RAMOS Micro

MONITOROVACÍ ZAŘÍZENÍ / ÜBERWACHUNGSGERÄT /
MONITORING DEVICE / DISPOSITIF DE SURVEILLANCE /
УСТРОЙСТВО МОНИТОРИНГА

NÁVOD K OBSLUZE A ÚDRŽBĚ > **CZ**

MONTAGE- UND BETRIEBSANLEITUNG > **DE**

ASSEMBLY AND OPERATING MANUAL > **EN**

MANUEL D'ASSEMBLAGE ET D'UTILISATION > **FR**

ИНСТРУКЦИЯ ПО СБОРКЕ И ЭКСПЛУАТАЦИИ > **RU**

CONTEG

Safety warning

The device has been tested and is in good working condition, meeting the standards required in the Czech Republic.

To keep it working properly, it's important to follow the safety and maintenance guidelines listed below. If the device is used improperly, it may not work safely.

Also, make sure that the power socket or the point where the device can be unplugged from the power supply is easy to reach.

Do not use the device if:

- It looks damaged
- It's not working properly
- There are loose parts inside
- It was exposed to moisture or water for a long time
- Someone who is not authorized tried to repair it
- The power adapter or its cable looks damaged
- You're using the device in a way that's not recommended, which may compromise its safety features
- The switch, fuse, and other power surge protection features must be part of the device's overall construction.

The manufacturer is only responsible for the device if it's being powered by an approved or supplied power source.

Obsah

RAMOS Micro

RAMOS Micro is a reliable environmental monitoring solution for remote locations. Email alerts and SNMP monitoring service available.

RAMOS Micro is a reliable LAN & WiFi remote sensor monitoring product. External sensors for 2× RJ11 ports & detectors to 2× DI (Digital Input).

Whenever a too high or too low temperature is detected (door opened), an Alert is sent. Alerts (Emails) can be sent directly from the device (SMTP) or via the GSM gateway (SMS and ring-out alerts).

RAMOS Micro can send alerts via an external SMS gateway (on the same network). With or without the Portal, the HWg monitor (iOS/Android mobile application) displays current sensor values.

Additional sensors can be connected to a second RJ11 sensor port (%RH, temperatures, CO2, VoC, water flooding, …). RJ11 sensors can be daisy chained or one physical sensor can measure multiple values (°C + %RH + VoC = 3 values).

Device package contains 3m RJ11 temperature sensor. Device is powered by PoE. Wall plug power adapter 5V is possible to order as option.

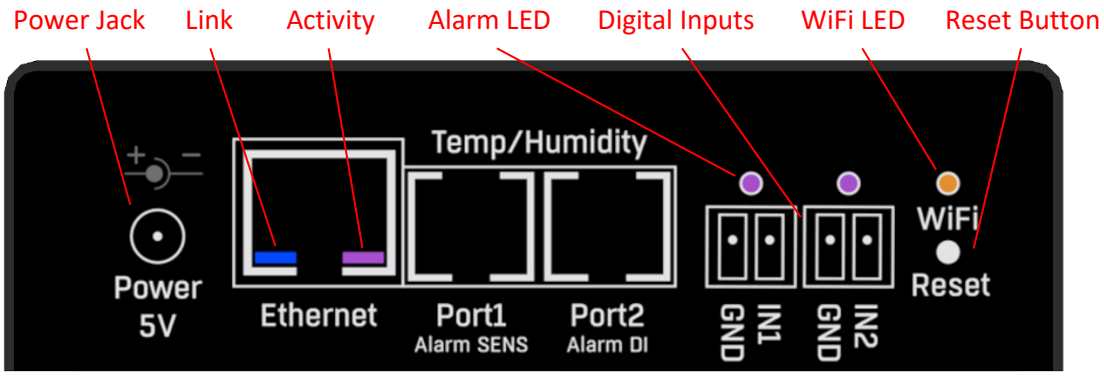
Basic features

- The device supports LAN and WiFi connections via 802.11 b/g/n (2.4 GHz).
- It supports Ethernet and WiFi operation for easy configuration.
- The device can be powered by 5V (external power adaptor) or PoE.
- The device comes with a built-in WEB server that supports HTTPS.
  Standard Internet browser is enough for configuration.
- Open API: It can be connected to higher-level monitoring systems via XML or SNMP.
- The device can handle HTTP and HTTPS traffic simultaneously, with the option to disable one or both protocols for security reasons.
- If the sensor value (temperature) goes out of Safe Range, the device can send an email as an alert.
- The device supports TLS authorization (Gmail…) and is password protected.

Application

- **AC (Air Conditioning) failure** - Changes in temperature alert you of the A/C cooling unit outages.
- **Heating monitoring** - Remote monitoring of the heating system, email or SMS alerts of freezing hazards.
- **Refrigerator or freezer monitoring** - Sends an email when your refrigerator fails. Logging of operating and storage conditions.
- **Heating optimization** - Save on heating and air conditioning costs.
- **Food storage** - Monitors optimal storage conditions.

Connectors and wiring



- **Ethernet** - LAN connectivity, default configuration also for WiFi connectivity.
- **2x RJ11 (Temp/Humidity)** - External RJ11 sensors from Conteg.
  - Each port is max. 60m.
  - One physical sensor can provide several sensor values.
  - Temperature & Humidity sensor provides 2 sensor values.
  - Sensor values limit is for both RJ11 ports together.
- **Power** - 5V power supply (external adapter).

Indication

- **Digital Inputs** - Lighting when DI = 1(On).
- **Link** - A yellow LED signalizes connectivity to the computer network.
- **Activity** - A green flashing LED signalizes ongoing communication.
- **WiFi** - A blue LED signalizes connection to the WiFi AP.
- **Alarm LED** - Two LEDs hidden in the Port1 and Port2 connectors.
  - **Alarm SENS** - LED signal Alarm state on any of sensors.
  - **Alarm DI** - LED signal Alarm state on one of DI (Digital Input).

Button

- **Reset** - serves to restore factory settings on the device.
  - Switch the device off.
  - Press and hold the button.
  - Switch the device on and press the button for another 5 seconds.
  - All the LEDs will gradually light up.
  - Restart the device. Factory settings will be restored.

Technical parameters	
Ethernet	10/100Mbit
WiFi	IEEE 802.11bgn
SNMP	v1
DHCP	YES
HTTP	YES
HTTPS	YES
XML	YES
SMTP	YES
SMTP TLS	YES
Net-GSM (SMS GW)	YES
1-Wire sensor values	Max. 5
1-Wire UNI	YES
DI (Digital Inputs)	2
Email destinations	5
SMS destinations	5
Power supply	5V / 300 mA
Connector	Jack (barrel, inner 1.35 mm outer 3.5 mm)
PoE	YES
PoE current	60 mA
PoE class	IEEE 802.3af Class 0
Operating / Storage	-30°C to 60°C 0% RH to 95% RH
Weight	91 g
Dimensions	98x68x33 mm
Environment	SoHo, IT
Installation	DIN, Table, Wall
Protection	IP40

First Startup

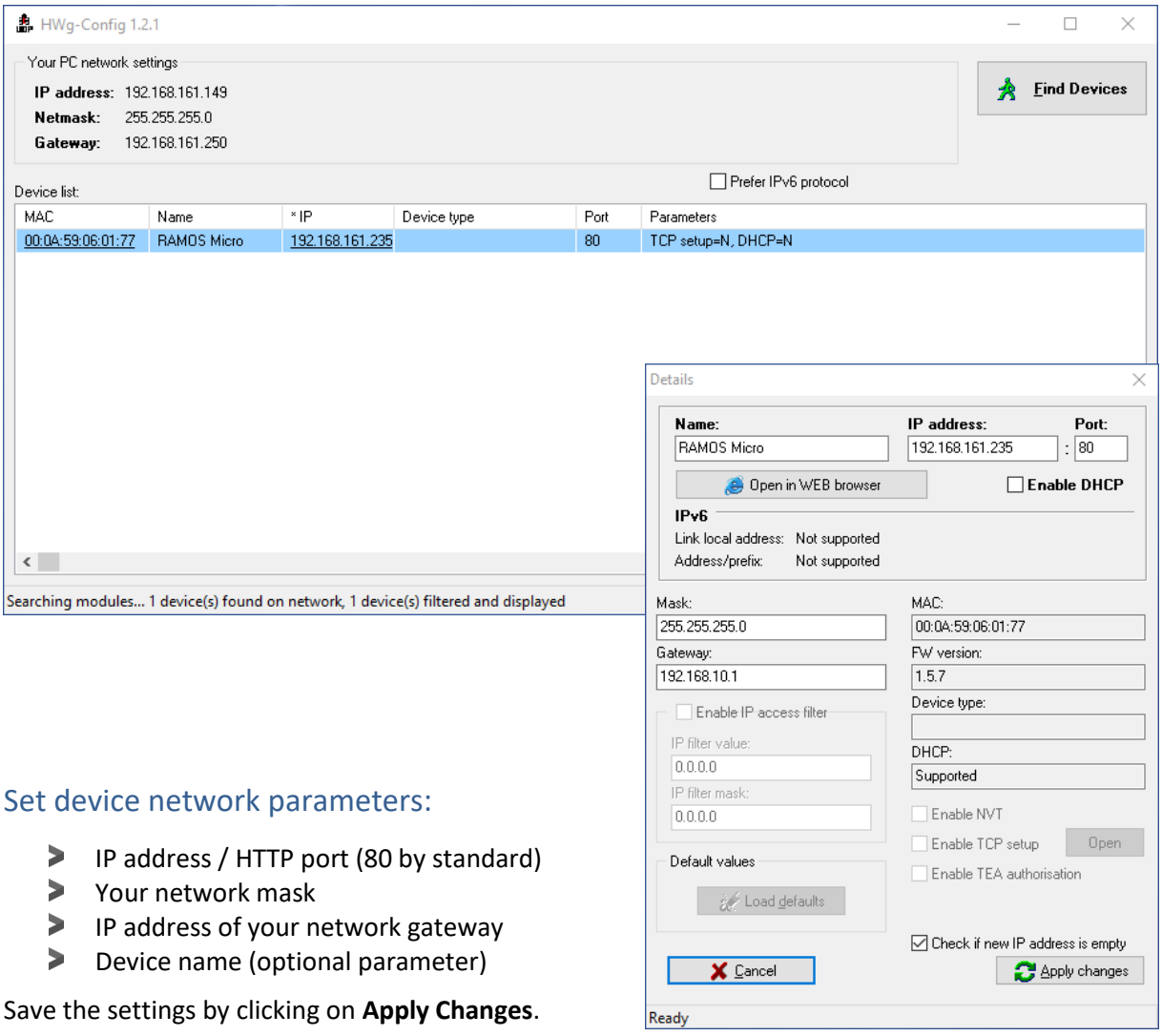
Cable connection

- Connect the device to the **Ethernet** (direct cable to the switch, crossed to PC).
- Connect the power adapter to the power grid and to the device (if not using PoE switch or Injector)
- If the Ethernet connection is OK, the **LINK (yellow)** light should come up a moment later. The **ACTIVITY light (green)** indicates Ethernet activity.
- The **LINK (yellow)** flashes rapidly to indicate communication with the DHCP server.

The setting of the IP address - RMS-Config

The **RMS-Config** program for MS Windows can be downloaded at :

- Launch RMS-Config, program automatically searches for LAN connected devices.
- If the device is connected later, click the Find Devices button. Local network devices will be listed. Click on the MAC address of the device to open the dialogue window for device settings.



Set device network parameters:

- IP address / HTTP port (80 by standard)
- Your network mask
- IP address of your network gateway
- Device name (optional parameter)

Save the settings by clicking on **Apply Changes**.

Note: The device provides 2 options how to restore its default settings:

1) Right-click on the device's MAC address. Click on the Load default values item.

Note: Device default values can be restored from the RMS-Config program only during the first 60 seconds after the device is powered up.

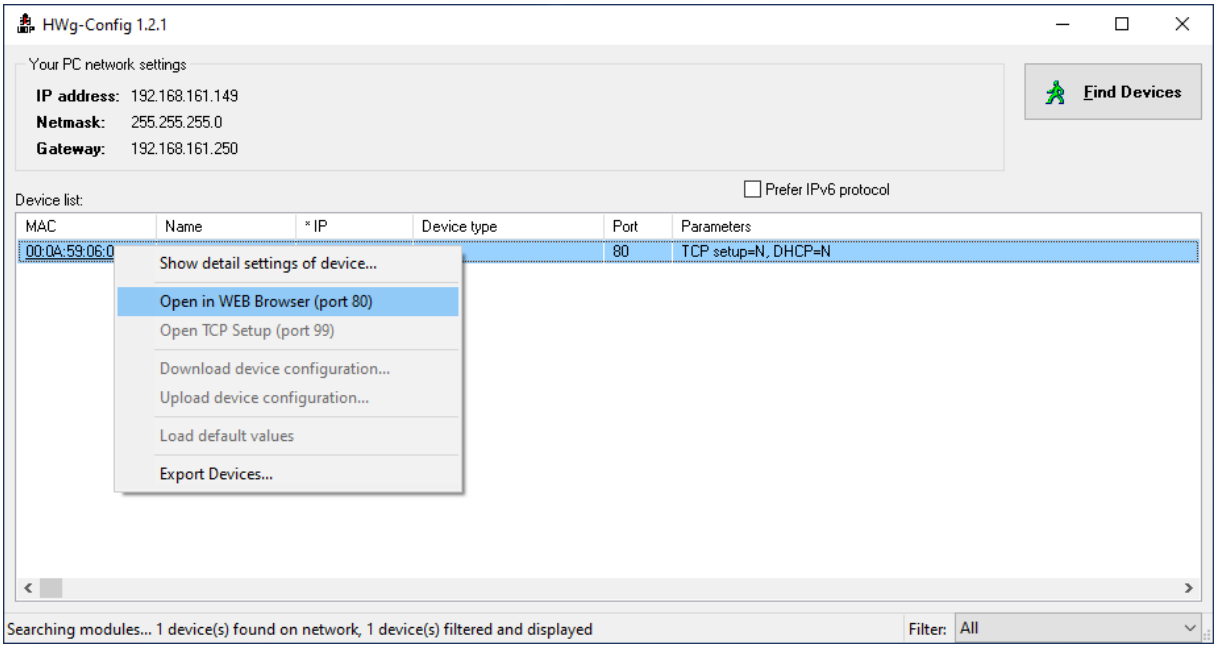
2) Switch off the device. Press the RESET button on the device, hold it down and connect the device power source (power adaptor). Hold the button down for another 5 seconds until all the LEDs light up.

How to open the device website

1) Enter the device IP address in your web browser if you know it.

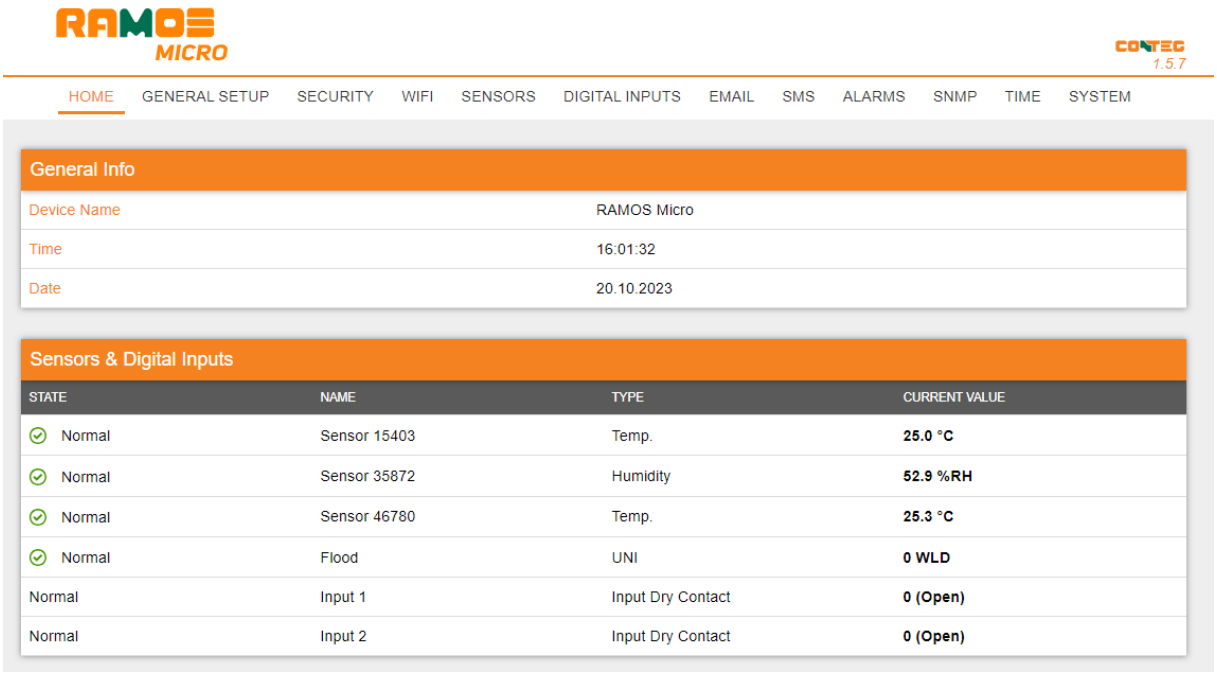
2) Use right-click on device in the RMS-Config program. Select Open in WEB Browser.

3) Click on the underlined IP address in the RMS-Config program.



WWW Interface

Home tab



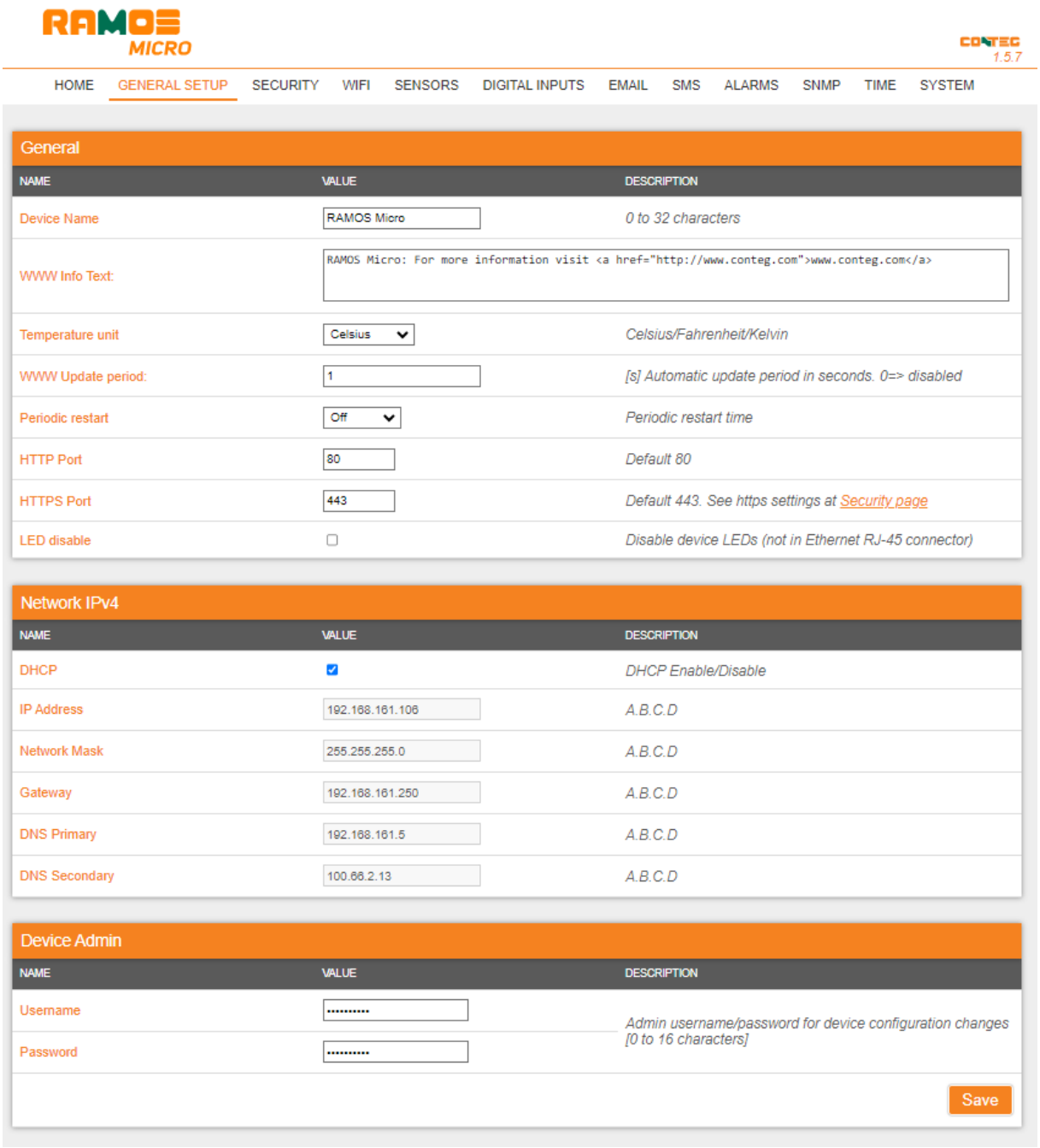
General Info section

- **Device Name** - This setting allows you to assign a unique name to the device, which can be helpful when managing larger installations. You can configure the device name on the General Setup tab.
- **Time** - Displays the current time of the device. You can set it manually in the Time tab, or you can choose to synchronize it automatically over the Internet. If the automatic synchronization is successful, the displayed time indicates that the device has Internet access.
- **Date** - Shows the current date of the device. You can set it manually in the Time tab, or you can synchronize it automatically over the Internet. If the automatic synchronization is successful, the displayed date indicates that the device has Internet access.

Sensors & Digital Inputs section

- **State** - Current state of the input or sensor.
  - **Normal** - Quiet state, everything is fine.
  - **Alarm High** - The value has exceeded the upper allowable limit.
  - **Alarm Low** - The value has dropped below the lower allowable limit.
  - **Alarm** - Binary input in Alarm state (as set by the Alarm Alert item on the Digital Inputs page).
- **Name** - The name of the sensor used for better identification in larger systems. The name can be set in the Sensors or Digital Input page.
- **Type** - Sensor Type; determines what type of sensor it is (temperature/humidity/digital input, etc.).
- **Current Value** - The current value, including the measured quantity.

General Setup tab



General part

- **Device Name** - The device name (default “STE2 r2 %Dev Hash%”) helps to differentiate individual devices in the network.
- **WWW Info Text** - Text displayed in the footer of the device's web page.
- **Temperature Unit** - Allows selecting the unit to display temperature - Celsius, Fahrenheit or Kelvin. Safe Range values are automatically calculated based on this option.
- **Periodic Restart** - A feature that enables periodic automatic restart of the device to improve its stability in exposed networks.
- **Disable LEDs** - Allows disabling certain signaling LEDs on the device, except for those on the RJ45 connector.

- **HTTP Port** - The port number on which the embedded WWW server listens, which can be changed to access multiple devices from an external network through a router. The default port is 80, and setting the value to 0 disables HTTP support.
- **HTTPS Port** - The port number on which the embedded WWW server listens for secure HTTPS connections, which can be changed to access multiple devices from an external network through a router. The default port is 443 and setting the value to 0 disables HTTPS support. It's essential to verify any changes with the network administrator.

Network IPv4 section

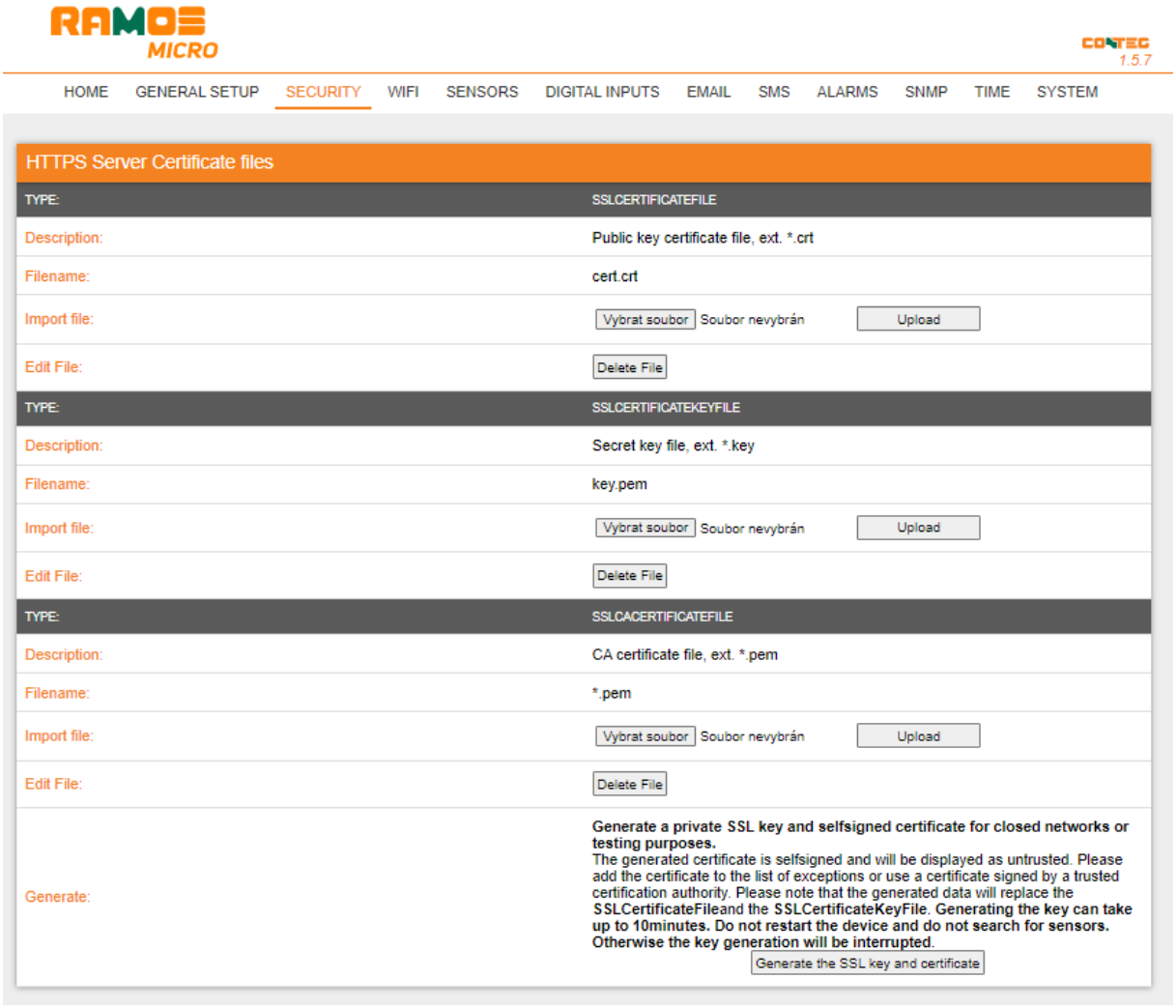
The IPv4 parameters of the RJ45 connection. The WiFi connection parameters are in the WiFi tab.

- **DHCP** - Enables the IP address setting function of the DHCP server, if available. Enabling or disabling DHCP depends on the needs of the user and the network administrator.
- **IP Address** - The IP address of the device, assigned by the network administrator.
- **Network Mask** - Network mask, assigned by the network administrator.
- **Gateway** - The IP address of the default gateway, assigned by the network administrator.
- **DNS Primary / DNS Secondary** - The IP address of the DNS server, assigned by the network administrator.

Device Admin section

- **Username / Password** - The username and password used to secure access to the web device environment.

Security tab



HTTPS Server Certificate files

Manages certificates required for the HTTPS server. Allows you to upload or delete a public key, a private key, or a certificate from the certificate authority (CA) that issued the public key certificate.

Generate SSL key and certificate

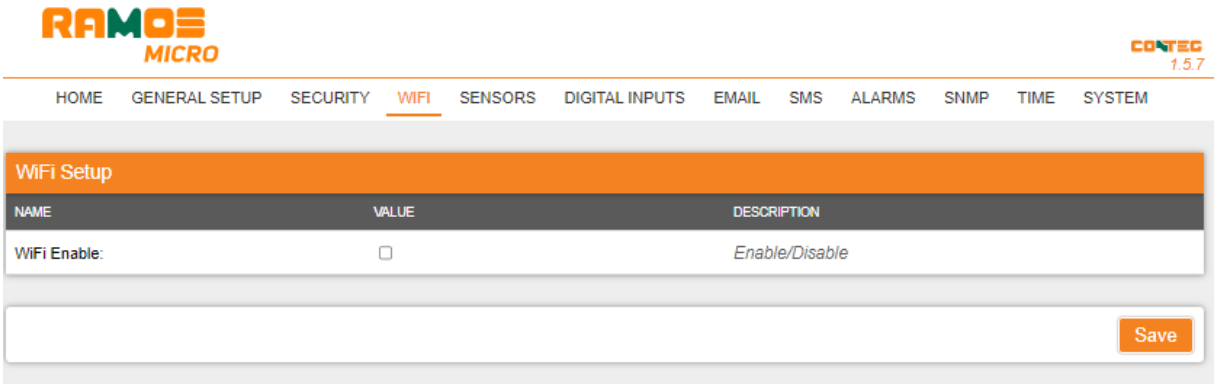
Generate a private SSL key and self-signed certificate for closed networks or testing purposes. The generated certificate is self-signed and will be displayed as untrusted.

Please add the certificate to the list of exceptions or use a certificate signed by a trusted certificate authority. Please note that the generated data will replace the SSL Certificate File and the SSL Certificate Key File.

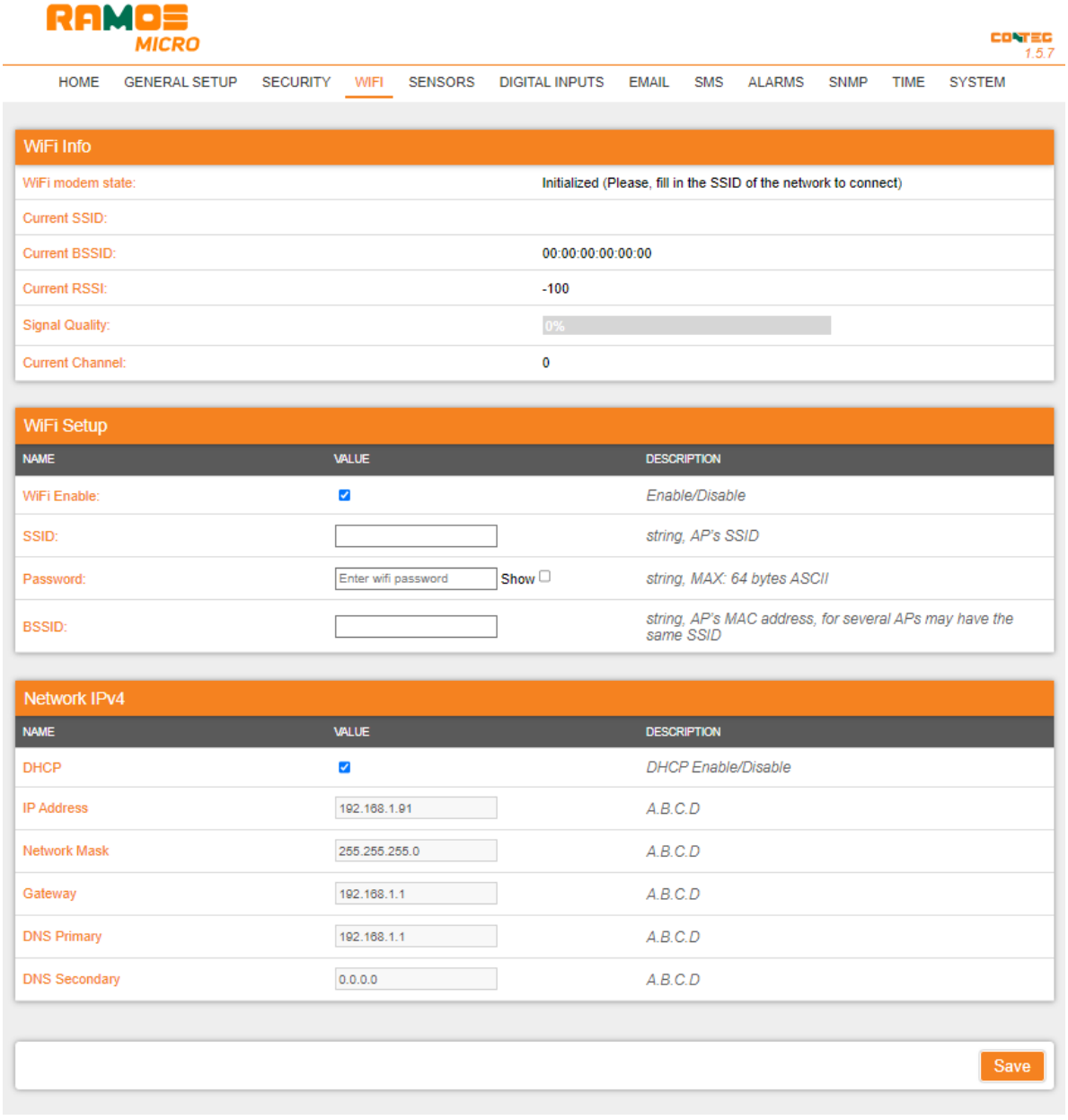
Generating the key may take several minutes. Do not restart the device and do not search for sensors. Otherwise, the key generation will be interrupted.

WiFi tab

When WiFi is off, only the Enable option is displayed:



All options are available after enabling (when mark value and press save button):



WiFi Info section

- WiFi modem state
  - **Disable** - WiFi is disabled.
  - **Wait for power on** - Waits for WiFi module when power on.
  - **Init** - Initializing of WiFi module.
  - **Connecting** - Connecting.
  - **SSID check** - SSID check.
  - **Connected** - Connected to selected WiFi network.
  - **Network WiFi scan** - Scans for available WiFi networks.
  - **Wait for scan** - Waits for Network WiFi scan.
- **Current SSID** - Current name of the network the device is connected to. If the parameter is missing, the device is not connected to any WiFi network.
- **Current BSSID** - Current identifier of the WiFi network connection point. If the parameter is missing, the device is not connected to any WiFi network.
- **Current RSSI** - Relative strength of signal input. The lower the RSSI, the stronger the signal.
- **Signal Quality** - Strength of WiFi signal in % with graphic indicator.
- **Current Channel** - WiFi channel on which the device communicates. If the parameter is missing, the device is not connected to any WiFi network.

WiFi Setup section

- **WiFi Enable** - Enable or disable WiFi. By default, the wireless interface is disabled. Device restart follows enabling.
- **SSID** - The name of the WiFi network to which you want the device to connect. If you do not know your network name, use the Scan AP function at the bottom of the page.
- **Password** - Secured network password. If you do not know it, contact your network administrator.
- **BSSID** - Identifier of the WiFi network connection point (MAC address of the connection point). Optional data.

Network IPv4 section

WiFi network parameters. Only the wireless interface is set here. Configure RJ45 LAN parameters in the General Setup tab.

- **DHCP** - Enables the IP address setting function of the DHCP server, if available. Enabling or disabling DHCP depends on the needs of the user and the network administrator.
- **IP Address** - The IP address of the device, assigned by the network administrator.
- **Network Mask** - Network mask, assigned by the network administrator.
- **Gateway** - The IP address of the default gateway, assigned by the network administrator.
- **DNS Primary / DNS Secondary** - The IP address of the DNS server, assigned by the network administrator.

Wifi Scan List section

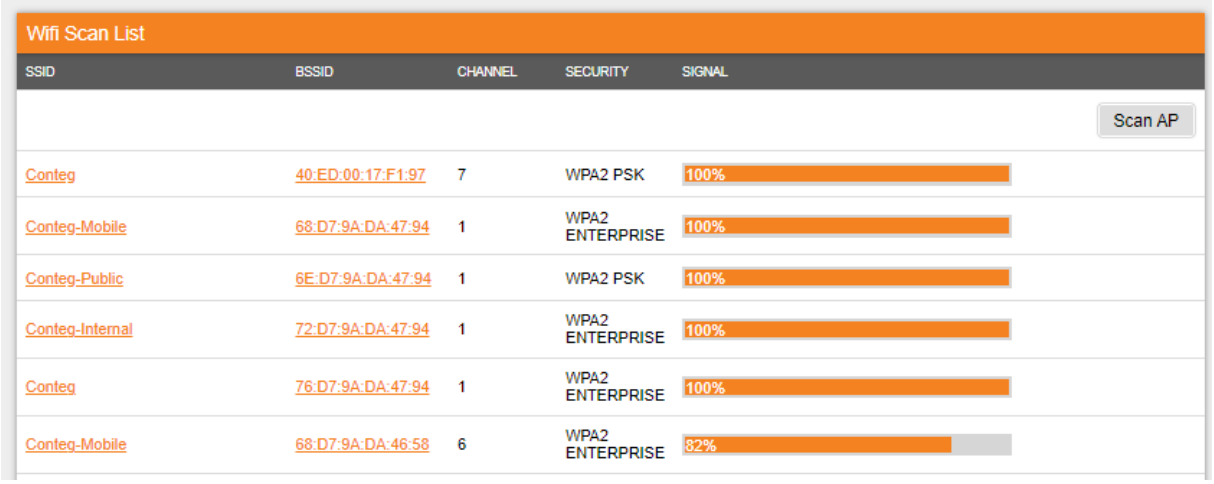
- **SSID** - Name of the WiFi network found.
- **BSSID** - Connection point identifier (MAC address).
- **Channel** - The WiFi channel where the AP communicates.

- **Security** - The security type of WiFi communication.
- **Signal** - WiFi signal strength in % with graphical indicator.

Connecting to a discovered WiFi

- Click on the SSID of the discovered network to pre-fill the WiFi settings and then just fill in the Password. The BSSID field will remain blank. Standard settings. When you change the AP, it will reconnect itself.
- Clicking on the BSSID will pre-fill not only the network name (SSID) but also the MAC address of the specific AP (BSSID). The device will connect to that AP and in the case of pooled networks will not try to reconnect.

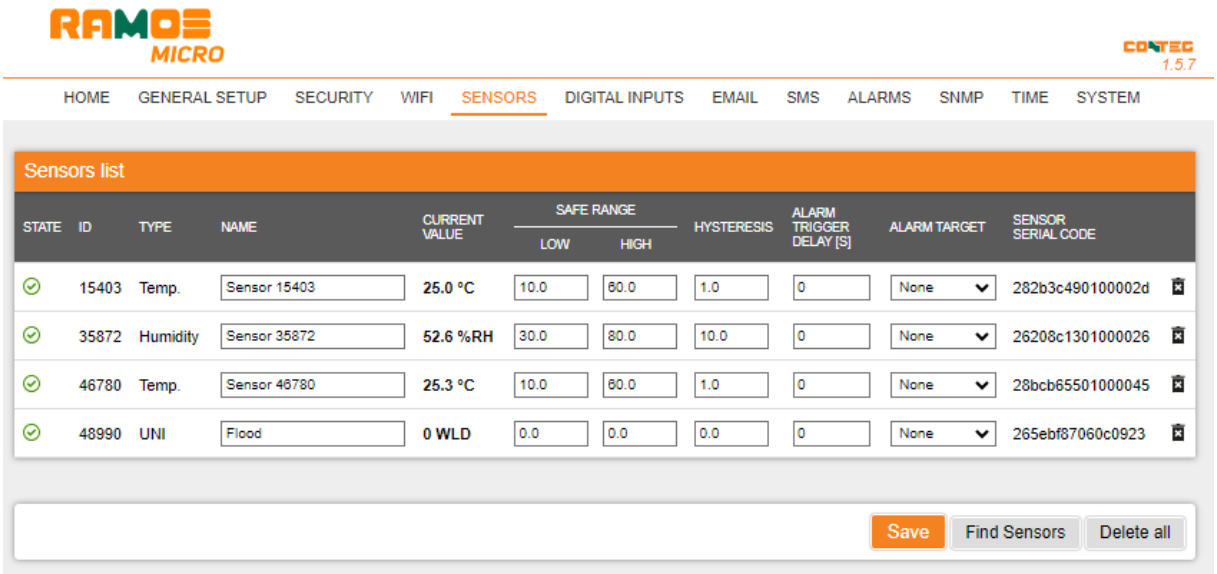
Scan AP (WiFi Access Points)



WiFi debug section

- Provides useful info for debugging WiFi connection

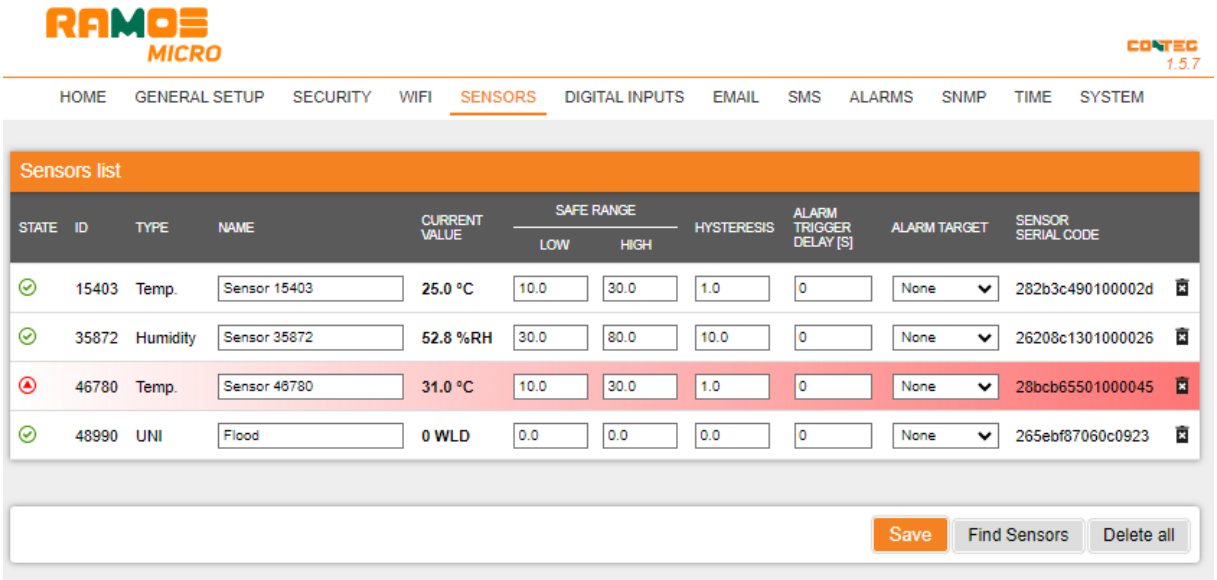
Sensor tab



Sensor List section

- **State** - State of the DI (input) or sensor.
  - **Normal** - Quiet state, everything is fine.
  - **Alarm High** - The value has exceeded the upper allowable limit.
  - **Alarm Low** - The value has fallen below the lower allowable limit.
- **ID** - 2 bytes sensor ID (identical to ID on Poseidon2 devices).
- **Type** - Sensor type; indicates what type of sensor it is (temperature/humidity etc.).
- **Name** - The name of the sensor, used for better identification in larger systems. It can be set on the Sensor or Digital Input tab.
- **Current Value** - The current value including the measured quantity.
- **Safe Range** - Refers to the range of acceptable (allowed) values that are considered within normal limits. If the current value falls outside the Safe Range, an alarm is triggered to indicate that the measurement is out of bounds and requires attention.
- **Hysteresis** - The parameter specifies a range of insensitivity when the measured value exceeds the limit value. It prevents triggering of multiple alarms when the value oscillates around the limit. For more details, please refer to page 23 of the manual.
- **Alarm Target** - Allows you to define targets where Alarm messages (SMS + Email) will be sent. Target destinations are set in the Alarms tab. The drop-down menu allows you to assign an existing set of targets to the sensor or create a new one.
- **Alarm Trigger Delay [s]** - Delays the sending of alarm start information by a defined time.
- **Sensor Serial Code** - The full ID of the 1-Wire sensor.
- **Delete** - The button to delete a specific sensor.

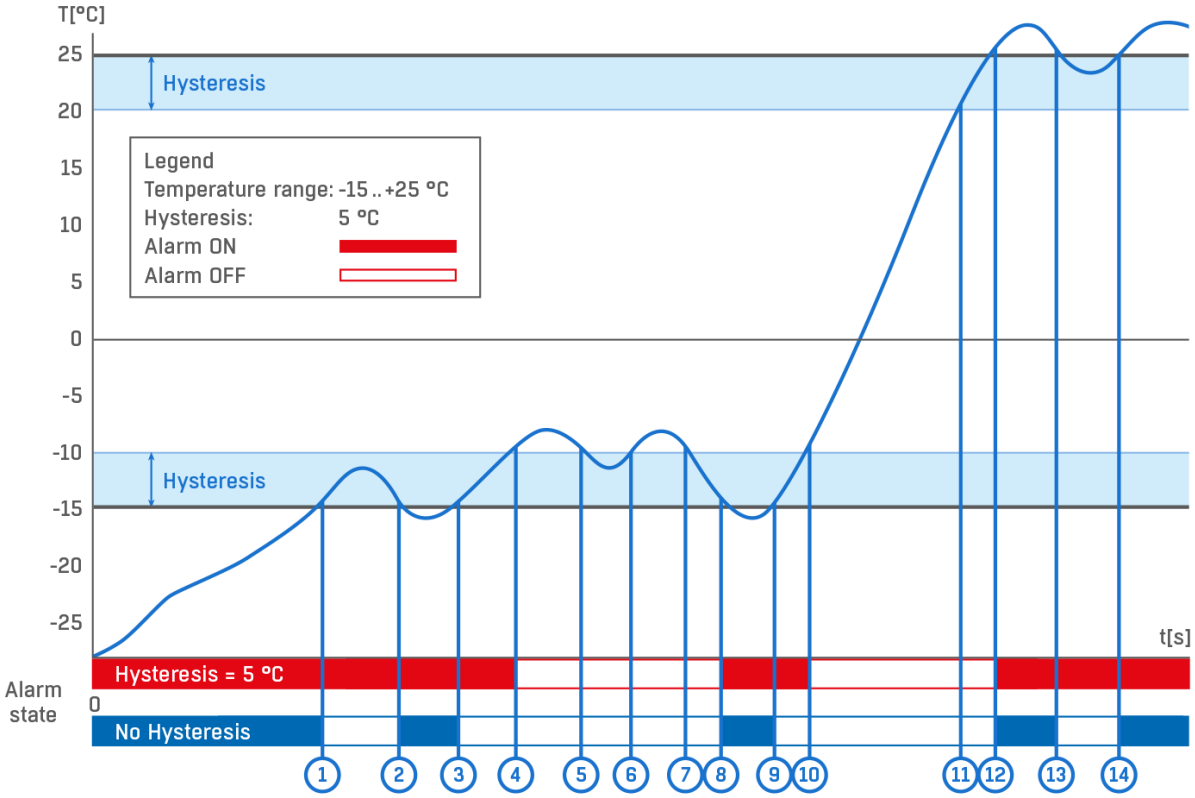
Sensor alarm state indication*



* Sensor in the Alarm state is highlighted.

Hysteresis

The Hysteresis value defines the width of the tolerance range for sending an alarm. This function stops multiple alarms from happening, when the value goes up and down around a set point. You can see this on the graph.



Within the internal 5°C hysteresis band, the alarm would be activated at **point 8** and would end at **point 9**. Because of the hysteresis function, the alarm is extended until the temperature reaches the end of the hysteresis zone (point 10) 5 °C + (-15 °C) = -10 °C.

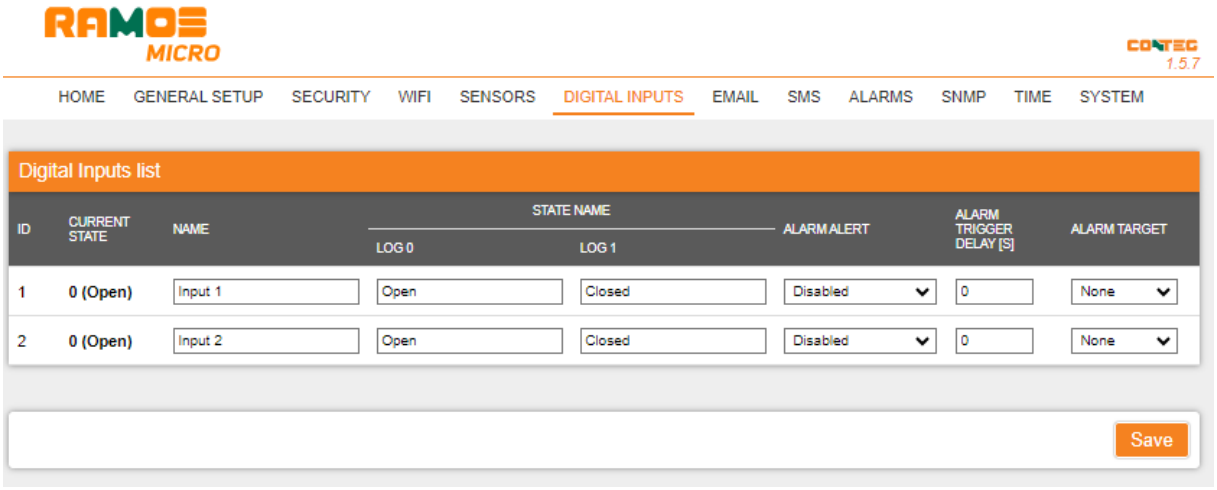
- Hysteresis (=5 °C): The unit sends 3 alerts (email, SMS, …)

  Alarm at points 0-4, 8-10, 12 and upwards.

- Without hysteresis (0 °C): The unit sends 8 alerts (email, SMS, …)

  Alarm at points 0-1, 2-3, 8-9, 12-13, 14 and upwards.

Digital Input tab

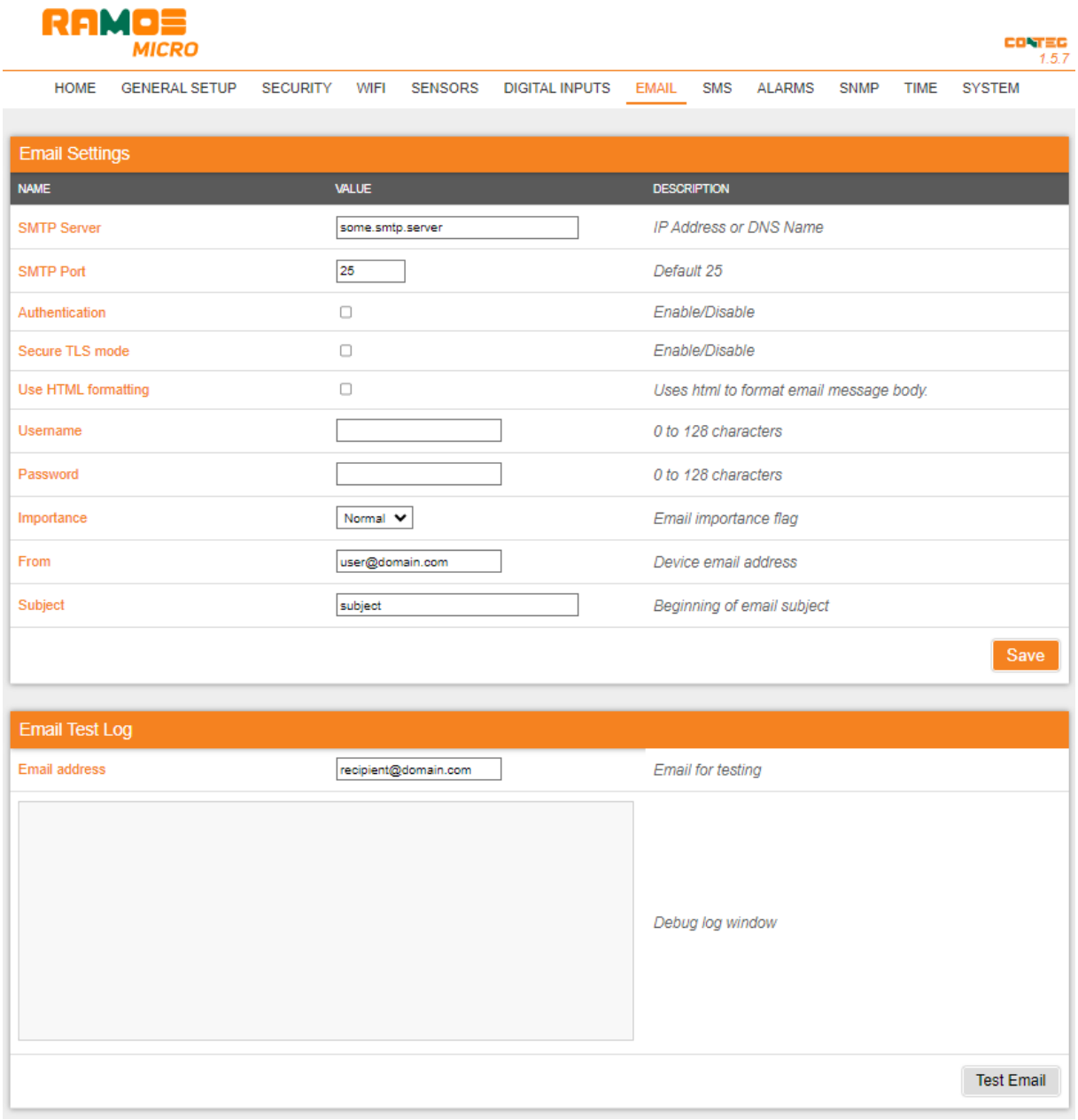


Digital Inputs List* section

- **ID** - Identification of the input within the device.
- **Current State** - List the current state of the input (0/1 and the state name).
- **Name** - Name of the input max. 22 characters (e.g. "2p door left", "smoke section 1").
- **Alarm Alert** - Alarm status definition for each input.
- **Alarm Target** - Allows you to define targets where Alarm messages will be sent (SMS + Email). Target destinations are set on the Alarms page. The drop-down menu allows you to assign an existing set of targets to the sensor or create a new one.
- **Active if Close** - Alarm active when the input is in state 1 (On).
- **Active if Open** - Alarm active when the input is in state 0 (Off).
- **Disabled** - The input does not have a defined Alarm state.
- **Alarm Trigger Delay [s]** - Delays the sending of alarm start information by a defined time.

** DI input in the Alarm state is highlighted.*

Email tab



Email Settings

- **SMTP Server** - The IP address or domain address of the SMTP server.

  Note: Consider the long-term stability of the used SMTP server. If the service provider changes security requirements (separate username or password for example) your device alerting functionality will be lost without any warning.

- **SMTP Port** - Port number on which the mail server listens – 25 by default.
- **Authentication** - Enable authentication; check if the SMTP server requires authentication.
- **Secure TLS mode** - Check if the SMTP server requires secure communication via SSL/TLS.
- **Username** - Username for the SMTP server authentication. If the Authentication field is not checked, the content of this field is irrelevant.

- **Password** - Password for the SMTP server authentication. If the Authentication field is not checked, the content of this field is irrelevant.
- **Importance** - Sets the priority of the email message. Important for filtering and further processing alarm messages.

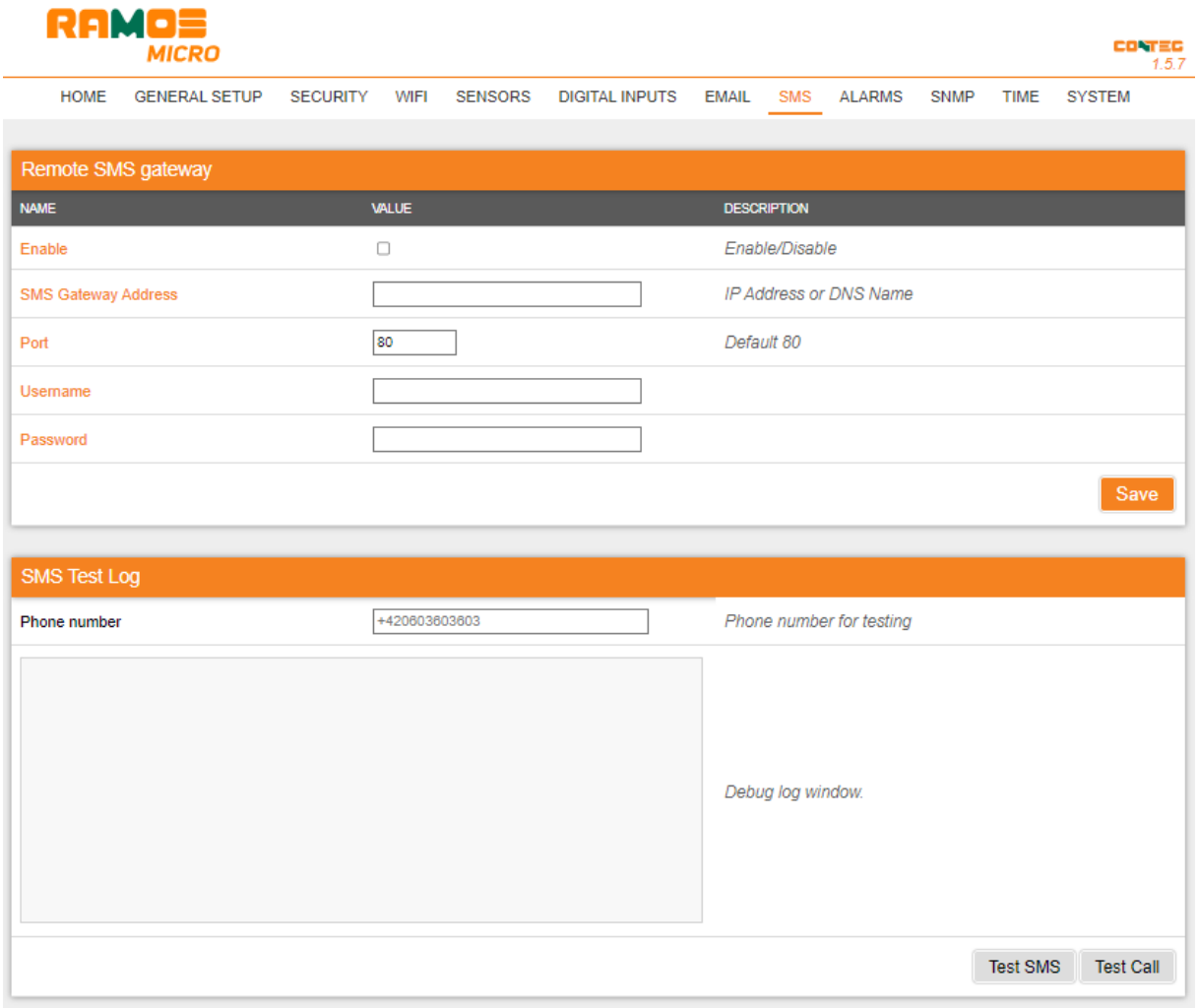
- **From** - Sender's Email address, i.e. of the device. The address may be required by the SMTP servers and can be used to identify the device or to filter and further process alarm messages.
- **Subject of the Email** - The field content can be used to identify the device or for filtering and further processing of alarm messages.

Email Test Log section

In this section, the SMTP server settings can be tested. Click Test Email to send a test Email to the specified Email address. The Debug log window shows the communication with the SMTP server.

SMS tab

This functionality requires a SMS gateway device with an active SIM card registered in the network.



Remote SMS gateway

- **Enable** - Turns on the SMS sending function.
  For sending alert, the SMS alarm action must be configured in the Sensors or DI settings.
- **SMS Gateway Address** - IP address where SMS-GW device is located. It can be set including service - typically /service.xml (for example "http://192.168.15.1/service.xml")
- **Port** - The TCP port on which the gateway listens.
- **Username** - Username for authorization in SMS GW.
- **Password** - Password for authorization in SMS GW.
- **SMS + Ring When Alarm** - Enables sending an SMS and then dialling the number.

SMS Test Log

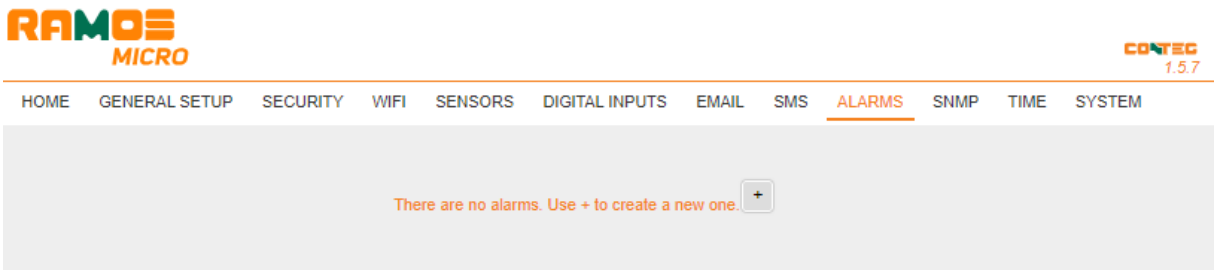
In this section, the SMS gateway settings can be tested.

- **Test SMS** - Sends a test text message to the specified Phone number.
- **Test Call** - Dials the specified Phone number.
- **Debug log window** - Shows the communication with the SMS gateway.

Alarms tab

This tab is used to set alarm targets. Up to 2 sets of destinations can be created and each set can contain up to 2 email destinations and 2 phone number destinations for SMS and voice call alarms.

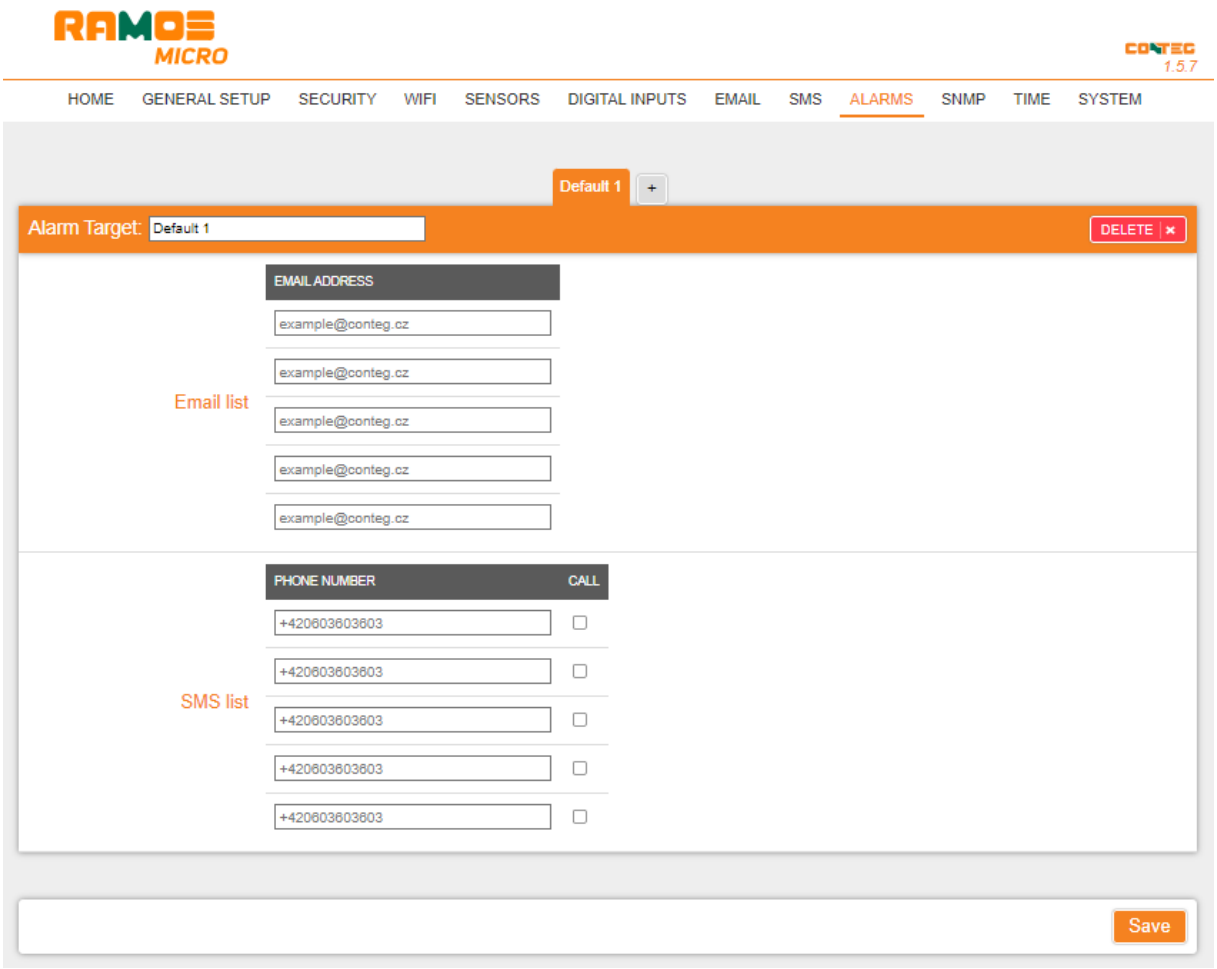
These sets are then assigned to individual sensors and Digital Inputs. The set is created either by pressing the + button on the Alarms page or by selecting **Add new...** on the Sensor or Digital Input edit page.



Alarm Target

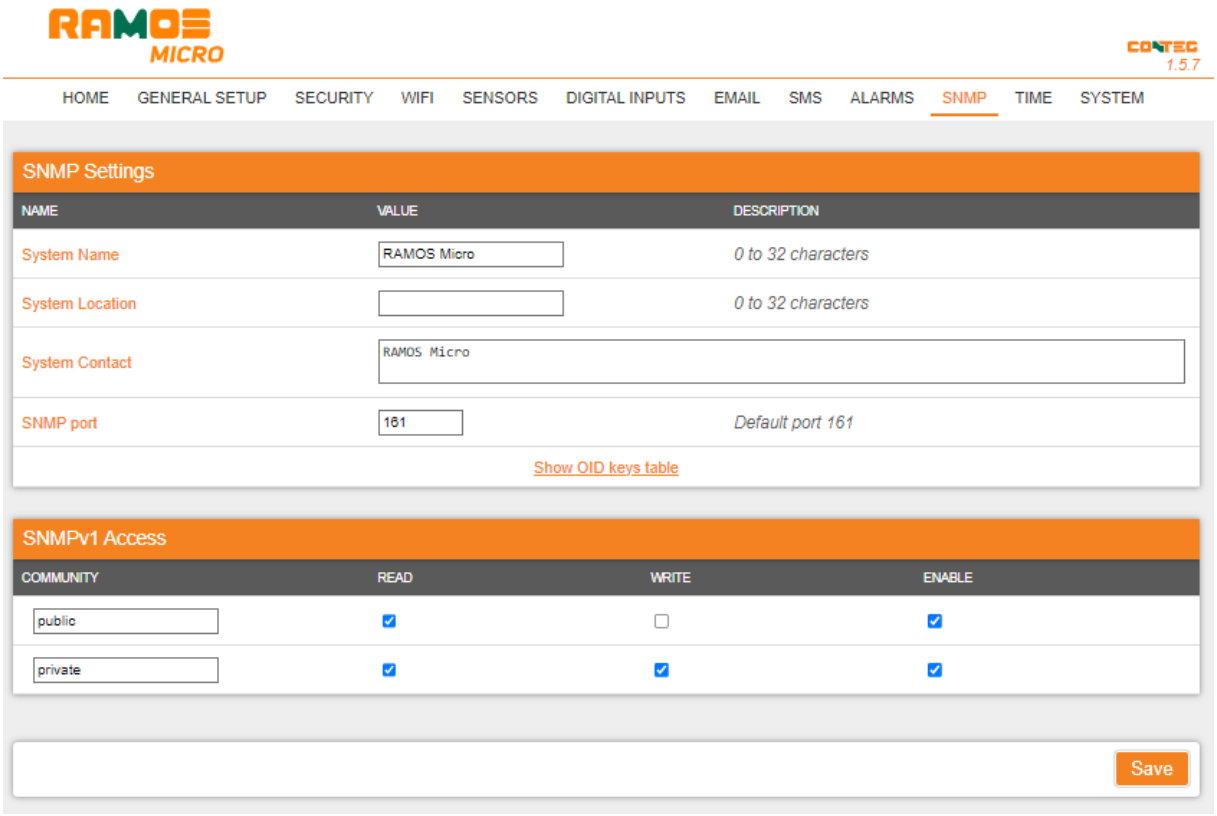
A set of targets. The set can be named for clarity.

- **Email list** - A set of email addresses to which alarm messages will be sent. The SMTP server on the Email tab must be set up correctly for the email to be sent.
  - ***Email address*** - The field can only contain one email address at a time.
- **SMS list** - A set of phone numbers to which alarm messages will be sent. To send SMS, the SMS gateway must be set up correctly in the SMS tab.
  - ***Phone number*** - The field may only contain one phone number at a time.
  - ***Call*** - If checked, the phone number will ring after the SMS is sent (the user does not need to hear the incoming SMS). Ringing lasts for about 20 seconds for each individual number and then is terminated. Answering the call only ends the ringing, no voice message is sent.



SNMP tab

The SNMP tab configure parameters for Open API - SNMP protocol.



SNMP Settings section

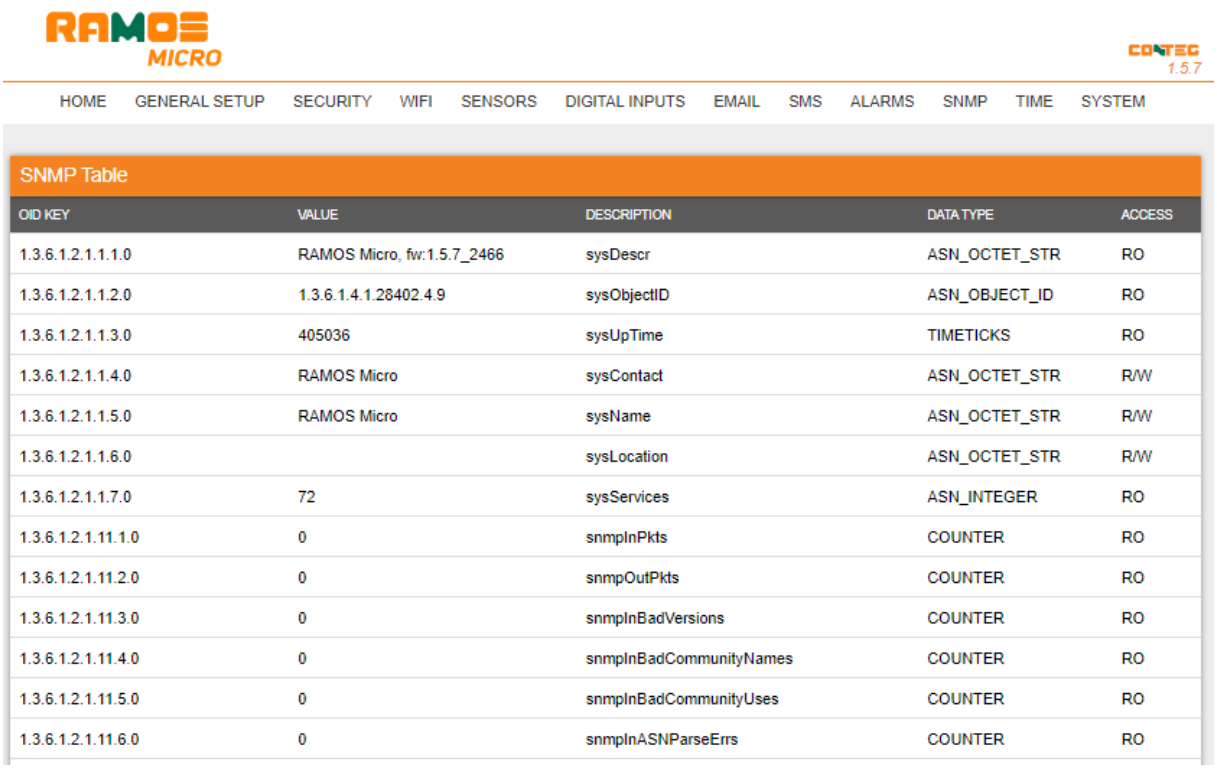
- **System Name** - The name of the device within SNMP.
- **System Location** - The location of the device within SNMP.
- **System Contact** - The contact for the device administrator within SNMP.
- **SNMP Port** - The port number on which SNMP can communicate - 161 by default.

SNMPv1 Access section

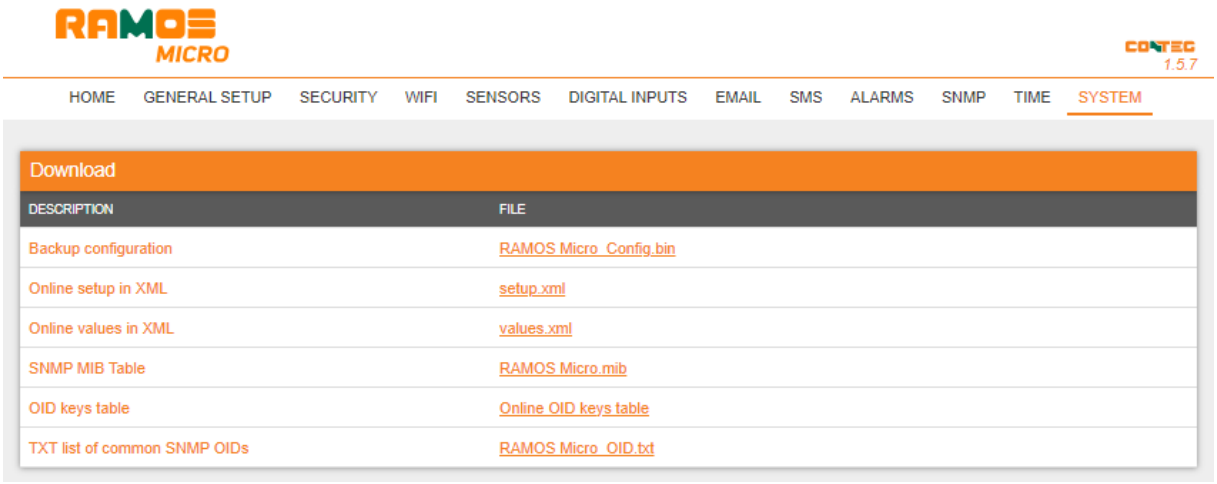
- **Community** - The name of the SNMP community for accessing the device over SNMPv1. 2 communities can be defined. For each Community you can define whether it has permissions for:
    - **Read** - Enables or disables the read function.
    - **Write** - Enables or disables the write function.
    - **Enable** - Enables or disables a specific community.

Show OID keys table

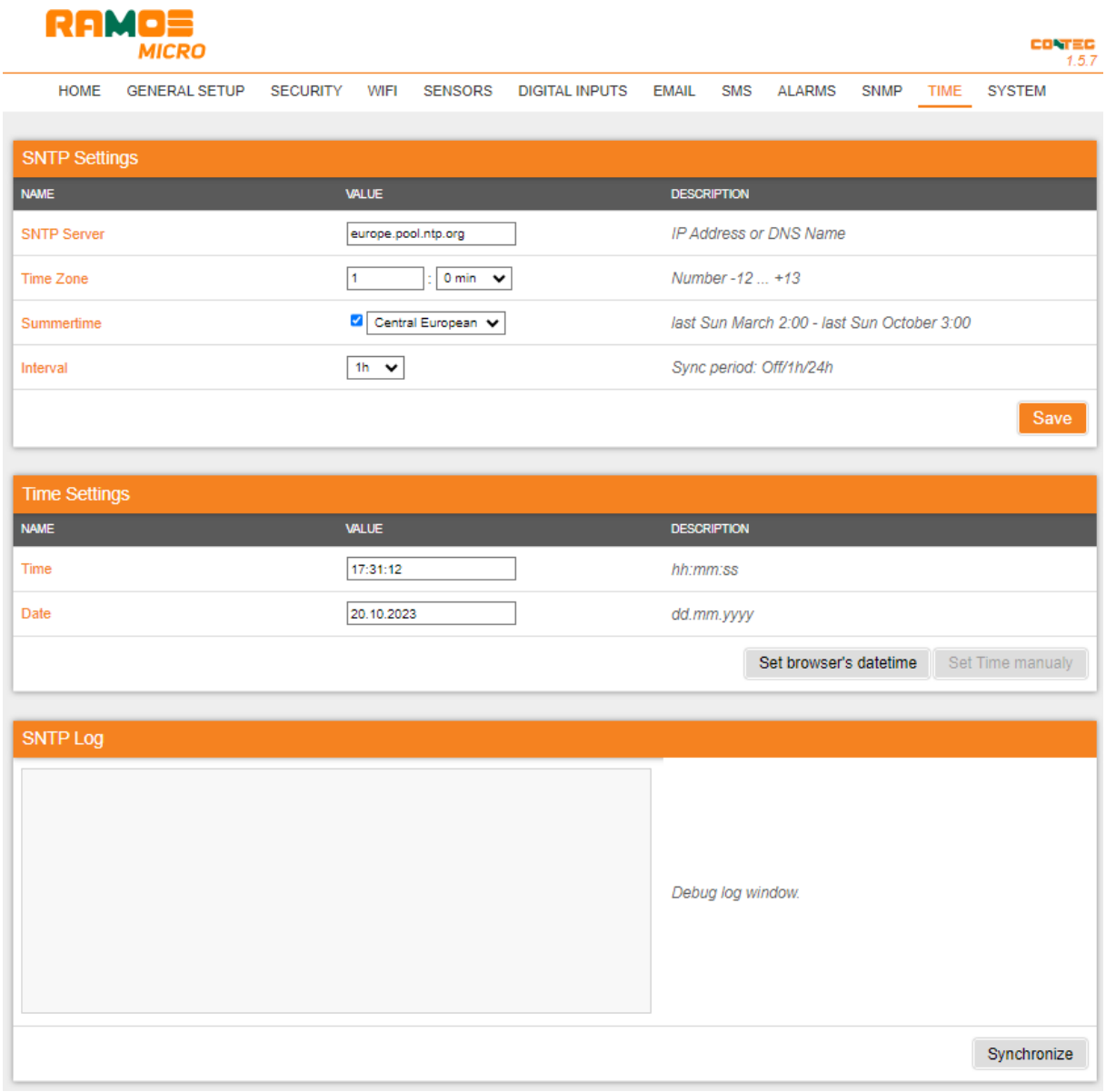
This function lists the entire tree of variables with the full SNMP OID and explanations about the type variables. A MIB is also available for connecting devices to 3rd party monitoring systems.



Download the MIB file in the System tab (Download MIB file).



Time tab



SNTP Settings section

- **SNTP Server** - The IP address or domain address of the time synchronization server; europe.pool.ntp.org by default.
- **Time Zone** - Set the time zone of the device location. Used to set the correct system time. Necessary for correct recording of measured values.
- **Summertime** - Enable daylight saving time. Used to set the correct system time. Required for correct recording of measured values.
- **Interval** - Interval of time synchronization with the server.

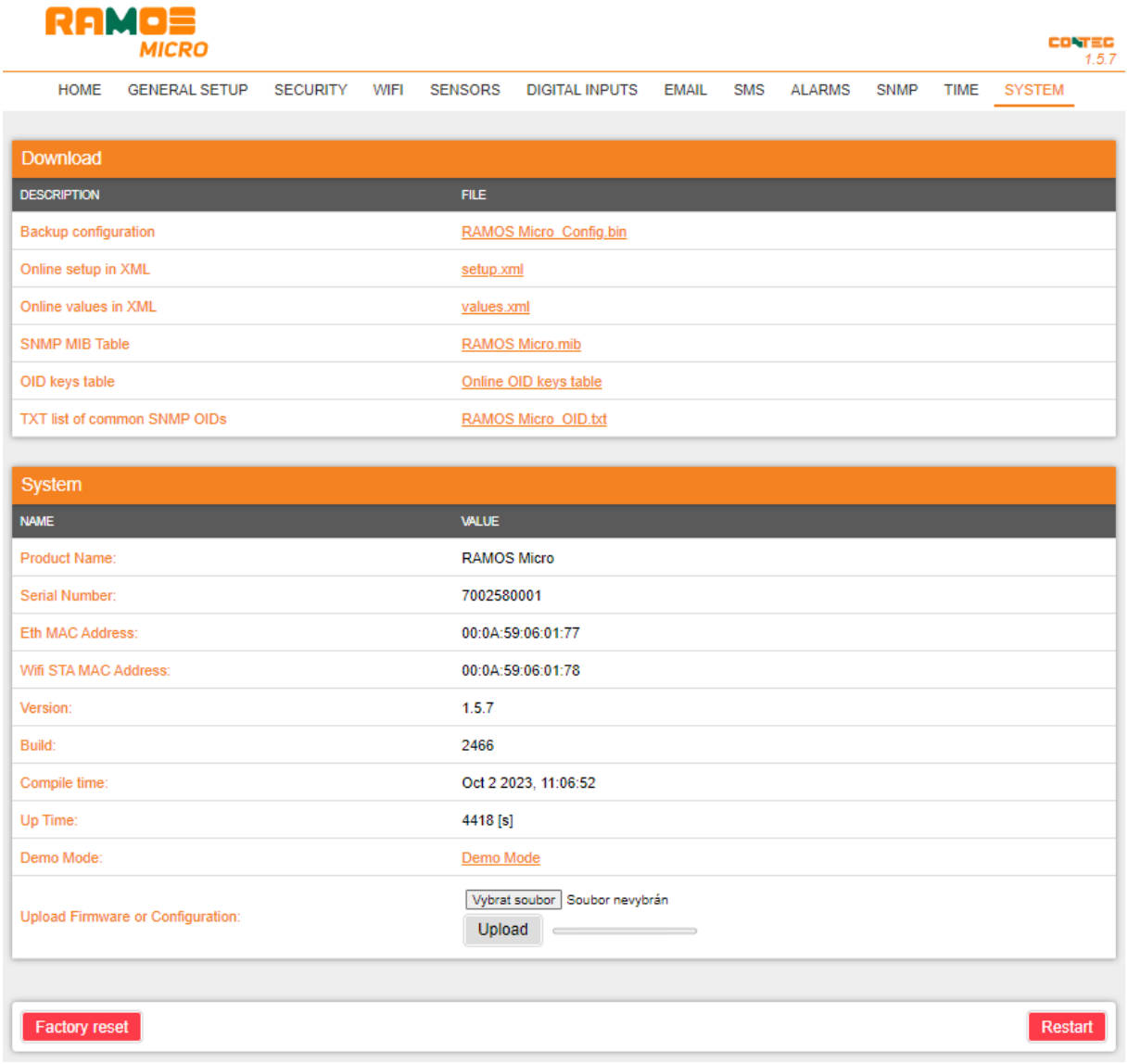
Time Settings section

Allows you to fill in the current date and time manually when synchronization with the time server cannot be used.

SNTP Log section

The Sync button is used to perform an instant synchronization with the time server. It can also be used to test the settings.

System tab



Download section

- **Backup configuration** - Device configuration backup in BIN format. Click on the link to save the current device configuration after its final settings for potential restore purposes.
- **Online setup in XML** - Configuration backup in XML format. Click on the link to save the current device configuration after its final settings for potential restore purposes.
- **Online values in XML** - Current values in XML format. Click on the link to save the current device configuration after its final settings for potential restore purposes.
- **SNMP MIB Table** - SNMP MIB file. MIB file address containing the definition of SNMP variables.

- **OID keys table** - The function draws up the entire tree of variables with an indication of the entire SNMP OID and explanations of the variable type.
- **TXT list of common SNMP OIDs** - Overview of the most important OID from the MIB table.

System section

- **Product Name** - Device name (type).
- **Serial Number** - Device serial number.
- **Eth MAC Address** - MAC address of the device for cable connection.
- **WiFi STA MAC Address** - MAC address of the device for WiFi connection.
- **Version** - Firmware version. Serves for diagnostic purposes when troubleshooting.
- **Build** - Serves for diagnostic purposes when troubleshooting.
- **Compile time** - Firmware compile time. Serves for diagnostic purposes when troubleshooting.
- **Up Time** - Runtime of the device since the last switching on or restarting. Serves for diagnostic purposes when troubleshooting.
- **Demo mode** - Active demo mode prevents any changes in the device configuration. In this mode, users can browse and view all the web interface pages, but they are not allowed to change any values. A device with this setting can be placed on the public Internet with no risk of changes to its configuration. Demo mode can be turned off in the same way after entering the password.
- **Read available version** - Lists the latest firmware version on the HW group update server.
- **Start Network Upgrade** - Launches a firmware upgrade from the HW group update server.
- **Upload Firmware or Configuration** - Install newer firmware or configuration file to the device.

Restore configuration may not work if there is too big difference in firmware versions.

Factory reset button

Restores factory settings. By default, DHCP setup is enabled. If the device does not receive an address within 60 seconds of switching it on, it defaults to 192.168.10.20 as the default IP.

Neither the username nor the password are defined by default.

Restart button

Restarts the device (reboot only, no default settings).

Technical parameters

Ethernet	
Interface	RJ45 (10/100BASE-T)
Supported protocols	IP: ARP, TCP/IP (HTTP, HTTPS, SNTP, SMTP, netGSM, TLS), UDP/IP (SNMP, Syslog)
SNMP	Version 1
WiFi	
Supported standards	802.11 b/g/n
Frequency	2.4GHz
Output	+19.5 dBm output power in 802.11b mode +16 dBm for 802.11n

Security	WEP / WPA / WPA2 PSK
Antenna	Internal
External sensors	
Port/connector	Port1, Port2 / RJ11 (1W-UNI)
Values limit	Up to 5 sensor values (°C, %RH, WLD, Voltage ...)
Sensor type	Only sensors from HW group s.r.o.
Sensors/distance	2× Max. 60 meters total length (per each RJ11 port)
DI INPUTS (Dry Contact Inputs)	
Port/connector	I1, I2 / ø2 mm terminal block
Type	Digital Input (supports NO/NC Dry contact)
Sensitivity	Sensitivity 1 (On) = 0-500 Ohm
Max. distance	Up to 50m
Power supply	
Power voltage	5V / 250 mA
Connector	Connector Jack Ø3.5 x 1.35 / 10 [mm]
PoE (Power over Ethernet)	PoE (Power over Ethernet) RJ45 - IEEE 802.3af Class 0
LED	
Link	Yellow - Ethernet connection state
Activity	Green - Ethernet activity
Alarm	Port 1 - Alarm SENS - LED is lit in case of alarm active on a sensor Port 2 - Alarm DI - LED is lit in case of alarm active on a DI
2x DI input	Green - LED indicates switching on the DI Input
WiFi	Blue - connection state in operation (shining), search indicator (flashing slowly) and connecting (flashing quickly)
Button	
Reset	Restore default settings: hold and connect power supply, keep holding button for 5 seconds.
Other parameters	
Operating temperature	-10 to 60 °C (device operating temperatures) Sensors temperature range can vary widely
Dimensions/weight	98 × 68 × 33 (W × H × D) / 91 g
Elmag. radiation	CE / FCC Part 15, Class B
Elmag. compatibility	EN 61326-1:2013, EN 61010-1:2010, EN 55011:2009, EN 62311:2008

WiFi Radio

Description	Min	Typical	Max	Unit
Input frequency	2412	-	2484	MHz
Tx power				
The output power of PA for 72.2 Mbps	13	14	15	dBm
The output power of PA for 11b mode	19,5	20	20,5	dBm
Sensitivity				
DSSS, 1 Mbps	-	-98	-	dBm
CCK, 11 Mbps	-	-91	-	dBm
OFDM, 6 Mbps	-	-93	-	dBm
OFDM, 54 Mbps	-	-75	-	dBm
HT20, MCS0	-	-93	-	dBm
HT20, MCS7	-	-73	-	dBm
HT40, MCS0	-	-90	-	dBm
HT40, MCS7	-	-70	-	dBm
MCS32	-	-89	-	dBm

Adjacent Channel Rejection				
OFDM, 6Mbps		37		dB
OFDM, 54Mbps		21		dB
HT20, MCS0		37		dB
HT20, MCS7		20		dB

WiFi signal strength

What is signal strength

WiFi is a radio signal and it has limitations in reach given firstly by the transmission output and secondly by the quality and shape of the antennas. Signal strength is indicated in decibels per milliwatt of output (dBm), often (incorrectly) simplified to "dB". Signal strength has a negative value and it applies that the lower the value (a higher number after the minus sign), the worse.

The decibel unit is non-dimensional and expresses the logarithm of a ratio of two values. In our case, it is the ratio of the received output to an etalon of 1 mW:

$$dBm = 10 * \log_{10} \frac{P_1}{1\ mW}$$

This means that if you have a signal of -54 dBm, it is higher (better) than a value of -82 dBm.

Supported interfaces

Digital Inputs

Dry contact, simple door contact or relay output can be connected to the green terminal block. DIs are galvanically connected to the power supply.

- Not switched input has a value of „0 (Off)".
- Switched input is identified as „1 (On)",
  Ohmic resistance 0 Ω to 500 Ω.

Connection parameters:

- Maximum cable length: 50 meters.
- Supported detectors: Any dry contact.
- Alarm alert setting for each DI input:
  - Alarm Disabled.
  - Alarm state = 1 (Active if close)
  - Alarm state = 0 (Active if Open)
- Alarm target:
  - None - No reaction.
  - Defined target (Notify of Alarm by sending an Email or SMS).
- Reading period: 800 ms.
- **Range of ID sensors**: DI (Digital Inputs) use address ID 1 or 2.
- **Name**: Each one DI can be named independently with up to 22 characters.

- **Sensor disconnection detection**: No, the disconnected sensor returns to the value „0 (Off)“.

Available detectors you can connect to DI port:

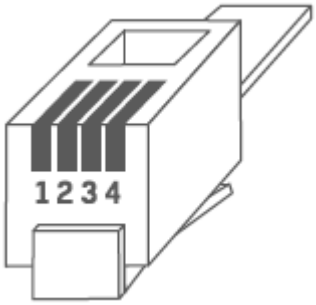
- Water flood detector (spot detection)
- WLD (Water Leak Detection) Relay with an external sensing cable
- Airflow detector
- Door contact detector
- PIR motion detector
- Gas leak detector
- Power presence (110/230V) detector
- Vibration detector

Sensors RJ11 (1W-UNI bus)

Digital sensor bus, each sensor has a unique ID.

- RAMOS Micro has 2 RJ11 ports
- Each port support max. distance 60m.
- Power: 5 V / 20 mA from RJ11 port.
- You can connect one RJ11 sensor to each port
- You can connect several physical RJ11 sensors to one port. Sensors can be daisy chained with respect to total max. distance.
- To help sensors daisy chaining, some sensors have 2 RJ11 ports.
- Avoid star topology (RJ11 splitters).
- Only sensors from Conteg are supported.

Do not connect any other sensors, it can damage the device.



RJ11 (1W-UNI)		
1)	-	Not used
2)	Data	2 Data Transmit Data
3)	GND	3 GND Ground
4)	+5V	4 +5V Power

Note:

If a cable line is more than 60 meters from a connector on the device, we can't guarantee that it will work perfectly. It depends on the type of cable, how the line is set up, and the environment where it's installed.

In case of issues, check your cable and RJ11 connectors quality.

Sensor values limit

Multiple sensor values can be connected to the device. Sensors can be daisy chained from RJ11 port. One physical sensor can measure several sensor values (°C + %RH = 2 sensor values).

- RAMOS Micro maximum limit is 5 sensor values in total.
- There can be limit based on powering external sensors. Contact our support.

Available 1W-UNI sensors:

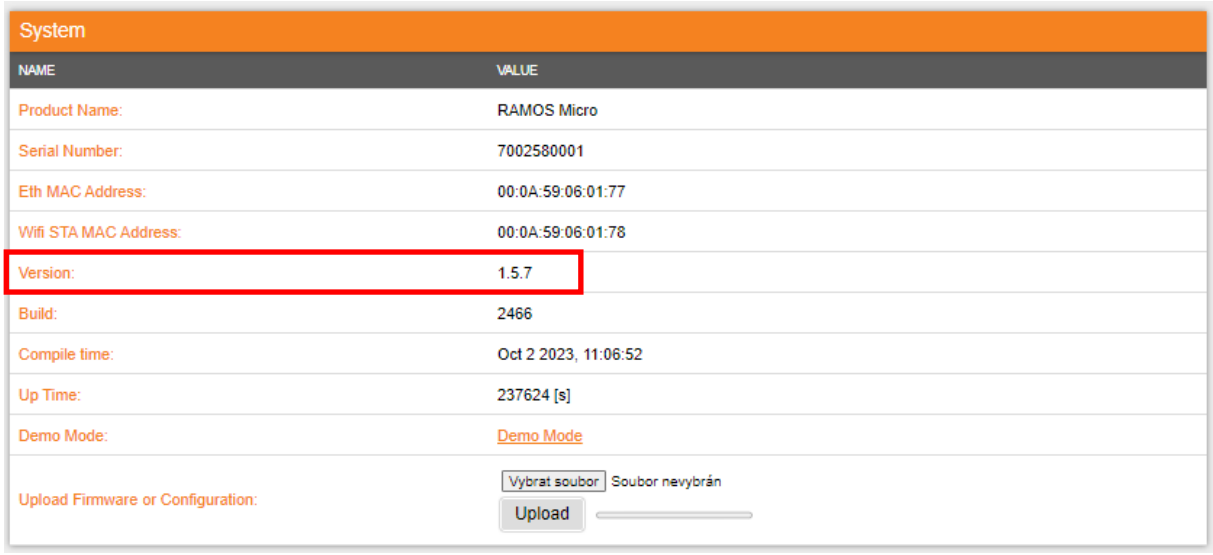
- Temperature sensors (Indoor / Outdoor / Cryo)
- Calibrated temperature sensors
- Relative Humidity sensors (Indoor / Outdoor)

- CO2 & VOC sensors
- Light sensor
- AC / DC Current sensors
- AC Voltage sensor (0-230V)
- 4-20 mA sensors (converter) for industrial probes
- Water flood detector (spot detection)
- WLD (Water Leak Detection) with an external sensing cable

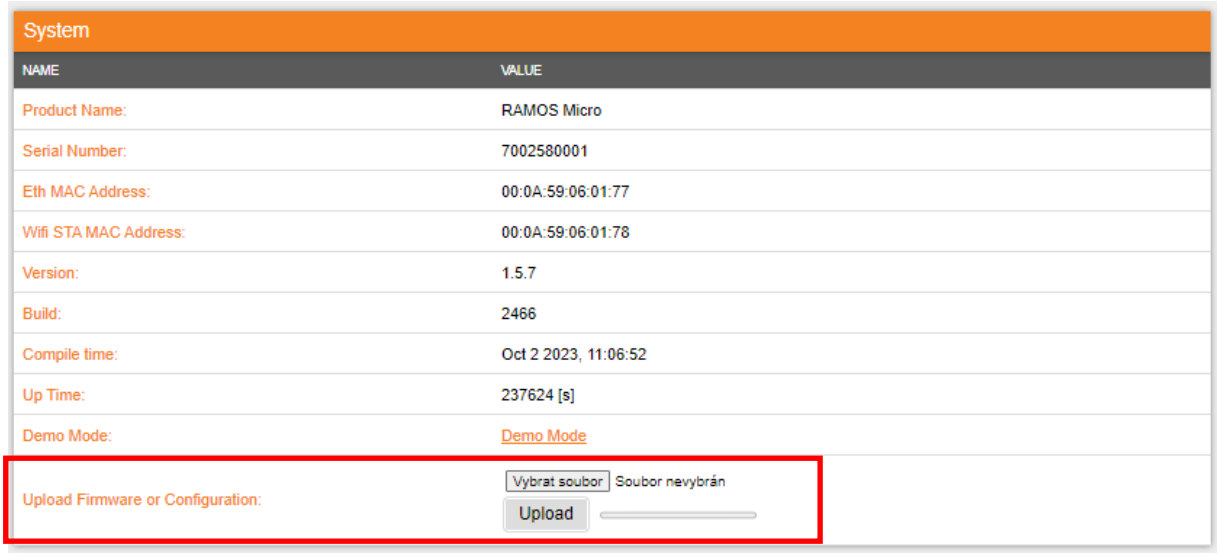
Firmware upgrade

1) Open the device web interface in the System tab.

2) The System section contains items to identify the current FW version.



3) Check available version on Conteg website. Select upgrade file and upload



4) Unit will restart.

CONTEG, spol. s r.o.

Headquarters:

Stetkova 1638/18

140 00 Prague 4

Czech Republic

Tel.: +420 261 219 182

conteg@conteg.com

www.conteg.com

Production plant:

K Silu 2179

393 01 Pelhrimov

Czech Republic

Tel.: +420 565 300 300