myBOX

User Manual

Version JAN 2016

www.myscada.org

SAFETY PRECAUTIONS

1. **PLEASE CHANGE THE DEFAULT PASSWORD BEFORE USING THE DEVICE IN A PRODUCTION ENVIRONMENT AS NOT DOING SO MAY RESULT IN A SYSTEM INTRUSION AND ANY PERSON COULD EASILY GAIN A FULL ACCESS TO THE CONTROLLED TECHNOLOGY!!!**

2. **USE INTEGRATED FIREWALL TO BLOCK ALL SERVICES YOU DO NOT NEED TO ACCESS.**

Table of Contents

General Information 5

1. Hardware Overview 6

Hardware Features 6
Technical Specifications 7
Dimensions 10

2. Installing Your Device 11

Mounting the Device 12
Power Wiring and Device Start-Up 12
Getting Online Help from mySCADA 13
Reset to Default Settings 13

3. Communication Connections 14

Connecting to Networks via Ethernet Interface 15
Connecting to Networks via RS-232/485 Interface 17
Using the RS-232 Interface 17
Using the RS-485 Interface 19
Connecting to Networks via Wireless 3G Interface 20
Access Point Mode with Wireless Wi-Fi Integrated Card 21

4. Graphical User Interface 22

Main Screen - SCADA/HMI Views, Trends & Alarms 22
Visualization Views 23
Trends 24
Alarms 27
Data-Log Views 30

5. Administration Level 33

My Account 33
System 33
Date & Time 33
NTP 33
SMTP 34
Send Info Email After Boot 34
SMS 35
Language 35
Update 35
Backup 36
Restore from Backup 37
Status 37
Reboot 39
Network 39
NETWORK MODE 39
LAN / WAN 40
Name server 41
3G Modem 41
Use 3G as Internet Back-up 42
DHCP Server 42
NAT / Routers 43

Firewall 43
DDNS 44
PPTP 44
Cisco VPN 45
OPEN VPN 46
IPSec 48
Ping 49
Status 49
Logout 50

6. Appendix A –Termination and Biasing an RS-485 Network 51

7. Appendix B – List of supported web browsers for the GUI 52

General Information

Purpose of This Manual

This manual is a reference guide for **myBOX** device whose purpose is to:

- explain how to install and wire your device
- give you an overview of the device system
- explain how to set up all necessary settings of the device for a correct operation

Who Should Use This Manual

Use this manual if you are responsible for designing, installing, programming or troubleshooting control systems using this device. You should have a basic understanding of electrical circuitry and familiarity with the relay logic.

Important: **IF YOU DO NOT HAVE THIS NECESSARY KNOWLEDGE, PLEASE OBTAIN AN APPROPRIATE TRAINING BEFORE USING THE PRODUCT!**

Important Information

The examples and diagrams in this manual are included solely for illustrative purposes. In no event will *mySCADA Technologies s. r. o.* be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment. Reproduction of the contents in this manual, in whole or in part, without written permission of *mySCADA Technologies s. r. o.*, is prohibited. *mySCADA Technologies s. r. o.* reserves the right to change this manual at any time without a notification.

Getting Help

For technical support, please visit *SUPPORT* section on our website *http://www.myscada.org*, where you can submit a ticket.

You can also send us an email to *support@myscada.org*. Please do not forget to write the product name as the email subject and provide as much information as possible, so we can best assist you.

It is always possible to view this manual by clicking on  icon, which is located in the upper right corner of the device's user interface (descibed later in the manual). It is strongly recommended to have this manual printed out and kept within reach of maintanance staff personnel.

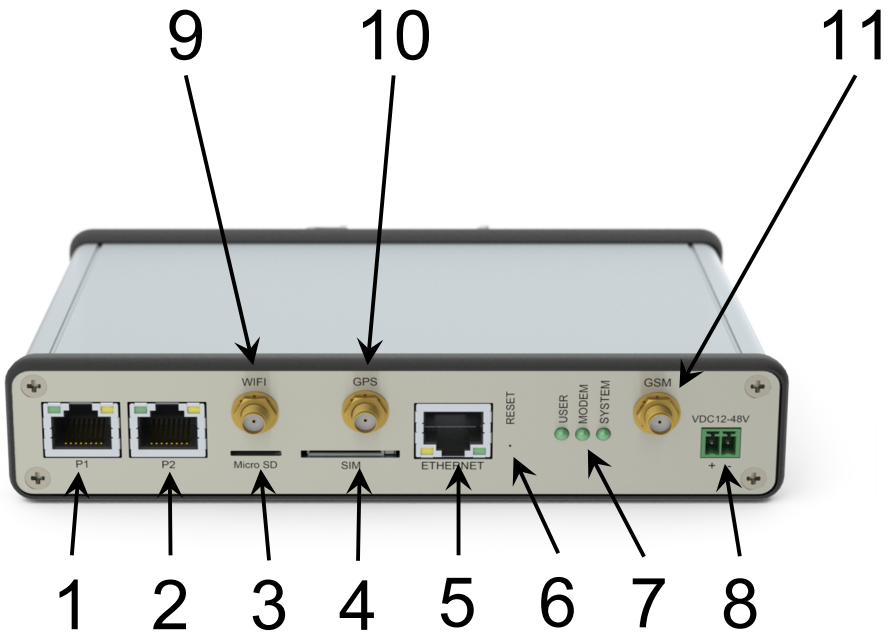
Warranty

All products manufactured by *mySCADA Technologies s. r. o.* ™ are under warranty, regarding defective materials for a period of one year from the date of delivery to the original purchaser.

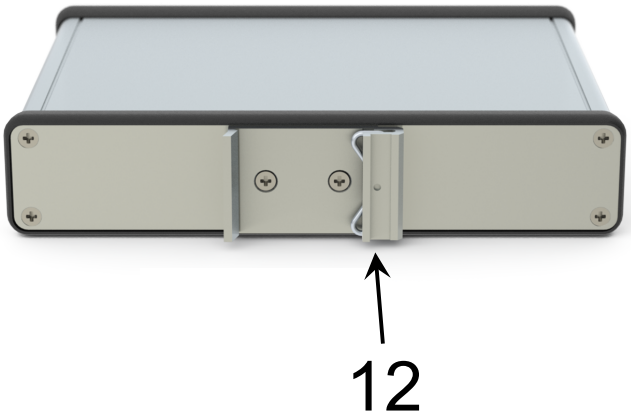
Hardware Overview

Hardware Features

The hardware features of the device are shown in the pictures below:



Feature	Description
1	Port 1 (optional Ethernet port or RS-232/RS-485 ports)
2	Port 2 (optional Ethernet port or RS-232/RS-485 ports)
3	Micro SD card slot
4	SIM card compartment
5	Ethernet port
6	Reset / Switch-off pin hole
7	Status LED indicators
8	Power supply socket
9	Wi-Fi antenna connector SMA (only for Wi-Fi version)
10	GPS antenna connector SMA (only for 3G version)
11	GSM antenna connector SMA (only for 3G version)



Feature	Description
12	DIN Rail holder

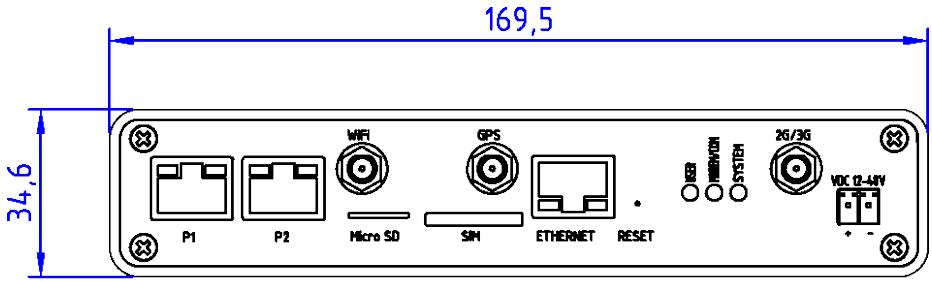
Technical Specifications

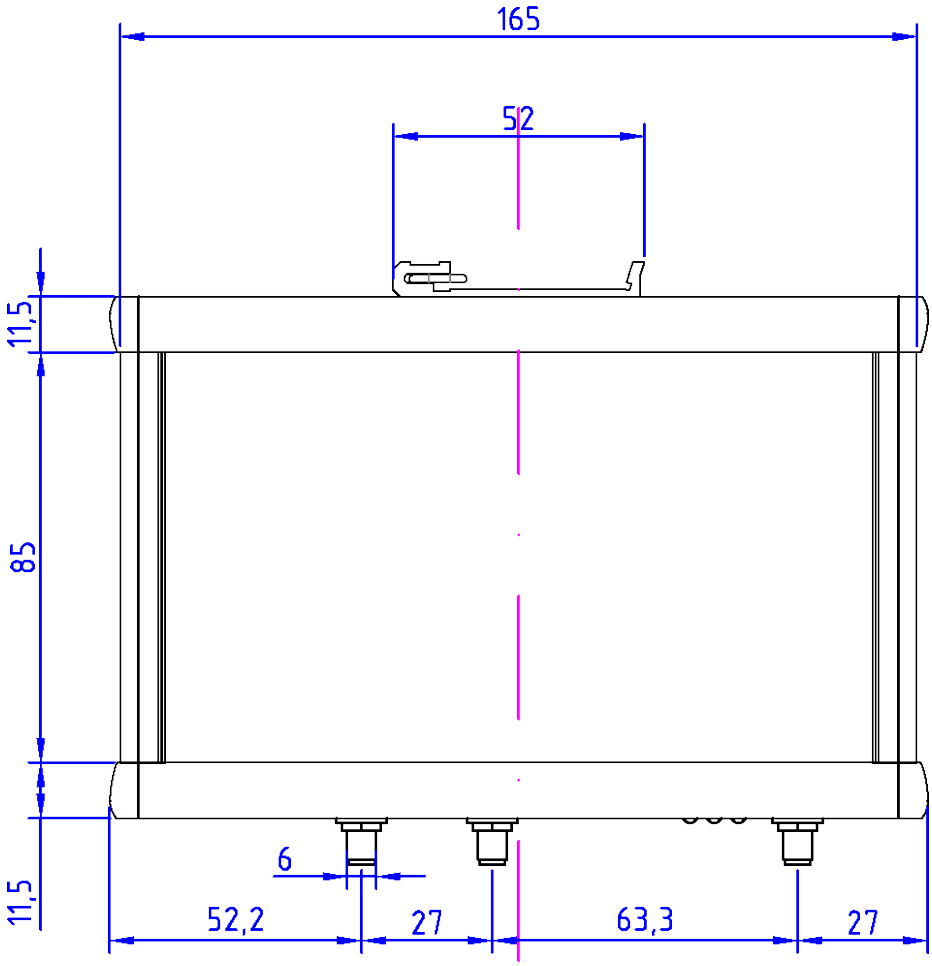
Parameters	
Storage	1 (2) GB Flash NAND Memory Optional SSD Drive
SD Card	Yes
Ethernet 10/100 Mbit	Up to 3 ports
RS-232	Up to 4 ports
RS-485	Up to 2 ports
HW Watchdog	Integrated
Power	12-48 VDC
Size	127 x 33 x 128 mm (W x H x D)
Temperature range	0° to 70° C -40° to 85° C (IT Version) -20° to 70° C (IT with 3G modem)

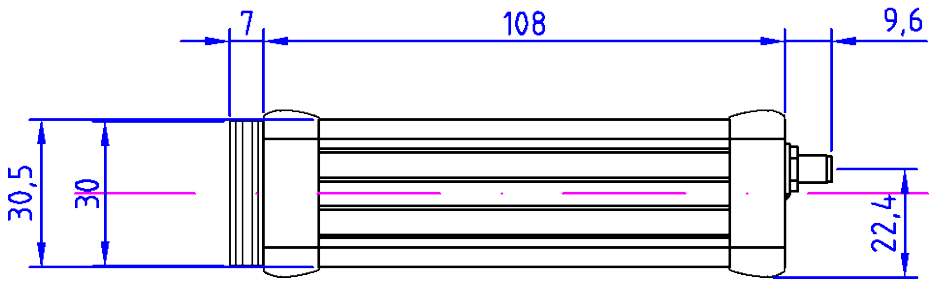
Certification	CE, FCC, RoHS
Ecology	Highly recyclable, RoHS, Ultra low power consumption
Networking	
DHCP	Client and Server
Interface	Routing and bridging supported
Network Address Translation (NAT)	Supported
Firewall	Integrated
Dynamic DNS	Supported
Security	
VPN PPTP	Client and Server
Cisco VPN	Direct import of pcf files
IPSEC	Full support
WiFi Module	
Type	802.11 b/g
Access Point Mode	Yes
No. of simultaneously connected clients	Max 7
Frequency	2.4 GHz WLAN
HW Encryption	WEP, TKIP, and AES
Speed	72.2 Mbps for 20 MHz channel 150 Mbps for 40 MHz channel
Frequency range	USA: 2.400 ~ 2.483GHz Europe: 2.400 ~ 2.483GHz Japan: 2.400 ~ 2.497GHz China: 2.400 ~ 2.483GHz
Certifications	CE, FCC, RoHS
3G Module	
Type	Quad-band HSPA+/HSUPA/HSDPA/WCDMA 2100/1900/900/850 (MHz)

	Quad-band GSM/GPRS/EDGE 850/900/1800/1900 (MHz)
Download Speed	21Mbps
Upload Speed	5.76Mbps
Certifications	CE, FCC, RoHS, IC, GCF, PTCRB, CCC
GPS	
Type	Standalone GPS, A-GPS, GPS Extra
Data format	Server-Side Script readable – JSON
PLC Protocols	
Siemens S7	S7-1200, S7-300, S7-400, …
EtherNet/IP	ControlLogix, CompactLogix, Micrologix 1200, Micrologix 1400, Micrologix 1500, SLC 500, PLC 5, Omron PLCs, …
Modbus TCP	Wago, Schneider, Micrologix, ABB, RTUs, …
Modbus Serial (can be used on any port RS-232 and RS-485)	IPCDAS, ADAM, RTUs, …
Melsec Binary	Melsec-Q, E71 controller type, 3E packets
Toyopuc	Full support with hierarchy
OPC UA	OPC UA client conforming to IEC 62541. Support of plain, crypted and user login.

Dimensions


169,5
34,6
WIFI
GPS
2G/3G
P1
P2
Micro SD
SIM
ETHERNET
RESET
VDC 12-48V


165
52
11,5
85
11,5
6
52,2
27
63,3
27


7
108
9,6
30,5
30
22,4

Installing Your Device

Compliance to EU Directives

This product has the CE mark and is approved for installation within the European Union and EEA regions. It has been designed and tested to meet the following directives:

EMC Directive

This product is tested to meet Council Directive 89/336/EEC Electromagnetic Compatibility (EMC) and the following standards, in whole or in part, documented in a technical construction file:

Test Standards

- EN 61000-4-2 ed.2:2009
- EN 61000-4-3 ed3:2006 + A1 + A2
- EN 61000-4-4 ed2:2005 + A1
- EN 61000-4-5 ed.2:2007
- EN 61000-4-6 ed.3:2009
- EN 55022 ed2:2007 + A1 art. 6, 10

Related Standards

- EN61326-1:2006 EN 61000-6-1 ed2:2007
- EN 61000-6-2 ed3:2006
- EN 61000-6-3 ed2:2007
- EN 61000-6-4 ed2:2007
- EN 55024 ed.2:2011

Installation Considerations

Most applications require installation in an industrial enclosure to reduce the effects of electrical interference and environmental exposure. Locate your device as far as possible from any power lines, load lines, and other sources of electrical noise, such as hard-contact switches, relays, and AC motor drives.

This product is intended for the use in an industrial environment.

Safety Considerations

Safety considerations are an important element of proper system installation. Actively thinking about the safety of yourself and others, as well as the condition of your equipment, is of primary importance.

Preventing Excessive Heat

For most applications, normal convective cooling keeps the device within the specified operating range. Ensure that the specified temperature range is maintained. Proper spacing of components within an enclosure is usually sufficient for heat dissipation. Please take into consideration that in some applications other equipment inside or outside of the enclosure may produce a substantial heat amount. In this case, place blower fans inside the enclosure to assist in air circulation and reduce “hot spots” near the device. Additional cooling provisions might be necessary when high ambient temperatures are encountered.

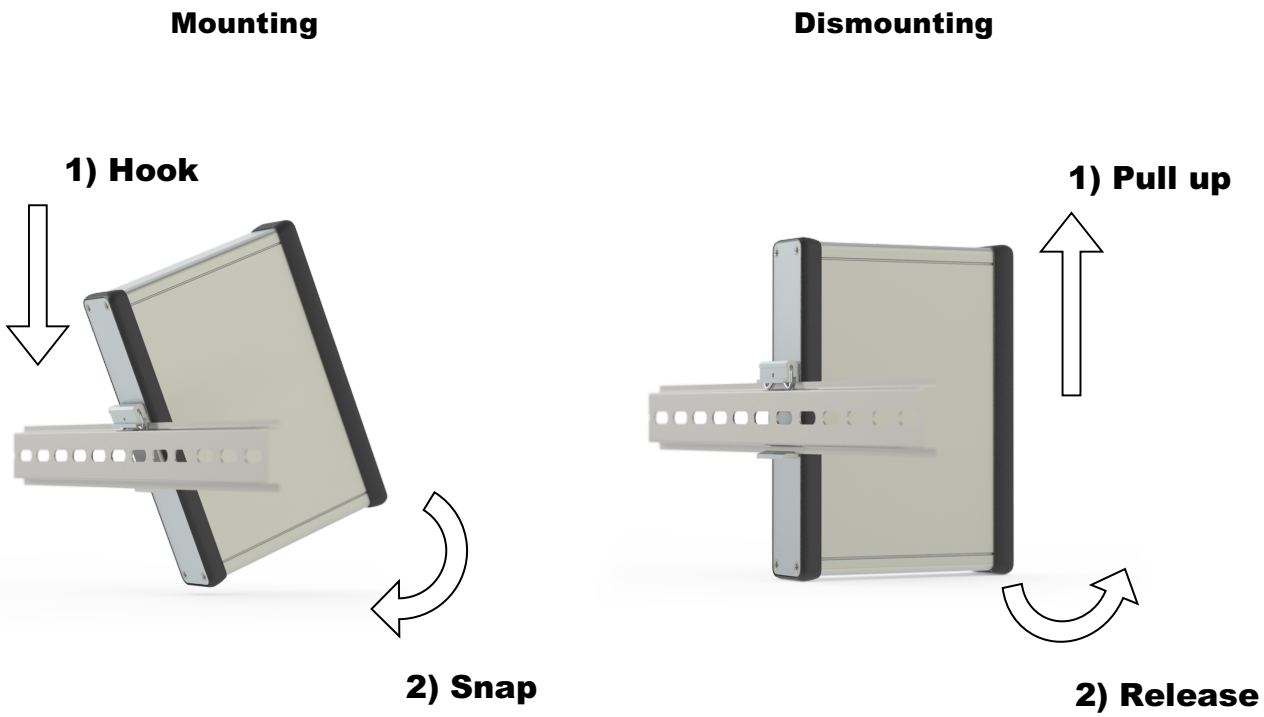
Do not bring in unfiltered outside air. Place the device in an enclosure to protect it from a corrosive atmosphere. Harmful contaminants or dirt could cause improper operation or damage to the components. In extreme cases, you may need to use air conditioning for protecting the device against the heat build-up within the enclosure.

Mounting the Device

This device is suitable for use in an industrial environment when installed in accordance to these instructions. It can be mounted vertically or horizontally. You should provide min. 50 mm (approx. 2 inches) of space on all sides of the device for adequate ventilation. Keep in mind to maintain spacing from enclosing walls, wire ways, adjacent equipment, etc.

DIN Rail Mounting

The device can be mounted to EN50022-35x7.5 or EN50022-35x15 DIN rails. There is no need for using any screwdrivers or tools. Simply hook the top slot over the DIN rail and then, while pressing the device down against the top of the rail, snap the bottom of the device into position. To remove your controller from the DIN rail press the bottom jutting part of the holder (you may need a screw driver to do so) and release the device from the DIN rail by carefully pulling it up and towards you.

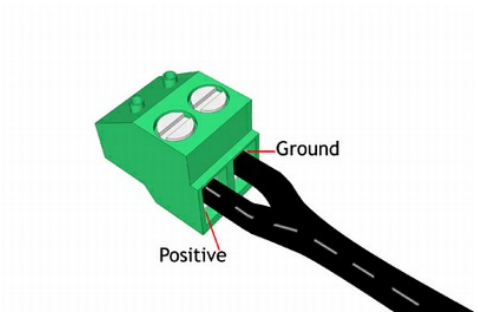


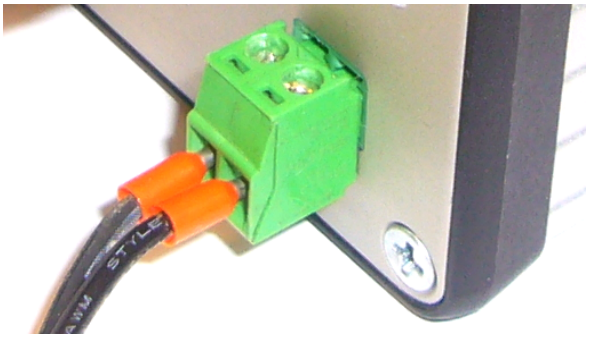
Power Wiring and Device Start-Up

Before you install and wire any device, make sure to disconnect the electric power from the system! Strip the ends of the cable so it could be slipped into the supplied green connector (as shown on the picture bellow). Do not forget to check the correct polarity! Tighten the terminal screw, using a small flat-blade screwdriver.

PLEASE KEEP IN MIND THE POWER INPUT VOLTAGE MUST ALWAYS BE

WITHIN THE RANGE OF 12~48V DC!





When the wires are attached plug in the green connector to the green socket, located in the bottom right corner of the front panel and plug it into the electrical socket. The device automatically starts up and performs the initialization process, indicated by the LED status indicators.

LED indicators

SYSTEM - system ready

MODEM/COM - modem/serial status

USER – user control LED

Getting Online Help from mySCADA

Should you need help with setting up your myBOX, you are welcome to use our online helpdesk. Please write to *support@myscada.org* first to schedule the online help time.

Prior to the set online help, please make sure your box is connected to the Internet. Press and hold the RESET button until SYSTEM led starts blinking. Now, the box should be securely connected to our *mySCADA* helpdesk through a secure VPN service and *mySCADA* support team can access your device and help you online.

Reset to Default Settings

If neccessary, the device can be reset to the factory settings by the following procedure:

1) Power the unit on (unplug and plug the power cord)
2) Wait for the SYSTEM led to light on
3) Press and hold the RESET button (use a paper clip to do so)
4) When the USER led lights on, release the RESET button
5) Now the system restores into default, please wait approx. 5 minutes for reboot

DO NOT INTERRUPT THIS PROCEDURE AS THE UNIT COULD BECOME BLOCKED!

!!! Attention: Once the device is reset, all saved data stored in the internal memory will be erased !!!

Communication Connections

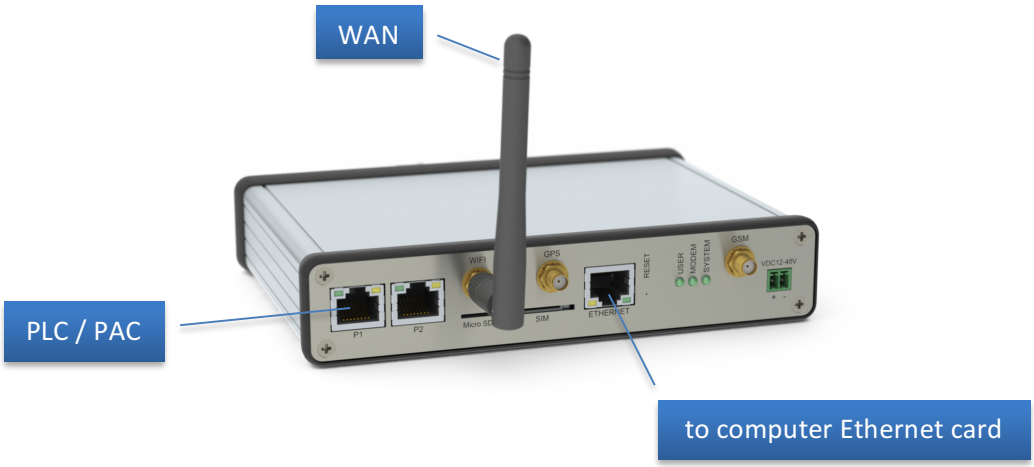
This device provides the following communication channels:

- Ethernet port, RJ-45
- Additional Ethernet port, RJ-45 (2x)
- Optional set of 2x RS-232 and 1x RS-485 ports

This device supports the following industrial communication protocols:

- EtherNet/IP
- Modbus TCP
- Siemens S7 (S7-300/400/1200 syntax)
- Melsec Q3
- Toyopuc
- OPC UA - OPC Unified Architecture driver
- KNX

A typical network topology is pictured below:



Once the device is connected to a local area network, it can be easily accessed and configured via a web browser installed on your computer. After entering a valid IP address in your web browser you will see the configuration interface of the device. The default IP address is set to:

192.168.13.20

You need to enter the correct username and password to access the advanced system settings. Default login details are:

user name: *admin*

password: *admin*

DO NOT FORGET TO CHANGE THE DEFAULT PASSWORD AFTER YOU LOG IN TO AVOID ANY UNAUTHORIZED ACCESS TO YOUR DEVICE!!

All components and settings of the configuration interface are described later in this manual.

Connecting to Networks via Ethernet Interface

The Ethernet communication channel allows your device to be connected to a local area network for various devices, providing 10 Mbps/100Mbps transfer rate. Shielded 6E category twisted-pair 10/100Base-T cables with RJ-45 connectors are only supported. The maximum cable length between the Ethernet port of the device and the 10/100Base-T port on an Ethernet router/switch (without repeaters or fiber) should be 100 m (323 ft). However, in industrial application the cable length should be kept to a minimum.

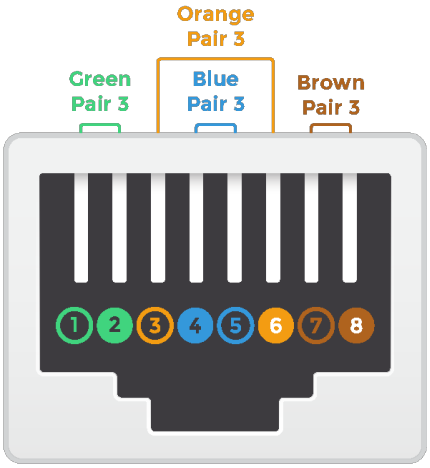
The connections are made directly from the device to an Ethernet router or switch via 8-wire twisted-pair straight-through cables. The following Ethernet settings are supported (mode selection is automatic):

- 10 Mbps half duplex or full duplex
- 100 Mbps half duplex or full duplex

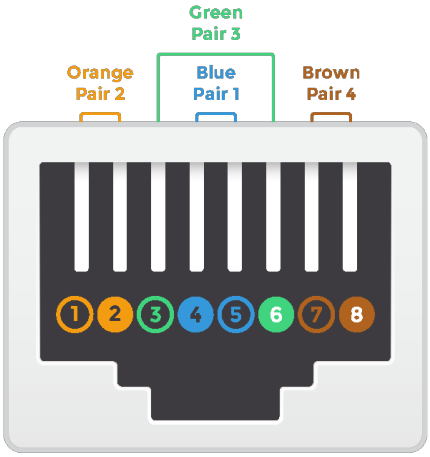
The Ethernet cabling with straight-through method is recommended as below.

PLEASE MAKE SURE YOU DO NOT MAKE AN INCORRECT CONNECTION!

Pin	Pin Name	Cable Color
1	Tx+ Transmit Data	Orange/White
2	Tx- Transmit Data	Orange
3	Rx+ Receive Data	Green/White
4	No used by 10/100Base-T	Blue
5	No used by 10/100Base-T	Blue/White
6	Rx- Receive Data	Green
7	No used by 10/100Base-T	Brown/White
8	No used by 10/100Base-T	Brown



RJ-45 JACK
EIA/TIA 568A STANDARD

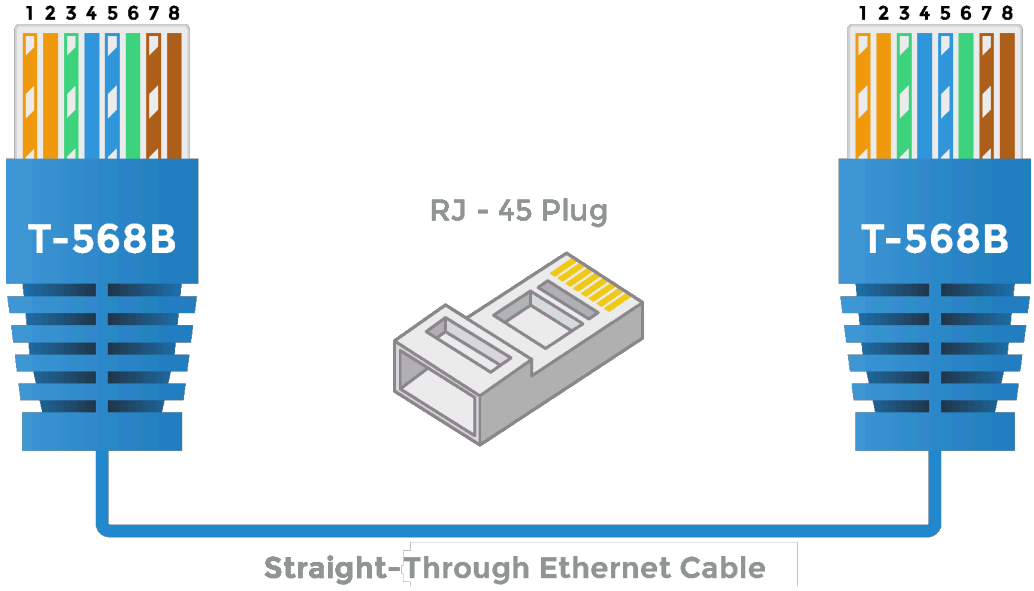


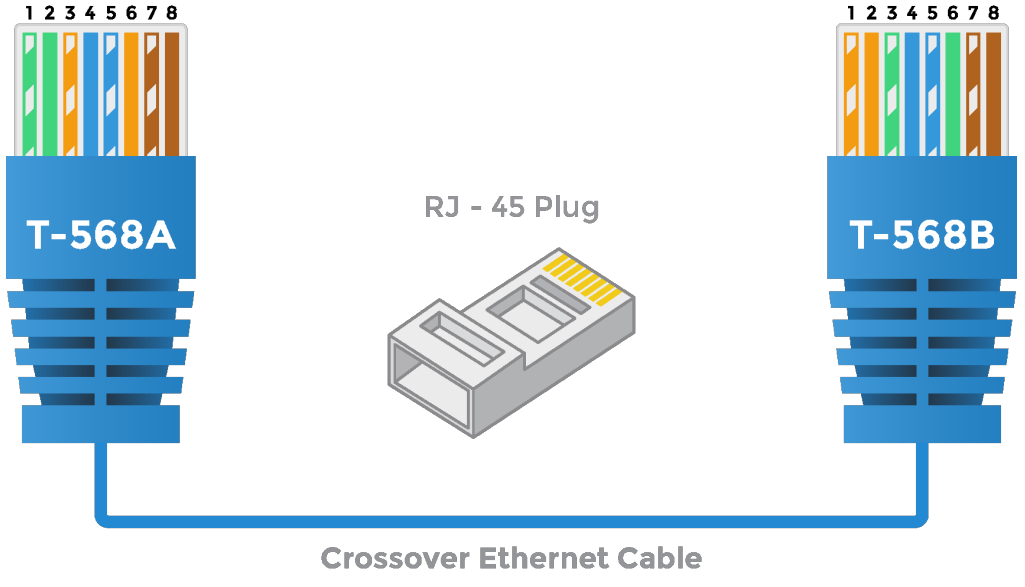
RJ-45 JACK
EIA/TIA 568B STANDARD

Useful Information on Ethernet Wiring:

The most common wiring for RJ-45 cables is the "**straight-through**" cable, which means that the pin 1 of the plug on one end is connected to the pin 1 of the plug on the other end. The straight through RJ-45 cable is commonly used for connecting network cards with hubs on 10Base-T and 100Base-Tx networks. On network cards, the pair 1-2 serves as a transmitter, and the pair 3-6 as a receiver. The other two pairs are not used. On hubs the pair 1-2 is the receiver and 3-6 the transmitter. It may be best to wire your cables with the same color sequence. In this cable layout, all pins are wired one-to-one to the other side. The pins on the RJ-45 connector are assigned in pairs and every pair carries one differential signal. Each line pair has to be twisted.

In a small network with only two computers the use of the "**crossover**" RJ-45 cable is necessary, where the transmitting and receiving lines on both RJ-45 connectors are cross connected. The color-coding for the crossover RJ-45 cable has been defined in the EIA/TIA 568A standard. In the crossover cable layout you should remember that one end is normal and the other end has the crossover configuration.





Connecting to Networks via RS-232/485 Interface

Note that this chapter is applicable only if the optional "**Serial ports**" kit has been purchased with the device.

The kit comprises of three serial ports, described in the table below:

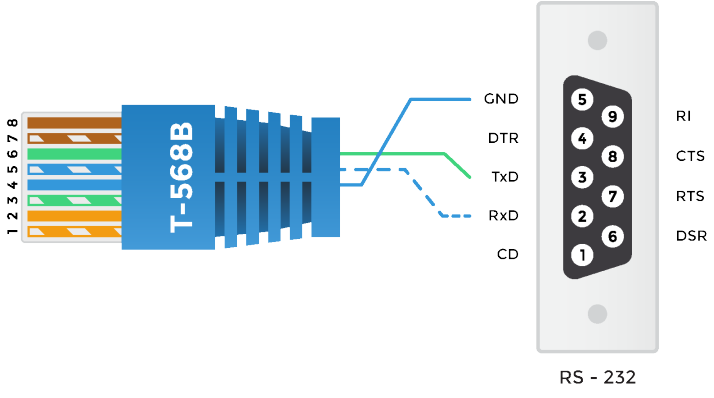
Port Name	Port Type	Connection
COM1	RS-232	EIA/TIA-561
COM2	RS-232	Proprietary
RS-485	RS-485	Proprietary

All these three serial ports are located in the "Port 1" of the device (physically RJ-45 Ethernet port). The connection scheme of the "Port 1" is as follows:

RJ-45 Pin	Pin Name	Description
1	GND	Signal Ground
2	RxD	COM 2 Receive pin
3	TxD	COM 2 Transmit pin
4	GND	Signal Ground
5	RxD	COM 1 Receive pin
6	TxD	COM 1 Transmit pin
7	A	RS-485 A also denoted as (-)
8	B	RS-485 B also denoted as (+)

Using the RS-232 Interface

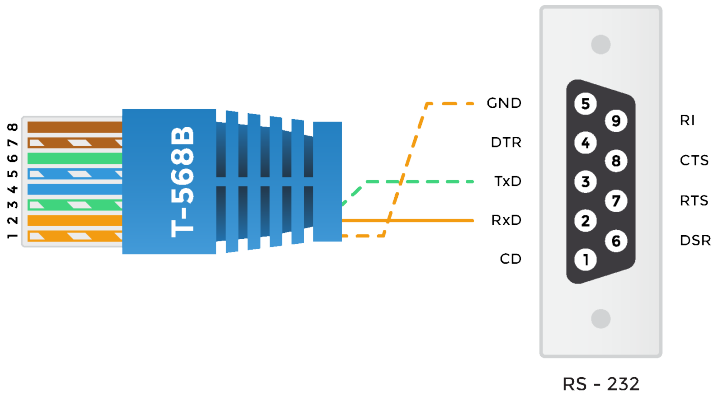
COM1 is routed according to **EIA/TIA-561 Pin Layout** (serial interface via 8-pin connector) while using only Rx,Tx and Ground pins. Every serial device connected to the port COM1 must have an interface cable conforming to EIA/TIA-561 standard. On one end this cable must have a male RJ-45 plug and on the other end it must have a connector fitting into your serial device. The diagram shows the pin connections for the COM1 conversion cable from RJ-45 "Port 1" into regular "CANON DB-9" connector.



COM 1 (EIA/TIA-561) Pin Layout Diagram with DB9connector

RJ-45 Pin	Pin Name	CANON DB-9 Pin	Function
1	GND	Do Not Use	Do Not Use
2	RxD	Do Not Use	Do Not Use
3	TxD	Do Not Use	Do Not Use
4	**GND**	**5**	**Signal Ground**
5	**RxD**	**2**	**Receive pin**
6	**TxD**	**3**	**Transmit pin**
7	A	Do Not Use	Do Not Use
8	B	Do Not Use	Do Not Use

COM2 is using only Rx,Tx and Ground pins. Every serial device connected to port COM1 must have an interface cable that conforms to the defined pinout. On one end this cable must have a male RJ-45 plug, on the other end it must have a connector that fits into your serial device. The diagram shows the pin connections for the COM2 conversion cable RJ-45 “Port 1” to regular “CANON DB-9” connector.

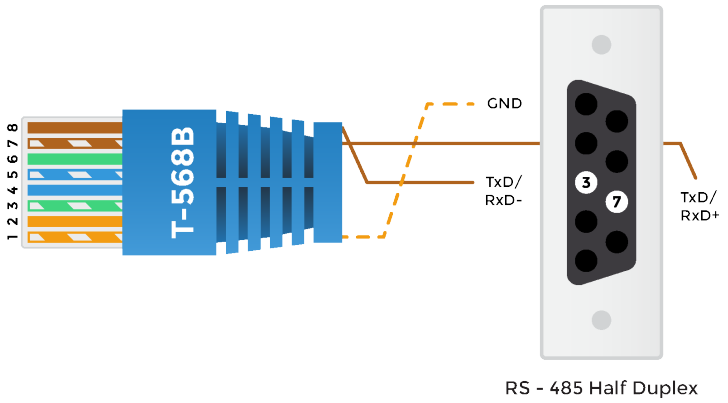


COM 2 Pin Layout Diagram with DB9 connector

RJ-45 Pin	Pin Name	CANON DB-9 Pin	Function
1	**GND**	**5**	**Signal Ground**
2	**RxD**	**2**	**Receive pin**
3	**TxD**	**3**	**Transmit pin**
4	GND	Do Not Use	Do Not Use
5	RxD	Do Not Use	Do Not Use
6	TxD	Do Not Use	Do Not Use
7	A	Do Not Use	Do Not Use
8	B	Do Not Use	Do Not Use

Using the RS-485 Interface

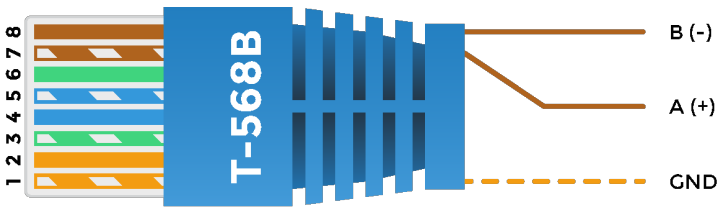
The RS-485 port has tri-state capabilities and allows a single pair of wires to *share*, *transmit* and *receive* signals for half-duplex communications. This "two wire" configuration (note that an additional ground conductor should be used) reduces the cabling cost. RS-485 devices may be internally or externally configured for two wire systems. RS-485 port is internally configured and thus it simply provides A and B connections (sometimes labeled "-" and "+").



RS485 Pin Layout Diagram with DB9 connector

RJ-45 Pin	Pin Name	CANON DB9 Pin	Function
1	**GND**	**5**	**Signal Ground**
2	RxD	Do Not Use	Do Not Use
3	TxD	Do Not Use	Do Not Use
4	GND	Do Not Use	Do Not Use
5	RxD	Do Not Use	Do Not Use
6	TxD	Do Not Use	Do Not Use
7	**A**	**3**	**(-)**
8	**B**	**7**	**(+)**

Alternatively A, B and GND wires can be connected directly to the PLC or device without a need of using BD-9 connector as such.



RS485 Pin Layout Diagram

Connecting to Networks via Wireless 3G Interface

Please note this chapter is applicable only for theh3G device versions, equipped with a wireless modem.

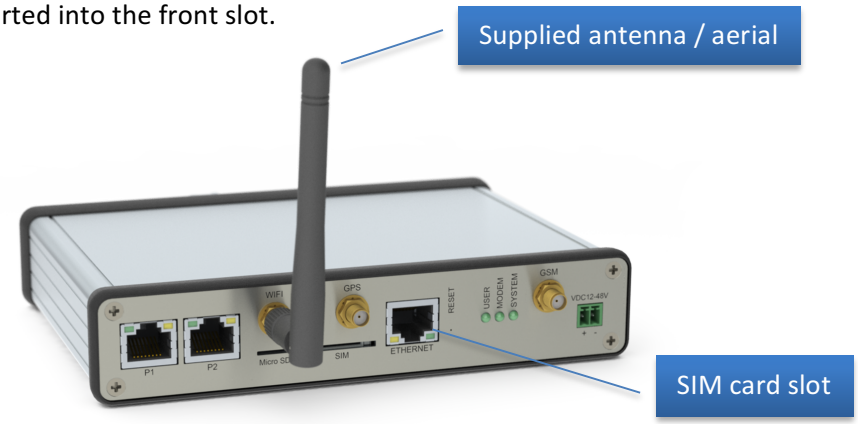
Connecting your device via a mobile network virtually allows for an access from anywhere in the world. This can be done on condition that firstly, the device is installed in an area with a mobile network access. Secondly, the device has contains a SIM card with an active mobile data plan (contact your local mobile network provider for more information).

The built-in wireless modem supports the following technology for mobile networks:

- GSM - Global System for Mobile Communications
- GPRS - General Packet Radio Service
- EDGE - Enhanced Data rates for GSM Evolution
- UMTS - Universal Mobile Telecommunications System, aka 3G
- HSDPA / HSUPA - High-Speed Downlink/Uplink Packet Access, aka 3G+
- LTE - a 4G mobile communications standard

PLEASE MAKE SURE THE POWER SUPPLY TO THE DEVICE IS COMPLETELY DISCONNECTED BEFORE HANDLING THE SIM CARD"

The SIM card can be inserted into the front slot.



It is recommended that you use the supplied aerial/antenna, however thank to the standard SMA connector you may use any other GSM antenna available on the market.

As soon as the device is powered on, the internal wireless modem starts to automatically login into a preset APN (Access Point Name). Therefore, the correct APN must be set for proper operation – this can be also done through the web user interface, which is described later in this manual. By default the APN is set as "***internet***".

Access Point Mode with Wireless Wi-Fi Integrated Card

PLEASE NOTE THE FOLLOWING INFORMATION APPLIES ONLY TO THE WI-FI VERSIONS OF myBOX, WHICH ARE EQUIPPED WITH THE WIRELESS MODEM.

myBOX can be equipped with a Wi-Fi access point card. If activated, you can connect to your device via Wi-Fi networks. Please note that standard protection can be applied for security reasons and there is a maximum of 7 simultaneous connections that can be achieved.

Graphical User Interface

The graphical user interface (GUI) of this device is based on standard web pages, meaning that any web browser installed on your computer, such as MS Internet Explorer, Apple Safari, Firefox, Chrome, etc. can view it. To access the GUI simply enter the correct IP address of the device into the address bar in your web browser.

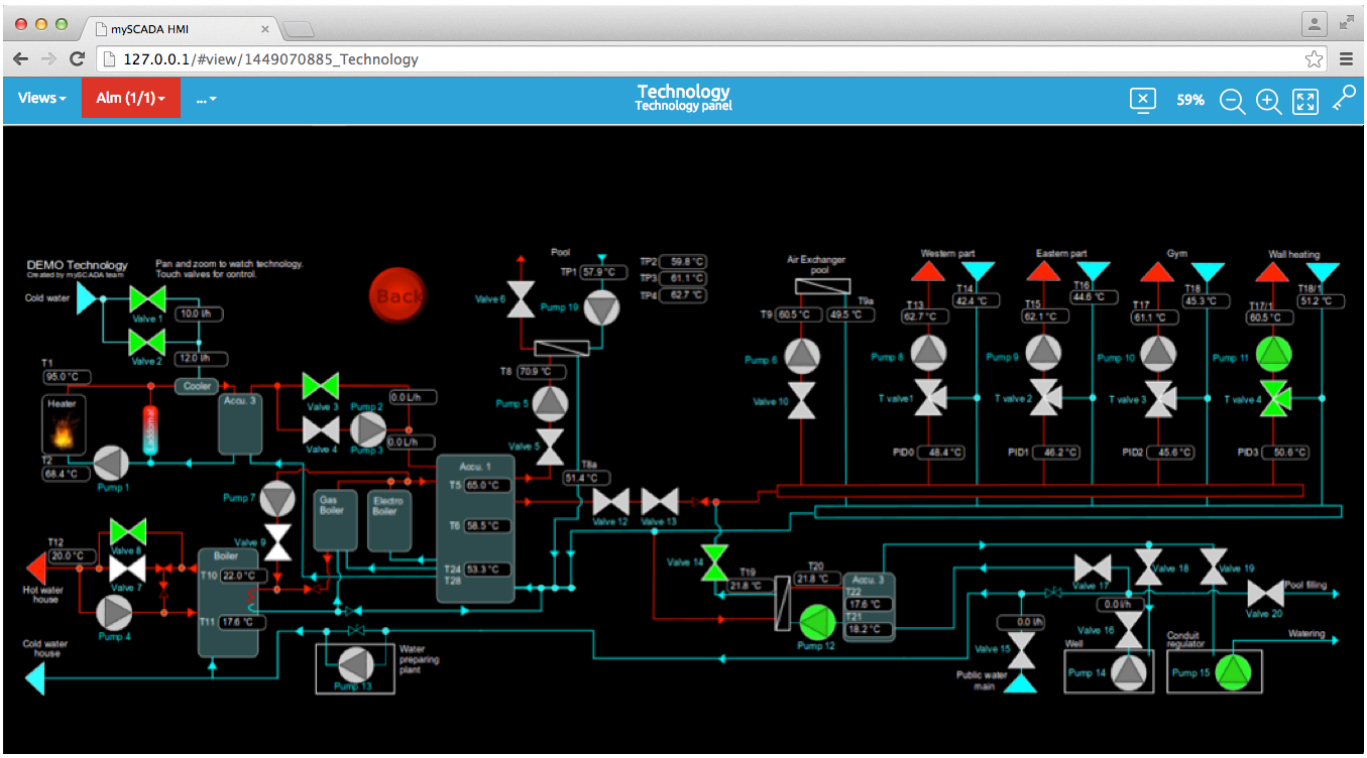
The GUI is divided into two main parts (levels):

1. **HMI** – allows viewing HMI screens and logged data (data-logs and alarms)
2. **Administration** – after successful login, various advanced settings can be set and adjusted, such as network, VPNs, accesses, SMTP, etc.

In this chapter the **HMI** level is described, while the **Administration** level is described later in the chapter "*GUI – Admistration level*".

Main Screen - SCADA/HMI Views, Trends & Alarms

Creating a visual representation of the system that myBOX should be monitoring simplifies the project management. With respect to the capability of mySCADA to create mimic graphics with animations, observation of your system operations can be done via a web browser installed on your computer.



The main toolbar is located in the upper part of the main screen and is divided into these parts:

1. **Main menu** in which you can switch between available visualization views, trends and active alarms stored in the particular myBOX unit.

2. **Zoom slider** – provided there is a visualization showed in the web browser screen, it can be easily resized by sliding the zoom bar. When a view is large, it is possible to "zoom in" it in order to see the visualization view in more details. Drag the slider to the left to zoom out (shrink), or to the right to zoom in (enlarge). The actual level of zoom is indicated by percent (10% to 1000%).

   ***TIP**: You can also zoom using the mouse scroll wheel or a track pad.*

3. **General menu settings** – By clicking on the monitor icon the right corner of the main toolbar, you can login into the settings part of the myBOX.

On the left and right of the zoom slider, there are three icons whose functions are described below:

Icon	Description
	By clicking on this icon you will get general information about the current loaded visualization view and its associated tags.
	Allows login into HMI for registered users. Depending on the set rights, the logged user can view HMI, write values, acknowledge alarms and also set up advanced configuration. Users' accounts creation and management is described in manual for myPROJECT Designer.

Visualization Views

The possibilities are virtually endless when it comes to choosing how you wish to represent the overall design of your system. Simple page elements are incorporated into a complete design and depending on the amount of effort put into the fabrication of the representation, a very detailed system imitation can be achieved.

Such detailed visualization screens can be easily created by a powerful sotware tool ***myPROJECT Designer*** which is available for downloading at www.myscada.org free of charge.

Once there is a visualization view showed, you can operate the zoom in two options (this is available in menu Mode):

Icon	Description
	Fit to page – a view is zoomed to show its entire content in the window
	Manual size – a view can be resized using the zoom slider

***Tip**: You can also easily resize the view by the mouse scrolling wheel.*

If you press **SHIFT+D** you can see detailed info about the visualisation. This page contains global info (such as number of definied tags, refresh period …), list of loaded tags and list of variables with their current values. It may be useful when you are debugging your project.

Info about view buttons

View scripts info

View script status	December 29, 2015 15:13:31 OK
function init() status	December 29, 2015 15:13:31 OK
function periodic() status	December 29, 2015 15:13:43 OK

Connections

Connection with id 0			
Tag	Value	Loaded from stack	Status
val@script	1	December 29, 2015 15:13:43	OK

View script variables

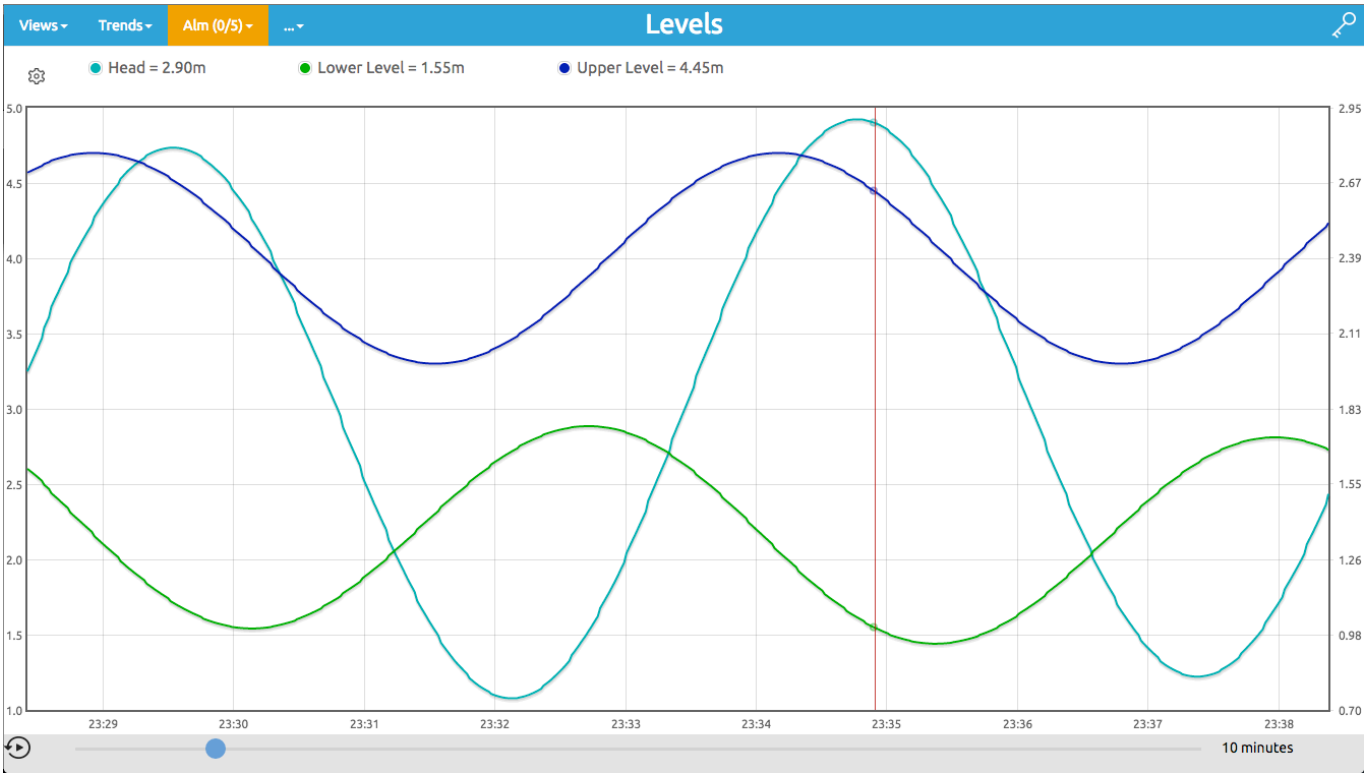
Type	Name	Value

System variables

Name	Value
myscadaRunCount	12
myscadaLoggedUser	"admin"
myscadaLoggedUserLevel	9
myscadaActiveAlarmsCount	0
myscadaNonAckAlarmsCount	0

Trends

Visualization of trends can be vital when monitoring your system. Trends allow tag values to depict certain, potentially dangerous patterns. For a correct trend operation, the recording of the current and previous values is needed. The displayed data are loaded from the inner unit memory.



There are two possible ways how to visualize trends:

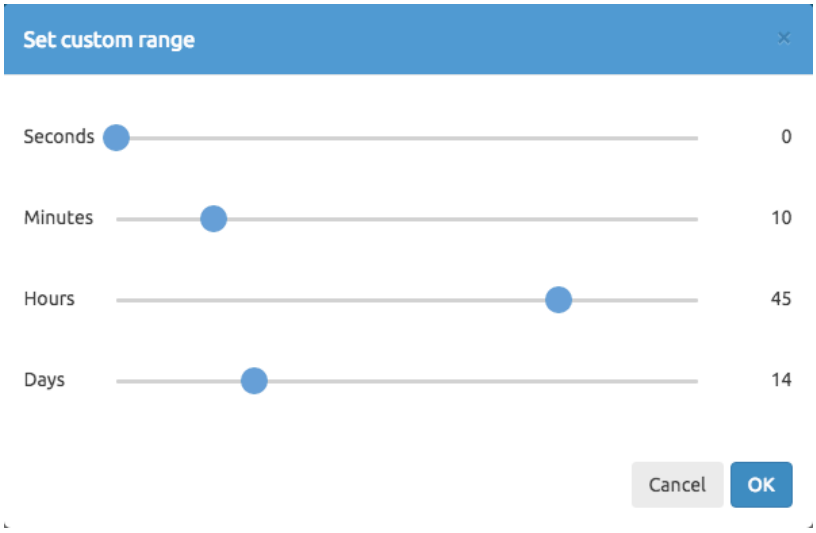
1. **Online** - data is shown starting from the current value
2. **History** - data is shown from a certain entered date

Online Mode:

Time range showed in a trend can be easily changed in the bar bellow the actual graph. Drag the slider to change the time range shown (from 1 minute up to 1 year)

Setting custom time interval:

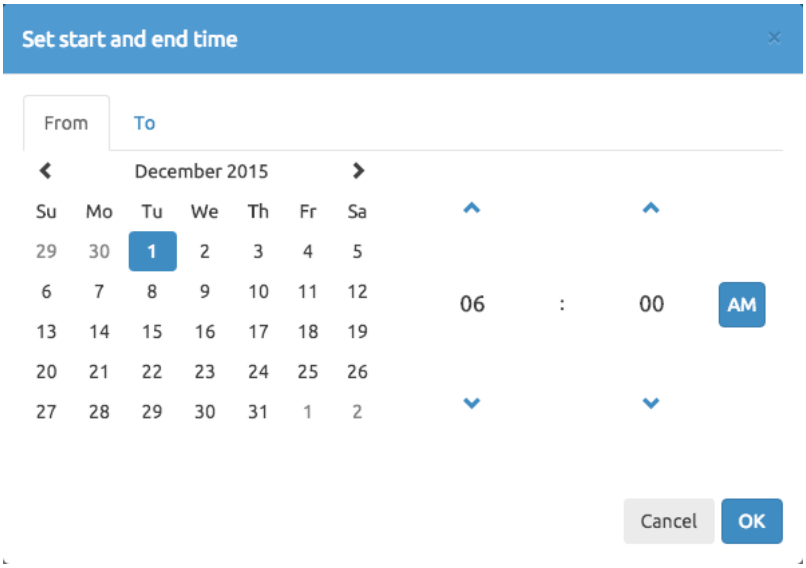
When you click on a time interval on the right, you will be presented with a dialog enabling you to set up custom time interval for viewing.



History Mode:

Switch to the history mode is done by clicking on the timer icon in the lower left corner.

In this mode, you can specify a date range in which data will be shown - click on a date to set:



By clicking on the left and right arrows, it is possible to change the date in accordance with an already set Time range. Clicking on the very left arrow will show first records available, clicking on the very right icon will show the latest records available. Again, by clicking on the time interval on the right, you will be presented a dialog enabling you to set up a custom viewing time interval.

***TIP**: The maximum of 10 000 values can be shown in one trend at one time. If there is more than 10 000 values in a selected Time range, the system will ask you to reduce the current Time range.*

Alarms

The crucial part of monitoring your system is being notified immediately when something unusual occurs i.e. tags reaching an undesired status will trigger alarms. The information regarding this dangerous and/or important status will be delivered immediately to the device for timely and appropriate actions to take place.

Alarms can signal that some device or process has ceased operating within acceptable, predefined limits, or they can indicate breakdown, wear, or a process malfunction. Often, it is also important to have a record of the alarms and whether they have been acknowledged.

You can also set an acousting warning, indicating that the alarm reached its severity level.

Online Alarms

The alarm window allows the operator to perform a complete management of the technology alarms. The window allows you to visualize the alarms present in the technology or in a restricted area of the technology.

The alarm window displays all the alarms of technology or only a set of them, arranged by areas defined by the programmer. If necessary, the operator can select the desired area by clicking on the filter button and filling the area name.

Alarm Acknowledgement

The operator can acknowledge HMI alarms displayed in the alarm window. Acknowledging the alarms does not correct their causes, but indicates that the operator is aware of them.

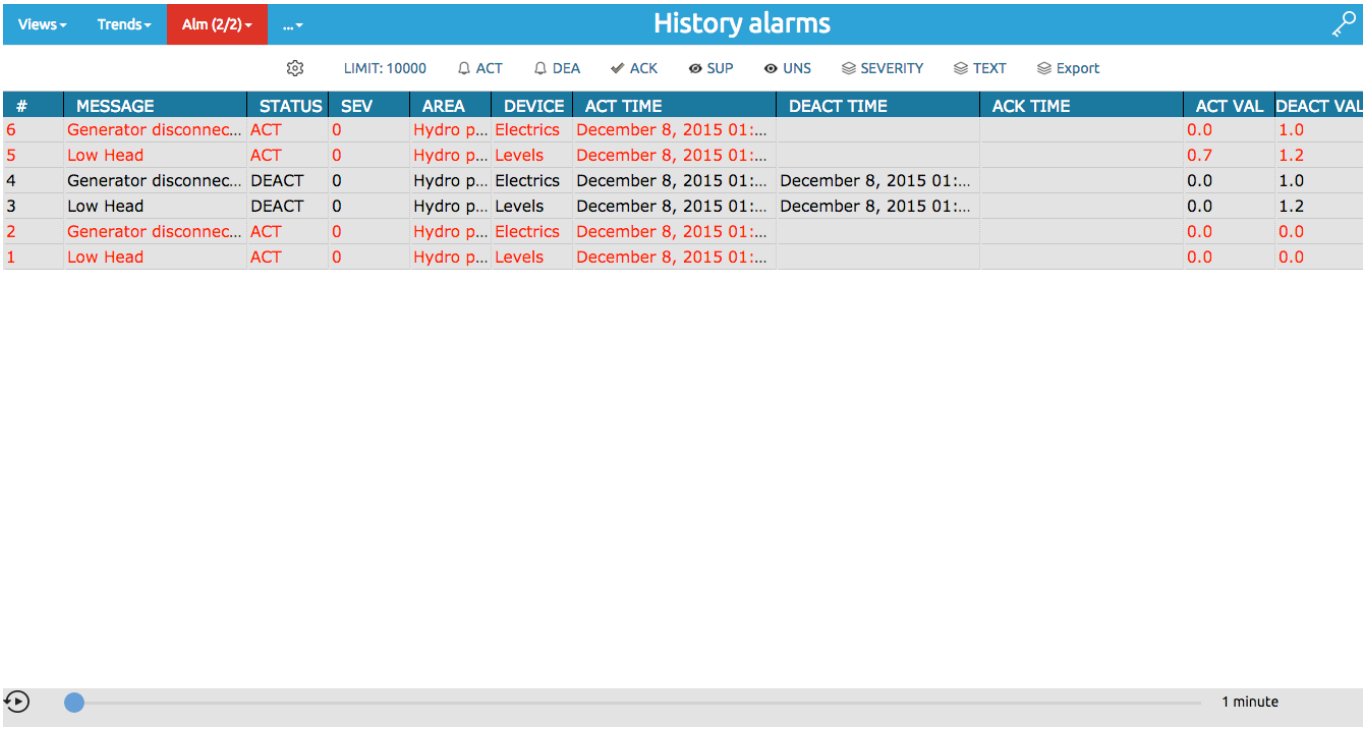
Sorting and Filtering in run-time

By default, the alarm information in the alarm summary is firstly sorted by the date and time, then by severity and the area name.

This means that alarms are presented in a chronological order i.e. if two or more alarms have the same time and date, they will be presented in order of severity; if any alarms have the same time and date and the same severity, then they will be sorted by the area name

History Alarms

mySCADA engine automatically logs your alarms into history. Every alarm action is logged with all relevant data, such as current time (with precision to 1 millisecond). You can browse through the alarm history in the Alarm History Window. Aside of direct data browsing, you can also filter your data based on criteria and export the shown alarms history into MS Excel.



Severity

Alarms can range in severity from 0 (the most severe) up to 4 byte unsigned integer value (the least severe), to indicate different levels of importance. For example, an alarm with severity of 10 might be warning that a tank is half full of liquid, while severity of 5 indicates that the tank is about to overflow. Both alarms monitor the same tag but have different severity levels.

When you are setting up the alarm severity, you need to specify what the severity levels mean and what actions they will trigger. Severity determines the order in which alarms are displayed in the alarm banner.

Alarm Areas

The alarms can be grouped into different areas so that they can be displayed in the alarm window, based on the area they belong to. This may be helpful for dividing the alarms by the plant zones they come from.

Message

The alarm messages report information about alarms.

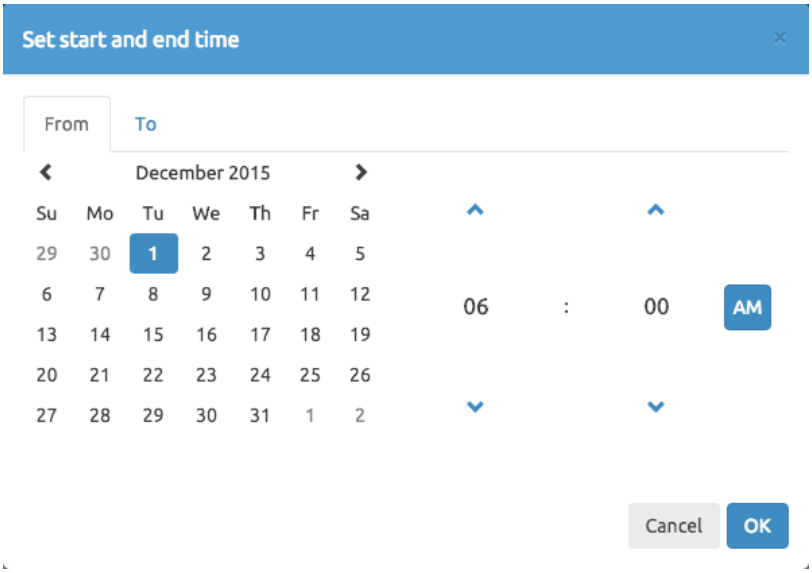
Device

You can define multiple alarms for a single device. In the live alarm view or during browsing of the alarm history you can filter your data, based on a device value.

Changing Date & Time

To change the date or intervals of shown results, use the bottom time toolbar.

You can specify the date range in which data will be shown - click on the date to set:



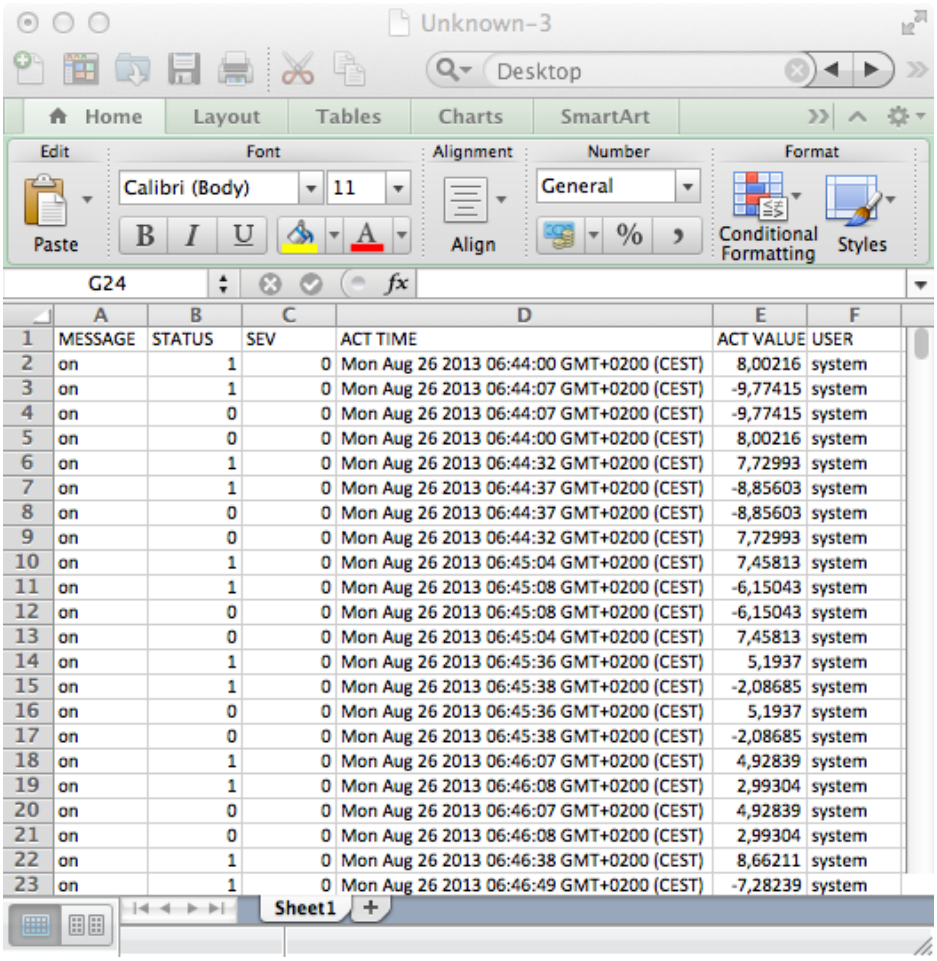
By clicking on the left and right arrows, it is possible to change the date in accordance with already set Time range. Clicking on the very left arrow will firstly show the records available, clicking on the very right icon will show the latest records available.

By clicking on the time interval on the right, you will be presented a dialog enabling you to set up a custom time interval for viewing.

***TIP**: The maximum number of shown rows is limited by the LIMIT button, located on the top bar. You can change this value any time during viewing the data.*

Export to MS Excel

Aside of the data preview, you can export the data into MS Excel. To do so, press the export button located on the top tool bar.



	A	B	C	D	E	F
1	MESSAGE	STATUS	SEV	ACT TIME	ACT VALUE	USER
2	on	1	0	Mon Aug 26 2013 06:44:00 GMT+0200 (CEST)	8,00216	system
3	on	1	0	Mon Aug 26 2013 06:44:07 GMT+0200 (CEST)	-9,77415	system
4	on	0	0	Mon Aug 26 2013 06:44:07 GMT+0200 (CEST)	-9,77415	system
5	on	0	0	Mon Aug 26 2013 06:44:00 GMT+0200 (CEST)	8,00216	system
6	on	1	0	Mon Aug 26 2013 06:44:32 GMT+0200 (CEST)	7,72993	system
7	on	1	0	Mon Aug 26 2013 06:44:37 GMT+0200 (CEST)	-8,85603	system
8	on	0	0	Mon Aug 26 2013 06:44:37 GMT+0200 (CEST)	-8,85603	system
9	on	0	0	Mon Aug 26 2013 06:44:32 GMT+0200 (CEST)	7,72993	system
10	on	1	0	Mon Aug 26 2013 06:45:04 GMT+0200 (CEST)	7,45813	system
11	on	1	0	Mon Aug 26 2013 06:45:08 GMT+0200 (CEST)	-6,15043	system
12	on	0	0	Mon Aug 26 2013 06:45:08 GMT+0200 (CEST)	-6,15043	system
13	on	0	0	Mon Aug 26 2013 06:45:04 GMT+0200 (CEST)	7,45813	system
14	on	1	0	Mon Aug 26 2013 06:45:36 GMT+0200 (CEST)	5,1937	system
15	on	1	0	Mon Aug 26 2013 06:45:38 GMT+0200 (CEST)	-2,08685	system
16	on	0	0	Mon Aug 26 2013 06:45:36 GMT+0200 (CEST)	5,1937	system
17	on	0	0	Mon Aug 26 2013 06:45:38 GMT+0200 (CEST)	-2,08685	system
18	on	1	0	Mon Aug 26 2013 06:46:07 GMT+0200 (CEST)	4,92839	system
19	on	1	0	Mon Aug 26 2013 06:46:08 GMT+0200 (CEST)	2,99304	system
20	on	0	0	Mon Aug 26 2013 06:46:07 GMT+0200 (CEST)	4,92839	system
21	on	0	0	Mon Aug 26 2013 06:46:08 GMT+0200 (CEST)	2,99304	system
22	on	1	0	Mon Aug 26 2013 06:46:38 GMT+0200 (CEST)	8,66211	system
23	on	1	0	Mon Aug 26 2013 06:46:49 GMT+0200 (CEST)	-7,28239	system

Data-Log Views

You can log eventually any data or information available in *mySCADA*. For the user convenience and easy access the data are grouped into so called "Data-Logs". You can think of data-logs as of similar data collections. It can be e.g. a set of temperatures read each second from the PLC, motor start-up voltage and the current logged each 100 milliseconds, run hours of process, operators' actions or computed production statistics.

Each data log can have defined multiple Data-Log Views. The data-Logs are thus viewed in a tabular form represented by one or multiple Data-Log Views. Data-Log Views are accessible from the main menu by clicking on "**…**" button.

There are two possible ways how to operate Data-Log views:

1. **Online** - data is shown starting from the current value
2. **History** - data is shown from a certain entered date

Online Mode:

Time range showed in a data-log can be easily changed in the bar bellow the actual graph. Drag the slider to change the time range shown (from 1 minute up to 1 year)

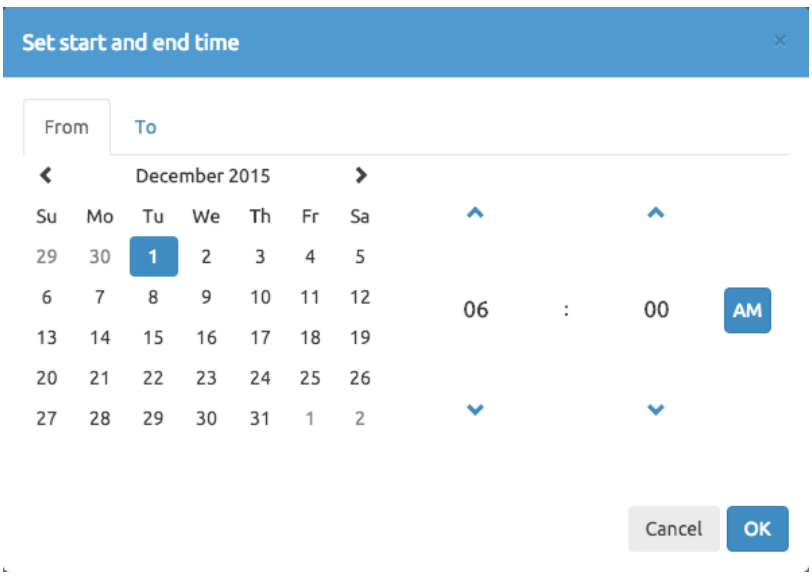
Setting a custom time interval:

When you click on a time interval on the right, you will be presented with a dialog enabling you to set up custom time interval for viewing.

History Mode:

Switch to history mode is done by clicking on the timer icon in the lower left corner.

In this mode, you can specify a date range in which data will be shown - click on a date to set:



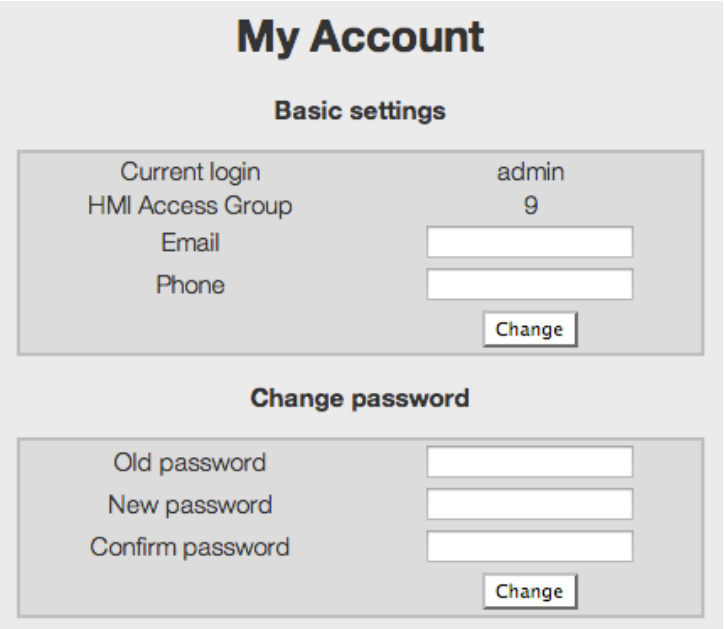
By clicking on the left and right arrows, it is possible to change the date in accordance with already set Time range. Clicking on a left most arrow will show first records available, clicking on a right most icon will show latest records available. Again by clicking on a time interval on the right, you will be presented with a dialog enabling you to set up custom time interval for viewing.

***TIP**: Maximum number of shown rows is limited by a LIMIT button located at the top bar. You can change this value any time during viewing a data.*

Administration Level

My Account

In this menu you can change administrator password and other useful settings such as email and phone number.

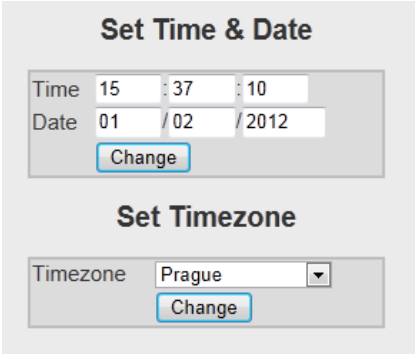


System

In this section you can set up all settings related to the device system.

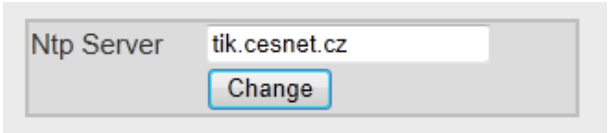
Date & Time

Enter the current date and time then click on „Change“ to save. You can also set a time zone where your country/city is located in.



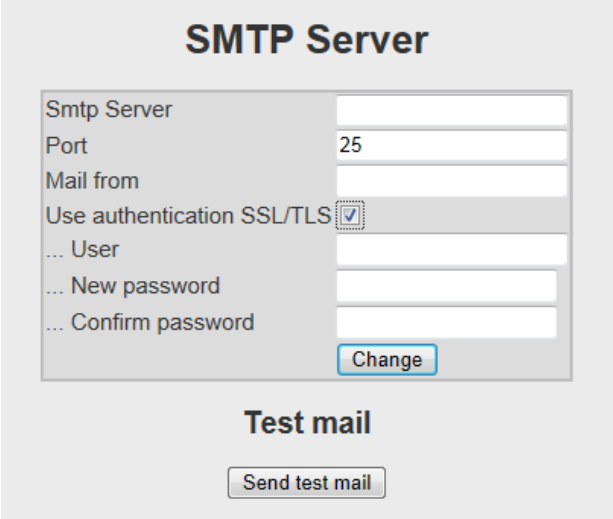
NTP

This feature allows time synchronization with a Network Time Protocol server (e.g. time.nist.gov). Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.



SMTP

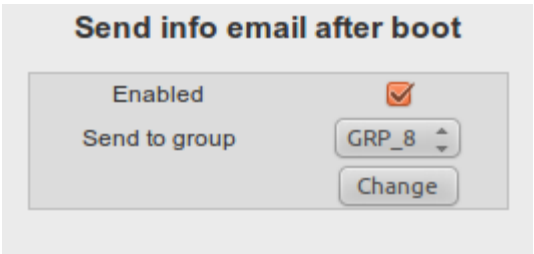
Here you can set an email server to be used to send email messages (this is provided by your ISP).



- SMTP Server – the IP address of the SMTP server
- Port – choose TCP port 25 (SMTP) or port 587 (Submission), or other given by your IT department or ISP provider
- Mail from – an email address which email messages will be sent from. Use the form user@company.domain
- Use authentication SSL/TSL – fill in the user name and password provided you desire to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for enhanced communication security

Send Info Email After Boot

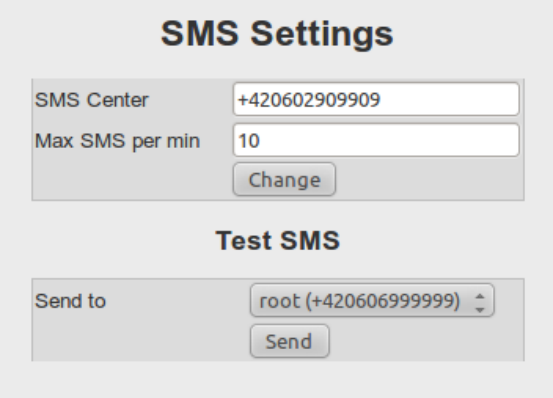
In case of unit reboot this choice generates an informational email for the specified group of users.



- Enable – enable the service
- Send to group - set the group of users to which will be informational mail send.

SMS

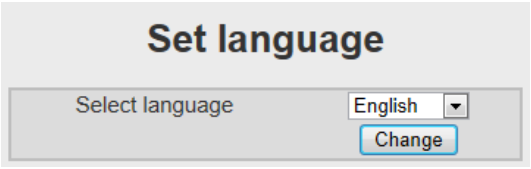
If you have unit with 3G Modem, you should set up the SMS Center settings.



- SMS Center - your service provider SMS center
- Max SMS per min – maximum number of SMS sent during a minute. This choice limits the price of SMS services to be paid.
- Test SMS / Send to – try to send the SMS to given number to test correct functionality

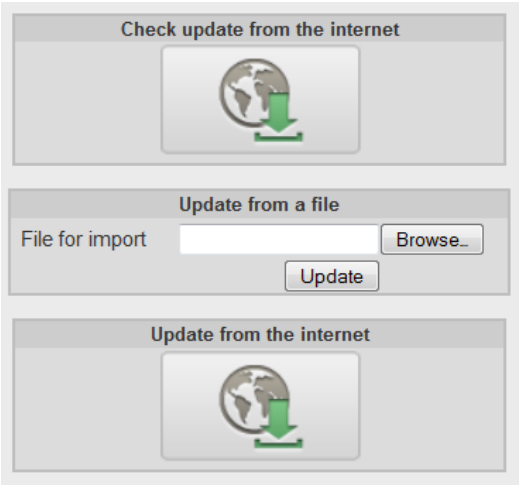
Language

It is possible to change a language of the whole device's GUI – choose one of available languages which are listed in the drop-down menu. You may have to reload your web browser for the change to take effect.



Update

If the device is connected to the Internet you can use the "*Auto update from Internet*" option to automatically have the software updated, provided there is a new version of firmware available. If there is no Internet connection you can still update manually from a file.

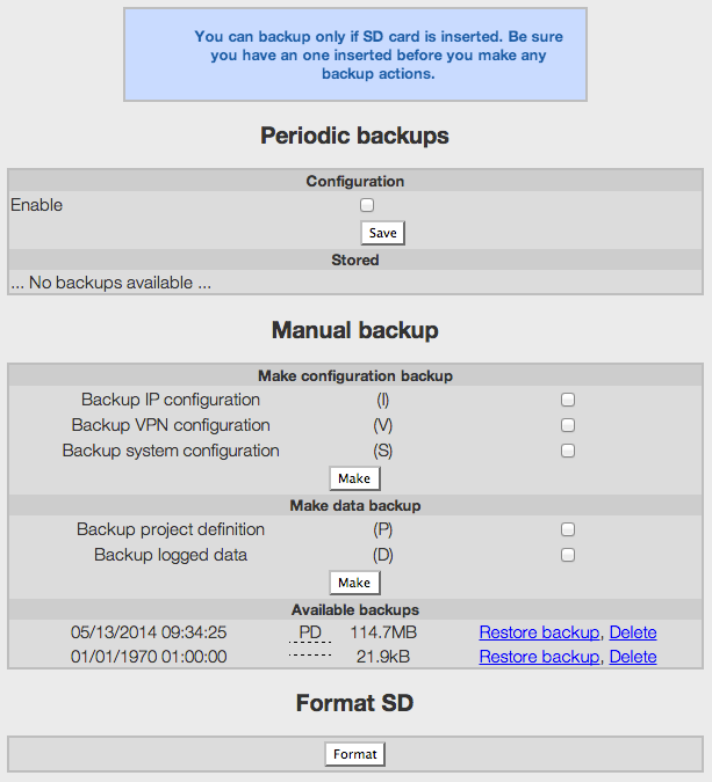


Backup

This function is only available, when the microSD card is inserted in the slot. You can backup complete system, or select only partial backup.

- Project
- Data-logs including alarm history, user actions history, advanced trends
- Network configuration
- System configuration

To perform the backup, put formatted microSD card into a front microSD slot of the device. You might need to restart the device to recognize the card insertion.

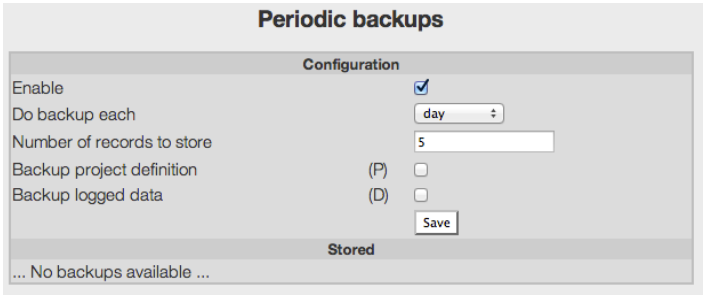


- Make – creates back-up
- Format – microSD card formatting with the file system FAT32

!!!! Please note that all the data stored on the microSD card will be deleted!!!!

- Restore/Delete - restore the back-up data, delete the back-up data from the microSD card

You can also perform a periodic backups based on your time selection. This way you can keep your data redundant in a case you would encounter a problem with a box.



Restore from Backup

This function is only available, when the microSD card is inserted in the slot. You can use restore from backup to quickly set up a new box or switch existing one in a case of failure.

To perform a restore from backup, go to the Backup menu and select from available backups.

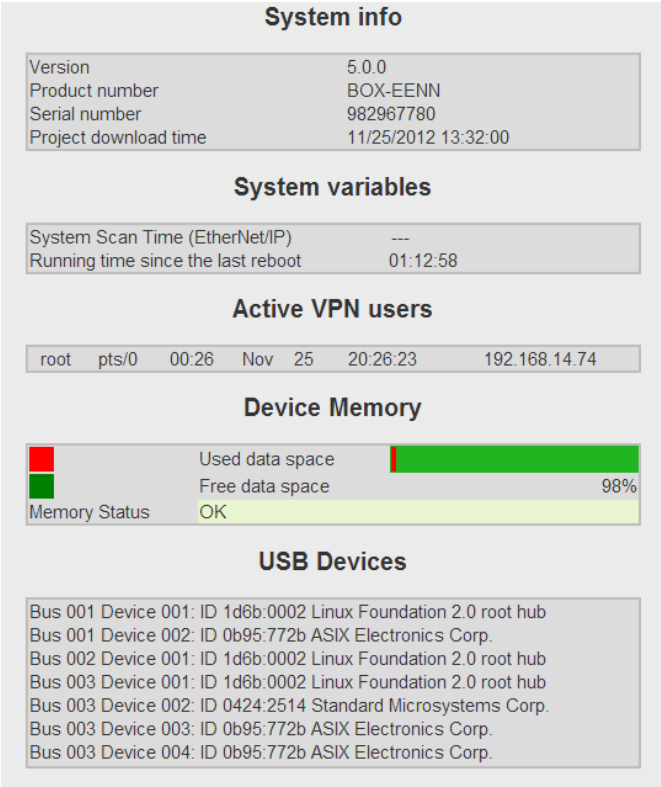
IMPORTANT: You will have to reboot your unit to complete a backup. If your selected backup contains also network settings, IP address of restored box can change.

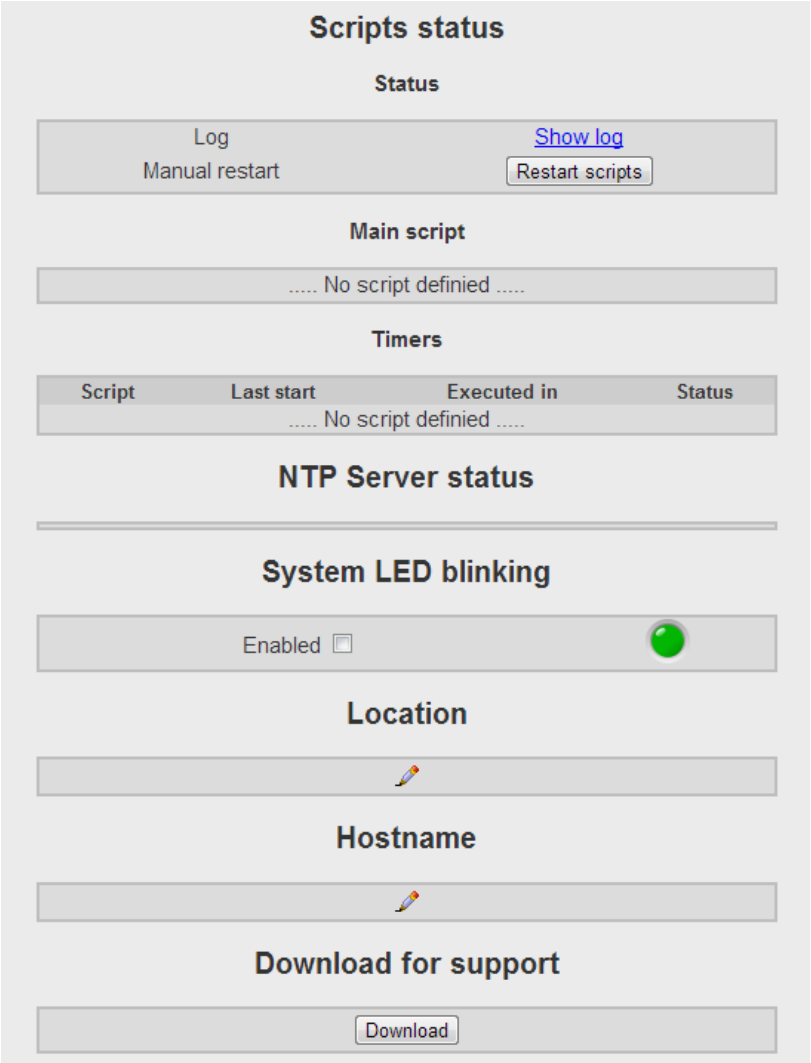
Status

This section provides useful information on the device's system, for example:

- Version of used firmware
- Device's serial number
- Running time since the last reboot
- SMS counter – counts the total number of sent SMS
- Active VPN user – displays the active VPN users
- The green/red chart shows used/available physical memory of the device.
- Scripts status
    - Status – displays script log and restart scripts
    - Main script – displays the status of main (initial) script
    - Timers – displays the status of each periodically started script
- NTP Server status – displays the server status set for time synchronization.
  * – time synchronized,
  = – time synchronization in progress

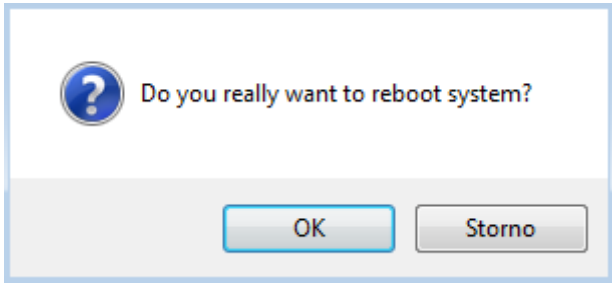
- System LED blinking – makes the system LED light on the panel to blink. Useful for identification of the equipment in the technology.
- Location – enter the location of the device, e.g. a name of your city or factory
  (this is used for identification in some SMS/e-mail notice)
- Hostname – again can be used to enter a user defined text or name, e.g. the connected router
- Download for support – generates a zipped file containing all settings which can be later sent to a support personnel, typically by emailing to *support@myscada.org*


System info
Version 5.0.0
Product number BOX-EENN
Serial number 982967780
Project download time 11/25/2012 13:32:00
System variables
System Scan Time (EtherNet/IP) ---
Running time since the last reboot 01:12:58
Active VPN users
root pts/0 00:26 Nov 25 20:26:23 192.168.14.74
Device Memory
Used data space
Free data space 98%
Memory Status OK
USB Devices
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 0b95:772b ASIX Electronics Corp.
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 003 Device 002: ID 0424:2514 Standard Microsystems Corp.
Bus 003 Device 003: ID 0b95:772b ASIX Electronics Corp.
Bus 003 Device 004: ID 0b95:772b ASIX Electronics Corp.


Scripts status
Status
Log
Show log
Manual restart
Restart scripts
Main script
..... No script definied .....
Timers
Script
Last start
Executed in
Status
..... No script definied .....
NTP Server status
System LED blinking
Enabled
Location
Hostname
Download for support
Download

Reboot

When it is required, you can reboot the device's system by clicking on the menu item "***Reboot***". You will be prompted to confirm the rebooting procedure.

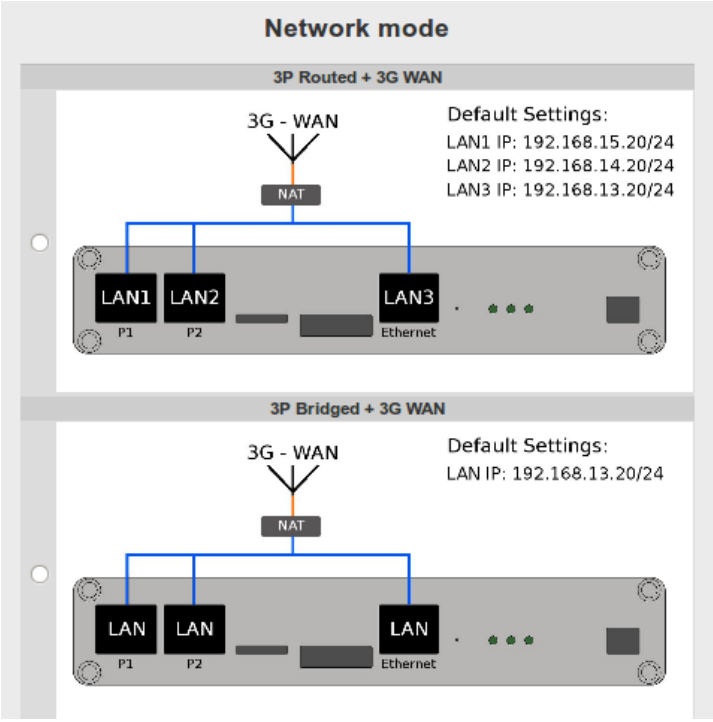


Network

A network grants you the ability to share resources and information among your interconnected devices. To communicate with other computers and devices, a communication channel must be properly established.

NETWORK MODE

To properly operate the device, you must first set the Network Mode. Select the desired networked mode by looking at the options (which depends on the version of your device). You can read through the Mode description when you select it. If you press apply new mode is selected.



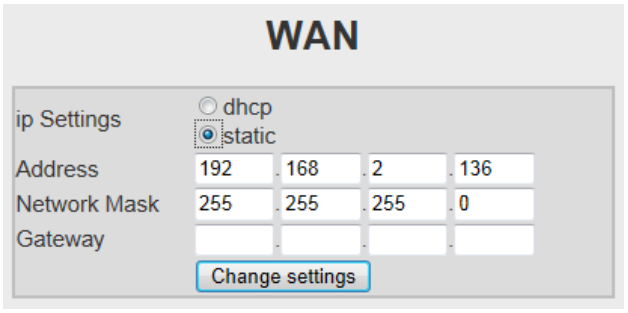
Individual ports setting depend on the HW configuration with following options:

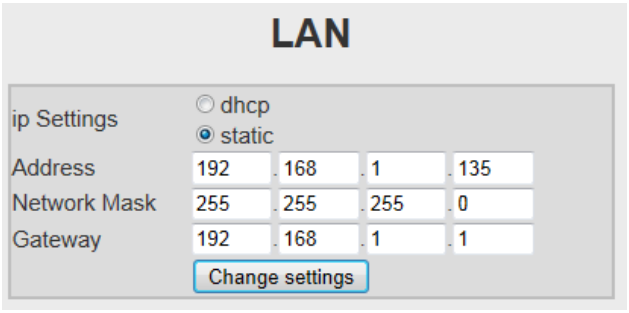
Interface	Mode
LAN/WAN	Routed
LAN/WAN	Bridged
3G/LTE	WAN
3G/LTE	Backup

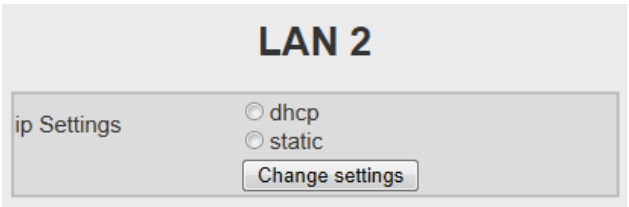
Routed port is a standalone port with its own IP address depending on the type of the port LAN, WAN.
Bridged port is a port included in the bridge group ((br0). IP and other features are set for the whole bridge.
3G WAN is a mobile connection and is considered to be the only access point into WAN.
3G Backup is a back-up connection into WAN (for setting see chapter 6.4.2)

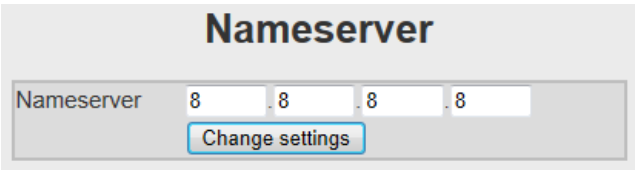
LAN / WAN

In this section basic network settings can be set or changed. There are settings for WAN, LAN, LAN2 and wireless modem. Depending on which version of the device is purchased, the following settings are available:









Setting a unique IP address for the device is essential for proper functionality in a computer network. There are two options how to assign an IP address to the device along with other network information:

1. **DHCP** – the device can obtain IP address and all other network information from a DHCP (Dynamic Host Configuration Protocol) server automatically. The server also eliminates duplicate IP assignments.

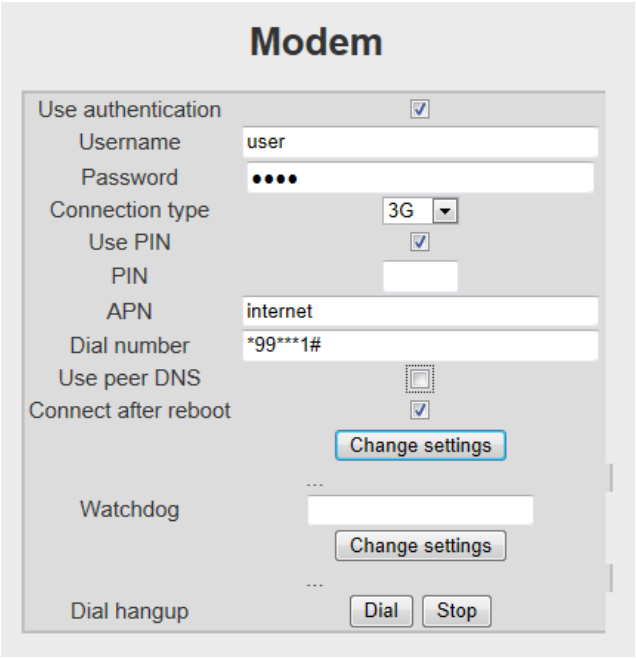
2. **STATIC** – manually enter an IP address and all the required network information

Name server

A name server is a computer server that hosts a network service for providing responses to queries against a directory service. It maps a human-recognizable identifier to a system-internal, often numeric identification or addressing component. This service is performed by the server in response to the request of the network service protocol. You can use a public name-server such as 8.8.8.8 or use the one provided by your ISP.

3G Modem

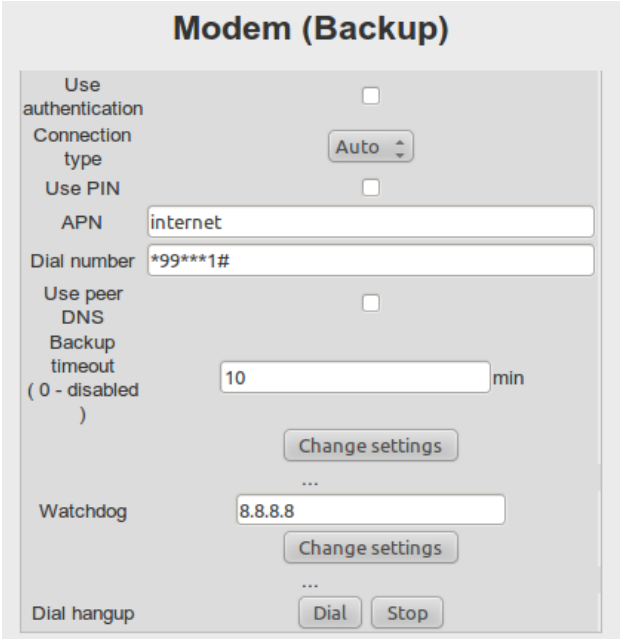
If is your unit equipped with the 3G modem, you should set it up before use. Modem parameters must be filled in order to operate correctly. For concrete parameters such as APN, please consult your SIM data provider.



- **Use authentication** – enter the correct user name & password (not always required)
- **Connection type** – select from 2G, 3G or Auto option (auto option will switch automatically based on the signal strength)
- **PIN** – when necessary enter a valid PIN for the SIM card inserted
- **APN** – Access Point Name (it is provided by your mobile operator, default name is "*internet*")
- **Dial number** – enter the correct number for data access (it is provided by your mobile operator)
- **Use peer DNS** – allows peer DNS
- **Connect after reboot** - start the service after rebooting the device
- **Watchdog** – watchdog performs periodic testing of the IP address accessibility. Note that without watchdog parameter set, connection check will be disabled, so lost connection would not restart the 3G Modem.

Use 3G as Internet Back-up

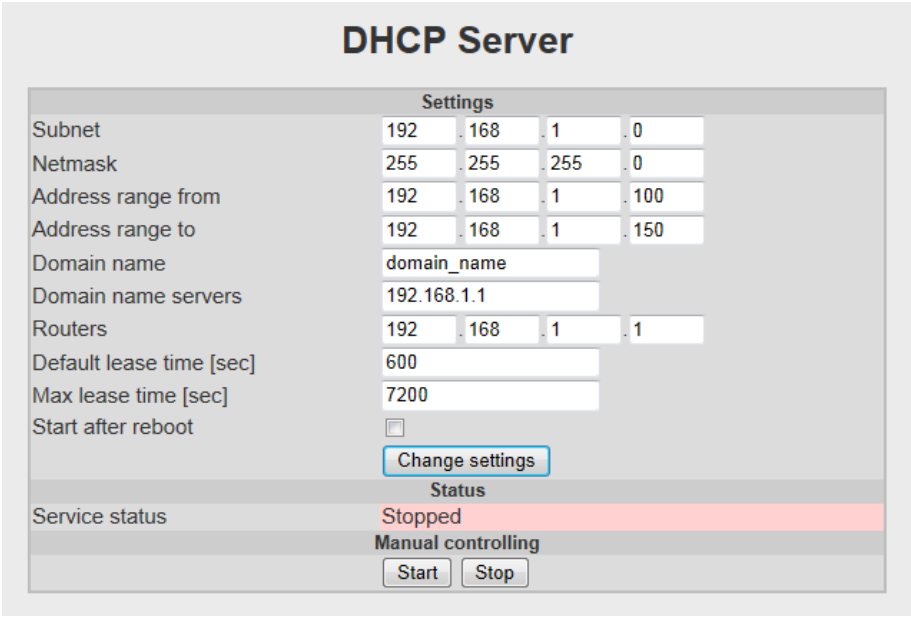
If you use WAN port as your primary connection to the network, you can use 3G Modem as your redundant connection. If your primary connection will go down, 3G modem will dial up and establish a connection. This way, your unit will be always reachable.



The “connect after reboot” setting is not available in this mode as modem connects only on primary connection failure. The modem will be connected only if there is no reply for ping command for host defined in the item “watchdog“. The fall back to primary connection will be recovered after the time specified in the “Backup timeout” parameter.

DHCP Server

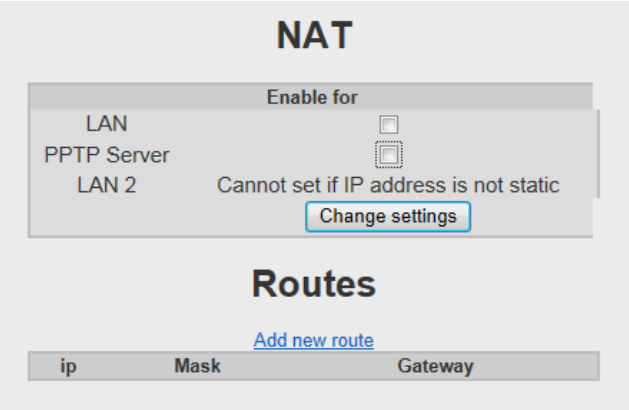
Internal DHCP (Dynamic Host Configuration Protocol) server automatically assigns network information, such as IP addresses. Your unit can work as DHCP server.



To have DHCP server always running, tick “Start after reboot” option.

NAT / Routers

NAT (network address translation) allows multiple hosts on a VPN to access the Internet from a single IP address. It essentially acts as an agent between a public network (e.g. the Internet) and a local/private network.

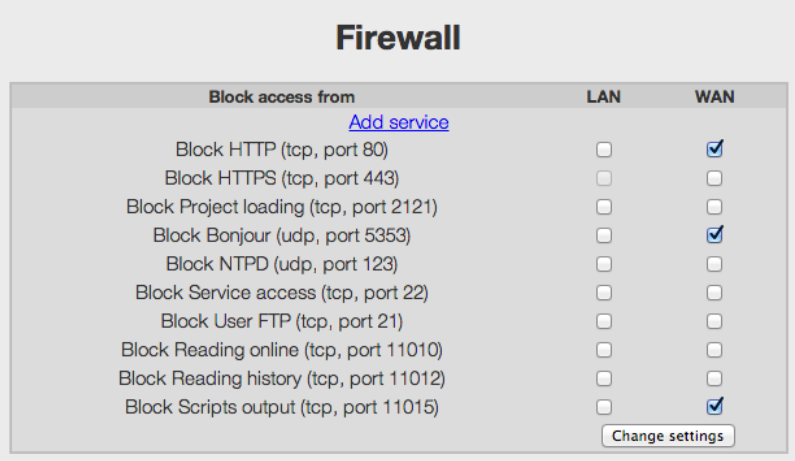


Source routing allows a host who is transmitting packets of data to partially or completely specify the route in which the packet will travel through the network. To define a new route, you would need to enter its IP address, Mask and Gateway.

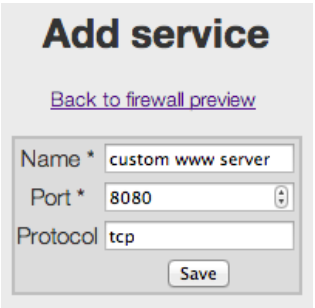
A reboot of the device's system must take place in order for the changes to take effect.

Firewall

Firewall is a network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted. In the Firewall option you can see all open ports for every network interface in your system. You can block any port (disabling service on that port) for given service.



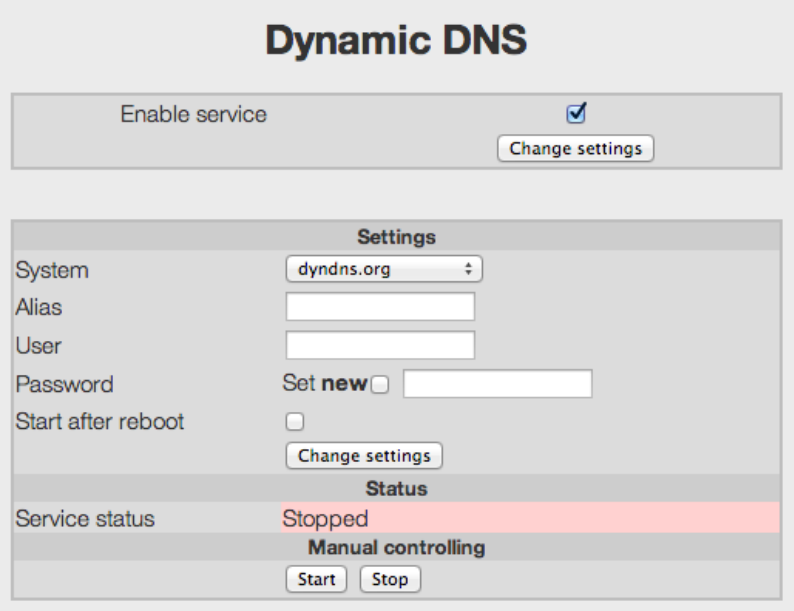
"Add service" – add your own setting for user defined port. This feature is usefull for user defined communication in server side scripts.



DDNS

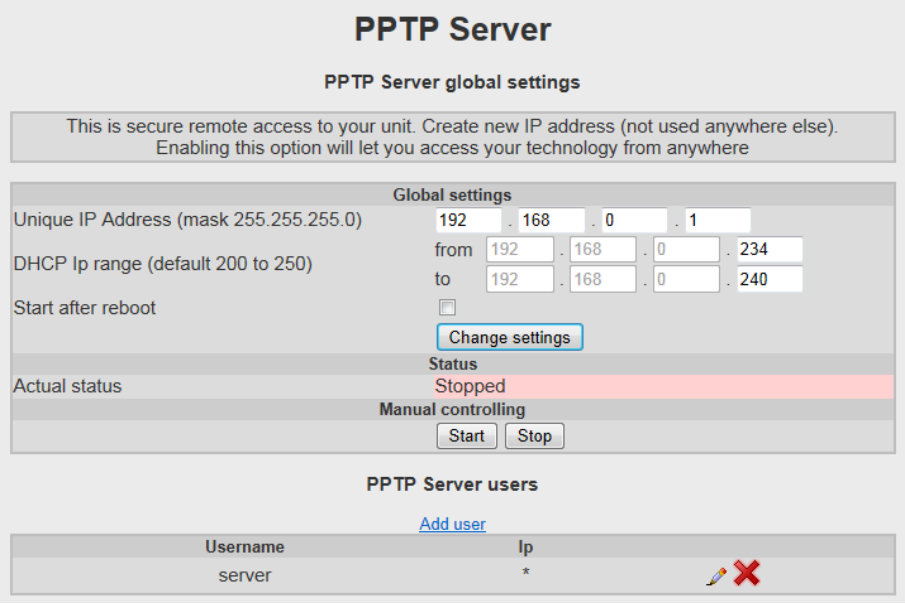
Update of DNS (Internet Domain Name System) name servers. Dynamic DNS (DDNS) is a method of automatically updating a name server in the Domain Name System (DNS), often in real time, with the active DNS configuration of its configured hostnames, addresses or other information.

To enable this option, please tick enable service and fill in the appropriate fields. Do not forget to tick “Start after reboot” option, to have your service running after a unit restarts.



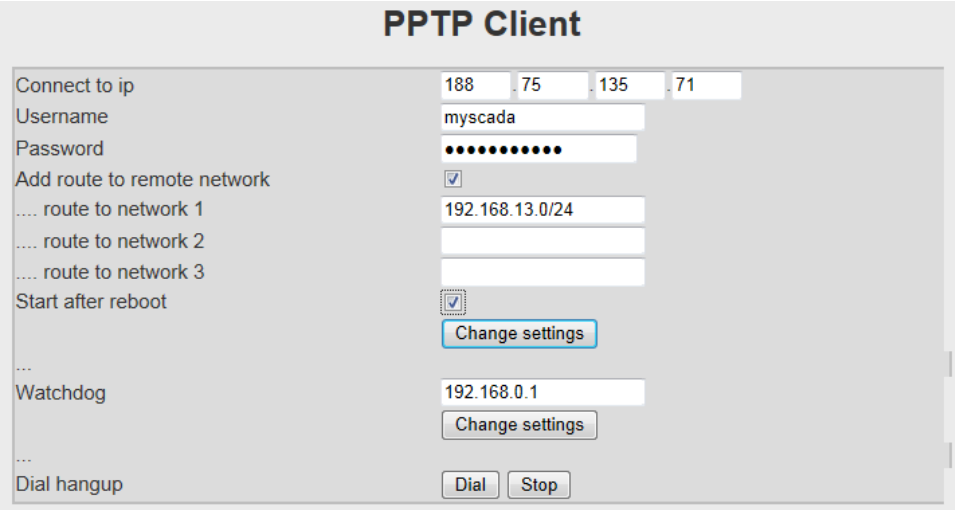
PPTP

A PPTP (Point-to-point Tunneling Protocol) server gives you the ability to securely connect to a LAN from a remote location. This allows you to receive the same service of your workplace in the comfort of your own home. The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.



- Unique IP Address – enter a unique IP address (which is not used anywhere else in your network)
- DHCP IP range – set a range of IP addresses
- Start after reboot – start the network service after rebooting the device
- PPTP Server users – you can add several PPTP Server users

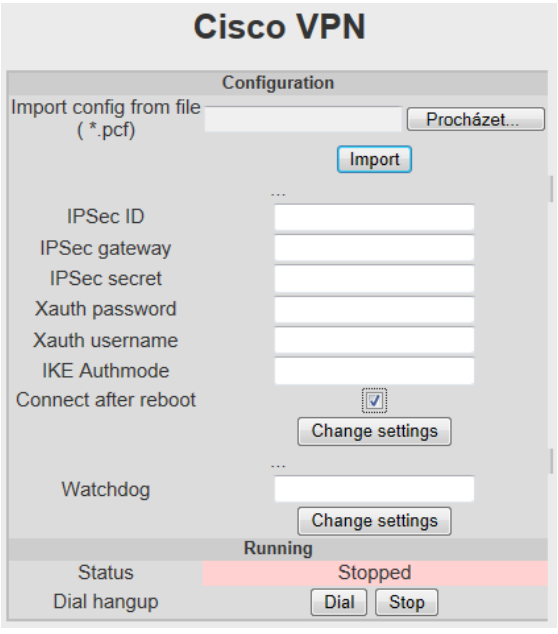
A PPTP Client allows you to connect to a PPTP based VPN (Virtual Private Network).



- Connect to IP – an address of PPTP server
- Username & Password – enter the correct username and password
- Add route to remote network – route is defined as "IP address/network mask", e.g. 192.168.1.1/24
- Start after reboot – start the network service after rebooting the device
- Watchdog – testing of the IP address accessibility via VPN (will be reconnected when necessary)
- Dial hang-up – manual dialing up

Cisco VPN

Similarly to the PPTP this service gives you an option to secure your network by encrypting communication between interconnected computers and devices.



- Import config from a file – if you already have a profile configuration file (*.pcf) that specifies the configuration of your VPN, you can load it from your computer by selecting “Browse”. Once the file is loaded, select “Import”.
- IPSec ID – used to identify which IPSec Secret to use
- IPSec gateway – enter a valid gateway
- IPSec secret – used to secure the exchange of the username and password between the client and the server.
- Xauth password – enter a valid password
- Xauth username – enter a valid username
- IKE Authmode – allows usage of IKE Autmode
- Connect after reboot – start the service after rebooting the device
- Watchdog – testing of the IP address accessibility via VPN (will be reconnected when necessary)

OPEN VPN

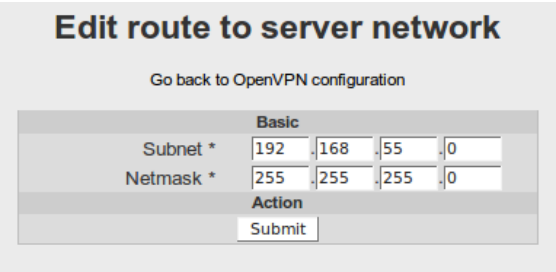
OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls.

Open VPN on myBOX is implemented in the way it is very easy to set up. You can use the box as an OPEN VPN server or use it as an OPEN VPN Client.

Open VPN SERVER Configuration

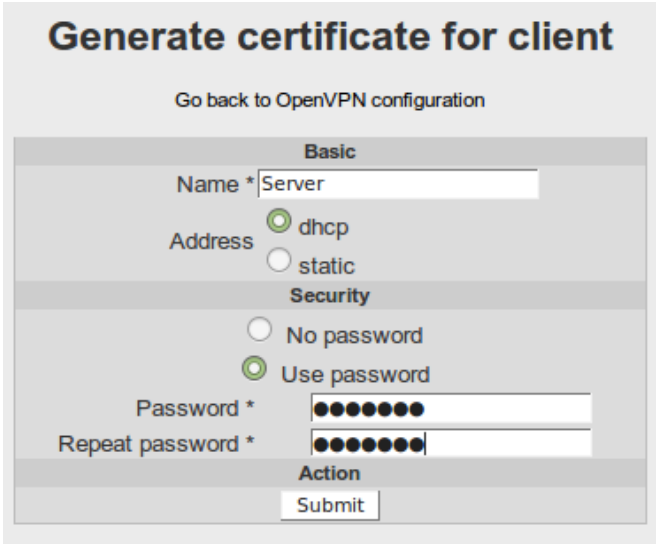
To enable open VPN Server fill in Unique Server IP and tic start after reboot.

If you want to have access to your internal network, you can add route to your internal networks. Click on the “Add route” button.



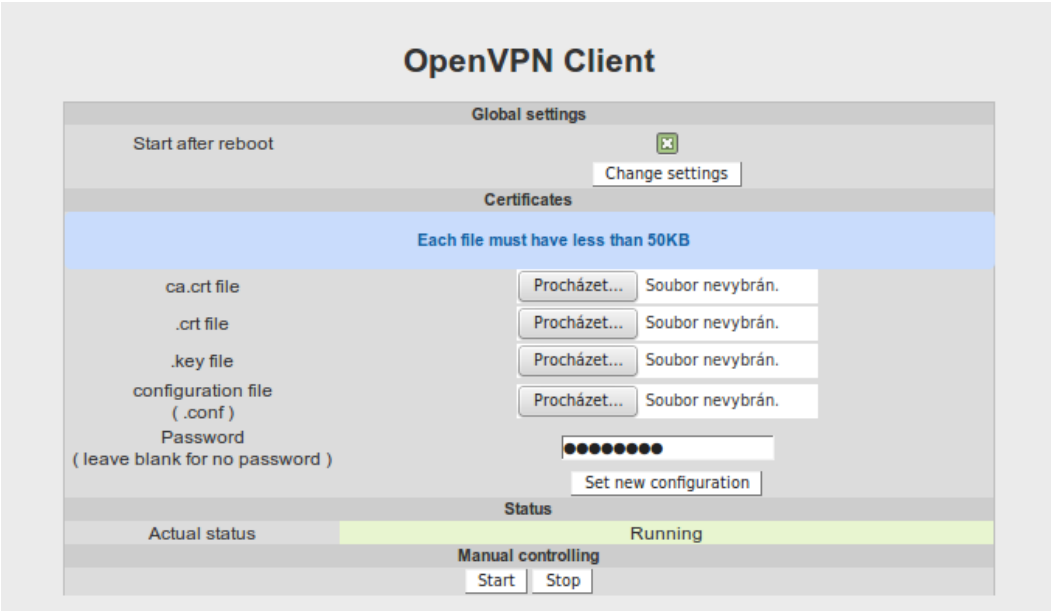
Fill in the subnet and netmask and click “Submit”

To connect clients, you should generate user certificate for each connected user. Click on the “Generate client certificate” button. Give it a name and we recommend also setting the user password.



Open VPN CLIENT Configuration

You can connect your myBOX to the Open VPN Server (this can be either other myBOX configured as a open VPN Server or any other open VPN server). First of all, import the certificates generated from the server. If you have your profile protected by password, fill in the password. Finally, click on “Start after reboot” and “Change settings” button.

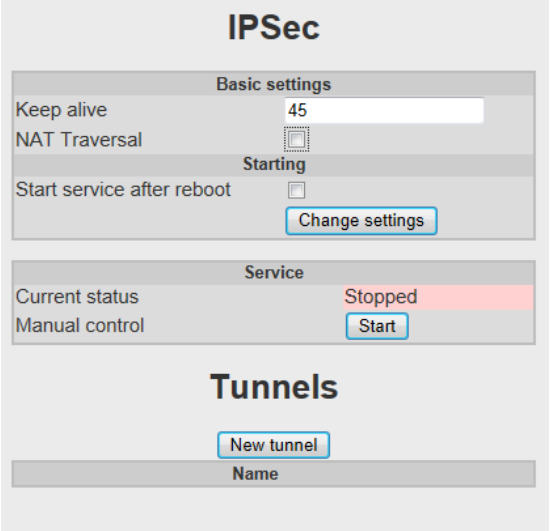


IPSec

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).[1]

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers of the TCP/IP model. Hence, IPsec protects any

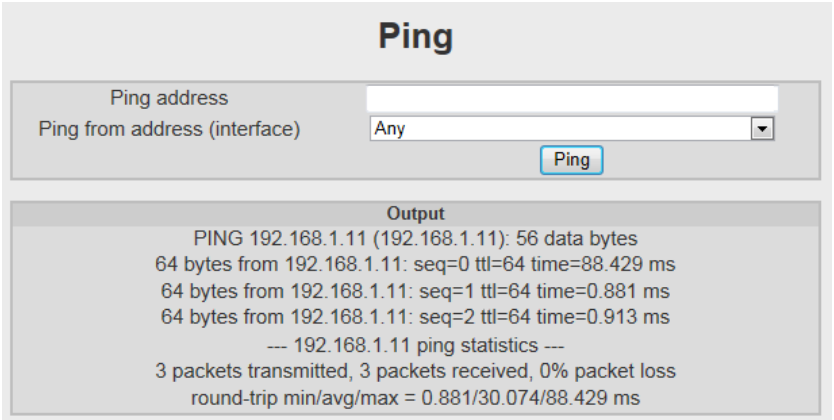
application traffic across an IP network. Applications do not need to be specifically designed to use IPsec. Without IPsec, the use of TLS/SSL had to be designed into an application to protect the application protocols.



- Keep alive – allows you to choose how many links/paths data can be sent through before the linkage fails
- NAT Traversal – allows NAT Traversal
- Starting - start the service after rebooting the device
- Tunnels – it is possible to define several tunnel

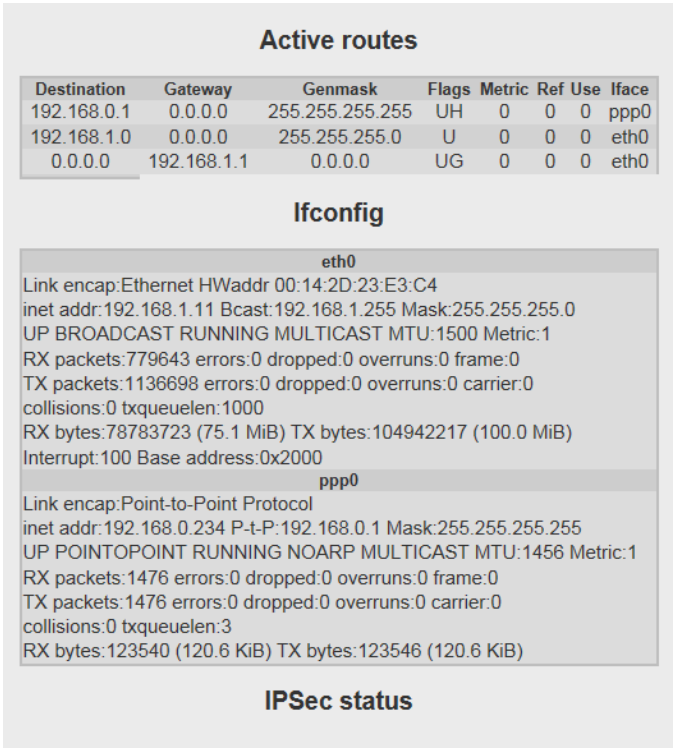
Ping

This internal Ping service is particularly useful when troubleshooting network communication. Simply fill in an IP address you need and hit the “Ping” button.

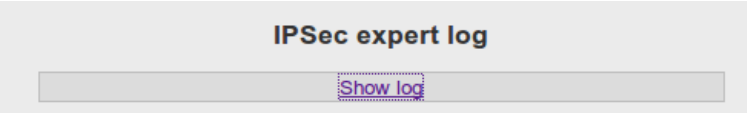


Status

A comprehensive status overview of all network settings and variables can be found here. Also displays detailed accounts on the active routes currently in your network including each individual destination, gateway and general masking address. Other important information given here is the interfacing configuration of each route, amount of data transmitted and received, IPSec status, and much more – essentially all information needed to make sure your network is operating properly.



IPsec tunnel detail function detection.



Logout

When you are logged in the system, you can log out of it by pressing the “Logout” menu item.

Alternatively, click on the  icon in the main screen to logout.

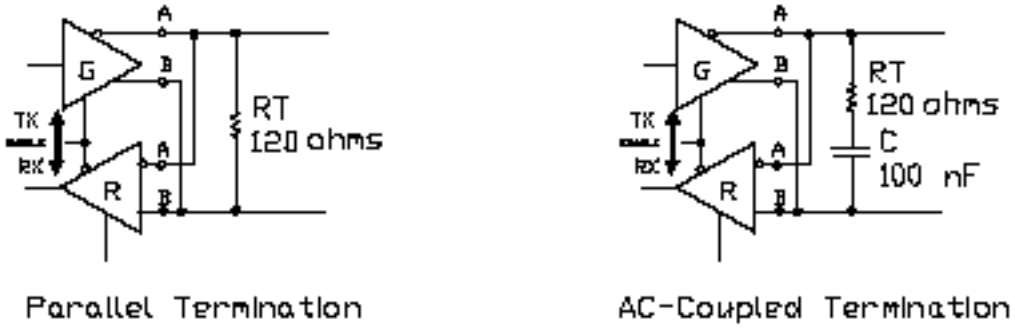
Appendix A –Termination and Biasing an RS-485 Network

Termination

Termination is used to match impedance with respect to impedance of the transmission line being used. When impedances are mismatched the transmitted signal is not completely absorbed by the load and the portion is reflected back into the transmission line. If the source, transmission line and load impedance are equal these reflections are eliminated. There are disadvantages of termination as well. Termination increases load on the drivers, increases installation complexity, changes biasing requirements and makes the system modification more difficult.

The decision whether or not to use termination should be based on the cable length and the data rate used by the system. A good rule of thumb is if the propagation delay of the data line is much less than one bit width, termination is not needed. This rule makes the assumption that reflections will damp out in several trips up and down the data line. Since the receiving port will sample the data in the middle of the bit, it is important that the signal level be solid at that point. In most cases termination is not required.

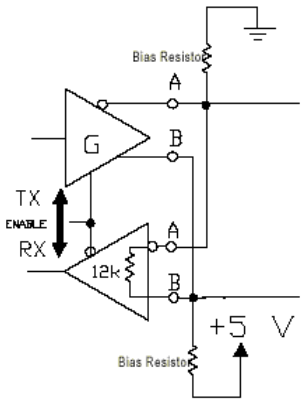
There are several methods of terminating data lines. Most commonly used is a parallel termination. A resistor is added in parallel with the receiver's "A" and "B" lines in order to match the data line characteristic impedance specified by the cable manufacturer (120 ohms. is a common value). This value describes the intrinsic impedance of the transmission line and is not a function of the line length. A terminating resistor of less than 120 ohms should not be used. Termination resistors should be placed only at the extreme ends of the data line, and no more than two terminations should be placed in any system that does not use repeaters. This type of termination clearly adds heavy DC loading to a system. Another recommended type of termination is AC coupled termination. It adds a small capacitor in series with the termination resistor to eliminate the DC loading effect. The picture below illustrates both parallel and AC coupled termination on an RS-485 two-wire node.



Parallel and AC Termination

Biasing an RS-485 Network

When an RS-485 network is in an idle state, all nodes are in listen (receive) mode. Under this condition there are no active drivers on the network. All drivers are tri-stated. Without anything driving the network, the state of the line is unknown. If the voltage level at the receiver's A and B inputs is less than ±200mV the logic level at the output of the receivers will be the value of the last bit received. In order to maintain the proper idle voltage state, bias resistors must be applied to force the data lines to the idle condition. Bias resistors are nothing more than a pull-up resistor on the data B line (typically to 5 volts) and a pull-down resistor (to ground) on the data A line. The picture below illustrates the placement of bias resistors on a transceiver. The value of the bias resistors is dependent on termination and number of nodes in the system. The goal is to generate enough DC bias current in the network to maintain a minimum of 200mV between the B and A data lines.



Transceiver with Bias Resistors

Bias resistors can be placed anywhere in the network or can be split among multiple nodes. The parallel combination of all bias resistors in a system must be equal to or less than the calculated biasing requirements. **This device uses 4.7Kohm bias resistors**. That value is adequate for most systems without termination. The system designer should always calculate the biasing requirements of the network. Symptoms of under biasing range from decreased noise immunity to complete data failure. Over biasing has less effect on a system, the primary result is increased load on the drivers. Some systems can be sensitive to over biasing.

Appendix B – List of supported web browsers for the GUI

The following Internet web browsers are supported and therefore recommended for correct viewing of provided web-based GUI:

- MS Internet Explorer 9.0 and newer
- Firefox 8.0 and newer
- Opera 11.6 and newer
- Apple's Safari 6.0 and newer
- Chrome 22