	N/A	Channel 1: 2412 MHz	N/A
Encryption	N/A	WPA-PSK (AES/CCMP)	The Wi-Fi encryption algorithm used for Wi-Fi client connections, such as to a laptop or phone. The encryption type is automatically detected by modern client devices.
Password	N/A	N/A	The password used for Wi-Fi client connections, such as to a laptop or phone.

iVolve mesh settings

Setting	Options	Default value	Description
IP address	N/A	N/A	The IP address used by the Nexis for iVolve mesh communication.
Subnet mask	N/A	255.255.255.0	The address used by the subnet mask.
Mesh password	N/A	N/A	The password used for wireless communication between Nexis mesh nodes. A Nexis will not mesh wirelessly with another Nexis if the Mesh password is different on the two devices.
Radio state	N/A	Operational	The current state of the radio.
IP address type	N/A	Static	N/A

Advanced settings

Setting	Options	Default value	Description
Radio state	N/A	Operational	N/A
IP address type	N/A	Static	N/A
IP address	N/A	N/A	N/A
Subnet mask	N/A	255.255.255.255	N/A
Default gateway	N/A	N/A	N/A
Bridge group	N/A	None	N/A
MTU	N/A	0	N/A
Mode	N/A	Access point mesh	N/A
Region	N/A	AU - Australia	N/A
Use 802.11g speeds only	Checked, Unchecked	N/A	N/A
Preferred access point	N/A	N/A	N/A
Antenna	N/A	Primary	N/A
Beacon interval	ms	100	N/A
RTS threshold	bytes	0	N/A
Frag threshold	bytes	250	N/A
Max distance	meters	N/A	N/A

Setting	Options	Default value	Description
WPA user name	N/A	N/A	N/A

External EAP authenticator

The following settings are used to specify the external RADIUS server that is required for WPA with EAP (eg. PEAP or TTLS) authentication.

Setting	Options	Default value	Description
IP address	N/A	N/A	N/A
IP port	N/A	1812	N/A
Shared secret	N/A	N/A	N/A
Mesh access	N/A	Any SSID	N/A
Mesh group	N/A	0	N/A

Cloud

Network

IVOLVE XD8

nexis-xd
12:00:00

Configure

ETHERNETWI-FICLOUD

Cloud

Enable cloud logging

Download cloud logs

Cellular

Enable cellular data

Virtual private network (VPN)

Enable VPN

VPN server

monitor.fleet4d.net

Restart OpenVPN

Save

Show advanced options

VPN certificate

Installed file: xd8-2004-5342

Choose fileNo file chosen

Upload

Version: 3

Thumbprint (SHA-256):

7145a95e3a08ffb3478de2a4d6d55

Not before: Aug 30 07:39:20 2020 GMT

Not after: Aug 30 07:39:20 2025 GMT

VPN key

Key valid for installed certificate!

Choose fileNo file chosen

Upload

Cellular connection details

APN auto configuration

Mobile country code

auto

Mobile network code

auto

Save

Network usage monitoring

Run interval (minutes)

30

File prune interval (hours)

168

Save network monitoring

Usage alert rules

Interface	Transmit rate	Receive rate
Add new usage alert rule:		
Interface	br0	
Transmit rate alert threshold	bytes per sec	
Receive rate alert threshold	bytes per sec	
Add		

2.4 Hardware Pages

The hardware section contains the configuration options for GNSS and corrections, tilt sensors, CAN, Serial and digital I/O.

Summary

The Summary page provides tabs for an overview of the status of the Primary and Secondary (if applicable) GNSS, satellites seen and used, signal strengths, sky plot, tracking information and fix status. It also has a tab for the corrections status.

Hardware

EX1700

13:17:09

Status

Primary GNSS

Secondary GNSS

Corrections

Primary GNSS

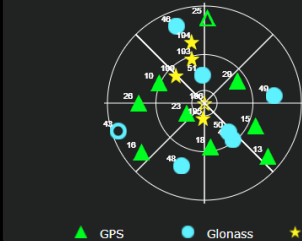
Fixed

Last updated a few seconds ago

Primary receiver

Description	Status
Last received	< 1s ago
Fix type	Fixed
Latitude	-23.28052743
Longitude	148.8768987
Horizontal RMS	0.012 m
Altitude	169.115 m
Vertical RMS	0.018 m
Speed	0 m/s
Track	334.4 deg (locked)
Track variance	3.3 deg
PDOP	1.4
GDOP	1.6
TDOP	0.8
HDOP	0.7
VDOP	1.1
Used/Total satellites	18 / 21
Receiver model	BX10
Serial number	Q1RYHE5D4AS
Software version	4.8 Apr,10,2020
Hardware version	210

Primary receiver skyplot



Primary receiver satellites

USI	System	Elevation	Azimuth	Used	Signal Strength
10	GPS	44	294	yes	46
13	GPS	13	130	yes	37
15	GPS	38	114	yes	45
16	GPS	16	232	yes	39
18	GPS	49	172	yes	45
23	GPS	71	240	yes	46
25	GPS	11	2	no	39
26	GPS	29	270	yes	43
29	GPS	53	56	yes	47
42	GLONASS47	142	yes	50	
43	GLONASS6	252	no	40	
46	GLONASS14	340	yes	46	
48	GLONASS28	200	yes	36	
49	GLONASS25	84	yes	48	
50	GLONASS55	140	yes	51	
51	GLONASS64	356	yes	51	
193	QZSS	47	344	yes	43
194	QZSS	32	348	yes	42
195	QZSS	76	186	yes	47
196	QZSS	90	510	no	44
199	QZSS	53	314	yes	40

Metric

US

Hardware

IVOLVE

appl-team
11:25:06

Status

Primary GNSS

Secondary GNSS

Corrections

RTK

Active

Last updated a few seconds ago

UHF radio

Description	Status
State	Online
Model	Satel EASy
RTK byte count	403909488
Last UHF radio bytes received	< 1s ago
Last UHF radio reset attempted	17.8d ago

RTK corrections

Description	Status
Link	Connected
Status	Active
Protocol	RTCM3
Quality	100 %
Bad messages	27 / 3698419
Last RTK bytes received	< 1s ago



GNSS

This page contains the configuration options for the GNSS and corrections.

☰

Hardware

IVOLVE

nexis-x0
02:58:57

Configure

GNSS

TILT SENSORS

CAN

Server status

Running

HPGPS type

Internal

GNSS settings

Elevation mask angle

10

Corrections

Protocol

RTCM v3.x

RTK base type

Auto

RTK extrapolation time

30

Corrections source

UHF radio

UHF radio via

Internal

UHF compatibility mode

paccrest-4fsk

UHF channel width (kHz)

12.5

UHF channel (MHz)

463.8125

Offsets (in metres)

X

Y

Z

Primary

Reportable offset

Pitch

Roll

Heading

Machine (deg)

Update

GNSS settings

Setting	Options	Default value	Description
Elevation mask angle	Number	10	Satellites lower than the given elevation are excluded from the computation. Satellites that appear near the horizon (at low angles) are subject to signal fade. They also pick up more atmospheric noise than satellites orbiting higher above the horizon.

Corrections

Setting	Options	Default value	Description
Protocol	RTCM v2.x RTCM v3.x Trimble CMR/CMR+ Topcon TPS	RTCM v2.x	Select the corrections protocol to use.
RTK base type	Auto Topcon Sokkia Trimble Leica Septentrio Novatel Ashtech Magellan Other	Auto	Select the RTK base type.
RTK extrapolation time	Number (seconds)	30	Select the extrapolation time.
Corrections source	UHF radio	UHF radio	Select which source to use for corrections.

Setting	Options	Default value	Description
	TCP UDP		Different options are available for each type of correction source.

Corrections source: Internal UHF radio

Setting	Options	Default value	Description
UHF radio via	Internal	N/A	The UHF radio is internal to the Nexis.
UHF compatibility mode	satellite-3as paccrest-4fsk paccrest-gmsk trimtalk-450sp trimtalk-450st paccrest-fst	satellite-3as	The compatibility mode of the UHF radio.
UHF channel width	12.5 kHz 20 kHz 25 kHz	12.5	The channel width used by the UHF radio.
UHF channel	330-473 MHz	463.8125	The channel used by the UHF radio.

Corrections source: External UHF radio

Setting	Options	Default value	Description
UHF radio via	External/RS232	N/A	The UHF radio is external and connected using RS232.
Baud rate	4800 9600 19200 38400 57600 115200 230400	N/A	The baud rate used to connect to the UHF radio.
UHF compatibility mode	satellite-3as paccrest-4fsk paccrest-gmsk trimtalk-450sp trimtalk-450st paccrest-fst	satellite-3as	The compatibility mode of the UHF radio.
UHF channel width	12.5 kHz 20 kHz 25 kHz	12.5	The channel width used by the UHF radio.
UHF channel	330-473 MHz	463.8125	The channel used by the UHF radio.

Corrections source: TCP UHF radio

Setting	Options	Default value	Description
UHF radio via	TCP	None	The UHF radio is external and connected over TCP. For example, over a serial device server.
Source	Hostname or IP address	None	The hostname or IP address of the TCP server used to connect to the UHF radio. If a hostname is used, the Nexis must be able to resolve the hostname using DNS.
Port	Number	None	The port number of the TCP server used to connect to the UHF radio.
UHF compatibility mode	satellite-3as paccrest-4fsk paccrest-gmsk trimtalk-450sp trimtalk-450st paccrest-fst	satellite-3as	The compatibility mode of the UHF radio.
UHF channel width	12.5 kHz 20 kHz 25 kHz	12.5	The channel width used by the UHF radio.
UHF channel	330-473 MHz	463.8125	The channel used by the UHF radio.

Corrections source: TCP

Setting	Options	Default value	Description
Source	Hostname or IP address	None	The hostname or IP address of the TCP server used to connect to the UHF radio. If a hostname is used, the Nexis must be able to resolve the hostname using DNS.
Port	Number	None	The port number of the TCP server used to connect to the UHF radio.

Corrections source: UDP

Setting	Options	Default value	Description
Listening port	Port number	None	The UDP port number the Nexis uses to listen for corrections.

Offsets

Setting	Options	Default value	Description
Primary	Directional distance in Front, Right, Above (metres) (Negative for Back, Left, Below)	N/A	Specify X, Y, and Z Offsets (in meters): Define the antenna's position relative to the machine model's reference point using X (forward/back), Y (left/right), and Z (up/down) offsets. - This setting is optional. If machine models are not used, offsets can reference any arbitrary point. - Setting all offsets to zero places the reference point at the antenna's location.
Reportable location	Directional distance in Front, Right, Above (metres)	N/A	Specify X, Y, and Z Offsets (in meters): Configure the machine's reported GPS location relative to its reference point using X (forward/back), Y (left/right), and Z (up/down) offsets. If all primary offsets are set to zero, the reported location matches the antenna's actual position.

Setting	Options	Default value	Description
	(Negative for Back, Left, Below)		For example, if the antenna is mounted at the front-left of a vehicle, set the offset to -1.0 m (forward) and 0.5 m (right) to report the GPS location from the vehicle's centre.
Machine	Number (degrees)	N/A	Specify your Pitch, Roll, and Heading in degrees.

Tilt Sensors

This page contains configuration options for installed tilt sensors, their ID numbers, orientation filter, and associated CAN interfaces.

Hardware

Configure

GNSS

TILT SENSORS

CAN

Body sensor

Sensor ID

39

Orientation

Left Of Vehicle, Arrow Front

Filter(HZ)

1

Boom sensor

Sensor ID

Orientation

Top Of Vehicle, Arrow Front

Filter(HZ)

None

Stick sensor

Sensor ID

Orientation

Top Of Vehicle, Arrow Front

Filter(HZ)

None

Bucket sensor

Sensor ID

Orientation

Top Of Vehicle, Arrow Front

Filter(HZ)

None

show advanced options

CAN Interface:

CAN0

Update

Sensor Options (Body, Boom, Stick, Bucket)

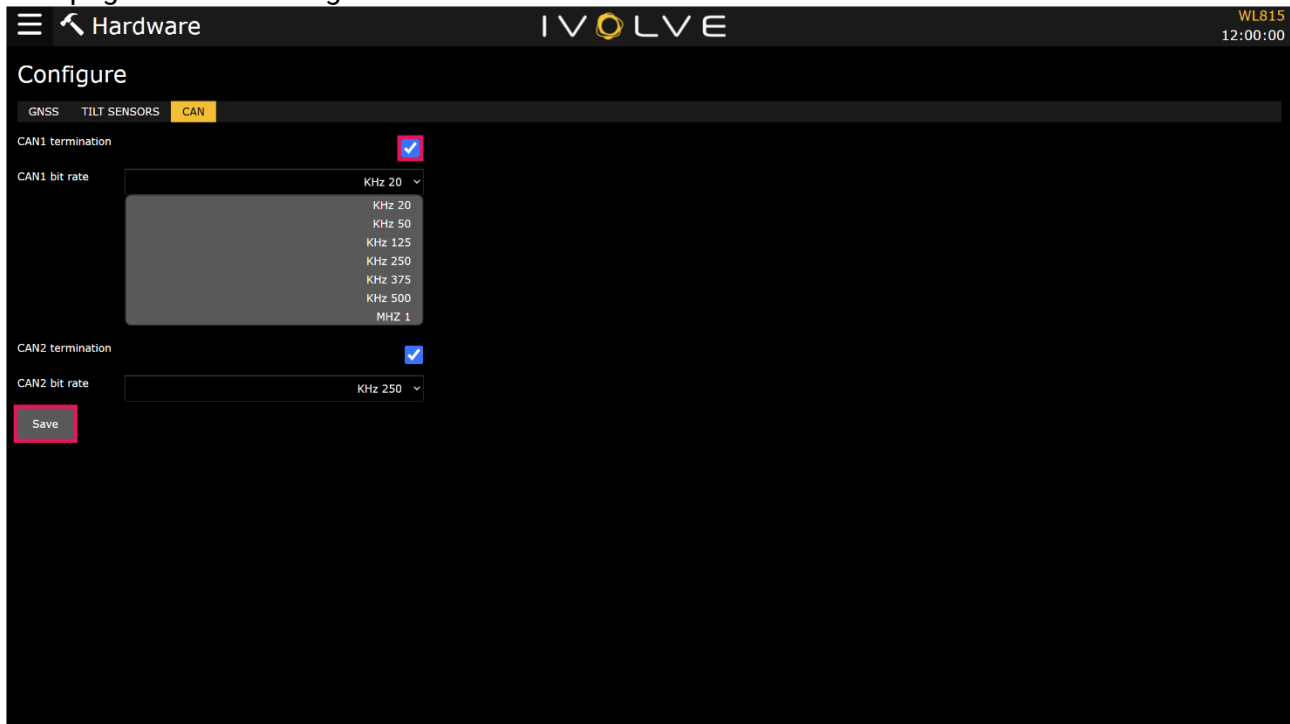
Setting	Options	Default value	Description
Sensor ID	Number	N/A	Enter the ID of the sensor.
Orientation	Top of vehicle, arrow front Top of vehicle, arrow right Bottom of vehicle, arrow front Bottom of vehicle, arrow right Right of vehicle, arrow front Right of vehicle, arrow top Left of vehicle, arrow front Left of vehicle, arrow top Front of vehicle, arrow top Front of vehicle, arrow right Back of vehicle, arrow top Back of vehicle, arrow right	Left of vehicle, arrow front	Select where the sensor is located and which direction it faces.
Filter (Hz)	None 1 Hz 2 Hz 5 Hz 10 Hz 20 Hz	None	What frequency to use (in Hertz) to filter out noise and vibrations. The frequency determines how much noise is filtered out so that it does not interfere with the accuracy and precision of the reading.

Advanced options

Setting	Options	Default value	Description
CAN interface	None CAN0 CAN1	None	Select which CAN interface the tilt sensors connect to on the Nexus.

CAN

This page contains configurations for the CAN interfaces.



The screenshot shows the 'Configure' page for the CAN interfaces. The 'CAN' tab is selected. Under 'CAN1 termination', there is a checked checkbox. Below it, 'CAN1 bit rate' is set to 'KHz 20' from a dropdown menu. Under 'CAN2 termination', there is a checked checkbox. Below it, 'CAN2 bit rate' is set to 'KHz 250' from a dropdown menu. A 'Save' button is located at the bottom left of the configuration area.

Setting	Options	Default value	Description
CAN1 termination	Checked, Unchecked	Unchecked	Select the check box to indicate the CAN1 cables are terminated here.
CAN1 bit rate	20 kHz	20 kHz	Select the bit rate of the CAN1 network.

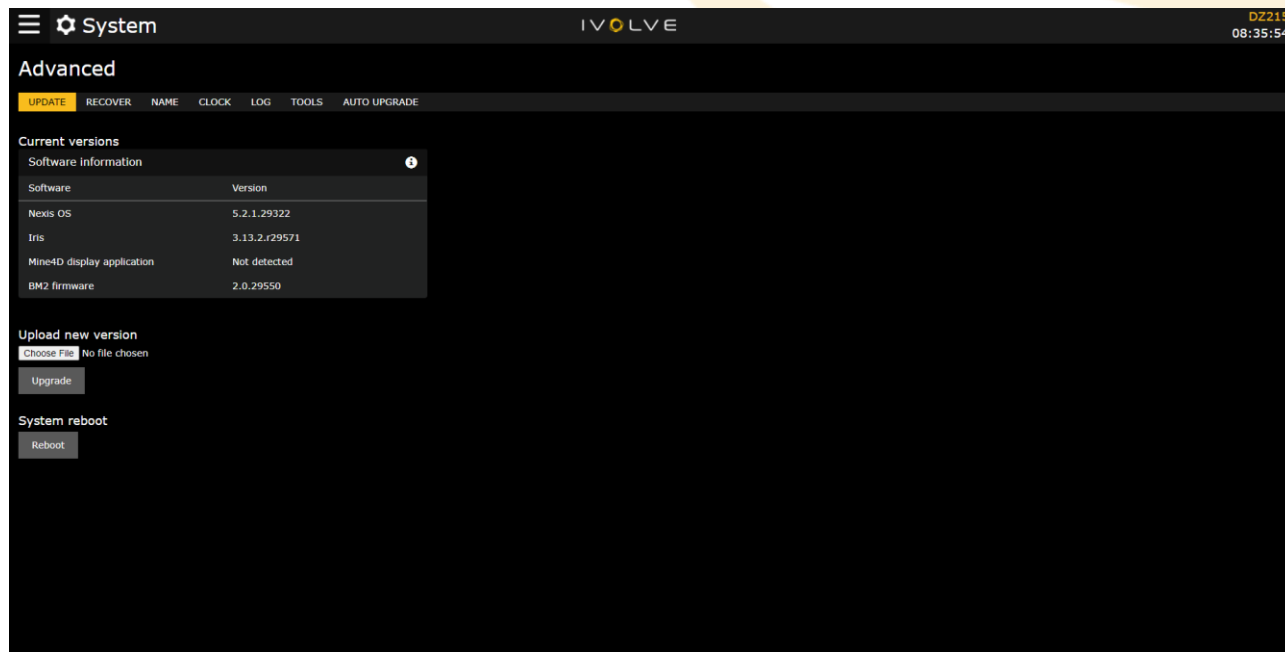
Setting	Options	Default value	Description
	50 kHz 125 kHz 250 kHz 375 kHz 500 kHz 1 MHz		
CAN2 termination	Checked, Unchecked	Unchecked	Select the check box to indicate the CAN2 cables are terminated here.
CAN2 bit rate	20 kHz 50 kHz 125 kHz 250 kHz 375 kHz 500 kHz 1 MHz	250 kHz	Select the bit rate of the CAN2 network.

2.5 System Pages

The system pages contain the Update, Recover, Name, Clock, Log, Tools and Auto Upgrade configurations.

Update

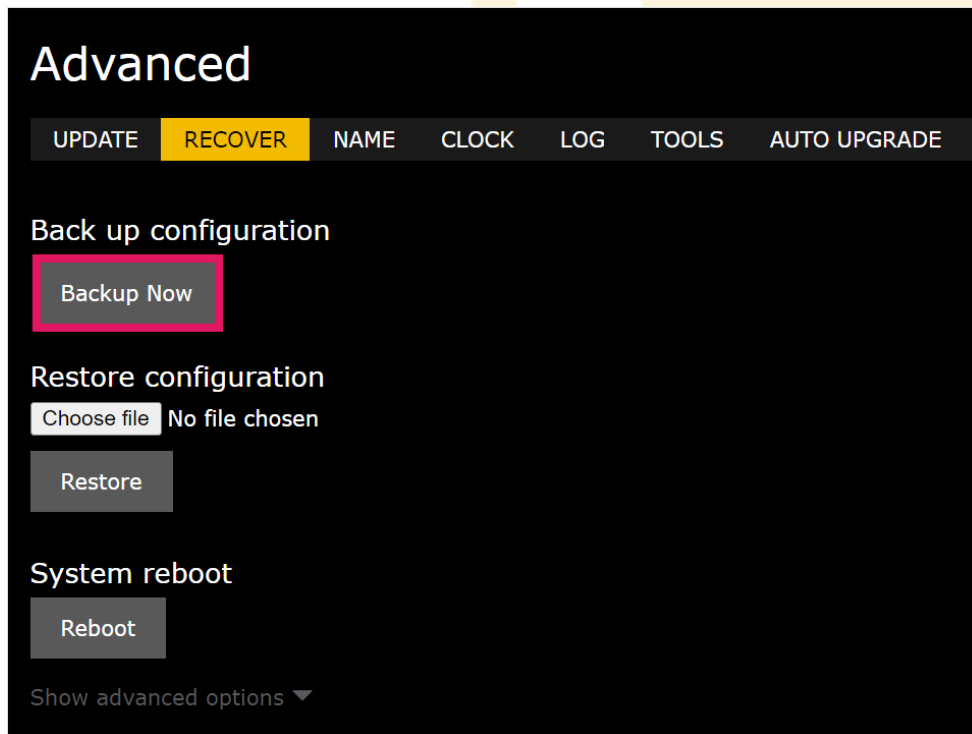
Here you can upload different upgrade packages to perform upgrades or downgrades to the various devices connected to the system and perform a reboot. The appropriate firmware files are required to perform the relevant update (Nexis OS, Iris, BM2, TS1B, Pinecone Fleet and Guidance).



Recover

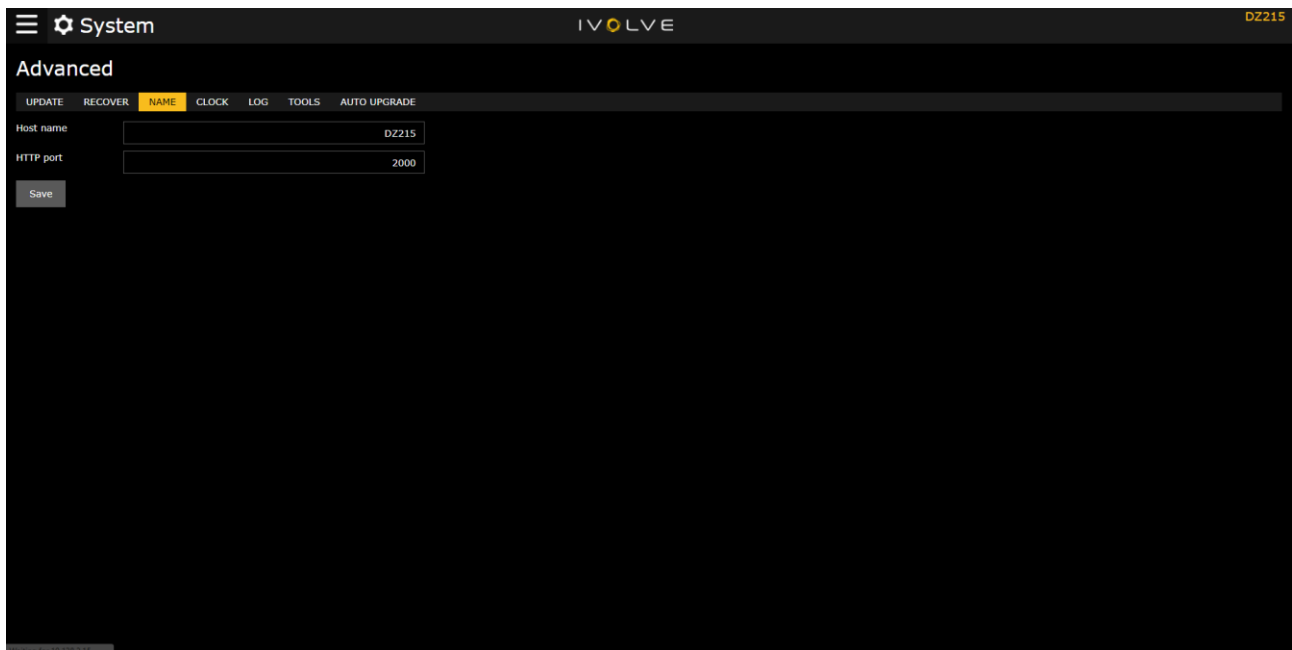
The Recover page allows you to back up the current configuration of the Nexis, restore the configuration using one of the backup files, reboot the system and perform a factory reset of the device.

The backup file will save as a generic filename 'nexis.tar.bz2'; iVolve recommends renaming this immediately so it is easy to identify in the future.



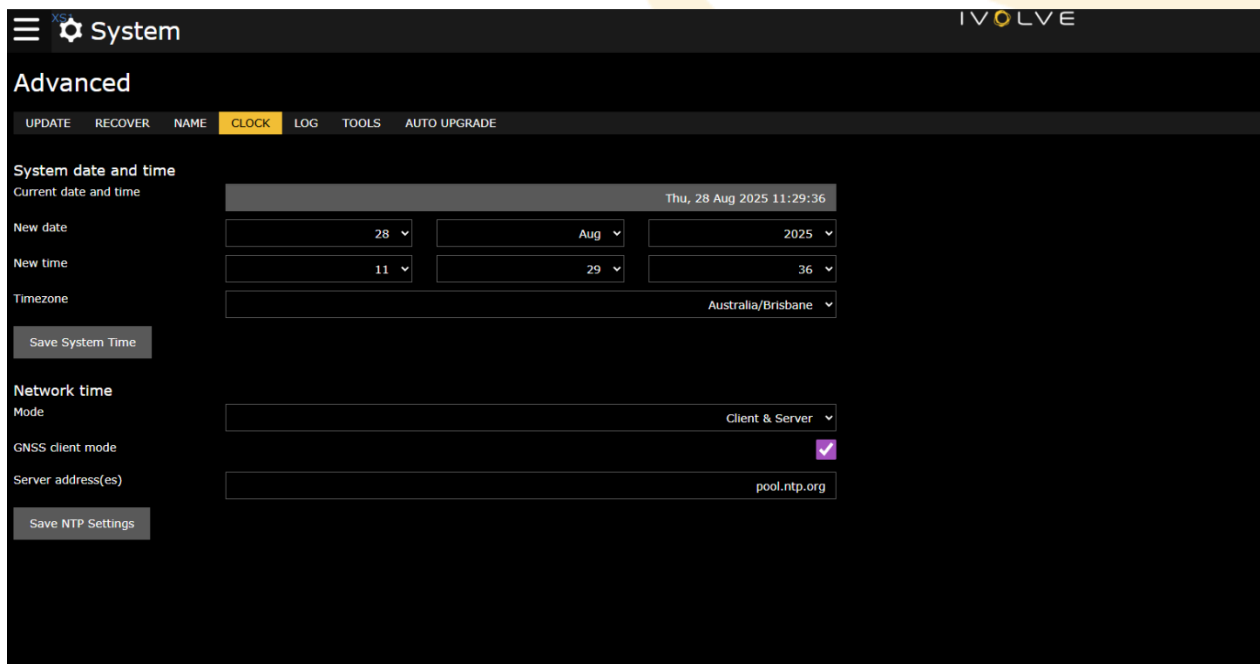
Name

In this section you can change the Host name (appears in the top-right corner of the screen) and the HTTP Port of the device. (Default is port 2000.)



Clock

The system date, time and NTP settings are configured here.



System iVOLVE

Advanced

UPDATE RECOVER NAME **CLOCK** LOG TOOLS AUTO UPGRADE

System date and time

Current date and time: Thu, 28 Aug 2025 11:29:36

New date:

New time:

Timezone:

Network time

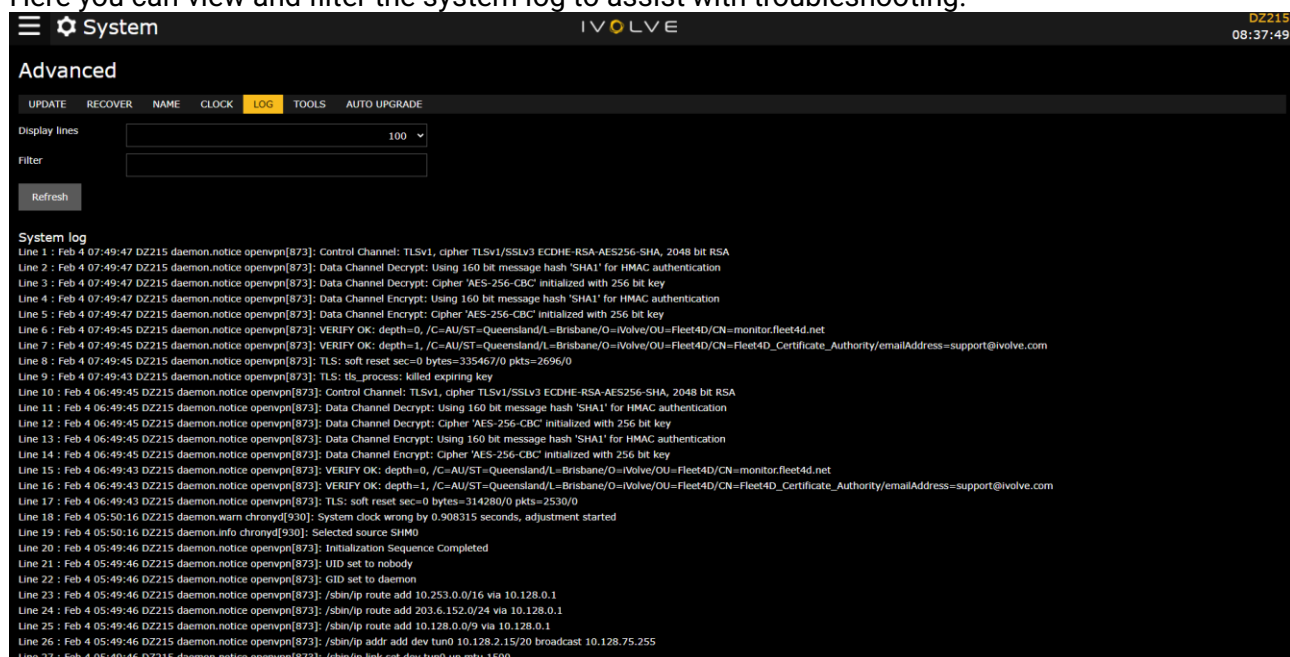
Mode:

GNSS client mode: ☒

Server address(es):

Log

Here you can view and filter the system log to assist with troubleshooting.



System iVOLVE DZ215 08:37:49

Advanced

UPDATE RECOVER NAME **CLOCK** **LOG** TOOLS AUTO UPGRADE

Display lines:

Filter:

System log

Line 1 : Feb 4 07:49:47 DZ215 daemon.notice openvpn[873]: Control Channel: TLSv1, cipher TLSv1/SSLv3 ECDHE-RSA-AES256-SHA, 2048 bit RSA

Line 2 : Feb 4 07:49:47 DZ215 daemon.notice openvpn[873]: Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication

Line 3 : Feb 4 07:49:47 DZ215 daemon.notice openvpn[873]: Data Channel Decrypt: Cipher 'AES-256-CBC' initialized with 256 bit key

Line 4 : Feb 4 07:49:47 DZ215 daemon.notice openvpn[873]: Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication

Line 5 : Feb 4 07:49:47 DZ215 daemon.notice openvpn[873]: Data Channel Encrypt: Cipher 'AES-256-CBC' initialized with 256 bit key

Line 6 : Feb 4 07:49:45 DZ215 daemon.notice openvpn[873]: VERIFY OK: depth=0, /C=AU/ST=Queensland/L=Brisbane/O=iVolve/OU=Fleet4D/CN=monitor.fleet4d.net

Line 7 : Feb 4 07:49:45 DZ215 daemon.notice openvpn[873]: VERIFY OK: depth=1, /C=AU/ST=Queensland/L=Brisbane/O=iVolve/OU=Fleet4D/CN=Fleet4D_Certificate_Authority/emailAddress=support@iVolve.com

Line 8 : Feb 4 07:49:45 DZ215 daemon.notice openvpn[873]: TLS: soft reset sec=0 bytes=335467/0 pkts=2696/0

Line 9 : Feb 4 07:49:43 DZ215 daemon.notice openvpn[873]: TLS: tls_process: killed expiring key

Line 10 : Feb 4 06:49:45 DZ215 daemon.notice openvpn[873]: Control Channel: TLSv1, cipher TLSv1/SSLv3 ECDHE-RSA-AES256-SHA, 2048 bit RSA

Line 11 : Feb 4 06:49:45 DZ215 daemon.notice openvpn[873]: Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication

Line 12 : Feb 4 06:49:45 DZ215 daemon.notice openvpn[873]: Data Channel Decrypt: Cipher 'AES-256-CBC' initialized with 256 bit key

Line 13 : Feb 4 06:49:45 DZ215 daemon.notice openvpn[873]: Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication

Line 14 : Feb 4 06:49:45 DZ215 daemon.notice openvpn[873]: Data Channel Encrypt: Cipher 'AES-256-CBC' initialized with 256 bit key

Line 15 : Feb 4 06:49:43 DZ215 daemon.notice openvpn[873]: VERIFY OK: depth=0, /C=AU/ST=Queensland/L=Brisbane/O=iVolve/OU=Fleet4D/CN=monitor.fleet4d.net

Line 16 : Feb 4 06:49:43 DZ215 daemon.notice openvpn[873]: VERIFY OK: depth=1, /C=AU/ST=Queensland/L=Brisbane/O=iVolve/OU=Fleet4D/CN=Fleet4D_Certificate_Authority/emailAddress=support@iVolve.com

Line 17 : Feb 4 06:49:43 DZ215 daemon.notice openvpn[873]: TLS: soft reset sec=0 bytes=314280/0 pkts=2530/0

Line 18 : Feb 4 05:50:16 DZ215 daemon.warn chronyd[930]: System clock wrong by 0.908315 seconds, adjustment started

Line 19 : Feb 4 05:50:16 DZ215 daemon.info chronyd[930]: Selected source SHM0

Line 20 : Feb 4 05:49:46 DZ215 daemon.notice openvpn[873]: Initialization Sequence Completed

Line 21 : Feb 4 05:49:46 DZ215 daemon.notice openvpn[873]: UID set to nobody

Line 22 : Feb 4 05:49:46 DZ215 daemon.notice openvpn[873]: GID set to daemon

Line 23 : Feb 4 05:49:46 DZ215 daemon.notice openvpn[873]: /sbin/ip route add 10.253.0.0/16 via 10.128.0.1

Line 24 : Feb 4 05:49:46 DZ215 daemon.notice openvpn[873]: /sbin/ip route add 203.6.152.0/24 via 10.128.0.1

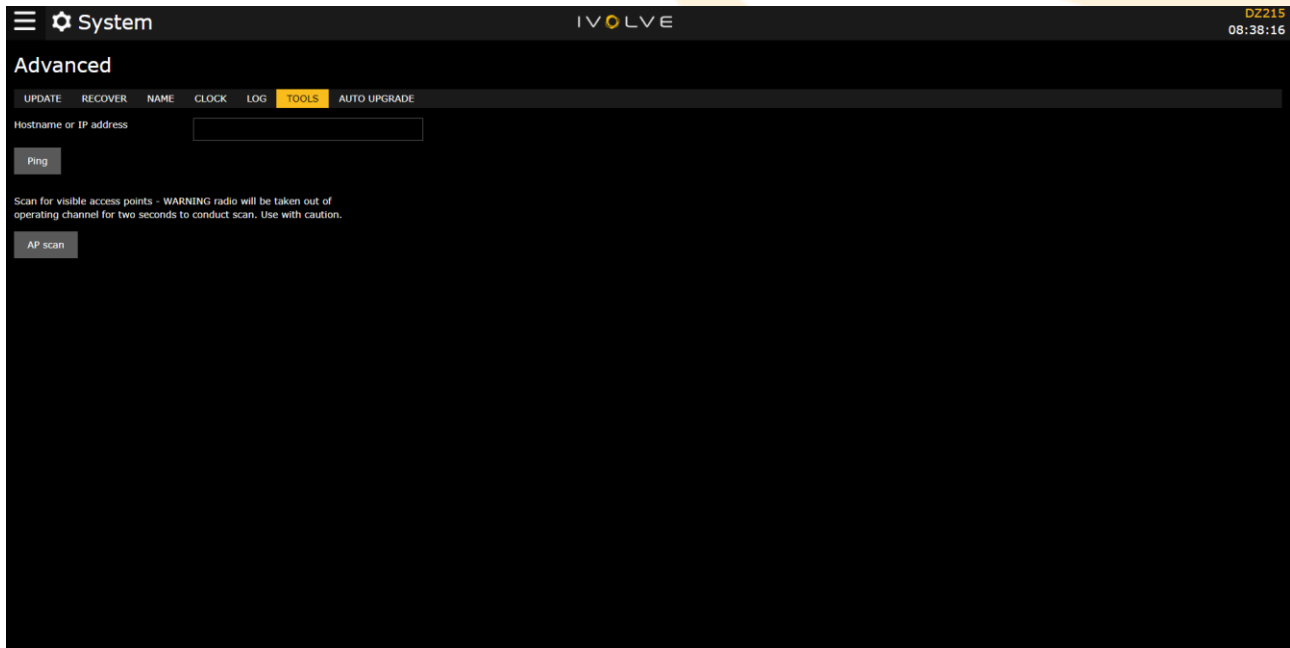
Line 25 : Feb 4 05:49:46 DZ215 daemon.notice openvpn[873]: /sbin/ip route add 10.128.0.0/9 via 10.128.0.1

Line 26 : Feb 4 05:49:46 DZ215 daemon.notice openvpn[873]: /sbin/ip addr add dev tun0 10.128.2.15/20 broadcast 10.128.75.255

Line 27 : Feb 4 05:49:46 DZ215 daemon.notice openvpn[873]: /sbin/ip link set dev tun0 up mtu 1500

Tools

The tools page contains a ping and access point scan tool to assist with setup and troubleshooting.



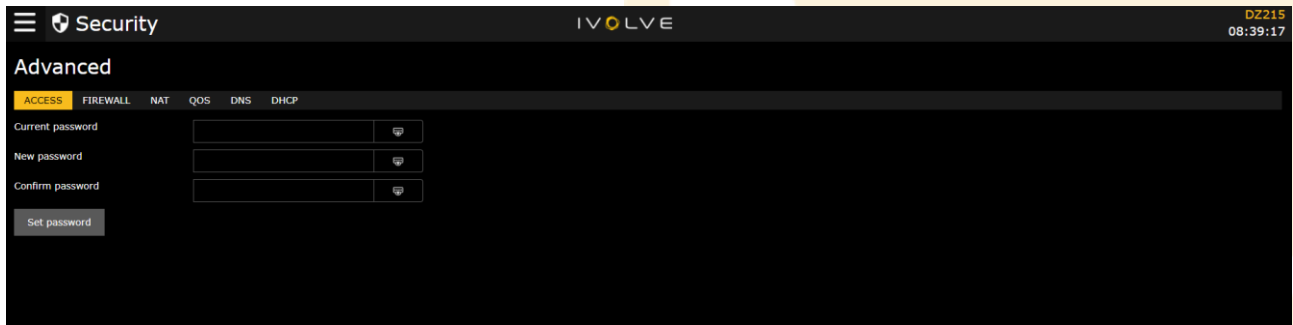
Auto Upgrade

The auto upgrade is a legacy and deprecated feature superseded by the Central Management system.

2.6 Security Pages

Access

The Access page allows users to change the password for the Nexis. Any changes to the password must be noted and notified to your support representative.



The screenshot shows the 'Security' section of the iVolve web interface. The 'Advanced' tab is selected, and the 'ACCESS' sub-tab is active. The 'Current password' field is empty, and the 'New password' field is also empty. The 'Confirm password' field is empty. A 'Set password' button is visible at the bottom left of the form. The top right corner of the interface shows the user 'DZ215' and the time '08:39:17'.

Firewall

This contains the configuration options for the firewall. The Nexis firewall controls how incoming and outgoing networking traffic is handled. For security reasons, the firewall must be reactivated before any saved changes take effect.

Security

IVOLVE

XD8TRUCK
12:50:43

Advanced

ACCESS

FIREWALL

NAT

QOS

DNS

DHCP

Reactivate Firewall

Enable firewall

Private LTE/cellular connection

Network address translation (NAT)

Allow NAT outbound (LAN->WLAN) packets

Allow NAT outbound packets from LAN subnet only

Allow NAT outbound LAN1 packets

Allow NAT inbound (WLAN->LAN) packets

Allow NAT FTP sessions

Access control

Reject AUTH packets

Block class A (10.0.0.0/8) traffic

Block class B (172.16.0.0/12) traffic

Block class C (192.168.0.0/16) traffic

Block multicast (224.0.0.0/4) traffic

Block reserved (240.0.0.0/5) traffic

Allow SSH access via WLAN

Allow ICMP via WLAN

Allow TCP packet forwards on LAN0

Allow TCP packet forwards on LAN1

Update

Show advanced options ▼



General firewall settings

Setting	Description
Enable Firewall	Specify whether the Nexis firewall is turned on or off. If turned off, none of the other firewall options available on this page have any effect and all inbound connections are allowed.
Private LTE/cellular connection	For Nexis with cellular connections only. Enable the SSH and web interface access over the cellular network interface. When this checkbox is selected, the firewall allows inbound connections on port 22 (SSH) and port 2000 (web interface) over the cellular network interface when the Nexis is connected to a private LTE network.

NAT firewall settings

Setting	Description
Allow NAT outbound (LAN->WLAN) packets	Specify whether to NAT packets coming in on the Nexis LAN and going out the Nexis WLAN.
Allow NAT outbound packets from LAN subnet only	If Allow NAT outbound packets is enabled, specify whether to NAT all outbound traffic that has come in on the Nexis LAN or only traffic that has come in on the Nexis LAN and is on the Nexis LAN subnet. This option is ignored if Allow NAT outbound packets is not enabled.
Allow NAT outbound LAN1 packets	Specify whether to allow NAT packets going out the LAN1 interface.
Allow NAT inbound (WLAN->LAN) packets	Specify whether to allow NAT packets that came in on the Nexis WLAN and are going out the Nexis LAN.
Allow NAT FTP sessions	Specify whether to allow the source address embedded in outbound FTP packets.

Access control settings

Setting	Description
Reject AUTH packets	N/A
Block class A (10.0.0.0/8) traffic	N/A
Block class B (172.16.0.0/12) traffic	N/A
Block class C (192.168.0.0/16) traffic	N/A
Block multicast (224.0.0.0/4) traffic	N/A
Block reserved (240.0.0.0/5) traffic	N/A
Allow SSH access via WLAN	SSH access is automatically enabled for LAN interface(s). This option allows SSH access over the wireless interface as well.
Allow ICMP via WLAN	N/A
Allow TCP packet forwards on LAN0	Specify whether to allow the Nexis to forward any TCP packets that come in or are due to be forwarded out LAN0.
Allow TCP packet forwards on LAN1	Specify whether to allow the Nexis to forward any TCP packets that come in or are due to be forwarded out LAN1.

Advanced access control settings

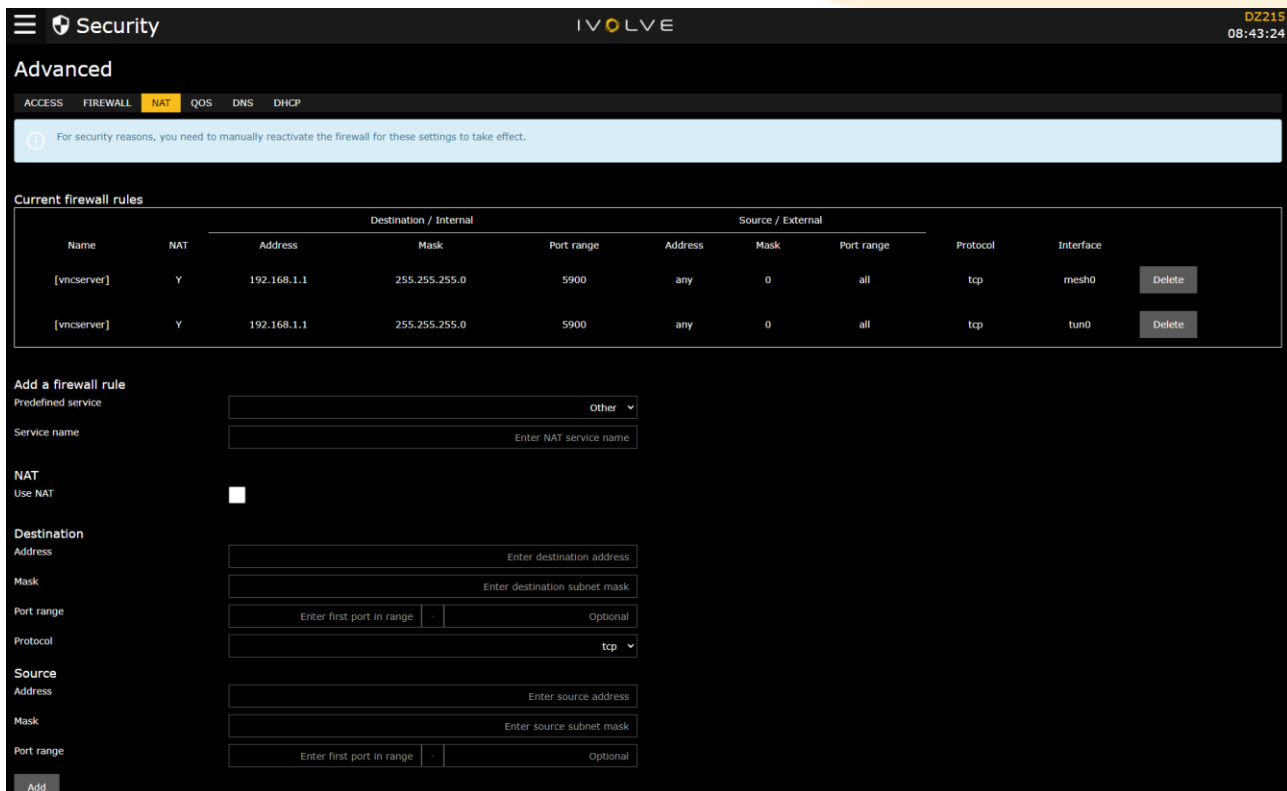
To add specific IP addresses or subnets by which inbound connections can be allowed or denied (blocked) by the firewall, enter the IP address or subnet and click **Add**. Select the check box next to that item to enable its firewall.

Enabled	Address/Subnet	Access	Action
---------	----------------	--------	--------

Yes/No | For example, 192.168.0.0/16. | Allow/Deny | Add/Delete

NAT

Here firewall and NAT routing rules can be created. For security reasons, the firewall must be reactivated before any saved changes take effect.



Security iVOLVE DZ215 08:43:24

Advanced

ACCESS FIREWALL **NAT** QOS DNS DHCP

For security reasons, you need to manually reactivate the firewall for these settings to take effect.

Current firewall rules

Name	NAT	Destination / Internal			Source / External			Protocol	Interface	
		Address	Mask	Port range	Address	Mask	Port range			
[vncserver]	Y	192.168.1.1	255.255.255.0	5900	any	0	all	tcp	mesh0	Delete
[vncserver]	Y	192.168.1.1	255.255.255.0	5900	any	0	all	tcp	tun0	Delete

Add a firewall rule

Predefined service: Other

Service name: Enter NAT service name

NAT: ☒ Use NAT

Destination

Address: Enter destination address

Mask: Enter destination subnet mask

Port range: Enter first port in range - Optional

Protocol: tcp

Source

Address: Enter source address

Mask: Enter source subnet mask

Port range: Enter first port in range - Optional

Add

Adding a firewall rule

To add a firewall rule, enter the details and click **Add**.

After you add a firewall rule, select the **Firewall** tab and click **Reactivate Firewall**.

Removing a firewall rule

To remove a firewall rule, click **Delete** next to that rule in the **Current firewall rules** table.

After you remove a firewall rule, select the **Firewall** tab and click **Reactivate Firewall**.

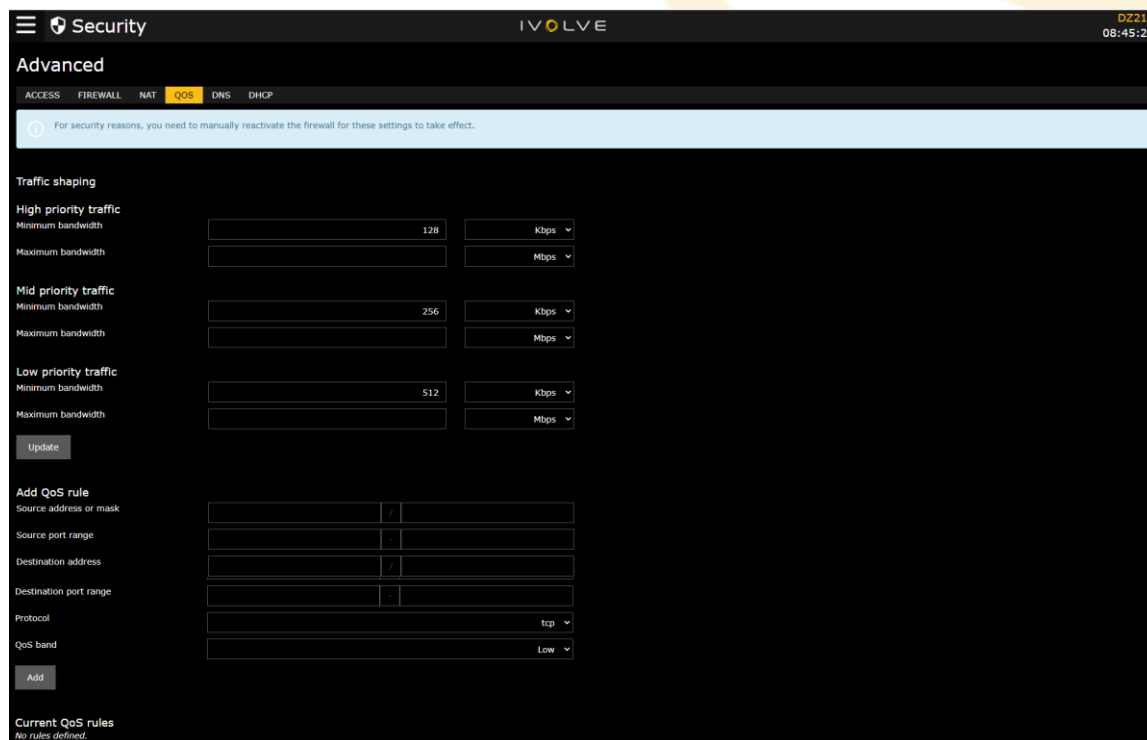
Current firewall rules

Setting	Description
---------	-------------

Name	A name for the firewall rule.
NAT	Specify whether to use network address translation (NAT).
Destination	The internal destination of the data.
Address	The IP address.
Mask	The subnet mask.
Port range	The range of ports where the rule applies.
Source	The external source of the data.
Address	The IP address.
Mask	The subnet mask.
Port range	The range of ports where the rule applies.
Protocol	The protocol to use for the rule.
Interface	The network interface to use for the rule.

QoS

This page contains configuration and rule options for QoS and traffic shaping, instruction the Nexis how to prioritise incoming and outgoing traffic.



Security DZ215
08:45:22

Advanced

ACCESS FIREWALL NAT **QoS** DNS DHCP

For security reasons, you need to manually reactivate the firewall for these settings to take effect.

Traffic shaping

High priority traffic

Minimum bandwidth: Kbps

Maximum bandwidth: Mbps

Mid priority traffic

Minimum bandwidth: Kbps

Maximum bandwidth: Mbps

Low priority traffic

Minimum bandwidth: Kbps

Maximum bandwidth: Mbps

Add QoS rule

Source address or mask:

Source port range:

Destination address:

Destination port range:

Protocol:

QoS band:

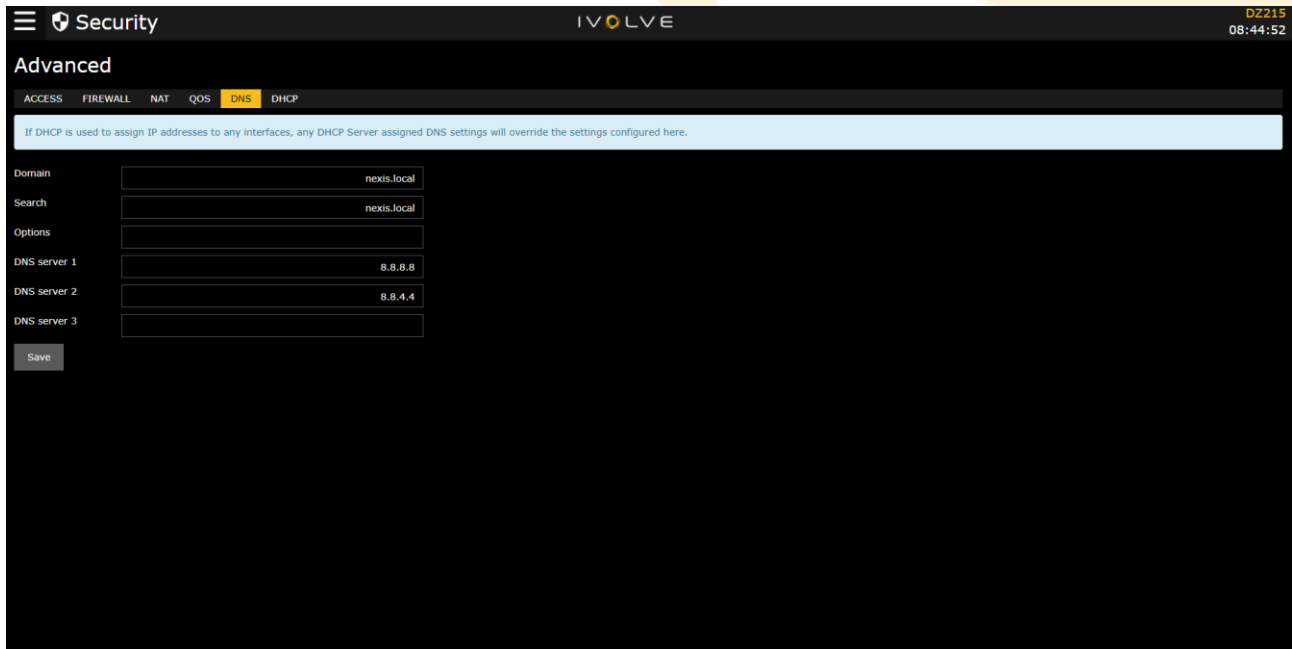
Current QoS rules

No rules defined.

Setting	Description
Source address or mask	The source IP address or subnet mask.
Source port range	The range of ports the rule applies to.
Destination address	The destination IP address.
Destination port range	The range of ports where the rule applies.
Protocol	The protocol to use for the rule.
QoS band	Specify whether the traffic is Low, Mid, or High priority.

DNS

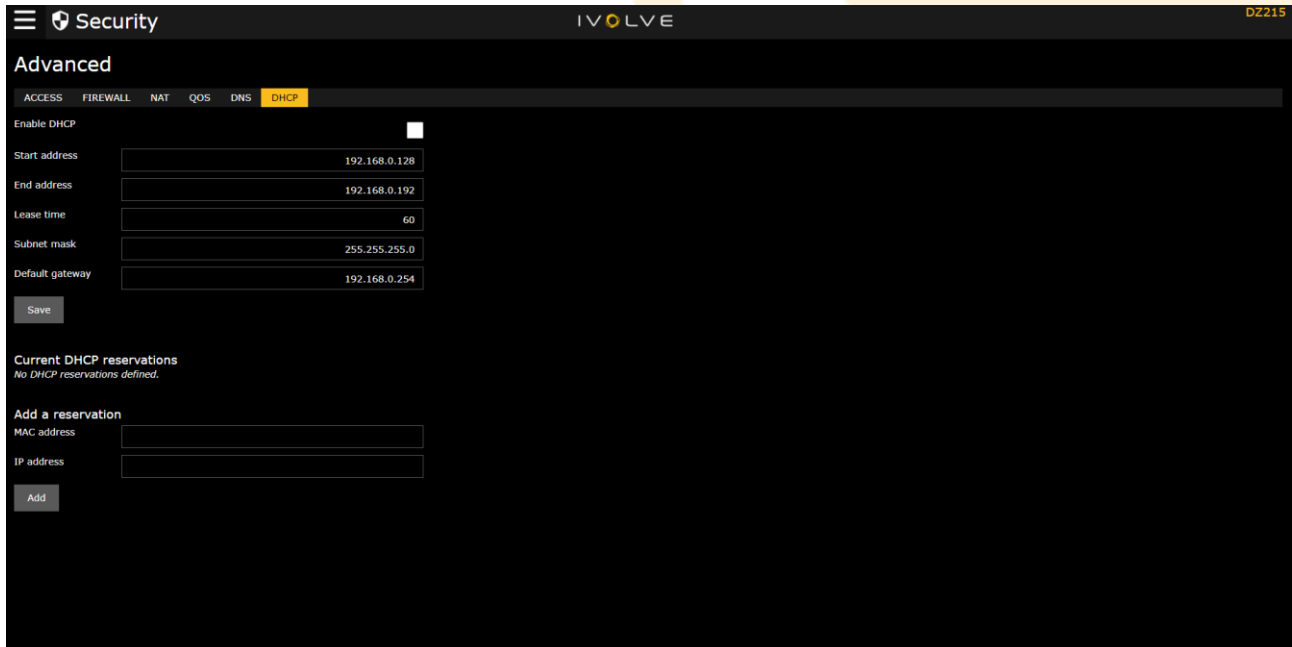
Here the user can configure DNS settings for the Nexis; these are required to resolve host names. Note, if you set up DHCP on the **DHCP** tab and use it to assign IP addresses to any interfaces, any DHCP server that is assigned DNS settings overrides any DNS settings configured here.



Setting	Option	Default	Description
Domain	N/A	nexus.local	N/A
Search	N/A	nexus.local	N/A
Options	N/A	Blank	N/A
DNS server 1	IP address	Blank	N/A
DNS server 2	IP address	Blank	N/A
DNS server 3	IP address	Blank	N/A

DHCP

Here the user can enable DHCP and configure its settings. This can be useful for simplifying wireless access to the device.



Setting	Option	Default	Description
Enable DHCP	Checked, Unchecked	Unchecked	Specify whether to enable DHCP.
Start address	IP address	192.168.0.128	The first available IP address in the DHCP range.
End address	IP address	192.168.0.192	The last available IP address in the DHCP range.
Lease time	Time	60 (seconds)	The amount of time to hold the DHCP lease.
Subnet mask	IP address	255.255.255.0	The subnet mask to use for the DHCP network.
Default gateway	IP address	192.168.0.254	The default gateway of the DHCP network.

Adding a DHCP reservation

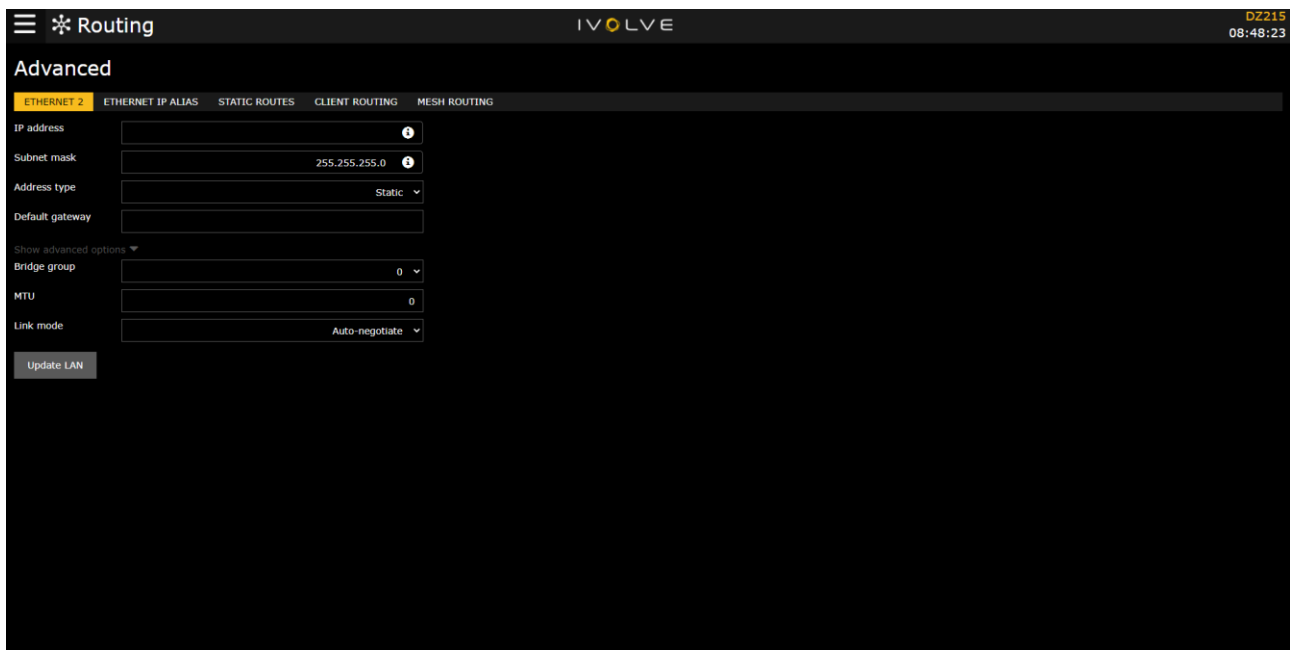
Setting	Description
MAC address	The MAC address of the device you want to assign the DHCP reservation to.
IP address	The IP address of the device you want to assign the DHCP reservation to.

2.7 Routing Pages

This section contains pages related to the secondary LAN connection, IP aliases and routing options.

Ethernet 2

Here you can configure the settings for the secondary Ethernet (LAN2) port.



The screenshot shows the 'Routing' section of the iVOLVE web interface. The 'Advanced' tab is selected, and the 'ETHERNET 2' sub-tab is active. The configuration fields are as follows:

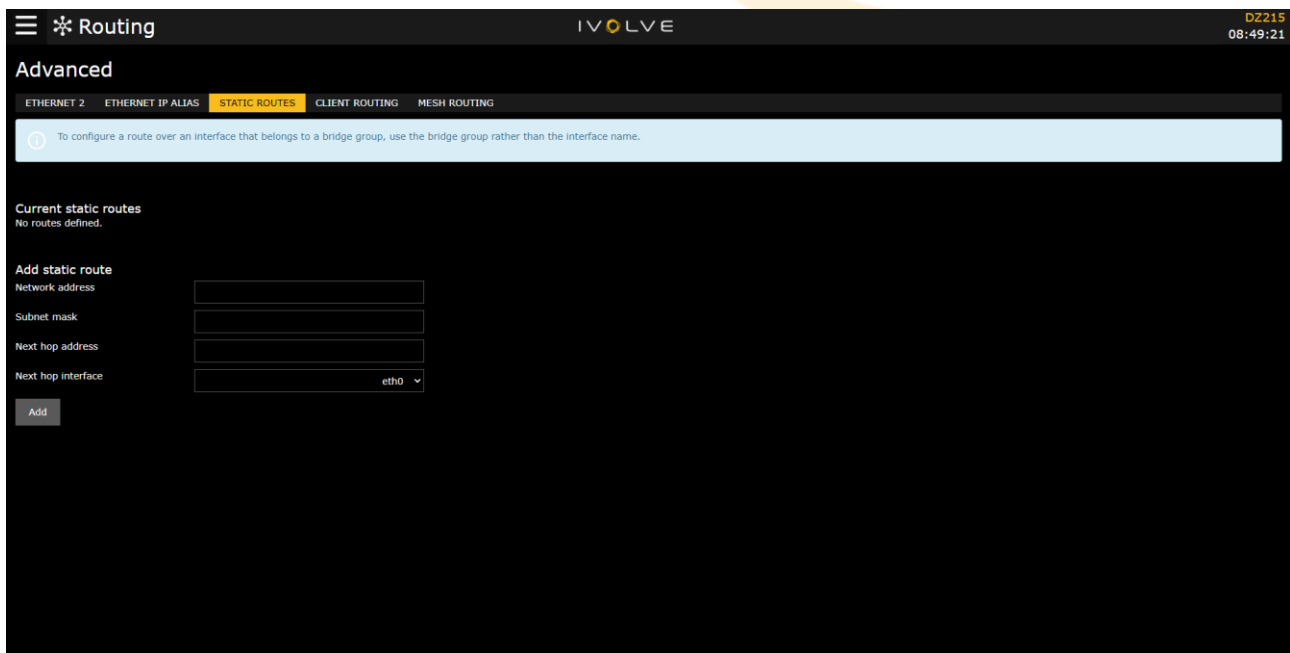
- IP address: [Empty field]
- Subnet mask: 255.255.255.0
- Address type: Static
- Default gateway: [Empty field]
- Show advanced options: [Dropdown arrow]
- Bridge group: 0
- MTU: 0
- Link mode: Auto-negotiate
- Update LAN: [Button]

Setting	Options	Default value	Description
IP address	Any valid IP address.	Blank	The IP address of the secondary Ethernet (LAN) interface.
Subnet mask	Any valid subnet mask.	255.255.255.0	The subnet mask to use to define the available IP addresses in the network.
Address type	Static, DHCP	Static	Whether the IP address is static or assigned using DHCP.
Default gateway	Any valid IP address.	Blank	Which address to route LAN traffic through to. For backbone devices, this points toward the server, but only needs to be set up on one backbone device and it broadcasts this to others.
Bridge group	0,1,2,3,4, None	N/A	Set the bridge group. Mesh units should be set to zero and backbone devices should be set to None.
MTU	N/A	0	N/A
Link mode	Auto-negotiate 10 Mbps half-duplex 10 Mbps full-duplex 100 Mbps half-duplex 100 Mbps full-duplex	Auto-negotiate	N/A

Ethernet IP Alias

Static Routes

Configuring and adding static routes can be done on this page.

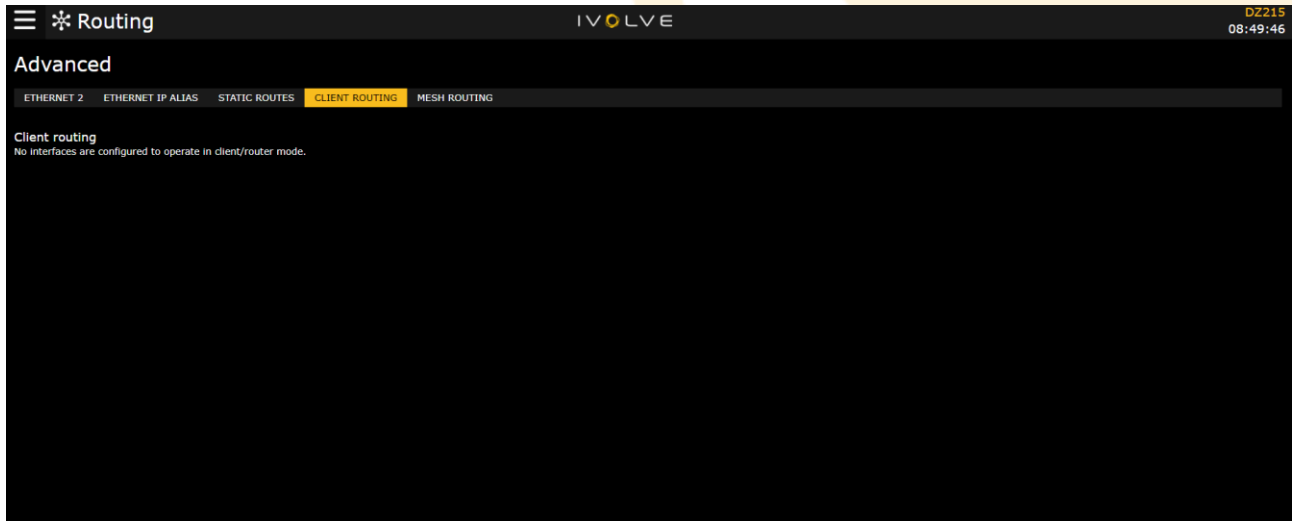


The screenshot shows the 'Routing' section of the iVOLVE interface, specifically the 'Static Routes' tab. The page has a dark theme. At the top, there's a navigation bar with 'Routing' and 'iVOLVE' logo. Below it, a sub-header 'Advanced' is visible. A breadcrumb trail shows 'ETHERNET 2' > 'ETHERNET IP ALIAS' > 'STATIC ROUTES' > 'CLIENT ROUTING' > 'MESH ROUTING'. A light blue informational banner states: 'To configure a route over an interface that belongs to a bridge group, use the bridge group rather than the interface name.' Below this, the 'Current static routes' section shows 'No routes defined.' The 'Add static route' section contains four input fields: 'Network address', 'Subnet mask', 'Next hop address', and 'Next hop interface' (which has a dropdown menu currently showing 'eth0'). An 'Add' button is located at the bottom left of this section.

Setting	Options	Default Value	Description
Network address	Any valid IP address	Blank	The IP address to use for the static route.
Subnet mask	Any valid subnet mask	Blank	The subnet mask of the static route.
Next hop address	Any valid IP address in the network	Blank	Define the IP address of the next hop along the route.
Next hop interface	eth0, eth1, br0	eth0	Define which network interface to use for this static route.

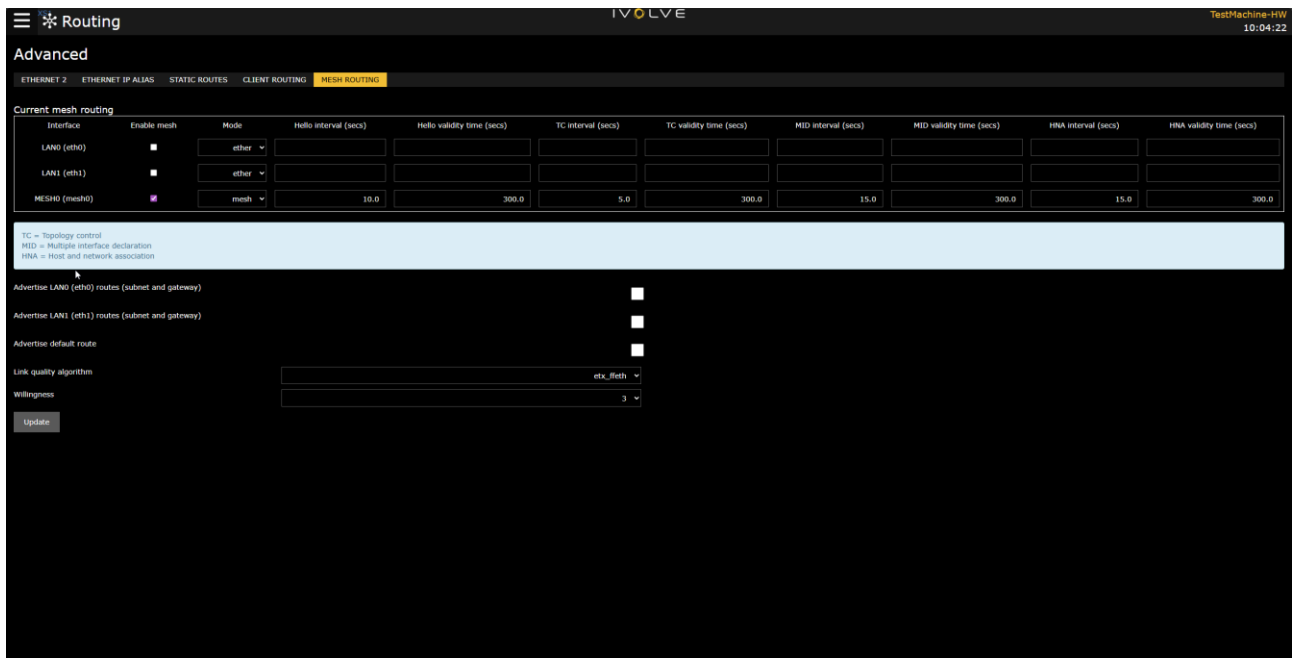
Client Routing

In this page you can configure a network interface to act as a client or router.



Mesh Routing

Here you can configure the routing table for the Mesh and LAN interfaces.



3. Compliance

FCC Warning

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.

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.

Note: The Grantee is not responsible for any changes or modifications not expressly approved by the party responsible for compliance. such modifications could void the user's authority to operate the equipment.

The device has been evaluated to meet general RF exposure requirement.

To maintain compliance with FCC's RF exposure guidelines, the distance must be at least 30 cm between the radiator and your body, and fully supported by the operating and installation

In accordance with eCFR: 47 CFR §15.203 antenna requirements, the requirement for a non-standard antenna connector does not apply to equipment that must be professionally installed. The LX1 is classified as equipment requiring professional installation.

Nexis LX1 is sold only to mining sites and is installed and commissioned on-site, particularly on heavy equipment (such as haul trucks) and dedicated communication towers.

Any electrical equipment (such as LX1) installed at such mining sites may only be installed by trained and authorized professional personnel.

The general public does not have access to these locations.

Nexis LX1 is installed in locations that are not easily accessible—typically inside locked cabinets or behind panels that require tools to remove, at least partially.

Due to the difficulty of access and the industrial nature of the installation, the risk of unauthorized antenna modification is effectively eliminated.

N-type female connectors are the industry standard for Wi-Fi connections on industrial and mining equipment.

