



# **NIO200 IAG User Manual**

V1.2

# Content

Preface.....	4
<b>1. General Information .....</b>	<b>11</b>
1.1 Document Purpose.....	11
1.2 Definitions, Acronyms and Abbreviations.....	11
<b>2 Product Overview .....</b>	<b>14</b>
2.1 About the NIO200IAG Gateway .....	14
2.2 Package Contents .....	15
2.3 Logical Interfaces.....	15
<b>3 Getting Started .....</b>	<b>17</b>
3.1 NIO200IAG Gateway .....	17
3.2 Hardware installation Guide .....	17
3.2.1 Water proof connector installation .....	18
3.2.2 Power installation.....	21
3.2.3 Antenna installation .....	22
3.2.4 Earth grounding .....	22
3.2.5 Mounting of NIO200 Series.....	23
3.3 Connecting to the NIO200IAG Gateway .....	25
3.4 Accessing NIO200 Admin website .....	25
3.5 Configuring the IP Address .....	25
3.6 Configuring the NTP settings.....	26
3.7 Monitoring Control System.....	27
<b>4 Home page .....</b>	<b>29</b>
<b>5 Administration for the Network Devices .....</b>	<b>30</b>
5.1 Dashboard .....	31
5.2 Topology .....	33
5.3 Devices .....	39
5.4 Device Details .....	42
5.5 Network Health .....	56
5.6 Readings .....	58
5.7 Commands Log .....	60
5.8 Alerts .....	62
5.9 Troubleshooting.....	64

5.10	Bulk Transfers .....	70
5.11	Set Country Code .....	72
6	Configuration.....	73
6.1	Backbone Router .....	74
6.2	Gateway.....	77
6.3	System Manager .....	79
6.4	Device Management .....	82
6.4.1.	Configuring Backbones.....	84
6.4.2.	Configuring Gateways.....	86
6.4.3.	Configuring Devices .....	87
6.5	Monitoring Host .....	91
6.6	MODBUS .....	93
6.7	Alert Subscription .....	94
6.8	Advanced Settings .....	94
6.8.1.	Edit Configuration Variables.....	95
6.8.2.	Restart.....	96
6.8.3.	Access NIO200 Wi-Fi Configuration website .....	97
6.9	Bulk Transfers .....	98
7	System Status .....	99
8	Administration.....	101
8.1	Device Firmwares .....	101
8.2	System Upgrade .....	103
8.3	Custom Icons.....	105
8.4	Custom Settings .....	106
9	Session.....	108
9.1	Change Password .....	108
10	Wi-Fi Mesh Configuration.....	109
10.1	Login .....	109
10.2	Status.....	111
10.2.1	Overview .....	111
10.2.2	Firewall .....	115
10.2.3	Routes .....	115
10.2.4	System Log .....	117
10.2.5	Kernel Log .....	117
10.2.6	Processes .....	118
10.2.7	Real-time Graphic.....	118
10.3	System.....	122
10.3.1	System.....	122

10.3.2	Administration.....	124
10.3.3	Backup/Flash Firmware .....	125
10.3.4	Reboot .....	129
10.4	Network .....	130
10.4.1	Interfaces .....	130
10.4.1.1	Configuration of IP address.....	130
10.4.2	Wi-Fi .....	136
10.4.2.1	Wireless Overview.....	136
10.4.2.2	Associated Stations.....	137
10.4.2.3	Wireless configuration.....	137
10.4.3	Mesh Advanced.....	142
10.4.3.1	Mesh Advanced.....	142
10.4.4	DHCP and DNS .....	144
10.4.4.1	General Settings .....	146
10.4.4.2	Resolve and Hosts Files .....	146
10.4.4.3	TFTP Settings .....	147
10.4.4.4	Advanced Settings .....	148
10.4.5	Hostnames .....	149
10.4.6	Static Routes .....	150
10.4.7	Diagnostics .....	152
10.4.8	Firewall .....	153
10.4.8.1	General Settings .....	153
10.4.8.2	Port Forwards .....	154
10.4.8.3	Traffic Rules .....	154
10.4.8.4	Custom Rules .....	155

## Preface

This manual is for user to set up a network environment using the NIO200 series Product line. It contains step-by-step procedures and graphic examples to guide installer or individuals with slight network system knowledge to complete the installation.

## Copyright

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. No part of this manual may

be reproduced, copied, translated or transmitted in any form or by any means without the prior written consent from NEXCOM International Co., Ltd.

## Disclaimer

The information in this document is subject to change without prior notice and does not represent commitment from NEXCOM International Co., Ltd. However, users may update their knowledge of any product in use by constantly checking its manual posted on our website: <http://www.nexcom.com>. NEXCOM shall not be liable for direct, indirect, special, incidental, or consequential damages arising out of the use of any product, nor for any infringements upon the rights of third parties, which may result from such use. Any implied warranties of merchantability or fitness for any particular purpose is also disclaimed.

## Acknowledgements

IWF series are trademarks of NEXCOM International Co., Ltd. All other product names mentioned herein are registered trademarks of their respective owners.

## Safety Information

Before installing and using the device, note the following precautions:

- Read all instructions carefully.
- Do not place the unit on an unstable surface, cart, or stand.
- Follow all warnings and cautions in this manual.
- When replacing parts, ensure that your service technician uses parts specified by the manufacturer.
- Avoid using the system near water, in direct sunlight, or near a heating device.

## Installation Recommendations

Ensure you have a stable, clean working environment. Dust and dirt can get into components and cause a malfunction.

Use containers to keep small components separated.

Adequate lighting and proper tools can prevent you from accidentally damaging the internal components. Most of the procedures that follow require only a few simple tools, including the following:

- A Philips screwdriver
- A flat-tipped screwdriver
- A grounding strap

- An anti-static pad

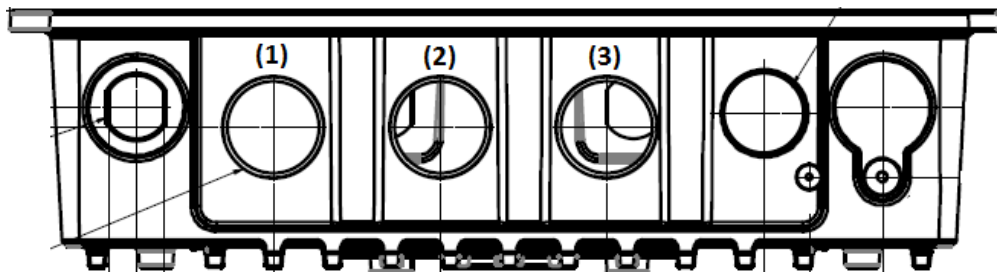
Using your fingers can disconnect most of the connections. It is recommended that you do not use needle-nose pliers to disconnect connections as these can damage the soft metal or plastic parts of the connectors.

## **Safety Precautions**

1. Read these safety instructions carefully.
2. Keep this User Manual for later reference.
3. Disconnect this equipment from any AC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
4. For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
5. Keep this equipment away from humidity.
6. Put this equipment on a stable surface during installation. Dropping it or letting it fall may cause damage.
7. The openings on the enclosure are for air convection to protect the equipment from overheating. DO NOT COVER THE OPENINGS.
8. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
9. Place the power cord in a way so that people will not step on it. Do not place anything on top of the power cord. Use a power cord that has been approved for use with the product and that it matches the voltage and current marked on the product's electrical range label. The voltage and current rating of the cord must be greater than the voltage and current rating marked on the product.
10. All cautions and warnings on the equipment should be noted.
11. If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.
12. Never pour any liquid into an opening. This may cause fire or electrical shock.
13. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
14. If one of the following situations arises, get the equipment checked by service personnel:
  - a. The power cord or plug is damaged.
  - b. Liquid has penetrated into the equipment.
  - c. The equipment has been exposed to moisture.
  - d. The equipment does not work well, or you cannot get it to work according to the user's manual.
  - e. The equipment has been dropped and damaged.

- f. The equipment has obvious signs of breakage.
15. Do not place heavy objects on the equipment.
16. Be sure to ground the 0.75mm<sup>2</sup> with an appropriate grounding wire (not included) by attaching it to the grounding screw on the unit and to a good ground connection. Earth, Green/Yellow wire, 18AWG, the minimum cross-sectional area of Earth conductor shall equal to Input wiring cable.
17. The front of the Equipment requires wiring terminals with the following specifications:
- **Wire size: 30-12 AWG** (0.0509-3.3088 mm<sup>2</sup>)
  - **Wire Type: copper wire only**
  - **Terminal Blocks Torque: 5 lb In.** (0.565 N-m).
  - For supply connections, use wires suitable for at least 75 degree C ambient environment
- **There must be a disconnect device in front of “NIO200 series” to keep the worker or field side maintainer be cautious and aware to close the general power supply before they start to do maintenance. The disconnect device hereby means a 20A circuit-breaker. Power installation must be performed with qualified electrician and followed with National Electrical Code, ANSI/NFPA 70 and Canadian Electrical Code, Part I, CSA C22.1.**

18.



- (1) DC IN: 12-48Vdc, 2.1-0.6A
- (2) LAN
- (3) WAN(POE):57Vdc, 600mA

19. This equipment is intended to Ex nA IIC T4 Gc.

## Note:

This equipment is intended to be mounted on a pole with the mounting bracket, wall mounting or DIN mounting; the mounting should always let water proof connectors down to bottom position.

Cet équipement est destiné à être monté à la place avec le support de montage, montage mural ou montage DIN; Le montage doit toujours laisser les connecteurs imperméable à la base.

This equipment is suitable for use in Class I, Division 2, Groups A, B, C, and D or non-hazardous locations only.

Cet équipement est adapté à une utilisation en Classe I, Division 2, Groupes A, B, C et D ou des zones non dangereuses uniquement.

- WARNING – EXPLOSION HAZARD. DO NOT CONNECT OR DISCONNECT WHEN ENERGIZED.”
- AVERTISSEMENT - RISQUE D'EXPLOSION. NE PAS CONNECTER NI DÉCONNECTER LORSQU'IL EST EN CHARGE.
- Product is UL Listed with UL Listed Fittings for use with liquid-tight flexible metal conduit. This wiring method is suitable for flexible connections in accordance with Article 501.10(B)(2) of the National Electrical Code (ANSI/NFPA 70). Suitability for installation in particular applications is at the discretion of the Authority Having Jurisdiction (AHJ) or similar.
- Le produit est homologué UL avec des accessoires homologués UL pour conduit métallique flexible étanche aux liquides.  
ette méthode de câblage convient aux flexibles connexions conformément
- à l'article 501.10 (B) (2) du National Code électrique (ANSI / NFPA 70). Pertinenced'installation dans certaines applications à la discrétion de l'Autoritéayant Juridiction (AHJ) Ou similaire.

## Technical Support and Assistance

1. For the most updated information of NEXCOM products, visit NEXCOM's website at [www.nexcom.com](http://www.nexcom.com).
2. For technical issues that require contacting our technical support team or sales representative, please have the following information ready before calling:
  - Product name and serial number



- Detailed information of the peripheral devices
- Detailed information of the installed software (operating system, version, application software, etc.)
- A complete description of the problem
- The exact wordings of the error messages

## Warnings

Read and adhere to all warnings, cautions, and notices in this guide and the documentation supplied with the chassis, power supply, and accessory modules. If the instructions for the chassis and power supply are inconsistent with these instructions or the instructions for accessory modules, contact the supplier to find out how you can ensure that your computer meets safety and regulatory requirements.

1. Handling the unit: carry the unit with both hands and handle it with care.
2. Opening the enclosure: disconnect power before working on the unit to prevent electrical shocks.
3. Maintenance: to keep the unit clean, use only approved cleaning products or cleans with a dry cloth.

### **Safety Warning: This equipment is intended for installation in a Restricted Access Location only**

Avertissement de sécurité: Cet équipement est destiné à être installé uniquement dans un lieu d'accès restreint

## Cautions

Electrostatic discharge (ESD) can damage system components. Do the described procedures only at an ESD workstation.

If no such station is available, you can provide some ESD protection by wearing an antistatic wrist strap and attaching it to a metal part of the computer chassis.

## Conventions Used in this Manual



Warning: Information about certain situations, which if not observed, can cause personal injury. This will prevent injury to yourself when performing a task.



Caution: Information to avoid damaging components or losing data.



Note: Provides additional information to complete a task easily.



**WARNING**  
**HOT SURFACE**  
**DO NOT TOUCH**

Note: The surface temperature of enclosure may exceed 70°C under working condition.

Remarque: La température de surface de l'enceinte peut dépasser 70 °C dans des conditions de travail.

# 1. General Information

## 1.1 Document Purpose

The purpose of this document is to provide instructions for using ISA100.11a Monitoring Control System (MCS) and to provide information about the NEXCOM NIO200IAG ISA100 All-In-One Gateway as well as instructions on how to configure certain settings.

## 1.2 Definitions, Acronyms and Abbreviations

The following table lists definitions, acronyms, and abbreviations that are only suitable to this document.

Term	Description
API	Application Programming Interface
Backbone	Any data network (e.g. industrial Ethernet, IEEE 802.11, etc.) within a facility interfacing to the plants network.
Backbone Router	An entity in the ISA100.11a network with routing capability which serves as an interface between the radio network and the backbone network.
BBR	Backbone Router
Blacklisted channel	A channel on which transmission is prohibited.
Broadcast	Transmission intended for all the devices in an ISA100.11a network (used for advertisements with all devices including the BBR, or for receive links for field devices only).
CCA backoffs	The count of transmissions on an RF channel that were aborted due to CCA.
CGI	Common Gateway Interface
Channels	Divisions of radio frequencies supported in a wireless network.
Contract	An agreement between the system manager and a device in the network involving the allocation of network resources by the system manager to support a particular communication need of that device.
Device role	Device capabilities that will be accepted by the Security Manager.

Term	Description
DHCP	Dynamic Host Configuration Protocol – a method to automatically configure the IP settings of a host connected in a LAN.
EUI64, EUI-64	The 64-bit address of a device in the network; it is a unique identifier usually set at the manufacturing of the device.
Field	The geographic space that contains all the nodes of a wireless network.
Field device	A physical device designed to meet the rigors of plant operation that communicates via DPDU's conforming to the ISA100.11a protocol.
Gateway	An entity in the ISA100.11a network that serves as an interface between the ISA100.11a network and a client.
Graph (communication)	A collection of unidirectional interconnected devices, which defines a set of communication paths between a source device and a destination device.
Graph (Topology)	A graphical representation of the network topology.
GW	Gateway
Input/output	A device with minimum characteristics required to participate in an ISA100.11a network and which provides or uses data from other devices.
ISA100.11a	A communication protocol used in wireless networks, set up by the Wireless Compliance Institute.
JSON	JavaScript Object Notation
LAN	Local Area Network
Link	A momentary or persistent interconnecting path between two or more devices for the purpose of transmitting and receiving messaging.
MCS	Monitoring Control System
Network Address	The 128-bit address of a device in the network.
Packet Error Rate	The ratio, in percent, of the number of lost packets (DPDU's) to the total number of packets sent by the selected device to its parent.
Process value	The quantity being controlled or the measurement value.
Provision	To update settings on an entity in order to prepare it for working in the network.
Revision	The device software revision related to vendor/model.
Router	A device that has data routing capability.

Term	Description
Security Manager	An entity in the ISA100.11a network that assigns the security keys that are required for communication between devices.
SM	System Manager
Superframe	A collection of timeslots with a common repetition period and possibly other common attributes.
System Manager	An entity in the ISA100.11a network that supervises the various operational aspects of a network other than security.
TR	Transceiver – the BBR radio
User Application Process	From ISA100.11a standard: An active process within the highest portion of the application layer that is the user of OSI (Open Systems Interconnection) services.
UTC	Coordinated Universal Time – A universal timekeeping standard that is based on the Greenwich Mean Time (GMT). Local time is calculated in UTC and offset by the local time zone.
FD	Field Device

## 2 Product Overview



NIO200 CID2



NIO200 ATEX

### 2.1 About the NIO200IAG Gateway

The NIO200IAG is an All-in-One ISA100 Wireless (IEC62734) compliant System and Security Manager, Gateway and Backbone Router. ISA100 compliance allows the NIO200IAG to establish full mesh field network topologies to ensure robust and reliable communication for mission-critical industrial wireless applications. The integration of both IEEE 802.11n Wi-Fi Mesh and ISA100 technologies ensures a fully redundant, mesh powered infrastructure for both the field network and the backbone infrastructure. It is CID2 and ATEX compliant for deployment in hazardous environments and is a perfect solution for critical data monitoring and control in process automation verticals such as oil & gas. The NIO200 co-exists gracefully with Wi-Fi based communication systems due to advanced spectrum management techniques. It hosts an intuitive web interface that allows end users to visualize process data, alerts and alarms as well as manage and configure ISA100 Wireless

compliant field instruments. All software and firmware components are remotely upgradeable.

## 2.2 Package Contents

Each NIO200IAG package contains the following items:

- One NIO200IAG unit
- Two simple wall mounting kit
- Three liquid-tight cable gland or conduit based on the ATEX or CID2 model. (used only for DC power input and Ethernet port)
- Two-pin DC power connector for 12~48 VDC power input
- Grounding screws
- Fi outdoor antennas for evaluation purpose ( when deployed in field site, the antenna may be changed to meet the application requirement )

## 2.3 Logical Interfaces

Interface	Description
<b>Serial Port</b>	The serial port is used as a kernel console and emergency backup.
<b>TCP</b>	<p>The NIO200IAG Gateway accepts the following TCP connections.</p> <ul style="list-style-type: none"><li>➤ The NIO200IAG Gateway has an http server listening on port 80.</li><li>➤ The NIO200IAG Gateway has an http server listening on port 8080.</li><li>➤ The NIO200IAG Gateway has an https server listening on port 443.</li><li>➤ The MODBUS TCP server is listening on TCP port 502.</li><li>➤ The Standard GSAP interface is listening on TCP port 4900.</li><li>➤ The GSAP over SSL is listening on TCP port 4901.</li></ul>
<b>UDP</b>	<p>The NIO200IAG Gateway utilizes the NTP protocol to synchronize time with Internet time servers. The UDP port 123 must be open in both directions to allow time synchronization.</p>

Interface	Description
-----------	-------------

**NOTE:** Not all interfaces are guaranteed to be up in all cases. Some might be disabled for specific applications.



## 3 Getting Started

### 3.1 NIO200IAG Gateway

The web-based administration is the preferred method to administer/configure the NIO200IAG Gateway. It requires a web browser and the IP of the NIO200IAG Gateway. The NIO200IAG Gateway must be connected to the local LAN then powered on, and the IP/mask or the router must be accessible from the PC where the browser is running.

### 3.2 Hardware installation Guide

Hardware connection of NIO200 includes the power, Ethernet interfaces and RF connectors. The installation of NIO200 should be carefully done with standard waterproof connectors accessories in the package (CID2: conduit connector, ATEX: cable gland connector).

**Note:** the mounting of NIO200 should always let water proof connectors down to bottom position. The following picture illustrates the proper mounting direction of NIO200 in the field.



### 3.2.1 Water proof connector installation

#### A. Installation of conduit connector for CID2 model



To install conduit in NIO200 enclosure, please follow the steps below:



- Put conduit through cap nut and gland packing.

- Position the ferrule at the end of the conduit.  
( Just have the bottom of ferrule cover the conduit, over-tighten may enlarge conduit diameter and loosen

- Pass DC power cable or Ethernet cable through conduit



- Connect connector into NIO200 enclosure, tighten locknut with body.

- Insert the conduit with ferrule into connector of NIO200 enclosure.

- Push gland packing and cap nut forwards to NIO200 conduit connector and tighten the cap nut

To install the conduit, user should implement with Flexible Metal Conduit, Liquid-tight which meets UL360 standard. Here is the requirement of the diameter and size information for the selection of Metal Conduit that mate with NIO200 conduit connectors.

Nominal size (inch)	Inner diameter min. (mm)	Inner diameter max. (mm)	Outside diameter min. (mm)	Outside diameter max. (mm)	Min bending radius (mm)	Packing length (m)
3/8"	12.29	12.80	17.50	18.00	50.50	30
1/2"	15.80	16.31	20.80	21.30	82.50	30
3/4"	20.83	21.34	26.20	26.70	108.00	30
1"	26.44	27.08	32.80	33.40	165.00	20
1-1/4"	35.05	35.81	41.40	42.20	203.00	20
1-1/2"	40.01	40.64	47.40	48.30	228.50	20

## B. Installation of cable gland connector for ATEX model



To install cable gland with power / Ethernet cable on NIO200 enclosure, please follow the steps below:

### Power connector installation



1. De-assembly the cable gland connector.

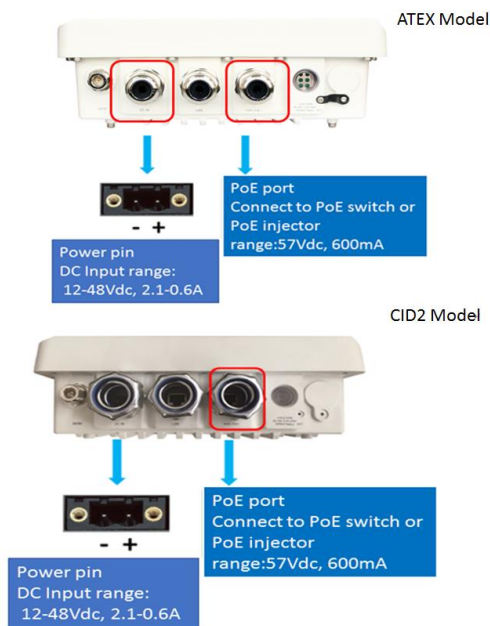
2. Pass power and Ethernet cable through cable gland as the illustration at the left.



### 3. Connect cable gland to NIO200 unit:

- Screw up the tips of power cable to green power connector.
- Fit the power cable to the left screw hole and tightly fasten cable gland to enclosure of NIO200 unit.
- Fit the Ethernet cable into the LAN or WAN hole on the enclosure. Tightly fasten cable gland to enclosure of NIO200 unit.

## 3.2.2 Power installation



- Prepare DC power source (12~48 VDC) or standard PoE facility such PoE switch or PoE injector.
- If use external DC power source, please carefully check if the polarity of power cord fits the polarity drawing in this diagram.
- When use PoE power source, just plug the Ethernet cable into PoE port.
- If the power connects correctly, then the “Power LED” will light accordingly

### 3.2.3 Antenna installation



Wi-Fi antenna connector for Wi-Fi Mesh connection (WLAN 1 & WLAN 2)



IWSN antenna connector ( for connecting to ISA100 or WirelessHART ), not used in NIO200WMR.

### 3.2.4 Earth grounding



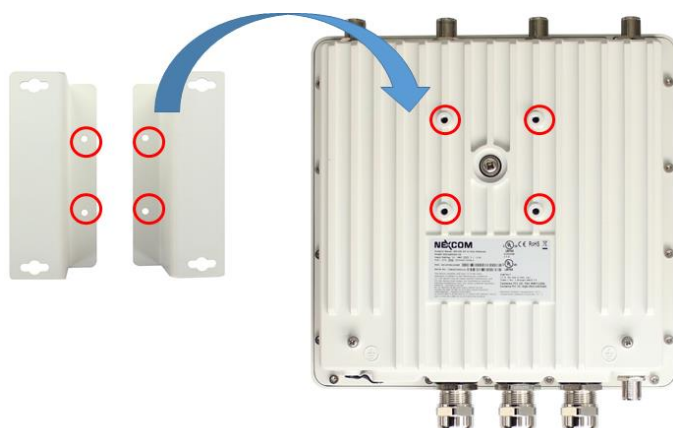
1. Be sure to ground the 0.75mm<sup>2</sup> ground screw with an appropriate grounding wire ( Earth, Green/Yellow wire 18AWG, not included) by attaching it to a good earth ground connection.
2. There must be a disconnect device in front of “NIO200 series” to keep the worker or field side maintainer be cautious and aware to close the general power supply before they start to do maintenance.
3. The disconnect device hereby means a 20A circuit-breaker. Power installation must be performed with qualified electrician and followed with National Electrical Code, ANSI/NFPA 70 and Canadian Electrical Code, Part I, CSA C22.1.

### 3.2.5 Mounting of NIO200 Series

Mounting method in NIO200 is default with simple wall mounting kit. If the installation is with pole mounting method, then user should purchase pole mounting kit for the installation. Here is the guide for both simple wall mounting method and pole mounting method:

A. Simple wall mounting method:

1. Screw the simple wall mounting kit to the bottom of NIO200 enclosure.

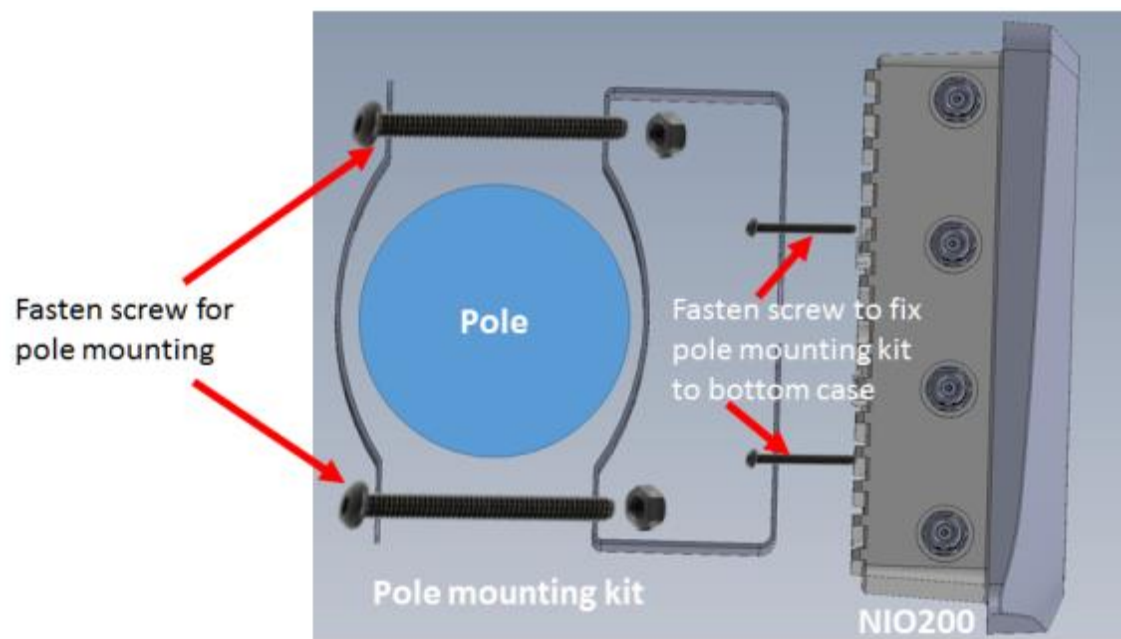


2. Be sure to fasten the mounting kit with horizontal position as below:



3. Hang on NIO200 to the wall with water proof connector at the bottom direction.

B. Pole mounting method:





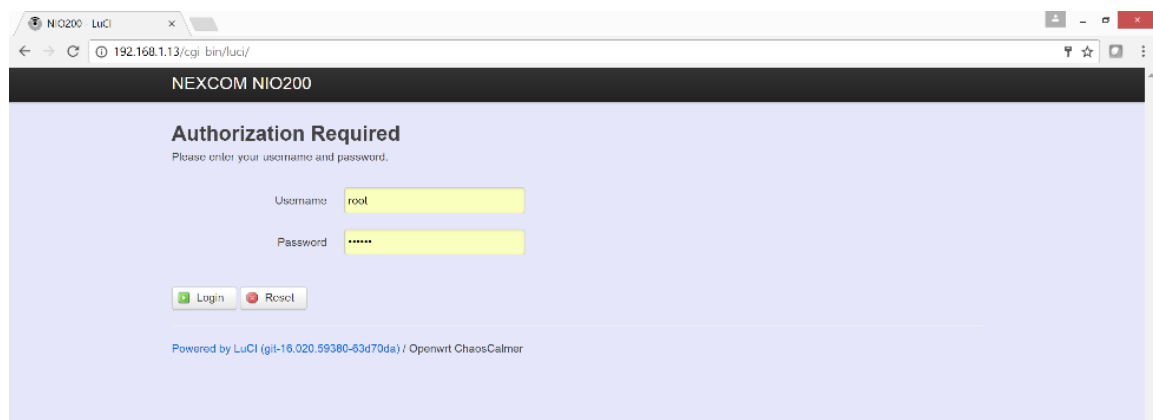
### 3.3 Connecting to the NIO200IAG Gateway

The NIO200IAG is pre-configured a static IP address **192.168.1.1** for connection directly to a computer. In order to communicate with the NIO200IAG, the user must temporarily set the computer IP address to a static address (**192.168.1.100** for example) and may use an Ethernet cross-over cable to connect the NIO200IAG to the computer.

### 3.4 Accessing NIO200 Admin website

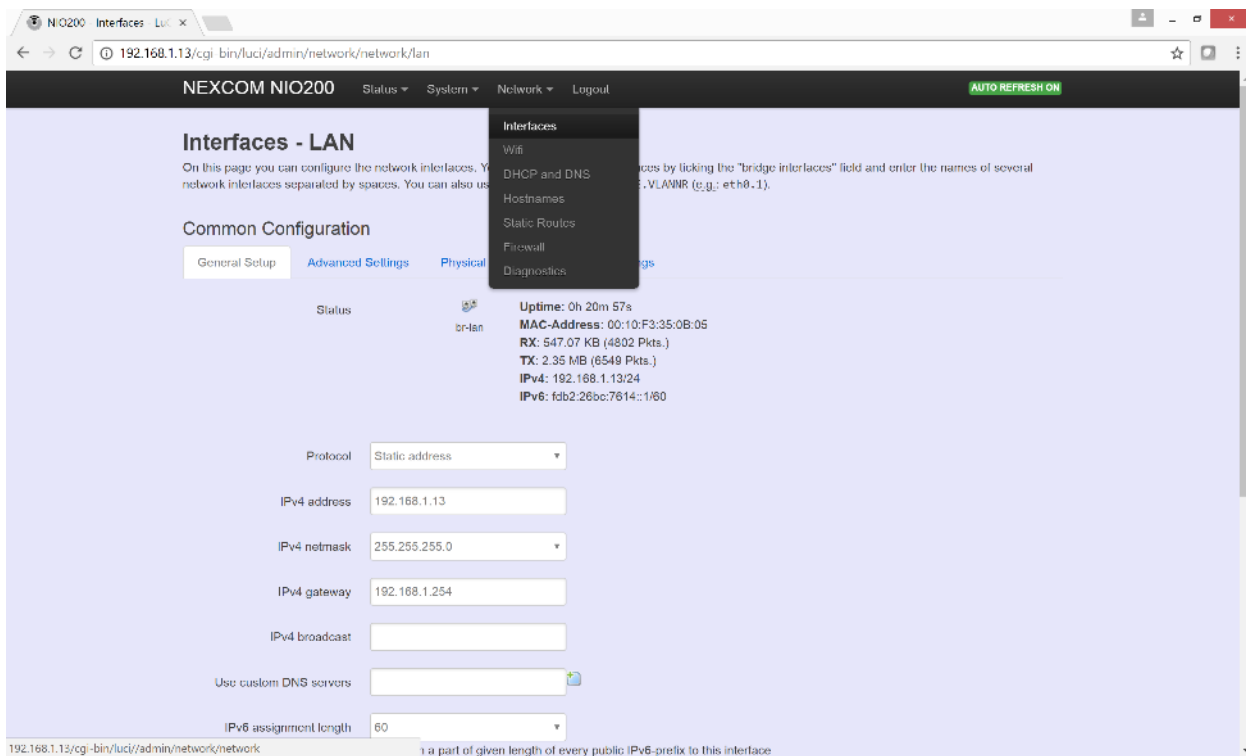
Once the communication has been established with the NIO200IAG, the user can log in the NIO200 Admin website to change the network configuration, including its IP address. To the access this website:

- In browser, open a connection to <http://192.168.1.1/> (or the user defined IP Address)
- Admin website requires authentication, the default *username* and *password* are *root* and *admin*.



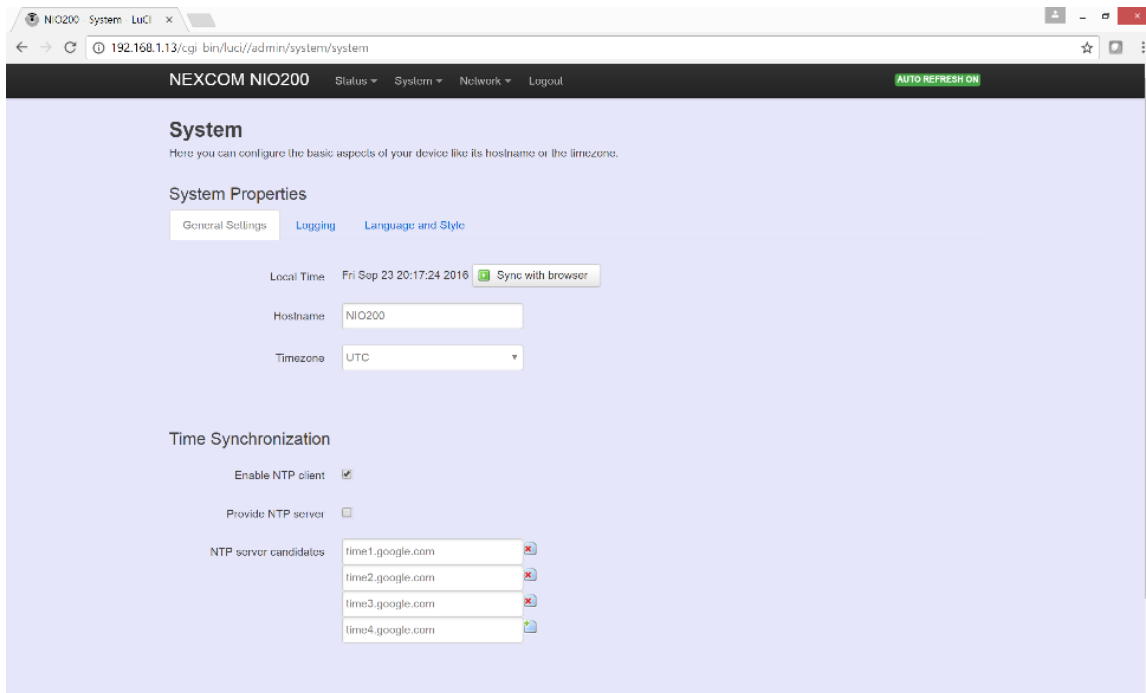
### 3.5 Configuring the IP Address

The IP Address can be changed in System page. The user must click “Save” or “Click Save and Apply” when done.



## 3.6 Configuring the NTP settings

The NTP Settings can be changed in System page. The user must click “Save” or “Click Save and Apply” when done. It is strongly recommended to have access to the Internet in order to allow the NTP client configured on the IAIG to synchronize with external time servers present online. ISA100.11a mandates the existence of a master source clock exists in each network. In this implementation this role is fulfilled by the System Manager through the NTP application running on the device.



## 3.7 Monitoring Control System

ISA100 specific network management and configuration takes place into the Monitoring Control System (MCS). Steps to access the MCS:

Step	Action
1.	Open the following URL: <a href="http://&lt;NIO200IAG_IP&gt;:8080/">http://&lt;NIO200IAG_IP&gt;:8080/</a> replacing <NIO200IAG_IP> with NIO 200IAG Gateway IP.
2.	Type the following user name and password in the <b>Login</b> fields: <ul style="list-style-type: none"><li>➤ Username: the username provided.</li><li>➤ Password: use the password provided.</li></ul>
3.	Click the <b>Login</b> button.

Login

User Name:

Password:

Login

## 4 Home page

Once the credentials are entered and access is granted, the browser will display the Device List by default.

The screenshot displays the NEXCOM Monitoring Control System web interface. The browser address bar shows the URL `192.168.1.11:8080/app/devicelist.html`. The page header includes the NEXCOM logo and the text "ISA 100 Wireless". The main content area is titled "Devices" and features a search bar for "EUI-64 Address" and "Device Tag", a "Show Devices" dropdown set to "Registered only", and a "Search" button. Below the search bar, a table lists the devices. The table has columns for "EUI-64 Address", "IPv6 Address", "Tag", "Revision", "Role/Model", "Status", and "Last read". The table shows 7 items, with the first item being the System Manager/SM. The left sidebar contains a "Network" menu with links to Dashboard, Topology, Devices, Network Health, Readings, Commands Log, Alerts, Troubleshooting, Bulk Transfer, and Set Country Code. Below this is a "Configuration" menu with links to Backbone Router, Gateway, System Manager, Device Management, Monitoring Host, MODBUS, Alert Subscription, Advanced Settings, Bulk Transfer, and System Status. At the bottom is an "Administration" menu with links to Device Firmware, System Upgrade, Custom Icons, and Custom Settings.

EUI-64 Address	IPv6 Address	Tag	Revision	Role/Model	Status	Last read
0000:0000:0010:0000	FE80:0000:0000:0000:4E7B:C0A3:010B	NEXCOMSystem_Mng	2.7.28	System Manager/ SM	FULL_JOIN	N/A
0000:0000:FFFF:0000	FE80:0000:0000:0000:4E7D:C0A3:010C	NEXCOM Backbone	B8_04.15.01	Backbone Router/ FREESCALE_VN310	FULL_JOIN	N/A
0022:FF00:0002:B170	FC00:0000:0022:FF00:0002:B170:0004:0009	Centers_B170	BK_04.11.01	10 Router Device/ FREESCALE_VN210	FULL_JOIN	2016-09-19 01:59:25
0102:0304:0506:0000	FC00:0000:0102:0304:0506:0000:0004:0000	TLV_00D	V2_00.00.10	10 Router Device/ WISA	FULL_JOIN	2016-09-19 01:58:54
0102:0304:0506:00B4	FC00:0000:0102:0304:0506:00B4:0004:004C	Centers_B64	V2_00.00.08	10 Router Device/ WISA	FULL_JOIN	2016-09-19 01:59:24
0102:0304:0506:00B5	FC00:0000:0102:0304:0506:00B5:0004:004D	Centers_0BB5	V2_00.00.F3	10 Router Device/ WISA	FULL_JOIN	N/A
0000:0000:0000:0000	FE80:0000:0000:0000:4E7C:7F00:0001	NEXCOM Gateway	2.7.33	Gateway/ GATEWAY	FULL_JOIN	N/A

\* using UTC Time


The user interface consists of two sections:

- The menus on the left, which allow you to navigate through the pages of the website
- The main section, which displays the contents of the selected page

# 5 Administration for the Network Devices

The Network section provides information about various network tasks accessed from the Monitoring Control System Webpage.

Monitoring Control System

  
The Intelligent Systems

ISA 100  
Wireless

Network

- Dashboard
- Topology
- Devices
- Network Health
- Readings
- Commands Log
- Alarms
- Trunk+Routing
- Bulk Transfers
- Set Country Code

Configuration

- Backbone Router
- Gateway
- System Manager
- Device Management
- Monitoring Host
- MCDBUS
- Alert Subscription
- Advanced Settings
- Bulk Transfers
- System Status

Administration

- Device Firmware
- System Upgrade
- Custom Icons
- Custom Settings

Devices

EUT-64 Address:

Device Tag:








Search

Show Devices: Registered only

Reset

Items per page: 20 out of total 7

1/1

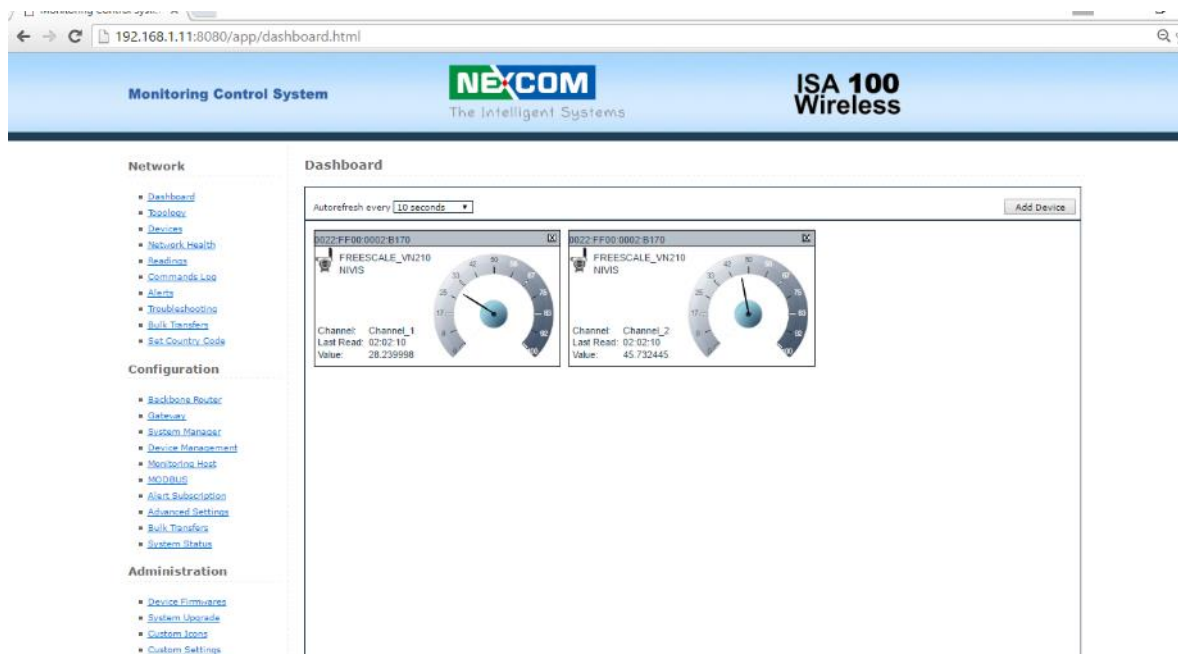
EUT-64 Address	IPv6 Address	Tag	Revision	Role/Model	Status	Last read
 0000:0000:0A12:00A0	FE80:0000:0000:0000:4E7B:CDAB:010B	NEXCOMSystem_Mng	2.7.28	System Manager/SM	FULL_JOIN	N/A
 0000:0000:FFFF:000C	FE80:0000:0000:0000:4E7D:CDAB:010C	NEXCOM Backbone	BB__04.15.01	Backbone Router/FREESCALE_VT0310	FULL_JOIN	N/A
 0032:FF00:0002:B170	FC00:0000:0022:FF00:0002:B170:0004:0009	Centers_B170	IK__04.11.01	3D Router Device/FREESCALE_VT0210	FULL_JOIN	2016-09-19 01:59:25
 0102:0304:0506:0000	FC00:0000:0102:0304:0506:000D:0004:000D	TLV_00D	V2__00.00.10	3D Router Device/WISA	FULL_JOIN	2016-09-19 01:58:54
 0102:0304:0506:00B4	FC00:0000:0102:0304:0506:00B4:0004:004C	Centers_BB4	V2__00.00.09	3D Router Device/WISA	FULL_JOIN	2016-09-19 01:59:24
 0102:0304:0506:00B5	FC00:0000:0102:0304:0506:00B5:0004:004D	Centers_00B5	V2__00.00.F3	3D Router Device/WISA	FULL_JOIN	N/A
 5000:0000:0000:0000	FE80:0000:0000:0000:4E7C:7F00:0001	NEXCOM Gateway	2.7.33	Gateway/GATEWAY	FULL_JOIN	N/A

using UTC time

## 5.1 Dashboard

The **Dashboard** page is a report zone that allows you to monitor reading variations for selected devices. The Dashboard consists in a series of panes added by the user, which provide a visual representation of the information published by selected devices on selected channels.

The information is refreshed automatically at regular intervals (10 seconds, 30 seconds, or 1 minute).



To delete a device from the dashboard, click ☒ in the top right corner of the pane. No confirmation is required for the system to delete the pane.

To add a device to the dashboard, perform the following steps:

Step	Action
------	--------


1. Click on the **Add Device** button.

## Step

## Action

2. The **Device** dialog box will open:


**Add device to dashboard**

**Device**  
Devices:   
Channels:   
Min value:   
Max value:   
Slot number:   
Gauge: 

Select a **Device** from the drop-down list.

3. Select the **Channel** that you wish to monitor from the drop-down list.
4. Type the desired gauge value range for the readings; if the selected values are out of range, a message on the pane will notify you.
5. Optional, select the **Slot number** (up to the current slot number); if you do not select a slot number, the system automatically assigns the next available slot.
6. Select the desired **Gauge** type.
7. Click **OK** to add the device to the dashboard.

### NOTE:

- You can also add a reading to the dashboard from the Device Details page: in the Information pane, click the **Add to dashboard (ATD)** icon  next to a reading.
- Up to 9 devices are supported in the dashboard.



## 5.2 Topology

The **Topology** page displays a graphical representation of the current network topology as well as allows users to view data about contracts and devices.



The system performs regular automatic updates of the topology information. When you load the page, the topology graph is generated based on the latest topology information available. The time of the last topology information update is indicated at the top of the page. To view the latest topology, press **Refresh** – this will generate a Request Topology command and will refresh the page.

In the **SubnetID** drop-down list located at the top of the topology window, select a subnet to view.

The registered devices are displayed on multiple levels represented as grey bands. The levels are numbered from 0 to n. The level number is indicated in the upper left corner of a level. The Gateway, the System Manager, and the Backbone Router are found on level 0. The level is given by the preferred clock source. A device is on level one, if its preferred clock source is a backbone router. A device is on level 2 if its preferred clock source is on level 1 and so on.

Communication-wise, field devices are linked to the backbone router, which is the central device in the network, either directly or via other devices. The backbone

router further relays to the Gateway, while the System Manager organizes the entire network. The field devices can have various sensors attached: temperature sensors, humidity sensors, etc.

The devices are identified in the topology by the last four characters of their EUI-64 address. For easier identification, the backbone router, the gateway and the system manager are identified with the abbreviations BBR, GW, and SM. The devices are placed within a level in the order of their EUI64 address. They can be moved freely within the range of their level by *drag-and-drop* to obtain better legibility of the topology.

In addition, they are represented by suggestive icons and against backgrounds of different colors, to distinguish their roles (also shown in the Devices legend at the bottom of the page):



- Gateway – purple background
- Backbone Router – blue
- System Manager – dark green
- IO/Router Devices – blue
- IO Devices – light green
- Routers - red

By positioning the cursor over an icon, you can view the tooltip, which includes the following details for a device:

- EUI-64 address
- device role
- subnet ID
- device tag
- manufacturer
- model

The available Topology page elements and viewing options are described in the following paragraphs.

### **Adjusting Width and Height**

You can adjust the size of the topology representation using the buttons  and  for height and width.

You can also adjust the height and width to the size of the Topology pane by clicking  , or revert to the original viewing settings by clicking  .

## Links

When the page is loaded, the **Links** option located above the topology graph is selected by default. The backbone router is also selected by default in the topology graph and the Preferred ClockSource links to it are displayed as **green** lines.

To view the Preferred ClockSource for a particular device, click on the device in the topology graph, or select the device in the drop-down list located on top of the Topology window. The MCS will display the device's link to its preferred ClockSource.

To view the Secondary ClockSource links for a selected device, check this option in the Links Legend. These links are displayed in **blue** in the topology graph.

To view the transmission links between a selected device and other, check the **Links** option in the Links Legend. The regular links are displayed in **black** in the topology graph.

To view all the other links formed between the network devices, check the **Show all links** option.

This option is unchecked by default.

To view the RSQI signal value for a device's links, check the Show signal quality/PER option. The signal quality value is displayed next to each link and is colored in the color of the respective link.

To view the packet error rate for a device:

- First check the Show signal quality/PER option
- In the Links Legend, select the desired ClockSource links to display (Preferred or Secondary, or both)
- Click the Get PER for selected device button located in the Links Legend. The PER is shown as a percentage next to the respective link

## Contracts

To view the contracts for a selected device:

Step	Action
------	--------

1. Check the **Contracts** option located at the top of the topology graph.

## Step

## Action

2. Choose a device by clicking on it in the topology graph or by selecting it in the **Devices** drop-down list located above the graph.
3. In the **Contracts** drop-down list you will view the selected device's inbound and outbound contracts with the System Manager and the Gateway. To show a contract on the graph, select it in the list.

The contract will be represented by a **green** line if it is periodic or by a **blue** line if it is aperiodic.

The Contracts legend located at the bottom of the Topology page also indicates how the types of contracts and links are represented.

### NOTE:

A device can have both a periodic and an aperiodic contract with the same SM or GW at the same time.



### Contract details

In addition, when you select a contract, information about the contract parameters will be shown in the Contract details section at the bottom of the page.

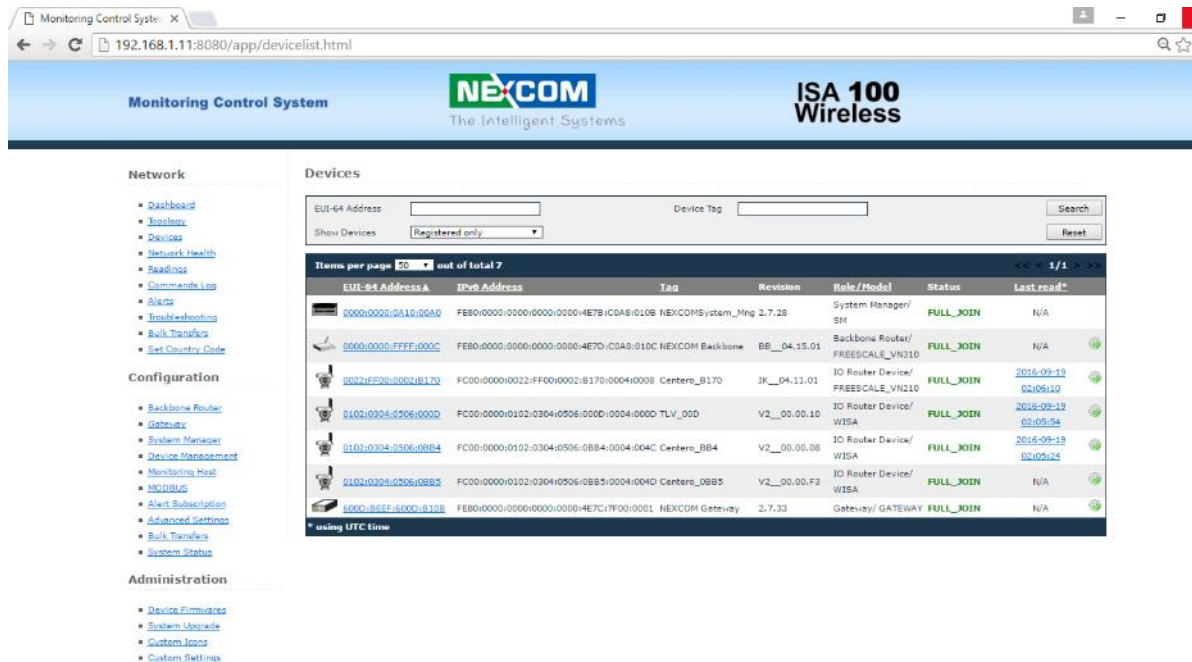
The contract information includes the following parameters:

- Contract ID – the contract identifier based on the contract owner
- Service type – can be periodic or aperiodic
- Source/destination device – the EUI64 address of the requester, and the destination device respectively
- Source / destination SAP –“0” is the default value for the DMAP on a device; “1” is the default value of a SMAP on the System Manager; the other values represent custom SAP's
- Activation time – the date and time when the contract was established
- Expiration time – the date and time when the contract terminates
- Priority – indicates the base priority for all messages sent using the contract
- NSDU Size – the packet size at network layer
- Reliability – the requested reliability for delivering the transmitted packets to the destination
- Period – identifies the desired publishing period, for periodic contracts
- Phase – identifies the desired phase (within the publishing period) of publications, for periodic contracts
- Deadline – the maximum end-to-end transport delay desired, in periodic communication
- Committed Burst – for long-term aperiodic communication; it specifies the bandwidth:
  - A positive value specifies the packets transmitted per second; e.g. a committed burst of 2 indicates that two packets per second are guaranteed
  - A negative value specifies the number of seconds per packet; e.g. a committed burst of -15 indicates that a packet transmitted every 15 seconds is guaranteed
- Excess Burst – for short-term aperiodic communication; it has the same significance as the committed burst, but is only used in exceptional situations where aggressive communication is needed on a short-term
- MaxSendWindow – the maximum number of client requests that may be simultaneously awaiting a response, in the case of aperiodic communication



## 5.3 Devices

The devices page features the list of devices that exist in the network and a search form that enables you to search devices based on their EUI-64 address, tag and/or state.



## Search devices

When the device page is loaded, the registered devices are displayed by default.

Step	Action
Search by EUI-64 address	

1. To search a device by its EUI-64 address, type the address in the **EUI-64 Address** input field,  
or  
For a partial search:
  - Type part of the EUI-64 address in the **EUI-64 Address** input field
  - Select the desired state from the **Show Devices** drop-down list

Step	Action
------	--------

2. Click **Search**. The system will retrieve all the devices whose EUI-64 addresses contain the characters provided by the user.

**NOTE:** To delete the search parameters, click **Reset**.

### Search by device tag

1. A tag is a custom description that you can assign to a device in order to facilitate identification of that device in the plant. One tag can be assigned to a single device.

To search for devices based on their tag, type the tag in the **Device Tag** input field.

2. Click **Search**.

**NOTE:**

- The tag field is case sensitive.
- To delete the search parameters, click **Reset**.

### Search by device state only

1. To display devices based on their state at a given time, select the desired state from the **Show Devices** drop-down list. The device list will update automatically.

A device can be in only one of the following states at a given moment in time:

- Registered – the device has successfully joined the network and is ready to operate
- Joining process – the device has been provisioned and is attempting to join the network
- Unregistered – the device has lost connection with its neighbors in the network


### Device List

The **Device list** shows the network devices in a table, one item per line, with main information about each **logical** device:

- EUI-64 address (the MAC address),



- IPv6 address
- Tag – the device tag
- Revision – the firmware version available on the device
- Role (Gateway, System Manager, Backbone Router, Field Router) and model (manufacturer information)
- Status (“Full Join” for registered devices; “Joining” for joining devices; “Not Joined” for unregistered devices), and
- Last Read (the date and time of the last reading from the device) and a link to the Readings page for the device in question.

In addition, the device list provides a quick link  to the Run Commands page for that specific device.


When you load the page, the registered devices are displayed by default. To view unregistered or joining devices, select the corresponding option in the Show Devices drop-down list.

The total number of items in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number of items displayed in a page is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table.

The last time the page was refreshed is also indicated at the top of the page. The page does not refresh automatically; therefore you must click **Refresh** to update it.

### **Delete a device**

In the devices page you have the option of deleting an unregistered device. When you delete a device, it will be removed from the network and any related data, including previous readings, will be deleted from the database.

To delete the device, click the icon  located next to the device. The system will require confirmation to perform the action. Click **OK** to delete the device or **Cancel** to abort the action.

## 5.4 Device Details

In this page you can see all the information available for the selected device and perform device-specific commands. The page is accessed by clicking on the device **EUI-64 address** in the device list.

The page is organized into seven tabbed panes by types of information and also features a Back button to allow you to quickly revert to the Devices page, as well as an indication of when the last page was updated and a Refresh button (where applicable) that enables you to retrieve up-to-date information in the specific page.

### Information

The Information pane displays general as well as activity specific information about the device. When the page is loaded, it shows the latest information available. To update the information, click **Refresh**.

The following details are shown in addition to those already indicated in the device list:

- Manufacturer – the name of the device manufacturer
- Revision – the radio firmware version
- Subnet ID – the ID of the subnet that includes the device
- Power Supply Status – represented as a battery with the following colors:
  - green, when the device is line powered
  - blue, when the device is battery powered, and the remaining capacity of the battery is greater than 75%
  - yellow, when the device is battery powered, and the remaining capacity of the battery is between 25% and 75%
  - red, when the device is battery powered, and the remaining capacity of the battery is less than 25%
- Data transmission statistics – the number of transmitted/received packages and the number of failed transmissions/receptions
- Process values – the parameters measured by the device.

## Device Details

**Information** Settings Registration Log Neighbors Health Schedule Report Channels Statistics Run Commands

**EUI-64 Address:** 0022:FF00:0002:B174  
**IPv6 Address:** FC00:0000:0022:FF00:0002:B174:0003:000C  
**Subnet ID:** 3  
  
**Device Role:** IO Router Device  
**Device Status:** FULL\_JOIN  
**Last Read (UTC):** 2016-08-15 20:32:10  
**Power Supply Status:**  
**Energy Left:** N/A

**Manufacturer:** NIVIS  
**Model:** FREESCALE\_VN210  
**Revision:** IK\_\_04.11.01  
  
**DPDUsTransmitted:** 301  
**DPDUsReceived:** 130  
**DPDUsFailedTransmission:** 2  
**DPDUsFailedReception:** 0

Back

Last refreshed on: 2016-08-15 20:29:54 (153 seconds ago) Refresh

Items per page 10 out of total 4 << < 1/1 > >>

Name	M.U.	Format	TSAP ID	Object ID	Attribute ID	Index1	Index2	ATD
Channel_1	Channel_UM_1	Float32	2	129	5	0	0	
Channel_2	Channel_UM_2	Float32	2	129	6	0	0	
Channel_3	Channel_UM_3	Float32	2	129	7	0	0	
Channel_4	Channel_UM_4	Float32	2	129	8	0	0	

## Process values

The process values are displayed in a table with the following related information:

- Name - the process value name
- M.U. - the unit of measurement for the process value
- Format - various formats are possible, defining the value range of the measured parameter: int8, uint8, int16, uint16, int32, uint32, float32
- TSAP ID
- Object ID
- Attribute ID, and
- Two indices.

The total number of items in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number of items displayed in a page is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table.

## Settings

The settings reflect the current operation of the ISA100.11a stack on a device.

The type of information displayed in this pane includes neighbor details, routes and graphs:

## Device Details

Information	Settings	Registration Log	Neighbors Health	Schedule Report	Channels Statistics	Run Commands
EUI-64 Address: 0022:FF00:0002:B174						Back
IPv6 Address: FC00:0000:0022:FF00:0002:B174:0003:000C						
Last refreshed on (UTC): 2016-08-15 20:32:50 (18 seconds ago)						Refresh
Neighbors			Graphs			
Address 64	Is Clock Source	Signal Quality	Graph ID	Neighbor Address 64		
0000:0000:FFFF:000B	Preferred	N/A (0)	1	0000:0000:FFFF:000B		
0102:0304:0506:0BB6	No	N/A (0)	4	0102:0304:0506:0BB6		
Routes						
Route ID	Alternative	Selector	Forward Limit	Route Element		

## Neighbors

The Neighbors section lists the registered neighbors of the selected device as well as indicates their signal quality and whether they are clock sources for the selected device.

A clock source neighbor can have one of the following roles:

- Preferred clock source – the reference clock source for the selected device.
- Secondary clock source – a backup clock source that becomes preferred, when the reference clock source is not available.

Multiple neighbors may be designated as clock sources for a selected device.

The Signal Quality column displays the received signal quality indicator (RSQI) values and their associated labels, as shown in the following table:

RSQI	Signal Quality
1-63	Poor signal
64-127	Fair signal
128-191	Good signal
192-255	Excellent signal

## Graphs

The Graphs section lists all the graphs that include the selected device, with the specific graph ID's and neighbor addresses within each graph.

Graph 1 is the inbound graph, while the other graphs are outbound graphs.

## Routes

The Routes section lists the routes of which the source is the selected device.

Routes can be classified into:

- Routes based on graphs, established between two field devices or a field device and the Backbone Router
- Hybrid routes – established between the Backbone Router and a joined device (the destination of the route) for which an outbound graph has not been created yet. Hybrid routes consist of the node's parent's outbound graph and the destination node.

Routes are listed in a table displaying the following information:

- Route ID – route identification data; ID's are given in the order of creation of the routes. Route 1 is the default route established between field devices and the Backbone Router.
- Alternative – a number ranging from 0 to 3 that enables you to differentiate between routes based on their source and destination:
  - If the alternative is 0, the route is based on a contract requested by the System Manager or the Gateway. This feature will be available in future releases.
  - If the alternative is 1, the route is established between two field devices
  - If the alternative is 2, the Backbone Router is the source of the route and a field device is the destination.
  - If the alternative is 3, this is the device's default route (Route 1) to the Backbone Router.
- Selector – identifies the destination of the route; the selector varies based on the value of the alternative:
  - If the alternative is 0, the selector indicates the contract ID and the address of the source (SM or GW)
  - If the alternative is 1, the selector field indicates the contract ID.
  - If the alternative is 2, the selector field indicates the address of the destination device.
  - If the alternative is 3, the selector is null.
- Forward Limit – the maximum number of nodes that a route can include

- Route Element – indicates the ID of the graph that stands at the basis of the route, or the graph ID and the destination's address, for hybrid routes.

To view the updated device settings, click the **Refresh** button. The **Request Topology** and **Get Contracts and Routes** commands will be sent to the System Manager.

When the command is generated, a message at the bottom of the screen will indicate that the device information is refreshing.

## Registration Log

The registration log displays the registration history for the selected device, at different dates and times, commonly known as timestamps.

### Device Details

Information Settings **Registration Log** Neighbors Health Schedule Report Channels Statistics Run Commands

EUI-64 Address: 0022:FF00:0002:B174  
IPv6 Address: FC00:0000:0022:FF00:0002:B174:0003:000C

Start Time: 8/15/2016 2:47 PM End Time: : AM Search

Registration Status: All \*\* all registration entries for current device Delete\*\*

Items per page: 10 out of total 2 << < 1/1 > >>

Timestamp*▲	Device Status
2016-08-15 19:51:12	SEC_CNFRM_Req
2016-08-15 19:51:57	FULL_JOIN

\* using UTC time

Use the Search functionality to view the behavior of the device over a specific period time:

- Choose the status you wish to view from the **Registration Status** drop-down list
- Optional, fill in the **Start Time** and the **End Time** fields, and then click **Search**.

The results are displayed in a table that indicates the timestamp and the device status at that specific timestamp. A device can have one of the following statuses at a given moment:

- SEC\_JOIN\_Req – the security join request was received by the System Manager
- SEC\_JOIN\_Rsp – a security join response was sent to the device

- NETWORK\_Req – the network join request was received by the SM
- NETWORK\_Rsp – the network join response was sent to the device
- CONTRACT\_Req – the join contract request was received by the SM
- CONTRACT\_Rsp – the join contract response was sent to the device
- SEC\_CNFRM\_Req – the security join confirmation was received by the SM
- SEC\_CNFRM\_Rsp – the security join confirmation response was sent to the device
- FULL\_JOIN – the device is joined and configured and all information about it is available
- NOT\_JOINED – the device is not joined

The total number of items in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number of items displayed in a page is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table.

## Neighbors Health

This pane provides a communication health report about the selected device's neighbors.

### Device Details

Information	Settings	Registration Log	Neighbors Health	Schedule Report	Channels Statistics	Run Commands
EUI-64 Address: 0022:FF00:0002:B174						Back
IPv6 Address: FC00:0000:0022:FF00:0002:B174:0003:000C						
Last refreshed on (UTC): 2016-08-15 20:47:53 (10 seconds ago)						Refresh
Items per page 10 out of total 2						<< < 1/1 > >>
Neighbor▲	Link status	Transmitted/Failed	Received/Failed	Signal Strength(dBm)	Signal Quality	
0000:0000:FFFF:000B	Available	381/4	114/0	-37	Excellent (237)	
0102:0304:0506:0BB6	Available	23/0	47/0	-80	Fair (64)	

The report includes:

- Neighbor identification information - the EUI-64 address
- The timestamp of the report request
- A general link status:

- Available – if the neighbor is available for communication
  - Unavailable – if the neighbor is unavailable for communication
- Communication health information:
- The number of DPDU's transmitted to the neighbor and the number of failed transmission attempts
  - the number of DPDU's received from the neighbor and the number of failed receptions from the neighbor
- The neighbor signal strength (measured in dBm) and
- The signal quality (for the RSQI ranges and associated labels)

The total number of items in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number of items displayed in a page is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table.

## Schedule Report

The schedule report pane provides information about time slot and channel allocation for the selected device.

## Superframes and links

The active Superframes that the device uses for communication are listed in the page along with information regarding size (the number of time slots), start time, and the number of links allocated on each Superframe.

### Device Details

Information
Settings
Registration Log
Neighbors Health
Schedule Report
Channels Statistics
Run Commands

EUI-64 Address: 0022:FF00:0002:B174
IPv6 Address: FC00:0000:0022:FF00:0002:B174:0003:000C

Last refreshed on (UTC): 2016-08-15 20:48:21 (7 seconds ago)

Items per page 10 out of total 4
<< < 1/1 > >>

Superframe ID	Time Slots	Start Time*	Links
1	3000	2016-08-15 20:47:27	<a href="#">1</a>
2	3000	2016-08-15 20:47:27	<a href="#">2</a>
4	3000	2016-08-15 20:47:27	<a href="#">4</a>
5	5700	2016-08-15 20:47:27	<a href="#">1</a>

\* using UTC time

RF Channels: No records !

In use
Blacklisted
Idle



Clicking on the number of links will display a new page with link related information for each individual link allocated on the selected Superframe, as shown in the following screen:

#### Device Details

Information
Settings
Registration Log
Neighbors Health
Schedule Report
Channels Statistics
Run Commands

EUI-64 Address: 0022:FF00:0002:B174
Device Type: IO Router Device
Superframe ID: 2

Neighbor device ..... All
Direction ..... All
Link type ..... All

Items per page 10 out of total 9

Neighbor Device	Slot Index	Link Period	Slot Length	Channel No	Direction	Link Type
FFFF:FFFF:FFFF:FFFF	1	500	10464	0	Reception	Periodic Management Communication
0102:0304:0506:0BB6	59	500	10464	0	Transmission	Periodic Management Communication
0102:0304:0506:0BB6	159	500	10464	0	Transmission	Periodic Management Communication
0102:0304:0506:0BB6	259	3000	10464	0	Transmission	Periodic Management Communication
FFFF:FFFF:FFFF:FFFF	359	500	10464	0	Reception	Periodic Management Communication
0102:0304:0506:0BB6	459	1000	10464	0	Transmission	Periodic Management Communication
0000:0000:FFFF:000B	499	500	10464	6	Transmission	Periodic Data Communication
0000:0000:FFFF:000B	601	3000	10464	6	Transmission	Periodic Management Communication
0000:0000:FFFF:000B	801	1000	10464	6	Transmission	Periodic Management Communication

RF Channels: 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

In use Blacklisted Idle

The following details are shown:

- Neighbor – the EUI-64 address of the neighbor or the broadcast address FFFF:FFFF:FFFF:FFFF (used only for advertisements and receive links)
- Slot index – the ID of the slot within the Superframe
- Link period – the periodicity of a link (measured in No. of slots) within a Superframe cycle
- Slot length – expressed as a multiple of  $2^{-20}$  seconds
- Channel number
- Direction – reception or transmission
- Link type, which can be:
  - aperiodic data communication
  - aperiodic management communication
  - periodic data communication
  - periodic management communication

You can use the search form on the top of the page to sort links based on neighbor device, the link type of the direction of the communication.

In addition, in both the Superframes and Links tables you can sort the information by the number of items listed per page. The default number of records displayed in a page is 10. Paging controls at the bottom of the table enable you to navigate through the pages of the table.

When the pages are loaded, the latest information available is shown. To update the information, click **Refresh**.

**RF Channels**

The channels of the device are represented at the bottom of the pane. The channels that are clear for communication are highlighted in blue, the unused channels are highlighted in gray, while blacklisted channels are highlighted in red. Channel 26 has been disabled by default for purposes of compliance in certain countries.

**Channel Statistics**

This pane displays statistical information about CCA backoffs per channel.

**Device Details**

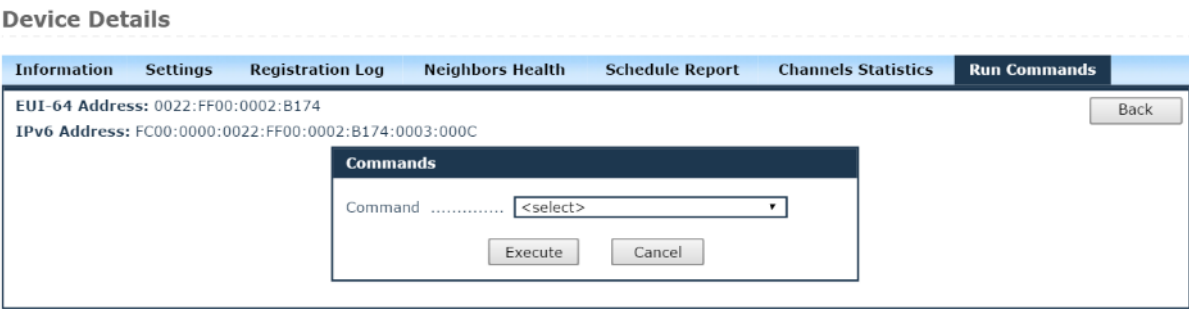
Information	Settings	Registration Log	Neighbors Health	Schedule Report	Channels Statistics	Run Commands
EUI-64 Address: 0022:FF00:0002:B174						Back
Device Role: IO Router Device						
Last refreshed on (UTC): 2016-08-15 20:48:49 (13 seconds ago)						Refresh
Channel No		Value				
11		0				
12		0				
13		0				
14		0				
15		0				
16		0				
17		0				
18		0				
19		0				
20		0				
21		0				
22		24				
23		0				
24		1				
25		0				
26		0				

The information is presented in a table, with the value column expressing the percentage (0% to 100%) of aborted transmissions for each channel.

To update the information, click **Refresh**.

**Run Commands**

This pane enables you to perform device-specific commands.



To go to a specific command, select it from the Commands drop-down list. After you generate the command, a message at the bottom of the screen will indicate its status ("Command sent successfully", "Command sent error"). The tracking number of the command is also indicated, together with a link to the Commands Log, where you can view the results of the command.

The following types of commands are available:

## Read Value

This command is available only for field devices and enables you to read a value on a particular channel of the selected device.

### Device Details

The screenshot shows the 'Device Details' page with the 'Run Commands' tab selected. The page header includes tabs for Information, Settings, Registration Log, Neighbors Health, Schedule Report, Channels Statistics, and Run Commands. The main content area displays the device's EUI-64 Address (0022:FF00:0002:B174) and IPv6 Address (FC00:0000:0022:FF00:0002:B174:0003:000C). A 'Back' button is visible in the top right corner. A 'Commands' dialog box is open, showing the 'Read Value' command selected. The 'Process Value' is set to 'Channel\_1' and the 'Committed Burst' is set to '-15'. 'Execute' and 'Cancel' buttons are at the bottom of the dialog box.

To generate the command, select the process value for which to request a reading and click *Execute*. The returned value will be displayed in the Readings page, in engineering units under the Value column as well as in the Command Log, under the Response column.

**NOTE:** When the device is unregistered, the Run Commands tab is unavailable.

## Reset Device

This command resets the firmware on the specific device.

Three types of resets can be performed on a device:

- Warm Restart – performs a software reset; as a consequence, the device will unregister and re-register
- Restart as provisioned – resets the device while keeping provisioning information
- Reset to factory defaults – deletes the provisioning information and resets the device to its manufacturing settings; the device must be re-provisioned in order to be able to join the network

## Device Details

Information	Settings	Registration Log	Neighbors Health	Schedule Report	Channels Statistics	Run Commands
<b>EUI-64 Address:</b> 0022:FF00:0002:B174 <b>IPv6 Address:</b> FC00:0000:0022:FF00:0002:B174:0003:000C						Back
<div><b>Commands</b></div> <div>Command ..... <input type="text" value="Reset Device"/></div> <div>Restart Type ..... <input type="text" value="&lt;select&gt;"/></div> <div><input type="button" value="Execute"/> <input type="button" value="Cancel"/></div>						

This command is available for all network devices with two exceptions:

- The command cannot be performed on the System Manager
- The **Reset to factory defaults** option is not available on the gateway

## Read Object Attribute

Using this command you can read attributes from an object on the selected device.

## Device Details

Information	Settings	Registration Log	Neighbors Health	Schedule Report	Channels Statistics	Run Commands
<b>EUI-64 Address:</b> 0022:FF00:0002:B174 <b>IPv6 Address:</b> FC00:0000:0022:FF00:0002:B174:0003:000C						Back
<div><b>Commands</b></div> <div>Command ..... <input type="text" value="Read Object Attribute"/></div> <div>TSAP ID (port) ..... <input type="text" value="2"/></div> <div>Object ID ..... <input type="text" value="129"/></div> <div>Attribute ID ..... <input type="text" value="4"/></div> <div>Index1 ..... <input type="text" value="0"/></div> <div>Index2 ..... <input type="text" value="0"/></div> <div>Committed Burst ..... <input type="text" value="-15"/></div> <div><input type="button" value="Execute"/> <input type="button" value="Cancel"/></div>						

To read an attribute, type in the UAP specific **TSAP ID (port)**, the **Object ID**, and the **Attribute ID** you wish to read. Then click **Execute**.

**NOTE:** The values of the two indices are 0 by default and the value of the Committed Burst field is -15 by default.

The command returns the content of the attribute, which will be displayed in hex format in the Response column of the Commands Log page.

## Write Object Attribute

This command enables you to write/edit a value to an object on the selected device. Only certain attributes are editable.

Device Details

InformationSettingsRegistration LogNeighbors HealthSchedule ReportChannels StatisticsRun Commands

EUI-64 Address: 0022:FF00:0002:B174  
IPv6 Address: FC00:0000:0022:FF00:0002:B174:0003:000C

Back

Commands

Command ..... Write Object Attribute ▾

TSAP ID (port) .....  
Object ID .....  
Attribute ID .....  
Index1 ..... 0  
Index2 ..... 0  
Values (HEX) .....  
Committed Burst ..... -15

ExecuteCancel

To write the attribute, type in the **TSAP ID (port)**, the associated **Object ID**, and the **Attribute ID** you wish to write or edit. Then type the desired hex value(s) in the Values input field. And click **Execute**.

**NOTE:** The values of the two indices are 0 by default and the value of the Committed Burst field is -15 by default.

### Execute Object Attribute

The execute service is used to execute a network visible method on an object on the selected device.

#### Device Details

InformationSettingsRegistration LogNeighbors HealthSchedule ReportChannels StatisticsRun Commands

EUI-64 Address: 0022:FF00:0002:B174  
IPv6 Address: FC00:0000:0022:FF00:0002:B174:0003:000C

Back

Commands

Command .....Execute Object Method

TSAP ID (port) .....  
Object ID .....  
Method ID .....  
Index1 .....0  
Index2 .....0  
Details (HEX) .....  
Committed Burst .....-15

ExecuteCancel

To execute the method, type in the **TSAP ID**, the associated **Object ID**, and the **Method ID** you wish to execute. Provide the method details in hex format in the Details input field. Click **Execute**.

**NOTE:** The values of the two indices are 0 by default and the value of the Committed Burst field is -15 by default.

## 5.5 Network Health

The Network Health page provides a communication health report at network level.

The page consists of two sections containing network summary statistics and device-specific communication health information.

The screenshot shows the NEXCOM Monitoring Control System interface. The top header includes the NEXCOM logo and 'ISA 100 Wireless'. The left sidebar contains navigation links for Network, Configuration, and Administration. The main content area is titled 'Network Health' and displays the following summary statistics:

- ID: 1
- Devices Count: 5
- Join Count: 5
- Current Date (UTC): 2016-09-19 02:07:14
- Start Date (UTC): 2016-09-18 16:13:24
- DPDUs Sent: 11509
- DPDUs Lost: 244
- GPDU Latency: 50%
- GPDU Path Reliability: 100%
- GPDU Data Reliability: 100%
- Network Type: 0

The averaging interval for GPDU statistics is 600 sec. The last refresh was on UTC 2016-09-19 02:07:16 (-94 seconds ago). Below the summary is a table with 8 columns: EUI-64 Address, Start Date\*, DPDUs Sent, DPDUs Lost, GPDU Latency (%), GPDU Path Reliability (%), GPDU Data Reliability (%), and Join Count. The table contains 5 rows of data for different devices.

EUI-64 Address	Start Date*	DPDUs Sent	DPDUs Lost	GPDU Latency (%)	GPDU Path Reliability (%)	GPDU Data Reliability (%)	Join Count
0000:0000:FFFF:000C	2016-09-18 16:14:47	1884	0	0	0	0	1
0022:FF00:0000:8170	2016-09-18 16:17:37	4551	83	0	100	100	1
0102:0304:0506:000D	2016-09-18 16:22:28	1810	25	0	0	0	1
0102:0304:0506:08B4	2016-09-18 16:16:47	2012	65	100	100	100	1
0102:0304:0506:08B5	2016-09-18 16:22:23	1252	71	0	0	0	1

\* using UTC time

In the network summary section the following information is indicated:

- Network ID and Network Type - network identification data (where applicable)
- Devices Count – the total number of registered devices, including the Backbone Router
- Join count – the total number of joins of all the devices in the network
- Current Date – the present time
- Start Date – the date and time the System Manager application was started
- Transmission and reliability statistics, based on the summary report per device
- The averaging interval for GPDU statistics, reported in seconds

The device communication report section consists of a table displaying the following information for each device:



- EUI-64 Address – the network address of the device
- Start Date – the date and time of the device's first join
- DPDU's Sent – the total number of packets sent by the device
- DPDU's Lost – the total number of packets sent by the device which failed to reach destination
- GPDU Latency – the percentage of scheduled GPDU's that arrive later than expected
- GPDU Path Reliability – the percentage of GPDU's transmitted successfully on a primary path
- GPDU Data Reliability – the percentage of successful GPDU's (transmit GPDU's that are transferred correctly on the first attempt plus receive GPDU's that pass integrity checks)
- Join Count – the total number of joins per device

The total number of items in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number of items displayed in a page is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table. The last time the page was refreshed is also indicated in the page. To update the information, click **Refresh**.

## 5.6 Readings

In this page you can view the readings received from devices, which are generated either on demand by Read Value commands or by automatic Publish/Subscribe commands. The readings can be filtered by **Device**, **Process Value**, or **Reading Type** (Publish/Subscribe or On Demand).

Monitoring Control System

NEXCOM The Intelligent Systems

ISA 100 Wireless

Network

- Dashboard
- Topology
- Devices
- Network Health
- Readings
- Commands Log
- Alarms
- Troubleshooting
- Bulk Transfers
- Set Country Code

Configuration

- Backbone Router
- Gateway
- System Manager
- Device Management
- Monitoring Host
- MODBUS
- Alert Subscription
- Advanced Settings
- Bulk Transfers
- System Status

Administration

- Device Firmware
- System Upgrade
- Custom Joins
- Custom Settings

Readings

Device: All Process Value: All Search Export

Items per page: 10 out of total 7

EUI-64 Address	Timestamp*	Channel Name	Value	Unit Of Measurement
0022:FF00:0002:8170	2016-09-19 02:07:40	Channel_1	28.199997	Channel_UM_1
0022:FF00:0002:8170	2016-09-19 02:07:40	Channel_2	45.727745	Channel_UM_2
0022:FF00:0002:8170	2016-09-19 02:07:40	Channel_3	15.388794	Channel_UM_3
0022:FF00:0002:8170	2016-09-19 02:07:40	Channel_4	0.019536	Channel_UM_4
0102:0304:0506:08B4	2016-09-19 02:07:24	Channel_1	35494.000000	Channel_UM_1
0102:0304:0506:0000	2016-09-19 02:06:54	Channel_1	0.073450	Channel_UM_1
0102:0304:0506:0000	2016-09-19 02:06:54	Channel_2	3.092407	Channel_UM_2

\* using UTC time

To search for readings, select the desired device, process value and reading type as shown in the screen above, and click **Search**. The results are displayed in a table that contains the following information for each reading:

- Device EUI-64 address (MAC address of the device that reported the reading)
- Timestamp (date and time of the reading)
- Channel Name (the process value name)
- Value (the value received on that particular reading) – shown in engineering values
- Unit of Measurement (if applicable)
- Reading Type

The total number of items in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The

default number of items displayed in a page is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table.

From this page you can also save the search results into a Microsoft Excel CSV file, by clicking **Export**.

## 5.7 Commands Log

In this page you can view all the commands issued on the registered devices in the system. The commands can be filtered by **Device**, **Command** (type), or **Command Status** (New – command posted in database, Sent – command sent to device, Responded – device responded successfully to the command, Failed – command failed to execute).

Monitoring Control System

NEXCOM The Intelligent Systems

ISA 100 Wireless

Network

- Dashboard
- Topology
- Devices
- Network Health
- Readings
- Commands Log
- Alerts
- Troubleshooting
- Bulk Transfers
- Get Country Code

Configuration

- Backbone Router
- Gateways
- System Manager
- Device Management
- Monitoring Host
- MODBUS
- Alert Subscription
- Advanced Settings
- Bulk Transfers
- System Status

Administration

- Device Firmware
- System Upgrade
- Custom Icons
- Custom Settings

Commands Log

Device: All Command Status: All Search

Command: All Show system generated commands Export

Items per page 10 out of total 5

Tracking No.	EUI-64 Address	Command	Parameters	Status	Posted Time*	Response Time*	Response
827	600D-BEEF-600D-B10E	Network Health Report		Responded	2016-09-19 02:05:30	2016-09-19 02:07:16	Success
826	600D-BEEF-600D-B10E	Network Health Report		Responded	2016-09-19 02:05:27	2016-09-19 02:07:14	Success
825	0000-0000-0A10-00A0	Neighbor Health Report	Device ID: 0002-0304-0506...	Responded	2016-09-19 02:02:45	2016-09-19 02:04:32	Success
824	0000-0000-0A10-00A0	Request Topology		Responded	2016-09-19 02:02:22	2016-09-19 02:04:08	Success
823	0000-0000-0A10-00A0	Neighbor Health Report	Device ID: 0002-FF00-0002...	Responded	2016-09-19 02:02:03	2016-09-19 02:03:50	Success

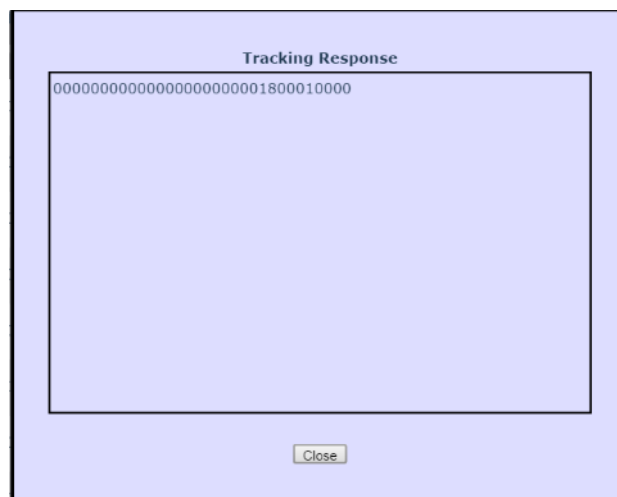
\* using UTC time

To search for commands, select the desired device, command and command status and click **Search**. The results will be displayed in a table, as shown in the screen above, with the following information for each command:

- Tracking Number (internal ID of the command),
- EUI-64 address (MAC address of the command destination device),
- Command (name of the executed command)
- Parameters (description of the parameters chosen for the command, if applicable)
- Status (current status of the command)
- Posted Time (date and time when the command was generated)
- Response Time (date and time when the command was responded successfully or not)

- Response (the response for the issued command if the command was responded successfully or the error reason if the command failed), which can consist of:
  - The measured value expressed in engineering units for the Read Value command
  - The hex value for Read/Execute Object Attribute commands
  - The mention success for all the other types of commands executed on devices

If the length of the response exceeds the size of the Response cell, click on the response link to open the **Tracking Response** form and view the full response:



Given the large number of commands generated automatically by the system at regular intervals, these commands are hidden by default. To view them, check the **Show system generated** commands option in the Search dialog and click **Search**.

The total number of items in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number of items displayed in a page is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table.

From this page you can also save the search results into a Microsoft Excel CSV file, by clicking **Export**.

## 5.8 Alerts

The Alerts page enables you to view alarms and events generated by devices.

Alerts consist in application messages that advise or warn the recipient of the presence of an impending or existing situation of interest.

Monitoring Control System

NEXCOM The Intelligent Systems

ISA 100 Wireless

Network

- Dashboard
- Topology
- Devices
- Network Health
- Readings
- Commands Log
- Alerts
- Troubleshooting
- Bulk Transfers
- Get Country Code

Configuration

- Backbone Router
- Gateways
- System Manager
- Device Management
- Monitoring Host
- MODBUS
- Alert Subscription
- Advanced Settings
- Bulk Transfers
- System Status

Administration

- Device Firmware
- System Upgrade
- Custom Icons
- Custom Settings

Alerts

Device: All Category: All Search

Priority: All Class: All Export

Start Time: 9/18/2016 12:00 AM End Time: 12:00 AM

Items per page: 10 out of total 1063

EUI-64 Address	Tsap ObjID	Time	Class	Direction	Category	Type	Priority	Value
0022:FF00:0002:B170	0	4	2016-09-19 02:07:57	Event	N/A	Communication Diagnostic	1	7-Medium 00
0102:0304:0506:08B4	0	4	2016-09-19 02:07:24	Event	N/A	Communication Diagnostic	1	7-Medium 00
0000:0000:FFFF:000C	0	4	2016-09-19 02:06:17	Event	N/A	Communication Diagnostic	1	7-Medium 00
0000:0000:FFFF:000C	0	4	2016-09-19 02:03:00	Event	N/A	Communication Diagnostic	1	7-Medium 00
0000:0000:FFFF:000C	0	4	2016-09-19 01:59:44	Event	N/A	Communication Diagnostic	1	7-Medium 00
0102:0304:0506:000D	0	4	2016-09-19 01:59:21	Event	N/A	Communication Diagnostic	1	7-Medium 00
0102:0304:0506:08B5	0	4	2016-09-19 01:57:49	Event	N/A	Communication Diagnostic	1	7-Medium 00
0000:0000:FFFF:000C	0	4	2016-09-19 01:56:29	Event	N/A	Communication Diagnostic	1	7-Medium 00
0000:0000:FFFF:000C	0	4	2016-09-19 01:53:12	Event	N/A	Communication Diagnostic	1	7-Medium 00
0022:FF00:0002:B170	0	4	2016-09-19 01:52:56	Event	N/A	Communication Diagnostic	1	7-Medium 00

\* using UTC time

Two types (classes) of alerts are supported in accordance with the ISA100.11a specification:

- Events – indicates that something happened with the device
- Alarms – indicates that a device has transitioned to an abnormal state, or has returned to normal from an abnormal state. An alert is sent to describe the change of state

To search for alerts:

- Select the device, the alert category, priority and class of alert
- Optional, fill in the Start Time and the End Time fields, and then click **Search**

The results are displayed in a table that indicates the following information:

- EUI-64 address – the MAC address of the device generating the alert
- TsapID and ObjectID – identification of the application process and the associated object that initiated the alert

- Time – the date and time when the alert condition was detected
- Class – the type of alert (alarm or event)
- Direction – with the following values:
  - Start/End – only for alarms, it indicates if the report is for an alarm condition, or a return to normal from an alarm condition
  - N/A – if the alert reports an event
- Category – device diagnostic, communication-related, security-related, or process related
- Priority – indicates the importance of the alert, with the following ranges and associated labels, in compliance with the specification:
  - 0 - 2: Journal-only
  - 3 - 5: Low
  - 6 - 8: Medium
  - 9 - 11: High
  - 12 -15: Urgent
- Value – indicates the value associated with the alert condition.

You can set the number of records to be displayed per page in the table. The default number of records displayed in a page is 10. Paging controls at the bottom of the table allow you to navigate through different pages of the search results.

From this page you can also save the search results into a Microsoft Excel CSV file, by clicking **Export**.

## 5.9 Troubleshooting

The Troubleshooting page displays the latest alerts related to various events in the network.

**Monitoring Control System**

**NEXCOM**  
The Intelligent Systems

**ISA 100 Wireless**

**Network**

- Dashboard
- Topology
- Devices
- Network Health
- Readings
- Commands Log
- Alerts
- Troubleshooting
- Bulk Transfers
- Set Country Code

**Configuration**

- Backbone Router
- Gateway
- System Manager
- Device Management
- Monitoring Host
- MOQBUS
- Alert Subscription
- Advanced Settings
- Bulk Transfer
- System Status

**Administration**

- Device Firmware

**Troubleshooting**

Show **EUI-64** Display last **50** alerts ☒ Autorefresh every **5** seconds Next refresh in 2 second(s) [Edit Filters](#)

**Filters**

Alerts: All  
Devices: All

EUI-64	Timestamp*	Event	Details	Last alert 09:20:10 (hh:mm:ss) ago
6000:BEEF:6000:B10B	2016-09-18 16:47:13	Contract Modify	[GW/UAPl] -> [0102:0304:0506:0BB5/UAPl] CB i -15 EB i -15 id i 6 Aperiodic	
6000:BEEF:6000:B10B	2016-09-18 16:45:00	Contract Modify	[GW/UAPl] -> [0102:0304:0506:0BB5/UAPl] CB i -15 EB i -15 id i 6 Aperiodic	
6000:BEEF:6000:B10B	2016-09-18 16:42:24	Contract Terminate	[GW/UAPl] -> [0102:0304:0506:0000/UAPl] CB i -15 EB i 4 id i 7 Aperiodic Reason: expired	
0102:0304:0506:0000	2016-09-18 16:32:52	Contract Establish	[0102:0304:0506:0000/UAPl] -> [GW/UAPl] P: 60 Ddn: 10.000 s id i 5 Periodic	
6000:BEEF:6000:B10B	2016-09-18 16:32:32	Contract Modify	[GW/UAPl] -> [0102:0304:0506:0000/UAPl] CB i -15 EB i 4 id i 7 Aperiodic	
0102:0304:0506:0000	2016-09-18 16:31:34	Contract Establish	[0102:0304:0506:0000/UAPl] -> [GW/UAPl] CB i 1 EB i 1 id i 4 Aperiodic	
0102:0304:0506:0000	2016-09-18 16:30:53	Contract Establish	[0102:0304:0506:0000/DMAP] -> [GW/UAPl] CB i -15 EB i -15 id i 3 Aperiodic	
6000:BEEF:6000:B10B	2016-09-18 16:27:59	Contract Modify	[GW/UAPl] -> [0102:0304:0506:0000/UAPl] CB i -8 EB i 4 id i 7 Aperiodic	
6000:BEEF:6000:B10B	2016-09-18 16:27:42	Contract Modify	[GW/UAPl] -> [0102:0304:0506:0000/UAPl] CB i -8 EB i 4 id i 7 Aperiodic	
6000:BEEF:6000:B10B	2016-09-18 16:27:07	Contract Establish	[GW/UAPl] -> [0102:0304:0506:0000/UAPl] CB i -15 EB i -15 id i 7 Aperiodic	
0102:0304:0506:0000	2016-09-18 16:26:42	Contract Establish	[0102:0304:0506:0000/DMAP] -> [SM/SHAP] P: 60 Ddn: 10.000 s id i 2 Periodic	
6000:BEEF:6000:B10B	2016-09-18 16:26:28	Contract Terminate	[GW/UAPl] -> [0102:0304:0506:0BB4/UAPl] CB i -15 EB i -15 id i 4 Aperiodic Reason: requested	
6000:BEEF:6000:B10B	2016-09-18 16:26:23	Contract Refusal	[GW/UAPl] -> [0102:0304:0506:0000/UAPl] CB i -15 EB i -15 id i 0 Aperiodic Req: create; Reason: delayed	
0102:0304:0506:0BB4	2016-09-18 16:26:15	Contract Establish	[0102:0304:0506:0BB4/UAPl] -> [GW/UAPl] CB i 1 EB i 1 id i 5 Aperiodic	
0102:0304:0506:0000	2016-09-18 16:26:13	Contract Refusal	[0102:0304:0506:0000/DMAP] -> [GW/UAPl] CB i -15 EB i 1 id i 0 Aperiodic	



The alerts are listed in a table, with the following information:

- EUI-64 or IPv6 Address or Device Tag – a drop down list allows you to choose the device identification information that will be displayed in the first column of the table. The drop-down box is set on EUI-64 by default
- Timestamp – the date and time when the alert was generated
- Event – the alert type
- Details – this column displays the following details, depending on the type of alert:

Alert Type	Details	Explanations	
Device Join	Device IPv6	IPv6 address of the device	
	Device Type	The tags GW, BB, or SM for field devices, the tag is not displayed	
Device Join Failed	Parent	The IPv6 address of the parent device	
	Phase	Join Phase	Join Phase Description
		4	SECURITY_JOIN_Req
		5	SECURITY_JOIN_Rsp
		6	NETWORK_JOIN_Req
		7	NETWORK_JOIN_Rsp
		8	JOIN_CONTRACT_Req
		9	JOIN_CONTRACT_Rsp
		10	SECURITY_CONFIRM_Req
	11	SECURITY_CONFIRM_Rsp	
Reason	The reason number and description		
Device Leave	Reason	The reason number and description	

- The time elapsed from the last alert

**NOTE:** Contract Alerts and Topology Alerts will be implemented in a future version of the MCS.

The Display last N alerts drop-down list allows you to select the maximum number of alerts to display in the table. You can choose a value between 50, 100, 150, and 200.

To always view the latest alerts, enable the **Autorefresh every N seconds** checkbox. You can choose a value between 5, 10, 15, 30, and 60 seconds.

## Filters

The Edit filters button allows you to define the filters to apply for displaying the alerts. Click the button to expand the upper section of the page:

The screenshot shows the NEXCOM Monitoring Control System interface. The main content area is titled "Troubleshooting" and displays a table of alerts. The table has four columns: "Alert Class & Type", "Devices", "IPv6 Address", and "Device Tag". The "Alert Class & Type" column lists various alert types such as "Device Join/Leave", "Device Join", "Device Join Failed", "Device Leave", "Contract", "Contract Establish", "Contract Modify", "Contract Refusal", "Contract Terminate", "Topology", "Recent Change", and "Backup Change". The "Devices" column shows the MAC address of the device. The "IPv6 Address" column shows the IPv6 address of the device. The "Device Tag" column shows the name of the device. The table is filtered to show alerts for EUI-64 devices. The left sidebar contains navigation links for Network, Configuration, and Administration.

Alert Class & Type	Devices	IPv6 Address	Device Tag
<input checked="" type="checkbox"/> All	<input checked="" type="checkbox"/> EUI-64		
<input checked="" type="checkbox"/> Device Join/Leave	<input checked="" type="checkbox"/> 0000:0000:0A10:00A0	FE80::0000:0000:0000:0000:4E7B:C0A8:010B	NEXCOMSystem_Mng
<input checked="" type="checkbox"/> Device Join	<input checked="" type="checkbox"/> 0000:0000:FFFF:000C	FE80::0000:0000:0000:0000:4E7B:C0A8:010C	NEXCOM Backbone
<input checked="" type="checkbox"/> Device Join Failed	<input checked="" type="checkbox"/> 0022:FF00:0002:8170	FC00::0000:0022:FF00:0002:8170:0004:0008	Centers_B170
<input checked="" type="checkbox"/> Device Leave	<input checked="" type="checkbox"/> 0102:0304:0506:0000	FC00::0000:0102:0304:0506:0000:0004:000D	TLV_00D
<input checked="" type="checkbox"/> Contract	<input checked="" type="checkbox"/> 0102:0304:0506:0BB4	FC00::0000:0102:0304:0506:0BB4:0004:004C	Centers_BB4
<input checked="" type="checkbox"/> Contract Establish	<input checked="" type="checkbox"/> 0102:0304:0506:0BB5	FC00::0000:0102:0304:0506:0BB5:0004:004D	Centers_BB5
<input checked="" type="checkbox"/> Contract Modify	<input checked="" type="checkbox"/> 600D:8EEF:600D:810B	FE80::0000:0000:0000:0000:4E7C:7F00:0001	NEXCOM Gateway
<input checked="" type="checkbox"/> Contract Refusal			
<input checked="" type="checkbox"/> Contract Terminate			
<input checked="" type="checkbox"/> Topology			
<input checked="" type="checkbox"/> Recent Change			
<input checked="" type="checkbox"/> Backup Change			

Under Devices, select the devices for which you want to display alerts.

Checking/unchecking the **All** checkbox in the table header will check/uncheck all the devices.

Under Alert Class & Types, you will view a hierarchy of application alerts and you can select the desired alerts combination.

Checking/unchecking an alert class will check/uncheck all the alert types in that class.


Checking/unchecking the All checkbox in the table header will check/uncheck all the alerts.

Pressing Clear Filter will reset the filters to All for both the Devices list and the Alerts list.

Each alert is preceded by an icon indicating the severity of the alert:

 - Information

 - Warning

 - Error

The Severity Icon is displayed for each Alert in the Troubleshooting table based on the following mapping:

Alert	Reason	Severity
Device join/leave alerts		
Device Join		info
Device Join Failed	1: Timeout (device does not respond to SM queries)	warning
	2: Re-join (new join request while joining)	warning
	3: Parent left the network during device join	warning
	8: Insufficient parent resources - will retry join through another router	warning
	4: Device removed from SM whitelist	error
	5: Device not found SM whitelist	error

Alert	Reason	Severity
Device Leave	6: Invalid join key - mismatch with key from SM whitelist	error
	7: Invalid challenge - already used in a Security_Join_Request (possible retry)	error
	9: SubnetID mismatch (device provisioning/SM whitelist mismatch)	Error
	1: Timeout - device does not respond to SM queries	error
	2: Re-join (new join request while joined)	error
	3: Parent left the network	error
	4: Device removed from SM whitelist	error
<b>Contract Alerts</b>		
Contract Establish		info
Contract Modify		info
Contract Refusal	1: Insufficient resources	error
	2: Delayed (try again later)	error
	3: Device not found	error
	4: Contract not found (it applies to modification/renewal)	error

Alert	Reason	Severity
	5: Invalid request (requested an operation that cannot be performed or the request contains invalid parameters)	error
	6: timeout (no response to contract request). This reason can only be set by the FD.	Error
Contract Terminate	1: requested	info
	2: expired	
	3: unjoin	
Topology alerts		
Parent Change		info
Backup Change		info

## 5.10 Bulk Transfers

The bulk transfers page enables you to monitor the status of configured bulk transfers.

### Bulk Transfers Status

EUI64 Address

Transfer Type 

All

Search

Refresh every 20 seconds ☒

Transfer Status 

All

Reset

Items per page 

10

 out of total 1

<< < 1/1 > >>

<u>EUI-64 Address</u> ▲	<u>Transfer Type</u>	<u>Transfer Status</u>	<u>AvgSpeed</u> (msg/min)	<u>Remaining</u> (hh:mm:ss)	<u>Duration</u> (hh:mm:ss)	<u>Started On*</u>	<u>Data</u>
0022:FF00:0002:B174	BTO	Not started	N/A	N/A	N/A	N/A	<a href="#">view</a>

\* using UTC time

Bulk transfers can be filtered by EUI-64 Address, Transfer Type and Transfer Status. To filter them, select the desired filters and/or type the EUI-64 Address for the desired device and click **Search**. To reset all the filters, click **Reset**.

The bulk transfers are displayed in a table with the following information:

- EUI-64 Address - the EUI-64 address of the target device
- Transfer Type:
  - UDO (Upload/Download Object) – the ISA-defined transfer method
  - BTO (Bulk Transfer Object) – an enhanced Nivis-defined transfer method
- Transfer Status - indicates the status of the transfer process at the time of viewing; the possible statuses are: Not Started, In Progress, Failed, and Completed
- Avg. Speed - the average transmission speed, calculated in packets (messages) per minute since the beginning of the transfer
- Remaining - the remaining time to completion
- Duration - the total duration of the transfer
- Started On - the date and time the bulk transfer operation started
- Data – Only for a completed transfer, click the **View** link to see the transferred data in HEX format, as shown in the figure below:

To refresh the information in the table regularly, check the **Refresh every 20 seconds** option in the Search form.

The total number of items in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number of items displayed in a page is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table.

## 5.11 Set Country Code

The page allows setting the Country Code on the field devices and on the transceiver, to follow country-specific RF regulations.

### Set Country Code

Country Code

None

Execute

Target device(s): none

EUI-64 Address

Device Tag

Revision

IK\_\_04.11.01

Search

Reset

Items per page 10 out of total 1 << < 1/1 > >>

EUI-64 Address	Device Tag	Device Role/Model	Revision	All
0022:FF00:0002:B174	Centero_B174	IO Router Device/FREESCALE_VN210	IK__04.11.01	

Choose the country in the “Country Code” drop down, select the devices to configure, click Execute.



## 6 Configuration

The configuration section enables you to view and edit certain settings for the configuration/provisioning of the devices and the network, including connection settings, publishers, alert subscriptions, and Modbus register mapping.

**IMPORTANT :** This section is intended for users with thorough technical knowledge, and certain configurations require advanced expertise, therefore they should be carefully planned, as any inconsistencies may render the devices/network inoperative.

**NOTE:** The changes you perform in the settings for each separate entity will also be reflected in the Advanced Settings page and vice-versa.

# 6.1 Backbone Router

The Backbone Router configuration page consists of 5 sections, as shown is the table below.

Step	Action
General Settings	

1.
- Specify the **EUI64** and the **BBR Tag**.

Backbone Router

General Settings

EUI64 .....

00000000FFFF000B

BBR Tag .....

NEXCOM Backbone

\*The Backbone must be restarted for the new settings to take effect.

NOTE:

- Hover over an edit box and a tooltip will appear, indicating the allowed format and range for each value.
- If you change any of these settings, you must restart the Backbone Router in order for the new settings to take effect.

Provision/security	
--------------------	--

2.
- Specify the **Subnet ID** – which must be the same for all the devices in a subnet, the **Subnet Mask**, and Specify the **APP Join Key**.

Provision/security

Subnet ID .....

0003

Subnet Mask .....

FFFF

App Join Key .....

c0c1c2c3c4c5c6c7c8c9cAcBcCcDcEcF

\*The Backbone must be restarted for the new settings to take effect.

Step	Action
<b>NOTE:</b>	<ul style="list-style-type: none"><li>➤ Hover over an edit box and a tooltip will appear, indicating the allowed format and range for each value.</li><li>➤ If you change any of these settings, you must restart the Backbone Router in order for the new settings to take effect.</li><li>➤ Take care: the subnet ID is <b>hexadecimal</b> in this page (while it is <b>decimal</b> in the Device management page, as well as in the Gateway Configuration page)</li></ul>

---

Step	Action
<b>Logging</b>	

3. Select the **Stack Logging level**. The numbers suggest the degree of detail provided in the Backbone Router logs:
  - 1 (ERROR) for error messages only
  - 2 (WARN) for error and warning messages
  - 3 (DEBUG) for error, warning and debug messages



The screenshot shows a window titled "Logging". Inside, there is a label "Stack Logging level" followed by a dotted line. To the right of the dotted line are three radio buttons labeled 1, 2, and 3. The radio button labeled 1 is selected, indicating the logging level is set to ERROR.

## Time Settings

4. Select **NTP servers** if the NIO 200IAG Gateway has access to internet  
 In case the NIO 200IAG does not have access to the internet, time synchronization can be performed by using the transceiver clock as the time source



The screenshot shows a window titled "Time Settings". Inside, there is a label "Get time from" followed by a dotted line. To the right of the dotted line are two radio buttons. The first radio button is labeled "NTP servers" and is selected. The second radio button is labeled "TR (NTP time server N/A)". Below the radio buttons are two buttons: "Save" and "Cancel".

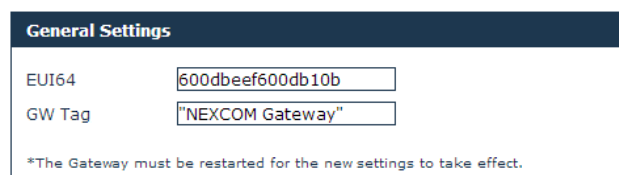
5. When you have finished editing the settings, click **Save**. As mentioned above, depending on the settings that you modify, the backbone router may need to be restarted for the changes to take effect.

## 6.2 Gateway

The Gateway configuration page consists of 3 sections, as shown in the table below.

Step	Action
General Settings	

1. Specify the **EUI64**, **IPv6 Address**, **UDP Port Number**, and the **GW Tag**.



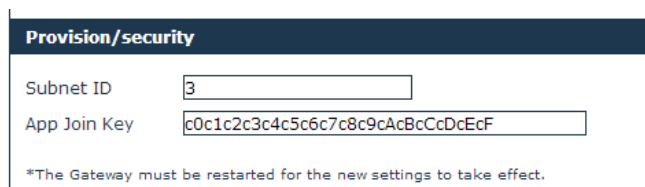
General Settings	
EUI64	<input type="text" value="600dbeef600db10b"/>
GW Tag	<input type="text" value="NEXCOM Gateway"/>
*The Gateway must be restarted for the new settings to take effect.	

**NOTE:**

- Hover over an edit box and a tooltip will appear, indicating the allowed format and range for each value.
- If you change any of these settings, you must restart the gateway in order for the new settings to take effect.

### Provision/security

2. Specify the **Subnet ID** and the **APP Join Key**.



Provision/security	
Subnet ID	<input type="text" value="3"/>
App Join Key	<input type="text" value="c0c1c2c3c4c5c6c7c8c9cAcBcCcDcEcF"/>
*The Gateway must be restarted for the new settings to take effect.	

Step	Action
------	--------

- NOTE:**
- Hover over an edit box and a tooltip will appear, indicating the allowed format and range for each value.
  - If you change any of these settings, you must restart the gateway in order for the new settings to take effect.

Step	Action
<b>Logging</b>	

3. Select the **App Logging level** and the **Stack Logging level**. The numbers suggest the degree of detail provided in the Backbone Router logs:
  - 1 (ERROR) for error messages only
  - 2 (WARN) for error and warning messages
  - 3 (DEBUG) for error, warning and debug messages

The screenshot shows a 'Logging' dialog box with the following configuration:

Setting	1	2	3
App Logging level	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Stack Logging level	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Buttons: Save, Cancel

4. When you have finished editing the settings, click **Save**. As mentioned above, depending on the settings that you modify, the backbone router may need to be restarted for the changes to take effect.

## 6.3 System Manager

The System Manager configuration page consists of 3 sections, as shown in the table below.

Step	Action
General Settings	

1. Specify the **EUI64**.

General Settings	
EUI64 .....	<input type="text" value="000000000a1000A0"/>
<small>*The System Manager must be restarted for the new settings to take effect.</small>	

**NOTE:**

- Hover over an edit box and a tooltip will appear, indicating the allowed format and range for each value.
  - If you change any of these settings, you must restart the system manager in order for the new settings to take effect.
-

Step	Action
Operational Settings	

- Fill in the input fields with the desired/appropriate values.  
Enable the desired frequency channels for communication with the network devices.

Operational Settings

Max Device Number (NSD) .....

Max Desired Latency (%) .....

Device Timeout Interval (s) .....

Advertise Period (s) .....

Join Links Period (s) .....

Channels .....

11☐

12☐

13☐

14☐

15☐

16☐

17☐

18☐

19☐

20☐

21☐

22☐

23☐

24☐

25☐

**NOTE:** Hover over an edit box and a tooltip will appear, indicating the allowed format, range and a description (where necessary for disambiguation) for each value.




Step	Action
<b>Logging</b>	

3. Select the **Logging level**, which indicates the degree of detail provided in the logs:
- ERROR for error messages only
  - WARN for error and warning messages
  - INFO for error, warning, and information messages
  - DEBUG for error, warning, information, and debug messages

The screenshot shows a dialog box titled "Logging". Inside, there is a label "Logging level" followed by a text input field containing the word "INFO". Below the input field are two buttons: "Save" and "Cancel".

4. When you have finished editing the settings, click **Save**.

5.	<p>Select the <b>Logging level</b>, which indicates the degree of detail provided in the logs:</p> <ul style="list-style-type: none"> <li>➤ ERROR for error messages only</li> <li>➤ WARN for error and warning messages</li> <li>➤ INFO for error, warning, and information messages</li> <li>➤ DEBUG for error, warning, information, and debug messages</li> </ul> 
6.	When you have finished editing the settings, click <b>Save</b> .

## 6.4 Device Management

This section enables you to edit the provisioning information (the SM whitelist) in the “system\_manager.ini” file for existing devices and to add new devices to the network.

**WARNING! Do not change these settings unless you were specifically instructed by a NEXCOM representative! Incorrect values may render the devices dysfunctional, or may cause difficulty to trace malfunctions.**

**NOTE:** This page is not exposed into the left-hand menu. The user must type its URL in order to access it.

To access the page, Open the following URL:

[http://<NIO200IAG\\_IP>/admin/devicemng.html](http://<NIO200IAG_IP>/admin/devicemng.html) replacing <NIO200IAG\_IP> with NIO 200IAG Gateway IP. Provide any credentials may be requested if the user is not already logged in

Click **Help** in the upper right corner of the window to view information and examples of the accepted data formats in all the sections.

The screenshot displays the NEXCOM Monitoring Control System web interface. The browser address bar shows the URL `192.168.1.11:8080/app/devicemng.html`. The page header includes the NEXCOM logo and the text "ISA 100 Wireless". The left sidebar contains a navigation menu with sections: Network, Configuration, and Administration. The main content area is titled "Device Management" and contains three sections: Backbones, Gateways, and Devices. Each section has a text input field for configuration, a "Save" button, and a "Delete" button. The "Devices" section also includes a "Manage device list" section with "Upload devices" and "Download devices" buttons. On the right side, there is a "Device Format" section with examples of device IDs and a "Note" at the bottom.

**Device Format (all sections):** <EUI64>.<Key>.<Subnet>.<Role>  
**EUI64:** 8 bytes grouped by 2, represented as hex, separated by colons  
**Key:** 16 bytes, represented as hex, can be separated by spaces  
**Subnet:** Integer in range [0-65535]  
**Role:** Integer in range [0-65535]

**Examples with one EUI64:**  
**Example1:** 6202-0304-0506-FC00.C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE CF,4  
**Example2:** 6202-0304-0506-FC00.C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE CF,3,10  
**Example3:** 6202-0304-0506-FC00.C0C1C2C3C4C5C6C7C8C9CABCBCDCDECF,3,10  
**Example4:** 6202-0304-0506-FC00.C0C1C2C3C4C5C6C7C8C9CABCBCDCDECF,3,10

**Examples with EUI64 range:**  
**Example5:** 6202-0304-0506-FC00 - 6202-0304-0506-FC0F.C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE CF,3,10  
**Example6:** 6202-0304-0506-FC00 - 6202-0304-0506-FC0F.C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE CF,3,10  
**Example7:** 6202-0304-0506-FC00 - 6202-0304-0506-FC0F.C0C1C2C3C4C5C6C7C8C9CABCBCDCDECF,3,10  
**Example8:** 6202-0304-0506-FC00 - 6202-0304-0506-FC0F.C0C1C2C3C4C5C6C7C8C9CABCBCDCDECF,3,10

**Note:** Do not use any spaces between EUI64, Key, Subnet or Role!

**NOTE:**

- The EUI-64 address is unique in a network.
- All the devices in a subnet must have the same security key and the same Subnet ID.
- The number of backbone routers in a network equals the number of subnets in that network.

## 6.4.1. Configuring Backbones

Step	Action
To add a backbone router in the network	
1.	Type the EUI64, security key, and subnet ID in the empty edit box.
2.	Click the <b>Save</b> button.
3.	The new backbone router will be added to the Backbones list.
4.	Click the <b>Activate</b> button to load the changes into the System Manager. The changes will be visible in the network topology and where applicable in the device list.
To edit a backbone router	
1.	Click on the entry that you want to edit in the backbones list.
2.	<p>Edit the security key and/or subnet ID, and click <b>Save</b> to save the changes in the “system_manager.ini” file.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"><li>➤ If you try to edit the EUI64 address of an existing backbone router, the SM will recognize it as a new entity and will add the new backbone router to the list.</li><li>➤ If you edit a BBR, it will be removed from an existing subnet and the devices in that subnet will be unable to join the network, unless you edit the same parameters for all the field devices in that subnet.</li><li>➤ Take care: the subnet ID is <b>decimal</b> in this page (while it is <b>hexadecimal</b> in the BBR Configuration page)</li></ul>
3.	Click the <b>Activate</b> button to load the changes into the System Manager. The changes will be visible in the network topology and where applicable in the device list.
To delete a backbone router	
1.	Select the desired backbone router in the list and click <b>Delete</b> .

Step	Action
2.	<p>You will be asked for confirmation. Click <b>Yes</b> to delete the backbone router or <b>No</b> to abort the action.</p> <p><b>NOTE:</b> When you delete a backbone router the devices in its subnet will be unable to join until a new backbone router provisioned with the same security key and subnet ID is added to that subnet.</p>
3.	<p>Click the <b>Activate</b> button to load the changes into the System Manager. The changes will be visible in the network topology and where applicable in the device list.</p>

## 6.4.2. Configuring Gateways

**NOTE:** By design the NIO 200IAG Gateway supports only one ISA100 Gateway; therefore it is not permitted to add more than one gateway to the system.

Step	Action
To edit the gateway	
1.	Click on the entry that you want to edit in the gateways list.
2.	Edit the security key and/or subnet ID, and click <b>Save</b> to save the changes in the "system_manager.ini" file.
3.	Click the <b>Activate</b> button to load the changes into the System Manager. The changes will be visible in the network topology and where applicable in the device list.
To delete the gateway	
1.	Select the desired gateway in the list and click <b>Delete</b> .
2.	You will be asked for confirmation. Click <b>Yes</b> to delete the gateway or <b>No</b> to abort the action.  <b>Caution! If you delete the gateway, you will no longer be able to access the system and retrieve any data, although the network remains functional.</b>
4.	Click the <b>Activate</b> button to load the changes into the System Manager. The changes will be visible in the network topology and where applicable in the device list.

### 6.4.3. Configuring Devices

#### Adding devices:

You can add devices either individually, one device at a time, or you can add multiple devices at a time.

- To add a single device in the network, type it's EUI64, security key, and subnet ID in the empty edit box and click Save. The new device will be added to the Devices list.
- To add multiple devices with consecutive EUI-64 addresses type the range of EUI-64 addresses corresponding to the devices that you wish to add; subsequently, type the security key, and the subnet ID and click Save.

The follow example shows how a series of devices with consecutive EUI-64 address can be added to a subnet.

#### Example:

"6302:0304:0506:0B1A - 6302:0304:0506:0B1E,C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE CF,17, 3"

**NOTE:** When you add a device or a range of devices into the network you can define their role, which is expressed as an integer value and is added after the subnet ID in the device format.

The following table details the role values and associated labels:

Integer Value	Role
1	IO Device
2	Router Device
3	IO Routing Device

The following aspects must be taken into consideration when defining the role for a device or range of devices:

1. Upon join, each device states its capacity.
2. The roles of the backbone router and the gateway cannot be changed, therefore providing a role value in this section is unnecessary.
3. The role selection for a field device is limited to the capacity stated by that device.

#### Examples:

- If a device has only the IO role, you cannot add the Routing role for that device in the Device Management section.
  - If a device has both the IO and the Routing roles, you can limit its role in the network to one of the two, by typing either 1 or 2 after the subnet ID.
  - If you do not specify a role in this section, the System Manager will admit the role(s) stated by the device.
4. If you add the role for a range of devices, all the devices in question will have the same role. If any device in the range does not support the assigned role, the device will not join the network.

Step	Action
<b>To edit a device/multiple devices</b>	
<b>1.</b>	In the device list, click on the entry that you want to edit.
<b>2.</b>	Edit the security key and/or subnet ID.  <b>NOTE:</b> See the previous Note on Device Roles if you wish to edit device roles.
<b>3.</b>	Click <b>Save</b> to save the changes in the “system_manager.ini” file.
<b>4.</b>	Click the <b>Activate</b> button to load the changes into the System Manager. The changes will be visible in the network topology and where applicable in the device list.
<b>To delete a device/multiple devices</b>	



Step	Action
1.	Select the desired entry in the list and click <b>Delete</b> .
2.	You will be asked for confirmation. Click <b>Yes</b> to delete the device(s) or <b>No</b> to abort the action.
3.	Click the <b>Activate</b> button to load the changes into the System Manager. The changes will be visible in the network topology and where applicable in the device list.

## Loading a List of Devices

You can add multiple devices at the same time by importing them from a file. The file will contain a list of devices with the <EUI64>, <Key>, and <subnet>) comma separated values.

Step	Action
To load a list	
1.	Click on <b>Browse</b> to locate the text file that you wish to load, and click <b>Upload</b> .
2.	Click the <b>Activate</b> button to load the new device list into the System Manager. The current “system_manager.ini” file will be overwritten and all previous settings will be lost.
Exporting the settings	
1.	This page also enables to export the configuration settings, by clicking <b>Save</b> in the “Manage device list” section.

## 6.5 Monitoring Host

This section enables you to configure the devices publishing settings stored in the “Monitor\_Host\_Publishers.conf” file. The settings are used by the Monitor Host to subscribe to the data published by the field devices.

The settings in this page do not get sent to the field devices.

**NOTE:** Field devices must be separately provisioned with publish settings (channels to publish, period, phase, endpoint, etc.)

Click **Help** in the upper right corner of the window to view information and examples of the accepted data formats in all the sections.



The publishers' configuration can be performed manually, by user adding/editing the lines in the page, or automatically, by interrogating automatically the field devices. The automatic publisher discovery is recommended method.

If the automatic publishers' discovery is enabled: Auto Activate ON means the changes take effect immediately as a device respond to MH interrogations. If Auto Activate is OFF the changes will not take effect until the user press the Activate button, or until the software gets restarted

## 6.6 MODBUS

This section enables you to map ISA100.11a attributes to Modbus registers.

Click **Help** in the upper right corner of the window to view information and examples of the accepted data formats in all the sections.

MODBUS Server

Input registers

Help

99,3,0022FF000002B174,2,129,5,0,0,0,2

102,3,0022FF000002B174,2,129,6,0,0,0,2

105,3,0022FF000002B174,2,129,7,0,0,0,2

108,3,0022FF000002B174,2,129,8,0,0,0,2

111,3,0022FF000002B174,2,129,5,0,0,0,1

114,3,0022FF000002B174,2,129,6,0,0,0,1

117,3,0022FF000002B174,2,129,7,0,0,0,1

120,3,0022FF000002B174,2,129,8,0,0,0,1

Save

Delete

Holding registers

99,3,0022FF000002B174,2,129,5,0,0,0,2

102,3,0022FF000002B174,2,129,6,0,0,0,2

105,3,0022FF000002B174,2,129,7,0,0,0,2

108,3,0022FF000002B174,2,129,8,0,0,0,2

111,3,0022FF000002B174,2,129,5,0,0,0,1

114,3,0022FF000002B174,2,129,6,0,0,0,1

117,3,0022FF000002B174,2,129,7,0,0,0,1

120,3,0022FF000002B174,2,129,8,0,0,0,1

Save

Delete

Manage host list

Upload hosts .... 

Choose File

 No file chosen 

Upload

Download hosts

Save

Activate

Input Register Format: <start\_address>,<word\_count>,<EU164>,<TSAPID>,<ObjId>,<AttrId>,<Idx1>,<Idx2>,<MethId>,<status\_byte>

start\_address: unsigned integer, 2 bytes

word\_count: integer, 2 bytes

EU164: 8 bytes hex represented (16 characters)

TSAPID: unsigned integer in range [1-15]

ObjId: unsigned integer, 2 bytes

AttrId: unsigned integer, 2 bytes

Idx1: unsigned integer, 1 byte

Idx2: unsigned integer, 1 byte

MethId: unsigned integer, 2 bytes

status\_byte: 0, 1, 2

Holding Register Format: <start\_address>,<word\_count>,<EU164>,<TSAPID>,<ObjId>,<AttrId>,<Idx1>,<Idx2>,<MethId>,<status\_byte>

start\_address: unsigned integer, 2 bytes

word\_count: integer, 2 bytes

EU164: 8 bytes hex represented (16 characters)

TSAPID: unsigned integer in range [1-15]

ObjId: unsigned integer, 2 bytes

AttrId: unsigned integer, 2 bytes

Idx1: unsigned integer, 1 byte

Idx2: unsigned integer, 1 byte

MethId: unsigned integer, 2 bytes

status\_byte: 0, 1, 2

Close

## 6.7 Alert Subscription

This page enables you to subscribe to alerts generated in the system.

### Alert Subscription

**Subscription Categories**

☒ Communication Diagnostic alerts enabled

☒ Security alerts enabled

☒ Device Diagnostic alerts enabled

☒ Process alerts enabled

Save

To subscribe to an alert category, enable the checkbox preceding it and click **Save**. When an alert to which you subscribed is generated, it will be listed in the Alerts page.

## 6.8 Advanced Settings

Monitoring Control System X

192.168.1.11:8080/app/advanced.html

Monitoring Control System

NEXCOM  
The Intelligent Systems

ISA 100  
Wireless

Network

- Dashboard
- Topology
- Devices
- Network Health
- Readings
- Commands Log
- Alerts
- Troubleshooting
- Bulk Transfers
- Set Country Code

Configuration

- Backbone Router
- Gateway
- System Manager
- Device Management
- Monitoring Host
- MODBUS
- Alert Subscription
- Advanced Settings
- Bulk Transfers
- System Status

Administration

- Device Firmware
- System Upgrade
- Custom Icons
- Custom Settings

Advanced Settings

Sections/variables

Configuration ..... System

Variable type ..... ☒ Standard ☐ Custom

Section ..... GLOBAL

Variable ..... AN\_ID

Value .....

Set Cancel

\*The associated application must be restarted for the new settings to take effect.

Restart/Stop/Reload

Apply all settin RestartApplic StopApplicatio RestartNIO200

\*After a restart the Monitoring Control System becomes inoperable for a few minutes.

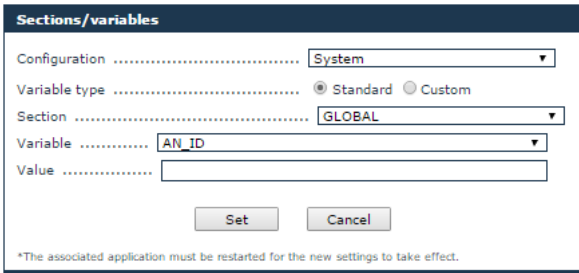
Mesh WiFi & NTP Settings

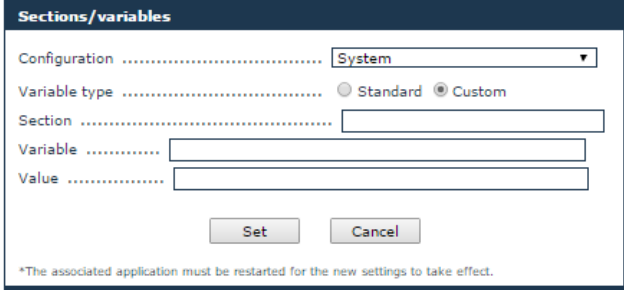
Open NEXCOM NIO200 admin website: Click here

# 6.8.1. Edit Configuration Variables

This page allows you to view/set less common configuration variables, which cannot be changed using the classic MCS web interface.

**IMPORTANT:** This page is for advanced users only – do not use unless you have been instructed exactly by a NEXCOM representative on what values to change. Incorrect values may render the router dysfunctional, or may cause difficulty to trace malfunctions.

Step	Action
1.	<div>The following form will open to the right of the operation list:</div> <div></div>
2.	In the form, select a Section in the drop-down list. The Variable list will change accordingly.
3.	<div>Select a Variable in the drop-down list.</div> <div><b>IMPORTANT:</b> Do not change [GLOBAL].AN_ID under any circumstance.</div>
4.	Set/edit the Value field, then click <b>Set</b> .

<p>5.</p>	<p>To add a new variable, select <b>Custom</b> under Variable type. The Sections/variables form will be empty.</p> 
<p>6.</p>	<p>Type the desired information in the Section, Variable, and Value fields, then click <b>Set</b>.</p>

### 6.8.2. Restart



This section enables the user to restart the applications running on the NIO 200IAG Gateway.

The “**Apply all settings**” button apply all settings (re-load into all modules the configuration files)

The “**Restart Applications**” restart all applications, without rebooting the board.

The “**Stop Applications**” stops all applications, for powering the board off after an ordered shut down.

The “**Restart NIO200**” reboots the NIO 200IAG Gateway.

**NOTE:** After restarting the applications or rebooting the NIO 200IAG Gateway, the Monitoring Control System becomes inoperative for a few minutes.



After Stopping the applications, the Monitoring Control System becomes inoperative until the next power cycle.

### 6.8.3. Access NIO200 Wi-Fi Configuration website



This section allows the user to navigate to NEXCOM NIO200 admin website, where the NIO200 Network Configuration ( Wi-Fi settings, IP Addresses, NTP Server, etc) can be changed.

## 6.9 Bulk Transfers



The Bulk Transfers page enables you to create and configure bulk transfers. Bulk data transfers are used to transfer large items between wireless devices (sensor boards) and gateway clients. This can be done via two methods:

- A transfer method described by ISA running on top of UDO
- A Nivis enhanced bulk data transfer protocol

Already configured bulk transfers are displayed in a table, with the following information:


### Bulk Transfers List

Add Bulk Transfer

Items per page 10 out of total 2		<< < 1/1 > >>		
EUI-64 Address▲	Transfer Type	TsapID	Device Tag	Status
<a href="#">0102:0304:0506:0601</a>	UDO	2	T102030405060601	Completed 
<a href="#">0102:0304:0506:0603</a>	BTO	2	T102030405060603	Failed 

- EUI-64 Address – the EUI-64 Address of the source device
- Transfer Type – the selected transfer protocol (UDO or BTO)
- TsapID –
- Device Tag – the device tag for the source device
- Status – the status of the transfer

The total number of items in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number of items displayed in a page is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table.

You can also delete a bulk transfer, by clicking the  icon next to it. The system will require confirmation to perform the action. Click **Yes** to delete the bulk transfer or **Cancel** to abort the action.

## 7 System Status

The Statistics page displays statistical information regarding processor and memory usage, and load average on the NIO 200IAG Gateway.

System Status			
Backbone Router			
Status:	Running		
Memory:	3.01 MB (0.40%)		
Processor:	1.5 %		
Gateway			
Status:	Running		
Memory:	3.46 MB (0.46%)		
Processor:	0.0 %		
System Manager			
Status:	Running		
Memory:	7.71 MB (1.02%)		
Processor:	0.5 %		
MODBUS			
Status:	Running		
Memory:	3.15 MB (0.42%)		
Processor:	0.5 %		
Monitor Host			
Status:	Running		
Memory:	6.33 MB (0.84%)		
Processor:	0.0 %		
System memory			
Total:	757.34 MB	Used:	333.95 MB Free: 423.39 MB
Flash memory			
Total:	20 MB	Used:	8.53 MB Free: 11.47 MB
Load average			
Load average (1',5',15'): 1.08 1.18 1.17 2/62 16569			
<input checked="" type="checkbox"/> Auto refresh page (every 1 minute)			

The first five sections indicate the status (“Running” or “Not Running”), memory usage and processor usage for the backbone router, gateway, system manager, modbus, and monitor host processes.

The following two sections display system memory and flash memory availability information.

The Load average section indicates:

- The system’s load average over the past one, five and fifteen minutes respectively
- The number of running processes out of the total number of processes
- The ID of the last started process

If you wish to regularly update the system status information, enable the Auto refresh page option at the bottom of the page. The page will auto refresh at one-minute intervals.

# 8 Administration

The administration section encompasses tools for the management of the ISA100.11a based system.

It allows the users to update device and system firmware and to manage device icons and apply custom settings to their site.

## 8.1 Device Firmwares

The Device Firmwares section is dedicated to firmware updates for field devices and the backbone router. Firmware updates require technical expertise and must be planned carefully or the devices will be unable to communicate on the ISA100.11a network. We recommend that you contact a Technical Support representative prior to executing such procedure.

This section provides a tool to upload binary firmware files into the system. These files will be used later to upgrade the device firmware.

In the Device Firmwares page you will view all the firmware update operations generated in the system. They can be filtered by Device, Firmware Type, and/or Download Status.

When the main page is loaded, the ongoing update operations (if any) are displayed by default. To search for firmware update operations, select the desired device, type and/or download status and click *Search*. The results will be displayed in a table, as shown in the following figure:

Device Firmwares

Execute

FW Files

Device

Type

All

Download Status

In Progress

Refresh every 20 seconds

Search

Export

Items per page 50 out of total 1

<< < 1/1 > >>

EUI-64 Address	Type	Status	Avg Speed (msg/min)	Crt Speed (msg/min)	Remaining (hh:mm:ss)	Duration (hh:mm:ss)	Started On*
0022:FF00:0002:B174	Device	7%	49	56	0:18:11	0:2:2	2016-08-15 21:06:42



\* using UTC time

1 firmware upgrade operation(s) started!

The following information is available:

- EUI-64 address – the EUI-64 address of the target device
- Type – the type of firmware uploaded on a device (for firmware types see [2.5.1.3 Firmware Files](#))
- Status – indicates the status of the update process at the time of viewing; the possible statuses are Completed, In Progress, Canceled, and Failed
- Completed – indicates the completion percentage at the time of viewing for ongoing operations, or the percentage at which the operation stopped, for canceled or failed updates. For completed updates, the percentage is 100%
- Avg speed – the average transmission speed, calculated in packets (messages) per minute since the beginning of the transfer
- Crt speed – the last recorded transmission speed, calculated based on the smallest of the bandwidths reserved for the two contracts: from and to the device. It varies slightly from the last instantaneous transmission speed
- Remaining – the remaining time to completion
- Duration – the total duration of the update
- Started on – the date and time the update operation started

To refresh the information in the table regularly, check the “Refresh every 1 minute” option in the Search form.

You can also cancel an ongoing firmware update by clicking the  icon next to it, or delete a completed/ failed/ canceled/ operation from the records by clicking the  icon next to it. The system will require confirmation before performing the requested action.

The total number of items in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number of items displayed in a page is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table.

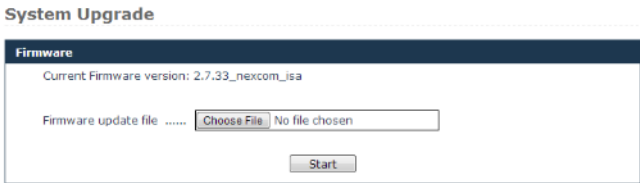
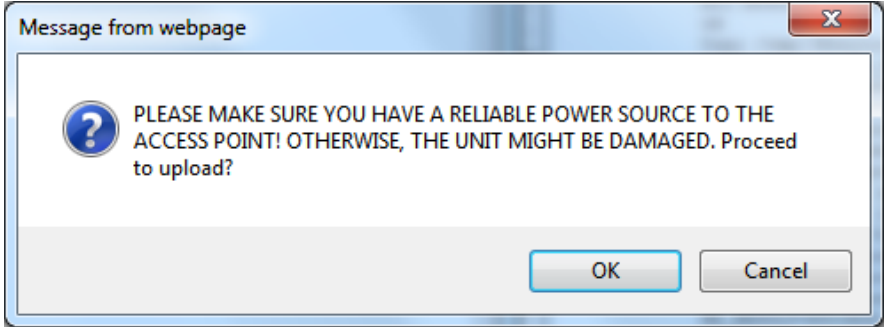
From this page you can export the search results into CSV format, for later use.

## 8.2 System Upgrade

The System Upgrade page enables you to upgrade the system components hosted on the connected NIO 200IAG Gateway.

The Firmware form indicates the current system version on the NIO 200IAG Gateway.

### To initiate the upgrade

Step	Action
1.	<p>Click <b>Browse</b> to locate and open the upgrade package that you wish to use:</p> 
2.	<p>Click the <b>Upload Firmware</b> button to initiate the process.</p>
3.	<p>Make sure the NIO200 has a reliable power source. When asked click OK</p> 

Step	Action
4.	<p data-bbox="339 297 1286 383">When the upgrade is complete, the page indicates the result of the upgrade:</p> <div data-bbox="339 483 1286 656"><p data-bbox="644 488 1031 515"><b>System has been upgraded successfully.</b></p><p data-bbox="753 542 922 568">System rebooting...</p><p data-bbox="791 624 884 651"><a href="#">Main Page</a></p></div>



## 8.3 Custom Icons

This page enables you to assign custom icons for the devices in a network based on their role, with a view to better distinguishing them.

When the page is loaded, the existing custom icons are displayed in a table, with the following information:

- Model – the device model
- Role – the device role
- Icon – shows the existing picture

The default icons are not listed.

## 8.4 Custom Settings

This page enables user to define whether the timestamps get shown using browser local time zone or UTC; apply color themes to the website; replace the NEXCOM logo with a logo of preference in the website header, and enable/disable various high-side interfaces.

The screenshot shows a web browser window with the address bar displaying `192.168.1.11:8080/app/customsettings.html`. The page header features the NEXCOM logo and the text "The Intelligent Systems" on the left, and "ISA 100 Wireless" on the right. The main content area is titled "Custom Settings" and contains three sections: "DateTime format", "Color theme", and "Application header".

**DateTime format**

☒ UTC ☐ LOCAL

**Color theme**

☒ Default ☐ Green ☐ Dark Red

**Application header**

☐ Show product logo (left)

☐ Show custom logo (middle)

Logo file:  No file chosen

☐ Show technology logo (right)

**Interfaces Configuration**

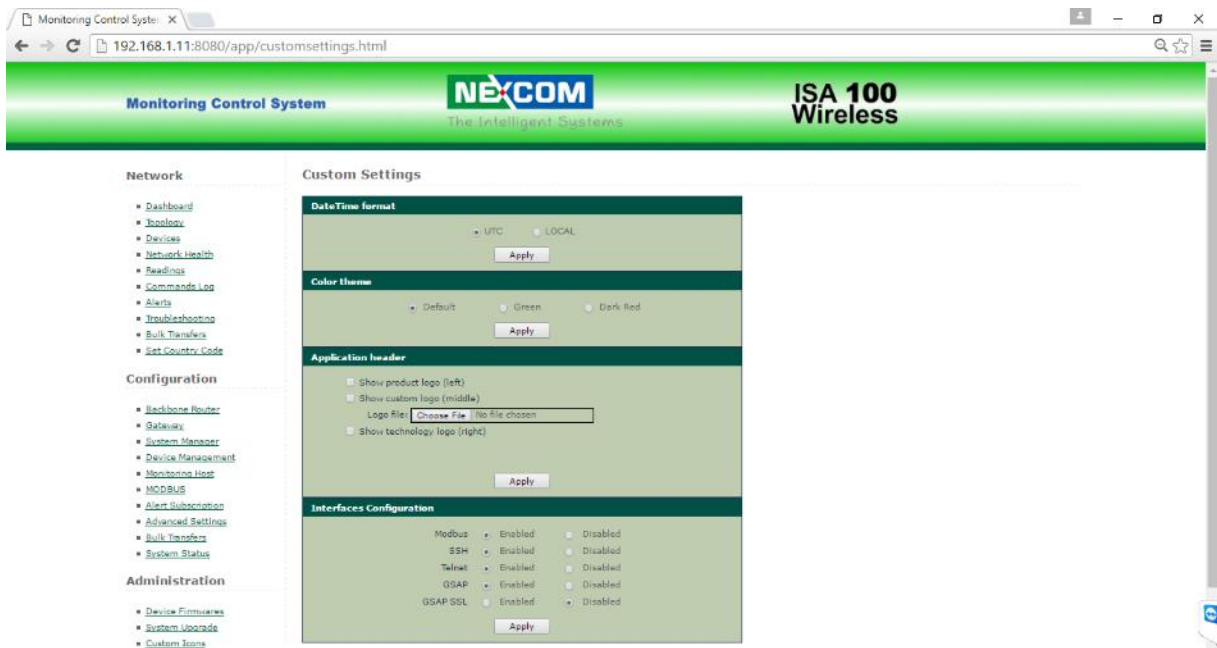
Modbus	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
SSH	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Telnet	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
GSAP	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
GSAP SSL	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled

**Navigation Menu:**

- Network**
  - Dashboard
  - Topology
  - Devices
  - Network Health
  - Readings
  - Commands Log
  - Alerts
  - Troubleshooting
  - Bulk Transfers
  - Set Country Code
- Configuration**
  - Backbone Router
  - Gateway
  - System Manager
  - Device Management
  - Monitoring Host
  - MODBUS
  - Alert Subscription
  - Advanced Settings
  - Bulk Transfers
  - System Status
- Administration**
  - Device Firmware
  - System Upgrade
  - Custom Icons
  - Custom Settings

Date Time Format defines the format to display timestamps: using the browser local time zone settings or using UTC.

To apply one of the three available themes, select the desired theme and click **Change**. The page will refresh and the new color scheme will be displayed:



The Interfaces configuration allow enabling/disabling the high-side interfaces.

# 9 Session

## 9.1 Change Password

This page enables you to change your own password.

Change password

Old password .....

.....

New password .....

.....

Confirm new password .....

.....

Save

Cancel

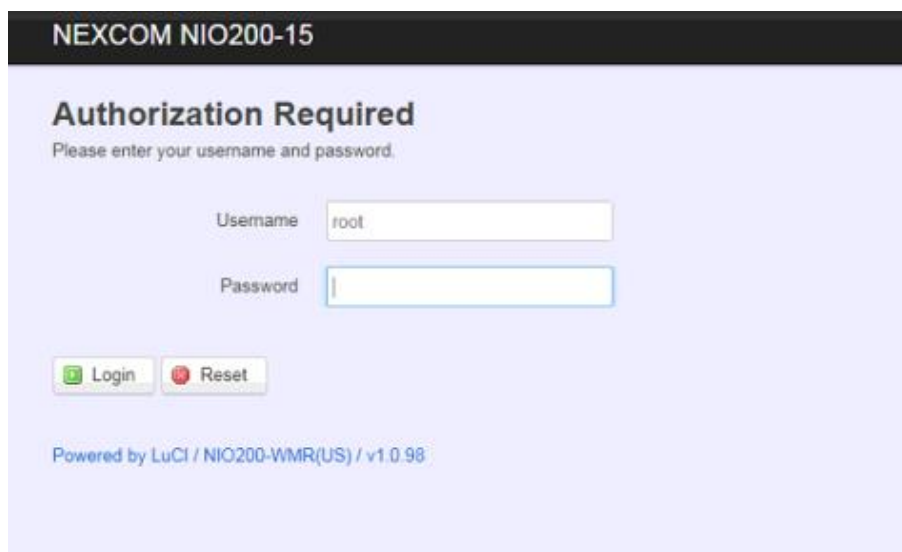
Step	Action
1.	In the form, type your current password in the Old Password field.
2.	Type the new password in the New password field.
3.	Retype the new password in the Confirm new password field, for verification.  <b>NOTE:</b> The passwords are case sensitive.
4.	Click <b>Save</b> at the bottom of the page to save the new password, which will become your current password.

**Tip:** To prevent unauthorized persons to gain access to your account, use a strong password in order to make it difficult for others to determine it and do not disclose your password to anyone.

## 10 Wi-Fi Mesh Configuration

### 10.1 Login

To access the Wi-Fi Mesh Web UI, you may open a browser to access the Web GUI via default IP address 192.168.1.1. The login Web page requires login information as below:



The image shows the login page of the NEXCOM NIO200-15. The page has a light blue background. At the top, there is a black header with the text "NEXCOM NIO200-15" in white. Below the header, the title "Authorization Required" is displayed in bold. Underneath the title, a message says "Please enter your username and password." There are two input fields: "Username" with the text "root" and "Password" which is empty. Below the input fields, there are two buttons: "Login" with a green arrow icon and "Reset" with a red circular icon. At the bottom, it says "Powered by LuCI / NIO200-WMR(US) / v1.0.98".

Default login information is:

Login: root

Password: admin

After successful login, you will see the “Status” page of the device Web UI.



The image shows the status page of the NEXCOM NIO200-15. The page has a light blue background. At the top, there is a black header with the text "NEXCOM NIO200-15" in white. To the right of the header, there are links: "Status", "System", "Network", and "Logout". In the top right corner, there is a green button labeled "AUTO-RESTART". Below the header, the title "Status" is displayed in bold. Underneath the title, the section "System" is shown. It contains a table with the following data:

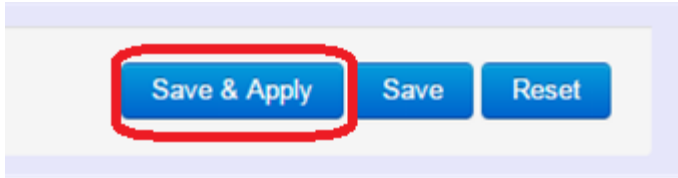
Hostname	NIO200-15
Model	NIO200-WMR
Firmware Version	NIO200-WMR(US)-v1.0.98 / LuCI (git-16.020.59380-63d70da)
Kernel Version	3.14.27
Local Time	Mon Jul 16 14:40:22 2018
Uptime	23d 4h 25m 53s
Load Average	0.03, 0.07, 0.12

Below the System section, the section "Memory" is shown. It contains a table with the following data:

Total Available	25860 kB / 775424 kB (3%)
Free	25860 kB / 775424 kB (3%)
Buffered	0 kB / 775424 kB (0%)

## Saving Changes

Saving & apply the configuration in WebUI after you do the changes at the bottom of WebUI.



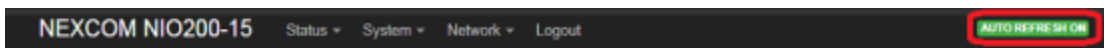
## Unsaved Changes



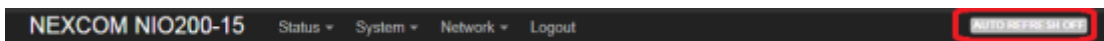
“UNSAVED CHANGES” provides the help to see the parameters which were not saved & applied,

Click “Save & Apply” button to save the parameters.

## Auto Refresh

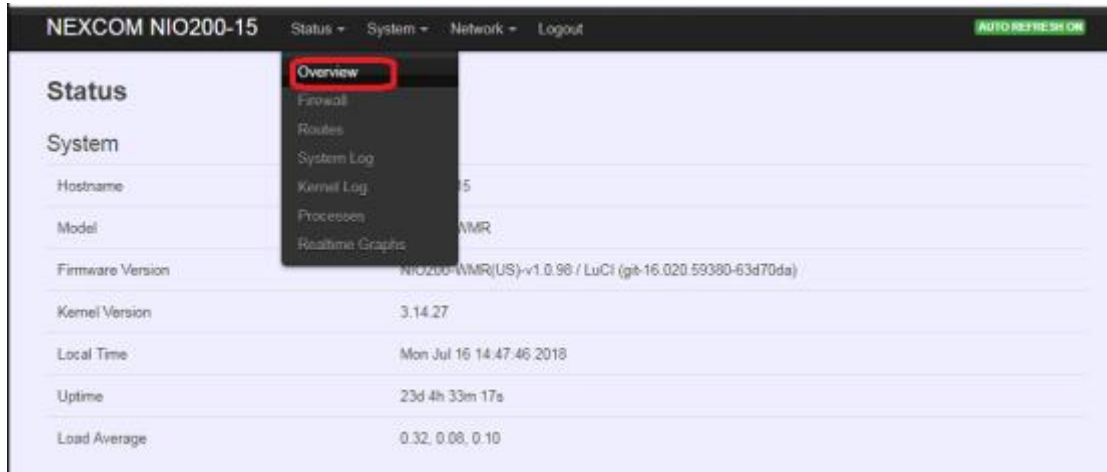


Toggle “AUTO REFRESH” button to turn on/off WebUI refresh function automatically



## 10.2 Status

To display more detailed status, you can click the “Status” under the page bar. This allows users to select the item of Overview, Firewall, Routes, System Log, Kernel Log, Process, and Real-time Graphs from the pull-down list like below screen:



### 10.2.1 Overview

To see NIO200 over all status, click “Overview” to displays the current system information and interface connection status.

#### 10.2.1.1 System



**Hostname:** Displays NIO200 host name

**Model:** Displays NIO200 HW basic information

**Firmware Version:** Displays NIO200 firmware version.

**Kernel Version:** Displays NIO200 Kernel version.

**Local Time:** Displays NIO200 current date and time.

**Uptime:** Displays how long NIO200 has been operating since last boot-up.

**Load Average:** CPU average loading in recent time frame.

For example,

Load Average	0.94, 0.43, 0.24
--------------	------------------

CPU average loading:

94% in the past 1 minute.

43% in the past 5 minutes

24% in the past 15 minutes.

### 10.2.1.2 Memory



Memory	
Total Available	101876 kB / 126316 kB (80%)
Free	99156 kB / 126316 kB (78%)
Buffered	2720 kB / 126316 kB (2%)

**Total Available:** Displays the available memory in percentage.

**Free:** Displays free memory of NIO200.

**Buffered:** Displays buffer memory used in the system.

### 10.2.1.3 Network

Network	
IPv4 WAN Status	 Type: dhcp eth0.2 Address: 10.15.1.138 Netmask: 255.255.255.0 Gateway: 10.15.1.254 DNS 1: 10.1.1.2 DNS 2: 10.1.1.6 DNS 3: 10.1.1.5 DNS 4: 10.1.1.1 DNS 5: 10.1.1.29 Connected: 7h 31m 37s
IPv6 WAN Status	 Not connected
Active Connections:	38 / 16384 (0%)

**IPv4 WAN Status:** Displays current connecting IPv4 information.

**IPv6 WAN Status:** Displays current connecting IPv6 information.

**Active Connections:** Displays current active connections.



#### 10.2.1.4 DHCP Leases

DHCP Leases			
Hostname	IPv4-Address	MAC-Address	Leasetime remaining
IM03-AndrewWang1	192.168.1.219	08:3e:8e:67:64:03	10h 25m 0s
IM03-JonesChen	192.168.1.215	9c:2a:70:1b:4c:9d	6h 1m 34s
?	192.168.1.142	94:a1:a2:87:6f:08	9h 22m 13s
NEXCOM-SQA	192.168.1.105	00:0d:f0:ac:c8:63	10h 34m 24s
River-Ubuntu	192.168.1.118	80:19:34:c9:04:00	6h 51m 48s

This displays information about hosts (Personal Computers or electronic devices) that are connected to NIO200 including IPv4, MAC address and leasing time

#### 10.2.1.5 DHCPv6 Leases

DHCPv6 Leases			
Hostname	IPv6-Address	DUID	Leasetime remaining
River-Ubuntu	fdfe:68c3:19eb::10b/128	0004767fc07324b68cbab02958b2991f645	6h 51m 39s
NEXCOM-SQA	fdfe:68c3:19eb::3b0/128	000100011e1b93b70010f32db9b8	10h 34m 17s
IM03-JonesChen	fdfe:68c3:19eb::d25/128	000100011b2c6cb9206a8a9612c0	4h 14m 5s
NIFE-3600-SQA	fdfe:68c3:19eb::ed2/128	000100011e1c6e5e0010f32db9b8	5h 13m 27s

This displays information about hosts (Personal Computers or electronic devices) that are connected to NIO200 including IPv6, DUID and leasing time.

#### 10.2.1.6 Wireless

Wireless	
Generic 802.11an Wireless Controller (radio0)	<b>SSID:</b> backbone <b>Mode:</b> Mesh <b>Channel:</b> 36 (5.180 GHz) <b>Bitrate:</b> 43 Mbit/s <b>MAC:</b> 00:10:F3:6D:48:B4 <b>Encryption:</b> NONE
Generic 802.11an Wireless Controller (radio1)	<b>SSID:</b> management-15 <b>Mode:</b> Master <b>Channel:</b> 0 (0.000 GHz) <b>Bitrate:</b> ? Mbit/s <b>MAC:</b> 00:00:00:00:00:00 <b>Encryption:</b> unknown

This displays Wireless information about NIO200 for radio 0&1.

**SSID:** Displays the name of the wireless network.

**Mode:** Displays the mode in this radio








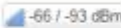



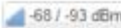
**Channel:** Displays current channel using.

**Bitrate:** Displays current wireless data rate.

**BSSID:** Displays MAC address of this radio

**Encryption:** Displays current encryption setting.

### 10.2.1.7 Associated Stations

Associated Stations					
	Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
	Mesh "backbone"	00:10:F3:77:28:5D	?	 -69 / -93 dBm	45.0 Mbit/s, MCS 2, 40MHz 28.9 Mbit/s, MCS 3, 20MHz
	Mesh "backbone"	00:10:F3:6E:E6:A2	?	 -77 / -93 dBm	30.0 Mbit/s, MCS 1, 40MHz 27.0 Mbit/s, MCS 1, 40MHz
	Mesh "backbone"	00:10:F3:6D:48:75	?	 -64 / -93 dBm	150.0 Mbit/s, MCS 7, 40MHz 135.0 Mbit/s, MCS 7, 40MHz
	Mesh "backbone"	00:10:F3:62:38:87	?	 -66 / -93 dBm	120.0 Mbit/s, MCS 5, 40MHz 121.5 Mbit/s, MCS 6, 40MHz
	Mesh "backbone"	00:10:F3:62:38:81	?	 -78 / -93 dBm	6.5 Mbit/s, MCS 0, 20MHz 27.0 Mbit/s, MCS 1, 40MHz
	Mesh "backbone"	00:10:F3:35:26:25	?	 -68 / -93 dBm	108.0 Mbit/s, MCS 5, 40MHz 81.0 Mbit/s, MCS 4, 40MHz

Displays current associated device information (Personal Computers or electronic devices) including device's MAC address, signal level, noise, connecting data rate.

## 10.2.2 Firewall

Firewall setting is a particular function which allows user to connect or block two or more interfaces in device with sophisticated and specifically defined parameters in this Web page.

It's highly recommended to keep this Firewall setup page as it is.

**NEXCOM NIO200-15** Status System Network Logout

### Firewall Status

**Table: Filter**

Chain **INPUT** (Policy: **ACCEPT**, Packets: 2816060, Traffic: 210.85 MB)

Pkts	Traffic	Target	Prot	In	Out	Source	Destination	Options
2816060	210.85 MB	delegate_input	all	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain **FORWARD** (Policy: **DROP**, Packets: 0, Traffic: 0.00 B)

Pkts	Traffic	Target	Prot	In	Out	Source	Destination	Options
0	0.00 B	delegate_forward	all	*	*	0.0.0.0/0	0.0.0.0/0	-

Reset Counters Restart Firewall

## 10.2.3 Routes

This section display information about routing list for current connecting device.

### 10.2.3.1 ARP

ARP		
IPv4-Address	MAC-Address	Interface
192.168.1.105	00:0d:f0:ac:c8:63	br-lan
192.168.1.118	80:19:34:c9:04:00	br-lan
10.15.1.142	00:10:f3:50:99:c0	eth0.2
10.15.1.254	78:48:59:64:5b:44	eth0.2
192.168.1.142	94:a1:a2:87:6f:08	br-lan
192.168.1.110	c4:54:44:de:fe:a5	br-lan
192.168.1.206	94:a1:a2:87:6f:48	br-lan
192.168.1.219	08:3e:8e:67:64:03	br-lan
10.15.1.201	00:26:73:29:15:7c	eth0.2

Displays APR table information of NIO200 including IPv4 address, MAC address and connecting interface.

### 10.2.3.2 Active IPv4-Routes

Active IPv4-Routes				
Network	Target	IPv4-Gateway	Metric	Table
wan	0.0.0.0/0	10.15.1.254	0	main
wan	10.15.1.0/24		0	main
lan	192.168.1.0/24		0	main

Displays active WAN and LAN port's IPv4 routing table.

### 10.2.3.3 Active IPv6-Routes

Active IPv6-Routes				
Network	Target	Source	Metric	Table
lan	fdfc:68c3:19eb:0:e5df:2aba:f91:5221		0	main
lan	fdfc:68c3:19eb::/64		1024	main
wan	:::1		0	local
wan	:::2		0	local
wan	:::c		0	local
wan	:::1.2		0	local
wan	:::1.3		0	local
wan	:::1:#f50:9e09		0	local
lan	:::/8		256	local
(eth0)	:::/8		256	local
wan	:::/8		256	local
lan	:::/8		256	local
lan	:::/8		256	local

Displays active IPv6 routing table of WAN and LAN port.

### 10.2.3.4 IPv6 Neighbors

IPv6 Neighbours		
IPv6-Address	MAC-Address	Interface
fdfc:68c3:19eb:0:1f4:f243:8e92:e881	80:19:34:c9:04:00	lan
fdfc:68c3:19eb:0:e5df:2aba:f91:5221	80:19:34:c9:04:00	lan
fdfc:68c3:19eb::3b0	00:0d:f0:ac:c8:63	lan
fdfc:68c3:19eb:0:21cf:78b5:a2c9:e438	00:0d:f0:ac:c8:63	lan
fdfc:68c3:19eb:0:b815:35d6:d8b7:dff8	00:0d:f0:ac:c8:63	lan
fdfc:68c3:19eb:0:691a:9a70:b879:924d	80:19:34:c9:04:00	lan
fdfc:68c3:19eb:0:468:1e7:d4fe:8c9a	9c:2a:70:1b:4c:9d	lan
fdfc:68c3:19eb:0:f118:d10c:ab71:1676	80:19:34:c9:04:00	lan
fdfc:68c3:19eb:0:7c3a:bc4c:52a3:da5a	00:0d:f0:ac:c8:63	lan
fdfc:68c3:19eb:0:6046:1236:d6c8:82c:1	00:0d:f0:ac:c8:63	lan
fdfc:68c3:19eb:0:c654:48ff:fede:fea5	c4:54:44:da:fa:a5	lan
fdfc:68c3:19eb:0:a151:5f16:e22f:fc7c	c4:54:44:da:fa:a5	lan
fdfc:68c3:19eb:0:61ad:92b6:99e2:bf9b	80:19:34:c9:04:00	lan

Display connected device with IPv6 information.

## 10.2.4 System Log

The “System Log” Web page contains the events log in NIO200 system for trouble shooting reference.

```
System Log
Tue Jul 10 01:58:46 2018 daemon.info mstpd: error, ethtool_get_speed_duplex: Cannot get speed/duplex for wlan1: Operation not supported
Tue Jul 10 01:58:46 2018 daemon.info mstpd: set_if_up: Port wlan1 : up
Tue Jul 10 01:58:46 2018 daemon.info mstpd: error, ethtool_get_speed_duplex: Cannot get speed/duplex for wlan1: Operation not supported
Tue Jul 10 01:58:46 2018 daemon.info mstpd: set_if_up: Port wlan1 : up
Tue Jul 10 01:58:46 2018 daemon.info mstpd: error, ethtool_get_speed_duplex: Cannot get speed/duplex for wlan1: Operation not supported
Tue Jul 10 01:58:46 2018 kern.info kernel: [1439056.639602] br-lan: port 4(wlan1) entered learning state
Tue Jul 10 01:58:46 2018 kern.info kernel: [1439056.639811] br-lan: port 4(wlan1) entered forwarding state
Tue Jul 10 01:59:04 2018 daemon.notice netifd: Interface 'lan' is now down
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_br_up: br-lan was up. Set down
Tue Jul 10 01:59:04 2018 daemon.info mstpd: MSTP_OUT_set_state: br-lan:eth1.0 entering disabled state
Tue Jul 10 01:59:04 2018 kern.info kernel: [1439075.062970] br-lan: port 4(wlan1) entered disabled state
Tue Jul 10 01:59:04 2018 kern.info kernel: [1439075.063040] br-lan: port 3(wlan0) entered disabled state
Tue Jul 10 01:59:04 2018 kern.info kernel: [1439075.065882] br-lan: port 1(eth1) entered disabled state
Tue Jul 10 01:59:04 2018 daemon.info mstpd: MSTP_OUT_set_state: br-lan:eth2.0 entering disabled state
Tue Jul 10 01:59:04 2018 daemon.info mstpd: MSTP_OUT_set_state: br-lan:wlan0.0 entering disabled state
Tue Jul 10 01:59:04 2018 daemon.info mstpd: MSTP_OUT_set_state: br-lan:wlan1.0 entering disabled state
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port wlan1 : up
Tue Jul 10 01:59:04 2018 daemon.info mstpd: error, ethtool_get_speed_duplex: Cannot get speed/duplex for wlan1: Operation not supported
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port wlan0 : up
Tue Jul 10 01:59:04 2018 daemon.info mstpd: error, ethtool_get_speed_duplex: Cannot get speed/duplex for wlan0: Operation not supported
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port eth1 : down
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port eth1 : down
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port eth2 : down
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port eth2 : down
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port wlan0 : up
Tue Jul 10 01:59:04 2018 daemon.info mstpd: error, ethtool_get_speed_duplex: Cannot get speed/duplex for wlan0: Operation not supported
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port wlan0 : up
```

## 10.2.5 Kernel Log

The “Kernel Log” displays the record of kernel activities. The administrator can monitor the system status by checking this log.

























```
NEXCOM NIO200 Status - System - Network - Logout

Kernel Log

[ 0.000000] Using P1020 RDB machine description
[ 0.000000] Memory CAM mapping: 256/256/256 Mb, residual: 256Mb
[ 0.000000] Linux version 3.14.27 (rnsu@rnsu-vm) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014.04 r682) ) #20 SMP Thu Oct 25 12:17:26 CST 2018
[ 0.000000] Found legacy serial port 0 for /soc@ffe00000/serial@4500
[ 0.000000] mem=ffe04500, taddr=ffe04500, irq=0, clk=399999996, speed=0
[ 0.000000] Found legacy serial port 1 for /soc@ffe00000/serial@4600
[ 0.000000] mem=ffe04600, taddr=ffe04600, irq=0, clk=399999996, speed=0
[ 0.000000] CPU maps initialized for 1 thread per core
[ 0.000000] (thread shift is 0)
[ 0.000000] bootconsole [udbg0] enabled
[ 0.000000] MPC85xx RDB board from Freescale Semiconductor
[ 0.000000] Top of RAM: 0x30000000, Total RAM: 0x30000000
[ 0.000000] Memory hole size: 0MB
[ 0.000000] Zone ranges:
[ 0.000000] DMA [mem 0x00000000-0x20000000]
[ 0.000000] Normal empty
[ 0.000000] Movable zone start for each node
[ 0.000000] Early memory node ranges
[ 0.000000] node 0: [mem 0x00000000-0x20000000]
[ 0.000000] node 0: [mem 0x00000000-0x20000000]
[ 0.000000] node 0: [mem 0x00000000-0x20000000]
```

## 10.2.6 Processes

This Webpage is designed for detailed trouble shooting/status monitoring by professional personnel in the field. Any improper terminating or killing individual process tasks may cause device malfunction. **It's highly recommended to keep this Firewall setup page as it is.**

Processes							
This list gives an overview over currently running system processes and their status.							
PID	Owner	Command	CPU usage (%)	Memory usage (%)	Hang Up	Terminate	Kill
1	root	/sbin/procd	0%	0%	 Hang Up	 Terminate	 Kill
2	root	[kthreadd]	0%	0%	 Hang Up	 Terminate	 Kill
3	root	[kssoftirqd/0]	0%	0%	 Hang Up	 Terminate	 Kill
5	root	[kworker/0.0H]	0%	0%	 Hang Up	 Terminate	 Kill
7	root	[rcu_sched]	0%	0%	 Hang Up	 Terminate	 Kill
8	root	[rcu_bh]	0%	0%	 Hang Up	 Terminate	 Kill
9	root	[migration/0]	0%	0%	 Hang Up	 Terminate	 Kill
10	root	[migration/1]	0%	0%	 Hang Up	 Terminate	 Kill

## 10.2.7 Real-time Graphic

This section provides utilities to monitor NIO200 system information including real-time load, real-time Ethernet traffic, Real-time wireless signal and real-time associated device traffic.

To monitor status in this section, please make sure WebUI “auto refresh” function must be **“turn on”**.

**AUTO REFRESH ON**

### 10.2.7.1 Load



Display real-time CPU average loading percentage.  
i.e.

1 Minute Load:	0.08	Average:	0.08	Peak:	0.33
5 Minute Load:	0.33	Average:	0.33	Peak:	0.39
15 Minute Load:	0.34	Average:	0.34	Peak:	0.36

1 minute	Minimum	8%	Average	8%	Peak	33%
5 minutes		33%		33%		39%
15 minutes		34%		34%		36%

10.2.7.2 Traffic

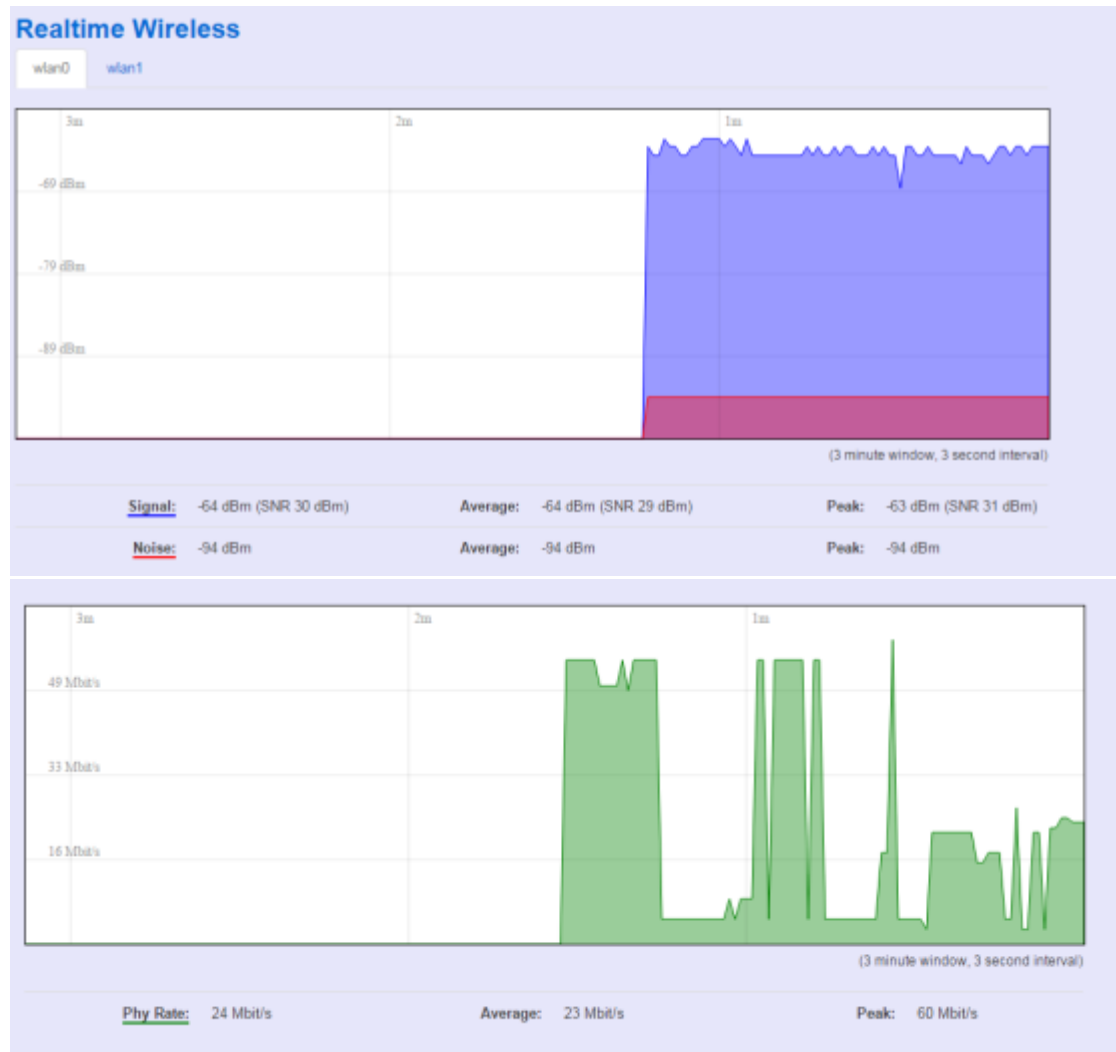


Display NIO200 real-time traffic loading of Ethernet, WLAN and internal bridge interfaces.

**Inbound:** Incoming data throughput of the observed interface.

**Outbound:** Outgoing data throughput of the observed interface.

### 10.2.7.3 Wireless



Display Wireless real-time signal quality including signal level, noise and data rate.

**wlan0:** Radio0 information.

**wlan1:** Radio1 information.

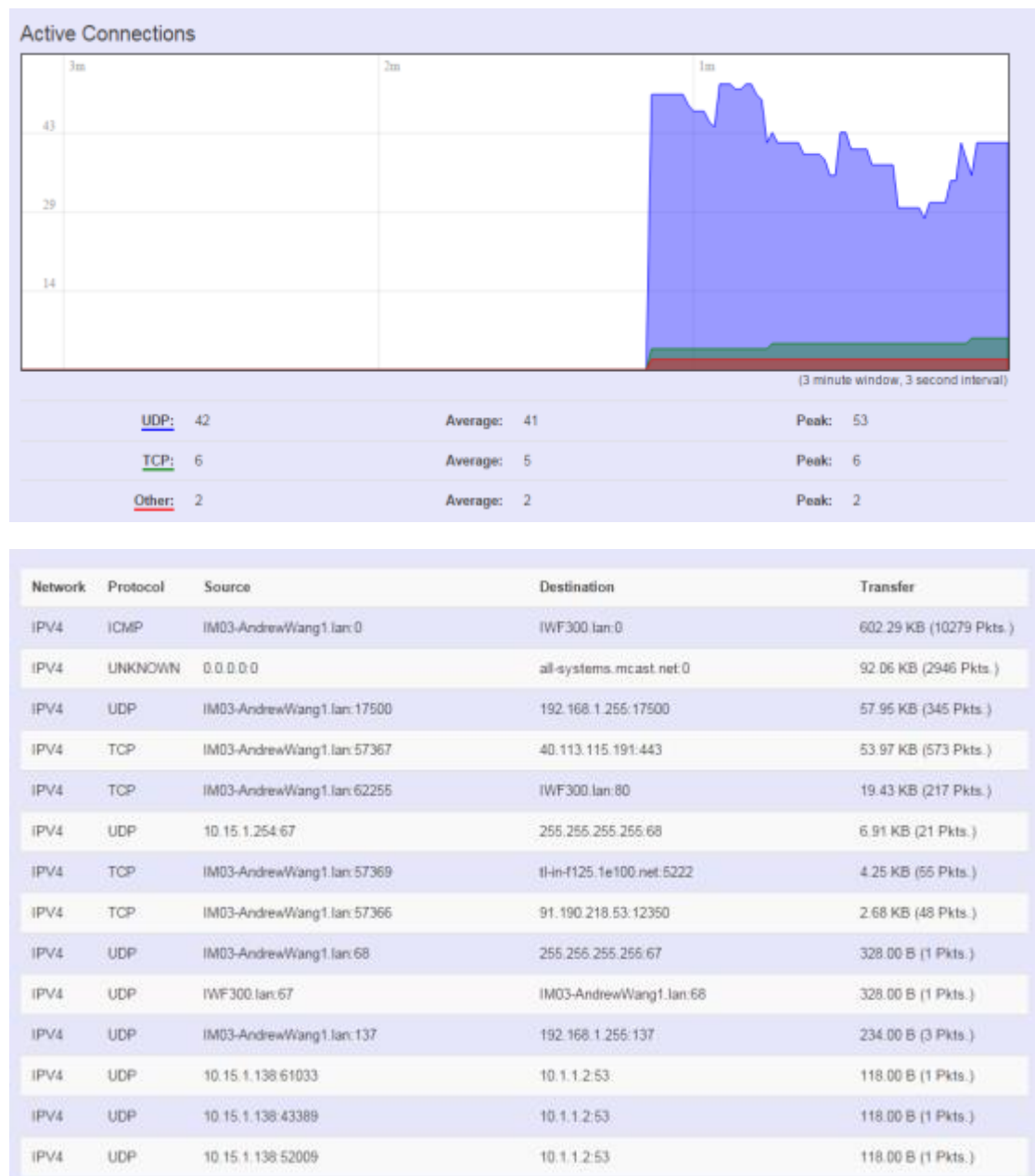
Note:

There will be no radio information when the WLAN interface is disabled.



### 10.2.7.4 Connections

This “Connections” displays NIO200 real-time active TCP/UDP/ICMP,... connection information for trouble shooting reference.



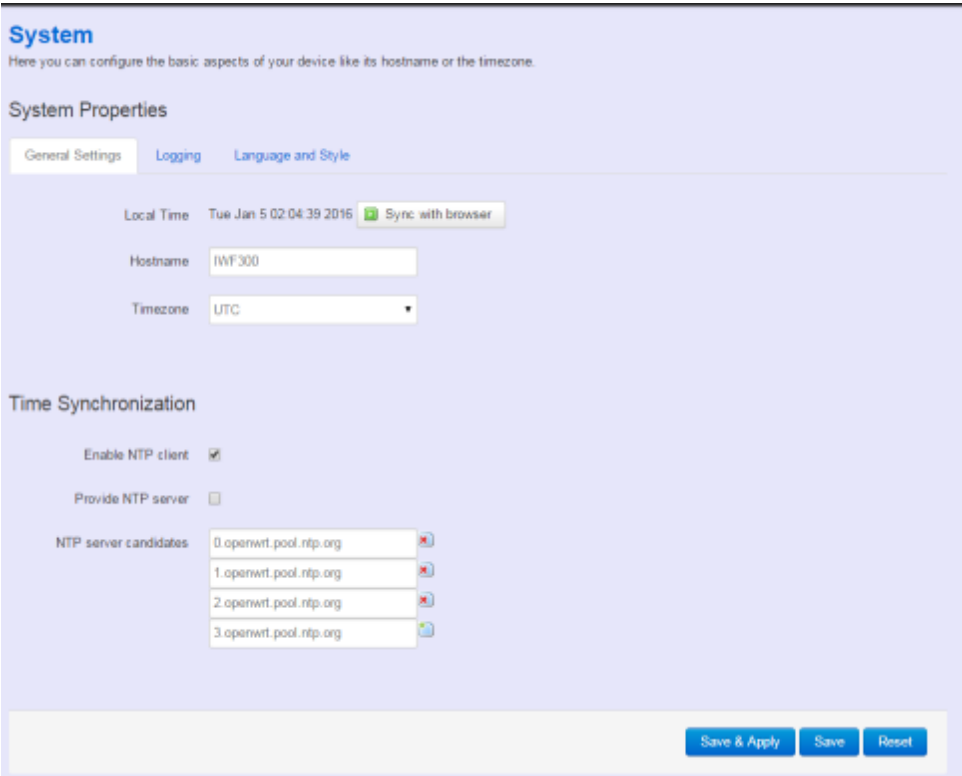
## 10.3 System

To setup detail configuration about NIO200 system, click the “System” under the page bar, then select the item of System, Administration, SNMP, Backup/Flash Firmware and Reboot from the pull-down list like below screen.

### 10.3.1 System

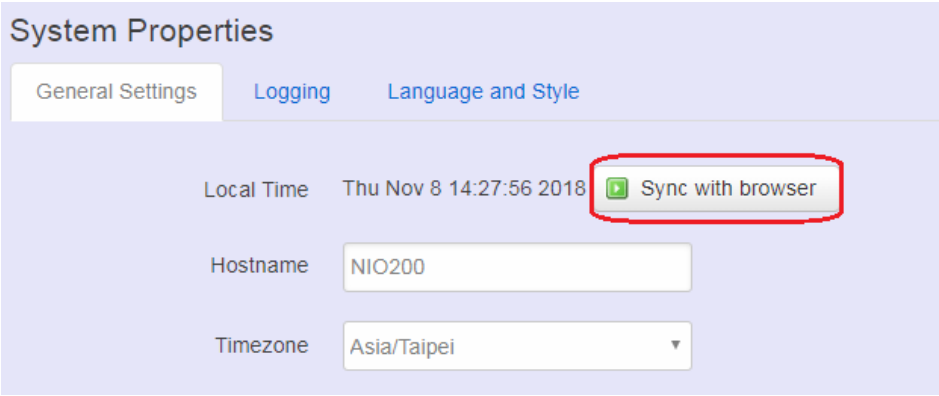
#### 10.3.1.1 General Settings

This section provide general settings of NIO200 including Time, Host name, Time zone and NTP.




The screenshot shows the 'System Properties' configuration page for NIO200. The 'General Settings' tab is active. The 'Local Time' is displayed as 'Tue Jan 5 02:04:39 2016' with a 'Sync with browser' button. The 'Hostname' is 'NWF300' and the 'Timezone' is 'UTC'. The 'Time Synchronization' section has 'Enable NTP client' checked and 'Provide NTP server' unchecked. Four NTP server candidates are listed, all pointing to '0.openwrt.pool.ntp.org'. At the bottom are 'Save & Apply', 'Save', and 'Reset' buttons.

Click “Sync with browser” let NIO200 sync time with your computer. And select country from the pull-down list in the Timezone.



This screenshot shows the same 'System Properties' page after modifications. The 'Local Time' is now 'Thu Nov 8 14:27:56 2018'. The 'Sync with browser' button is highlighted with a red rectangle. The 'Hostname' has been changed to 'NIO200' and the 'Timezone' is now 'Asia/Taipei'.

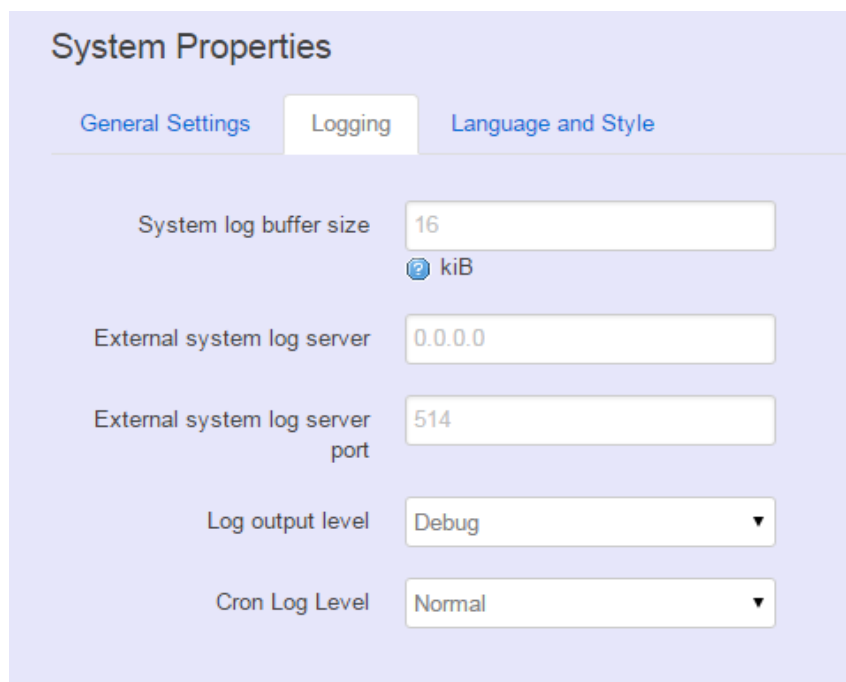
To make NIO200 system get time synchronization with NTP server, user may enable the NTP client and input the address of an NTP server to get the time updates.



The image shows a 'Time Synchronization' configuration window. It has a title bar 'Time Synchronization'. Below the title, there are two checkboxes: 'Enable NTP client' which is checked, and 'Provide NTP server' which is unchecked. Below these, there is a section labeled 'NTP server candidates' which contains a list of four text input fields. Each field contains the address '0.openwrt.pool.ntp.org', '1.openwrt.pool.ntp.org', '2.openwrt.pool.ntp.org', and '3.openwrt.pool.ntp.org' respectively. To the right of each input field is a small red 'X' icon, except for the last one which has a green plus icon.

### 10.3.1.2 Logging

This section provides the setting of log configuration.



The image shows a 'System Properties' configuration window with three tabs: 'General Settings', 'Logging', and 'Language and Style'. The 'Logging' tab is selected. It contains five configuration items: 'System log buffer size' with a value of '16' and a unit selector set to 'kiB'; 'External system log server' with a value of '0.0.0.0'; 'External system log server port' with a value of '514'; 'Log output level' with a dropdown menu set to 'Debug'; and 'Cron Log Level' with a dropdown menu set to 'Normal'.

**System log buffer size:** The size of log information. Unit: Kbytes.

**External system log server:** The server address of external log server.

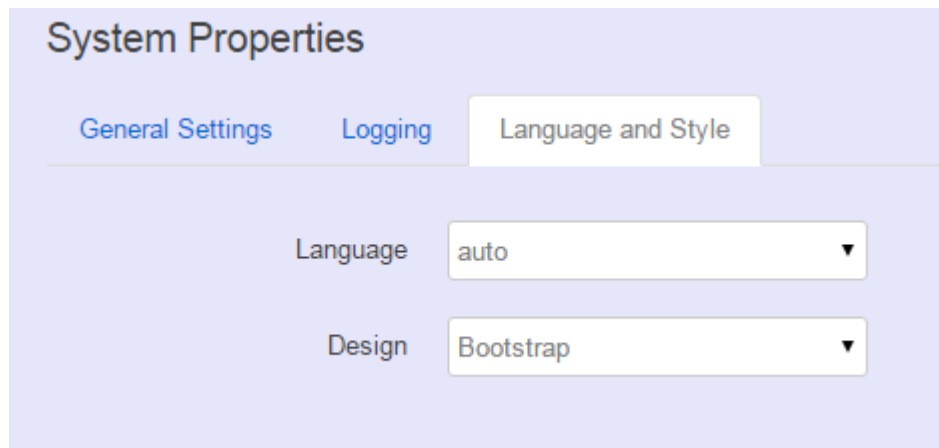
**External system log server port:** The port number of external log server.

**Log output level:** The output information of log, including Debug, Info, Notice, Warning, Error, Critical, Alert, and Emergency.

**Cron Log Level:** The minimal level for cron messages to be logged to syslog.

### 10.3.1.3 Language and Style

This section provides setting of language and WebUI style. NIO200 only provides English as default style.

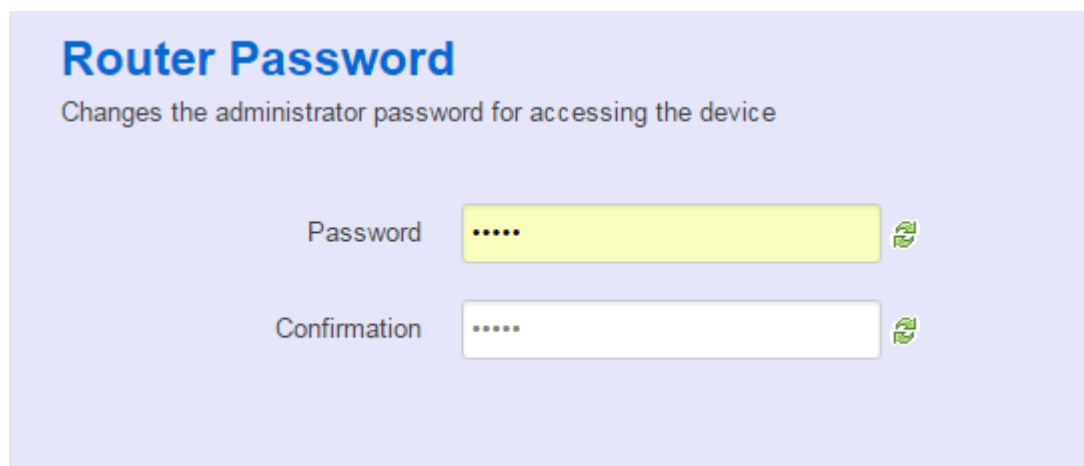


The screenshot shows the 'System Properties' configuration page. At the top, there are three tabs: 'General Settings', 'Logging', and 'Language and Style'. The 'Language and Style' tab is selected. Below the tabs, there are two dropdown menus. The first is labeled 'Language' and has 'auto' selected. The second is labeled 'Design' and has 'Bootstrap' selected.

## 10.3.2 Administration

### 10.3.2.1 Router Password

To change default password, enter new password and confirm new one.



The screenshot shows the 'Router Password' configuration page. The title 'Router Password' is in blue. Below it, a subtitle reads 'Changes the administrator password for accessing the device'. There are two input fields. The first is labeled 'Password' and contains five dots. The second is labeled 'Confirmation' and also contains five dots. To the right of each input field is a green icon representing a password strength indicator.

### 10.3.2.2 SSH Access





Secure Shell (SSH). Enable NIO200 to be accessed via SSH-based application. This increase the security in configuration of NIO200 remotely.

## SSH Access


Dropbear offers [SSH](#) network shell access and an integrated [SCP](#) server

### Dropbear Instance


Delete


Interface ☐ lan:    


☒ unspecified

 Listen only on the given interface or, if unspecified, on all

Port

 Specifies the listening port of this *Dropbear* instance

Password authentication ☒  Allow [SSH](#) password authentication

Allow root logins with password ☒  Allow the *root* user to login with password

**Interface:** Select the interface.

**Port:** Enter the port number for the communication via SSH.

**Password authentication:** Enable/Disable SSH password authentication.

**Allow root logins with password:** Enable/Disable the *root* user to login with password.

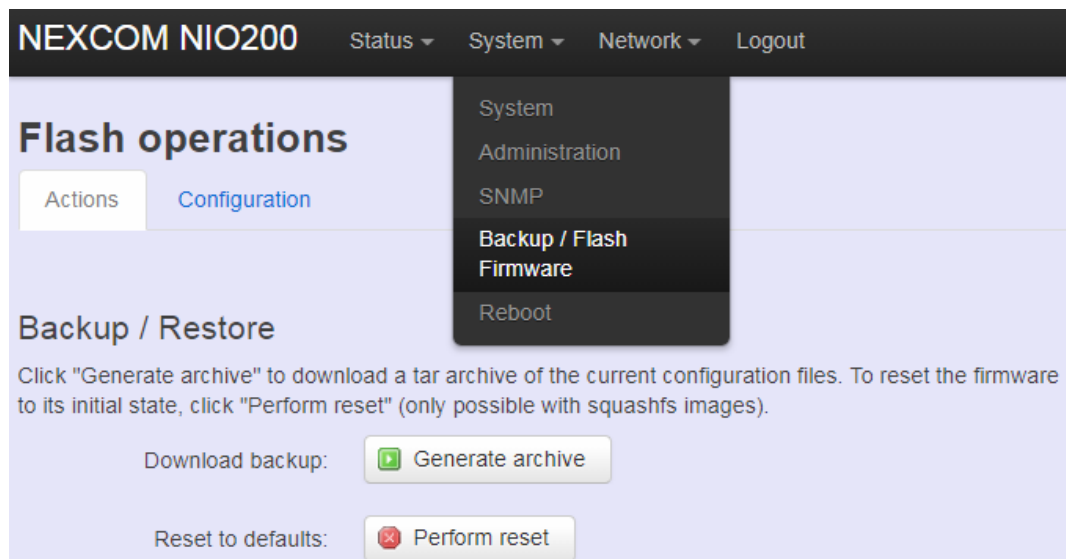
User may paste the public SSH-Keys (one per line) for additional SSH public-key authentication.

### SSH-Keys

Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

### 10.3.3 Backup/Flash Firmware

To upgrade new firmware on device, user may choose “Backup/Flash Firmware” from “Systme” in tool bar as below:

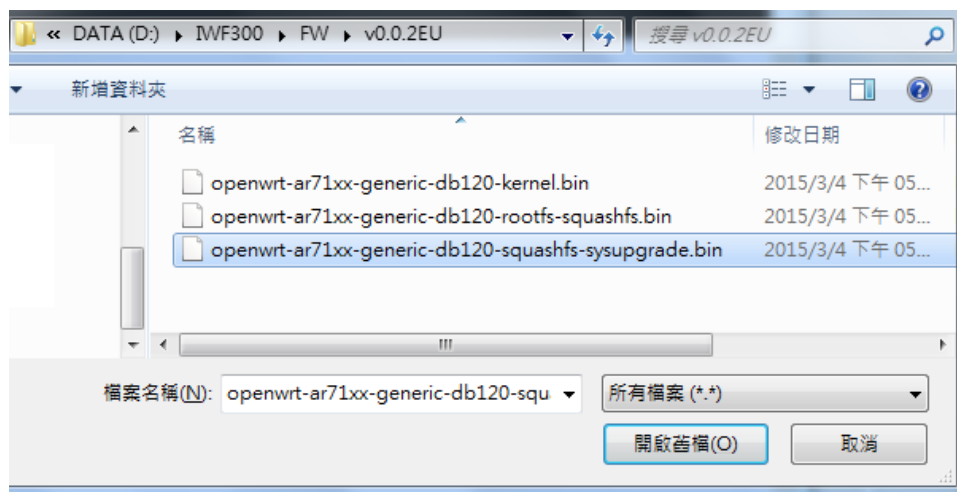


### 10.3.3.1 Upgrade Firmware

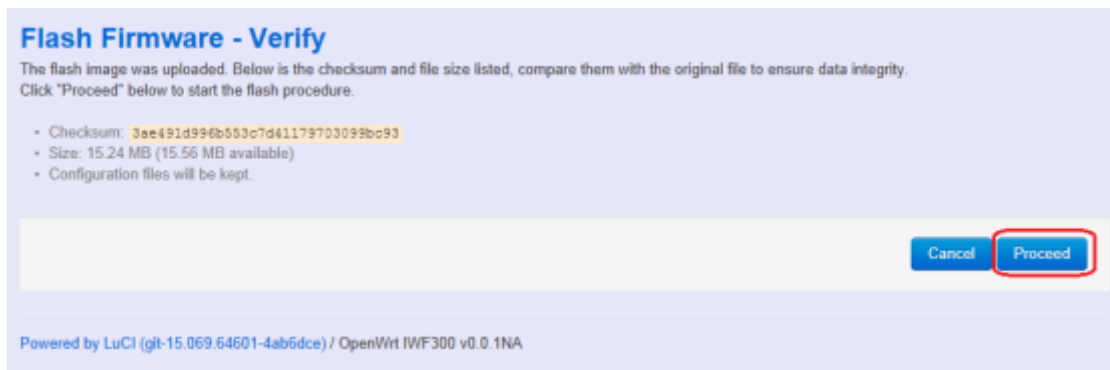
- To flash a new firmware image to NIO200, user may press the button of “Flash image” as below:



- Then select the correct firmware file from the file browser:

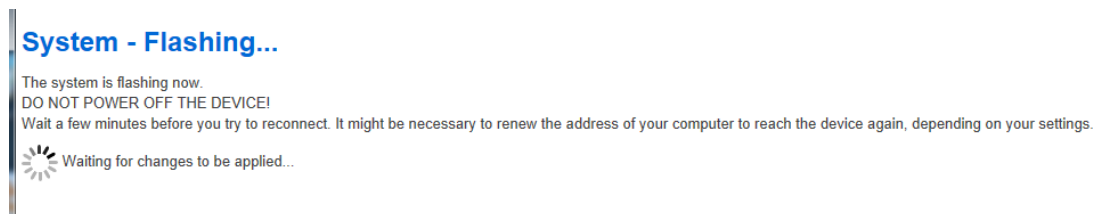


- Then, WebUI displays the file checksum.



- You can choose “Proceed” to start the upgrading.

**Note:** After you click “Proceed”, the DUT firmware will be upgraded with the file you selected, and the upgrade progress will display like below:

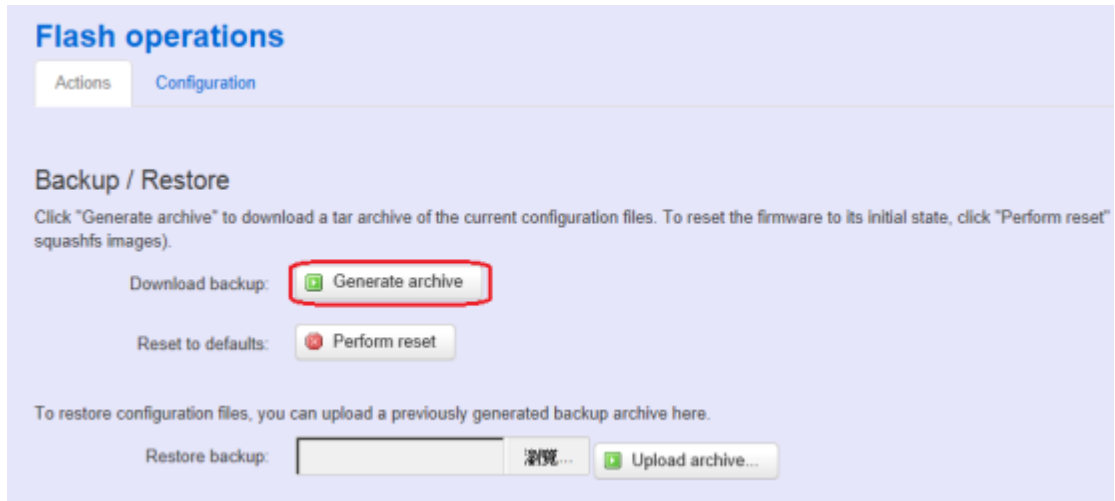


**Note:** The whole firmware image may take several minutes to complete the flash writing. **PLEASE DO NOT REBOOT OR POWER OFF THE DEVICE** before the whole progress.

If the firmware upgraded is successful, the WebUI should switch to the Login page. User can also confirm the firmware image is successfully upgraded via “Status” Web page.

### 10.3.3.2 Backup Configuration

To back up the configuration file, user may select the “Generate archive” button as below:



Then save it as a file in your PC.

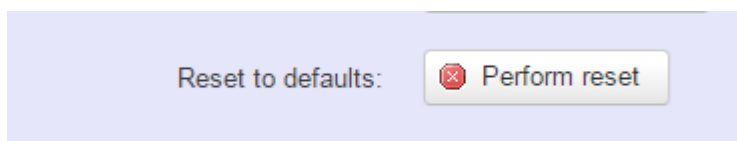
To restore previous configuration, user need to browse the backup file and then press "Upload archive..." button as below:



**Note:** After restore the file, system will apply the changes and automatically reboot. Due to configuration backup may cause IP address change, you have to enter new IP address accordingly. Otherwise, the new web page may not be accessible.

### 10.3.3.3 Reset to default

To reset NIO200 to factory default configuration, user will need to press "Perform reset" button as below.



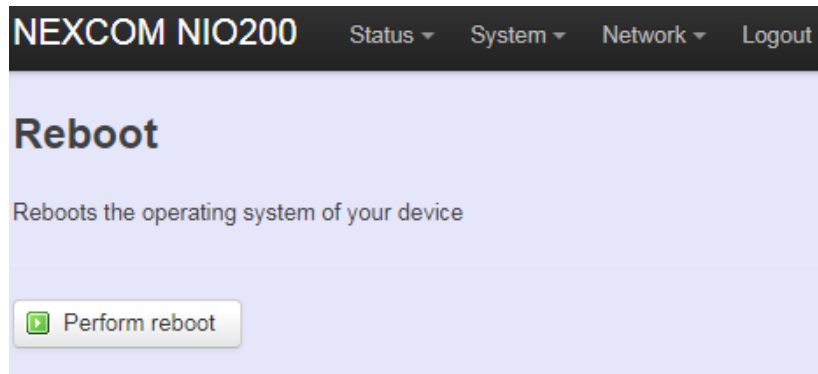
**Note:** The whole process may take several minutes to complete.



**PLEASE DO NOT REBOOT OR POWER OFF THE DEVICE** before the whole process being successfully done.

### 10.3.4 Reboot

Click the “Perform reboot” button will help to warm start the system. After system finish reboot process, it will back to Login page.

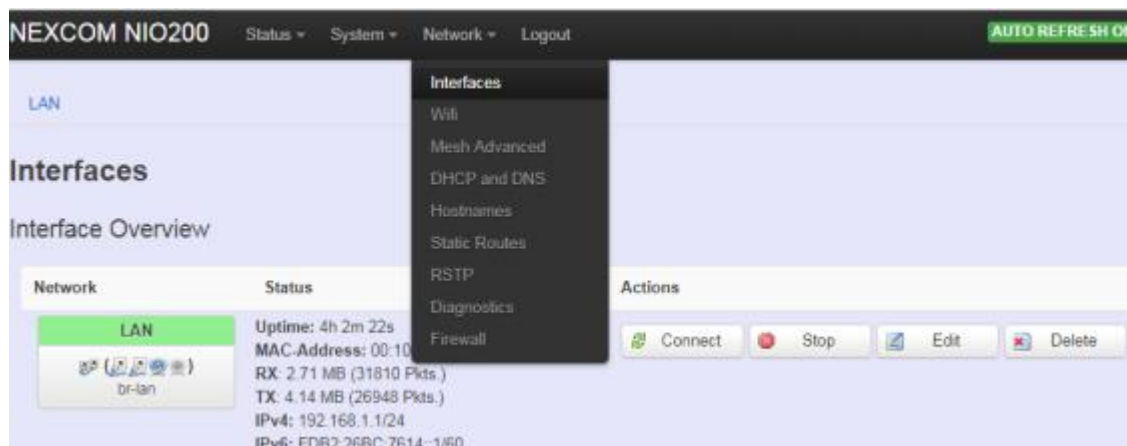


## 10.4 Network

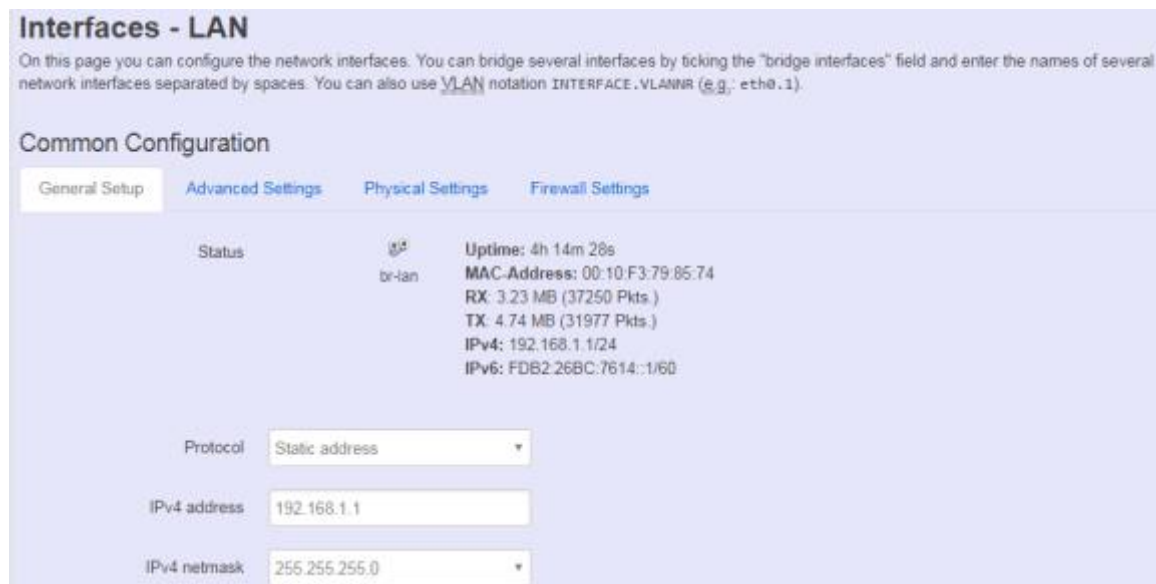
### 10.4.1 Interfaces

#### 10.4.1.1 Configuration of IP address

To set up a new IP address, please click “Network” from page bar, then select the “Interface”, and then click “Edit”



Edit IP address:



When modifying the IP address, user needs to input the IP address, netmask, gateway,... for this device and then click “Save & Apply” to save this new IP address into flash and apply it immediately.

**Note:** after apply new IP, it would take several minutes to switch to the Status page via

the new IP address. Please enter the new IP address on browser again if the browser does not switch to new Web page after 5 minutes.

## ● Interfaces overview

The screenshot shows the NEXCOM NIO200 web interface. At the top, there is a navigation bar with 'Status', 'System', 'Network', and 'Logout' tabs, and an 'AUTO REFRESH ON' button. The main content area is titled 'LAN' and 'Interfaces'. Below this, there is an 'Interface Overview' section. It contains a table with columns 'Network', 'Status', and 'Actions'. The 'LAN' interface is listed with its status and various statistics. Below the table, there is an 'Add new interface...' button. At the bottom, there is a 'Global network options' section with input fields for 'IPv6 ULA-Prefix' and 'Bridge Age Timeout'.

Network	Status	Actions
LAN br-lan	Uptime: 4h 21m 22s MAC-Address: 00:10:F3:79:85:74 RX: 3.56 MB (40678 Pkts.) TX: 5.09 MB (34954 Pkts.) IPv4: 192.168.1.1/24 IPv6: FDB2:26BC:7614::1/60	Connect Stop Edit Delete

Global network options

IPv6 ULA-Prefix: fdb2:26bc:7614::/48

Bridge Age Timeout: 300

**Connect:** Press this button to re-connect LAN interface to Ethernet network.

**Stop:** Shutdown this interface.

**Edit:** Modify WAN port setting or LAN port group settings

**Delete:** Delete this Interfaces from group

### Note:

- Do not perform "Stop" LAN interface when this is the only available interface, otherwise, the system will not be able to work.
- Under such condition, please press the button longer than 10 sec. to get system back to factory default setting. User can go on the configuration with default IP address "192.168.1.1".

## ● WAN(LAN) Interface overview

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces.

LAN

## Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANID (e.g.: eth0.1).

### Common Configuration

General Setup   Advanced Settings   Physical Settings   Firewall Settings

Status:	br-lan	Uptime: 2d 11h 12m 20s MAC-Address: 00:10:F3:62:AD:8B RX: 80.07 MB (735059 Pkts.) TX: 131.34 MB (893894 Pkts.) IPv4: 192.168.1.11/24 IPv6: FDB2:26BC:7614::1/60
---------	--------	--

Protocol: Static address

IPv4 address: 192.168.1.11

### <General Setup>

You can change your Protocol to link worldwide Internet.

DHCP client  
 Static address  
**DHCP client**  
 Unmanaged  
 PPP  
 PPTP  
 PPPoE  
 PPPoATM  
 UMTS/GPRS/EV-DO  
 L2TP

The default setting is DHCP client, send discover to find DHCP server.

#### Static address

Static IP (Manual):. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to NIO200 Wi-Fi interface.

#### DHCP client

When Dynamic IP (DHCP) is selected, the DHCP client to be functional once this selection is made

#### Unmanaged

This Interface have no configuration interface or options.

#### PPP




For old serial modem, provided point to point link for Wi-Fi interface.

#### PPPoE

For cable modem or ADSL user, link NIO200 Wi-Fi interface to your Internet provider.

### <Advanced Settings>

This is used for advanced settings and configure, strongly recommend user do not make change to this web page.

Bring up on boot	<input checked="" type="checkbox"/>	
Use builtin IPv6-management	<input checked="" type="checkbox"/>	
Use broadcast flag	<input type="checkbox"/>	 Required for certain ISPs, e.g. Charter with DOCSIS 3
Use default gateway	<input checked="" type="checkbox"/>	 If unchecked, no default route is configured
Use DNS servers advertised by peer	<input checked="" type="checkbox"/>	 If unchecked, the advertised DNS server addresses are ignored
Use gateway metric	<input type="text" value="0"/>	
Client ID to send when requesting DHCP	<input type="text"/>	
Vendor Class to send when requesting DHCP	<input type="text"/>	
Override MAC address	<input type="text" value="00:00:00:00:00:00"/>	
Override MTU	<input type="text" value="1500"/>	

### <Physical Settings>

Setup   **Advanced Settings**   Physical Settings   Firewall Settings

Bridge interfaces ☐ ? creates a bridge over specified interface(s)

Interface

- ☐ Ethernet Switch: "eth0"
- ☐ VLAN Interface: "eth0.1" (lan)
- ☒ VLAN Interface: "eth0.2" (wan)
- ☐ Ethernet Adapter: "eth1" (lan)
- ☐ VLAN Interface: "eth1.1"
- ☐ Wireless Network: Master "IWF300\_11N\_2G\_PM" (lan)
- ☐ Wireless Network: Mesh "IWF300\_11A\_5G\_PM" (lan)
- ☐ Custom Interface:

General Setup   **Advanced Settings**   Physical Settings   Firewall Settings

Bridge interfaces ☒ ? creates a bridge over specified interface(s)

Enable STP ☐ ? Enables the Spanning Tree Protocol on this bridge

Interface

- ☐ Ethernet Switch: "eth0"
- ☒ VLAN Interface: "eth0.1" (lan)
- ☐ VLAN Interface: "eth0.2" (wan)
- ☒ Ethernet Adapter: "eth1" (lan)
- ☐ VLAN Interface: "eth1.1"
- ☒ Wireless Network: Master "IWF300\_11N\_2G\_PM" (lan)
- ☒ Wireless Network: Mesh "IWF300\_11A\_5G\_PM" (lan)
- ☐ Custom Interface:

## Bridge interfaces

You can bridge an interfaces group for your WAN or LAN interface. Normally, only LAN interface need to enable bridge interfaces. After enable bridge interfaces, select interfaces to bridge.

## Interface

Select interfaces for your bridge group. Select both the Ethernet adapter ( most likely eth0.1' eth1) and the wireless network.

## ● DHCP Server

### <General Setup>

The screenshot shows the 'General Setup' tab of the DHCP Server configuration interface. It includes three tabs: 'General Setup' (selected), 'Advanced Settings', and 'IPv6 Settings'. The configuration options are as follows:

- Ignore interface:** A checkbox that is currently unchecked. To its right is a help icon and the text 'Disable DHCP for this interface.'
- Start:** A text input field containing the value '100'. Below it is a help icon and the text 'Lowest leased address as offset from the network address.'
- Limit:** A text input field containing the value '150'. Below it is a help icon and the text 'Maximum number of leased addresses.'
- Leasetime:** A text input field containing the value '12h'. Below it is a help icon and the text 'Expiry time of leased addresses, minimum is 2 minutes (2m)'.

**Ignore Interface:** Select this option to disable your DHCP server, you will need static IP or another DHCP server for your network interfaces. Default is “enable DHCP”

### <Advanced Settings>

The screenshot shows the 'Advanced Settings' tab of the DHCP Server configuration interface. It includes three tabs: 'General Setup', 'Advanced Settings' (selected), and 'IPv6 Settings'. The configuration options are as follows:

- Dynamic DHCP:** A checkbox that is checked. To its right is a help icon and the text 'Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.'
- Force:** A checkbox that is unchecked. To its right is a help icon and the text 'Force DHCP on this network even if another server is detected.'
- IPv4-Netmask:** A text input field. Below it is a help icon and the text 'Override the netmask sent to clients. Normally it is calculated from the subnet that is served.'
- DHCP-Options:** A text input field. Below it is a help icon and the text 'Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.'

**Dynamic DHCP:** Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

**Force:** Force DHCP on this network even if another server is detected.

## 10.4.2 Wi-Fi

### 10.4.2.1 Wireless Overview

**Wireless Overview**

radio0: Mesh "Test"   radio0: Mesh "backbone"   radio1: Mesh "MESH\_CAN4"

**Generic MAC80211 802.11an (radio0)**  
Channel: 36 (5.180 GHz) | Bitrate: ? Mbit/s

SSID: backbone | Mode: Mesh | MAC: 00:10:F3:62:38:87  
BSSID: 00:00:00:00:00:00 | Encryption: None

SSID: Test | Mode: Mesh | MAC: 00:10:F3:62:38:87  
BSSID: 00:00:00:00:00:00 | Encryption: None

**Generic MAC80211 802.11an (radio1)**  
Channel: 36 (5.180 GHz) | Bitrate: ? Mbit/s

SSID: MESH\_CAN4 | Mode: Mesh  
MAC: 00:00:00:00:00:00  
Encryption: unknown

**Associated Stations**

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
backbone	00:10:F3:6E:E6:A0	?	-68 dBm	-92 dBm	43.3 Mbit/s, MCS 10, 20MHz	72.2 Mbit/s, MCS 7, 20MHz

To set up the Wireless configuration, please select “Network” in the tab , then select “Wi-Fi”, which would show you the current radio interfaces status.

Wireless Overview includes channel’ SSID’ MAC address and security setting information.

**Scan:** Scan can explore how many AP signals can be detected. This is a good way to get the idea about how noisy the installation site is. User can choose a channel which is less interference with other APs.

**Join Network: Wireless Scan**

NEXCOM\_2.4G  
Channel: 1 | Mode: Master | BSSID: 00:10:F3:32:7C:6F | Encryption: WPA2 - 802.1X

O2O4  
Channel: 1 | Mode: Master | BSSID: 84:C9:B2:6B:4D:B2 | Encryption: WPA2 - PSK

168  
Channel: 1 | Mode: Master | BSSID: B4:B3:62:C2:A0:7D | Encryption: WPA2 - PSK

NEXCOM\_2.4G  
Channel: 1 | Mode: Master | BSSID: 00:10:F3:32:7B:7F | Encryption: WPA2 - 802.1X

**Add:** Add new virtual AP in the same radio interface. You will see new interface after click “add”

**Generic MAC80211 802.11abgn (radio0)**  
Channel: 7 (2.442 GHz) | Bitrate: ? Mbit/s

SSID: IWF300\_11N\_2G\_PM | Mode: Master  
BSSID: 00:10:F3:30:8A:22 | Encryption: WPA PSK (TKIP, CCMP)

SSID: OpenWrt | Mode: Master  
BSSID: 02:10:F3:30:8A:22 | Encryption: None



**Disable:** Disable the radio interface

**Edit:** Configure the radio interface

**Remove:** Remove radio interface. Please note that disable radio first when you don't want to use the radio interface.

### 10.4.2.2 Associated Stations

Associated stations show wireless client connection information. It includes the SSID wireless client connect' wireless client MAC/ IP address' RSSI signal strength and Tx/Rx rate.

Associated Stations						
SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
IWF300_11N_2G_PM	9C:2A:70:1B:4C:9D	192.168.1.215	-53 dBm	-93 dBm	162.0 Mbit/s, MCS 12, 40MHz	104.0 Mbit/s, MCS 13, 20MHz

### 10.4.2.3 Wireless configuration

Please select "network" -> "Wi-Fi" and click Edit to configure Radio0 or Radio1.

The screenshot shows the NEXCOM NIO200-11 web interface. The top navigation bar includes 'Status', 'System', 'Network', and 'Logout'. The 'Network' menu is expanded, showing options like 'Interfaces', 'Wi-Fi', 'Mesh Advanced', 'DHCP and DNS', 'Hostnames', 'Static Routes', 'RSTP', 'Diagnostics', and 'Firewall'. The 'Wi-Fi' option is selected. The main content area is titled 'Wireless Overview' and displays configuration for two radio interfaces: radio0 (Mesh 'Test') and radio1 (Mesh 'backbone'). For radio0, the 'Edit' button is highlighted. For radio1, the 'Edit' button is also highlighted.

The **Device Configuration** section covers physical settings of the radio hardware such as channel, transmit power...etc.

## Device Configuration

General Setup

Advanced Settings

Status

81% **Mode:** Master | **SSID:** IWF300\_11N\_2G\_PM  
**BSSID:** 00:10:F3:30:8A:22 | **Encryption:** WPA PSK (TKIP, CCMP)  
**Channel:** 7 (2.442 GHz) | **Tx-Power:** 20 dBm  
**Signal:** -53 dBm | **Noise:** -93 dBm  
**Bitrate:** 300.0 Mbit/s | **Country:** US

Wireless network is enabled

Disable

Operating frequency

Mode

N

Channel

auto

Width

40 MHz(AP or Client mode)

Transmit Power

20 dBm (100 mW)

## &lt;General setup&gt;

**Wireless network is enabled:** Enable or disable the radio interface

**Operating frequency:** Select radio frequency and channel bandwidth for signal transmission.

For channel bandwidth, please note you need to confirm AP/ client mode or mesh mode and which channel you will use

Width

40 MHz(AP or Client mode)  
20 MHz(AP or Client mode)  
40 MHz(AP or Client mode)  
40 plus MHz(Mesh mode, 2.4G(ch <= 6), 5G(ch=36,40,44,149)  
40 minus MHz(Mesh mode, 2.4G(ch >= 7), 5G(ch=48,153,157,161,165)

**Transmit Power:** Control the transmit power of a radio by selection of Transmission Power.

## &lt;Advanced settings&gt;

**Distance Optimization:** Specify the ACK timeout by entering the value manually. ACK timeout can be entered by defining the link distance. Too short value of the ACK timeout may cause transmission time out and no packet can be received. Too long value may cause low throughput rate.

**Fragmentation Threshold:** Default=off. Specify the Fragmentation threshold by entering the value manually [300-2346 bytes]. This is the maximum size for a packet before data is fragmented into multiple packets. Setting the Fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended

**RTS/CTS Threshold:** Default=off. RTS/CTS (Request to Send / Clear to Send) is the optional mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden node problem. RTS/CTS is an additional method to implement virtual carrier sensing in Carrier sense multiple access with collision avoidance (CSMA/CA). Specify the RTS threshold by entering the value manually [0-2346 bytes]. Typically, sending RTS/CTS frames does not occur unless the packet size exceeds this threshold.

This **Interface Configuration** section covers SSID' operation mode and encryption.

**NEXCOM NIO200-11** Status System Network Logout AUTO REFRESH ON

Distance Optimization   
Distance to farthest network member in meters.

Fragmentation Threshold

RTS/CTS Threshold

Transmitter/Receiver Antenna ☐ 1Tx1R ☐ 2Tx2R

**Interface Configuration**

General Setup Wireless Security

ESSID/Mesh ID

Mode Mesh, 802.11s

Network ☒ lan: ☐ create:

Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.

### <General setup>

**ESSID:** Edit the SSID or Mesh ID.

**Mode:** Select operation mode

- AP
- Client Router
- 802.11s ( Mesh mode)

### <Wireless Security>

**NEXCOM NIO200-15** Status System Network Logout AUTO REFRESH ON

Wireless network is disabled Enable

Operating frequency Mode Channel Width  
N 149 (5745 MHz) 20 MHz

Transmit Power 17 dBm (50 mW)  
dBm

**Interface Configuration**

General Setup Wireless Security MAC-Filter

Encryption No Encryption

No Encryption

WEP Open System

WEP Shared Key

WPA-PSK

WPA2-PSK

WPA-PSK/WPA2-PSK Mixed Mode

WPA-EAP

WPA2-EAP

Save & Apply
Save
Reset

**Encryption:** To setup the Security on Radio, please select one of the Encryption:

- No Encryption

- WEP Open System: WEP provides a basic level of security, preventing unauthorized access to the network. WEP uses static shared keys that are manually distributed to all clients that want to use the network
- WEP Shared Key: WEP provides a basic level of security, preventing unauthorized access to the network, and encrypting data transmitted between wireless clients and an access point. WEP uses static shared keys that are manually distributed to all clients that want to use the network
- WPA-PSK: Clients using WPA for authentication
- WPA2-PSK: Clients using WPA2 for authentication
- WPA-PSK/WPA2-PSK Mixed Mode: Clients using WPA or WPA2 for authentication

Interface Configuration

General Setup Wireless Security

Encryption WPA-PSK/WPA2-PSK Mixed Mode

Cipher auto

Key 12345678

**Cipher** : To select cipher, recommend to select TKIP and CCMP(AES)

- Force CCMP(AES)
- Force TKIP
- Force TKIP and CCMP(AES)

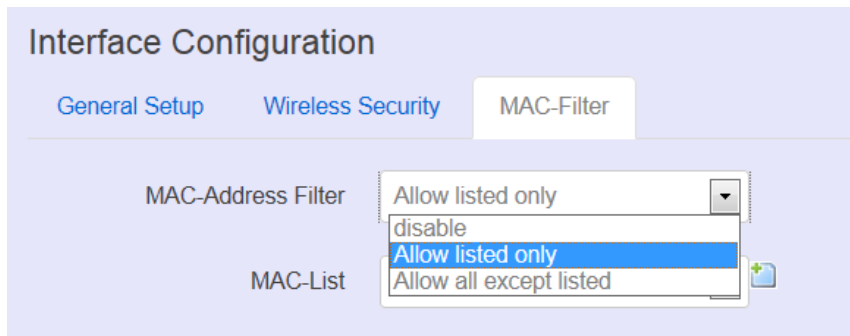
Encryption WPA-PSK/WPA2-PSK Mixed Mode

Cipher Force TKIP and CCMP (AES)

Key 12345678

The cycle icon will display the characters you just input.

<MAC filter>

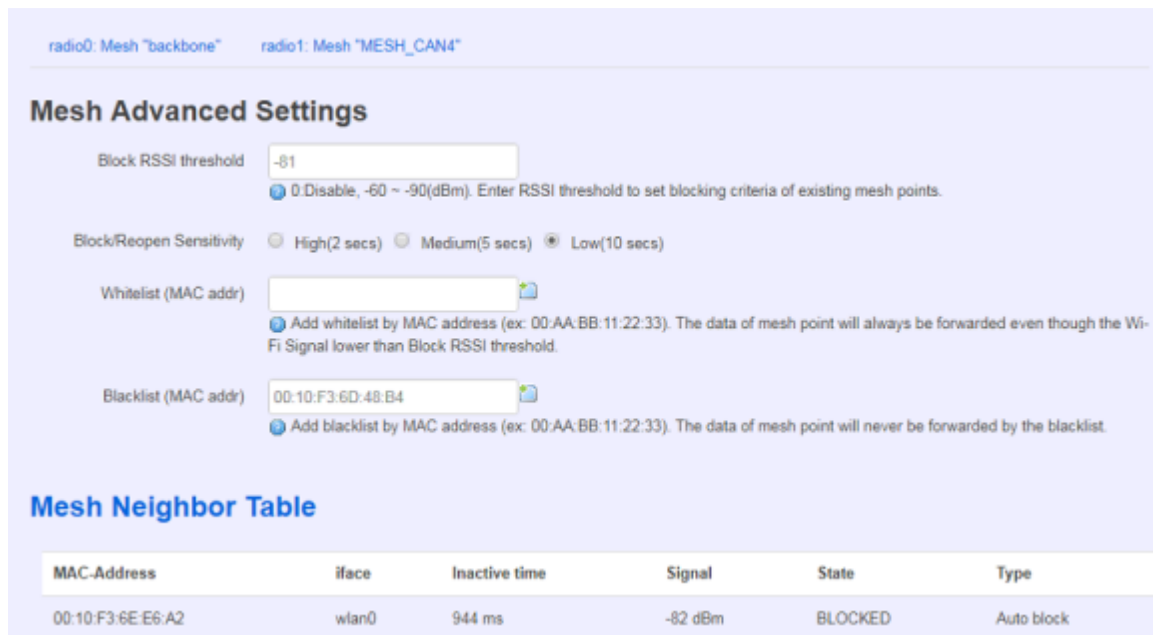


Select MAC Filtering. Specifies the MAC address to block or allow traffic from.

### 10.4.3 Mesh Advanced

Mesh Advanced setting contains the important information about real Mesh connection path and Neighbor node signal strength and blocking status. This is an advanced mechanism to keep Mesh network in stable and optimized condition.

#### 10.4.3.1 Mesh Advanced



- Block RSSI threshold: This is used to set the threshold of blocking current associated Mesh points. If there is only one Mesh link exists, then please select "0: disable".
  - 0: Disable
  - Input value between -60 ~ -90(dBm)
- Block/Reopen Sensitivity: This is a criteria for choosing the sensitivity level in Mesh path availability.
  - High:
    - After continuous 2 seconds with signal level higher than Block threshold, the blocked Mesh link can be available again.
    - After continuous 2 seconds with signal level lower than Block threshold, the

active Mesh link will be blocked.

■ Medium:

- After continuous 5 seconds with signal level higher than Block threshold, the blocked Mesh link can be available again.
- After continuous 5 seconds with signal level lower than Block threshold, the active Mesh link will be blocked.

■ Low:

- After continuous 10 seconds with signal level higher than Block threshold, the blocked Mesh link can be available again.
- After continuous 10 seconds with signal level lower than Block threshold, the active Mesh link will be blocked.

● Whitelist (MAC addr):

The Mesh device in Whitelist will be regarded available connecting path for data forwarding no matter the RSSI value is high or low.

● Blacklist (MAC addr):

The Mesh device in Blacklist will NOT be used for data forwarding no matter the RSSI value is high or low.

● Mesh Neighbor Table

**Mesh Neighbor Table**

MAC-Address	iface	Inactive time	Signal	State	Type
00:10:F3:6E:E6:A2	wlan0	828 ms	-79 dBm	BLOCKED	Auto block
00:10:F3:6E:E6:B6	wlan0	268 ms	-81 dBm	BLOCKED	Auto block
00:10:F3:6E:E6:A0	wlan0	8 ms	-79 dBm	BLOCKED	Auto block
00:10:F3:62:38:87	wlan0	96 ms	-65 dBm	ESTAB	Normal
00:10:F3:77:28:5D	wlan0	116 ms	-79 dBm	BLOCKED	Auto block
00:10:F3:6E:E6:9C	wlan0	512 ms	-80 dBm	BLOCKED	Auto block
00:10:F3:62:38:81	wlan0	324 ms	-68 dBm	ESTAB	Normal
00:10:F3:6D:48:B4	wlan0	872 ms	-85 dBm	BLOCKED	Auto block

- Iface: display the Mesh interface used in the Wi-Fi radio
- Inactive time: the elapsed time since last forward data by the according Mesh path.
- Shorter inactive time implies more frequently used in data forwarding by Mesh network. Too long inactive time means the Mesh path is almost un-used.
- Signal: display the dynamic RSSI signal strength when refresh
- State: display the current status is ESTAB ( established ) or BLOCKED ( blocked ). When BLOCKED, implies the signal strength is too low to use in data forwarding.

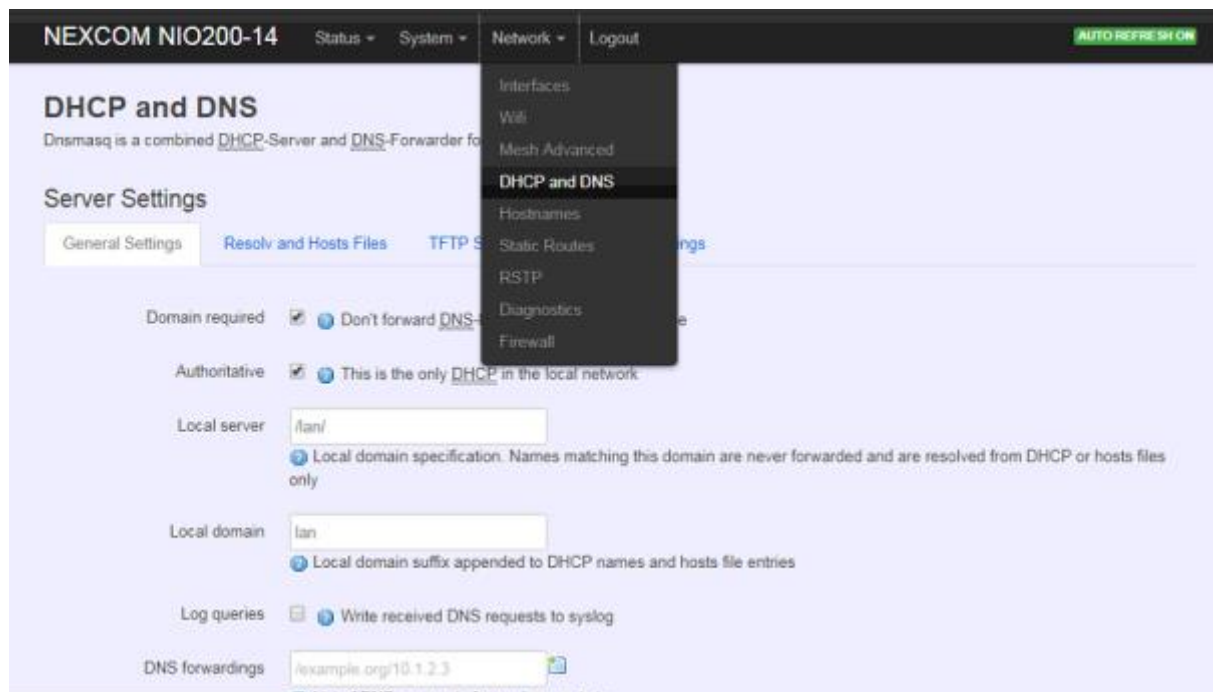
**Mesh Path Table**

Dest addr	Next hop	iface
00:10:F3:62:38:87	00:10:F3:62:38:87	wlan0
00:10:F3:62:38:81	00:10:F3:62:38:81	wlan0
00:10:F3:6E:E6:9C	00:10:F3:62:38:81	wlan0

- **Dest addr/Next hop:**  
When Dest (Destination) MAC address and Next hop MAC address is the same, the destination is available to connect directly from source Mesh node.  
When the two MAC address is different, the data forwarding to Destination MAC address should be routed via Next hop path.
- **Iface:** display the Mesh interface used in the Wi-Fi radio

**10.4.4 DHCP and DNS**

A combined DHCP-Server and DNS-Forwarder for NAT firewall is provided in NIO200. Click the “Network” -> “DHCP and DNS” in the GUI menu. The “DHCP and DNS” page will appear. There are four categories of settings or lease status: “Active DHCP Leases”, “Active DHCPv6 Leases”, “Static Leases”, and “Server Settings”.



Scroll to the following screen in the “DHCP and DNS” window.



**Active DHCP Leases**

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
There are no active leases.			

**Active DHCPv6 Leases**

Hostname	IPv6-Address	DUID	Leasetime remaining
There are no active leases.			

This screen displays the lease information to which DHCP server assigns automatically, including **Hostname**, **IP address**, **MAC address(or DUID)**, and Remaining Lease-time (DUID stands for the DHCP Unique Identifier). Please look at the frame in red above.

The next category that users can scroll to is “Static Leases” as follows.

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients by calculating MAC-Address. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

**Static Leases**

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. Use the *Add* Button to add a new lease entry. The *MAC-Address* identifies the host, the *IPv4-Address* specifies the fixed address to use and the *Hostname* is assigned as symbolic name to the requesting host.

Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)
This section contains no values yet			



Add

**Add:** Add a new lease entry.

After clicking “Add” button, a new entry with 4 blank input boxes will appear. Allow users to fill in the information such as The **MAC-Address** (identifies the host), the **IPv4-Address** (specifies the fixed address to use) and the **Hostname** (is assigned as symbolic name to the requesting host).

### Static Leases

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. Use the Add Button to add a new lease entry. The MAC-Address identifies the host, the IPv4-Address specifies the fixed address to use and the Hostname is assigned as symbolic name to the requesting host.

Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	 Delete
 Add				

**Delete:** delete the followed entry.

Scroll to the screen identified as “Server Settings” category.

There are 4 tabs to select more options for DHCP and DNS services in the NIO200

### 10.4.4.1 General Settings


#### Server Settings


General Settings


Resolve and Hosts Files


TFTP Settings


Advanced Settings


Domain required ☒  Don't forward DNS-Requests without DNS-Name


Authoritative ☒  This is the only DHCP in the local network


Local server   Local domain-specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only


Local domain   Local domain suffix appended to DHCP names and hosts file entries

Log queries ☐  Write received DNS requests to syslog

DNS forwardings   List of DNS servers to forward requests to

Rebind protection ☒  Discard upstream RFC1918 responses

Allow localhost ☒  Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services

Domain whitelist   List of domains to allow RFC1918 responses for

**Domain required:** default value is checked.

**Authoritative:** default value is checked.

### 10.4.4.2 Resolve and Hosts Files

**Server Settings**

[General Settings](#) [Resolv and Hosts Files](#) [TFTP Settings](#) [Advanced Settings](#)

Use `/etc/ethers` ☒ [Read /etc/ethers](#) to configure the DHCP-Server

Leasefile   
[file where given DHCP-leases will be stored](#)

Ignore resolve file ☐

Resolve file   
[local DNS file](#)

Ignore `/etc/hosts` ☐

Additional Hosts files

### 10.4.4.3 TFTP Settings

**IWF300** [Status](#) [System](#) [Network](#) [Logout](#) [AUTO REFRESH ON](#)

**Server Settings**

[General Settings](#) [Resolv and Hosts Files](#) [TFTP Settings](#) [Advanced Settings](#)

Enable TFTP server ☐

By default, TFTP server is not enabled.

## 10.4.4.4 Advanced Settings

NEXCOM NIO200-14   Status ▾   System ▾   Network ▾   Logout   [AUTO REFRESH ON](#)

### Server Settings

[General Settings](#)   [Resolv and Hosts Files](#)   [TFTP Settings](#)   [Advanced Settings](#)

Filter private ☒ Do not forward reverse lookups for local networks

Filter useless ☐ Do not forward requests that cannot be answered by public name servers

Localise queries ☒ Localise hostname depending on the requesting subnet if multiple IPs are available

Expand hosts ☒ Add local domain suffix to names served from hosts files

No negative cache ☐ Do not cache negative replies, e.g. for not existing domains

Additional servers file   
 This file may contain lines like 'server=/domain/1.2.3.4' or 'server=1.2.3.4' for domain-specific or full upstream DNS servers.

Strict order ☐ DNS servers will be queried in the order of the resolvfile

Bogus NX Domain Override   
 List of hosts that supply bogus NX domain results

---

DNS server port   
 Listening port for inbound DNS queries

DNS query port   
 Fixed source port for outbound DNS queries

Max. DHCP leases   
 Maximum allowed number of active DHCP leases

Max. EDNS0 packet size   
 Maximum allowed size of EDNS0 UDP packets

Max. concurrent queries   
 Maximum allowed number of concurrent DNS queries

### Active DHCP Leases

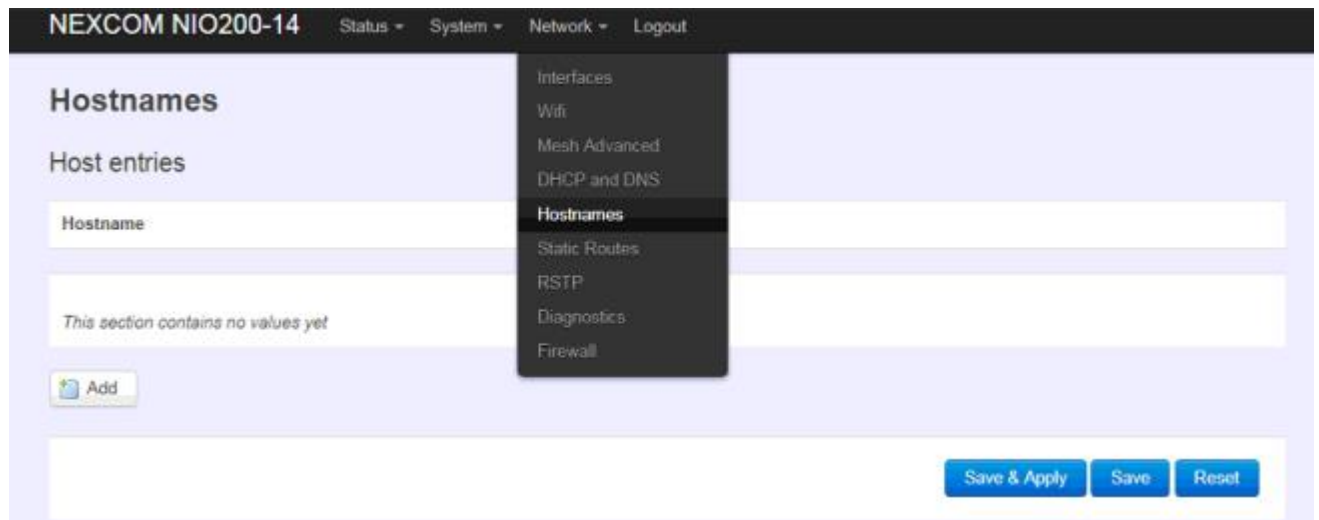
Hostname	IPv4-Address	MAC-Address	Leasetime remaining
----------	--------------	-------------	---------------------

**Max. DHCP Leases:** default value is unlimited.

**Max. concurrent queries:** default value is 150

## 10.4.5 Hostnames

Clicking the “Network” -> “Hostnames” in the GUI menu will appear the “Hostnames” page.



For those device does not have hostname or does not resolve automatically, users manually assign hostname-IP pair to specific devices.

**Add:** create a host entry (hostname-IP pair) for a specific device.

(For example, **Hostname** => “Test-Device”; **IP address** => “192.168.1.251”)

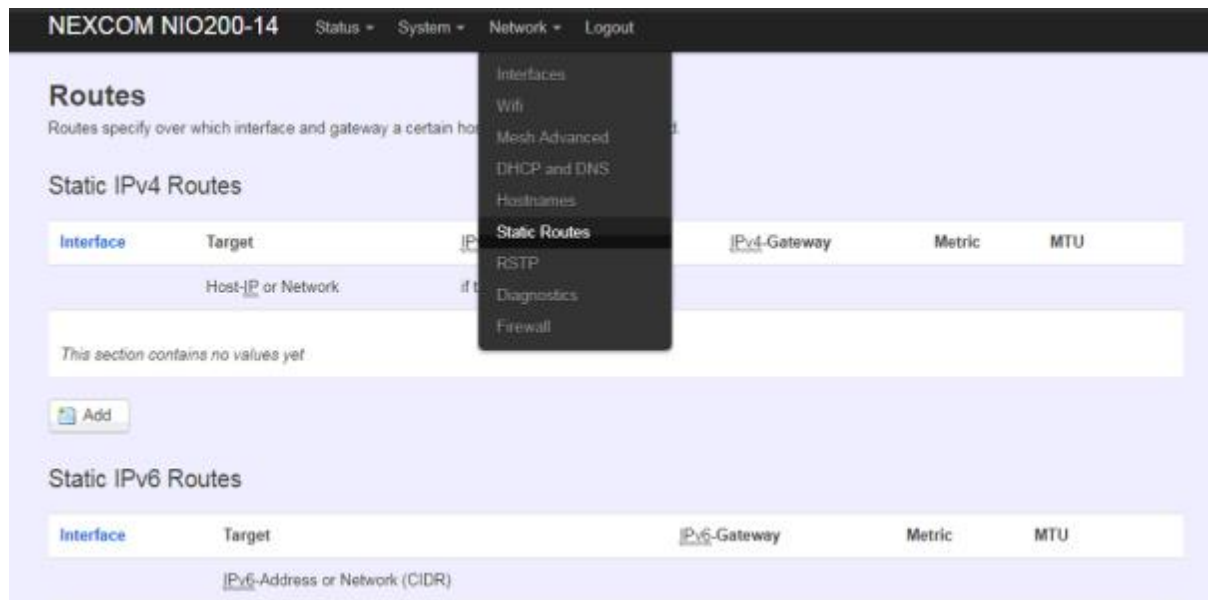


**Delete:** delete the followed host entry.

## 10.4.6 Static Routes

Clicking “Network” -> “Static Routes” in the GUI menu will appear the “Routes” page for two categories: “Static IPv4 Routes” and “Static IPv6 Routes”.

Static routes specify interface and gateway which certain host or network can be reached over. Such pair (interface and gateway) is called route.



For IPv4 network, scroll down to “Static IPv4 Routes” screen as follows.



**Add:** add an entry for route to an IPv4 network or host.

**For example:** Target network=192.168.10.0; Netmask=255.255.255.0; NIO200 WAN IP=192.168.0.1;

The route to be assigned will be “wan” for interface and “192.168.0.253” for gateway. Leave “Metric” and “MTU” field to have default values as 0 and 1500 respectively.



**Delete:** delete a followed route entry.

For IPv6 network, scroll down to “Static IPv6 Routes” screen as follows.

IWF300 Status System Network Logout



### Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU
IPv6-Address or Network (CIDR)				
This section contains no values yet!				
				

**Add:** add an entry for route to an IPv6 network or host.

Clicking “Add” button has an entry as follows.

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU	
lan			0	1500	
					

## 10.4.7 Diagnostics

Click “Network” -> “Diagnostics” in the GUI menu, and navigate to “Diagnostics” web page.



In this page, there are 3 utilities for users to diagnose interface settings and network paths: Ping, Traceroute, and Nslookup.



**Ping:** test the reachability of a host on an Internet Protocol (IP) network and measure the round-trip time for messages sent from the originating host to a destination host and back. The only required parameter is the name or IP address of the destination host.

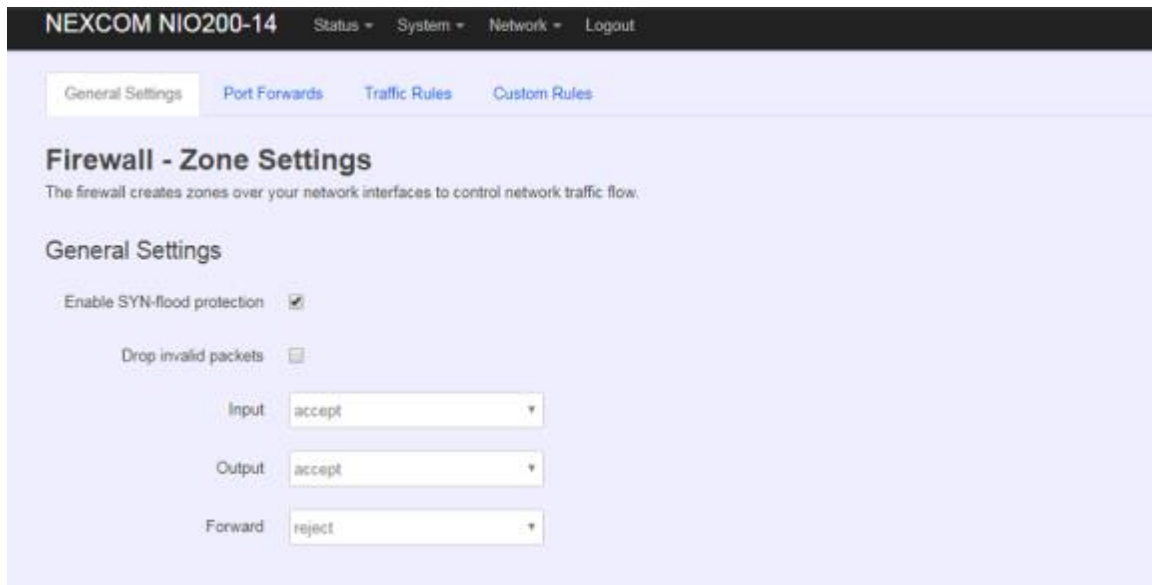
**Traceroute:** track the route packets taken from an IP network on their way to a given destination host. The only required parameter is the name or IP address of the destination host.

**Nslookup:** query the Domain Name System (DNS) to obtain domain name or IP address mapping.



## 10.4.8 Firewall

Click “Network” -> “Firewall” in the GUI menu, and navigate to page configuring firewall attributes in the NIO200 Wi-Fi interface.



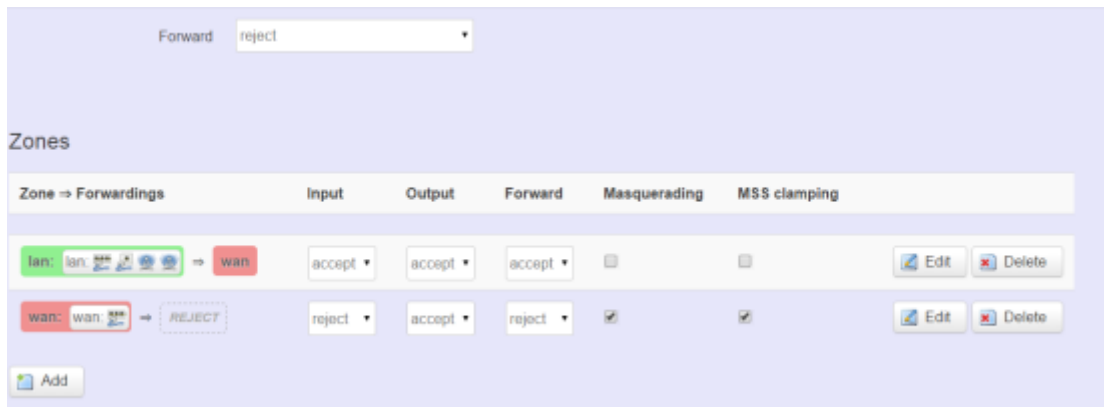
### 10.4.8.1 General Settings

Clicking “General Settings” tab on the top of screen will show the “Zone Settings” configuration including “General Settings” and “Zones” categories.

In the “General Settings” category, there are 5 basic options for traffic control over interfaces:

”Enable SYN-flood protection” (default: enabled), “Drop invalid packets” (default: disabled), “Input” (default: accept), “Output” (default: accept), and “Forward” (default: reject)

In the “Zones” category, users create or edit zones over your network interfaces to control network traffic flow.



There 3 control buttons as follows for “Zones” settings:

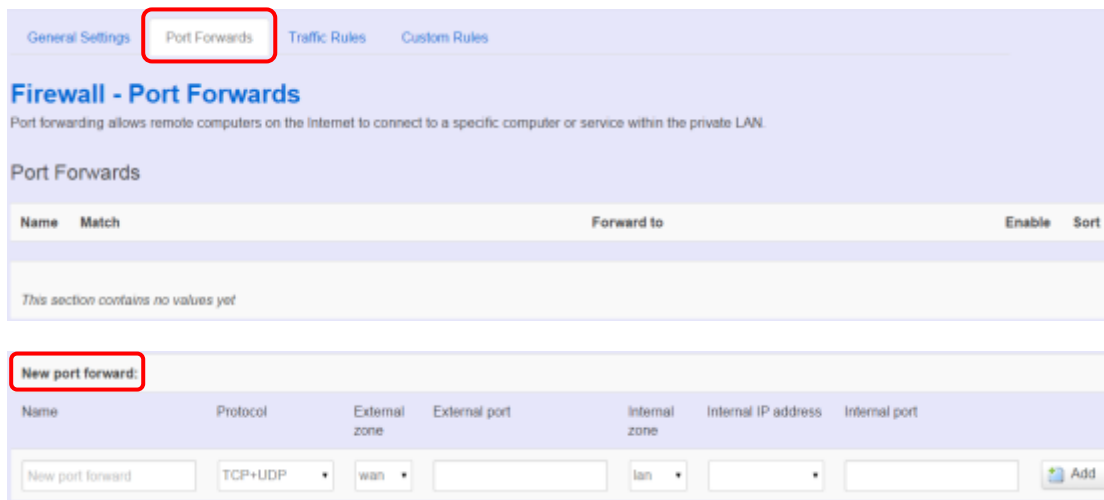
**Edit:** edit the followed flow entry.

**Delete:** delete the followed flow entry.

**Add:** create a new entry for traffic flow among zones over interfaces.

### 10.4.8.2 Port Forwards

Clicking the “Port Forwards” tab on the top of screen will show the tables for port forwarding. Adding or editing specific forwarding table allows remote computers on the Internet to connect to a specific computer or service within the private LAN.



In the “New port forward” category, there is only one button for flow editing:

**Add:** create a new flow entry for port forwarding among zones.

### 10.4.8.3 Traffic Rules

Clicking the “Traffic Rules” tab on the top of screen will appear the policy tables of 2 categories: “Traffic Rules” and “Source NAT”.

General Settings Port Forwards **Traffic Rules** Custom Rules

### Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

#### Traffic Rules

Name	Match	Action	Enable	Sort
Allow-DHCP-Renew	IPv4-UDP From <i>any host</i> in wan To <i>any router IP</i> at port 68 on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Allow-Ping	IPv4-ICMP with type <i>echo-request</i> From <i>any host</i> in wan To <i>any router IP</i> on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Allow-DHCPv6	IPv6-UDP From IP range <i>fe80::f0</i> in wan with source port 547 To IP range <i>fe80::f0</i> at port 546 on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

In the “Traffic Rules” category, the flow entries of traffic rule define policies for packets traveling between different zones (for example, to reject traffic between certain hosts or to open WAN ports on the router).

In “Source NAT” category, specific flow entries of masquerading that allow fine grained control over the source IP used for outgoing traffic(For example, to map multiple WAN addresses to internal subnets) can be added or edited.

**Source NAT**

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
This section contains no values yet				

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port
New SNAT rule	lan	wan	— Please choose	Do not rewrite

**Add and edit:** create a new entry with default values, and edit at once if required.

Please remember clicking “Save & Apply” button to activate the new settings.

#### 10.4.8.4 Custom Rules

Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall re-start, right after the default rule-set has been loaded.

[General Settings](#)[Port Forwards](#)[Traffic Rules](#)[Custom Rules](#)

## Firewall - Custom Rules

Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
```

[Submit](#)[Reset](#)