Netbiter LC300 Series

Important User Information

Liability

Every care has been taken in the preparation of this document. Please inform HMS Industrial Networks AB of any inaccuracies or omissions. The data and illustrations found in this document are not binding. We, HMS Industrial Networks AB, reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be considered as a commitment by HMS Industrial Networks AB. HMS Industrial Networks AB assumes no responsibility for any errors that may appear in this document.

There are many applications of this product. Those responsible for the use of this device must ensure that all the necessary steps have been taken to verify that the applications meet all performance and safety requirements including any applicable laws, regulations, codes, and standards.

HMS Industrial Networks AB will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features, timing, or functional side effects found outside the documented scope of this product. The effects caused by any direct or indirect use of such aspects of the product are undefined, and may include e.g. compatibility issues and stability issues.

The examples and illustrations in this document are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular implementation, HMS Industrial Networks AB cannot assume responsibility for actual use based on these examples and illustrations.

Intellectual Property Rights

HMS Industrial Networks AB has intellectual property rights relating to technology embodied in the product described in this document. These intellectual property rights may include patents and pending patent applications in the USA and other countries.

eWON® and Netbiter® are registered trademarks of HMS Industrial Networks AB. All other trademarks mentioned in this document are the property of their respective holders.

Table of Contents

1 Preface

This document describes the installation, configuration and use of Netbiter LC300 Series gateways.

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit www.netbiter.com/support.

1.1 Document History

Version	Date	Description
1.0	2017-10-02	First release
1.1	2017-10-27	Minor corrections
1.2	2017-11-06	Minor corrections

1.2 Document Conventions

Ordered lists are used for instructions that must be carried out in sequence:

1. First do this

2. Then do this

Unordered (bulleted) lists are used for:

• Itemized information

• Instructions that can be carried out in any order

...and for action-result type instructions:

► This action...

➥ leads to this result

Bold typeface indicates interactive parts such as connectors and switches on the hardware, or menus and buttons in a graphical user interface.

```
Monospaced text is used to indicate program code and other
kinds of data input/output such as configuration scripts.
```

This is a cross-reference within this document: *Document Conventions, p. 3*

This is an external link (URL): www.hms-networks.com

ⓘ *This is additional information which may facilitate installation and/or operation.*

❗ This instruction must be followed to avoid a risk of reduced functionality and/or damage to the equipment, or to avoid a network security risk.

⚠ **Caution**
This instruction must be followed to avoid a risk of personal injury.

⚠ **WARNING**
This instruction must be followed to avoid a risk of death or serious injury.

2   Installation

2.1   Basic Installation Steps

> **!** This product contains parts that can be damaged by electrostatic discharge (ESD). Use ESD protective measures to avoid equipment damage.

> **!** Connecting power with reverse polarity or using the wrong type of power supply may damage the equipment. Make sure that the power supply is correctly connected and of the recommended type.

Make sure that you have all the necessary information about the capabilities and restrictions of your local network environment before installation.

1. Mount the unit on a flat surface or on a DIN rail using the adapter kit (optional).

2. Connect the slave devices and/or Ethernet network as needed.

3. For mobile networking (LC350), connect the mobile antenna and insert the SIM card.

4. Connect a suitable power supply and apply power.

5. Configure the unit.

2.2   Factory Reset

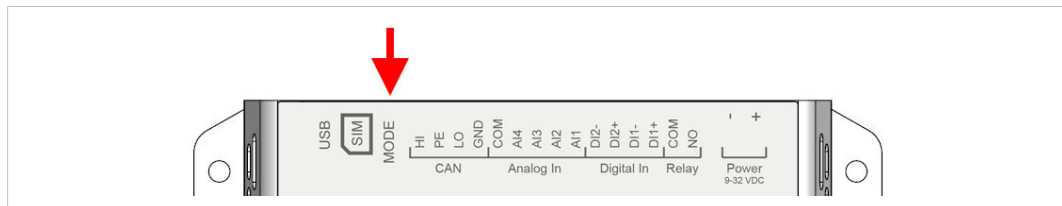Keep the **MODE** button pressed while powering on to reset to the factory default settings.

Fig. 1   Factory reset

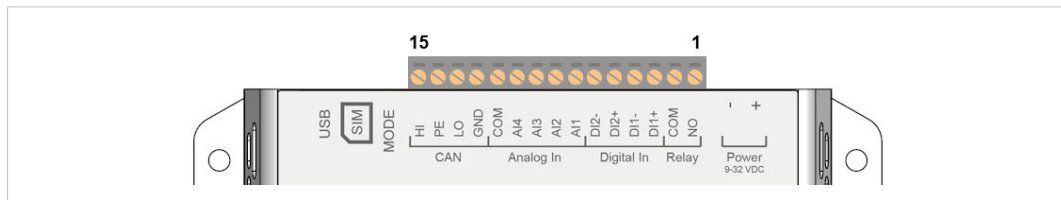## 2.3   Connectors and Indicators

2.3.1   I/O Terminal Block

Fig. 2   Terminal block

Pin	Label	Function	Note
15	HI	CAN High	(reserved for future use)
14	PE	CAN Shield	
13	LO	CAN Low	
12	GND	CAN Ground	
11	COM	Analog Input common	
10	AI4	Analog Input 4	0–20 mA or 0–10 VDC
9	AI3	Analog Input 3	0–20 mA or 0–10 VDC or PT100
8	AI2	Analog Input 2	0–20 mA or 0–10 VDC
7	AI1	Analog Input 1	0–20 mA or 0–10 VDC or PT100
6	DI2-	Digital Input 2	**Dry contact type – do not apply power to these inputs**
5	DI2+	Digital Input 2	
4	DI1-	Digital Input 1	
3	DI1+	Digital Input 1	
2	COM	Relay output common	Isolated inputs Rated load: 1 A @ 24 VDC
1	NO	Relay output, NO	

The analog inputs must be configured for voltage, current or PT100 input.

The digital inputs are of the dry contact type which require no control voltage.

> ❗ Do not connect power to the digital inputs as this may damage the unit.

> ❗ The relay output must be supplied from an isolating transformer using a secondary listed fuse rated at maximum 3.3 A and minimum 30 VDC.

2.3.2 Power Supply

> ❗ Connecting power with reverse polarity or using the wrong type of power supply may damage the equipment. Make sure that the power supply is correctly connected and of the recommended type.
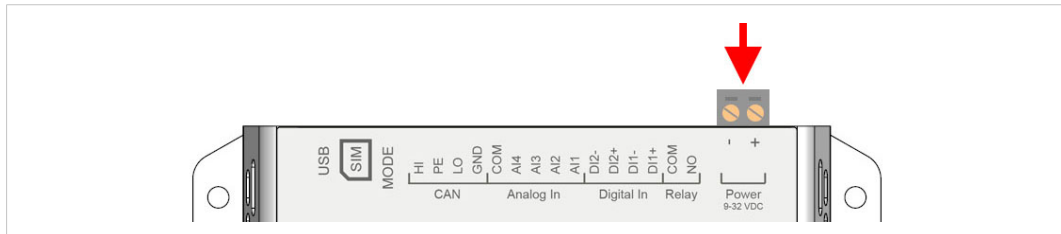

Fig. 3 **Power supply connection**

Connect a DC power supply of the recommended type to the **+** (plus) **-** (minus) terminals. See also *Technical Data, p. 42*.
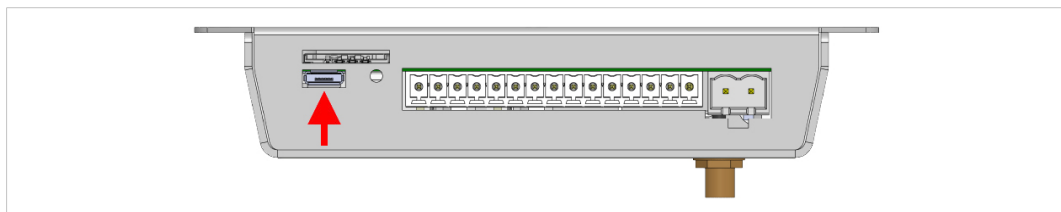
2.3.3 USB Connector

Fig. 4 **USB connector**

The USB micro B connector can be used to connect a computer to the unit for local configuration, firmware upgrades and troubleshooting.

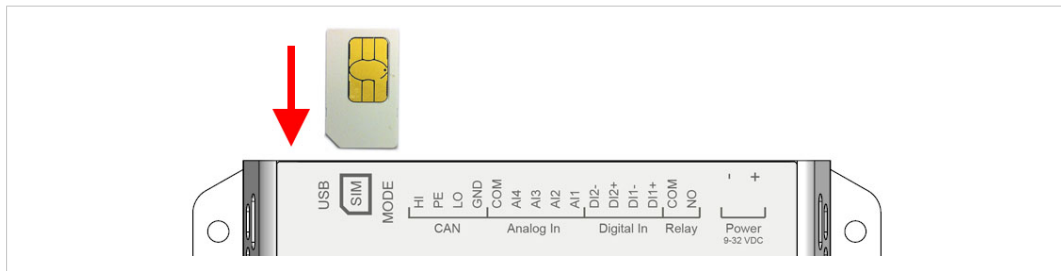## 2.3.4   SIM Card (LC350)

Fig. 5   Installing the SIM card

The SIM card must have a mobile data plan and PIN code security must be disabled. Additional configuration via the local web interface is required.

Insert the SIM card carefully and push it firmly downwards until it clicks into place. Observe the position of the cut-off corner and the contact surfaces.

> ❗ Make sure that the SIM card does not slip behind the holder.
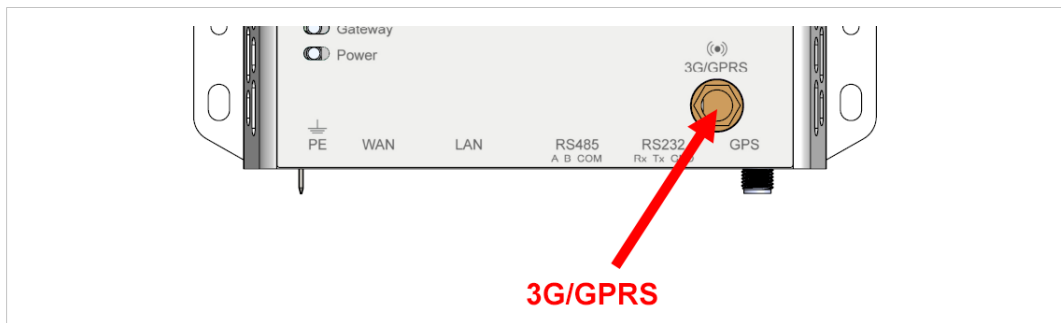
2.3.5   Antenna Connector (LC350)

Fig. 6   LC350 antenna connectors

Make sure that you attach the antenna to the **3G/GPRS** connector on the front panel. The **GPS** antenna connector is reserved for future use.

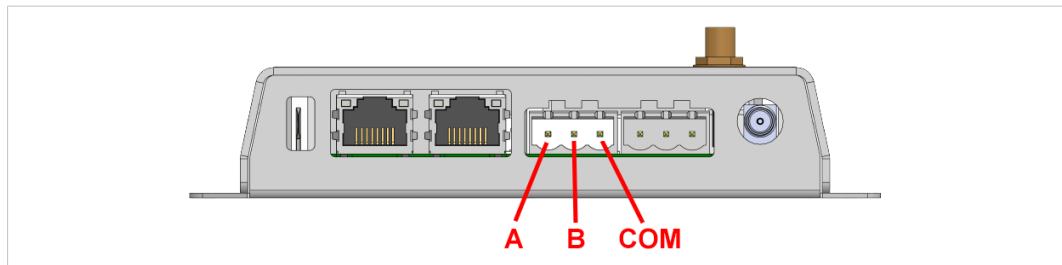## 2.3.6   RS-485 Serial Interface (3-pin)

Fig. 7   RS-485 connector

The RS-485 interface can be used for multiple Modbus RTU devices.

RS-485 connector pin layout

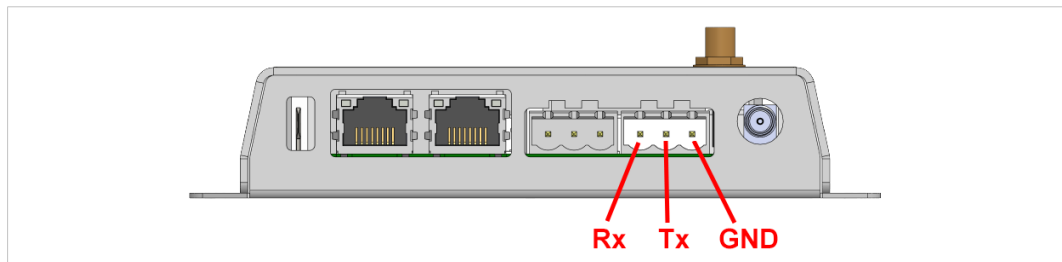| Pin	Function
A	RS-485 A line
B	RS-485 B line
COM	RS-485 common

2.3.7   RS-232 Serial Interface (3-pin)

Fig. 8   RS-232 connector

The RS-232 interface can be used for a single Modbus RTU device.

RS-232 connector pin layout

Pin	Function
Rx	Receive (input)
Tx	Transmit (output)
GND	Signal ground

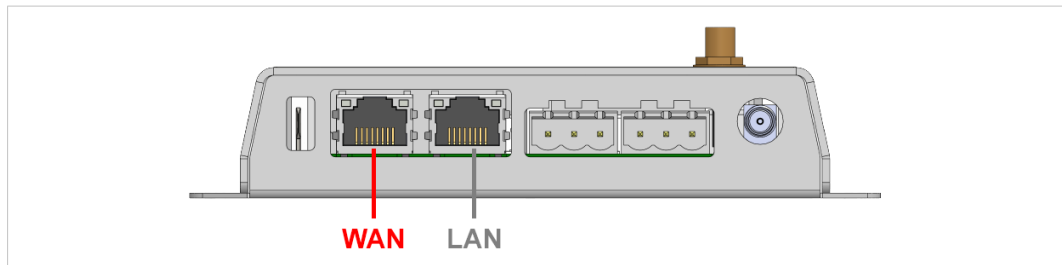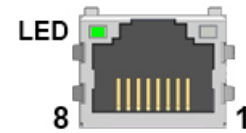## 2.3.8 Ethernet Port (RJ45)

Fig. 9   Ethernet Ports

The **WAN** Ethernet port allows Modbus TCP communication via Ethernet at the same time as Modbus RTU communication on the serial interfaces. It can also be used for accessing the web configuration interface over Ethernet.

The **LAN** port is reserved for future use.

RJ45 pin layout

Pin	Function
1	TD+
2	TD-
3	RD+
4, 5, 7, 8	(reserved)
6	RD-

Ethernet Port LED

Indication	Function
Off	No traffic
Orange, flashing	Traffic (10 Mbit/s)
Green, flashing	Traffic (100 Mbit/s)

2.3.9   LED Indicators

All indicators will light up briefly while the unit is starting up. When the startup sequence has completed they will indicate system status.

Fig. 10   LC350 LED indicators

LED	Indication	Meaning
Modem (LC350)	Off	Modem disabled
	Red	Modem failure
	Red, flashing	SIM card failure
	Orange	PIN code enabled on SIM card
	Orange, flashing	APN (Access Point Name) not set
	Green, flashing	Searching for mobile network
	Green	Connected to mobile network
CAN	-	(reserved for future use)
RS232/RS485	Off	Port disabled
	Red	Port failure
	Green	Port enabled
Status	Orange, flashing	Clock not set
	Green	Normal operation
Gateway	Off	No power or initializing
	Red	Hardware failure
	Red, flashing	Application failure
	Green, flashing	Firmware update in progress
	Green	Unit is operational
Power	Off	No power
	Green	Unit has power

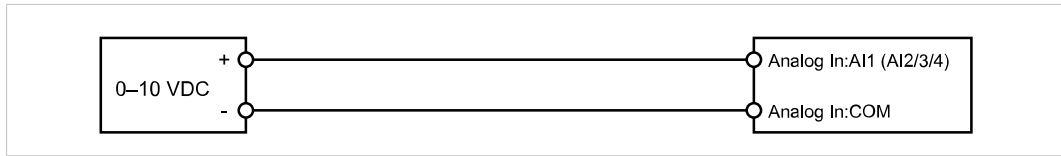## 2.4   Wiring Examples

Fig. 11   Analog Input – Voltage Sensor
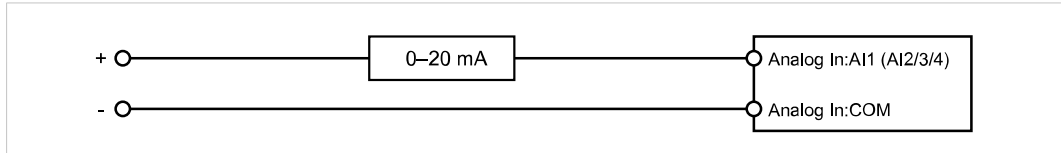

Fig. 12   Analog Input – 2-wire Current Sensor
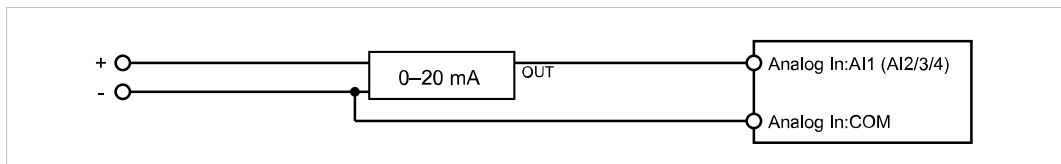

Fig. 13   Analog Input – 3-wire Current Sensor

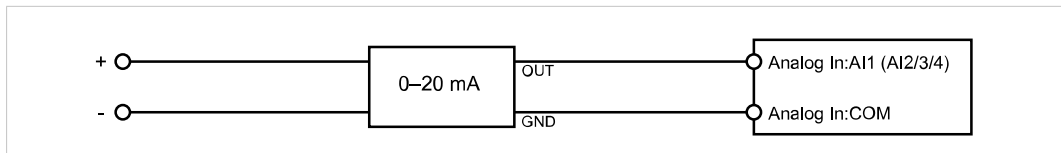

Fig. 14   Analog Input – 4-wire Current Sensor
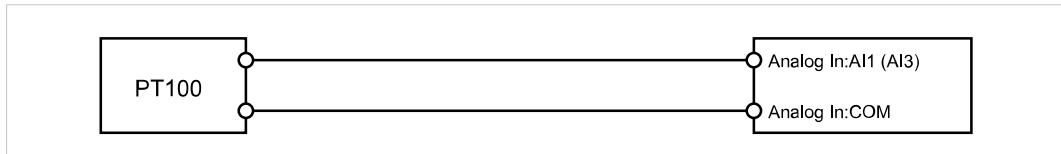

Fig. 15   Analog Input – Temperature Sensor
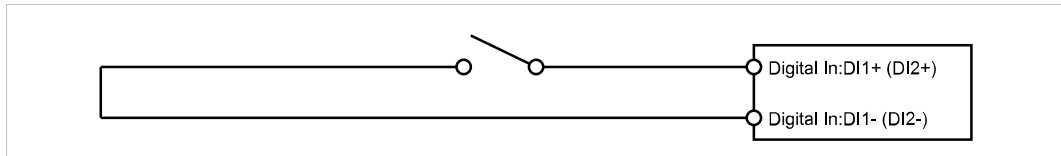

Fig. 16   Digital Input

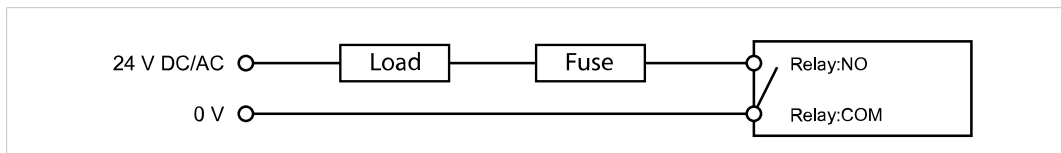! Do not connect a power source to the digital inputs as this may damage the unit.

Fig. 17   Relay Output

! The relay output must be supplied from an isolated transformer using a secondary listed fuse rated at maximum 3.3 A and minimum 30 VDC.

3   Configuration

3.1   Accessing the Web Interface

The Netbiter is configured via a built-in web interface which can be accessed by connecting a computer directly to the USB port (recommended), or over the local network connected to the WAN Ethernet port.

USB Port Access

1. Connect a computer to the USB port on the Netbiter. The USB device driver should automatically load and create a new virtual network interface on the computer.

(i)   *The USB driver can be downloaded from www.netbiter.com/support if it cannot be located automatically by the computer.*

2. Enter the IP address **169.254.200.200** in the address field of a web browser.

Ethernet Port Access

1. Connect a computer to the local network connected to the WAN port. The WAN port uses DHCP addressing as default.

2. Use the IPconfig tool to find the IP address of the Netbiter. IPconfig can be downloaded from www.netbiter.com/support.
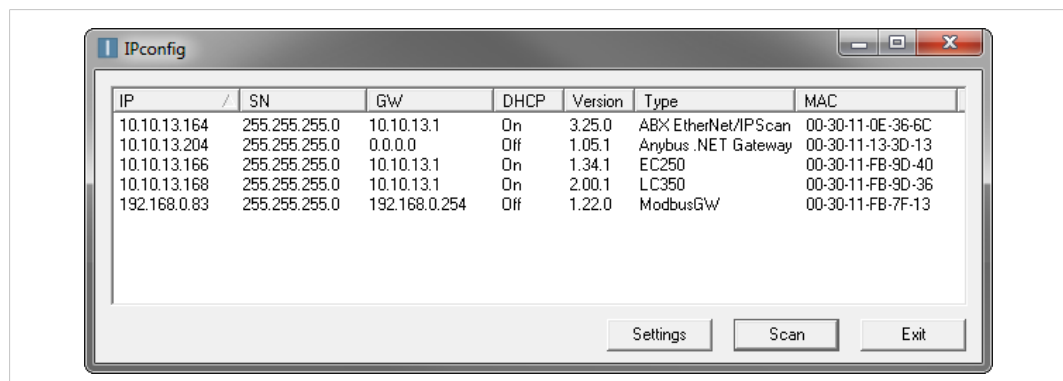

IP	SN	GW	DHCP	Version	Type	MAC
10.10.13.164	255.255.255.0	10.10.13.1	On	3.25.0	ABX EtherNet/IPScan	00-30-11-0E-36-6C
10.10.13.204	255.255.255.0	0.0.0.0	Off	1.05.1	Anybus .NET Gateway	00-30-11-13-3D-13
10.10.13.166	255.255.255.0	10.10.13.1	On	1.34.1	EC250	00-30-11-FB-9D-40
10.10.13.168	255.255.255.0	10.10.13.1	On	2.00.1	LC350	00-30-11-FB-9D-36
192.168.0.83	255.255.255.0	192.168.0.254	Off	1.22.0	ModbusGW	00-30-11-FB-7F-13

Fig. 18   IPconfig

3. Enter the IP address of the Netbiter in the address field of a web browser.

3.2 Login Screen

Fig. 19 Login screen

The default username is **admin**. This user has administration level access.

The password for the admin account is the activation code delivered with the Netbiter. This password cannot be changed.
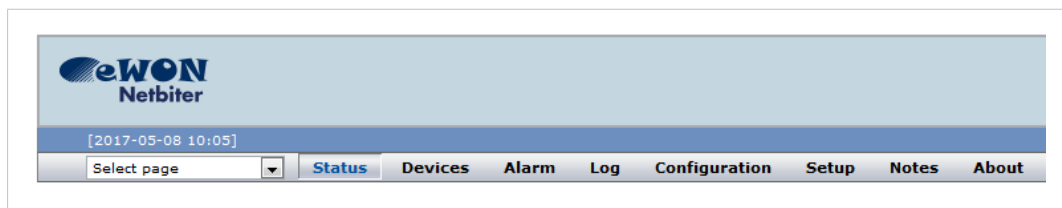
3.3 Main Menu Bar

Fig. 20 Main menu

The web interface allows access to different settings and information depending on the access level of the logged in user.

The recommended workflow is to start by setting up user access and hardware communication from the **Setup** menu, and then continue to the **Configuration** menu to set up data presentation, logs and alarms.

Main Menu Overview

Task	Use menu(s)	See section
Configuring hardware and setting up users	Setup	*Setup, p. 14*
Setting up data presentation, logs and alarms	Configuration	*Configuration, p. 12*
Everyday use	Status, Devices, Alarm, Log	*Usage, p. 35*

> **!** The web interface is designed for the latest stable versions of Internet Explorer, Firefox, Chrome and Safari. Other web browsers may not support all functions.

3.4   Setup

This menu contains settings for configuring users and hardware, and for setting up communication with the attached devices.

The recommended workflow is to work from left to right in the menus, starting with user setup.
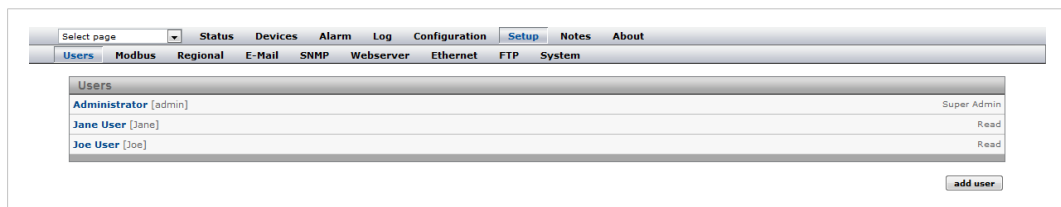
3.4.1   Setup | Users

Fig. 21   Users setup page

Users can have different access rights to logs, alarms, etc. Only users with user level *Super Admin* are able to add and edit users.

To add a new user, click on **Add user**. To edit an existing user, click on the user name. Click on **Save** when finished or **Back** to cancel.

Fig. 22   Add/Modify User dialog

Add/Modify User settings	
User ID	The login name for the user. Must not contain spaces or special characters.
Name	Full name of the user
E-mail	Email address of the user.
Mobile	Mobile phone number.
Receive log files via E-mail	If enabled in the log configuration, logs will be e-mailed to the address entered in the **E-mail** field.
Language	The user interface language for the user.
Show Device browser in menu	If enabled, all parameters of the device templates will be accessible from the **Devices** menu. For users with Read user level, the parameters can only be viewed, not changed.
Select user specific start page	Select which page should be the start page for this user.

User level
- **Read**: User can only monitor data.

- **Write**: Same as Read + user can acknowledge alarms and clear logs and alarm history.

- **Admin**: Same as Write + access to the **Configuration** menu. Admin users can add and change parameters, templates, devices, pages, alarms and bindings.

- **Super Admin**: Same as Admin + access to the **Setup** menu. The Super Admin has full access to all parts of the system.

Password   Enter a password here when adding a new user. To change the password for an existing user: check the box **Change password** and enter a new password.

Repeat password   When adding a new password the password has to be repeated here.

3.4.2   Setup | Modbus

Fig. 23   Modbus setup page

Make sure that the Modbus devices are correctly connected to the Netbiter gateway before continuing. Each Modbus device must also be setup with a template and a unique slave address, see *Configuration, p. 12*.

> ⚠ Two devices cannot have the same Modbus slave address. If this happens, the serial bus will not be able to communicate with all slaves on the bus.

Settings (Modbus RTU)

Transmission Mode	Select Modbus RTU or Modbus ASCII transmission mode. Default = RTU.
Slave Response Timeout	The time that the Netbiter will wait for a response from a slave before Serial Timeout will occur Default = 1000. Serial Timeout can be monitored on the **Status** page
Physical interface	The physical interface used on the Netbiter. Default = RS-485.
Baudrate	Baud rate setting: 300 bps to 115200 bps. Default = 9600.
Character Format	Parity and stop bit settings. Default = No Parity, 1 Stop Bit.
Extra delay between messages	Time in milliseconds between Modbus messages. Default = 0.
Use function code 15 when writing single bits (coils)	When enabled, all writes to coils will be done with function code 15 (useful if slaves do not support function code 05).
Use function code 16 when writing single registers	When enabled, all writes to registers will be done with function code 16 (useful if slaves do not support function code 06).
Disconnect non-responding slaves	Modbus slaves that do not respond within the Slave Response Timeout (see above) will be disconnected

Settings (Modbus TCP)

Modbus TCP	Enable/disable the Modbus TCP interface. Default = Disabled.

Transparent Modbus Settings (Modbus TCP – Modbus RTU)

Transparent Modbus/ TCP to Modbus/RTU	Enable/disable this function. Default = Disabled.
Port Number	The TCP port to use for Modbus communication. Default = 502.
Internal module registers via Modbus/ TCP	When enabled, the Modbus slave address for the interface is set here.
Server Idle Timeout	When enabled, the idle timeout in seconds for the Modbus TCP connection can be set. If there is no response within this time the connection will be closed. Default = 60.
IP Authentication	When enabled, the IP address allowed to connect to the gateway can be configured. A range of IP addresses can be set using the Mask field.
	Example: IP Number = 192.168.0.1 and Mask = 255.255.255.0 will allow all IP addresses from 192.168.0.1 to 192.168.1.254 to connect.

(i) *The **Status** page gives information about the Modbus connection and can be useful as a trouble-shooting tool when setting up the Modbus interface.*

3.4.3   Setup | Modem

Fig. 24   Modem setup page

Netbiter LC350 has a built-in 3G/GPRS modem that enables communication with the Internet without an Ethernet connection.

Modem Settings	
Enable	Enable/disable the modem
Access point name (APN)	The APN (Access Point Name) is the identifier for the mobile network. The APN is supplied by the network operator for the SIM card.
User name, Password	If required, enter the user name and password supplied by the mobile network operator

3.4.4   Setup | Regional

Fig. 25   Regional setup page

This page contains date/time settings, choice of separator characters, and general info about the installation. The date and time can be set either manually or automatically from an NTP (Network Time Protocol) server on the local network or the Internet.

Time and Date

Time zone	The time zone to use for the Netbiter.
	For time zones marked with * daylight saving will be used (the time entered should be the actual time, the Netbiter will adjust it automatically).
Network time protocol	Enables/disables automatic date/time setting from an NTP server on the local network or the Internet.
NTP server	The IP adress or host name of the NTP server to use.
Date (yyyy-mm-dd)	The current date.
Time (hh:mm:ss)	The current time.

Decimal separator

Decimal separator and log file value separator	The decimal separator and the separator character to use for CSV format log files.

Module Information

Site name	(Optional)
More information	(Optional)

3.4.5   Setup | E-Mail

Fig. 26   E-mail setup page

SMTP settings

SMTP Server	The host name or IP address of the e-mail server.
Port number	The port number to use when connecting to the SMTP server. This information should be supplied by the Internet Service Provider. The default port number is 25.
SMTP Authentication	If the SMTP server requires a login, select the type of authentication here.
User name	User name for the SMTP server (if required).
Password	Password for the SMTP server (if required).
Connection security	Enable/disable STARTTLS or TLS encryption
Sender	The name that will be shown in the FROM field in e-mails sent by the Netbiter.
Reply Path	The e-mail address to be used as the reply address in e-mails set by the Netbiter.
Send test E-mail	Enter an e-mail address and click **send** to send a test message.
	Some e-mail servers may treat the test message as junk e-mail.

3.4.6 Setup | SNMP

Fig. 27   SNMP setup page

SNMP settings	
SNMP Manager 1–3	The hostname or IP address of the SNMP Manager(s) to use.
Port	The port number that the SNMP Manager will listen on.

For information on how to set up the sending of alarms as SNMP traps, see *SNMP, p. 41*.

> **!** If a hostname is used for the SNMP Manager, make sure that the DNS server settings for the Ethernet connection are correctly configured.

3.4.7 Setup | Webserver

Fig. 28   Web server setup page

Settings for the internal web server in the Netbiter.

HTTP settings	
Extra webserver port	The web server can listen on a second port in addition to the default HTTP port (80). The extra port can be configured manually for some features that are automatically configured on the default port.
	To access the Netbiter web server on the extra port, add a colon followed by the port number to the URL in the browser.
	Example: http://10.10.10.30:8080 (if the extra port is set to 8080).
Automatic logout time	The timeout for the webserver session. When the session times out you must enter your login credentials again to continue.

3.4.8   Setup | Ethernet

Fig. 29   Ethernet setup page

Contact your network administrator if in doubt about how to configure these settings.

| Ethernet settings	
DHCP	If enabled, the WAN port will be assigned an IP address dynamically by a DHCP server.
	Do **not** enable this option unless there is a DHCP server available on the local network.
IP Address	Static IP address for the Netbiter. Must be unique.
Subnet mask	The subnet mask to use on the local network.
Gateway	The default gateway on the local network.
Primary DNS	Primary domain name server, needed to be able to access servers by host name.
Secondary DNS	Secondary domain name server (optional).
Dynamic DNS	Enable if using dynamic DNS.
DDNS System	Select the DDNS server to use
Update period	Update interval for the DDNS service
Username, Password	Login credentials for the DDNS server (if required)

3.4.9 Setup | FTP
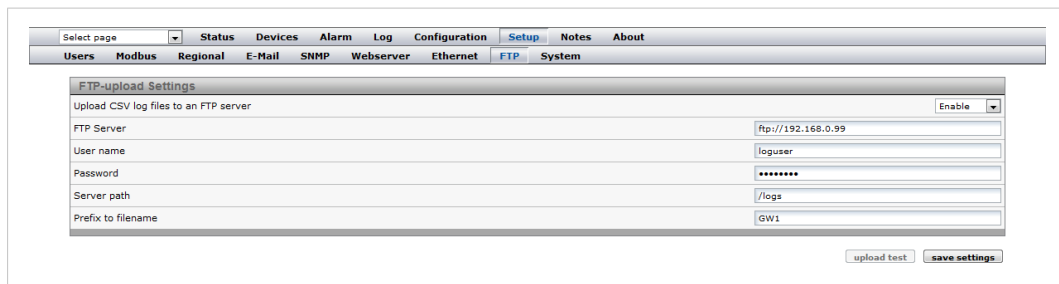
Fig. 30   FTP setup page

FTP-upload settings

|	
Upload CSV log files to an FTP server	Enable to upload log files to a server using FTP
FTP Server	The FTP server hostname or IP address
User name, Password	Login credentials for the FTP server
Server path	Path to the directory on the FTP server
Prefix to filename	A prefix can be added to each log file for identification
upload test	Click to test the FTP server connection

3.4.10 Setup | System
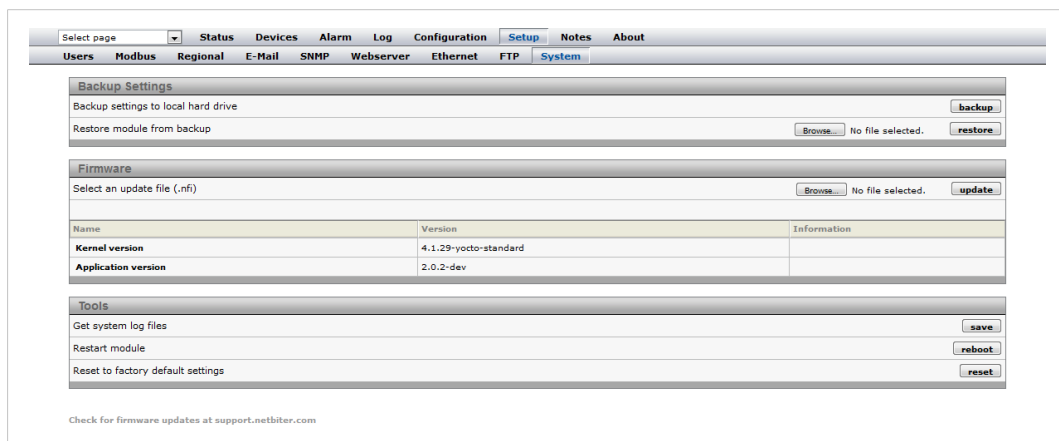

Fig. 31   System setup page

This page contains system information and settings for maintenance and backup.

A system backup will include all current settings and configurations except the Ethernet settings, which are excluded to prevent the risk of IP address conflicts.
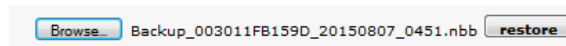
Backup settings

Backup settings to local hard drive	Click on backup to create a system backup. When the backup file has been created you will be asked to save it to your computer.
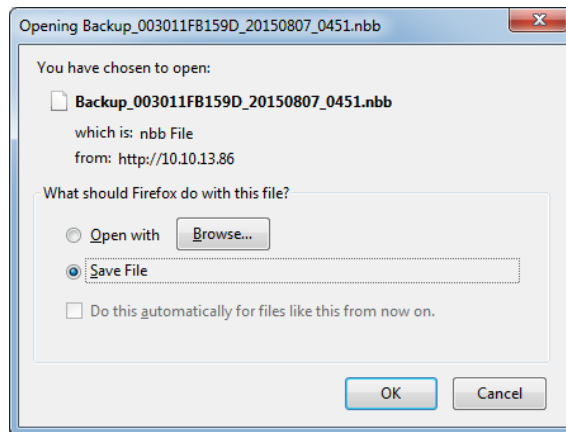
Restore module from backup	Click **Browse** to select a previously saved backup file (*.nbb) from your computer, then click on **restore** to upload the configuration.

> **!** Restoring from backup will remove all current settings and configurations (except the Ethernet settings) and replace them with those saved in the backup file.

Firmware

Select an update file	Click on **Browse** to select a firmware file (*.nbu) or patch file (*.nbp) to upload to the Netbiter, then click on **update** to start the procedure. The web pages may be temporarily unavailable until the update is finished. The latest firmware files and patches can be found at www.netbiter.com/support. Always take a system backup before updating firmware.
Kernel version	Kernel version used in the Netbiter.
Application version	Application version used in the Netbiter.

Tools

Get system log files	Click on **save** to download an archive in *.tar format containing all log files and system information.
Restart module	Click on **reboot** to restart the Netbiter.
Reset to factory default settings	Click on **reset** to remove all current settings and configurations and restore the Netbiter to the factory default settings.

> **ⓘ** *When using DHCP, the Netbiter may have been assigned a new IP address after being restarted. If you are not able to access the Netbiter in your browser after a reboot, use the IPconfig tool to check if the IP address has changed.*

3.5 Configuration

This menu is used to configure presentation and logging of data read from Modbus devices, and for setting up alarms and log messaging. The normal workflow is from left to right, starting with template setup.

> ℹ️ *To be able to read data from a Modbus device the communication interface must also be set up correctly. See Setup | Modbus, p. 15.*

3.5.1 Configuration | Templates

A *device template* describes the parameters in a connected device and how they will be presented. It contains information about available registers and data types, configuration of scaling and offsets, enumerations, and read/write conditions.

Each Modbus device connected to the Netbiter must have an associated template. The normal workflow is to upload or create a template on the **Templates** page, then add the device and associate it with the template on the **Devices** page.

Ready to use templates for Modbus devices can be downloaded from the Netbiter support website www.netbiter.com/support.
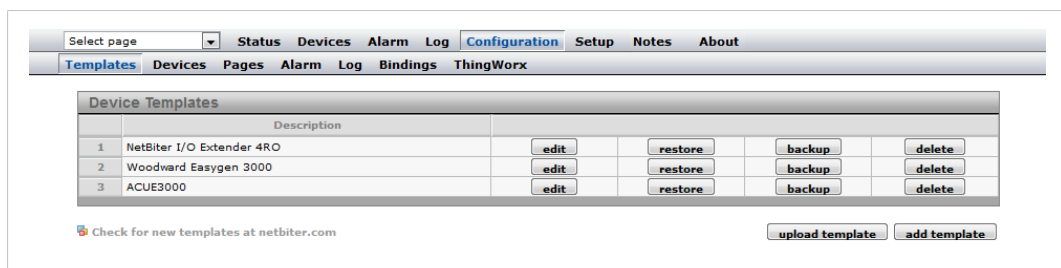
Fig. 32   Templates configuration menu

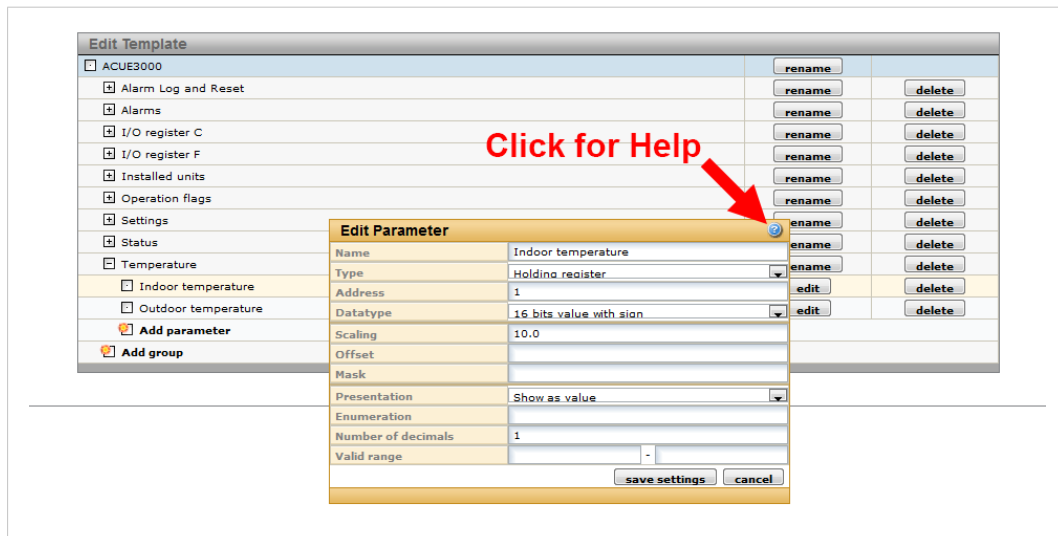| Templates	
Edit	Edit the template
Restore	Overwrite any edits in the template
Backup	Create a local backup of the template
Delete	Remove the template from the Netbiter
Upload template	Upload a template file to the Netbiter
Add template	Create a new template

Add, Upload and Edit Template

Fig. 33   **Editing template parameters**

A template is divided into groups of parameters. A parameter is description of a Modbus register with information about presentation, data type, etc. Parameter groups can be added, renamed and deleted as needed. A template must contain at least one group.

> **!**   Deleting a group will also delete all the parameters in that group.

Edit Parameter

Name	The name of the parameter
Type	Modbus register type
Address	Modbus register address
Datatype	Data type for the register value
Scaling	Scaling factor for the register value when presented
Offset	Offset for the register value when presented
Mask	Used to mask out specific bits from the Modbus register
Presentation	How the value should be presented on the page (read only, read/write, etc.)
Enumeration	Enumeration of values to present them as text. Example: 0=OFF;1=ON;
Number of decimals	The number of decimals to include when presenting the value
Valid range	Defines max/min allowed values for a write parameter

> **i**   *Click on the question mark icon* ? *in the Edit Parameter dialog to view detailed help about the different options when adding and editing parameters.*
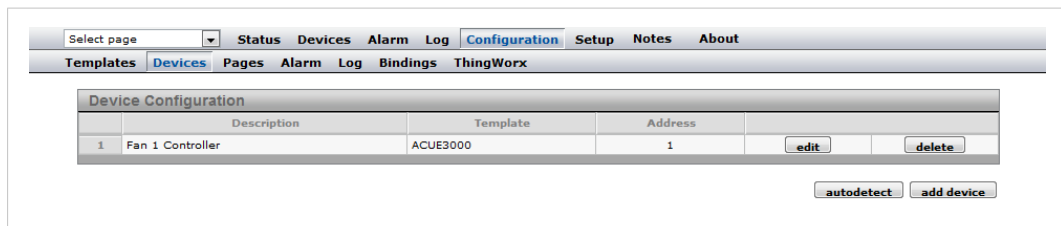
3.5.2   Configuration | Devices

Fig. 34   Devices configuration page

Each connected Modbus device must be configured with a unique Modbus slave address and be assigned a device template.

Devices can be added automatically by clicking on **Autodetect**. The Autodetect function will scan each Modbus address in turn, using the current Modbus serial interface settings (this may take several minutes).
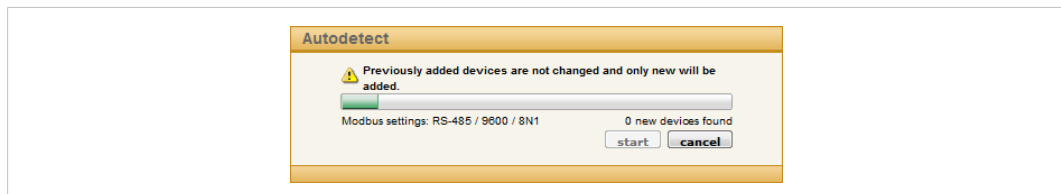

Fig. 35   Autodetect devices

If the templates support identification of Modbus devices the correct template will automatically be assigned to a detected device. Otherwise, the template must be assigned manually. To add a device manually, click on **Add device**.

Device	
Name	The name of the device
Template	The template to use with this device
Modbus/TCP server IP address	The IP address to use for a Modbus-TCP device
Modbus/TCP server port	The port used to connect to the Modbus-TCP server. Default = 502.
Modbus slave address	The unique Modbus slave address

Some templates support device-specific pre-configured alarms. The alarm conditions are set in the template and cannot be changed.

| Device-specific alarms	
Set	Click **Set** to set all alarms in the alarm list or an alarm group preconfigured in the template. To set a single alarm, use the check box for each alarm.
	The drop-down list to select an alarm class can be applied to a whole group or a single alarm. See also *Add/edit alarm parameters, p. 30*.
Clear	Clear all alarms for the device specific alarm list or alarm group.

3.5.3 Configuration | Pages
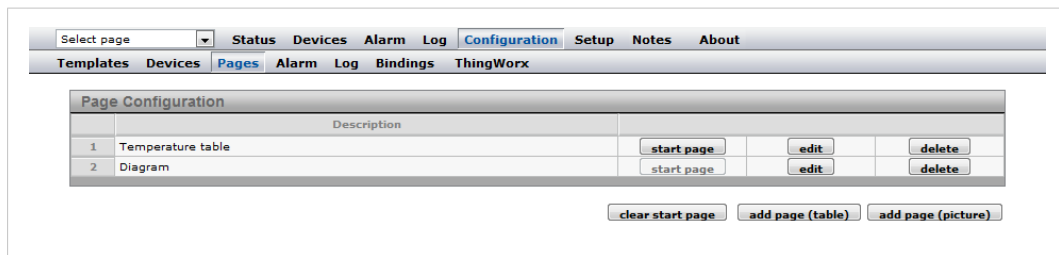
Fig. 36 Page configuration

A *page* is a customized interface for interacting with a connected Modbus device, using graphical or table representation of read data. A maximum of 30 pages can be added.

To create a new page, click on **Add page (table)** or **Add page (picture)**. Enter a name for the new page and click **OK** to save.

Click on **Edit** to edit an existing page, or **Delete** to remove it.

Click on **Start page** to make a page the first page presented when a user logs on. Click on **Clear start page** to revert to using the default start page.
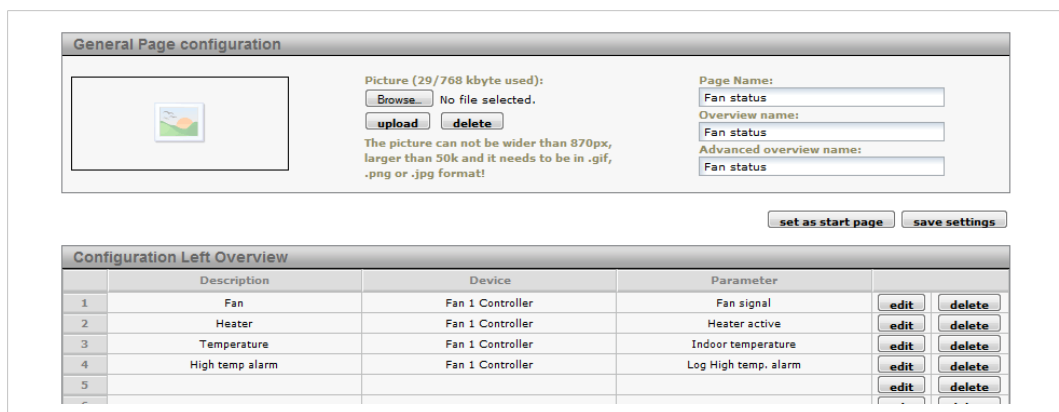

Fig. 37 General page configuration

General page configuration

Picture	An image can be uploaded which will be displayed at the top of the page. Click on browse to select an image file on your computer, then click on Upload to upload it to the Netbiter. Click Delete to remove the image.
	Uploaded image files will decrease the space left for log files. Keep the size of image files as low as possible!
Page name	Add a descriptive name for the page.
Overview name	The name shown in the **Select page** menu for all users.
Advanced overview name	The name shown in the **Select page** menu for administrators.
Set as start page	Make the page the first page presented when a user logs on.
Save settings	Save the settings made on this page.

After the General Configuration has been saved, it can be filled with parameters from the template. Each page can have one "normal" overview which is accessible for all users, and one advanced overview which is only accessible for admin level users. Each overview has 2 columns with 10 parameters in each column.

To add or delete a parameter in a row, click on **Edit** or **Clear**.

Fig. 38   Edit parameter

Configuration Left/Right Overview/Advanced Overview

|	
Device	Select a device
Group	Select a parameter group
Parameter	Select the parameter to be displayed on the web page
Description	A description that will be displayed next to the parameter
Presentation format	**Default** = Use the value format set in the template
	Hexadecimal = Show the value in hexadecimal format
	Binary = Show the value in binary format
Presentation scaling	The Modbus register value will be divided by this value before it is shown on the web pages, and multiplied with it before written to the Modbus device.
	Scaling is preferably set in the template, which will include scaling for use with alarms and logging.

3.5.4 Configuration | Alarm
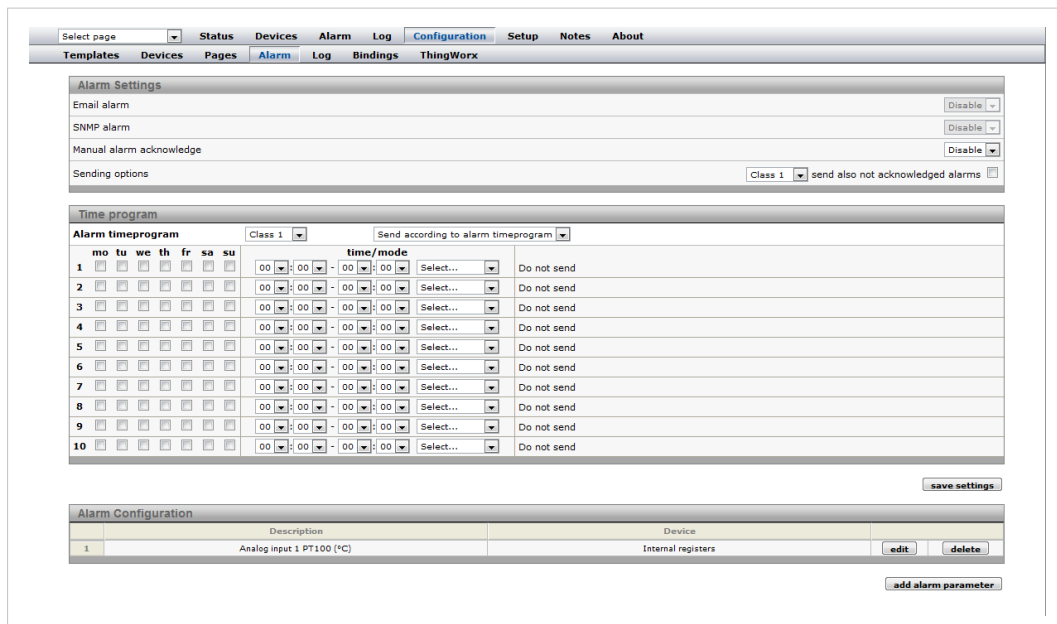
Fig. 39   Alarm configuration page

Alarm settings

Email alarm	Enables alarm messages to be sent as e-mail to users set up with the correct alarm class and a valid e-mail address.
	The e-mail server settings must also be correctly configured. See also *Setup	E-Mail, p. 19*.
SNMP alarm	Enables SNMP trap alarms if an SNMP manager has been configured. See also *Setup	SNMP, p. 20*.
Manual alarm acknowledge	If enabled, alarms must be manually acknowledged.
Sending options	**Class 1–10**: Select the alarm class to include in alarm messages.
	send also not acknowledged alarms: Check this box if messages should include alarms that have not been acknowledged.

Time program

Alarm timeprogram	Alarm messages can be sent immediately to all selected users, or at scheduled intervals according to an **Alarm timeprogram**. Time programs must be created separately for each alarm class.

Alarm Configuration

The alarm configuration section contains a list of all configured alarm parameters. Each alarm can be reconfigured by clicking **edit** or removed by clicking **delete**.

Click on **add alarm parameter** to add a new alarm. A maximum of 64 alarm parameters can be configured.

The poll time for alarms is ~20 seconds.

Add/edit alarm parameters

Fig. 40   Alarm parameters

Parameter select

Device   Select a device

Group   Select a parameter group

Parameter   Select the parameter to use for the alarm

Alarm trigger operation

Trig on   The condition that will trigger the alarm. Can be set to compare values in either decimal (**Value**) or binary (**Bit**) representation. The available conditions depend on the representation.

                      If scaling is used in the template, the value set here will be compared to the scaled value.

                      If the condition is set to **No response** the value represents the number of consecutive timeouts that will trigger the alarm.

Alarm properties

Alarm Class   The alarm class, used to sort which alarm is sent to which user.
                      See also *Setup | Users, p. 14*.

Severity   The severity of the alarm.

                      For SNMP the severity class *Clear* will be sent for an alarm that enters normal alarm condition.

Description   A text that will be displayed in the alarm list view and the alarm history, and sent to the SNMP manager (if configured).

Subject   The subject line of the alarm message to sent via e-mail.

Message   The message body of the alarm message to sent via e-mail.

3.5.5 Configuration | Log

Fig. 41 Log configuration page

The log can have a maximum of 64 log parameters configured, and is stored in a csv (comma-separated values) text file. This file can be viewed on the **Log | Graph** page, or downloaded and opened in a text editor or spreadsheet program such as Microsoft Excel.

| General Log Settings	
Estimated Log Time	Gives an estimation of the time before the log file is full. This estimation will depend on the configuration, i.e. the number of pages and parameters configured. The number and size of graphics used in the pages will also affect the log file size.
	If the log interval is set to a predefined time, this will show as the estimated log time.
Log Interval	Defines the time interval between the samples saved to the log file.
Log Type	Can be set to either overwrite the oldest entries as the log fills up (circular logging), or stop logging when the log space has been used up.
Maximum send log interval	This will set the time when a log should be sent. If a time period is selected the log will be sent with this interval, e.g. at the same minute for every hour when **At least every hour** is chosen.
Send log as E-mail attachment	If a Send log interval is specified the log file is sent as an e-mail attachment (if any users are configured to receive log e-mails).
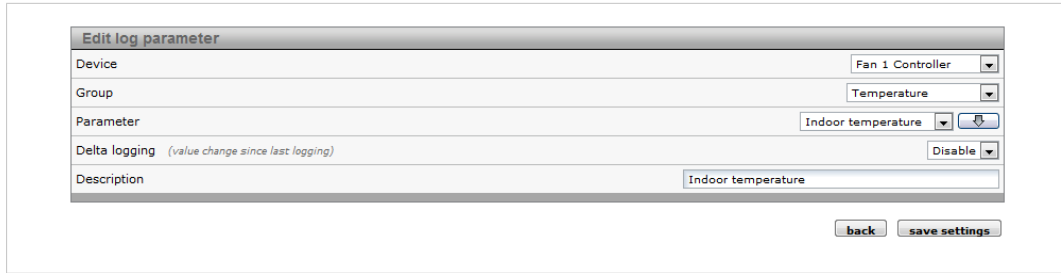
Fig. 42   Log parameters

To edit, delete or add log parameters, first click on **stop** (if the log is running) to stop the current log process.Then click on **edit** or **delete** for an existing log parameter, or click on **add log parameter** to add a new one. After you have finished adding/editing log parameters, click on **start**.

| Edit log parameter	
Device	Select a device
Group	Select a parameter group
Parameter	Select the parameter to log
Delta logging	If enabled, the difference between the two last samples will be logged.
	Example: The values read from a device parameter during the first 4 log cycles are: 5, 20, 32, 41. The logged values will then be: 5, 15, 12, 9.
Description	A text that will be displayed on the **Graph** page and in the downloaded log file.

3.5.6 Configuration | Bindings
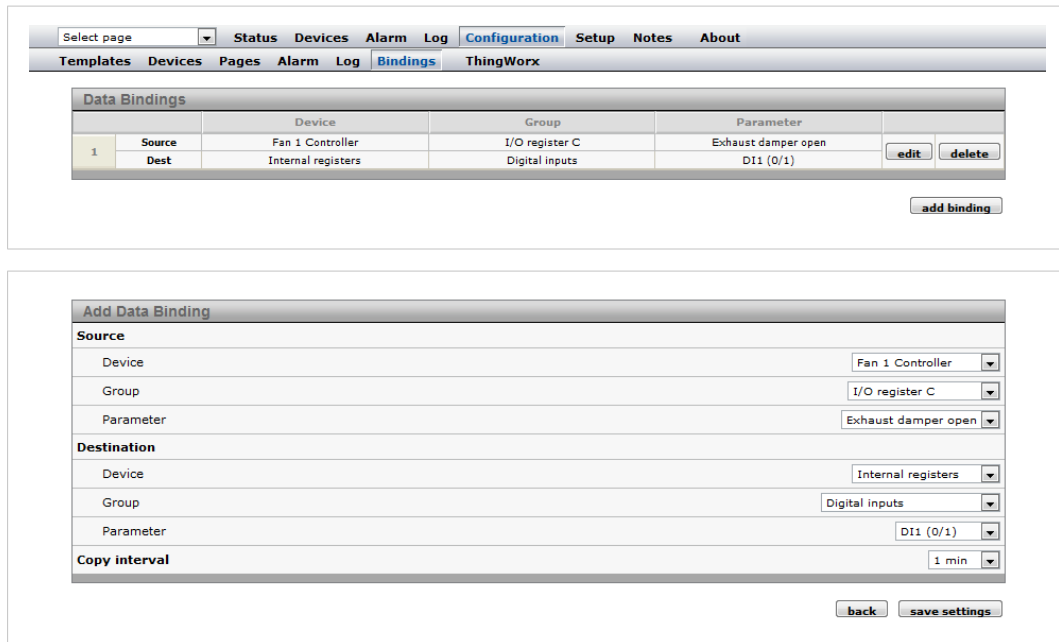
Fig. 43   Bindings configuration

Bindings makes it possible to copy one Modbus register to another.

Add Data Binding	
Source Device/Group/ Parameter	The device parameter to be copied
Destination Device/ Group/Parameter	The device parameter that will be copied to
Copy Interval	The time interval between each copy

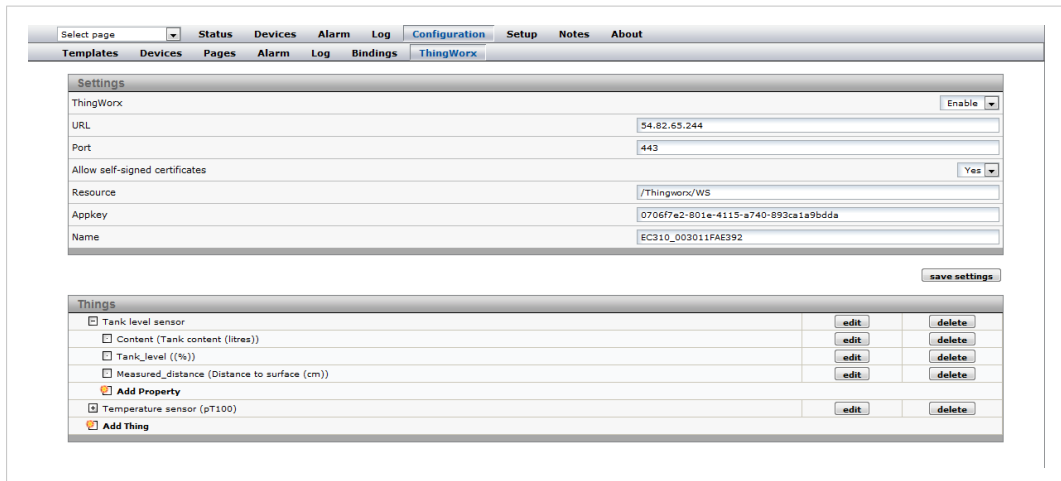## 3.5.7   Configuration | ThingWorx

Fig. 44   ThingWorx configuration
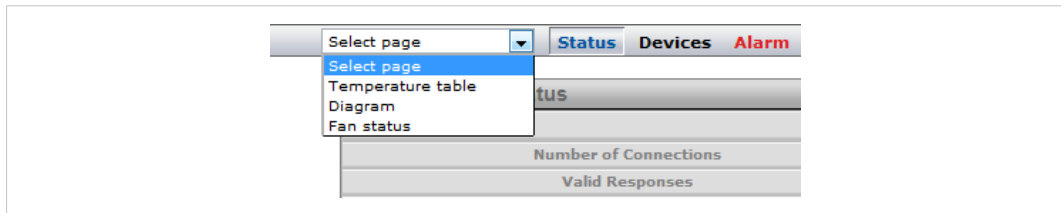
4   Usage

4.1   Select page

Fig. 45   Select page menu

Use the drop-down menu to select a page to display. If a page has been defined as *Start Page* it will open when you log in to the web interface. If no pages have been defined yet, the **Status** page will be used as start page.

4.2   Status

Fig. 46   Status page

Shows the current status of the Modbus interface and the internal/external modem (if present).
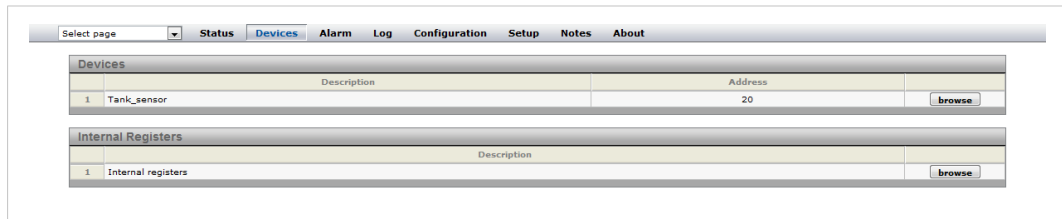
4.3   Devices

Fig. 47   Devices page

Lists all connected devices as well as the internal registers. Clicking on **Browse** will open a browser tree with all available groups and parameters for the device or internal register.
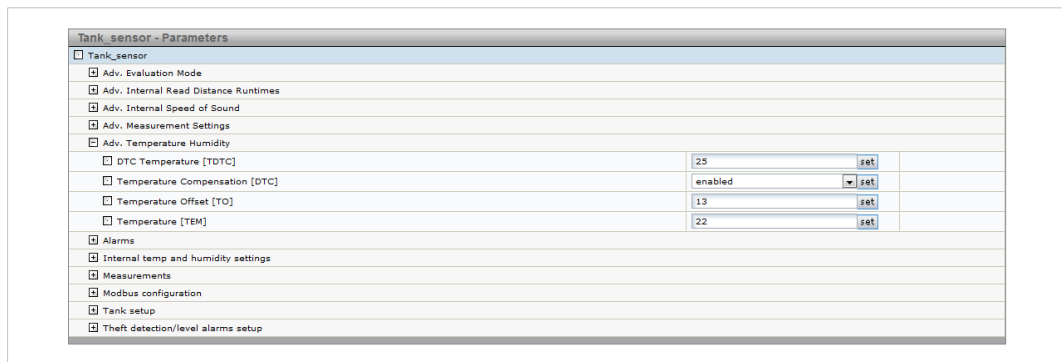
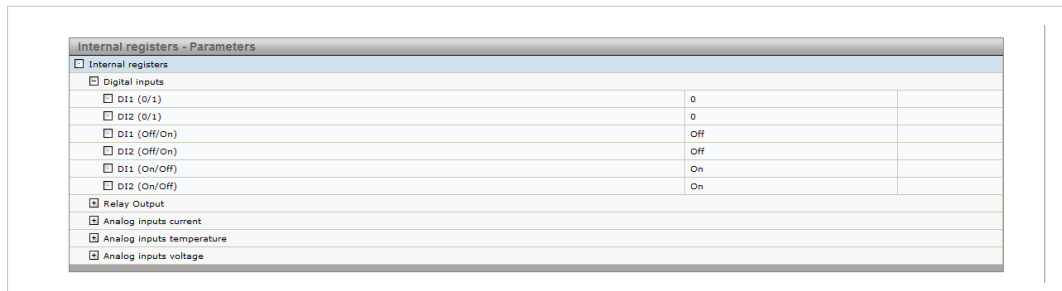

Fig. 48   Device parameter tree

Fig. 49   Internal register parameter tree

4.4   Alarm

Gives access to all configured alarm parameters, the current state of the alarms, and the alarm history.

When there is an active alarm the Alarm menu name will change color to red.

4.4.1   Alarm Status

Fig. 50   Alarm status page

Show active/Show all toggles between showing all configured alarms, or only those that are present and unacknowledged.

Alarms can be acknowledged individually by clicking on **Acknowledge**, or all at the same time by clicking on **Acknowledge all**. If an alarm does not require acknowledgement the button will be grayed out.

4.4.2   Alarm History

Fig. 51   Alarm history

Every status change for an alarm parameter is logged on the **Alarm History** page, along with information of the value for the parameter that triggered the alarm, and information about what alarm messages were sent by the Netbiter gateway.

The alarm history can hold a maximum of 100 entries. If the list is full and a new alarm occurs, the oldest alarm history entry will be deleted.

Show all events	All alarm events will be shown in the list.
Show occurrence	Only alarm entries of type *Occurred* will be shown.

Clicking on **Clear History** will clear the alarm history.

A Internal Registers

Holding register	Name	Values	Options	Comment
1	Digital input 1 status	0 or 1		Read only
2	Digital input 2 status	0 or 1		Read only
3	Number Active Connections MB/TCP	0-10		Read only
4	Number Active Internal Connections	0-10		Read only
	Serial Status (Modbus/TCP)			
5	Valid responses	0–65535		Can be cleared
6	Serial timeouts	0–65535		Can be cleared
7	CRC errors	0–65535		Can be cleared
8	Input Buffer overruns	0–65535		Can be cleared
9	Frame errors	0–65535		Can be cleared
10	Exception responses	0–65535		Can be cleared
	Serial Status (Buffered messages)			
11	Valid responses	0–65535		Can be cleared
12	Serial timeouts	0–65535		Can be cleared
13	CRC errors	0–65535		Can be cleared
14	Input Buffer overruns	0–65535		Can be cleared
15	Frame errors	0–65535		Can be cleared
16	Exception responses	0–65535		Can be cleared
	Serial Status (Internal requests and Webpages)			
17	Valid responses	0–65535		Can be cleared
18	Serial timeouts	0–65535		Can be cleared
19	CRC errors	0–65535		Can be cleared
20	Input Buffer overruns	0–65535		Can be cleared
21	Frame errors	0–65535		Can be cleared
22	Exception responses	0–65535		Can be cleared
	Configuration Registers			
23	Modbus/TCP Port	1–65535		Default = 502
24	Gateway Modbus address	(-1)–255		
		-1	Disabled	Default
		0–255	Enabled	
25	Modbus/TCP idle timeout	0–65535 (seconds)		Default = 60 s
		0	Disabled	
		1–65525	Enabled	
26	Baudrate	2400–115200 (bps)		Default = 9600
27	Parity	0–2		
		0	No parity	Default
		1	Even parity	
		2	Odd parity	
28	Number of Stop bits	1–2		Default = 1
29	Slave timeout time	25–65535 (milliseconds)		Default = 1000 ms
30	Physical interface	0–2		
		0	EIA-485 (RJ12)	Default
		1	EIA-232 (DSUB)	
		2	EIA-232 (RJ12)	

Holding register	Name	Values	Options	Comment
	Authentication			
31	Valid IP address 1	0–255		First byte of IP address
		0	Disabled	IP address auth disabled
		1–255	Enabled	
32	Valid IP address 2	0–255	Enabled	Second byte of IP address
33	Valid IP address 3	0–255	Enabled	Third byte of IP address
34	Valid IP address 4	0–255	Enabled	Fourth byte of IP address
35	Mask for Valid IP address 1	0–255	Enabled	First byte of mask
36	Mask for Valid IP address 2	0–255	Enabled	Second byte of mask
37	Mask for Valid IP address 3	0–255	Enabled	Third byte of mask
38	Mask for Valid IP address 4	0–255	Enabled	Fourth byte of mask

B   SNMP

If SNMP Alarms are enabled all alarms will be sent as SNMP traps to the host specified on the SNMP page.
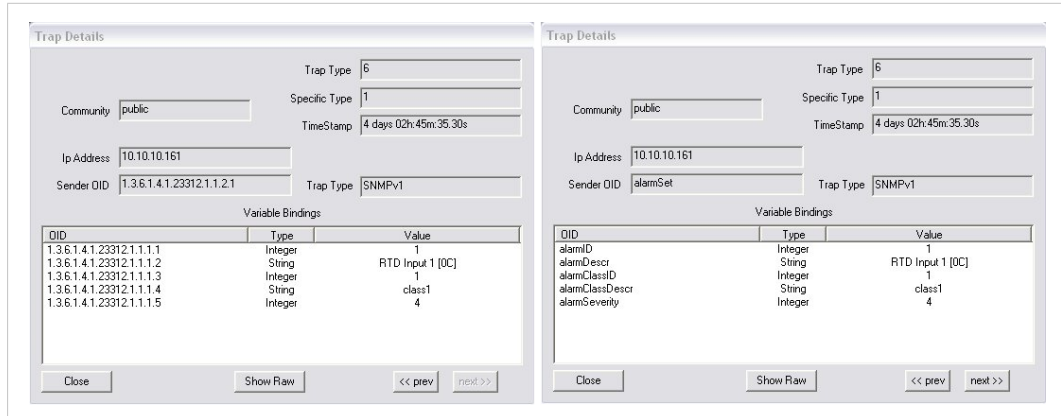

Fig. 52   SNMP trap example (high temperature alarm)

The OID is sent in the following numerical format:

```
.1.3.6.1.4.1.23312.1.1.2 [IP address][event]
```

```
.1.3.6.1.4.1.23312.1.1.[trap_id][trap_data]
```

where `23312.1.1` is the vendor/product identification.

Event 1 = Alarm set, event 2 = Alarm cleared.

The trap ID is divided into 5 messages with the following trap data:

1   Alarm ID

2   Alarm description

3   Class ID (1–10)

4   Class description

5   Alarm severity:

    0   Indeterminate

    1   Critical

    2   Major

    3   Minor

    4   Warning

    5   Cleared

C   Technical Data

Technical Specifications	Netbiter LC310	Netbiter LC350
Model name	NB301B	NB301A
Order code	NB1012-C NB1014-C (ThingWorx)	NB1013-C NB1015-C (ThingWorx)
Mobile communication	–	5-band 3G + GSM/GPRS
Antenna connector	–	SMA female
Ethernet interface	10/100 Mbit/s, RJ45 connector	
Alarm messaging	E-mail	
Relay output (NO)	Max. 24 V AC/DC, 1 A	
Digital inputs (DI1, DI2)	Dry contact type	
Analog inputs (AI1 - AI4)	0 to 20 mA, R = 3.3 %, A/D = 0.1 mV+0.15 % 0 to 10 VDC, R = 1.7 %, A/D = 0.1 mV+0.15 % AI1 and AI3 also support PT100, -50 to +150 °C (16-bit)	
Serial port #1	RS-232 up to 115.2 kbit/s	
Serial port #2 (isolated)	RS-485 up to 115.2 kbit/s	
Supported protocols	Modbus-RTU, Modbus-TCP	
Max. connected devices	32	
Baud rates	1200 to 115200 baud	
Mounting	Screw mount or DIN rail using optional mounting kit	
Dimensions (L x W x H)	92 x 135 x 27 mm	
Operating temperature	-40 to +65 °C	
Storage temperature	-45 to +85 °C	
Housing class	IP20	
Input voltage range	9–32 VDC	
Recommended power supply	24 VDC, 25 W	
Power consumption, typical	2.5 W @ 24 VDC	4.5 W @ 24 VDC
Certifications	See www.netbiter.com/support	

This page intentionally left blank