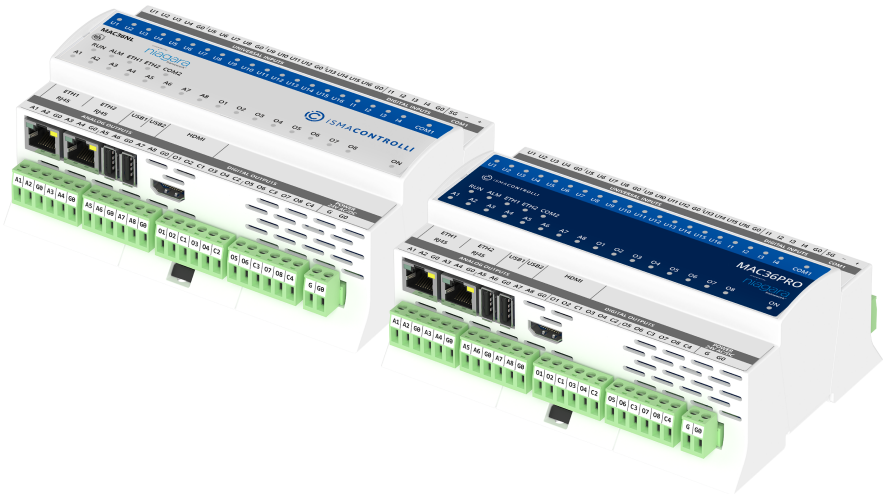
iSMACONTROLLI

iSMA-B-MAC36NL

iSMA-B-MAC36PRO

User Manual

Installation and Start-up Guide



iSMA CONTROLLI S.p.A. - Via Carlo Levi 52, 16010 Sant'Olcese (GE) - Italy | support@ismacontrolli.com

Table of Contents

1 Introduction

MAC36 are compact Master Application Controllers powered by the Niagara Framework, with various types of 36 onboard inputs and outputs. Using the specific local I/O set of 16 UI, 8 AO, 4 DI, and 8 DO allows to employ the devices in different applications. MAC36 controllers provide control, data logging, alarming, scheduling, integration, and visualization.

The range of MAC36 controllers consists of:

- iSMA-B-MAC36NL;
- iSMA-B-MAC36PRO.

1.1 Revision History

Date	Rev.	Description

17 Mar 2026	1.15	• MAC36PRO services:
		  ◦ LTE 4G support
		  ◦ SSH support
		  ◦ logs

25 Jul 2025	1.14	• Updated SD card installation section
		• MAC36PRO services:
		  ◦ Device Management web server
		  ◦ IP over USB: connection and programming
		  ◦ DHCP
		  ◦ VPN client

18 Jul 2024	1.13	Updated Preparations for Updating section
15 Mar 2024	1.12	Updated UI temperature input type information
23 Feb 2024	1.11	BTL certification of MAC36NL controllers
10 Nov 2023	1.10	Release of iSMA-B-MAC36PRO
9 Feb 2023	1.9	• Support of Niagara 4.12 • Updated M-Bus information
25 May 2022	1.8	Rebranded
24 Jun 2021	1.7	Document updated with support of the Niagara 4.10 information
16 Dec 2020	1.6	• Document updated with support of the Niagara 4.9 information • Chapter 3.11.4 updated with the web service configuration for HDMI support
27 Apr 2020	1.5	Controller system update–Chapter 3.7
31 Mar 2020	1.4	• Support of Niagara 4.8 • Change of passphrase saving destination • User fonts support • Pop-up control for the HDMI display • Auto-detection of the device extension • Log saving to the Niagara home directory • M-Bus support

Date	Rev.	Description
31 Oct 2019	1.3	Updated universal input supported sensors list
1 Apr 2019	1.2	• HDMI support • Restore to factory defaults
10 Dec 2018	1.1	• Data Recovery Service • Support of the Niagara 4.6 and later
1 Oct 2018	1.0	First edition

1.2 Key Features

- MAC36NL: Niagara 4.8 and later, MAC36PRO: Niagara 4.10.U7* and later;
- real-time programming;
- 2 Fast Ethernet (independent);
- 1 RS485 (opto-isolated), optional extension as second RS485 port;
- optional M-Bus extension;
- 2 USB (1 OTG, 1 host);
- 16 UI, 8 AO, 4 DI, and 8 DO;
- HDMI to connect an external display;
- built-in web server provides graphical user interface available from the web browser level;
- SD card to collect real-time data, history logs, and alarms;
- hardware replacement by SD card;
- different licensing models for various application types.

** Supported versions of Niagara are listed in detail in the product's Release Notes.*

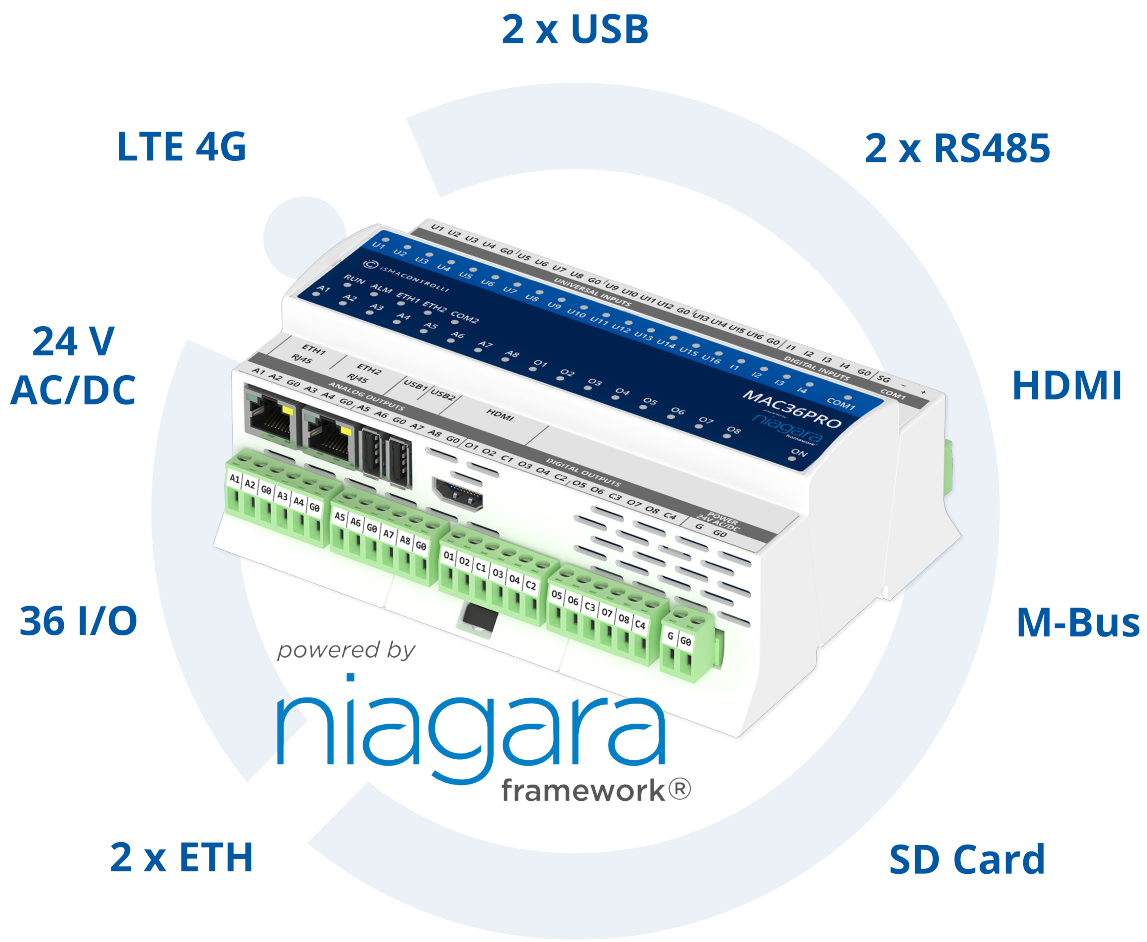


Figure 1. Key features of MAC36 controllers

2 Safety Rules

- Improper wiring of the product can damage it and lead to other hazards. Make sure that the product has been correctly wired before turning the power on.
- Before wiring or removing/mounting the product, make sure to turn the power off. Failure to do so might cause an electric shock.
- Do not touch electrically charged parts such as power terminals. Doing so might cause an electric shock.
- Do not disassemble the product. Doing so might cause an electric shock or faulty operation.
- Use the product only within the operating ranges recommended in the specification (temperature, humidity, voltage, shock, mounting direction, atmosphere, etc.). Failure to do so might cause a fire or faulty operation.
- Firmly tighten the wires to the terminal. Failure to do so might cause a fire.
- Avoid installing the product in close proximity to high-power electrical devices and cables, inductive loads, and switching devices. Proximity of such objects may cause an uncontrolled interference, resulting in an instable operation of the product.
- Proper arrangement of the power and signal cabling affects the operation of the entire control system. Avoid laying the power and signal wiring in parallel cable trays. It can cause interferences in monitored and control signals.
- It is recommended to power controllers/modules with AC/DC power suppliers. They provide better and more stable insulation for devices compared to AC/AC transformer systems, which transmit disturbances and transient phenomena like surges and bursts to devices. They also isolate products from inductive phenomena from other transformers and loads.
- Power supply systems for the product should be protected by external devices limiting overvoltage and effects of lightning discharges.
- Avoid powering the product and its controlled/monitored devices, especially high power and inductive loads, from a single power source. Powering devices from a single power source causes a risk of introducing disturbances from the loads to the control devices.
- If an AC/AC transformer is used to supply control devices, it is strongly recommended to use a maximum 100 VA Class 2 transformer to avoid unwanted inductive effects, which are dangerous for devices.
- Long monitoring and control lines may cause loops in connection with the shared power supply, causing disturbances in the operation of devices, including external communication. It is recommended to use galvanic separators.
- To protect signal and communication lines against external electromagnetic interferences, use properly grounded shielded cables and ferrite beads.
- Switching the digital output relays of large (exceeding specification) inductive loads can cause interference pulses to the electronics installed inside the product. Therefore, it is recommended to use external relays/contactors, etc. to switch such loads. The use of controllers with triac outputs also limits similar overvoltage phenomena.
- Many cases of disturbances and overvoltage in control systems are generated by switched, inductive loads supplied by alternating mains voltage (AC 120/230 V). If they do not have appropriate built-in noise reduction circuits, it is recommended to use external circuits such as snubbers, varistors, or protection diodes to limit these effects.

3 Technical Specification

		iSMA-B-MAC36NL	iSMA-B-MAC36PRO
Power Supply	Voltage	24 V AC/DC ± 20% isolated	
	Power consumption	14 W at 24 V DC; 24 VA at 24 V AC	
Universal Inputs	Temperature input	• Measurement with attached RTDs (resistance temperature detectors) • Accuracy ±0.1˚C • For sensor PT1000 and NI1000 use 16-bit resolution	
	Voltage input	• Voltage measurement from 0-10 V • Input impedance 100 kΩ • Measurement accuracy ±0.1% • Measurement resolution 3 mV at 12-bit and 1 mV at 16-bit	
	Current input	• Current measurement 0-20 mA • Required external resistor 200 Ω • Measurement accuracy ±1.1% • Measurement resolution 15 µA at 12-bit and 5 µA at 16-bit	
	Resistive input	• Measurement of resistance from 0 to 1000 kΩ • Measurement resolution for 20 kΩ load 20 Ω at 12-bit and 1 Ω at 16-bit • Measurement resolution for PT1000 and NI1000 0.1 Ω at 16-bit	
	Resistance measurement method	Voltage divider	
	Dry contact input	Output current ~1 mA Switching threshold: ON <5 kΩ, OFF >8 kΩ	
	Measurement resolution	12-bits (default) or 16-bits	
	Processing time	10 ms/channel at 12-bits 140 ms/channel at 16-bits	
Digital Inputs	Type	Dry contact	
	Switching threshold	ON <5 kΩ, OFF >8 kΩ	
	Max. input frequency	100 Hz	
Analog Outputs	Voltage range	0 to 10 V DC	
	Max. load current	20 mA	
	Resolution	12-bits	
	Accuracy	±0.5%	

Digital Outputs (relays)	Contact material	AgSnO2	
	Resistive load	3 A at 230 V AC/30 V DC	
RS485 Interface (base and optional)	RS485	Up to 128 devices	
		Half-duplex, opto-isolated	
	Communication protocols	Modbus RTU/ ASCII, BACnet MS/TP	
	Baud rate	From 2400 to 115200	
	Address	1 to 247	
M-Bus Interface (optional)	Voltage	30 V	
	Max. current load	30 mA	
	No. of devices	Up to 20	
	Baud rate	300-19200	
	Max. cable length	350 m	
	Niagara support	From N4.8 (1147)	From N4.10.U6
Ethernet	2 Fast Ethernet	Independent mode	
	Baud rate	10/100 Mb/s	
USB	2 USB	1 OTG, 1 host	
HDMI	1 HDMI	Standard type A	
SD Card	1 microSD	2 GB system reserved/2 GB user storage	4 GB system reserved/4 GB user storage
Host ID	Prefix	GC5-MACNL	iC-MAC
Ingress Protection	IP	IP20 for indoor installation	
Temperature	Storage	-40˚C to 85˚C (-40˚F to 185˚F)	
	Operating	0˚C to 50˚C (32˚F to 122˚F) When using HDMI, it is recommended to stay in range of: 0˚C to 40˚C (32˚F to 104˚F)	
Humidity	Relative	5% to 95% RH (without condensation)	
Connectors	Type	Removable screw terminals	

	Maximum cable size	2.5 mm^2
Housing	Construction	UL approved, self-extinguishing plastic (PC/ABS)
	Mounting	DIN (DIN EN 50022 norm)
Dimension	Width	111 mm/4.4 in
	Length	160 mm/6.3 in
	Height	62 mm/2.45 in

Table 1. Technical specification

4 Software License Notice

This product contains the code covered by the GNU General Public License (GPL).

Note: This product contains open source software code, the Intellectual Property Rights to which are the property of The Qt Company Ltd. with its registered office at Bertel Jungin aukio D3A, 02600 Espoo, Finland.

The usage of abovementioned open source software code in the product is covered by the GNU General Public License (GPLv3), which is available at: https://www.gnu.org/licenses/gpl-3.0.en.html.
The corresponding open-source code of this product can be obtained by sending an e-mail to rd@ismacontrolli.com. This offer is valid to anyone in receipt of this information.

5 Hardware Specification

This section outlines the hardware specification of MAC36 controllers.

5.1 Dimensions

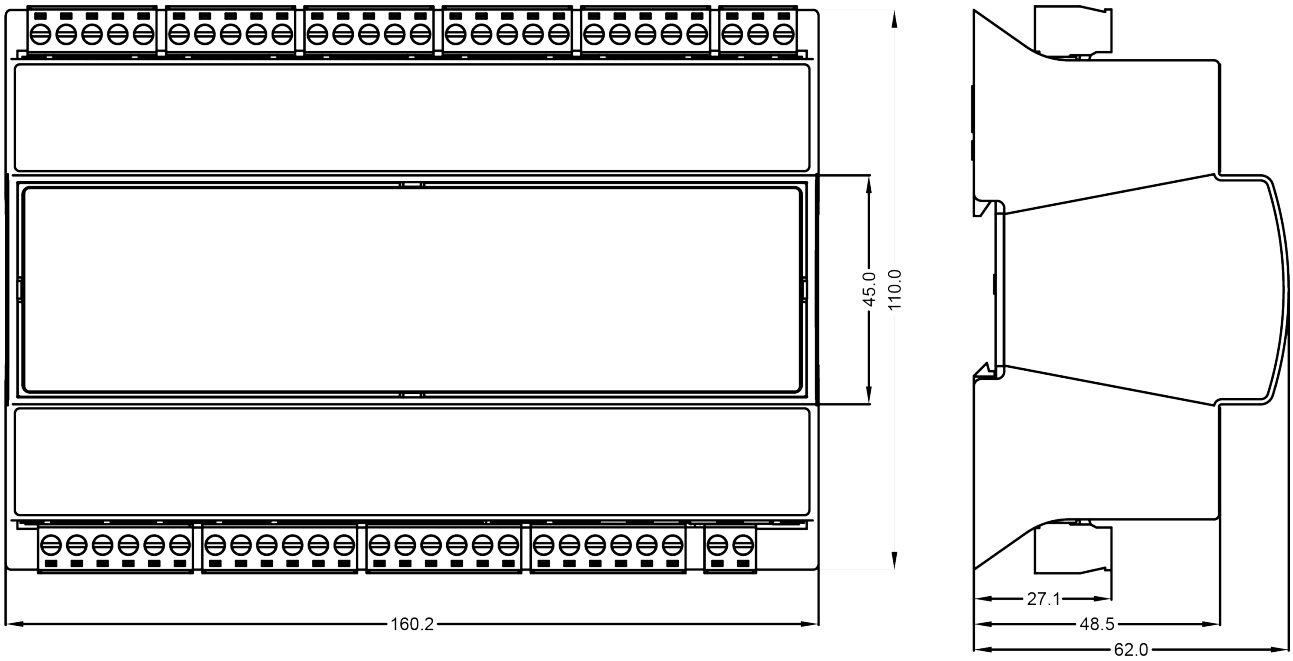


Figure 2. Dimensions

5.2 Terminals and Internal Connection Diagram

MAC36 controllers are supplied by 24 V AC/DC. The power supply block is separated. The grounding pin located next to power supply terminals must be connected to the ground.

The device has 36 local I/O on board:

- 8 digital outputs (8 DO), relay output with max. load 3 A at 230 V AC/30 V DC;
- 8 analog outputs (8 AO), voltage output 0-10 V DC maximum load up to 20 mA;
- 16 universal inputs (16 UI), temperature, voltage, current, resistive, or dry contact;
- 4 digital inputs (4 DI), dry contact inputs or fast counter up to 100 Hz.

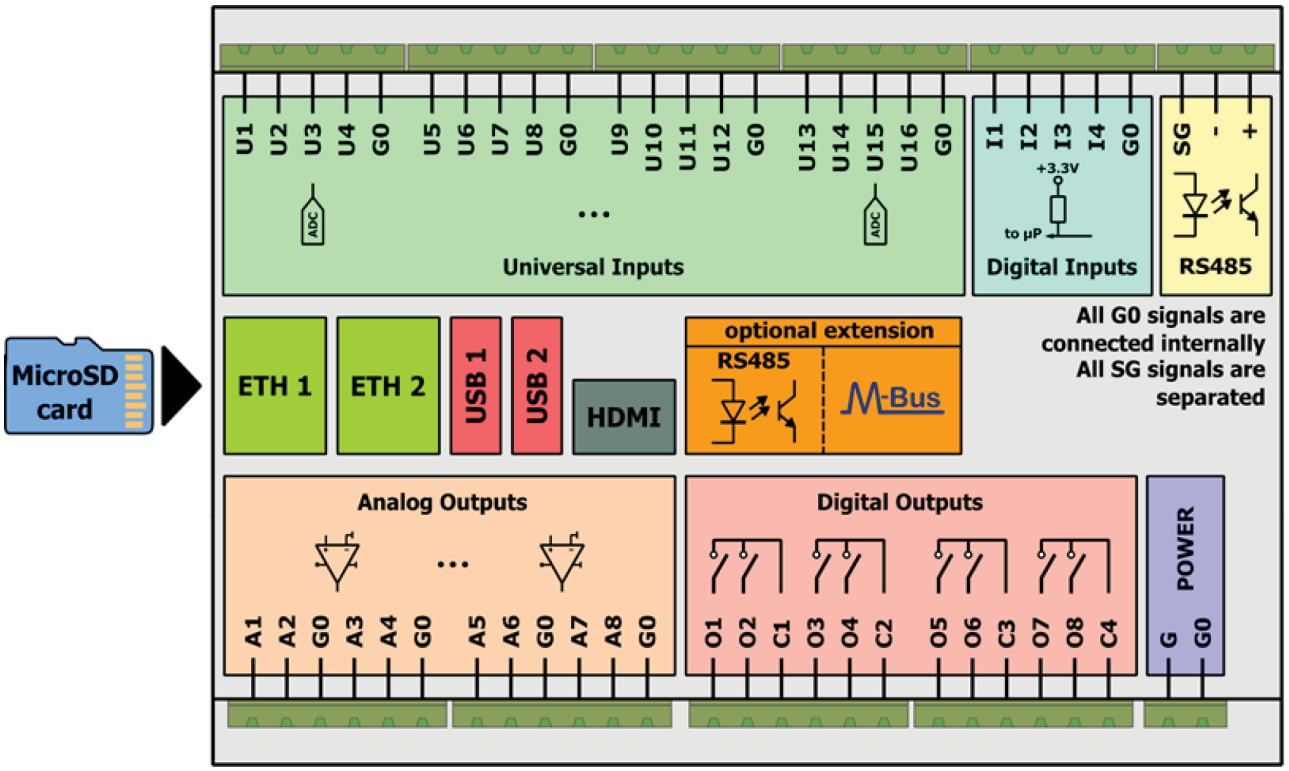


Figure 3. Block diagram

5.3 Micro SD Card Installation

All MAC36 controllers are equipped with a dedicated slot for a microSD card. The industrial-grade SD card is used for system storage, user station data, and is required for a proper controller operation. It is also used for licensing purposes as it also carries the host ID.

The controllers are compatible only with SD cards officially marketed by iSMA CONTROLLI. The following product codes shall be ordered if an SD card needs replacement:

- iSMA-B-SD-NL: for use with MAC36NL controllers,
- iSMA-B-SD-PRO: for use with MAC36PRO controllers.

Without the microSD card the device cannot operate properly.

The microSD card contains all main software parts, which are crucial for the device functioning:

- Linux operating system,
- Java Virtual Machine,
- Niagara N4.

The card slot is placed on the left side of the device, as it is shown in the figure below.

The microSD card must be inserted into the unit prior to the mounting process.

Proper SD card installation

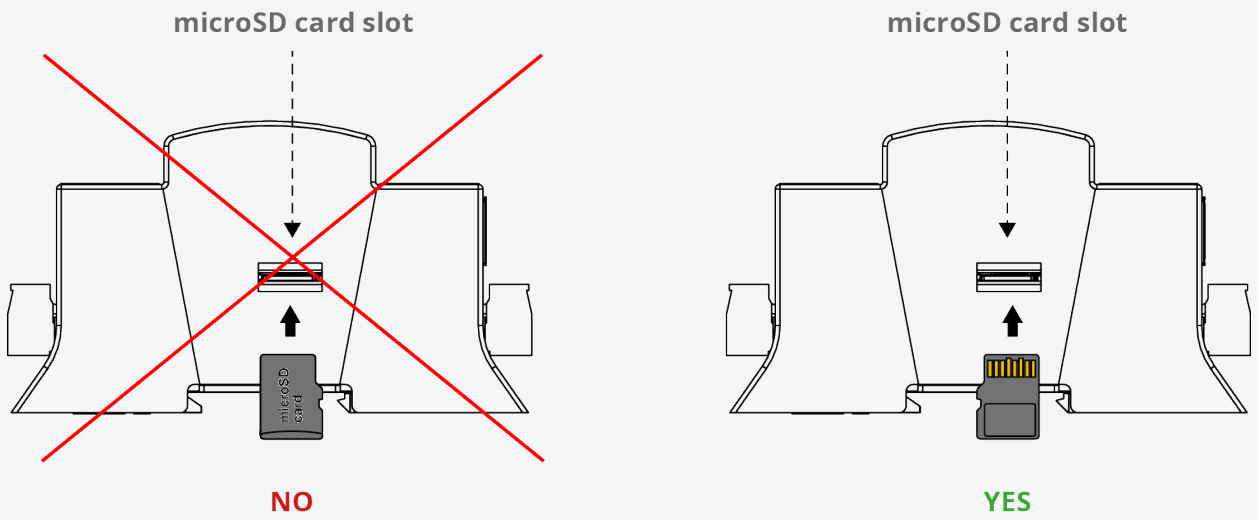


Figure 4. Proper SD card inserting

Warning!
The microSD card **must be inserted upside-down, with the gold pins facing up**, as illustrated on the controller front sticker. Incorrect installation may result in the controller malfunction. Always verify the card orientation before inserting it into the slot.

It is possible to move the SD card from one unit to another (the microSD card is not assigned to the particular hardware MAC36 unit). For example, the SD card may be removed from a unit that suffered a hardware failure and used it in a replacement unit.

Safe SD card replacement

- All power to the controller needs to be shut down before inserting/removing the micro SD card; otherwise equipment damage may occur.
- The controller needs to be unmounted from any DIN rail or screw tab mounting, as accessing the card requires access to the space behind the mounting base.
- Discharge any static electricity, which may have been accumulated, by touching a known, securely grounded object.
- Remove the micro SD card by pushing the card in, until the spring release pushes the card partially out of the card socket. Grasp the card, and pull it completely out of the unit. Store the micro SD card in a static-free protective case.

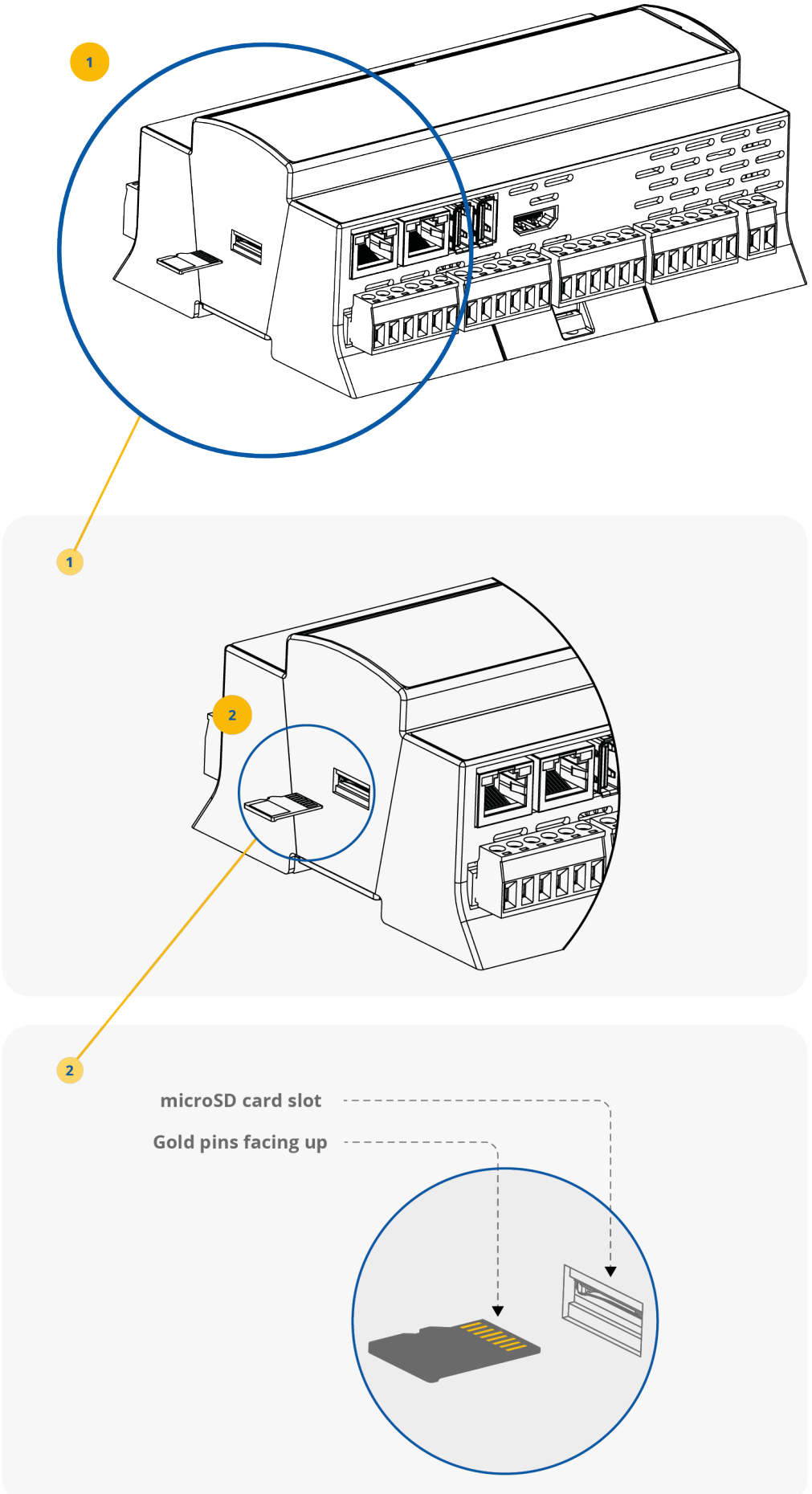


Figure 5. SD card mounting

5.4 Power Supply

The device is designed to work with 24 V AC/DC separated power supply.

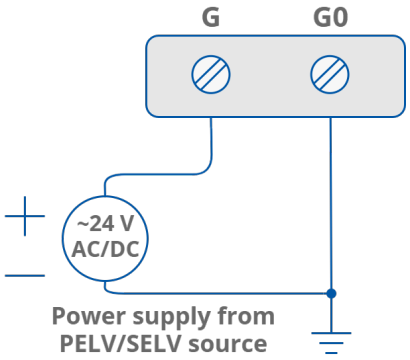


Figure 6. Power supply connection

5.4.1 Earth Grounding

Earth grounding protects from electrostatic discharge or other forms of EMI. Connecting the controller's ground spade lug to nearby earth ground is possible in hardware versions below 2.1.

5.5 RS485 Communication Bus

The device is equipped with an opto-isolated RS485 base port, which allows connecting the device to the BMS in order to communicate with other devices in the network. The optional controller version has an extension of a second RS485 port. All rules are the same as in the base port. The way of proper bus cable connection is shown in the figure below.

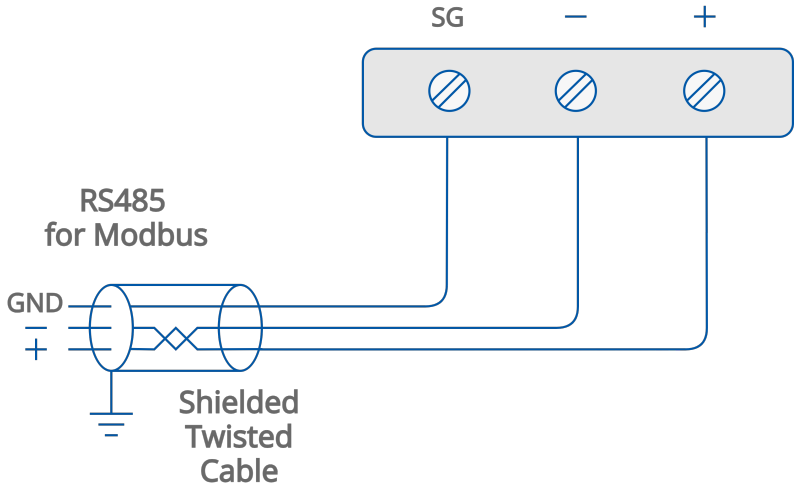


Figure 7. RS485 communication bus connection

5.5.1 RS485 Grounding and Shielding

The device can be exposed to electromagnetic environment. The electromagnetic radiation can induce electrical noise into both power and signal lines, as well as direct radiation into the device causing negative effects to the device functioning. Appropriate grounding, shielding and the other protective steps should be taken at the installation stage to prevent undesirable effects. The preventions include making control cabinets grounding, cables shield grounding, using protective elements for electromagnetic

switching devices, using correct wiring as well as appropriate cable types selection and cable cross-sections.

5.5.2 RS485 Network Termination and Biasing

The transmission line often creates communication problems. These problems include reflections and signal attenuation.

To eliminate the presence of reflections at the ends of the bus cable, it must be terminated at both ends with a resistor across the line. The resistor value has to be the same as a characteristic impedance of the bus cable. Both ends must be terminated since the direction of propagation is bidirectional. In case of an RS485 twisted pair cable, the termination is typically 120 Ω.

In the iSMA-B-MAC36NL and iSMA-B-MAC36PRO versions, there is a built-in 3-position switch on the back side of the device (access after removing the back cover), which is dedicated to connecting termination resistor and/or biasing resistors. In the iSMA-B-MAC36NL-RS and iSMA-B-MAC36PRO-RS versions, a 3-position switch is installed below a terminal connector, as shown in the figure below on the right side.

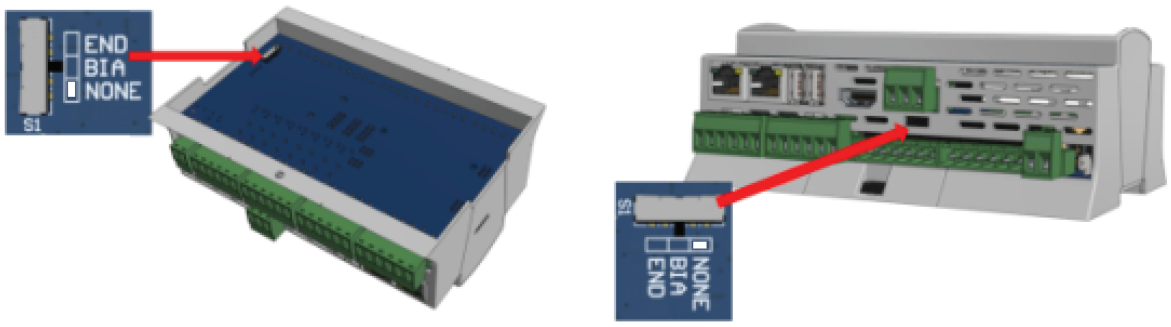


Figure 8. Switch for termination and biasing for the base (on the left) and optional extension port (on the right)

Switch position	Biasing	Termination
END	ON	ON
BIA	ON	OFF
NONE (default)	OFF	OFF

Table 2. Switch for termination and biasing

If the switch is in the END position, it connects the termination resistor 120 Ω and biasing resistors 680 Ω (pull-down to ground SG and pull-up to +5 V DC) to the RS485 bus.

Instead of using additional resistors, the termination and biasing can easily be done by a simple switch activation.

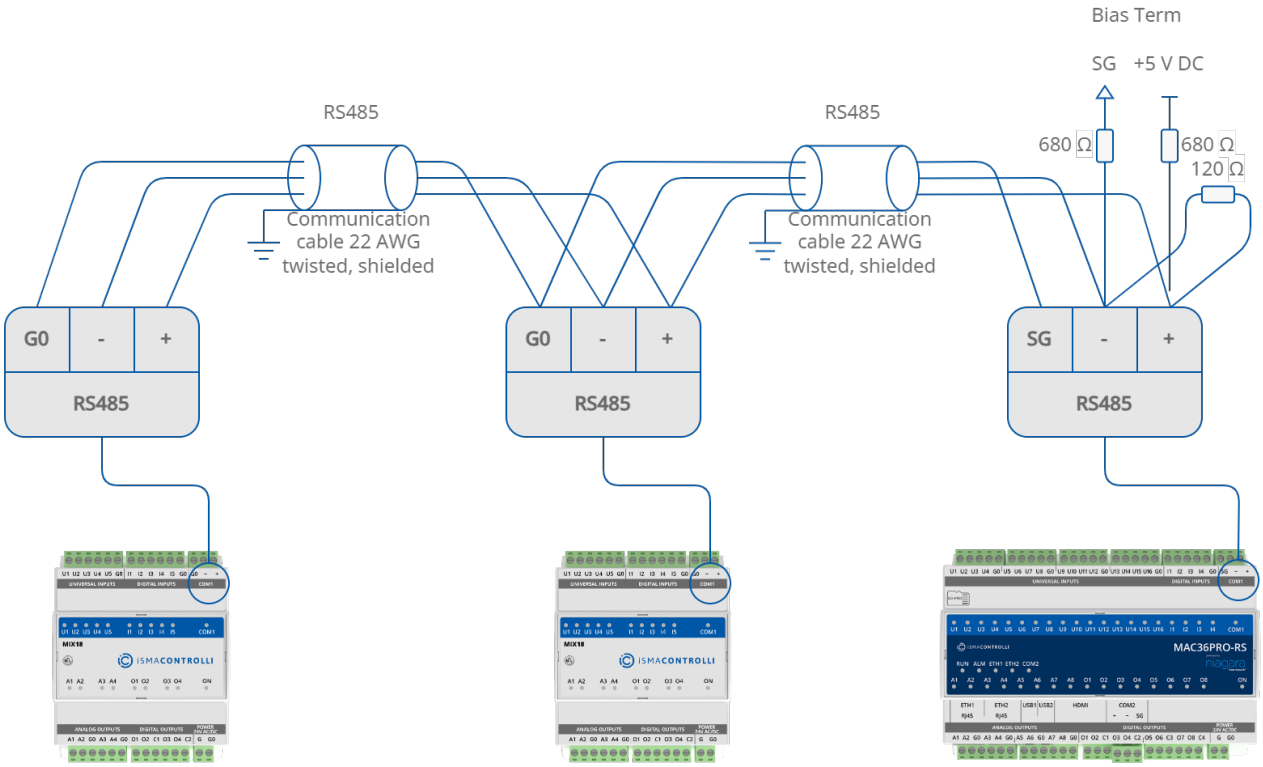


Figure 9. RS485 network termination and biasing

If the switch is in the BIA position, it connects the biasing resistors 680 Ω (pull-down to ground SG and pull-up to +5 V DC) to the RS485 bus. The biasing is added to the RS485 bus in order to reduce communication failures.

WARNING! Only one single device on the network can have biasing resistors connected. Connecting biasing resistors on two or more devices on a single RS485 bus will take the opposite effect–increase the number of communication problems.

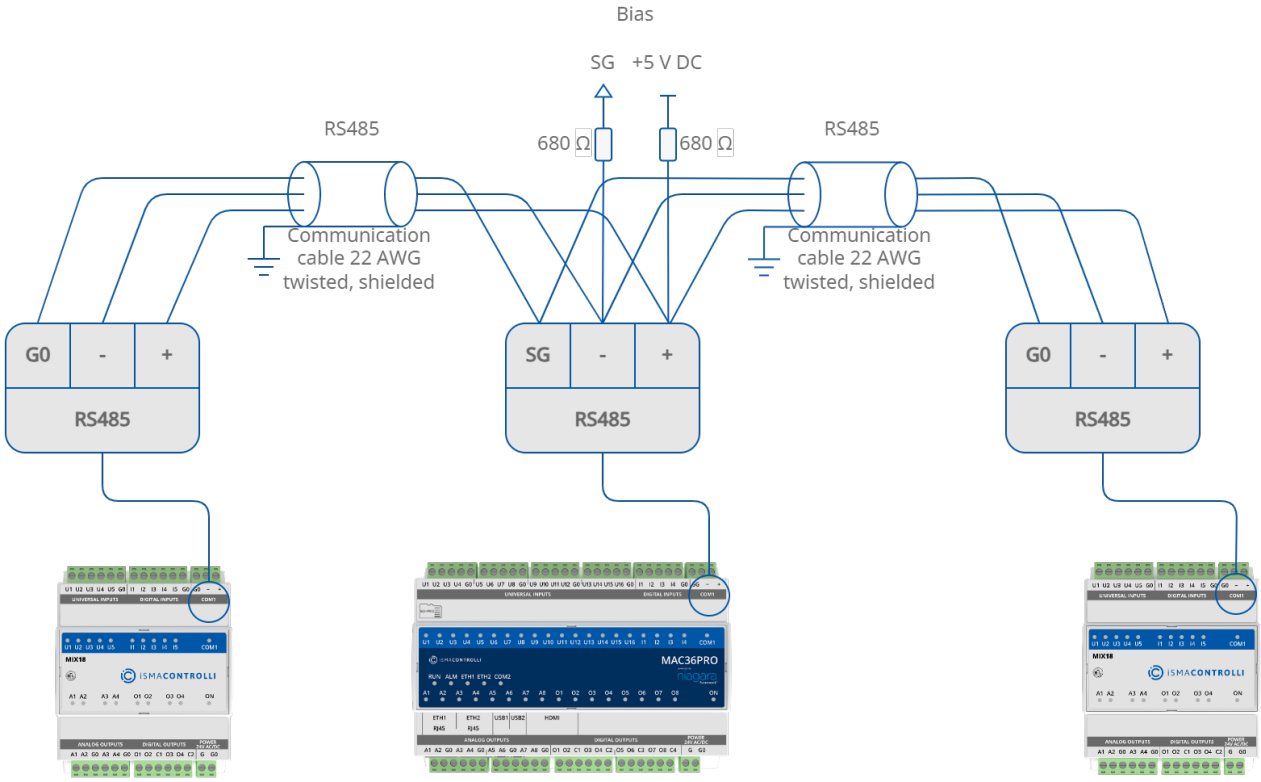


Figure 10. RS485 network biasing

5.6 M-Bus Connection

5.6.1 About M-Bus

The M-Bus (Meter Bus) was developed to fill the need for a system for the networking and remote reading of utility meters, for example, to measure the consumption of gas or water in the house. This bus fulfills the special requirements of remotely powered or battery-driven systems, including consumer utility meters. When interrogated, the meters deliver the data they have collected to a common master, for example, a DDC controller or a hand-held computer, connected at periodic intervals to read all utility meters of a building.

5.6.2 M-Bus Topology and Cable

The M-Bus is a hierarchical system, with communication controlled by a master device. The M-Bus consists of the master, a number of slaves (end-equipment meters), and a two-wire connecting cable. The slaves are connected in parallel to the transmission medium - the connecting cable.

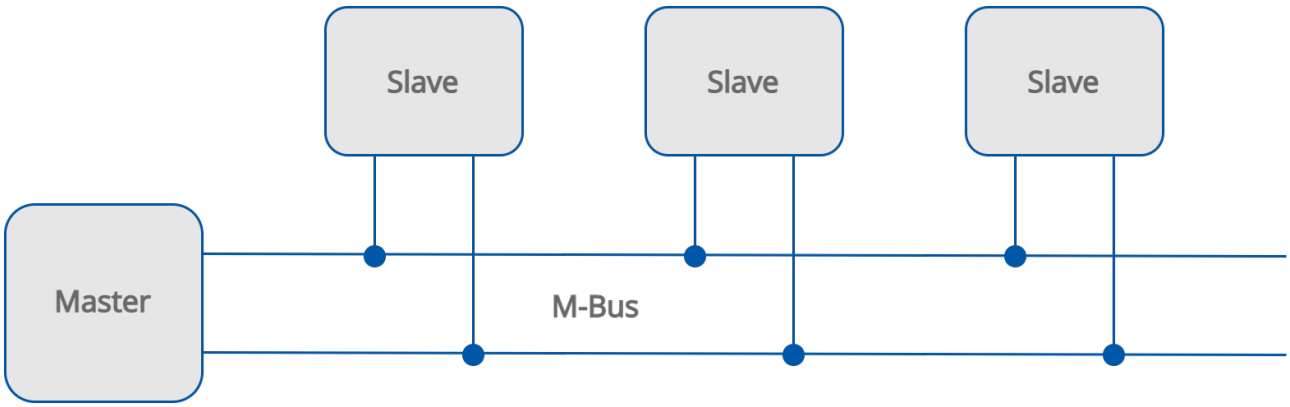


Figure 11. M-Bus network

A two-wire cable (jYStY N*2*0.8 mm) is used as the transmission medium for the M-Bus. The maximum distance between the slave and the repeater is 350 m; this length corresponds to a cable resistance of up to 29 Ω. This distance applies for the standard configuration having a baud rate between 300 and 9600 baud rate, and a maximum of 250 slaves. The maximum distance can be increased by limiting the baud rate and using fewer slaves, but the bus voltage in the Space state must at no point in a segment fall below 12 V, because of the remote powering of the slaves. In the standard configuration, the total cable length should not exceed 1000 m, in order to meet the requirement of a maximum cable capacitance of 180 nF.

5.6.3 M-Bus Addressing

The M-Bus devices are using two types of addressing:

- primary: this address is assigned by the user in a commissioning process (all new M-Bus devices have this address, set by the factory to 0); this type of address has a limited range from 0 to 250;
- secondary: this address has a wider range than primary and by default contains a device serial number. All out of box devices connected to the bus have unique secondary addresses.

5.6.4 Connection

M-Bus devices can be connected directly only to the iSMA-B-MAC36NL-M and iSMA-B-MAC36PRO-M, the controller's hardware version with the M-Bus interface (max. 20 devices).

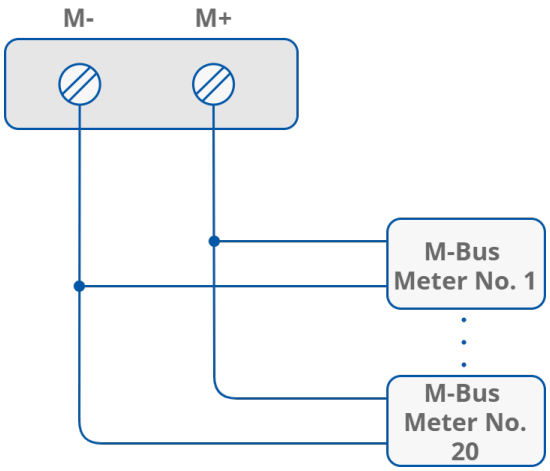


Figure 12. M-Bus connection

5.7 LED Indicators

The device is equipped with LEDs for quick status checking and diagnostics:

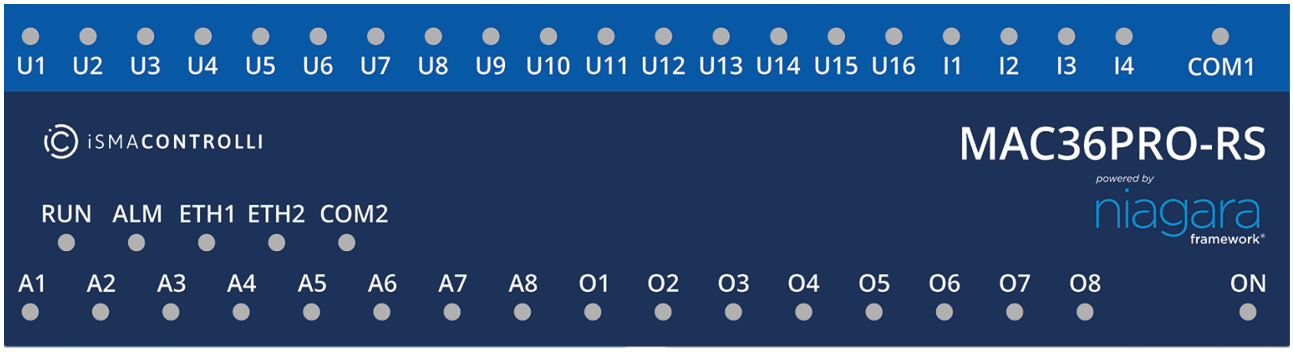


Figure 13. LEDs on a front panel of the iSMA-B-MAC36PRO controller

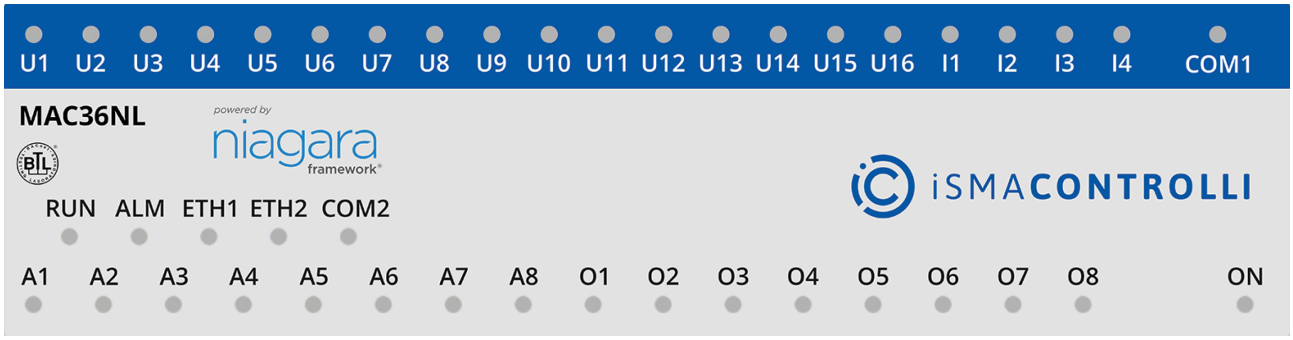


Figure 14. LEDs on a front panel of the iSMA-B-MAC36NL controller

- The power LED (ON) lights up (green), and then turns the power supply on.
- The communication LED (COM1) lights up (orange) for 20 ms in the transmit state for sending each package through the main RS485 port. As long as the device sends packages, the communication LED blinks continuously.
- The communication LED (COM2) lights up (orange) for 20 ms in the transmit state for sending each package through the extension RS485 port. As long as the device sends packages, the communication LED blinks continuously.

- The communication LEDs (ETH1 and ETH2) light up (orange) in the transmit or receive state when sending/receiving each package through the particular Ethernet port. As long as the device sends/receives packages, the communication LEDs blink continuously.
- The universal inputs LEDs (U1-U16) indicate the statuses of the universal inputs. If the LED is on, the resistance value connected to the input is lower than the switching threshold value (dry contact input is active).

Note: The LED also lights up if the voltage connected to the input has a very low potential.

- The digital inputs LEDs (I1-I4) indicate the statuses of the digital inputs. If the LED is on, the input is active (resistance value connected to the input is lower than the switching threshold value).
- The analog outputs LEDs (A1-A8) indicate the statuses of the analog outputs. If the LED is on, the output voltage or PWM factor is different than 0.
- The digital outputs LEDs (O1-O8) indicate the statuses of the digital outputs. If the LED is on, the output is active (closed circuit).
- The status LED (RUN) does not light if the power is connected. After the operating system (Linux) has started up, the RUN LED lights up continuously (green). Next, after the Platform has started up, the RUN LED also flashes very quickly. If a station exists in the controller, after the station has been started up and it operates correctly, the RUN LED flashes slowly (1Hz).
- The alarm LED (ALM) lights up in red color if there is no SD card inserted, there is a problem with the SD card connection/reading/writing, the station is in fault status, has been removed or stopped.

5.8 Mini USB

The mini USB port is dedicated to debugging connection through the console.

A description, how to connect to the system console, is included in the Connection to the Console section.

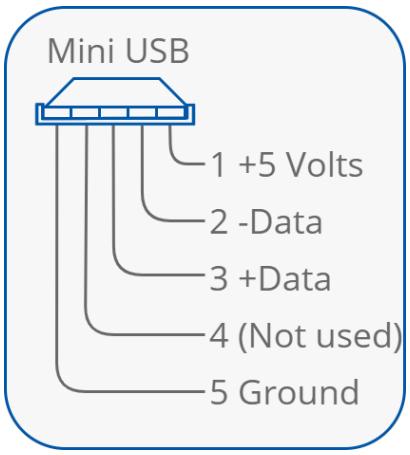


Figure 15. mini USB pinout

6 Start-up

6.1 Before the Start

To be able to operate normally, the device needs to have:

1. its SD card fitted in SD card box, and
2. its license assigned.

The hardware itself is only the base for the SD card, which consists of all the software parts necessary for hardware management.

The SD card is not assigned to a particular hardware unit. It can be moved to another controller. This function allows for easy hardware replacement. Together with the SD card all the parameters, such as the communication settings, station, Niagara, JVM, and operation system, are moved.

The license file provides a limited number of points, which can be used to build the application. Without the license file, the user is not allowed to run the station on the device.

6.2 Factory Settings

Out of the box, the SD card image has the factory settings. Whenever the controller is restored via clean or update distribution file, the default settings are restored. Please refer to the Controller System Update section for more details.

> Warning!
> Cleaning deletes the station, please save it before update!

The factory settings can be divided into two groups:

6.2.1 Factory Communication Settings

- IP address: 192.168.1.123;
- Subnet mask: 255.255.255.0;
- Default gateway: 192.168.1.1;
- Nameserver (DNS): 192.168.1.1;
- Host name: (for iSMA-B-MAC36NL) MACNL, (for iSMA-B-MAC36PRO) MAC36PRO.

6.2.2 Factory Platform Credentials

- User: tridium
- Password: niagara

Out of the box, the controller has no default station installed.

Note: Starting from the iSMA-B-MAC36NL hardware version 2.1, the passphrase is saved on the SD card. Once the Niagara Framework is upgraded to 4.8 version, the passphrase is reset to “niagara”; therefore, the station will not restart automatically, and it is required to re-enter the passphrase and manually restart the station.

Figure 16. Passphrase reset

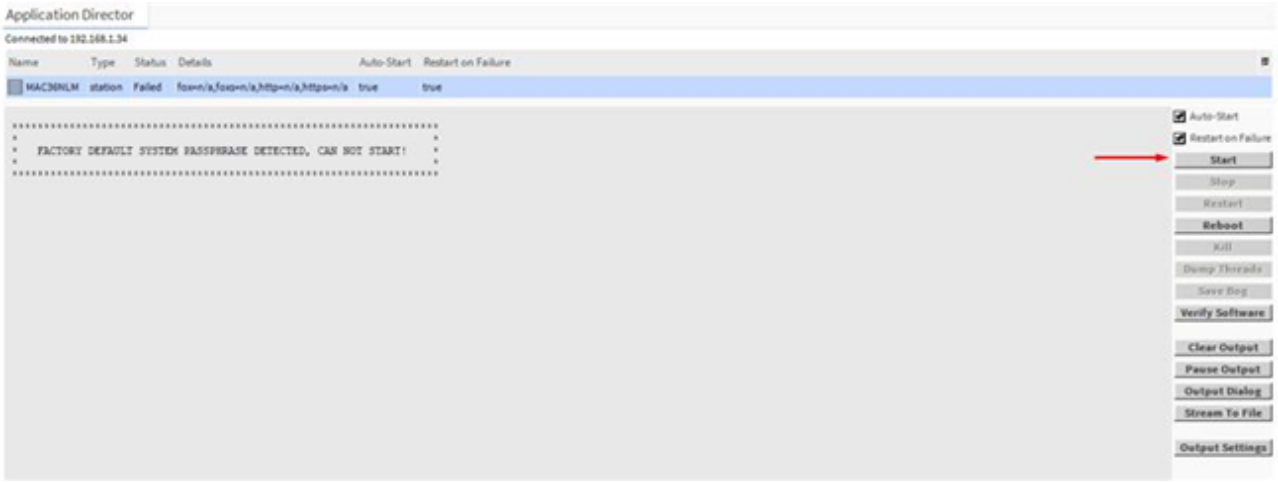


Figure 17. Passphrase reset

6.3 First Login

6.3.1 First Login to the Controller Platform in Workplace

Warning!
It is highly advisable to install the Data Recovery Service with the first commissioning of the controller. See more in the section Data Recovery Service.

After opening the Workplace software, to log into the controller for the first time, please do the following steps:

- Click File > Open > Open Platform in the menu bar.
- The Open Platform dialog window appears.
- Fill the fields in the Open Platform dialog window as follows:
    - Type: select Image Platform Connection, if not already selected.
    - Host: leave at default IP, and type in the default IP address of the new controller (the default IP address is 192.168.1.123);
    - Port: leave the default 3011 port number.
    - Credentials:
        - Username: type in the factory default username (tridium);
        - Password: type in the factory default password (niagara);

Note: Workbench may by default be set to a secure image platform TLS connection. If so, for any new controller change the type to a regular (non-TLS) platform connection. After conversion, the recommended TLS platform connection should always be used.

- Click the OK button to accept all settings.

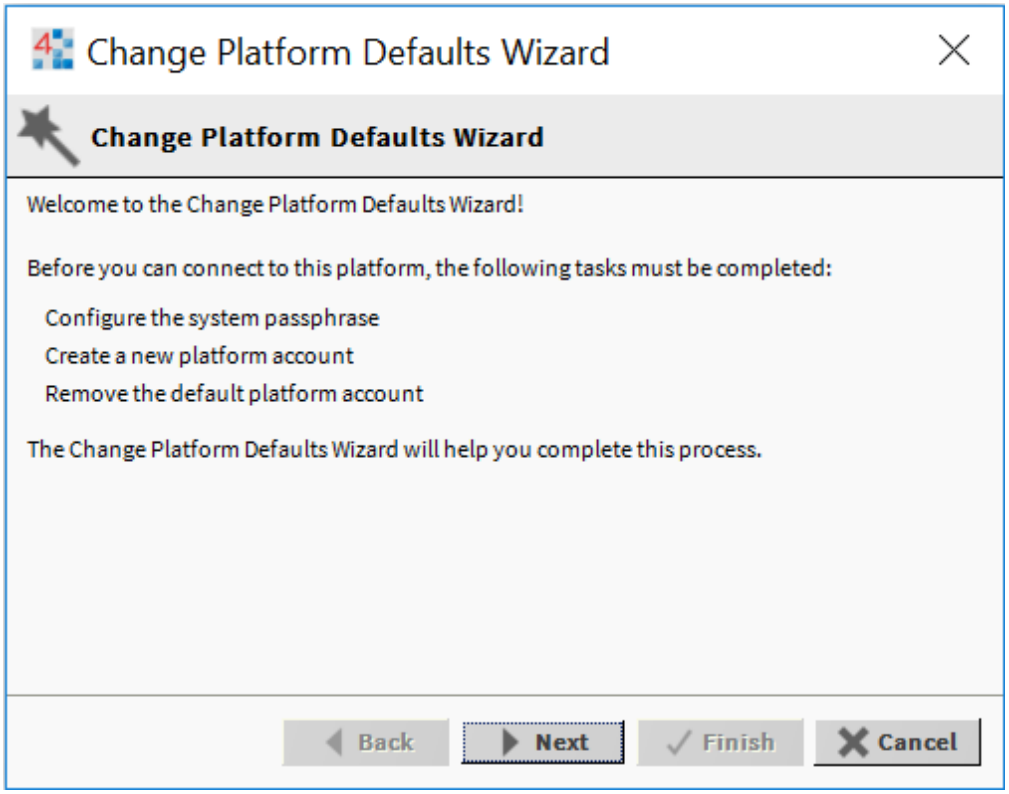


Figure 18. First login view

If the Change Platform Defaults Wizard displays, click Next to step through creating a system passphrase, creating a new platform account, and removing the default platform account, as shown below.

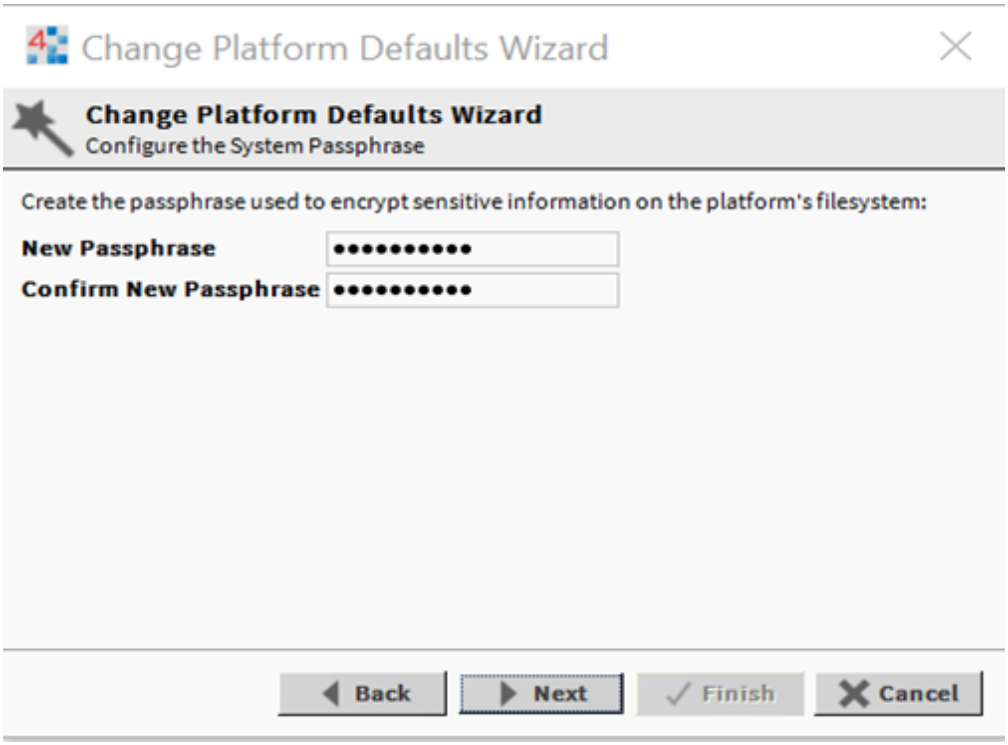


Figure 19. First login view

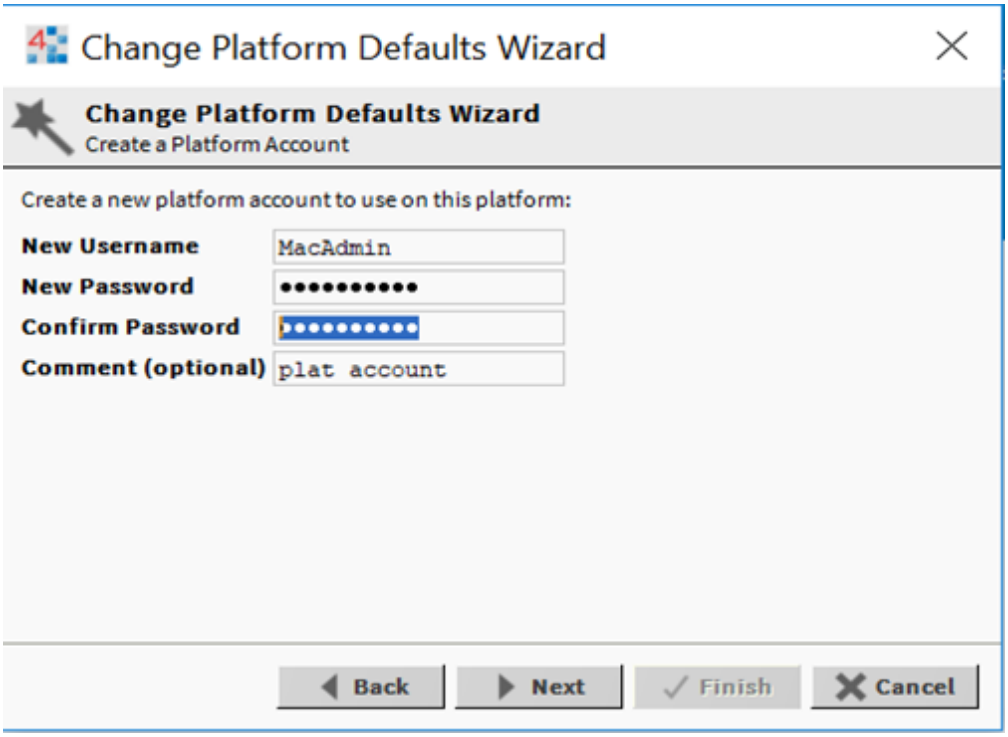


Figure 20. First login view

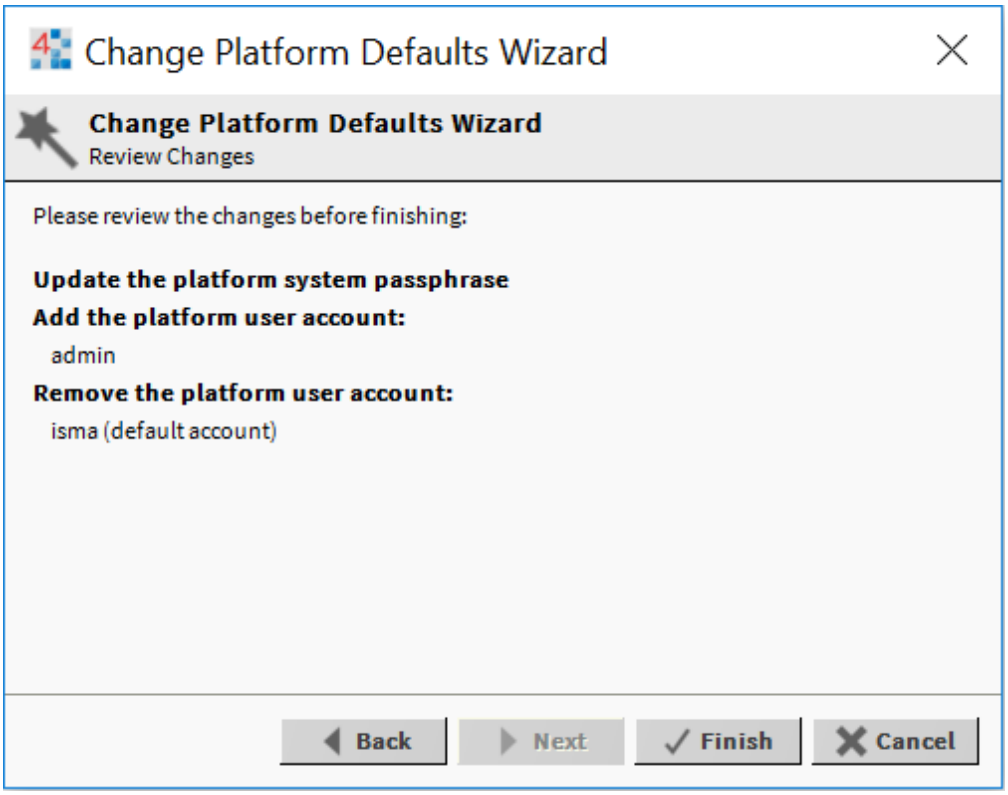


Figure 21. First login view

Click Finish to complete these changes.

The system completes making the connection between the host and Workbench, and displays the Nav Container View.

6.4 TCP/IP Configuration

6.4.1 TCP/IP Settings

A TCP/IP Configuration is one of several platform views. Typically, it is used to initially configure a remote controller's TCP/IP settings.

Configuring TCP/IP communication settings is a task for the systems integrator, while initially setting up a controller.

Perform the following steps:

- Open a connection to the platform.
- Expand the Platform container in the Navigation tree, and double-click the TCP/IP Configuration container.

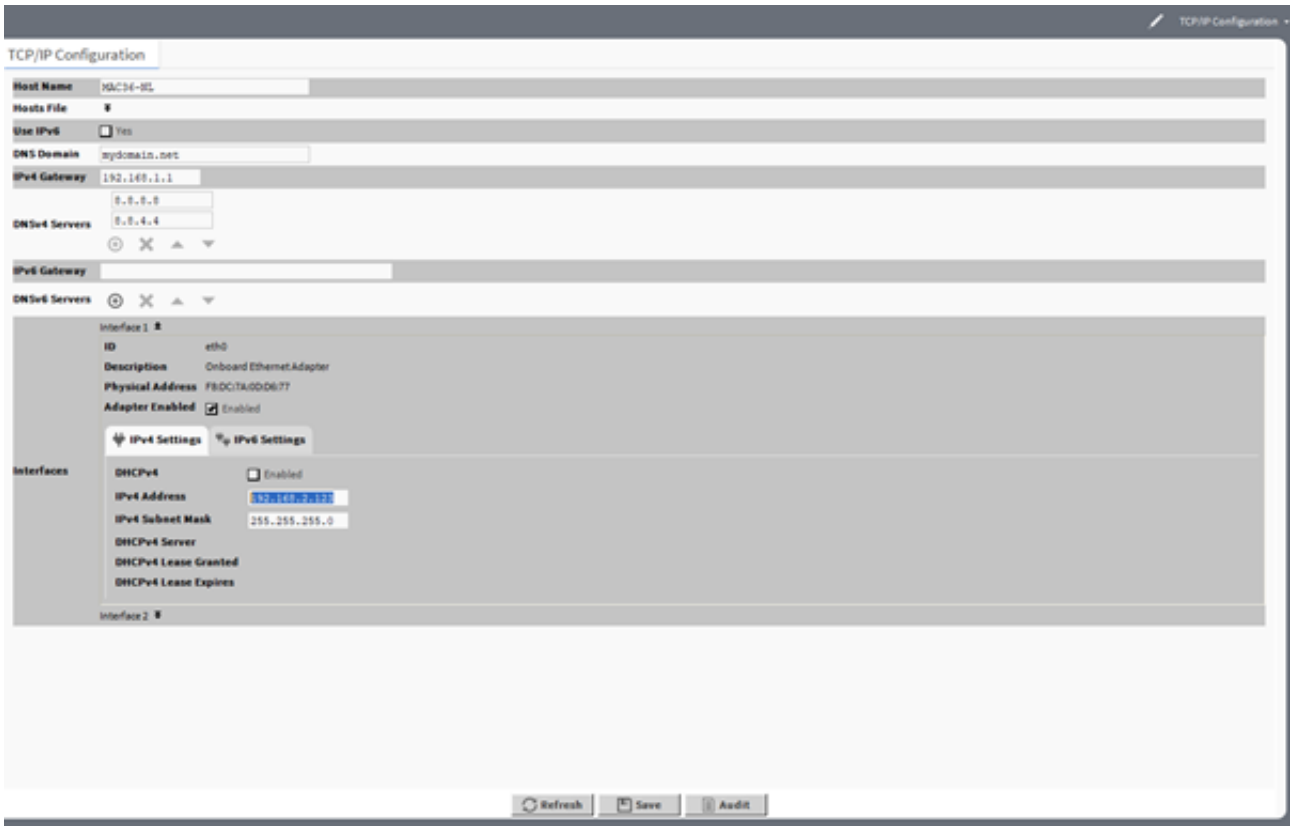


Figure 22. TCP/IP configuration

- Click the drop-down arrows to expand a group of properties.

For each Ethernet port on the connected platform, the TCP/IP Configuration platform view provides an expandable interface in the Image section.

All compatible MAC36 controllers have two Ethernet ports: ETH1 and ETH2. In the TCP/IP Configuration view, they are listed as Interface 1 (eth0) and Interface 2 (eth1).

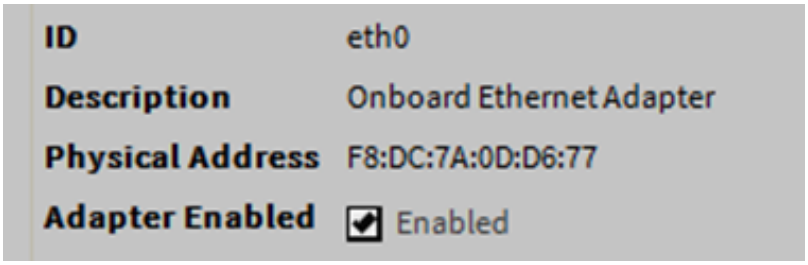


Figure 23. Ethernet port configuration

As shown above, each Interface has the following properties at the top:

- ID: a read-only OS identifier for the hardware interface, such as “eth0” for the MAC36 controller, or, for a Windows platform, either a 128-bit GUID (globally unique identifier) or a Windows network connection name, such as “Local Area Connection 2”.
- Description: a read-only text string such as “Onboard Ethernet Adapter eth0” for the MAC36 controller, or, i.e., “Intel(R) PRO/100 VE Network Connection” for a Win32-based host, describing a NIC model.
- Physical Address: the unique 48-bit MAC address of the Ethernet adapter, in six two-hexadecimal digits. For example, for the “eth0” Interface 1 port of the MAC36 controller: F8:DC:7A:0D:D6:77.
- Adapter Enabled: a checkbox to specify whether the Ethernet port is usable.

The top of the TCP/IP Configuration view provides the platform’s TCP/IP host settings.

Figure 24. TCP/IP host setting

These available host fields are as follows:

- Host Name: synonymous with "computer name," this is a string that can be processed by a DNS server to resolve to an IP address. On Windows-based systems, this hostname is the computer's identification in its workgroup or domain. If using host names, each Niagara platform should have a unique host name.
- Hosts File: the hosts file is a standard TCP/IP hosts file, where each line associates a specific IP address with a known host name. To review, click the expand control to see all entries.

For the MAC36 controllers, its hosts file can be edited.

To add an entry, click at the end of the last line and press Enter.

Then type the IP address, at least one space, then enter a known host name.

To delete an entry, drag to highlight the entire line, then press Backspace.

Click the expand control again to collapse the Hosts File editor.

- Use IPv6: the default setting is No (unchecked). If set to Yes (checked), Niagara (platform daemon and station) responds to IPv6 requests, that is, creates IPv6 server sockets (daemon) and IPv6 fox multicast sockets.

If connected to the MAC36 controller, the DNS and gateway settings are also "host-level" parameters in the TCP/IP Configuration view, as shown below.

Note: For a Windows-based host, DNS and gateway settings are available under each Interface section.

Figure 25. DNS gateway

The available fields for MAC36 controllers are as follows:

- DNS Domain: the TCP/IP Domain Name System (DNS) domain this host belongs to, if used.
- IPv4 Gateway: the IP address of the router that forwards packets to other IPv4 networks or subnets. A valid gateway address is required in multi-station (MAC36) jobs to allow point discoveries under Niagara Networks.
- DNSv4 Servers: the IP address of one or more DNS servers (if available), where each can automate associations between host names and IPv4 addresses. Included are

icon-buttons to Add (enter the IP address of the server), Delete, and move Up/Down (set the DNS search order).

- IPv6 Gateway: the IPv6 address for the router that forwards packets to other IPv6 networks or subnets.
- DNSv6 Servers: the IPv6 address for one or more IPv6 DNS servers (if available), where each can automate associations between host names and IPv6 addresses. Included are icon-buttons to Add (enter the IP address of the server), Delete, and move Up/Down (set the DNS search order).

To save time, when making multiple changes, enter all changes before continuing.

When the configuration is finished, click Save.

The system displays:

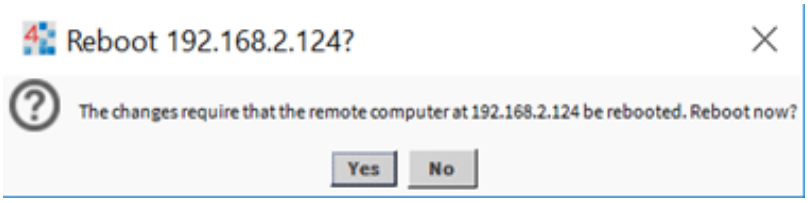


Figure 26. Reboot

Reboot the controller for the changes to take effect.

6.5 Connection to the Console

The console is used for service purposes, including registration of system logs, which can be analyzed by the support department.

Note: With Niagara 4.8 and up, the logs are saved directly into the user home directory, which allows for historical reviews.

To put the controller into the debug system console mode, plug-in the USB-to-miniUSB cable. This makes the system console available at the debug port, at a predefined serial rate: 115200, 8, N, 1.

More detailed instruction is described below:

- Connect to the controller's debug port using the USB cable.
- Start terminal emulation software on your PC. The PuTTY is a recommended software, and it can be downloaded from https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html.
- In the category tree expand "Connection" branch and choose "Serial".
- Set the "Serial line to connect to" USB COM port, in which the controller has been detected. It is possible to check which port is in use in the Windows Device Manager.
- Set the "Configure the serial line" fields, as shown in the figure below:

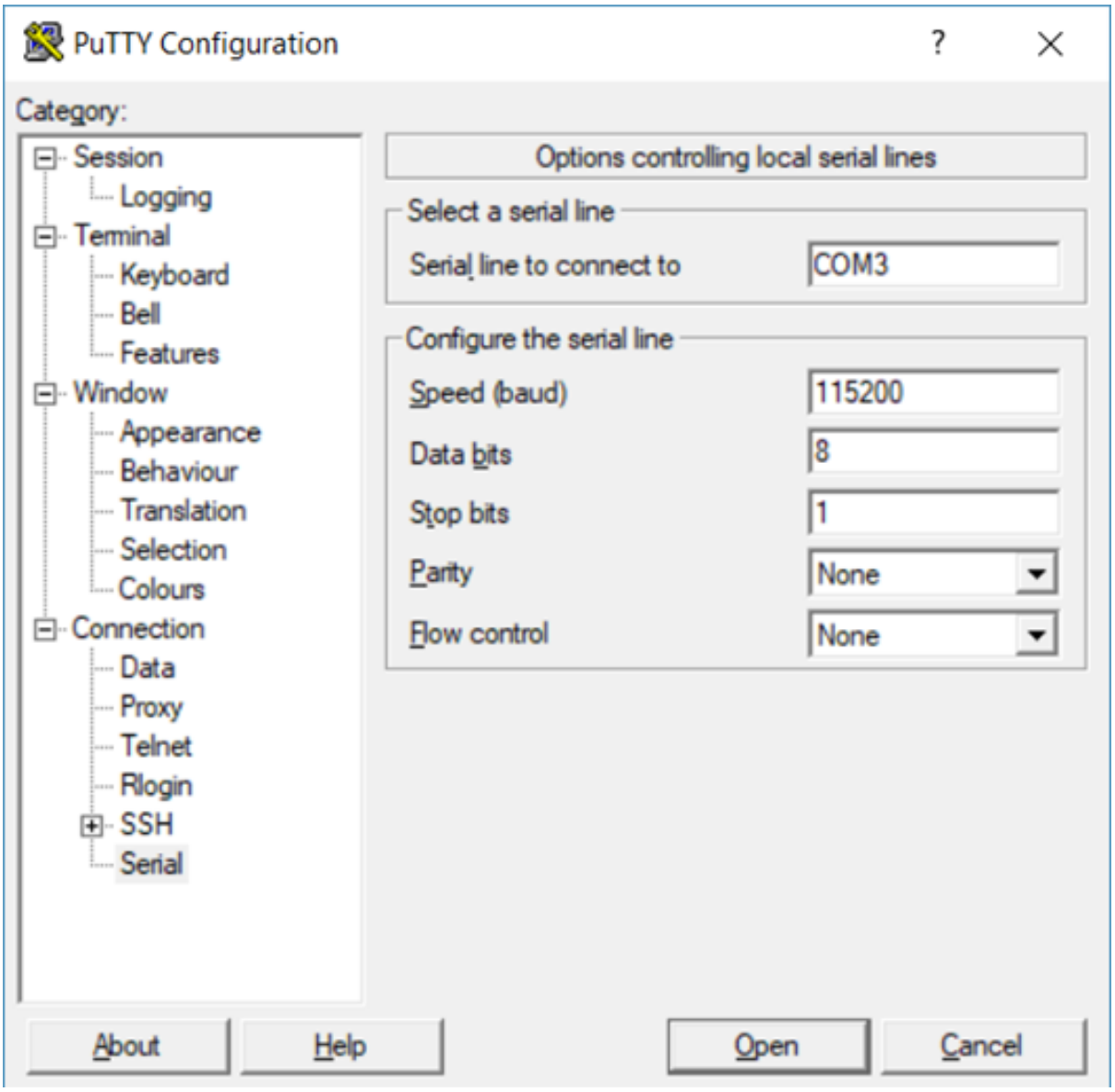


Figure 27. COM port setting in PuTTY

- In the Category tree click "Session", and choose "Connection type" as a "Serial".
- Click "Open" button at the bottom of the PuTTY window.
- There are the system logs and collect dumps for service purposes by the iSMA CONTROLLI support department.

6.6 Controller System Update

6.6.1 Preparations for Updating

If the iSMA CONTROLLI releases an update of one or more components of the controller system (OS, NEL, JVM, modules), such an update may be performed remotely, using a distribution file without physically accessing the SD card.

Note: Performing the Clean dist process is required before making a system upgrade of the controller. Follow steps from the Restore Controller to the Default State section.

MAC36 controllers are compatible with iC Workbench, Vykon Workbench, and others. The iC Workbench contains all support files necessary for the controller update and requires no additional action before the update.

- If the iC Workbench is used, go to the Installing the Update section.

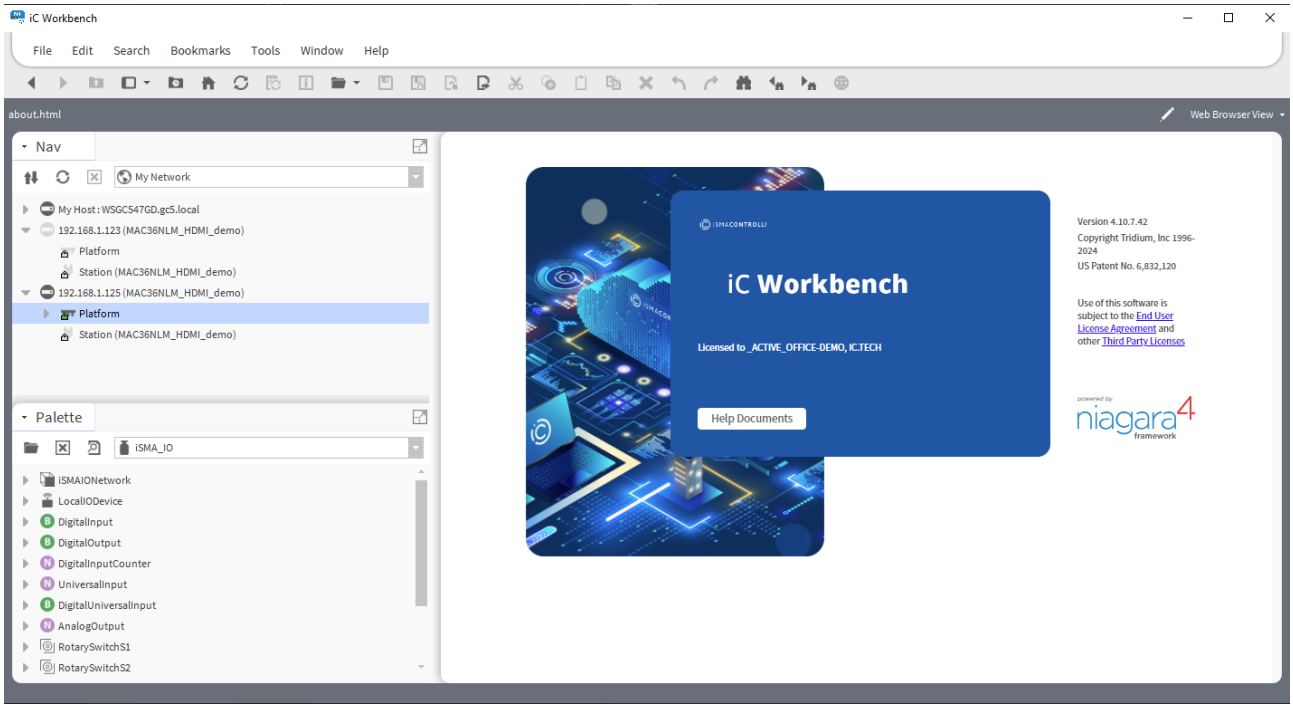


Figure 28. iC Workbench About window

- If a third-party Niagara Workbench is used, download and install the supported version of the iC Niagara Expansion Pack.

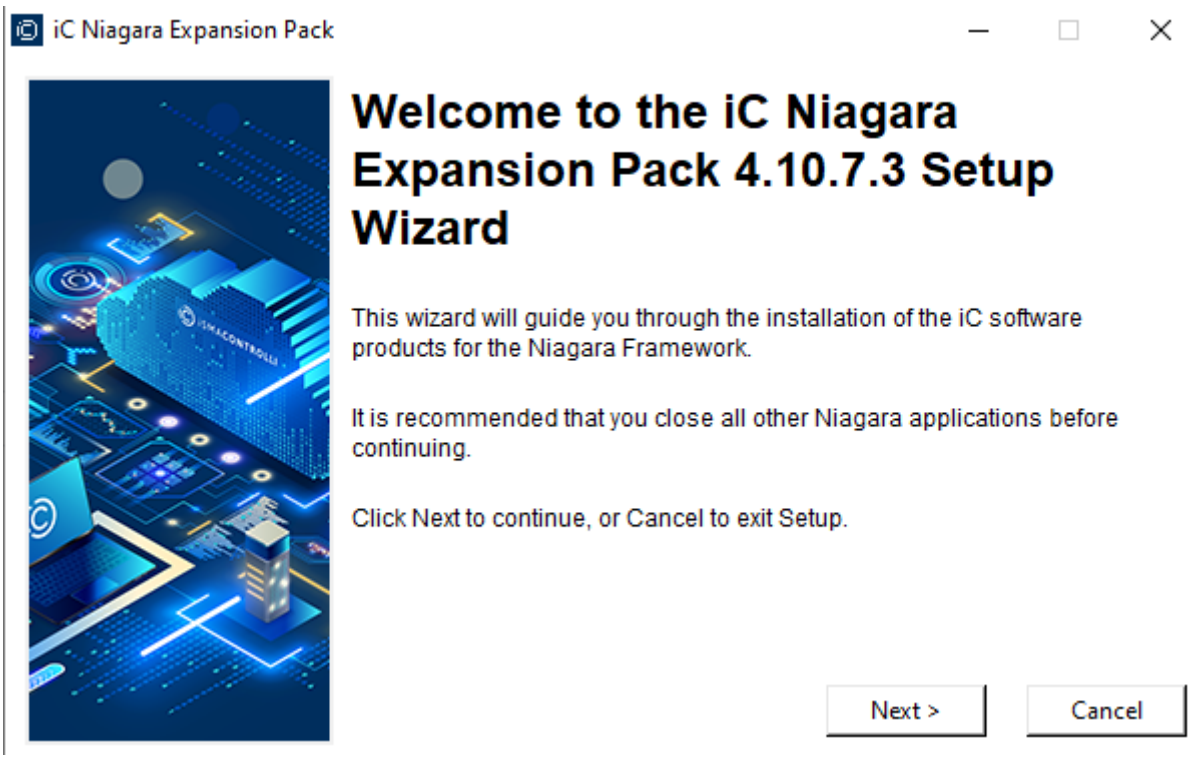


Figure 29. iC Niagara Expansion Pack for 4.10.7 Niagara Workbench welcome screen

Once the iC Niagara Expansion Pack is installed, follow the go to the Installing the Update section.

The MAC36NL supports the following legacy versions of the Niagara Framework:

- 4.4.73.24;
- 4.6.96.28;
- 4.7.109.20;
- 4.8.0.110;
- 4.9.1.30;
- 4.10.3.20;
- 4.11.1.16;
- 4.12.2.16

For the above versions, download the legacy iSMA_MAC36NL_files_installer_v1.10.

The package contains elements of the system that will be updated as new elements of the system, or as newer versions of Niagara, operating system, modules, and the Clean dist file. After unpacking, run the bat file. The installer will automatically copy all files to the appropriate disk space with Niagara installations. The next step is to run the required version of the Workplace, connect to the platform of the driver to be updated, and perform the command Commissioning Wizard. When performing the Commissioning Wizard, select the Upgrade All Out of Date option for all modules used, as shown below:

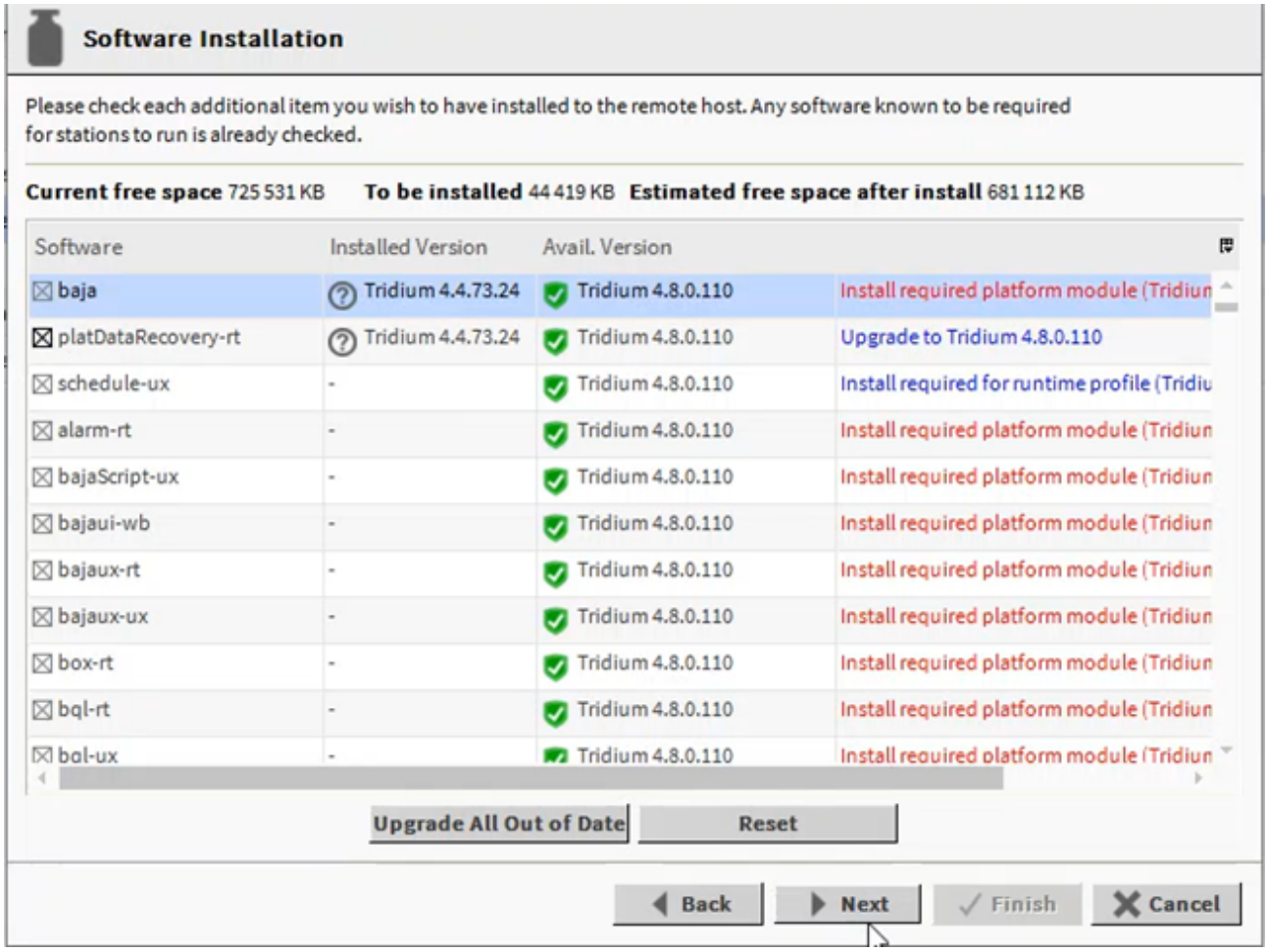


Figure 30. Update all out of update modules

6.6.2 Installing the Update

After logging in to the Platform of the controller, right click on the Platform, and run the Commissioning Wizard process.

Going through the next wizard windows, an additional dialog window will appear, informing about the need to update the appropriate controller system component (OS, NEL, JVM).

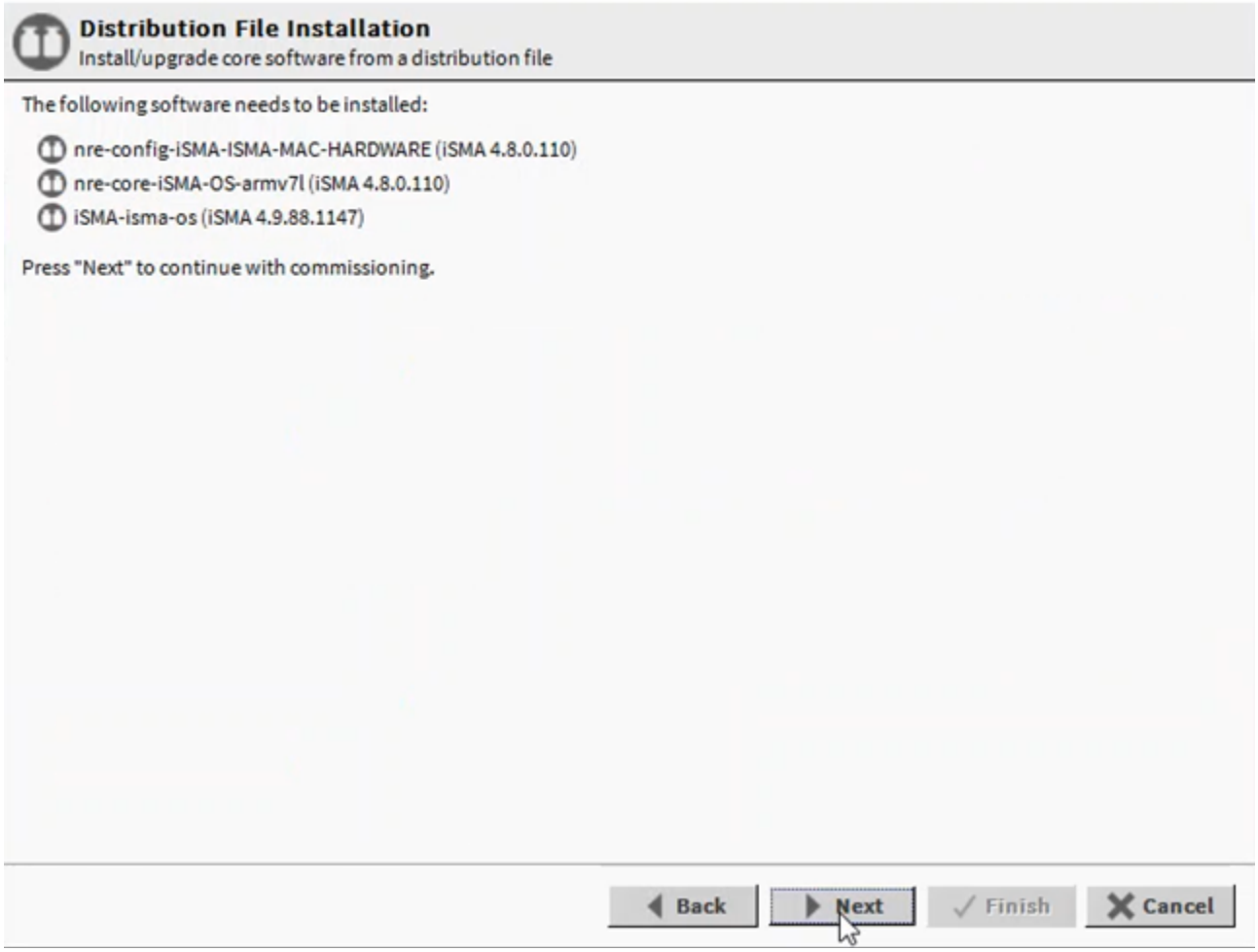


Figure 31. Commissioning Wizard with tab informing about the needs to update

Note: No additional dialog window in the Commissioning Wizard means that the controller has the current version of the system component, and there is no need before an update– the Commissioning Wizard process can be freely cancelled.

Go to the last window of the wizard, and click the Finish button. The automatic update of the controller system component is complete.

After the update is completed, the controller is rebooted. After the reboot, the latest available version of the controller's system component is properly installed.

Current version numbers of the controller's system components can be checked in the Platform / Platform Administration.

6.7 Restore Controller to the Default State

6.7.1 Default State

At times, it may be necessary to restore the controller to an empty state, either to recommission it with the current release build, or before recommissioning it with an earlier build. To do this, a clean dist (distribution) file is used.

Note: Installing a clean dist wipes the entire file system, and installs an appropriate version of Niagara platform daemon, resetting the unit to a near factory state. All other data is deleted from the file system, including station bog files, Px files, modules, etc. The unit's TLS private key information is also deleted. In addition, installing a clean dist deletes all configured platform users, restoring the factory-default platform credentials and port (3011). Only TCP/IP settings, license file, and secure communication configuration (TLS) will be preserved.

To perform the restore to the default state, open a Platform connection to the controller. To access the Clean Dist directory, open the Distribution File Installer and click the Cleaning button. Each clean dist file has the suffix -clean in its name. Clean distribution files are located in C:\Niagara\Niagara-4.x\cleanDist version of Niagara and the appropriate folder for a later version of Niagara.

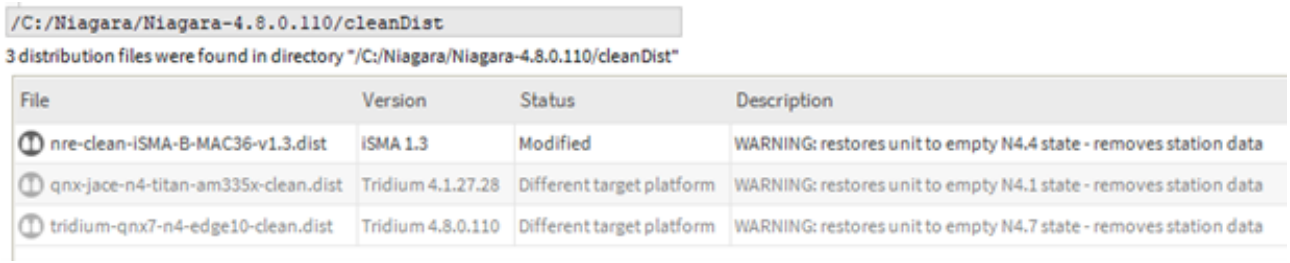


Figure 32. Distribution file list with Clean Dist files

Next, select the appropriate clean dist file for the platform and click Install. Removing a file system takes a few minutes, then the controller automatically reboots. Wait for the reboot to complete.

Note: After reboot from a clean dist install, the controller requires port (3011).

Finally, the software versions must be re-installed to the controller. Please open a version of the Workbench that uses the same software version that is required on the controller, and use the Platform \ Commissioning Wizard to install the desired software build.

6.8 Restore Controller to the Factory Default

6.8.1 Factory Default

In case the username and/or password to the platform have been lost, or the connection to the controller cannot be established because the IP address of the MAC36 controller remains unknown, there is a function to restore factory values.

The factory default function causes:

1. Removes all users of the platform and restores the factory user "tridium" with the password "niagara".
2. Removes the IP network settings and restores the factory IP address: 192.168.1.123.
3. Removes all modules and leaves the jar module in the version, in which the Commissioning Wizard was carried out (necessary to connect to the controller).
4. Removes the station.
5. Removes the passphrase.

Note: Restoring the factory default is not the same as performing a clean-up procedure using the Clean Dist.

To restore the factory values, open the top cover by undershooting it with a flat screwdriver in the grooves on the left and right side and on the top and bottom (in the middle of the cover along each side).

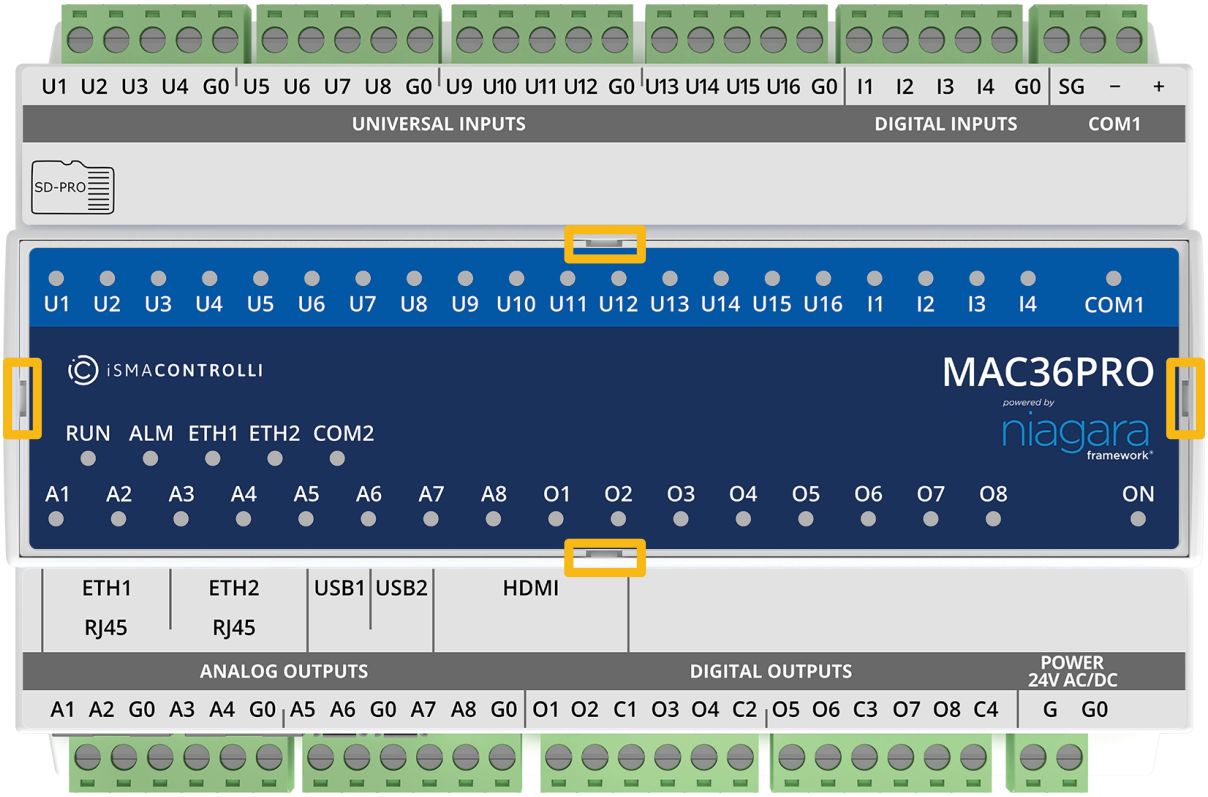


Figure 33. Top cover

After removing the cover, there are two DIP switches and two rotary switches. Looking at the description on the right, there is an information about the function of the switch 6 in the S3 DIP switch. Switch 6 in the S3 DIP switch is used to perform the function of restore factory settings.

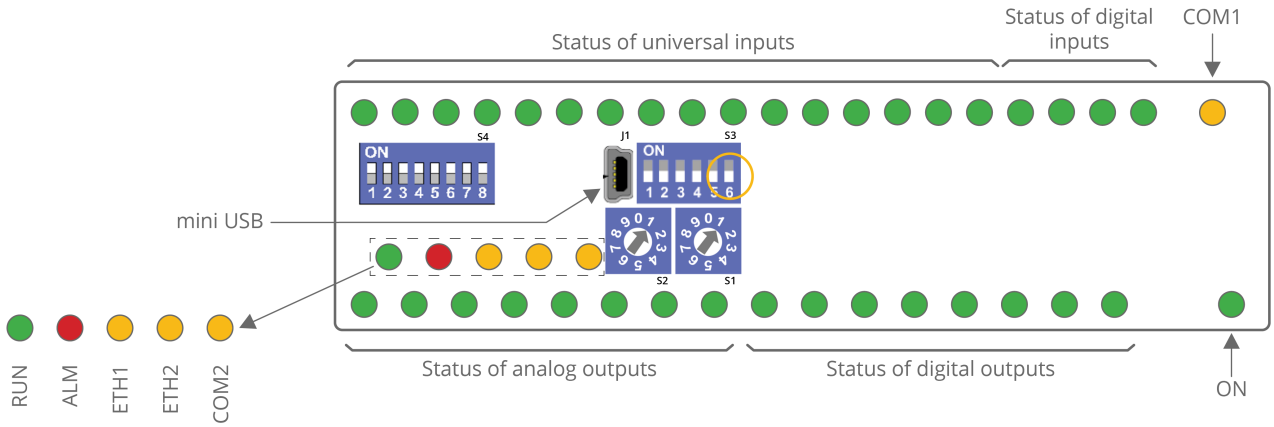


Figure 34. DIP switch

The sequence of restore factory settings is as follows:

1. Disconnect the power supply from the controller.
2. Pull up the switch 6 in the S3 DIP switch to the ON position (up).
3. Connect the power supply to the controller.
4. The controller starts flashing quickly with the ALM LED.

5. Pull down the switch 6 in the S3 DIP switch to the OFF position (down). This starts the procedure of restoring the factory values
6. After executing the restore factory settings sequence, the system starts from the beginning until the platform starts (the RUN LED flashes fast).

After finishing the procedure of restoring factory settings, the Commissioning Wizard procedure should be carried out in the required version of Niagara.

Note: In case of accidental switching of the switch 6 and switching on the power supply, normal system start-up can be restored by disconnecting the power supply, switching the switch 6 to the OFF position, and reconnecting the power supply.

Note: If the factory default procedure is performed, the station cannot be recovered from the controller.

6.9 Data Recovery Service

The Data Recovery Service is the station platform service that provides an NV-RAM support for MAC36 controllers. Providing the platDataRecovery module is installed, this service automatically appears under Platform Services.

Warning!
Please note that the from the Niagara 4.10 version and up the Data Recovery Service is carried out automatically–there is no need to manually install the PlatDataRecoveryService module, it is installed by default.

Note: A station running in the MAC36 has no seamless immunity to power surges. Although all station data, including components, histories, and alarms, are automatically restored to pre-event values, as part of a station start-up (following power restoration), the briefest power outage results in a controller reboot.

MAC36 controllers solve that problem, as all station-generated data (changed from that stored in its non-volatile flash memory at the time of a power loss) is always preserved in the NV-RAM. Upon power restoration, this data is reinstated in the station during start-up, then saved in its non-volatile flash memory.

Note: The NV-RAM does not preserve data or files external to the station.

Please note that, if the power surge occurs when station users have unsaved file changes, for example, a Px file or Nav file being edited, these unsaved changes are lost.

Station users may be aware of such event and react by saving changes (click the Save button in the active view).

Providing that communication is still established, the edited file may be saved. Or, if the power is lost only momentarily and then remains stable, the user can save the file normally.

Note: MAC36 controllers do not provide a similar saving opportunity after a power surge —it is already rebooting. Therefore, as a best practice, the MAC36 controllers' system users are advised to often save their files manually if editing items like Px graphics or Nav files.

The Data Recovery Service writes current values as they occur to a block of the NV-RAM. If such block is full, the service copies it from the NV-RAM to the controller's flash memory. A station that creates rapid COV (change of value) histories may fill the NV-RAM data

blocks too frequently, triggering a database saving possibly every couple of minutes. Ideally, such database saving to flash memory should occur no more than once an hour.

For the most effective functioning of the Data Recovery Service, maximum history intervals cannot exceed the below ranges:

No. of history points	Interval
0-299	5 s
300-999	30 s
1000-2499	60 s
2500-4999	120 s
>5000	240 s

Table 3. Recommended history intervals

Saving the database too frequently results in an inefficient use of the controller's CPU time and in potential flash problems.

Flash memory is designed to be written to a certain number of times. Several variables contribute to how often the database needs to be saved, including:

- rate of changes that need to be persisted;
- size of the changes (histories, alarms, and setpoint changes differ in size);
- amount of free flash memory space.

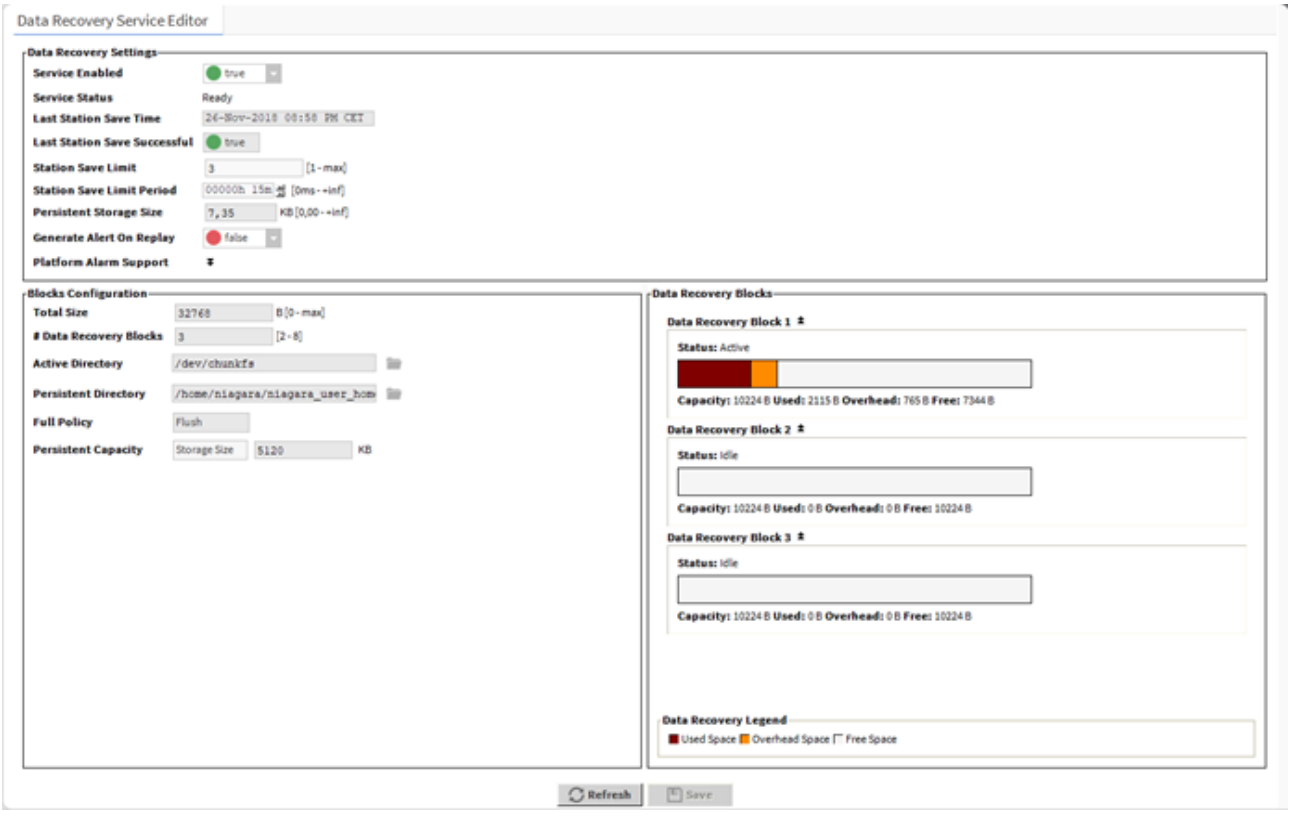


Figure 35. Data Recovery Service Editor in PlatformServices of the MAC36 controller

The figure above shows the default view for the service: the Data Recovery Service Editor.

Note: The example above reflects a scenario, where a station saving has occurred at least once since the service was created. Some NV-RAM data recovery blocks have already been flushed to flash ("Persistent Storage Size" is not 0.00 kB).

6.9.1 Data Recovery Service Editor

This Data Recovery Service Editor is the default view of the Data Recovery Service.

The Data Recovery Service Editor view has the following three main areas:

- Data Recovery Settings;
- Blocks Configuration;
- Data Recovery Blocks.

Data Recovery Settings include the following:

- Service Enabled: by default set to true, enables the NV-RAM support via this service.
- Service Status: the current status of the DataRecoveryService, which, typically, is Ready. Other states include Starting, Configuring, Replaying, Saving, Stopping, Stopped, Fault, and Unknown.
- Last Station Save Time: reflects the last time a station saving occurred (config.bog written to flash memory). This save may (or may not) have occurred as a result of the DataRecoveryService.
- Last Station Save Successful: the Boolean value that reflects if the last station save attempt was successful, as either true or false. This save may (or may not) have occurred as a result of the DataRecoveryService.

Note: In the case of a newly created DataRecoveryService, this value is false until the next save occurs.

- Station Save Limit: the number of station saving operations that are allowed to occur during the Station Save Limit Period, before it is determined that the station is spending too much time saving. Exceeding the limit throws the Data Recovery Service into the fault status, since too much data is being generated.
- Station Save Limit Period: the period of time defined for Station Save Limit. If enough number of saving operations occur during the Station Save Limit Period to exceed the Station Save Limit, then the service goes into the fault status. For example, more than 5 station saving operations in 3 minutes period triggers a fault status.
- Persistent Storage Size: reflects the total size of all the data block files flushed to the flashmemory (".drdb" files) that exist in the station's /dataRecovery folder, in kB. Initially, this will be 0, until the first NV-RAM block flushes to flash. It will then increment by that kB amount for each subsequent NV-RAM block flushed.

Note: This value is continually compared to the Persistent Capacity property in the Blocks Configuration property section.

- Generate Alert On Replay: the Boolean (true/false) value that generates an alert (low priority alarm type), which indicates whether a Data Recovery Replay occurred (power was lost). This is a persistent artifact that will show up in the alarm console, since it is useful to know when the power loss occurred. By default the value is false. If set to true, upon any controller boot sequence in which the NV-RAM recorded data is discovered and played back, a corresponding alert is routed to the Alarm Class named in the Data Recovery Alarm Support container. The figure 34. shows details for such an example alert.

- Data Recovery Alarm Support: this is the standard container slot for routing platform service-generated alarms or alerts; in this case, an alert from the DataRecoveryService upon any controller boot sequence in which NV-RAM recorded data is discovered and played back. These properties work in the same fashion as those in an alarm extension for any control point.

6.9.2 Blocks Configuration

These status properties include the following:

- Total Size: reflects, in bytes, the total amount of the NV-RAM buffer memory available to the service. For example, this is 32768 for the 128 kB NV-RAM memory.
- Number of Data Recovery Blocks: reflects the number of data block partitions of the used NV-RAM, for example, 3.
- Active Directory: reflects the directory used in the NV-RAM for the active data block.
- Persistent Directory: reflects the full flash file directory path used to store flushed .drdb files, which equates to: /dataRecovery.
- Full Policy: reflects the current policy in case an NV-RAM data block becomes full (by default: Flush).

Persistent Capacity: reflects the size limit, in kB, for the total of all data block files (.drdb files) that has been flushed to the flash memory. If this limit is exceeded (see property “Persistent Storage Size”), the service automatically triggers a station saving operation.

6.9.3 Data Recovery Blocks

This area provides expandable bar graphs for each of the NV-RAM buffer data blocks, to visually represent the current amount of the used space, overhead space, and available free space, along with numerical values. By default, the currently active NV-RAM block is expanded, showing a bar graph of current buffer usage.

Above the bar graph of each block, its Status is described, typically as either: Active, Idle, or Flushing, with other states Purging, Awaiting Idle, Flush Queued, Defragmenting, Reserved, Fail, and Unknown.

Below the bar graph of each block, numerical amounts display, in bytes, for its total capacity, currently used space, calculated overhead space, and available free space.

6.9.4 Data Recovery Service Properties

In addition to the (default) Data Recovery Service Editor view, the Data Recovery Service also has properties on its Platform Service Properties view, many of which are shown here.

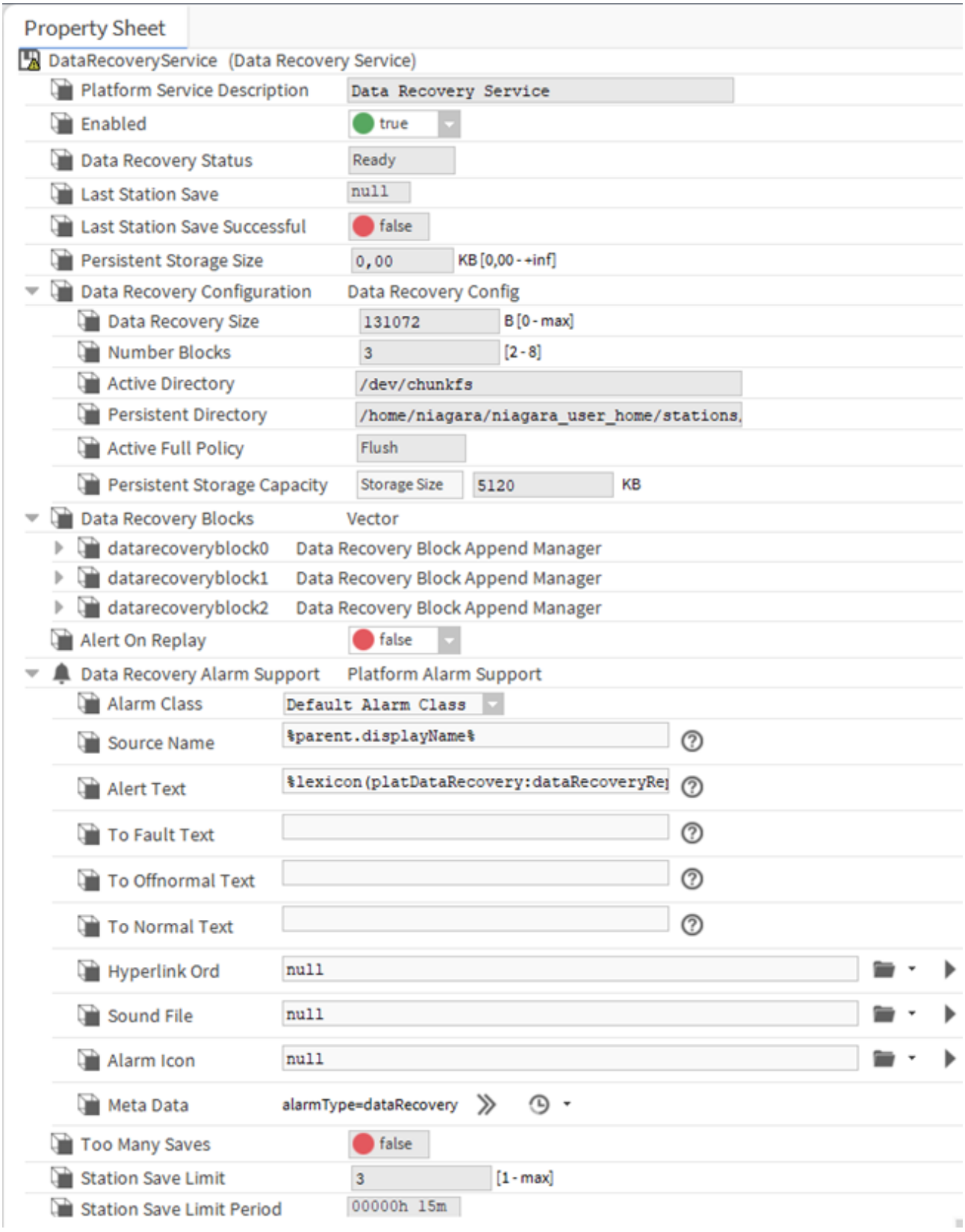


Figure 36. MAC36 Platform Service Properties view of DataRecoveryService

Most of these properties are also on the Data Recovery Service Editor default view.

6.10 HDMI Connection

The iSMA-B-MAC36PRO and iSMA-B-MAC36NL controllers support the built-in HDMI port, which allows connecting an external display by a standard HDMI cable (HDMI

standard type A). The HDMI connection allows viewing the user's station data directly on the display, without a need of connecting PC with a web browser. **It is recommended to use the HMI panels from the iSMA CONTROLLI offer–other panels may not work or may operate incorrectly, and may have problems with resolution and touch**. iSMA CONTROLLI does not take the responsibility for the proper operation of the MAC36 controllers with other HMI panels.

Note: MAC36 controllers have a built-in USB port, which supports a display's touchpad.

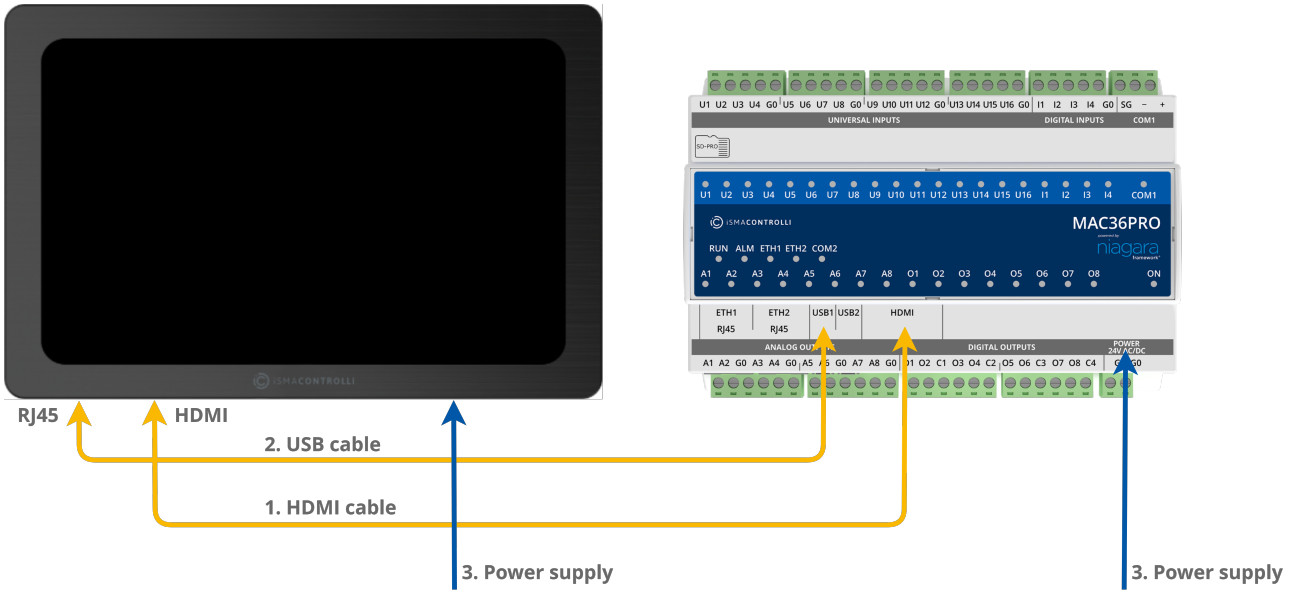


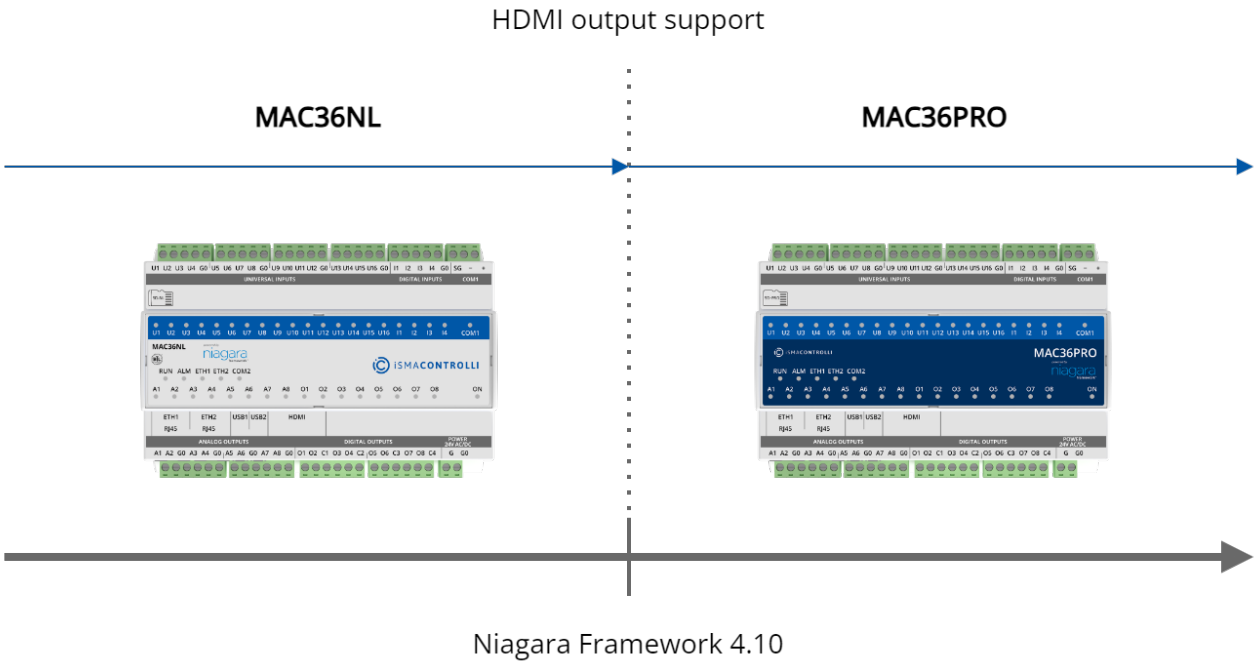
Figure 37. Connecting HDMI panel

6.10.1 Supported Niagara Versions for HDMI Connection

HDMI functionality depends on the combination of the controller hardware and installed version of the Niagara Framework.

- The iSMA-B-MAC36NL supports HDMI output only up to and including Niagara 4.10.
- The iSMA-B-MAC36PRO supports HDMI output from Niagara 4.10 and newer.

Using an unsupported version may result in incomplete support for all Niagara views in the MAC36NL controller.



Note
For best performance and responsiveness, it is recommended to use the HDMI output with the latest version of the Niagara Framework and the MAC36PRO controller. The MAC36PRO, with its more powerful processor and iSMA OS64, combined with the Chromium browser for visualization, improves performance, supports pinch-to-zoom functionality, and provides full support for HTML5 views.

6.10.2 Preparation for HMI

For convenient use, it is recommended to use a handheld profile for users, who support HMI views. The use of HMI views via HDMI is conditioned by the launch of the web browser on the Niagara 4 environment in the MAC36 controllers. Using HDMI will cause a significant increase in CPU usage and its operation in a higher temperature range. HMI views via HDMI are dedicated to local application support in the MAC36 controllers. The size and level of complexity of the PX pages is related to the responsiveness of local service. The more complex the graphics, the longer it takes to go between the pages, and, therefore, in order to provide smooth navigation, it is recommended to use 15-20 graphic widgets and 2-3 gif animations in lower resolution than the default (e.g., 1024x576 px with ratio fit scaling for full screen). With more powerful hardware, the visualization will be more responsive on MAC36PRO compared to MAC36NL. For now, the only resolution supported in the MAC36PRO controller is 1280x720, which is also a default resolution in the MAC36NL version.

Note: Web browser works only with HTTP, therefore, it is necessary to enable an HTTP support in Station/Config/Services/WebService; by default, the HTTP support is disabled.

6.10.3 Update to Support HDMI Port

Preparation for using the HMI panel:

- Download the update from the iSMA CONTROLLI support site, which allows to support HMI views via HDMI port, and is necessary to install the required files and modules for the appropriate version of Niagara.
- Perform the update on the MAC36 controller using the Commissioning Wizard procedure to support HDMI port.

The iSMA_HDMI module is not installed by default on the MAC36 platform. It needs to be installed during the commissioning or by using the Software Manager tool under the platform component.

An important development in the MAC36PRO version is that the iSMA_HDMI module is no longer required for the HDMI service just to operate. It can be operated directly from the web browser. The module is, however, necessary to change HDMI configuration parameters (same as in MAC36NL), if so required.

The iSMA_HDMI module has been created to service, configure and maintain the HDMI connection in MAC36.

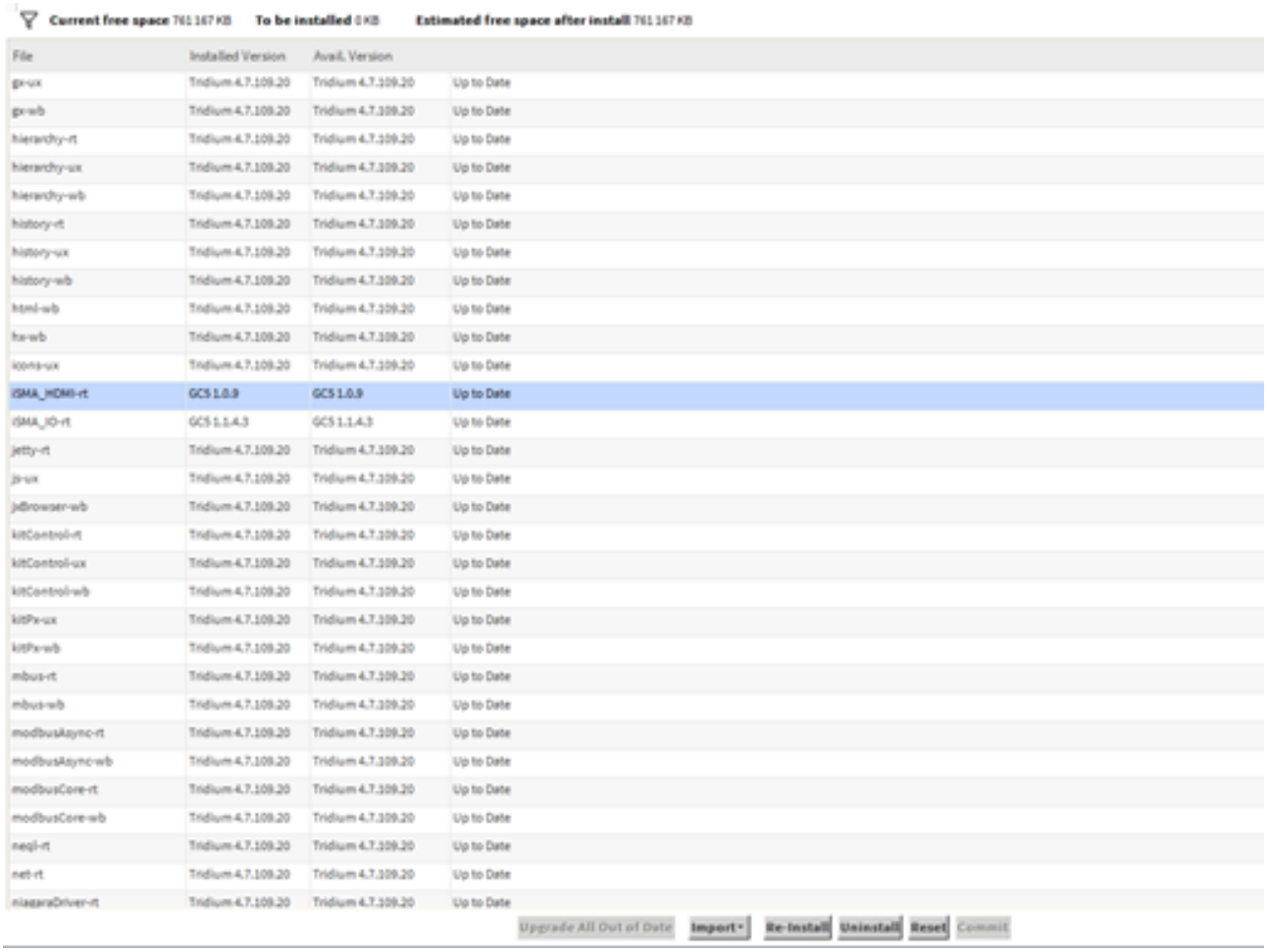


Figure 38. iSMA HDMI update

- After completing the update, go to the configuration of the HDMI support.
- After completing the configuration, it is recommended to restart the station.

6.10.4 Module iSMA_HDMI

The **iSMA_HDMI** module has only one component, the **iSMAHDMI** service, which needs to be added under **Station/Config/Services**.

The iSMAHDMI component contains all settings, which are needed to successfully connect and configure the HDMI support.

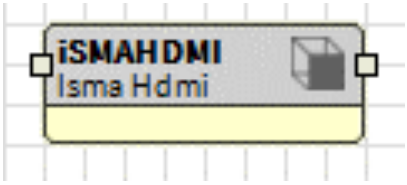


Figure 39. iSMA module

The HMI panel connected to HDMI port can work in 3 independent modes:

- Normal mode: the panel displays the station data and it is ready for interaction with the user;
- Screensaver mode: the panel displays the image chosen by the user. Turning back from this mode to the Normal mode is executed right after the user's activity (touch). The last open site is displayed.
- Standby mode: the panel is in an energy-saving mode, the backlight is switched off. Turning back from this mode to the Normal mode is executed after the user's activity (touch) and takes around 10 seconds. The last open site is displayed.

The iSMAHDMI component consists of the following slots:

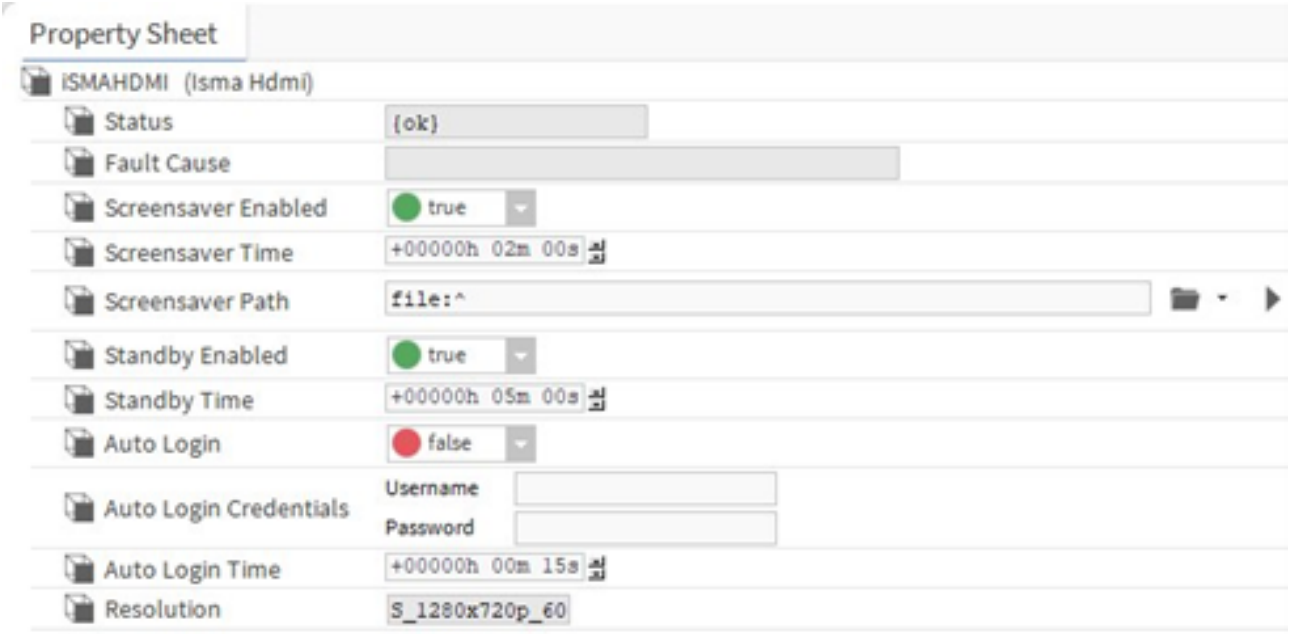


Figure 40. iSMA HDMI Property sheet

- Status: status of HDMI Service, available states:
  - OK: the service is working properly;
  - Fault: a fault has occurred.
- Fault Cause: shows a fault cause description:
  - None: no fault;
  - Could not connect to HDMI server. Connection refused: the service cannot connect with HDMI–the MAC36 software is not up to date or there is a problem with a hardware;
  - Service is duplicated: the HDMI Service is added twice.

The slots assigned with the Screensaver mode:

- Screensaver Enabled: this slot switches on or switches off the Screensaver mode (true–mode enabled, false–mode disabled). By default, the Screensaver mode is active;
- Screensaver Time: this slot contains the time value in hh:mm:ss format. This time starts counting down, when there is no user activity on the display (no touch). If the time elapses, the display goes to the Screensaver mode. The default value is 2 minutes.
- Screensaver Path: the slot contains the path to the custom image, which is displayed on the screen in the Screensaver Mode. The default image for the screensaver is shown below.

Figure 41. Screensaver

- Standby Enabled: this slot switches on or switches off the Standby mode (true–mode enabled, false–mode disabled). By default, the Standby mode is active.
- Standby Time: this slot contains the time value in hh:mm:ss format. This time starts counting down, when there is no user activity on the display (no touch). If the time elapses, the display goes to the Standby mode. The default value is 5 minutes.

Auto Login Function

Due to the user's requirement to login after a power outage, and to ensure a better ease of use of the HMI panel, the Auto Login function was created. Thanks to this function, after each power failure, the browser automatically logs in the user and launches the start page according to the navigation file assigned to the user.

To start the auto login function:

- Enter the name of the existing user with Config\Services\UserServices in the Auto Login Credentials\Username slot, which will be used for Auto Login function.
- Enter the password entered the user in the Auto Login Credentials\Password
- Activate the Auto Login function in the Auto Login slot (switch to true).

Now the Auto Login function allows to view the station's home page without a need of entering the user's credentials every time after power failure.

Slots assigned to the Auto Login function

- Auto Login: this slot enables or disables the Auto Login function (true –function enabled, false–function disabled). By default, the Auto Login is disabled. After configuring the user to log in automatically and enabling the Auto Login function, the user's default Auto Logoff Enabled function will be automatically inactivated (switched to false) in Config\Services\UserServices. The Auto Logoff Enabled function does not automatically return after disabling the Auto Login function in the iSMA HDMI Service for a given user.
- Auto Login Credentials: username and password for the station user. If the Auto Login is enabled, the user with the credentials stored in this slot will be logged in to the station.
- Auto Login Time: this slot contains the time value in hh:mm:ss format. This time allows to decide to log in another user than the one that has been configured for the Auto Login function. This time starts counting down when the login site appears and there is no user activity on the display (no touch). During the countdown, there is an option to log in as another user by clicking on the Change User link. Entering any character in the login field cancels the Auto Login function. If there is no reaction from the user after the elapsed time, the user from the Auto Login Credentials slot will be automatically logged in to the station. After logging out of another user, to return to the Auto Login function, simply click on the Change User link, and autostart working again. The default value is up to 15 seconds.

Note: After the power failure, the Auto Login function takes place immediately without counting down the time. After logging out of the HMI views, the user can be changed during the time count down.

Slots assigned to the resolution of the connected HMI panel

- Resolution: shows the used resolution of the HMI panel in order to properly prepare the resolution of PX files.

6.10.5 Adding and Start-up of the HDMI Service

Below steps describe actions required to run the HDMI service.

For MAC36PRO, step 1 can be omitted–the iSMA_HDMI module has to be installed only on the MAC36NL version. The HDMI service will run on the MAC36PRO version regardless, unless it is necessary to change any of HDMI configuration parameters, then installing the module is required.

Step 1: Install the latest iSMA_HDMI-rt module with platform Software Manager.

(a) The HDMI Service uses the HTTP 80 port internally to run web server. To enable it, open Config\Services\WebService, and set the Https Only slot to false and the Http Enabled slot to true, as in the figure below.

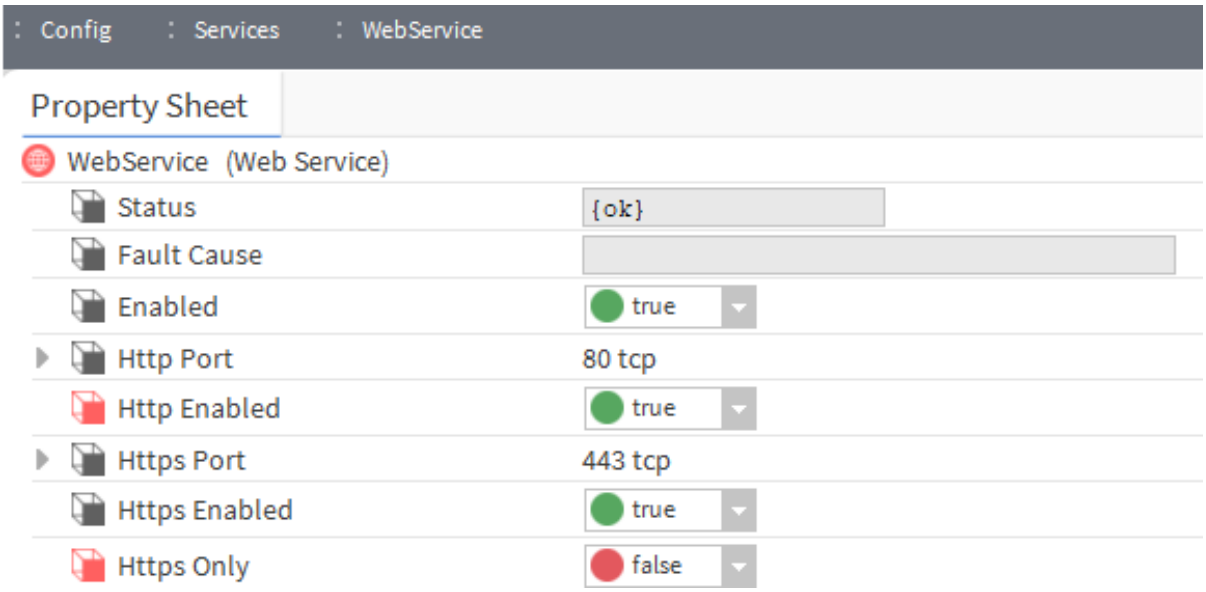


Figure 42. Proper WebService configuration for HDMI support

(b) Find and open the **iSMA_HDMI**.

(c) Drag and drop the **iSMAHDMI** component to **Config\Services** of the station.

(d) Save the station.

Step 2: Disconnect the power supply from the MAC36 controller.

Step 3: Connect the MAC36 controller with the panel HMI as in the above diagram.

Step 4: Connect the power supply to the MAC36 controller and the HMI panel, which will make the panel detectable by the controller.

Note: Connecting the panel to the HDMI port, while the power supply is connected, makes it not detectable by the controller.

For MAC36NL, during the start-up of the controller (platform/station), and provided the HDMI service is not configured in the running station, the following image will be visible:

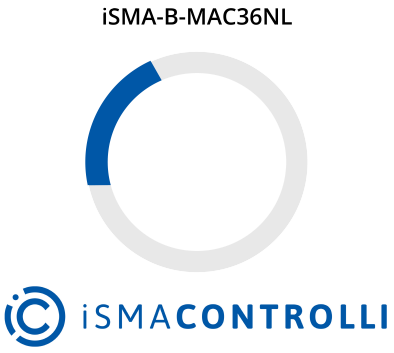


Figure 43. No HDMI service

Step 5: After starting the station with the configured HDMI service, the Login window will appear, as shown below:

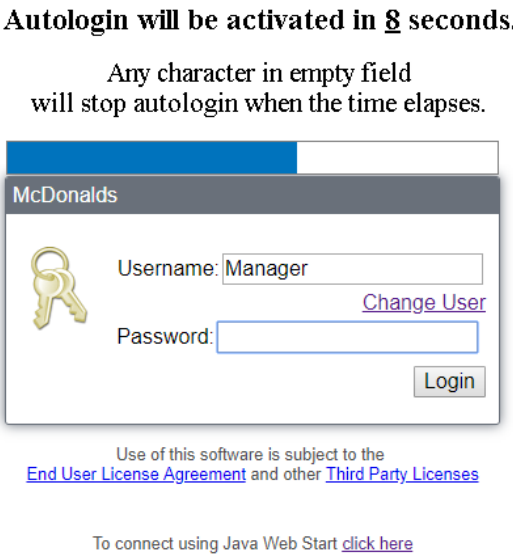


Figure 44. Login view

In case of the configuration of the Auto Login function, the user login fields will be completed automatically, along with the activation of the login button, and the start page of the HMI views will be opened (the following sample view).

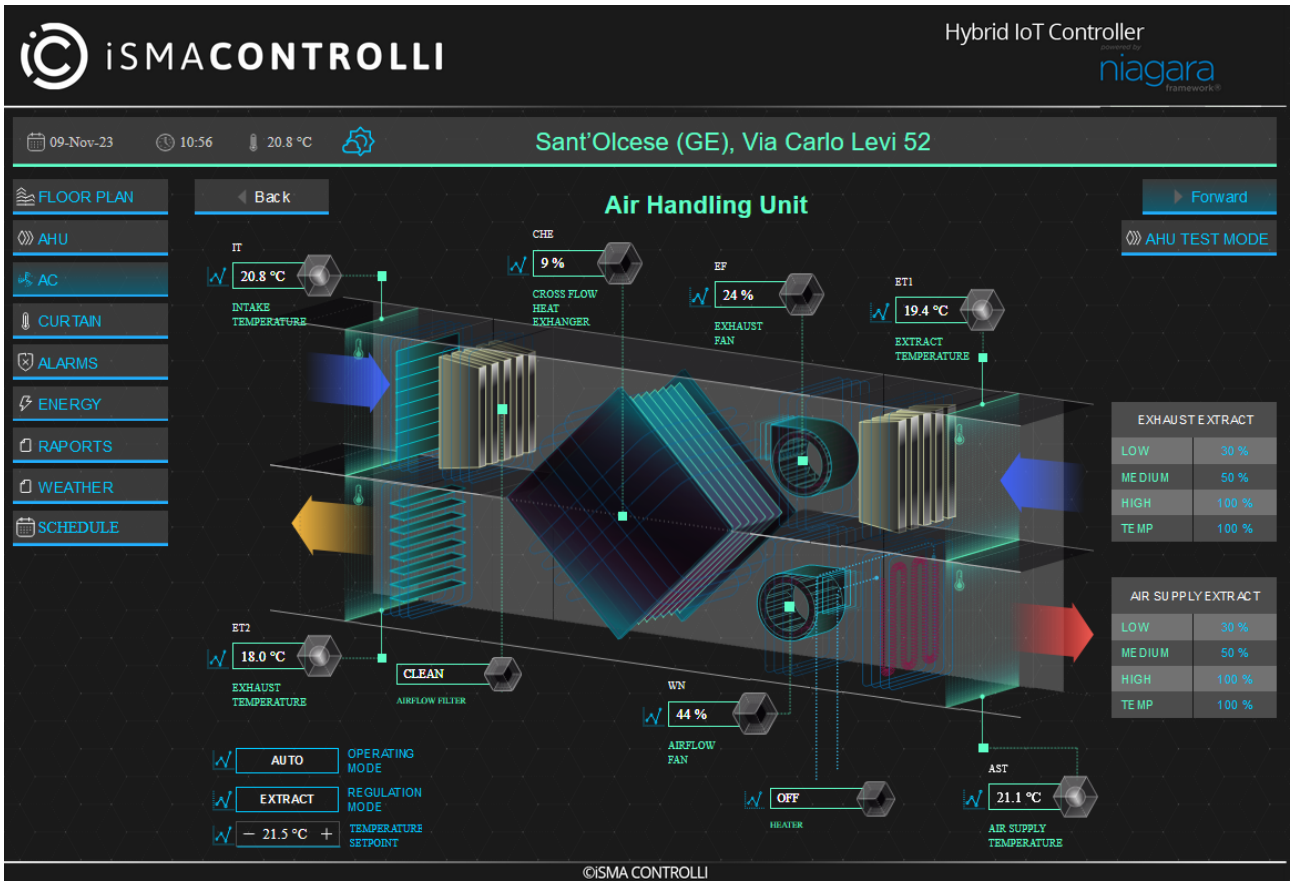


Figure 45. Start page

Note: A HDMI refresh rate, the hx.poll.freq parameter, cannot be less than 1000 ms (by default, 5000 ms).

In case of unexpected problems with establishing a connection or suspension of the view page, or, for example, the need to quickly return to the start page, there is a special service menu available.

To access it on the MAC36NL controller, swipe from the top of the screen and the following service menu view becomes accessible on the top of the screen.

Figure 46. Menu

Function buttons fulfill a similar role as in the web browser:

- BACK (left arrow): return to the previously opened page.
- FORWARD (right arrow): move to the next page in the case of a BACK action.
- REFRESH (circle with an arrow): refresh the current page (reload).
- HOME (house): opens the start page defined in the navigation file (does not open the login page).

MAC36PRO adopts a different approach and instead of a swipe-down menu supports swipe-left for backward and swipe-right for forward commands, as well as two-finger zoom in and out options. The on-screen keyboard is movable and is available in 3 languages: English, German, Spanish, and French.

6.10.6 User Fonts Support

The MAC36 controllers have a built-in database of most popular fonts, used to efficiently depict visualizations on the HDMI panels. The database includes the free substitutes of most common fonts, according to the list below (the bracketed names are the names of free substitutes):

- Arial [Liberation Sans];
- Courier New [Liberation Mono];
- Tahoma [Wine Tahoma];
- Times New Roman [Liberation Serif];
- PT Sans [implemented directly];
- Source Sans Pro [implemented directly];
- Inconsolata [implemented directly];
- Hunkyfonts Sans [implemented directly];
- Ubuntu-font-family [implemented directly];
- Niagara default font [Adobe Source Sans Pro].

Note: In case of HDMI panels, if the user adds text to graphics (i.e., PX file) using an unsupported font, the outcome will be depicted using the Déjà vu font, which may cause moving the whole text to the right.

The user has an option to add additional fonts, which requires uploading a font file to the controller.

In order to upload a font to the controller, log in to the platform and go to the "File Transfer Client"; on the left side of the view choose a file location on the PC, and on the right side of the view go to \UserHome\daemon\fonts location on the controller:

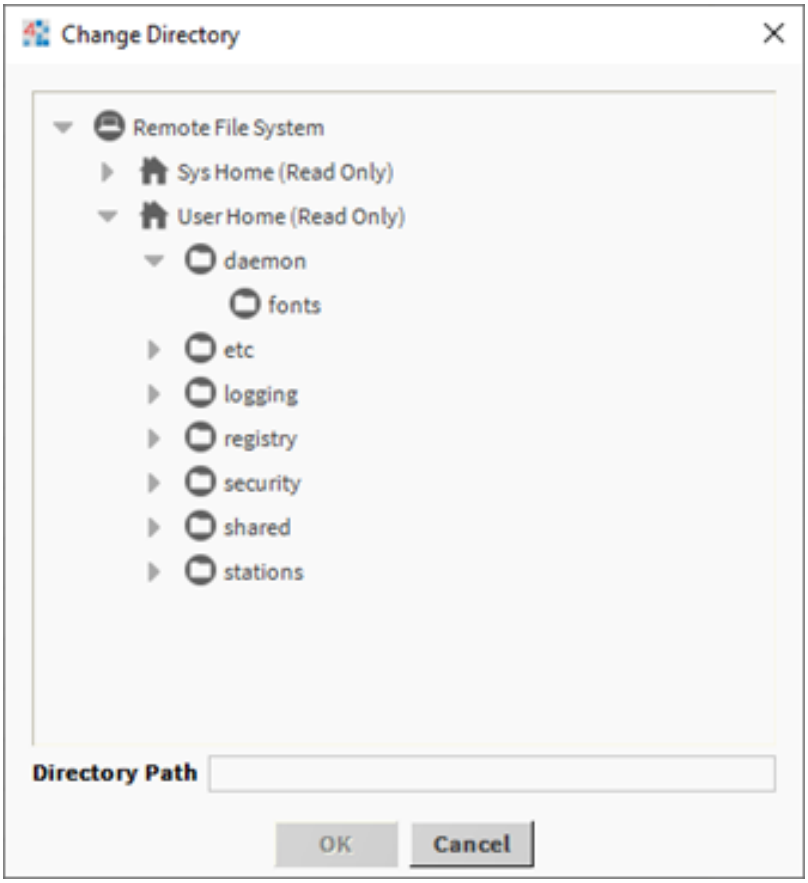


Figure 47. Fonts adding view

On the left side choose fonts to be uploaded, and transfer them to the controller using the right arrow.

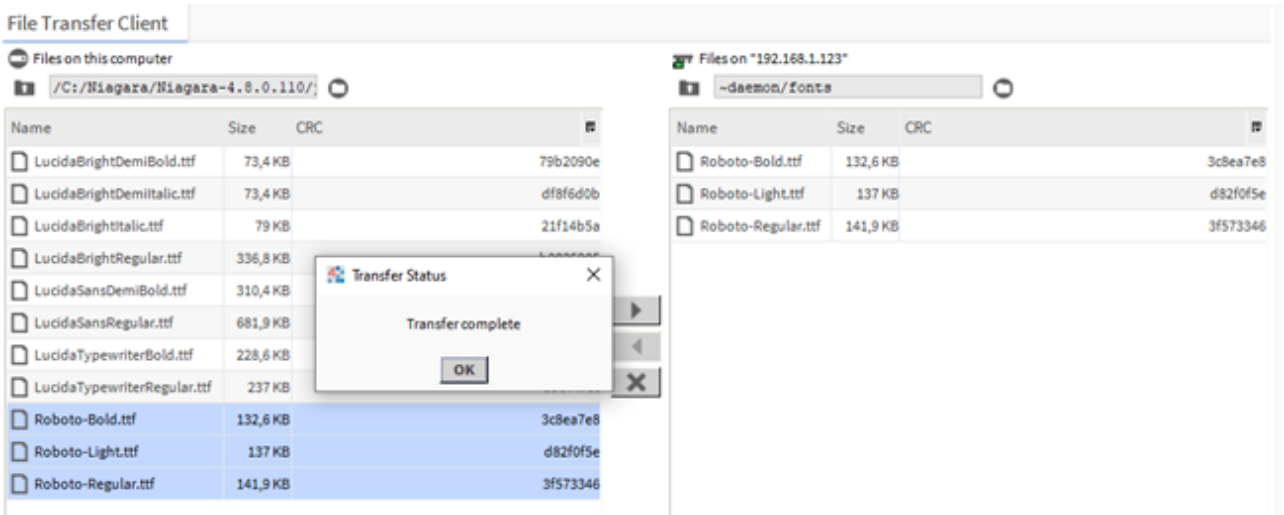


Figure 48. Transferring fonts

Upon a successful transfer, a „Transfer complete" window pops up.

Once all the user fonts are successfully transferred, go to the Application Director and reboot the controller (restart of the station is not enough).

After the controller is rebooted and the station loaded, the HDMI panel will properly depict text with user-uploaded fonts.

7 MAC36PRO Services

This chapter describes the functions available in the MAC36PRO controller. The features are part of the iSMA OS64 system and are available with iC Niagara 4.15.1 update.

Note: In order to use the features listed below, please ensure that the correct version of the Niagara Framework is installed on the controller.

7.1 IP over USB

The MAC36PRO controller supports an IP over USB connection, enabling an instant, plug and play network connectivity between PC and the controller, without a need of any additional drivers using static IP address.

7.1.1 USB Hardware Connection

The connection is established through the USB2 (OTG) port on the MAC36PRO. A USB A–A male-male cable is required to link the controller with the PC.

Note: Please ensure the connection is done by using the supported USB2 OTG port.

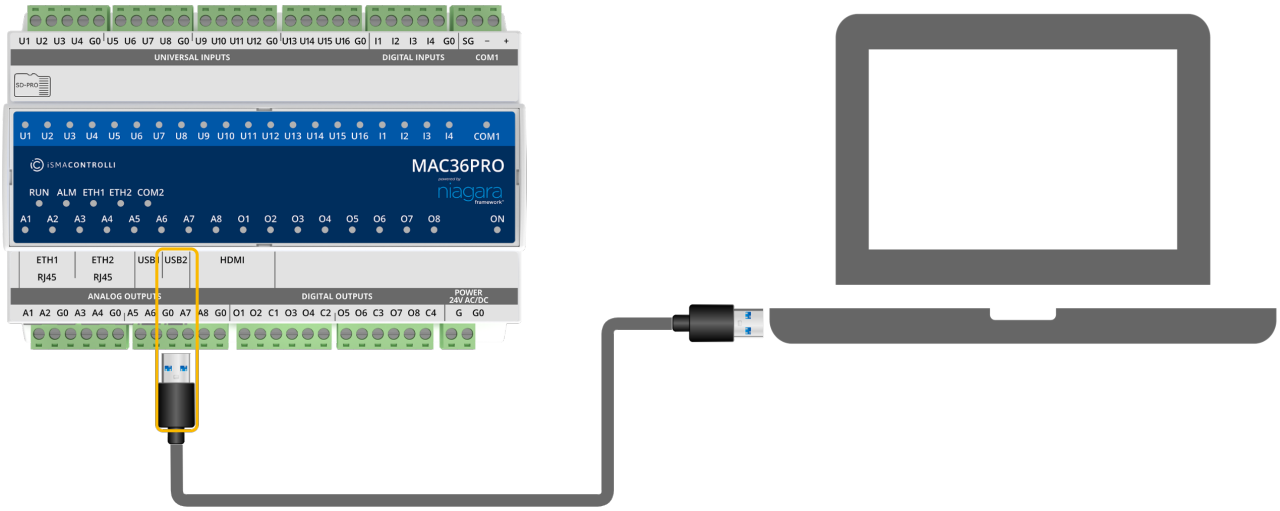


Figure 49. USB A-A male-male connector

IP address
Static IP address of the MAC36PRO controller when USB is connected: 169.254.1.123.

7.1.2 Network Configuration

Once the USB connection is established, the MAC36PRO controller emulates a Virtual Network Interface using the RNDIS protocol.

No additional configuration is required on the PC if the virtual Ethernet interface is automatically recognized. The controller creates a local DHCP network and assigns an IP address to the connected device.

Note: If the controller cannot be reached, please make sure that the Virtual Network Interface has been properly detected and installed in the PC's network settings.

7.2 Device Management Web Server

The MAC36PRO features a built-in Device Management Web Server, a web-based interface designed for pre-commissioning the controller, monitoring the system parameters and health status, managing the controller network parameters, and configuring the iSMA OS-level settings.The web server can be used to pre-commission the controller even if the host ID has not been licensed yet. By default, the web server is enabled and accessible via HTTPS connection on port 5580. It can be accessed using ETH1, ETH2, and USB network connection.

HTTPS
For security reasons, a standard HTTP connection is disabled by default. Connection to the MAC36PRO web server is possible only via a secure HTTPS protocol. Please make sure that the https://<MAC36PRO_IP_ADDRESS>>:5580 address is used while connecting with the controller's web server.
HTTPS - first connection
When connecting to the MAC36PRO web server for the first time, a browser warning may appear because of the self-signed certificate. This is expected behavior for embedded systems using HTTPS. It is required to accept the certificate to access the web server.

The first connection can be established using the default IP address of the controller (192.168.1.123) or through the USB connection on static IP address (169.254.1.123).

7.2.1 Login

To access the web server functions, the user must be logged in. The web server is secured with Niagara Platform credentials.

First Login

If the controller has not been commissioned yet, please use the default Niagara Platform credentials (tridium:niagara).

If the default credentials are used, the system will prompt the user to change them. A dialog window appears requiring:

- new username,
- new password,
- system passphrase,

The default tridium user will be removed and the new user will be created. The same user will be used to log in to the controller platform in Niagara Workbench.

7.2.2 Home Page

Home page of the MAC36PRO device management web server contains basic data about the device. It is displayed after a successful logging in to the device. It is useful for troubleshooting, and monitoring controller health status.

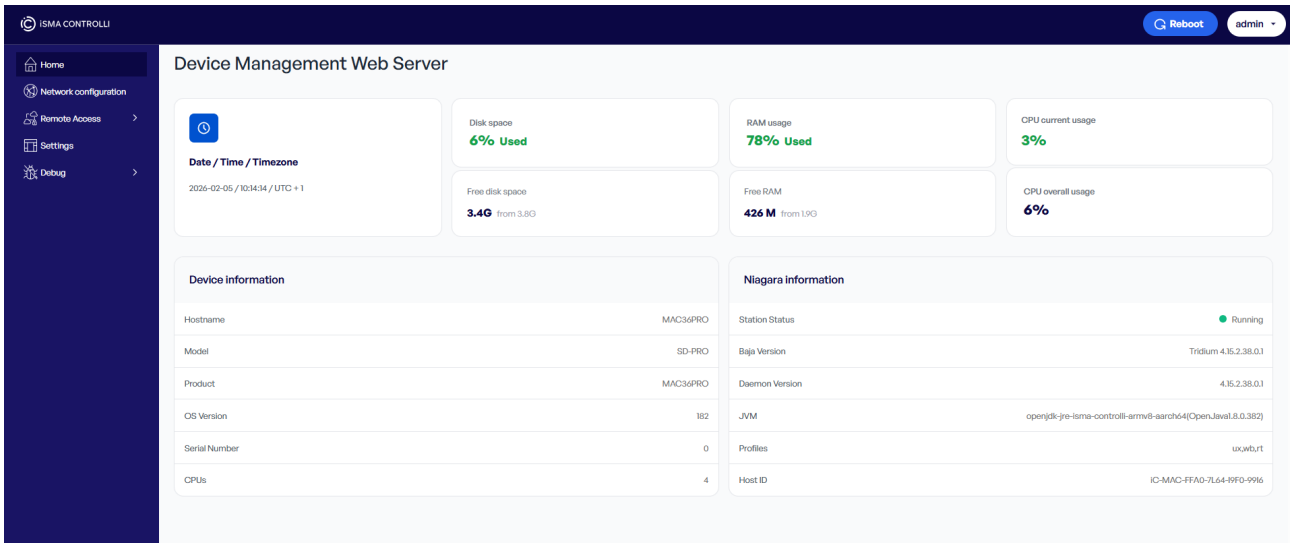


Figure 50. Device Management Web Server - home

Home page contains the following data:

- **Date/Time/Time Zone:** shows a current date, time, and time zone set on the controller,
- **Disk Space:** shows a current usage of the disk space on the controller (presented in %),
- **Free Disk Space:** shows an amount of free disk space out of the total disk space available on the controller (presented in GB),
- **RAM Usage:** shows a current RAM usage by the controller (presented in %),
- **Free RAM:** shows an amount of free RAM out of total RAM available on the controller (presented in MB/GB),
- **CPU Current Usage:** shows a current CPU usage by the controller (presented in %),
- **CPU Overall Usage:** shows a summary CPU usage by the controller from the device start (presented in %),
- **Hostname:** shows a hostname of the controller; the hostname can be configured in the Network Configuration section,
- **Model:** shows a Niagara model of the controller,
- **Product:** shows a product code of the controller,
- **OS version:** shows an OS version installed on the controller,
- **Serial Number:** shows a serial number of the controller,
- **CPUs:** shows a number of CPUs in the controller,
- **Station status:** shows a status of the station saved on the controller,
- **Baja Version:** shows a Baja version,
- **Deamon Version:** shows a Niagara deamon version,
- **JVM:** shows a Java Virtual Machine version,
- **Profiles:** shows used Niagara profiles,
- **Host ID:** shows a host ID for the licensing purposes.

In the top right corner of the device management web server, there are 2 buttons available for the device reboot and logging off. These are available regardless of which tab of the web server is being displayed at the moment.

Figure 51. Two buttons available in top right corner of the view

For a reboot, a confirmation pop-up is displayed:

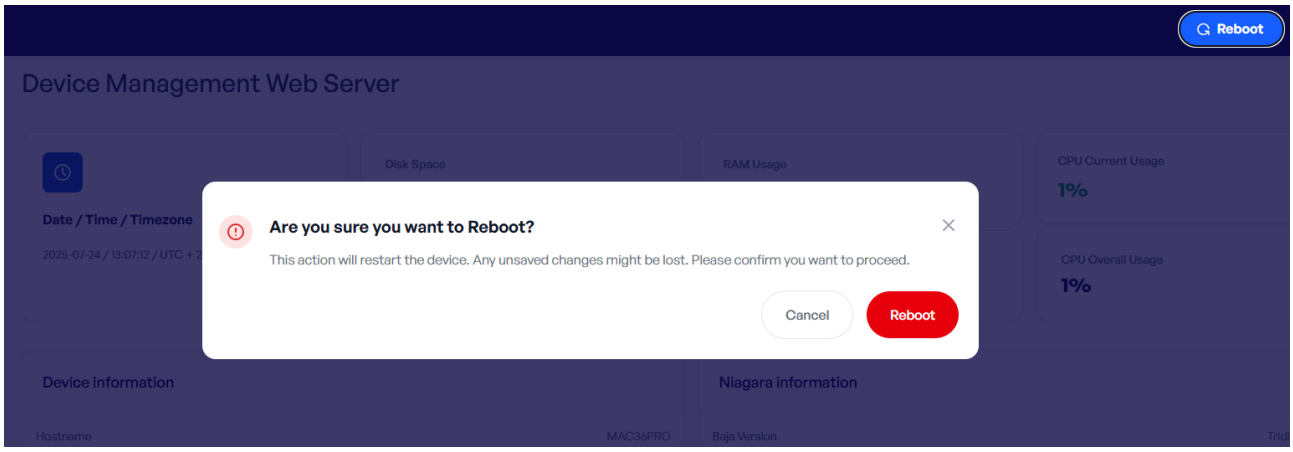


Figure 52. Reboot confirmation pop-up window

7.2.3 Network Configuration

The Network Configuration tab shows the settings of the controller's network interfaces and allows to manage them. It allows to pre-configure network parameters for each Ethernet interface available on the controller, before accessing the platform in the Niagara Workbench or in case of any changes to the network parameters during the controller operation.

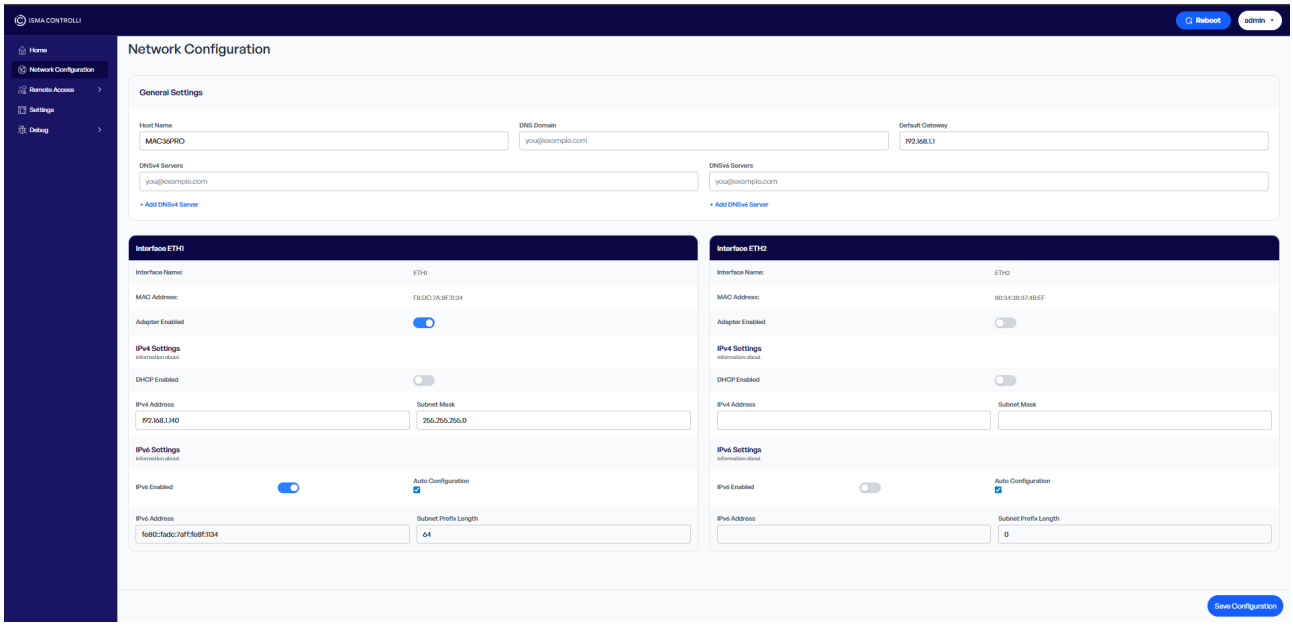


Figure 53. Device Management web server - network configuration

The Network Configuration tab has the following fields:

General Settings tab:

- **Host Name:** allows to set a network hostname of the controller,
- **DNS Domain:** allows to set a DNS domain,
- **Default Gateway:** allows to set a default IP gateway,
- **DNSv4 Servers:** allows to set a DNS server for IPv4,
  - **+Add DNSv4 Server:** allows to add an additional DNS server for IPv4,
- **DNSv6 Servers:** allows to set a DNS server for IPv6,
  - **+Add DNSv6 Server:** allows to add an additional DNS server for IPv6;

Interface ETH1/ETH2 tabs (dependent on controller's interfaces):

- **Interface Name:** shows the interface's name,
- **MAC Address:** shows the MAC address of the controller's eth1/2 interface,
- **Adapter Enabled:** allows to enable/disable the Ethernet adapter mode;

IPv4 Settings:

- **DHCP Enabled:** allows to switch on/off a DHCP mode,
- **IPv4 Address:** allows to set an IP address of the controller,
- **Subnet Mask:** allows to set a subnet mask of the controller;

IPv6 Settings:

- **IPv6 Enabled:** allows to enable the IPv6 addressing for the controller,
- **Auto Configuration:** allows to set the controller's IPv6 address and subnet prefix length automatically,
- **IPv6 Address:** allows to set the controller's IPv6 address if the auto configuration is checked off,
- **Subnet Prefix Length:** allows to set the controller's subnet prefix length if the auto configuration is checked off.

After making any change in the Network Configuration tab, it **is required to** confirm changes with the Save Configuration button.

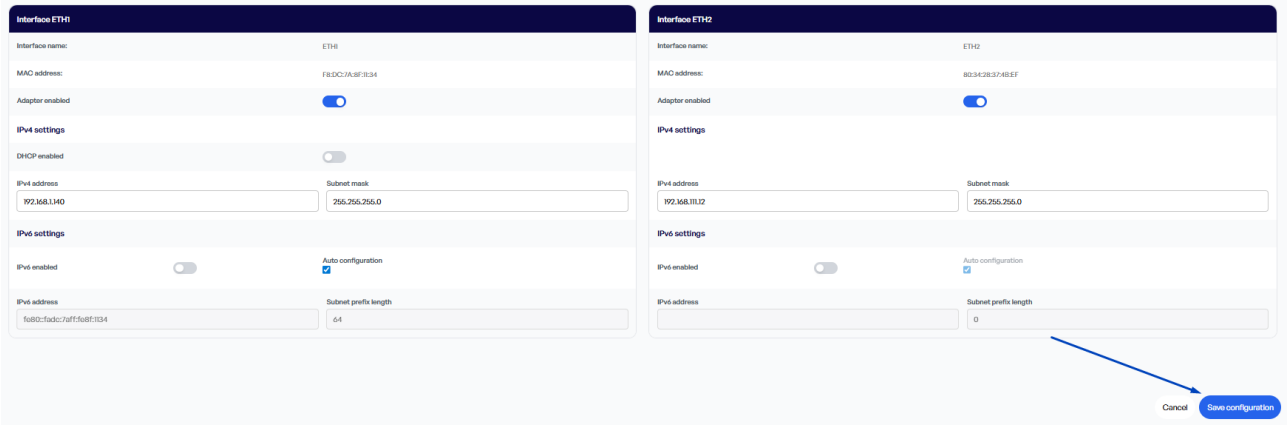


Figure 54. Save Configuration button

Any change made to the network settings is validated. A green pop-up upon saving a new configuration informs that entered data are correct and a reboot is required:

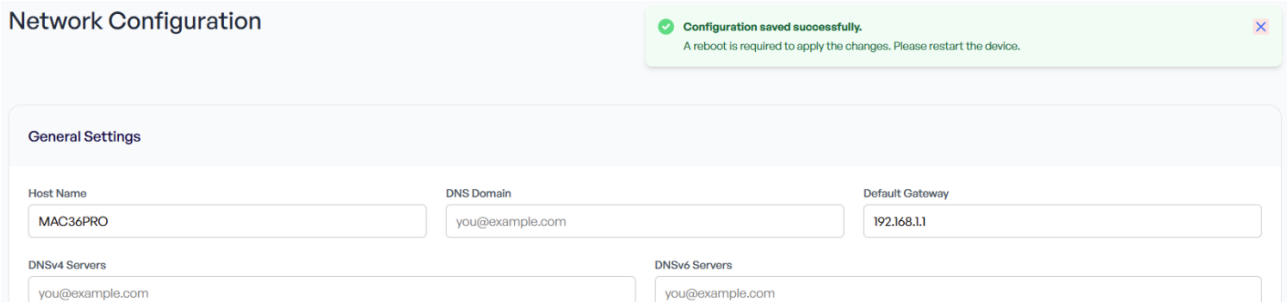


Figure 55. Correct validation pop-up

A red pop-up informs that entered data are incorrect. Saving will not be possible until corrected data are filled in.

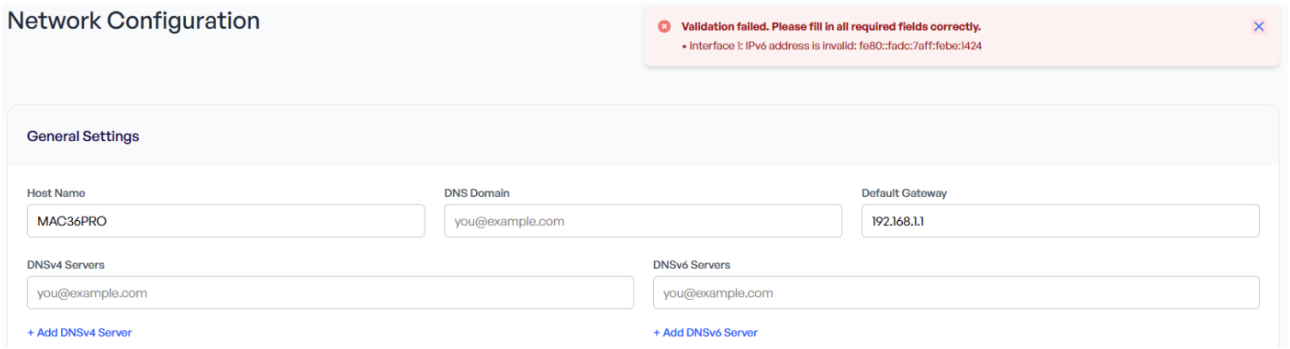


Figure 56. Incorrect validation pop-up

7.2.4 Remote Access

In the Device Management web server's tree, under Remote Access, the VPN, LTE, and SSH tabs are available.

WireGuard VPN

The WireGuard VPN tab allows to manage the VPN connection supported by the MAC36PRO controller.

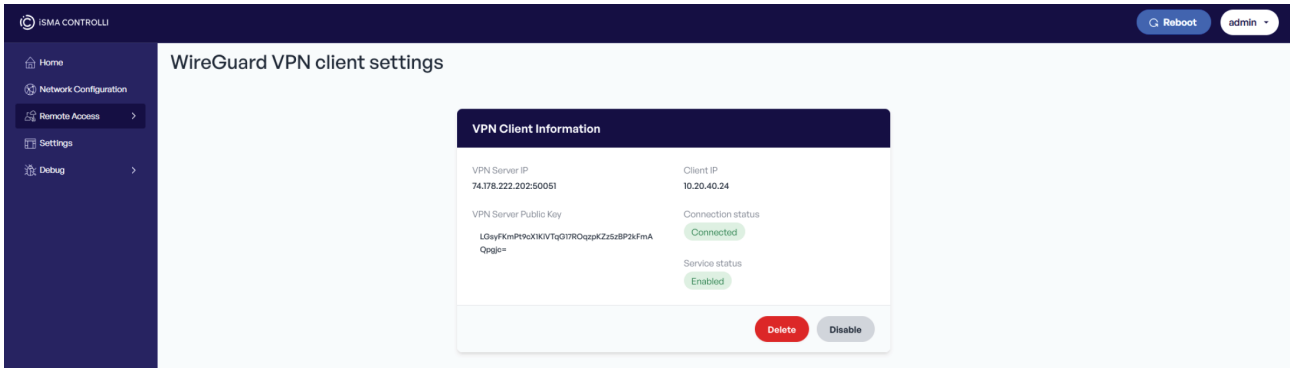


Figure 57. Remore Access - VPN settings

The MAC36PRO supports a connection to a WireGuard VPN network in a client mode. It enables to secure remote access to the controller through an encrypted tunnel. Once the VPN connection is established, the controller's web server, platform, and station can be accessed using the VPN IP address, providing complete remote control of the MAC36PRO controller.

> Note
> The MAC36PRO acts as a VPN client only. A separate WireGuard infrastructure is required to establish the WireGuard VPN connection with the controller.

To establish a VPN connection, a valid WireGuard configuration file (.conf) must be provided by the VPN server administrator. This is a standard file, which defines all necessary parameters including:

- interface private key,
- VPN server (peer) public key,
- client IP,
- VPN server IP (endpoint address),
- allowed IP ranges.

To set up the WireGuard VPN Client, follow the three step process:

Step 1: Upload configuration

Add the .conf file provided by the VPN server administrator. Use the Choose File button to select the file and Upload button to send it.

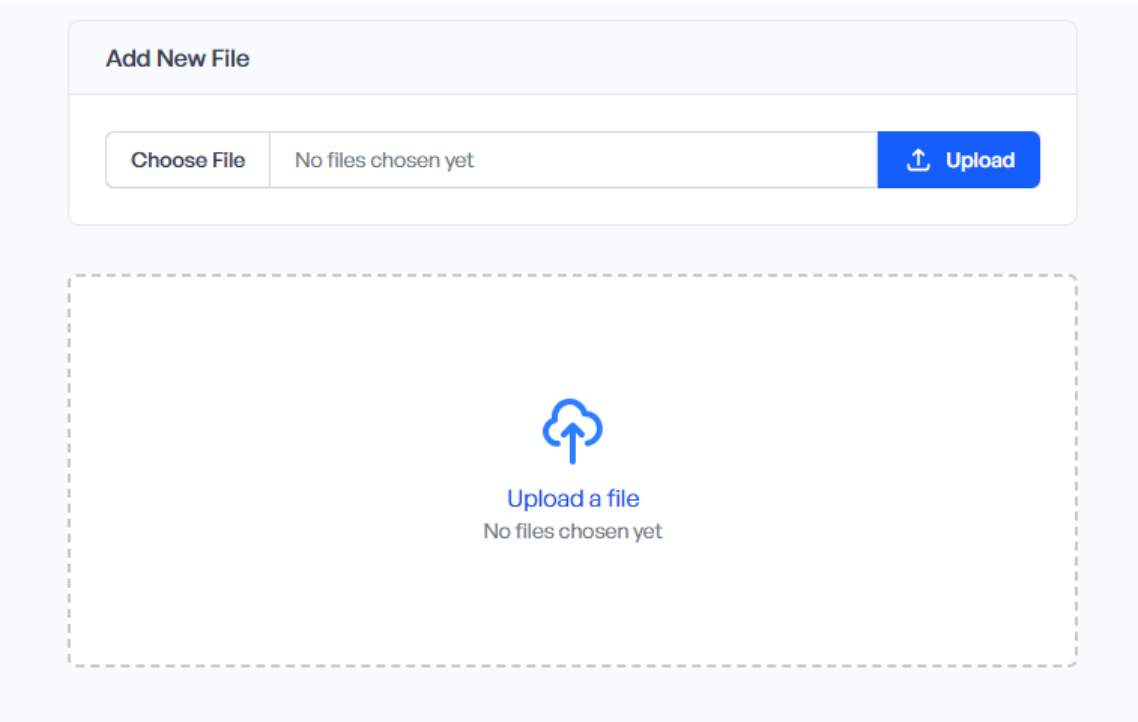


Figure 58. Adding new VPN configuration

> **Note**
> The upload window becomes available only if there is no previously uploaded VPN configuration currently on the device. If the configuration file has been uploaded, it must be removed first using the Delete button before uploading a new one.

Step 2: Activate the configuration

After uploading a configuration file, it is required to activate it in order to initiate the VPN connection.

Step 3: Controller reboot

A device restart is required to apply the changes and establish the connection with the WireGuard VPN server. Reboot can be initiated using the button in the top right corner of the web server.

A correctly configured VPN service will display information about the established connection to the WireGuard VPN server.

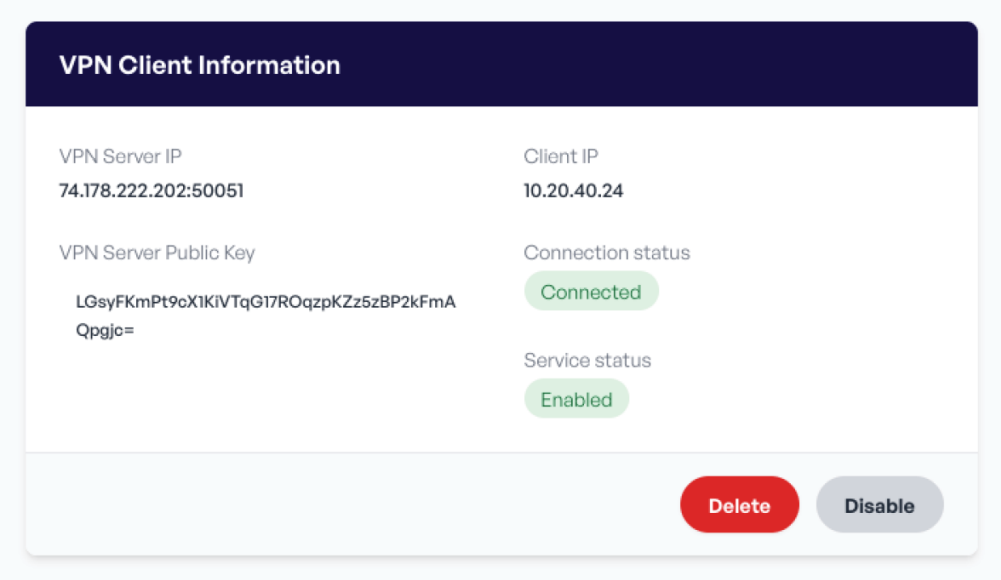


Figure 59. Correctly connected VPN

LTE

The LTE Settings tab is dedicated to the configuration of an LTE 4G connection with the MAC36PRO controller.

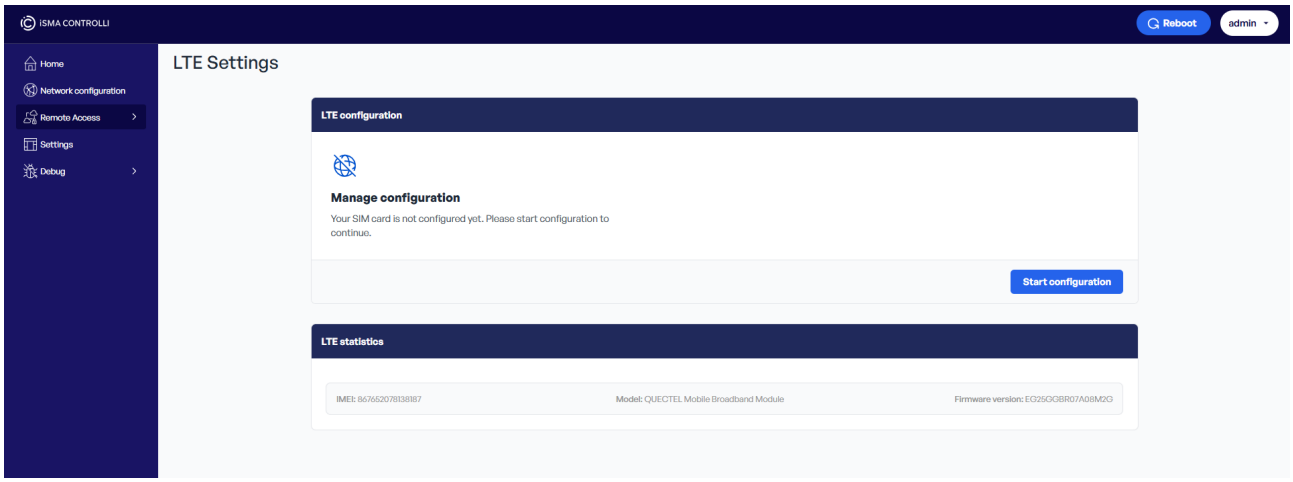


Figure 60. Remote access - LTE

- LTE Configuration:

The LTE Configuration section allows to set up a SIM card configuration for the LTE connection. To start, press the Start configuration button and follow the instructions, which prompt to fill in a PIN number (if required), APN, and public access protection requirements.

> Note
> A reboot is required after setting up a SIM card configuration.

- LTE Statistics:

The LTE Statistics section allows to enable/disable the LTE service, it indicates the LTE service and connection status and shows the LTE signal strength.

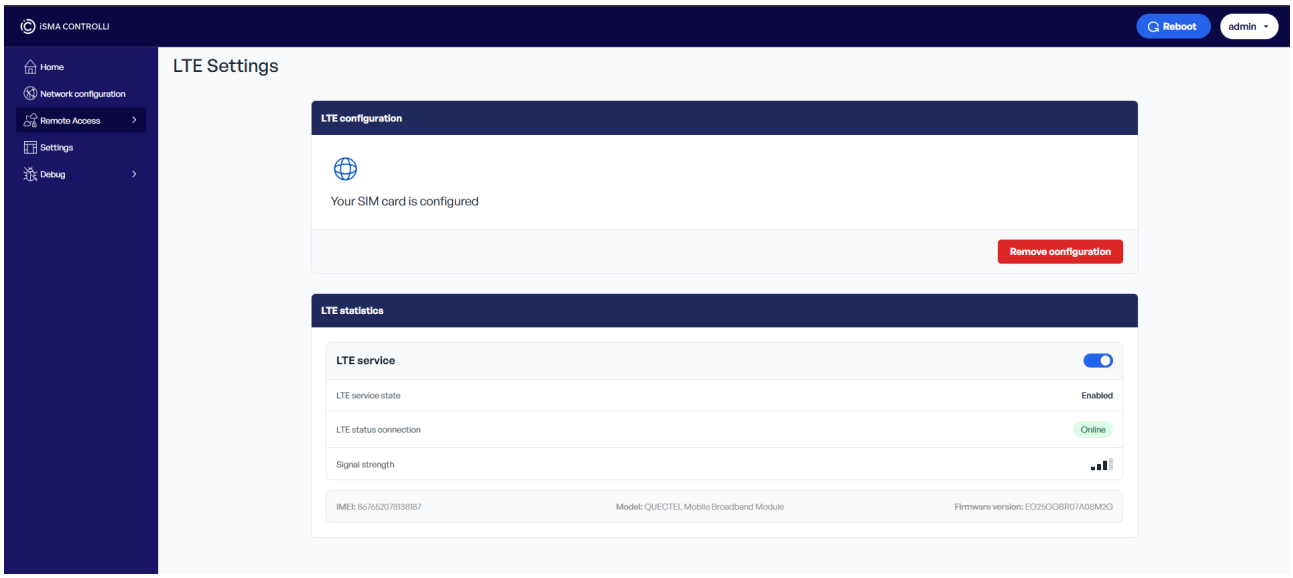


Figure 61. Remote access - LTE statistics

To learn more about the LTE connection, please see: LTE Configuration.

SSH

The SSH tab allows to set up an SSH connection on the MAC36PRO controller.

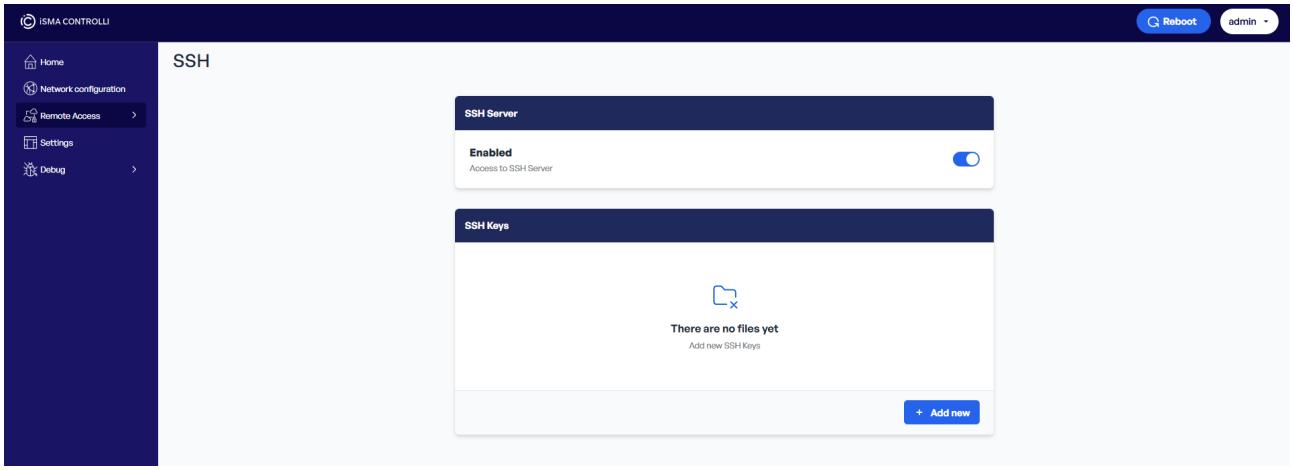


Figure 62. Remote access - SSH

- SSH Server:

The SSH Server section allows to enable/disable access to the SSH server.

- SSH Keys:

The SSH Keys section allows to add a public SSH key(s) to the MAC36PRO controller. To add a new key, use the Add new button. Select the public key file and upload it to the controller. Each new key is associated with a currently logged user in the web server. Each user can be affiliated to a few keys with different names.

To learn more about the SSH connection, please see: SSH Management.

7.2.5 Settings

The Settings tab refers to the basic configuration options related to the web server's operation and security.

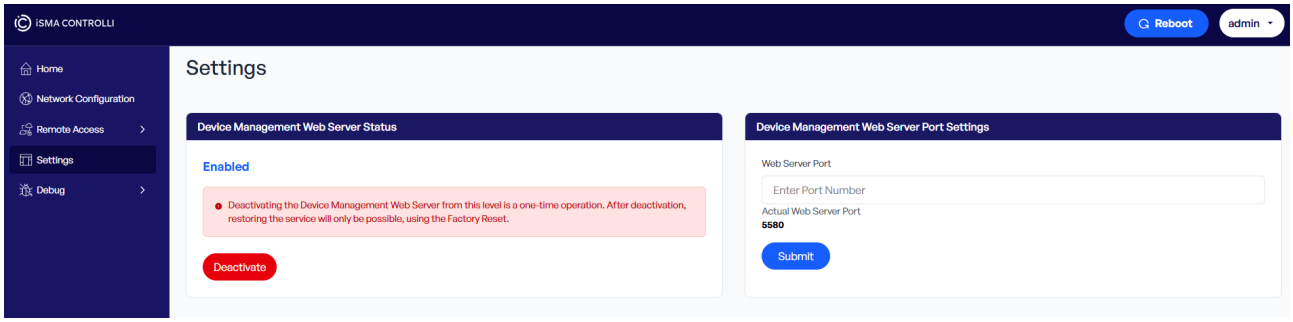


Figure 63. Device Management web server - settings

- Device Management Web Server Status:

For projects with increased security requirements, the Device Management web server can be **permanently** disabled after the commissioning process.

> Note
> Once disabled, the Device Management web server becomes inaccessible. The only way to re-enable the web server is a device **factory reset**.

- Device Management Web Server Port Settings:

The Device Management web server is configured to use TCP port 5580 by default for incoming HTTPS connections. This port can be changed in the Settings tab to comply with the site-specific security policies or avoid conflicts with other services.

> Note
> Once the port is changed, access to the web server must be done using the new port number in the URL format: https://[MAC36PRO_IP_ADDRESS]:[new_port]

To confirm changes, it is required to use the Submit button **and reboot the controller**.

7.2.6 Debug

Logs

The Logs tab allows to manage logs available for diagnostic and troubleshooting purposes.

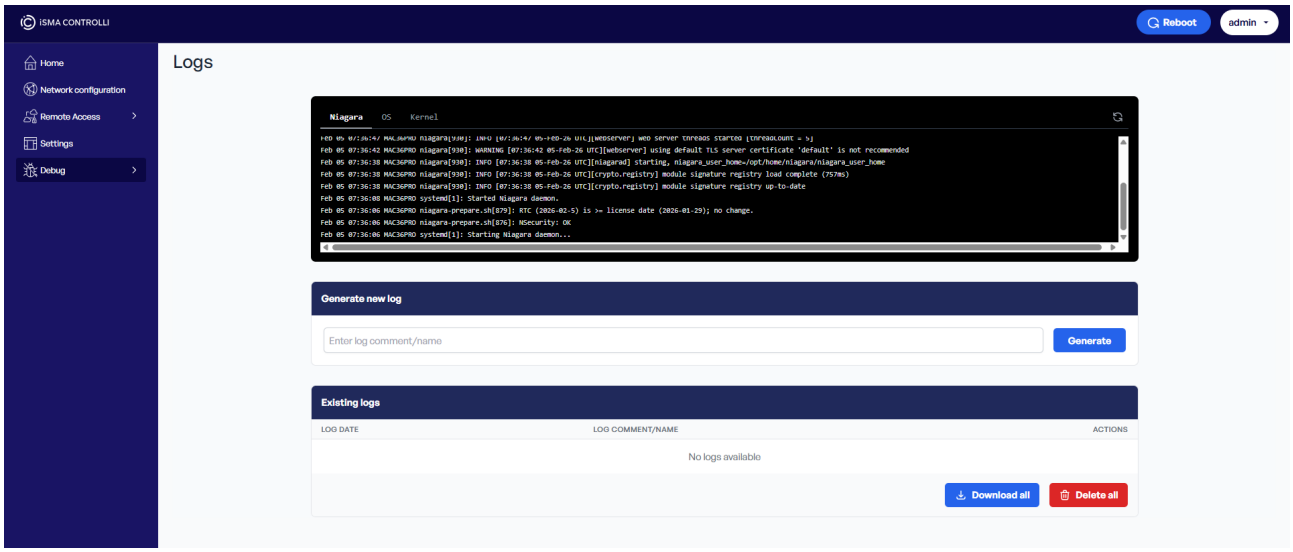


Figure 64. Debug - logs

The Logs section offers to download logs categorized in three groups:

- **Niagara:** logs from platform,
- **OS:** logs from any other applications/scripts executed on the MAC device,
- **Kernel:** more HW/FW related logs directly from the kernel of Linux OS.

These logs are downloaded only once, when the web server page is opened. To update logs, use the Refresh icon in the top right corner of the black logs section or refresh the whole page.

- **Generate new log:**

The Generate new log section allows to generate a new logs package. To this end, enter a name for the new logs file and use the Generate button.

> **Tip**
> For diagnostic purposes, the name of the logs package should be informative and include, for example, a reference to the targeted problem or status of the issue if it is possible to reproduce it.

- **Existing logs:**

Once the logs package has been generated, it becomes available to download in the Existing logs section. Use the Download option to download it to a specified location, or Delete to removed it.

> **Note**
> Please note that there is a limit of generated logs packages of 10 files. Once the 11th package is generated, the oldest package (1St) is removed.

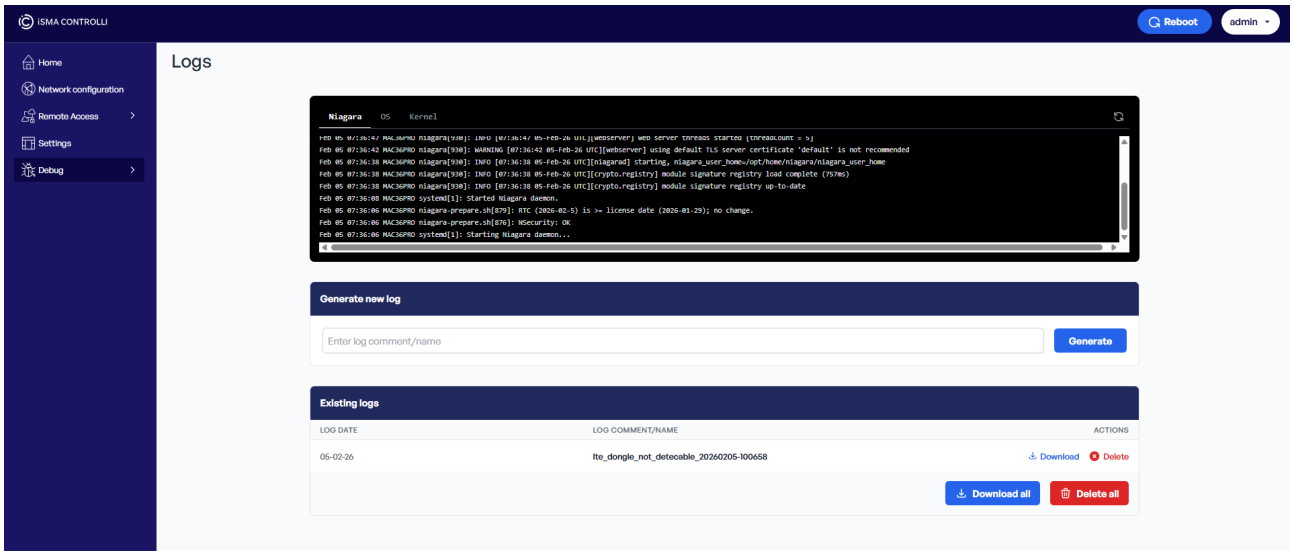


Figure 65. Debug - logs

To learn more about the logs functionality, please see: Logs Manager.

Ping

In the Device Management web server's tree, under Debug, the Ping tab is available. The Ping tab provides a basic utility for network troubleshooting by allowing users to send ICMP echo requests (ping) directly from the MAC36PRO network stack. It is especially useful for verifying the connection to devices on the OT network, such as IP Multiprotocol I/O modules, VAV14-IP, or RAC18-IP.

To ping the controller, a raw IP address must be entered in IPv4 address format. Domain names are not accepted.

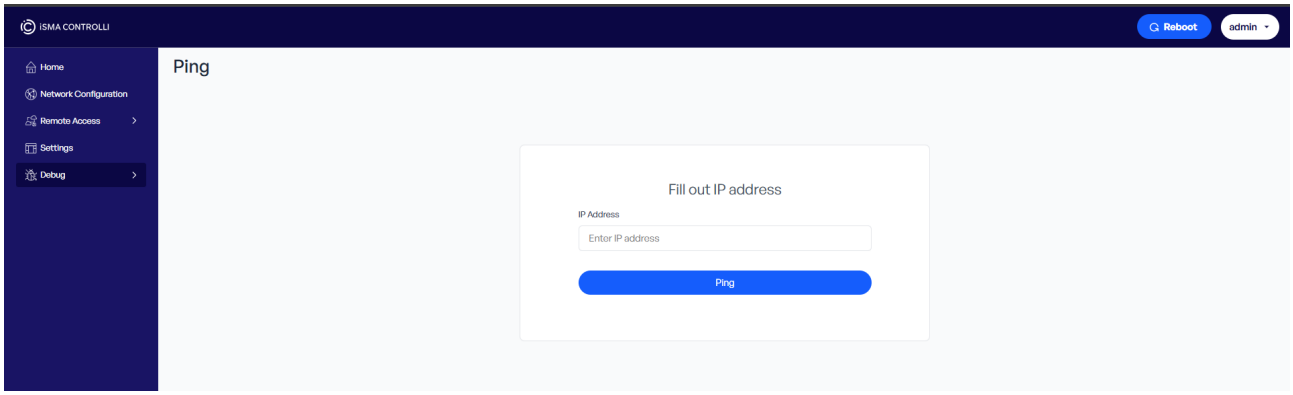


Figure 66. Debug - ping

SSH Super User

The SSH Super User tab allows to activate the SSH Super User access to the MAC36PRO controller.

> Warning
> Please note that the SSH Super User option is strictly reserved for access by the iSMA CONTROLLI Support Department and **must not be enabled without a direct request** from the iSMA CONTROLLI technical personnel.

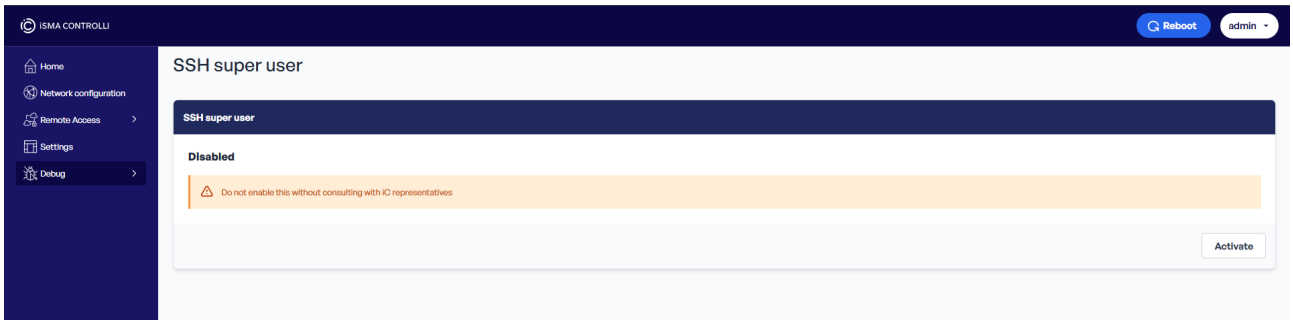


Figure 67. Debug - SSH Super User

To activate the root key for the SSH Super User access to the MAC36PRO controller. use the Activate button.

To learn more about the SSH Super User access, please see: SSH Management.

7.3 DHCP

The MAC36PRO supports a DHCP server functionality, enabling an automatic assignment of IP addresses and network parameters to devices within the local network, e.g., Multiprotocol I/O modules or Niagara-enabled controllers.

Note: This feature is available only in MAC36PRO controllers secondary Ethernet port, configurable in Niagara version 4.14 and up.

The DHCP server can be configured directly in the device Platform via the Niagara TCP/IP Configuration View or in the station, using PlatformServices>TcpIpService.

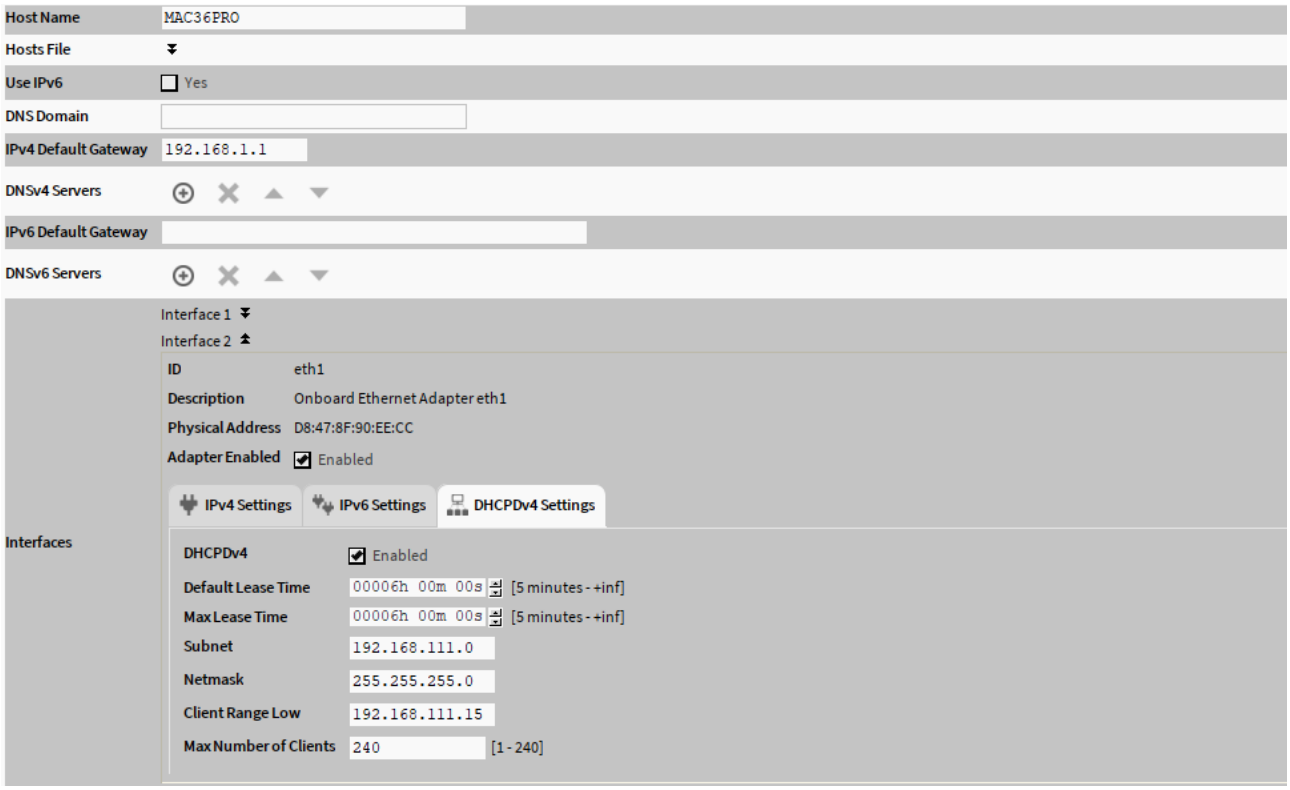


Figure 68. DHCP configuration

To set up the secondary interface as a DHCP server:

- Go to the Interface2 section and make sure that the Adapter Enabled and DHCPDv4 checkboxes are selected.
- Go to the DHCPDv4 Settings tab. Configure the properties:
  - **Default Lease Time:** allows to set a DHCP IP address lease; before this parameter expires, the lease must be renewed;
  - **Max Lease Time:** allows to set a maximum DHCP IP maximum address lease;
  - **Subnet:** allows to define a subnet of IP addresses assigned by the DHCP server; this parameter is required to assign addresses on a different subnet that the one used in other LAN or access point configurations; if the subnet is not configured, the ports will not function correctly;
  - **Netmask:** allows to define the IP addresses assigned by the DHCP server;
  - **Client Range Low:** allows to define the lowest IP address in the range; the order of assigning IP address from the access point is undetermined;
  - **Max Number of Clients:** allows to define a maximum number of clients that can connect.

Note
The adapter's IP address should be in the same subnet, but not in the range of addresses defined by the Client Range Low parameter.

- Go to the IPv4 Settings tab and enter the IPv4 address and subnet mask.

Note
Make sure that the secondary Ethernet port's (Interface 2) IP address is outside the DHCP server's client IP pool.

Confirm configuration with the Save button.

7.4 VPN Connection

VPN (Virtual Private Network) allows to extend a private network to other networks with an ability to isolate it. It allows remote users to access the network.

7.4.1 MAC36PRO VPN Client Connection

The MAC36PRO supports a connection to a WireGuard VPN network in a client mode. It enables to secure remote access to the controller through an encrypted tunnel. Once the VPN connection is established, the controller's web server, platform, and station can be accessed using the VPN IP address, providing complete remote control of the MAC36PRO controller.

Note
The MAC36PRO acts as a VPN client only. A separate WireGuard infrastructure is required to establish the WireGuard VPN connection with the controller.

7.4.2 Setting Up VPN Server

To configure a VPN server, basic networking knowledge is required, particularly in server administration, security best practices, and deployment contexts such as cloud or on-premises environments. Below are some best practices commonly applied when

configuring a VPN server; however, these should not be treated as guidelines, as the responsibility for correct configuration of the VPN environment lies solely with the VPN server administrator.

Initial requirements:
A Debian/Ubuntu-based server:
- with a physical access to Internet and an open port,
- possibly, a virtual machine (e.g., AWS Amazon, Microsoft Azure, Google Cloud),
- with a public IP address or ability to forward ports to DefGuard server.

Minimal required server parameters (for an instance of up to 20 devices; for bigger instances, the required parameters may be higher:
- 1 core,
- 1 GB RAM,
- 10 GB disk space.

Recommended VPN Servers

There are numerous VPN server solutions available on the market, open-source and subscribed. For the time being, for the MAC36PRO VPN connection, the following VPN servers are recommended:

- WireGuard VPN standard solution (open-source)

For VPN server setup instructions, please visit: WireGuard installation

- WireGuard server as a service

In addition to self-hosted deployments, WireGuard VPN servers can also be provided through commercial hosting services. These services typically offer Virtual Private Servers (VPS) with WireGuard pre-installed or available as a ready-to-use configuration, simplifying the deployment process. For example, some VPS providers offer pre-configured WireGuard environments that allow users to quickly deploy a VPN server without performing a full manual installation. One example of such a service is is*hosting: Dedicated Servers and VPS Hosting, which provides VPS instances that can be configured to run WireGuard VPN.

- DefGuard solution (subscribed)

For VPN server setup instructions, please visit: DefGuard installation

Note
iSMA CONTROLLI is not affiliated with, endorsed by, or associated with DefGuard, is*hosting, or WireGuard®. Any references to these products or services in this documentation are provided for illustrative and example purposes only.
The configuration examples presented were used during internal testing of a WireGuard-based VPN solution and are intended solely to demonstrate possible implementation approaches. The user is fully responsible for the deployment, configuration, maintenance, and security of any VPN server or related infrastructure used in their environment.

7.4.3 VPN Connecting to MAC36PRO

The MAC36PRO supports a connection to a WireGuard VPN network in a client mode. It enables to secure remote access to the controller through an encrypted tunnel. Once the VPN connection is established, the controller's web server, platform, and station can be accessed using the VPN IP address, providing complete remote control of the MAC36PRO controller.

To establish a VPN connection, a valid WireGuard configuration file (.conf) must be provided by the VPN server administrator. This is a standard file, which defines all necessary parameters including:

- interface private key,
- VPN server (peer) public key,
- client IP,
- VPN server IP (endpoint address),
- allowed IP ranges.

MAC36PRO AllowedIPs Limitation
Please note that the MAC36PRO implementation does not support full-tunnel configurations.
Using:

```
AllowedIPs = 0.0.0.0/0
```

is not supported and will not be accepted by the device configuration.
Instead, the **AllowedIPs** parameter must specify the VPN network or subnet that should be reachable through the tunnel. Only traffic destined for the defined VPN network will be routed through the WireGuard connection.
Example:

```
AllowedIPs = 10.20.40.0/24
```

This configuration allows the device to communicate only with hosts located within the VPN server network.
For more details, please see: MAC36PRO - VPN - WireGuard Configuration File Structure

To set up the WireGuard VPN Client, follow the three step process:

Step 1: Upload configuration
Add the .conf file provided by the VPN server administrator. Use the Choose File button to select the file and Upload button to send it.

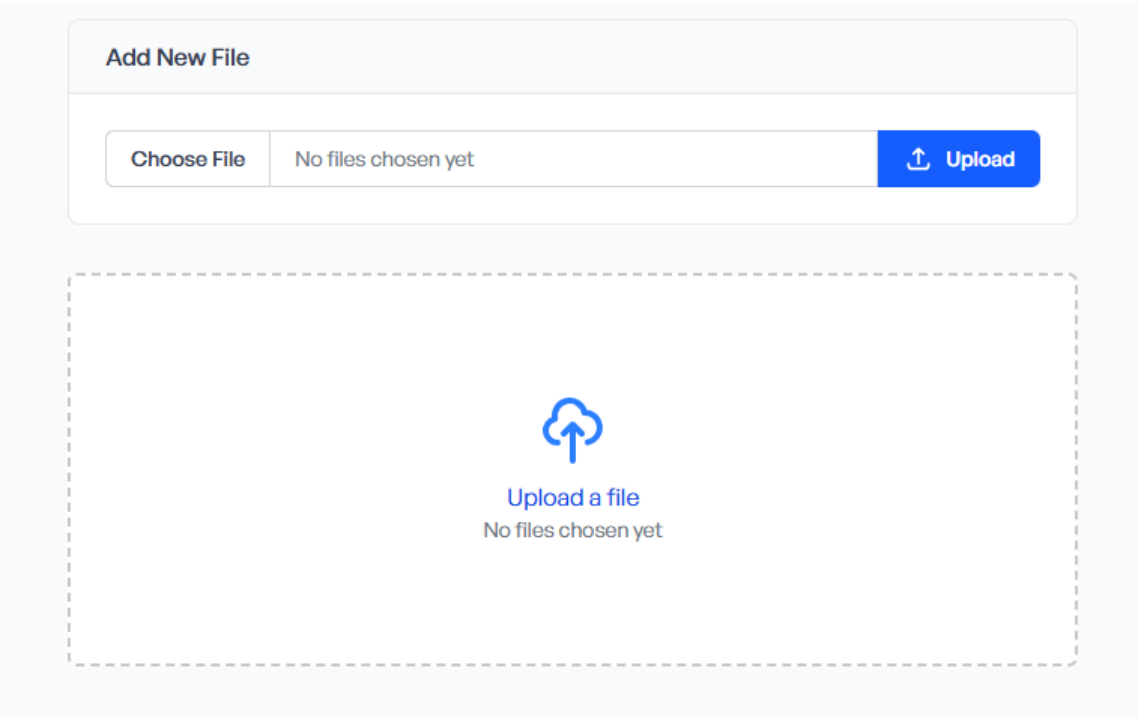


Figure 69. Upload configuration dialog window

Note
The upload window becomes available only if there is no previously uploaded VPN configuration currently on the device. If the configuration file has been uploaded, it must be removed first using the Delete button before uploading a new one.

Step 2: Activate the configuration

After uploading a configuration file, it is required to activate it in order to initiate the VPN connection.

Step 3: Controller reboot

A device restart is required to apply the changes and establish the connection with the WireGuard VPN server. Reboot can be initiated using the button in the top right corner of the web server.

A correctly configured VPN service will display information about the established connection to the WireGuard VPN server.

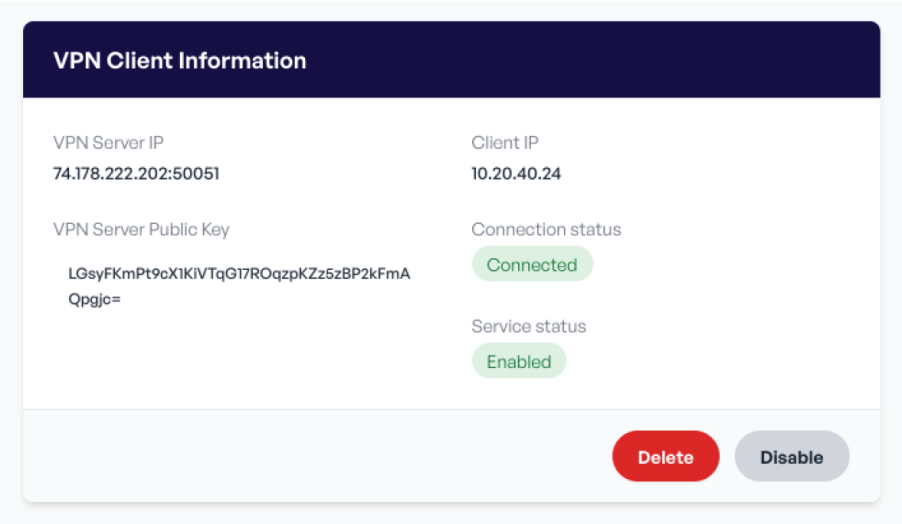


Figure 70. Established VPN connection

7.5 LTE Extension

The MAC36PRO controller can be remotely accessed with the LTE 4G cellular network, which allows for a full connectivity with the controller by a wireless connection. The solution enables maintaining a full functionality including programming and configuration with all advantages of the wireless transmission. LTE connection with the MAC36PRO controller is carried out with the use of the LTE-DIN-EXT-SET extension.

The LTE-DIN-EXT-SET set includes:

- LTE-USB-EXT: Onyx 4573326591584 LTE USB modem (SIM card not included) with a 1 m USB-A/A cable,
- LTE-ANT 698–2700 MHz: LTE antenna GA.130.201111 with a magnetic mount and CRC9-SMA-150 converter,
- LTE-DIN-ACC: accessories for USB-A DIN rail mounting including AN-25184 adapter and FX-USB/B Keystone
  module.

Note
Please note that it is strongly recommended to use the elements included in the set for connection, most importantly, the USB cable. The USB cable, which is seemingly easily replaceable, is essential for establishing a functioning connection, and the one included in the LTE-DIN-EXT-SET provides required parameters. USB cable replacements are likely to fail to provide, for example, proper data transferring parameters.
All technical details of the contents of the set is available in the datasheet: iSMA CONTROLLI Download Center - MAC36.

The LTE modem is connected to the MAC36PRO controller with a use of the USB cable, directly or through a USB hub with external power supply.

SIM Card
A SIM card **is not part of** the LTE extension set. However, the LTE extension for MAC36PRO supports a wide range of SIM cards available worldwide with the only requirement of providing an LTE 4G coverage. The supported SIM card type is 4FF (Nano SIM).

7.5.1 LTE Connection Security

When the MAC36PRO controller connects to the Internet using a USB LTE 4G dongle (LTE-DIN-EXT-SET), it takes advantage of the security features of modern cellular networks. However, once it connects to the public Internet, the device can still face common cyber threats, such as unauthorized access or data interception. To combat these risks, the device has a built-in VPN functionality. This allows all network traffic to be securely encrypted between the device and a trusted remote server.

Recommended Security Steps

- **Enable and configure the VPN.** Always use the device's VPN feature with strong encryption and trusted VPN endpoints to protect data in transit.
- **Keep Niagara version up to date** to fix known vulnerabilities.
- **Use strong authentication.** Change default passwords, use strong and unique credentials, and enable a certificate-based or key-based authentication where available.
- **Limit network exposure.** Disable unnecessary services and close unused ports to reduce the risk of attacks.
- **Physically secure the device and dongle.** Prevent an unauthorized physical access, as this could potentially lead to tampering or credential theft.

Combination of the cellular connectivity, VPN protection, and good security practices can greatly diminish the risk of cyber attacks and ensure a secure operation of the device in the field.

7.5.2 LTE Set Installation

The LTE extension can be mounted in two ways:

- using a DIN rail adapter included in the set and a direct USB cable connection,
- using a USB hub with external power supply **(USB hub is not included in the set)**.

Direct Installation on DIN Rail

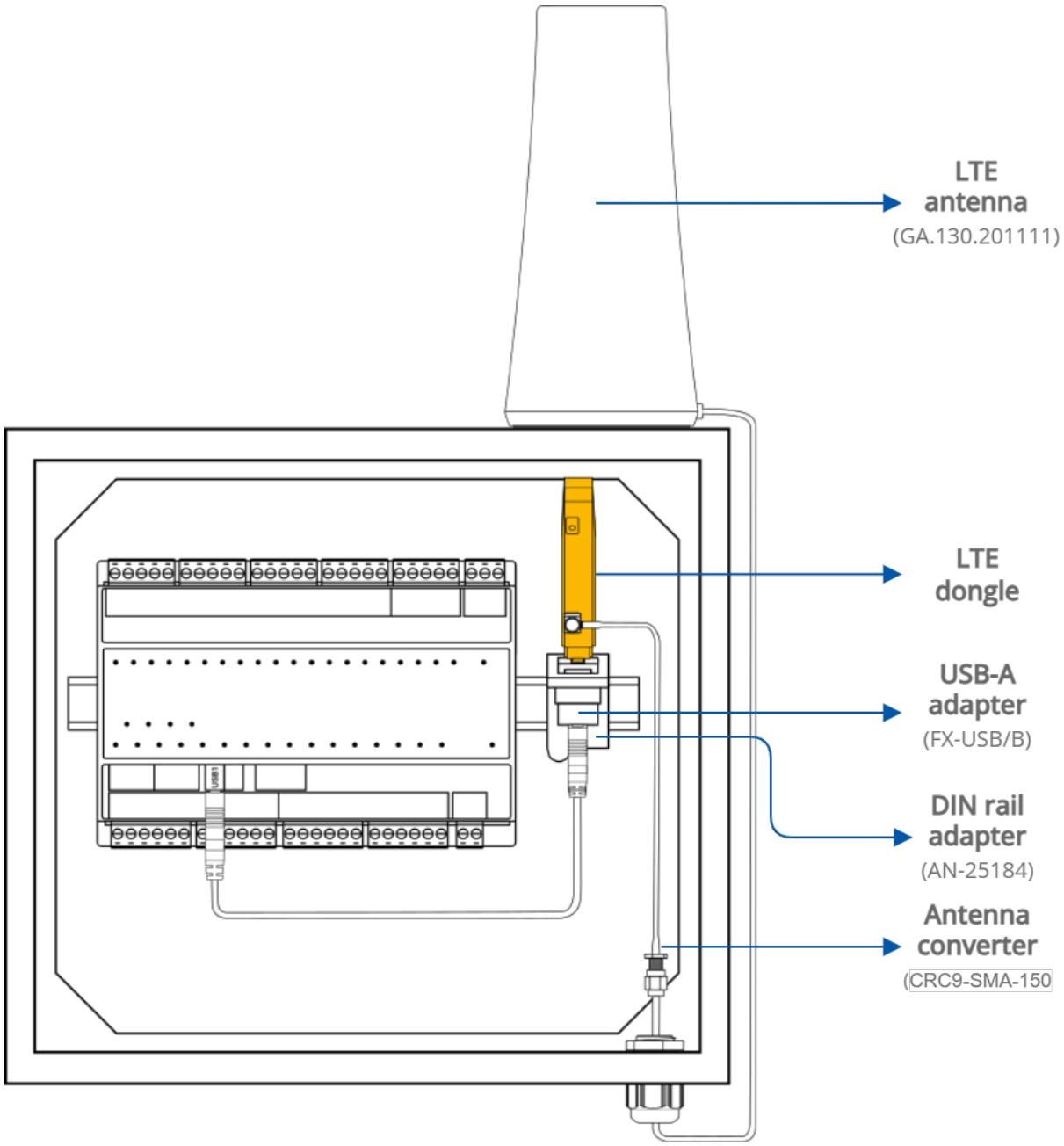


Figure 71. Elements of the LTE-DIN-EXT-SET installed directly on a DIN rail in a cabinet

A direct installation on the DIN rail involves the following actions

- mounting the DIN rail adapter,
- attaching the USB-A adapter on the DIN rail adapter,
- connecting the LTE dongle to the USB-A adapter and then directly to the MAC36PRO controller's USB1 port,
- connecting the LTE antenna to the LTE modem using the antenna converter,
- mounting the LTE antenna on the cabinet (magnetic mount for metal cabinets, double-sided tape for plastic cabinets),
- insert a SIM card to the LTE dongle (SIM card is not included in the set).

Installation with the USB Hub

USB Hub
Please note that the USB hub is not included in the LTE-DIN-EXT-SET.

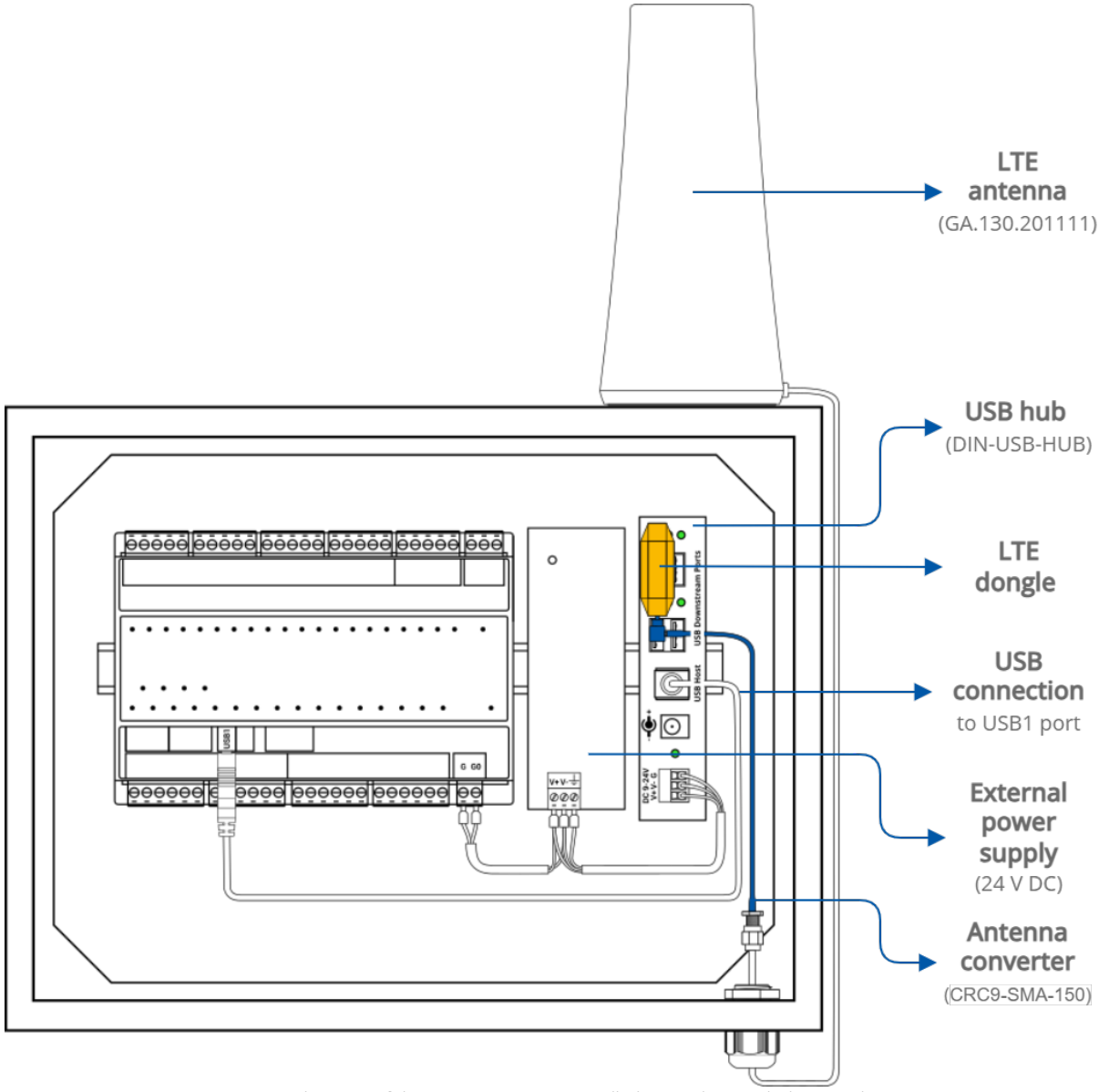


Figure 72. Elements of the LTE-DIN-EXT-SET installed using the USB hub in a cabinet

The installation with the use of the USB hub involves the following actions:

- mounting the external power supply on the DIN rail, connected to the MAC36PRO controller and the USB hub,
- mounting the USB hub on the DIN rail (or using mounting brackets),
- connecting the LTE dongle to the USB hub to any of the downstream USB ports,
- connecting the LTE antenna to the LTE modem using the antenna converter,
- mounting the LTE antenna on the cabinet (magnetic mount for metal cabinets, double-sided tape for plastic cabinets)
- connecting the USB host on the USB hub to the USB1 port on the MAC36PRO controller,
- insert a SIM card to the LTE dongle (SIM card is not included in the set).

7.5.3 LTE Configuration

Configuration of the LTE connection in the MAC36PRO controller is carried out in the Device Management Web Server.

Device Management Web Server
More details as to how to connect and log in to the web server are available here: Device Management Web Server.

SIM Card
An initial prerequisite for configuring the LTE connection on the MAC36PRO controller is inserting a SIM card.
A SIM card **is not part of** the LTE extension set. However, the LTE extension for MAC36PRO supports a wide range of SIM cards available worldwide with the only requirement of providing an LTE 4G coverage. The supported SIM card type is 4FF (Nano SIM).
The SIM card is very easily inserted into the LTE dongle. To open it, slide its cover to the side, remove it, insert the card, and replace the cover.

To start configuring the LTE connection, go to LTE Setting in the Device Management Web Server.

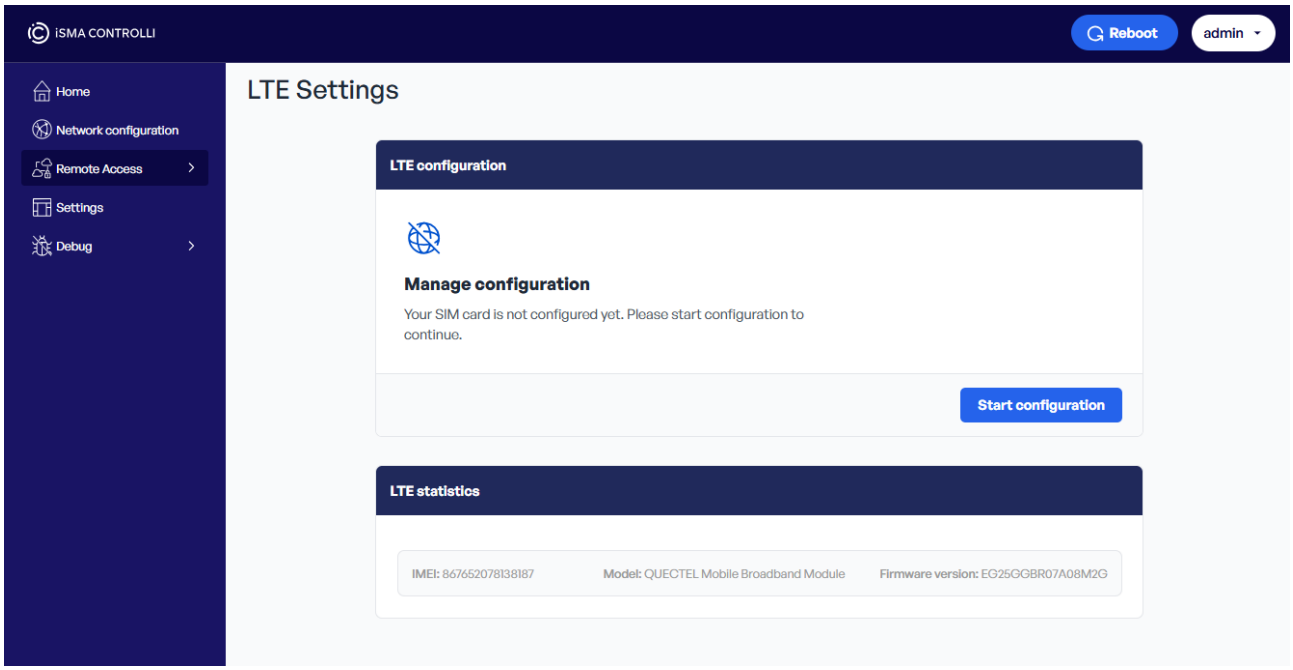


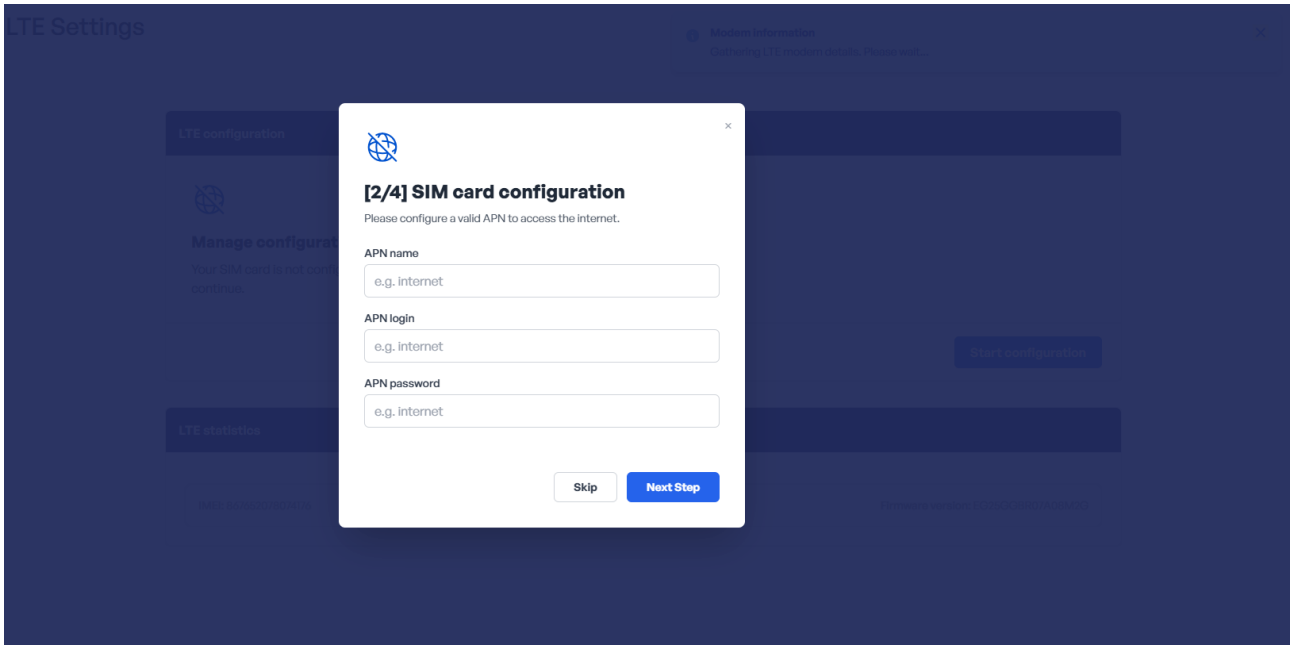
Figure 73. LTE settings

SIM Card Configuration

PIN

First - if required - enter the SIM card's PIN. This step is dependent on the SIM card and if there is no PIN protection, it will be omitted.

APN



Enter the APN (access point name) data provided by the SIM card supplier.

Public Access Configuration

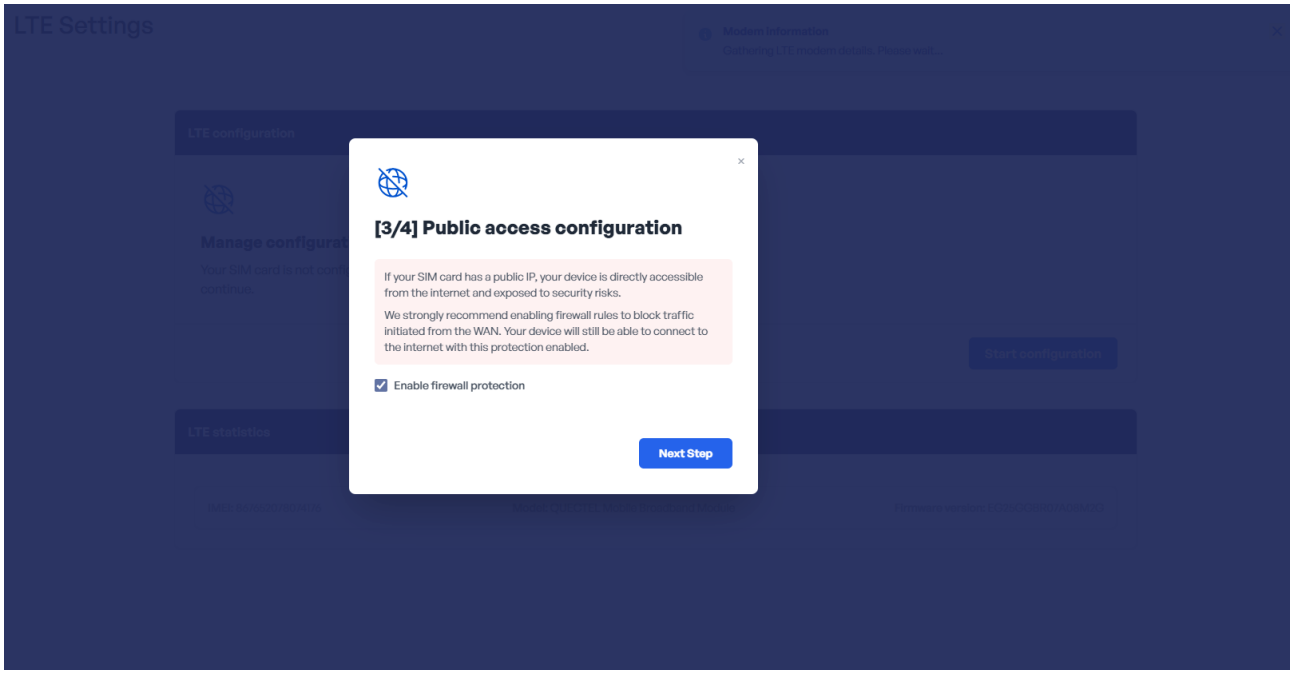


Figure 74. Firewall protection notification

The next step is a public access protection notification. It is strongly recommended to enable the protection due to security reasons.

Firewall protection mechanism

The firewall protection feature is enabled by default to ensure the device remains protected even when the SIM card is assigned to a public IP address by the LTE network operator.

When this protection is enabled, the device rejects all unsolicited inbound connections originating from the LTE network. This prevents external hosts from directly initiating connections to the device using its LTE-assigned IP address.

The firewall operates according to the following principle:

- If an external host initiates a connection to the device via the LTE interface, the connection is automatically rejected.
- If the device initiates the communication first, the corresponding return traffic is permitted as part of the established session.

This mechanism ensures that the device cannot be directly accessed from the public internet through the LTE interface while still allowing normal outbound communication.
This protection applies only to traffic entering through the LTE interface. Network traffic arriving through other interfaces, such as Ethernet (ETH) ports, or through secure Wireguard VPN tunnels, is not restricted by this feature and is processed according to the normal network configuration.
The feature provides an additional security layer for LTE deployments. For secure remote access, it is recommended to use a VPN connection together with the LTE connection rather than exposing services directly to the public internet.
The firewall setting must be configured during the LTE configuration process. If the firewall configuration needs to be changed or disabled later, the LTE connection must be recommissioned for the new setting to take effect.

Success

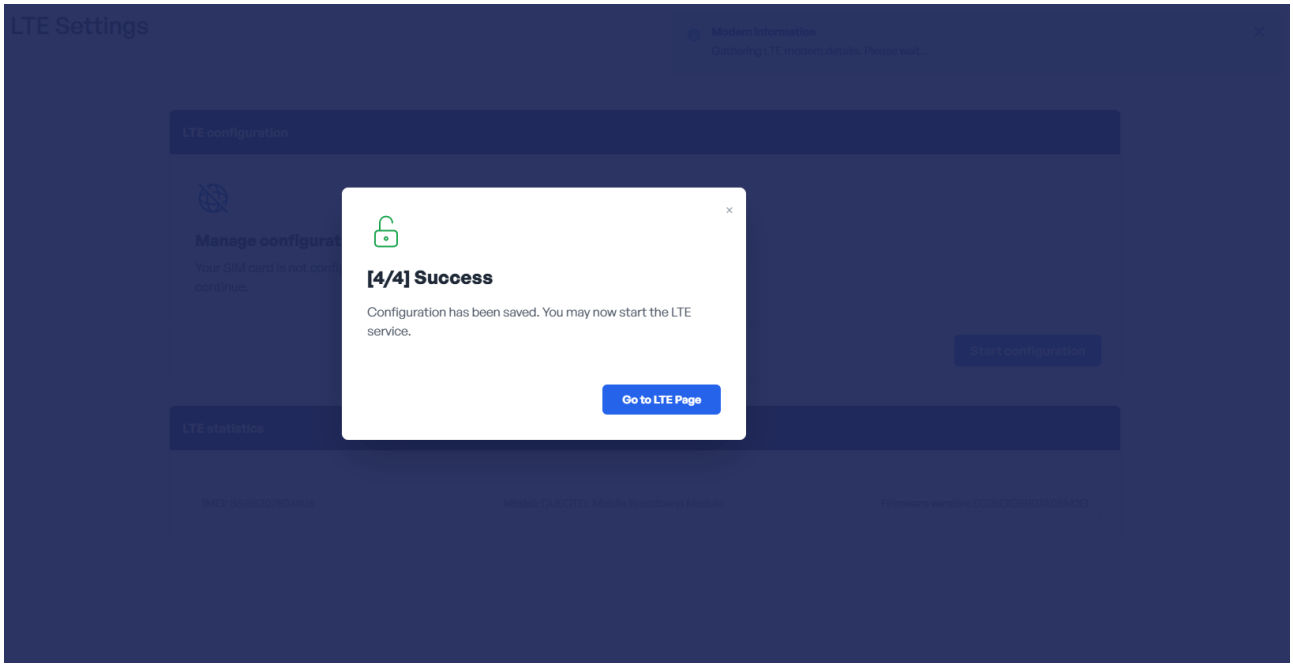


Figure 75. Success notification

A success notification is displayed upon a correct configuration of the SIM card.

Configuration removal

If required, it is possible to remove the SIM card configuration using the red button:

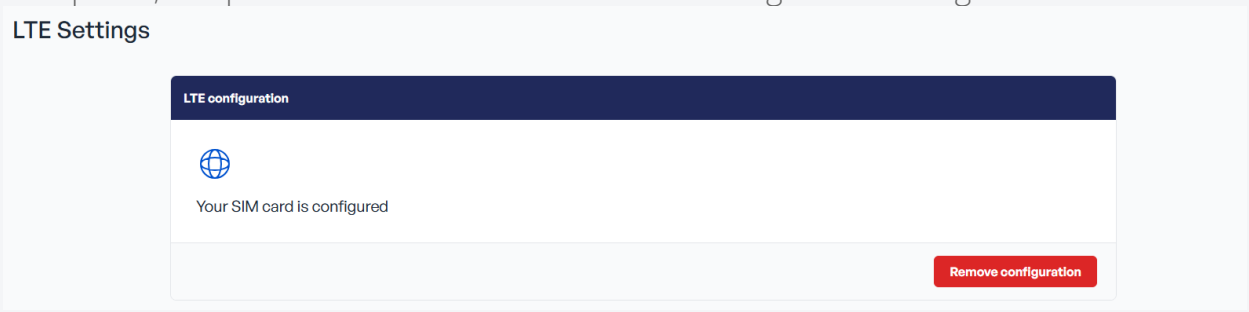


Figure 76. Remove configuration

The action will invoke a confirmation prompt. Once confirmed, the SIM card configuration will be deleted.

Reboot

After a first configuration of the SIM card, it is required to reboot the device.

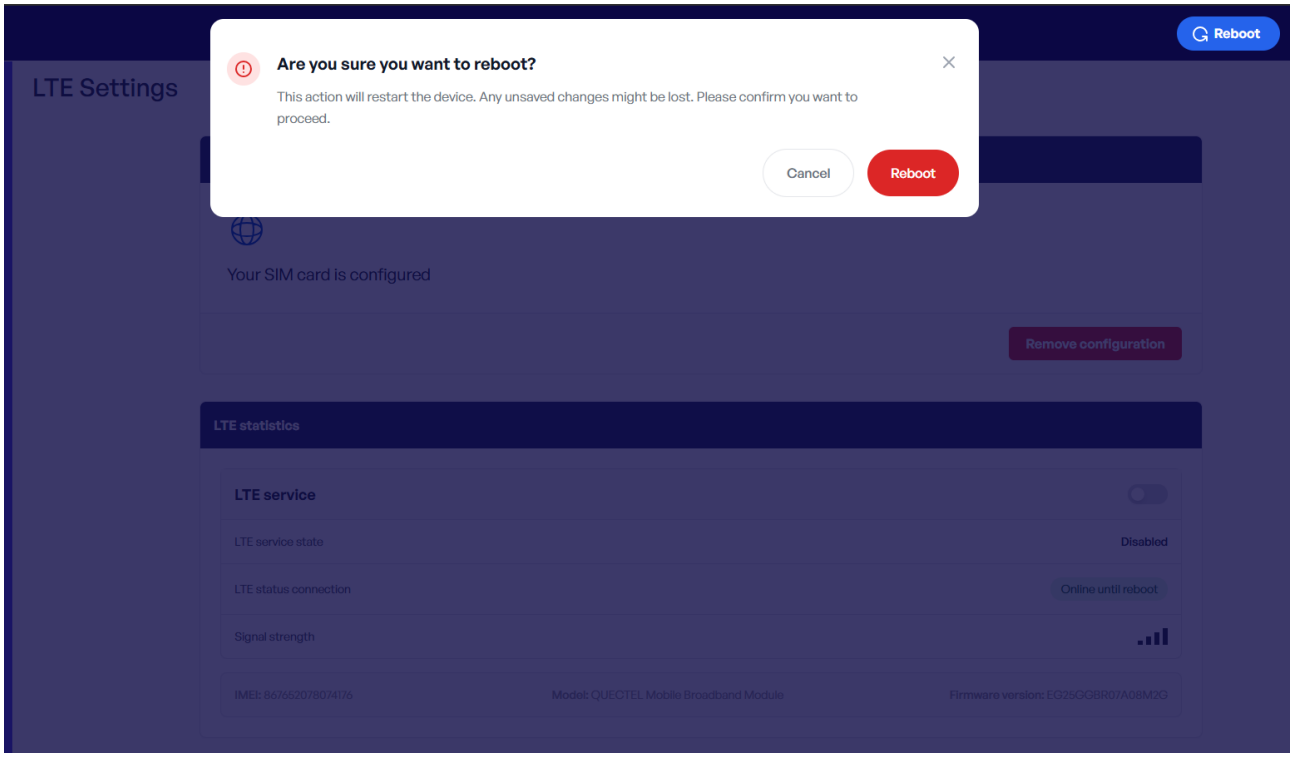


Figure 77. Reboot notice

Confirm the reboot notice. After the controller reboots, log again to the Device Management Web Server.

LTE Service

After the first reboot, it is required to enable the LTE service.

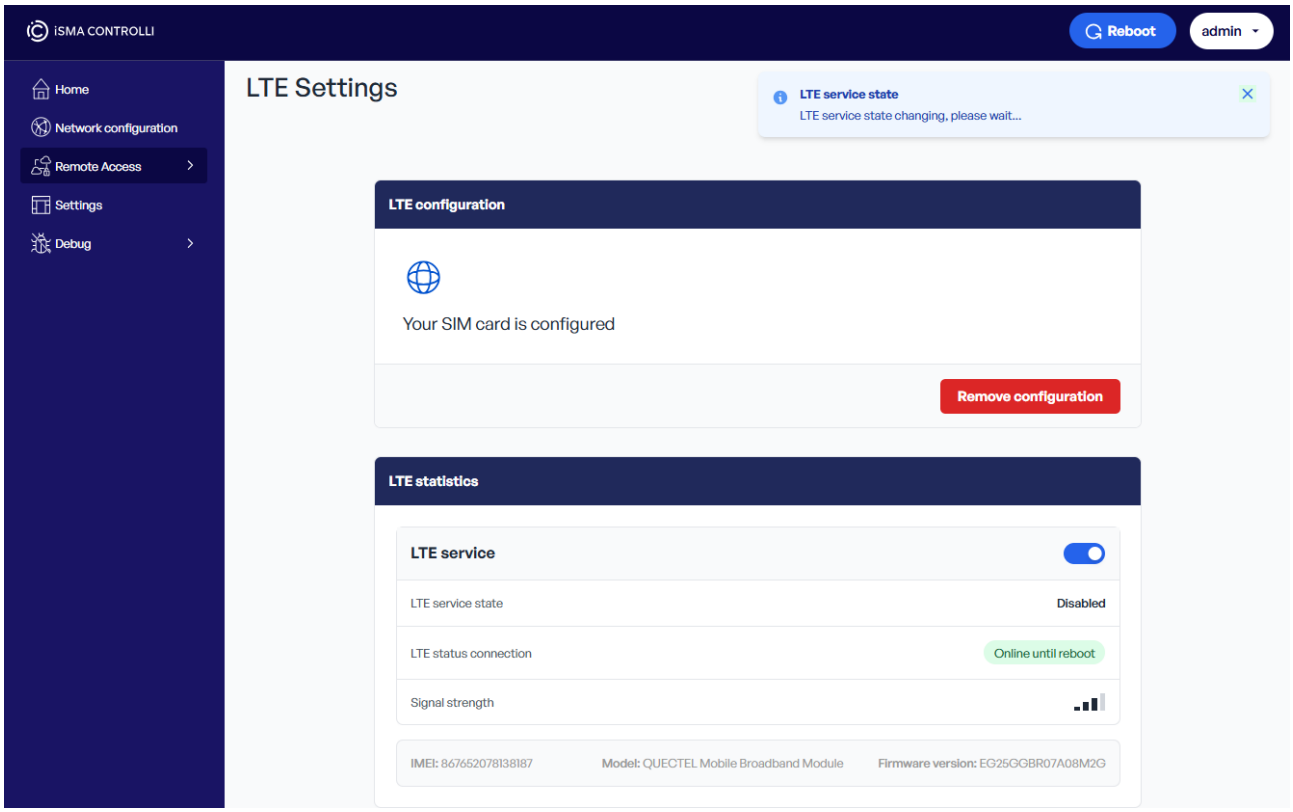


Figure 78. Enabling the LTE service

To enable the LTE service, toggle it to an active state. While in progress, the LTE service state notification will appear.

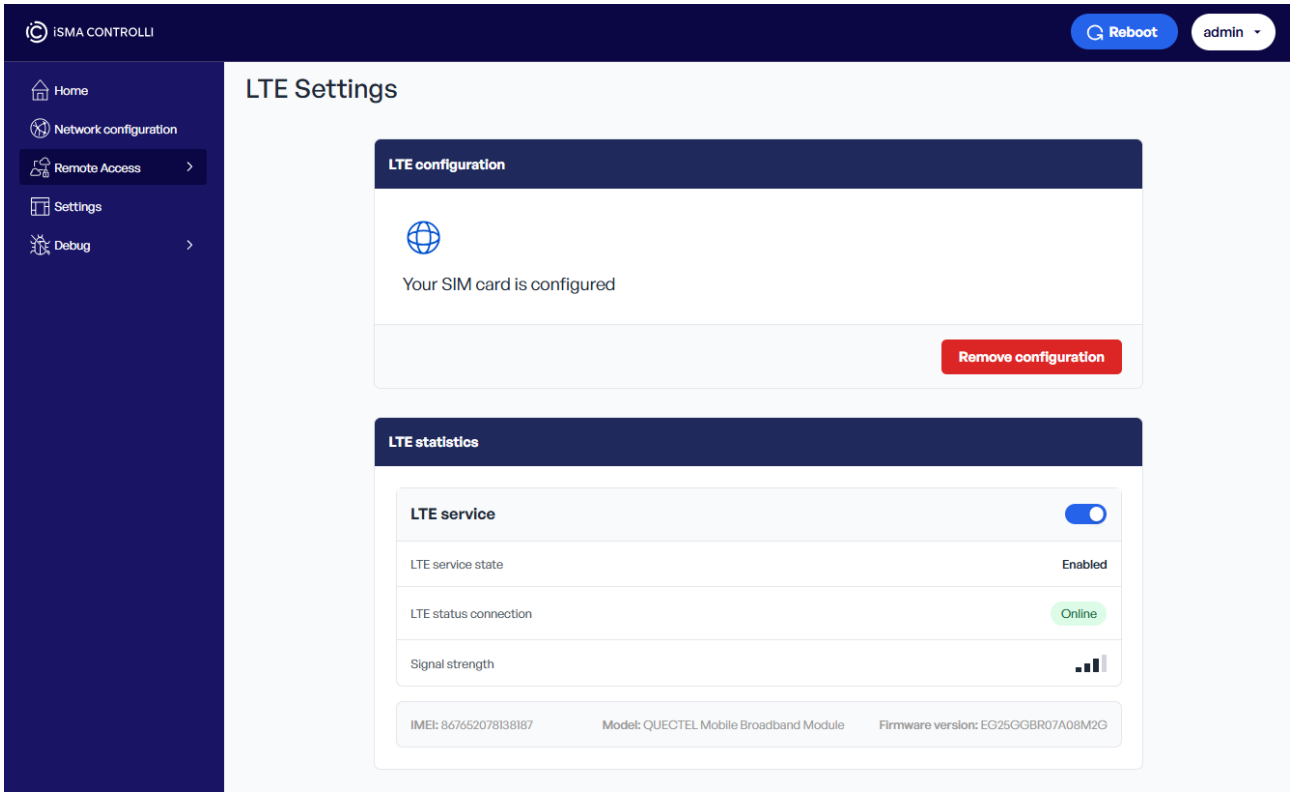


Figure 79. LTE service enabled

When updated, the following configuration appears:

- **LTE service:** toggle is in active state,
- **LTE service state:** enabled,

- LTE status connection: online,
- Signal strength: indicated.

Error

If, after reboot, the LTE service is enabled but the LTE service state shows an Error, toggle the LTE service again.

LTE Dongle not connected

If for any reason, the LTE dongle is not detected by the controller, a notification shows up:

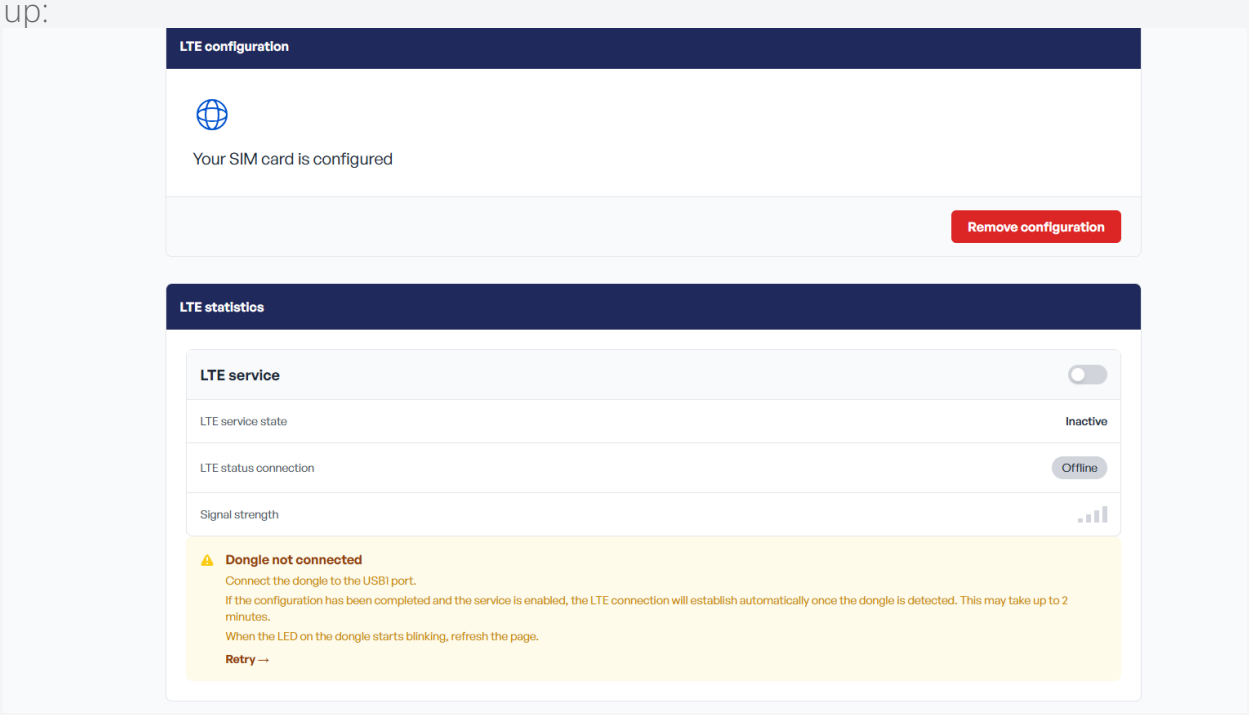


Figure 80. LTE dongle not connected

Make sure that the original USB/A-A cable has been used to connect the LTE dongle (directly or via the USB hub) to the controller. Make sure to enable the LTE service.

7.6 SSH Management

The SSH protocol allows for a secure, encrypted connection between two devices over an unsecured network. Such a remote secure connection allows to perform diagnostics and support operations and is a convenient method of a remote assistance.

In the MAC36PRO controller, it is possible to enable the SSH server for a remote access to a Linux console for diagnostic purposes. However, for security reasons, the SSH is by default disabled and has to be enabled when required to establish a secure connection.

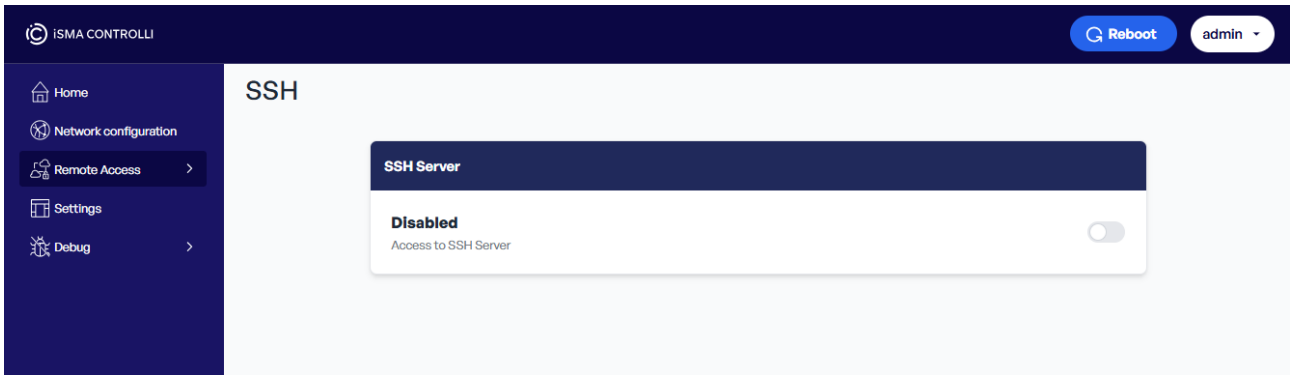


Figure 81. SSH server disabled by default

To establish an SSH connection, it is required to use a public/private key pair.

7.6.1 Generating SSH Public-Private Key Pair

From the public/private SSH key pair, a public SSH key is added to the MAC36PRO controller and a private key is used to authenticate a connection.

Cybersecurity
For security reasons, the SSH server is by default disabled in the MAC36PRO controller. Also, it is strongly recommended to keep the private key used for authentication secured from any unauthorized access.

Each new key is associated with a currently logged user in the web server. Each user can be affiliated to a few keys with different names.

Creating an SSH Public-Private Key Pair
There are numerous ways to generate a public-private SSH key pair, most of which are based on running an `ssh-keygen` command on the host.
For general reference, please visit the SSH Academy by SSH:
https://www.ssh.com/academy/ssh/keygen#creating-an-ssh-key-pair-for-user-authentication
Please see an example of a correct SSH public key:

```
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIBIcDqv8VY+KSHliX5YZDcqz7lwCipOw2PUul5G+hyD9
```

7.6.2 Adding SSH Key in the Device Management Web Server

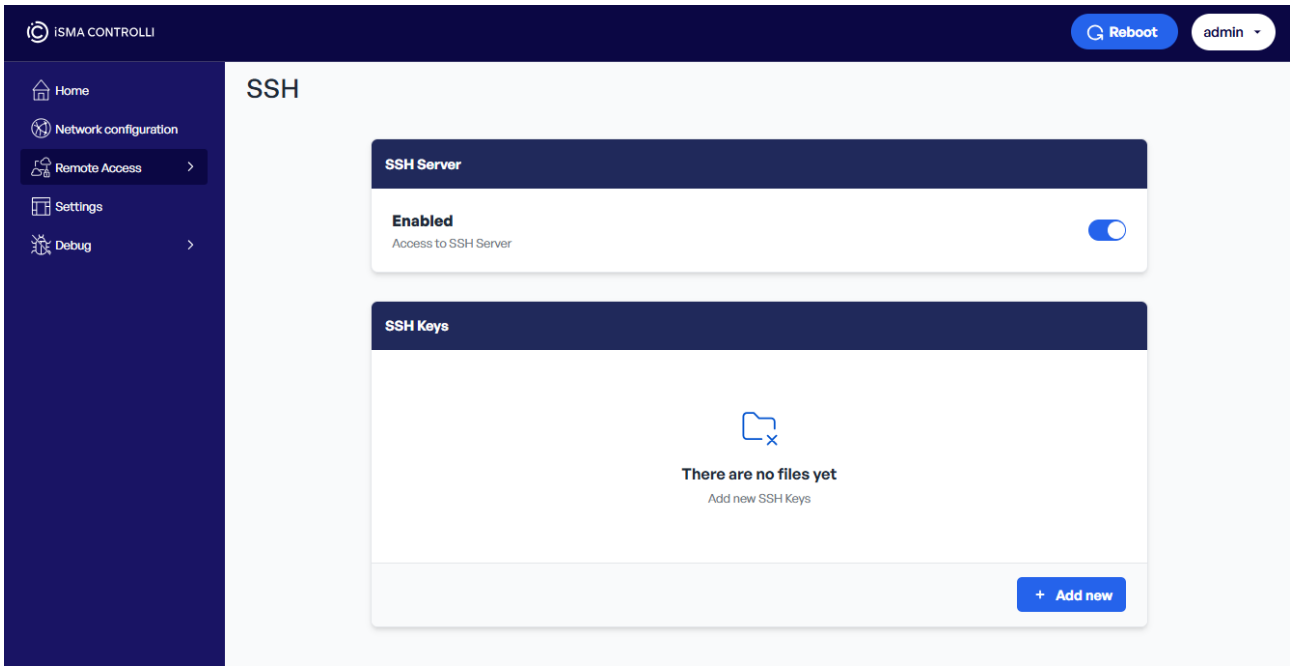


Figure 82. SSH server enabled

For the SSH connection, it is required to add the SSH public key to the MAC36PRO controller. To this end, go to the Device Management Web Server, then to Remote Access, and select the SSH tab. Once the SSH server is enabled, go to the SSH Key section and use the Add new button to upload the SSH public key file.

> Note
> Once the public key is added to the MAC36PRO controller, there is no specific way recommended to further establish the SSH connection. Any SSH client program can be used to establish such connection, for example, the PuTTY SSH client program.

7.6.3 SSH Super User Access for iSMA CONTROLLI Support

> Warning
> Please note that the SSH Super User option is strictly reserved for access by the iSMA CONTROLLI Support Department and **must not be enabled without a direct request** from the iSMA CONTROLLI technical personnel.

Apart from the standard SSH connection with the MAC36PRO controller, which is based on the SSH public/private key pair, there is also a possibility of enabling the SSH Super User access that is **designed only for the iSMA CONTROLLI Support Department** and allows for an advanced troubleshooting of a particular controller. The SSH Super User access is based on a root key for connection.

To enable the SSH Super User connection for the iSMA CONTROLLI support, it is required to enable the root key, which can be activated by the platform administrator in the Device Management Web Server in the Debug section, in the SSH Super User tab. Enabling this option activates the root key.

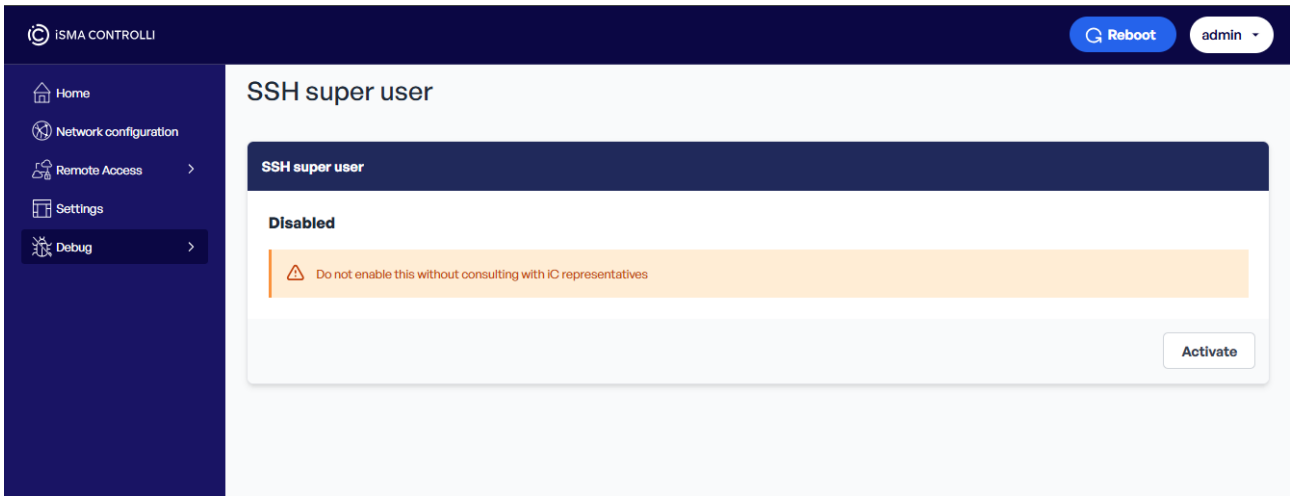


Figure 83. SSH Super User access activation

When the root key is activated, the iSMA CONTROLLI team will have a full access to the MAC36PRO controller provided the following conditions:

- the SSH server is enabled,
- the controller is available in the network (by Internet or VPN access),
- the SSH port is not blocked,
- the IP address of the controller is provided to the iSMA CONTROLLI team.

Such connection will be used only for emergency situations when there is no other way for the Support Department to solve the issue and available logs are not enough to diagnose it.

7.7 Logs Manager

The Logs functionality, accessible in the Device Management Web Server, offers a debug possibility by gathering all of required logs and diagnostic data for troubleshooting. In problematic situations, such as when a station is not starting or it breaks the connection, logs are a convenient tool for the iSMA CONTROLLI Support Department to perform diagnostics and expedite the troubleshooting process.

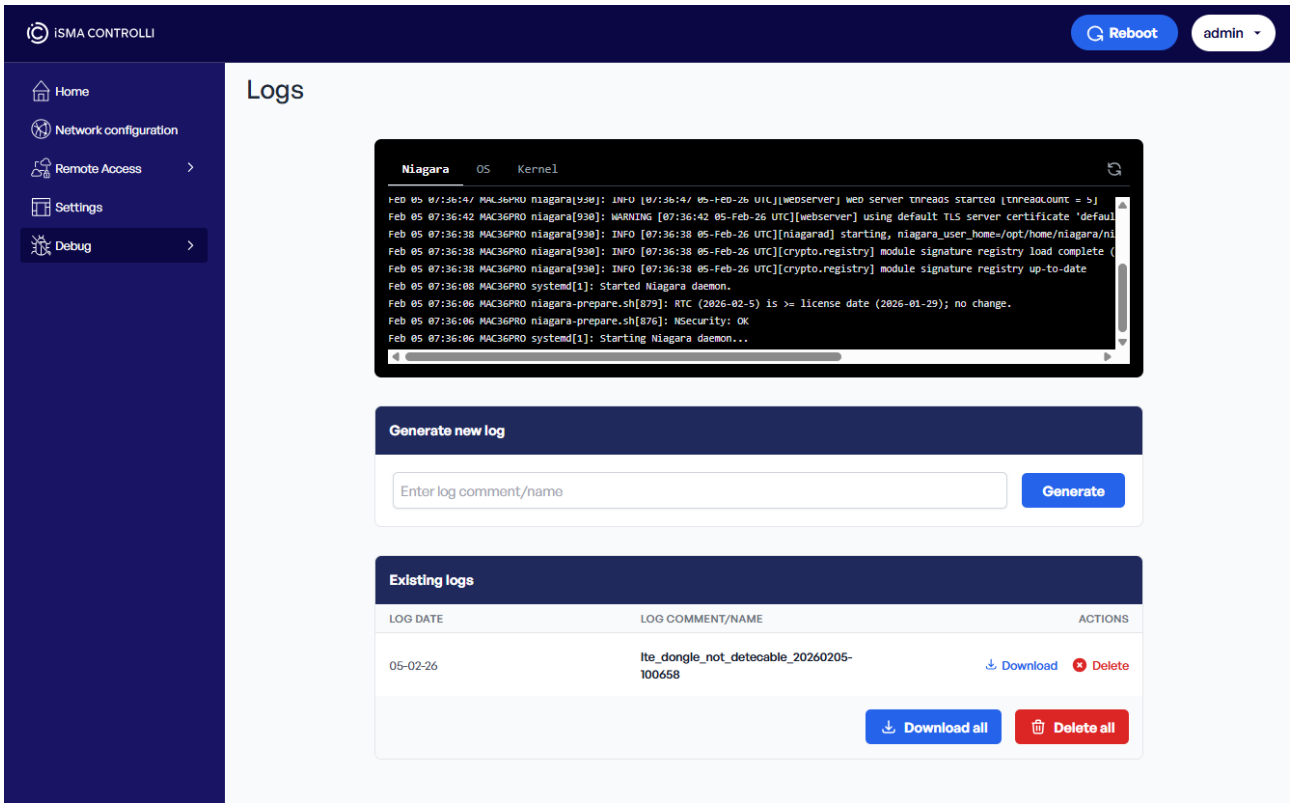


Figure 84. Logs section in the Device Management Web Server

The logs available for preview are categorized into three groups:

- **Niagara:** logs from platform,
- **OS:** logs from any other applications/scripts executed on the MAC device,
- **Kernel:** more HW/FW related logs directly from the kernel of Linux OS.

These logs are downloaded only once, when the web server page is opened. It is possible to refresh them with a Refresh icon or by reloading the web server page.

> To learn more about the logs functionality in the Device Management Web Server, please see: Device Management Web Server.

7.7.1 Logs Packages

Logs packages are a convenient way to provide data for diagnostic purposes. The logs package contains logs and other diagnostic data such as RAM and disk usage, running processes, etc., which is more than the preview displayed in the logs tab of the Device Management Web Server. Such a package is easily generated in the Device Management Web Server, in the Debug section, Logs. Logs package is not encrypted and the user can review it before submitting it to the support department.

For clarity, it is recommended to name a log package indicating the issue: for example, `lte_dongle_cannot_be_detected_<timestamp>.tar.gz`. The name should be informative, clearly indicate the problem, and possibly differentiate before/after scenarios if it is possible to reproduce the issue.

Note

Please note that there is a limit of generated logs packages of 10 files. Once the 11th package is generated, the oldest package (1St) is removed.