NetBiter® webSCADA 3
User Manual

Revision 3.10

IntelliCom Innovation AB
Pilefeltsgatan 73
SE-302 50 Halmstad
SWEDEN

Phone +46 35 18 21 70
Fax +46 35 17 29 09
email info@intellicom.se
www www.intellicom.se

Revision List

Revision	Date	Author	Chapter	Description
1.00	04-10-06	JOAK	All	First released version
1.10	04-12-12	JOAK		Added support for more datatypes
2.0	05-03-15	JOAK		New functionality, firmware release 2.0
2.01	05-06-20	JOAK	4.4, 4.8	Minor web-page updates
3.0	06-06-20	JOAK	All	New functionality, firmware release 3.10
3.01	06-10-23	JOAK	3.3.1, 4.2, 4.4.1, 5.3.3, 5.7.1	New functionality, firmware release 3.11
3.02	07-01-10	JOAK	4.6, 5.1, 5.2, 5.7	New functionality, firmware release 3.12
3.10	07-02-19	JOAK	1.3.5	New hardware revision, 1.4x

Preface

The data and illustrations found in this document are not binding. We 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 a commitment by IntelliCom Innovation AB. IntelliCom Innovation AB assumes no responsibility for any errors that may appear in this document.

Trademarks

NetBiter® is a Trademark of IntelliCom Innovation AB. All other trademarks or registered marks in this manual belong to their respective manufactures.

Table of contents

Warranty and support

To obtain fast and simple support for your NetBiter products, please use our Internet support service at http://www.intellicom.se/support. Here you will find the latest documentation, configuration utilities, drivers etc. You can also contact our support at support@intellicom.se.

Product return

If you experience any problems with a NetBiter device and wish to have it repaired or exchanged, you'll need to follow these steps:

- Obtain a Product Return Number, PRN, from http://www.intellicom.se/support.
  To get this number you'll need to provide some information about the problem you have, contact information etc.
- Print the "PRN Acknowledge side" and send it to IntelliCom together with the product.
  Make sure the PRN is visible on the outside of the package, and that the delivery is pre-paid, otherwise the delivery won't be accepted by IntelliCom. Also provide evidence of original purchase.
- If the faulty product is covered by the 12-month warranty, IntelliCom will repair or exchange the unit and return it within three weeks. If the product is not covered by Warranty, IntelliCom will respond with a cost estimation for repairing the unit.

Terminology

Term	Extract	Description
TCP/IP	Transmission Control Protocol/ Internet Protocol	TCP (Transmission Control Protocol) is a set of rules used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet.
HTTP	Hyper Text Transfer Protocol	HTTP is a set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the Web.
DHCP	Dynamic Host Configuration Protocol	DHCP is a standard protocol that automates the process of configuring network hosts by allowing hosts to obtain IP addresses and configuration parameters
Gateway		A device that makes it possible to transfer data between networks of different kind, e.g. Modbus/RTU and Modbus/TCP.
Template		Describes a Modbus slave device, as a collection of groups and parameters.
Device		A Modbus slave unit that is connected to the webSCADA.

This symbol indicates important information or useful instructions on how to use the product.

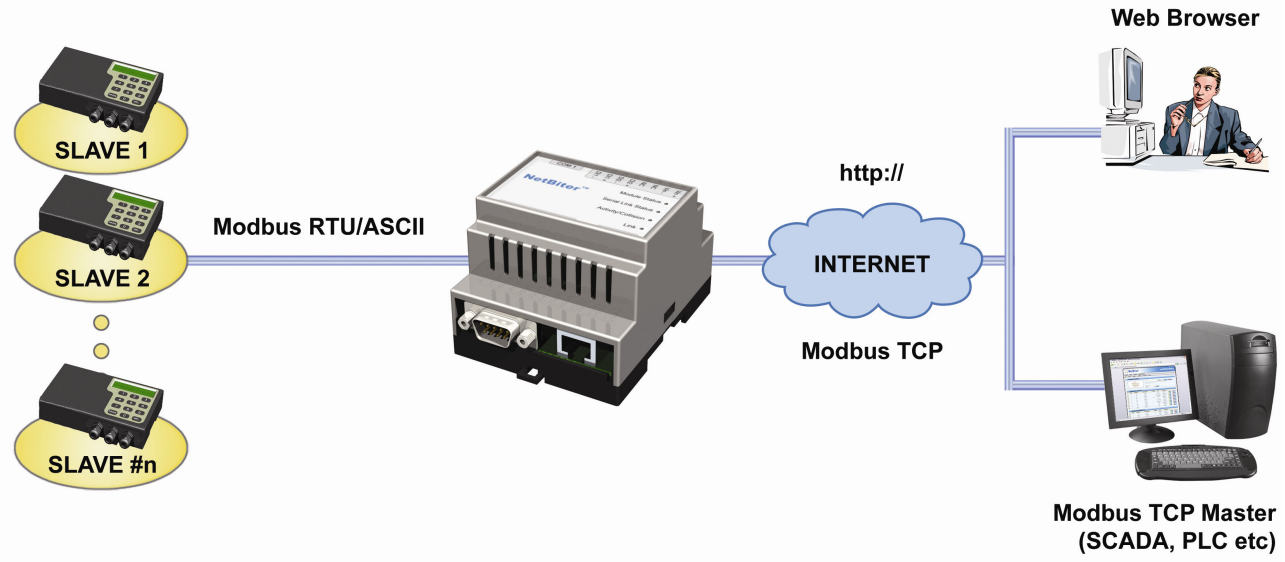
1 About the NetBiter Modbus Gateway

1.1 General

This application note describes how to create a configuration in the NetBiter® webSCADA module. The NetBiter® webSCADA module acts as a bridge from Modbus TCP to Modbus RTU, making it possible for a Modbus TCP based controller to connect with Modbus RTU based devices. The NetBiter® webSCADA is a device designed that is not only designed to provide the bridging function, but to also handle alarm management, data-logging as well as providing a web-based user interface for accessing data.

Some webSCADA features

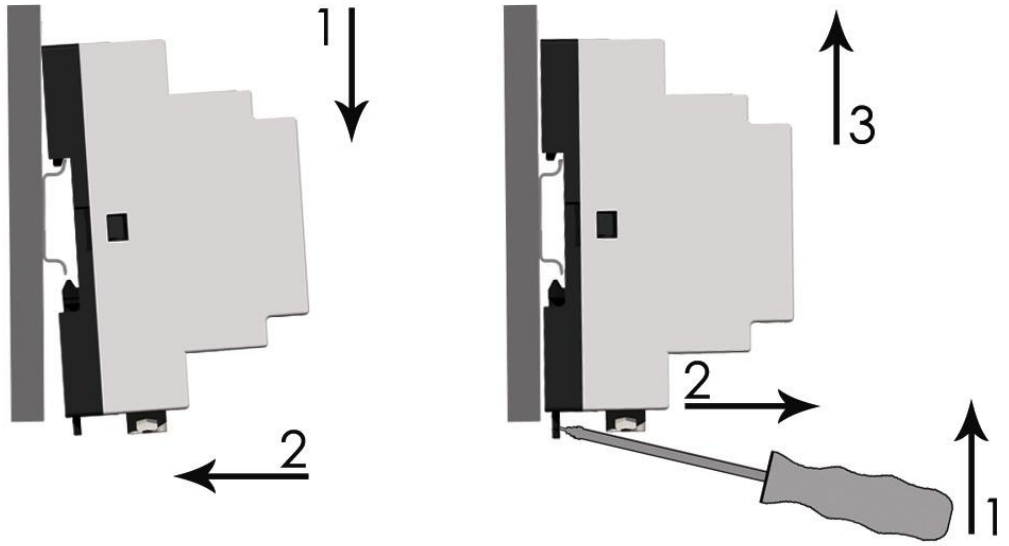
- Graphical interface that is easy to work with.
- Support for device templates to allow easy and flexible management of configurations.
- Advanced modem handling, with support for GSM/GPRS modems as well as analogue (PSTN) modems.
- Improved alarm handling, now with alarm history and SNMP support.
- Language support.
- Support for sending log-files with email.



The NetBiter Modbus Gateway supports an RS-232 connection through a 9-pole DSUB or RS-485 through an RJ12 connector. It also supports 10/100Mbps Ethernet through a standard Ethernet connector (RJ-45). It can be configured via a user-friendly web-interface or by using the NetBiter Config utility.

1.2 Mounting

A – Snap on **B – Snap off**



1 – Snap the NetBiter on to the DIN-rail (as described on picture A above).

2 – Connect the Ethernet cable to the RJ45 connector.

3 – Connect the ModbusRTU network to the DSUB connector (RS-232) or the 6-pole RJ12 connector (RS-485).

4 – Connect the Power Supply and apply power.

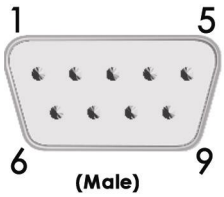
5 – Now you can start using the Gateway. Use the "NetBiter Config Utility" to configure the IP address and other network settings. See section 2.1 for further information.

The default IP address of the NetBiter is 10.200.1.1
Please change this IP-address to a valid address in your network. Also, make sure not to power up more than one network attached NetBiter before IP-address is changed or DHCP enabled.

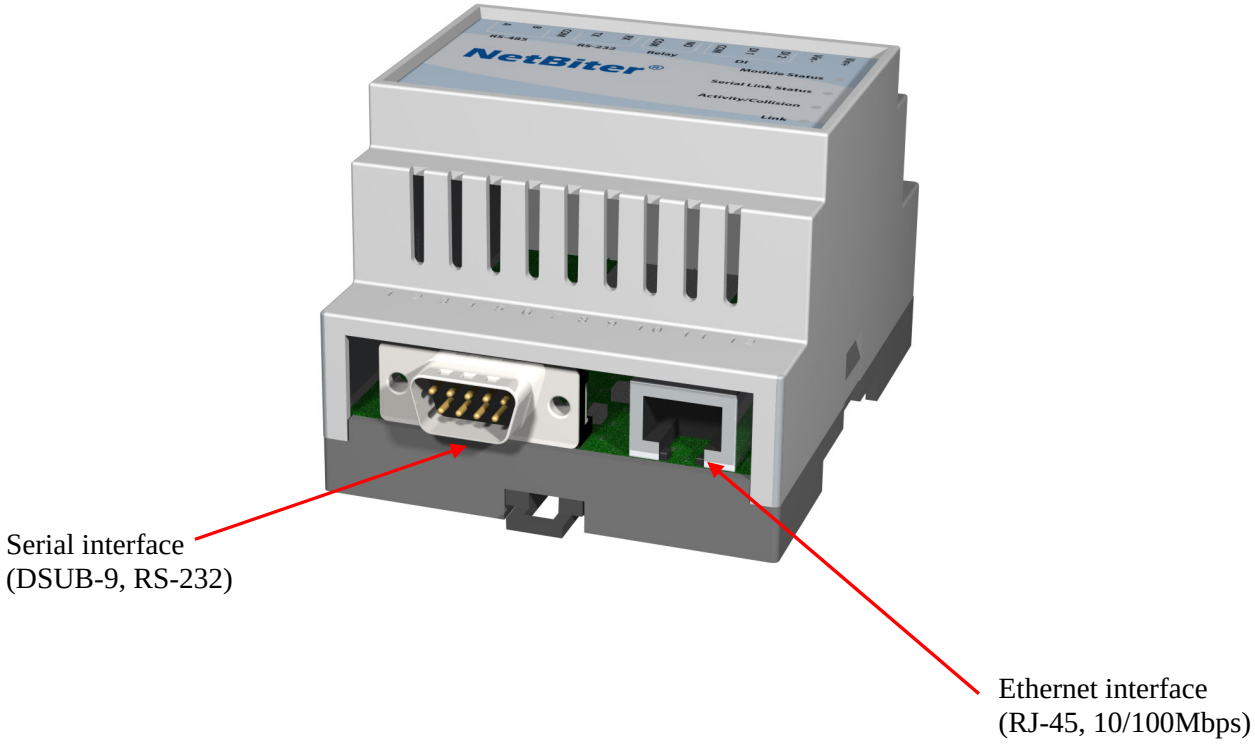
1.3 Connectors

1.3.1 ModbusRTU or Modem interface, RS-232

The 9-pole DSUB, male connector on the NetBiter unit contains an RS-232 interface. This port can be used to connect to any equipment with an RS-232 interface.

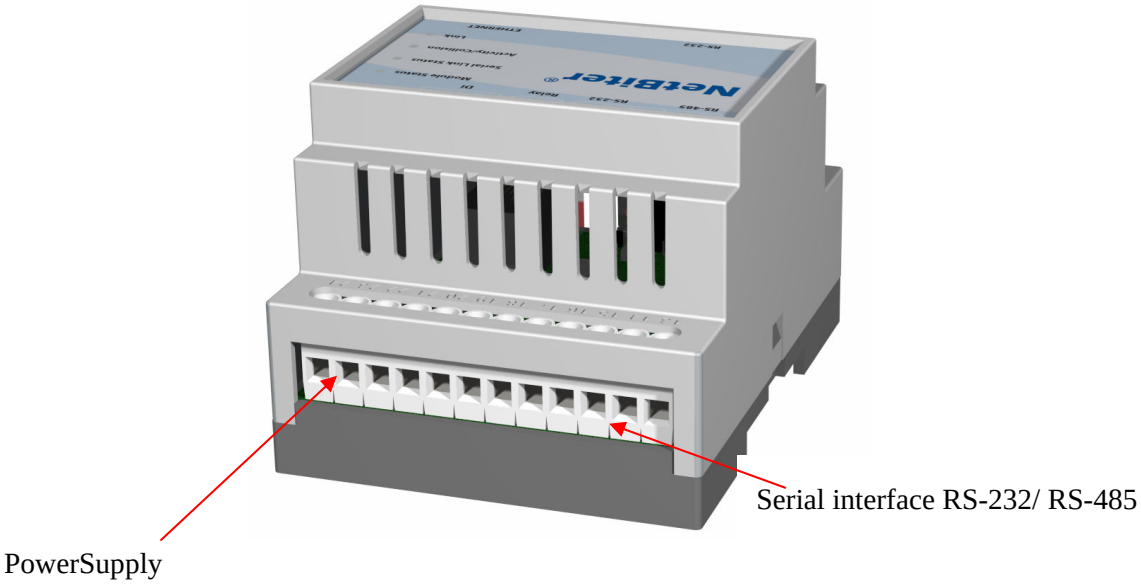


Pin number	Function
1	CD (Carrier Detect)
2	Rx (Receive)
3	Tx (Transmit)
4	DTR (Data Terminal Ready)
5	GND
6	DSR (Data Set Ready)
7	RTS (Request To Send)
8	CTS (Clear To Send)
9	RI (Ring Indicator)



1.3.2 Ethernet interface

The Ethernet interface supports 10/100Mbps, using a standard RJ-45 connector.



1.3.3 Power supply connection

The NetBiter can be powered by a 9-32VAC/DC supply (Power requirement 1.7W).

1.3.4 Digital inputs

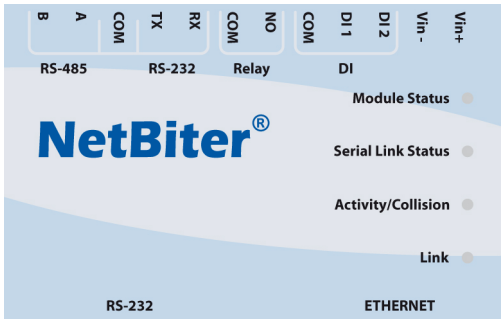
The digital inputs are opto-isolated, and can accept a **10-24VDC** signal for logic HIGH input.
For logic LOW the voltage should be in the range **0-2VDC**.

The status of the inputs can be read in the Gateway Internal Registers (if enabled).
See section 5.2.1 for more information.

1.3.5 RS232/RS485 interface

Pin number	Function
24	Vin+
23	Vin- (Ground connection)
22	Digital input 2+
21	Digital input 1+
20	Digital input Common
19	No Connect
18	No Connect
17	RS-232 Receive (Input)
16	RS-232 Transmit (Output)
15	Common
14	RS-485 Line A
13	RS-485 Line B

1.4 LED Indicators



LED description

Name	Colour	Function
Module Status	OFF	No power
	Green	Module is running in normal mode
	Orange	During boot-up
Serial Link Status	Flashing Green	Serial Packet receive
	Flashing Red	Serial Packet transmit
	Orange	During boot-up
Ethernet Activity/Collision	Flashing Green	Ethernet Packet received
	Flashing Red	Ethernet Collision detected
Link	OFF	No Ethernet Link detected
	Green	Ethernet network detected, 10Mbps
	Orange	Ethernet network detected, 100Mbps

2 Getting started

2.1 Configure the NetBiter IP-address

2.1.1 About the NetBiter Config utility

The NetBiter Config utility is a PC-based configuration utility to set TCP/IP network settings in the NetBiter. This utility has the ability to scan the Ethernet network for connected NetBiter devices and let the user set IP-address, net mask, gateway, DNS and hostname for each unit.

2.1.2 Installation

System Requirements

- Pentium 133 MHz or higher
- 5 Mb of free space on the hard drive
- Win 95/98/ME/NT/2000/XP
- Network Interface Card (Ethernet)

Installation Procedure

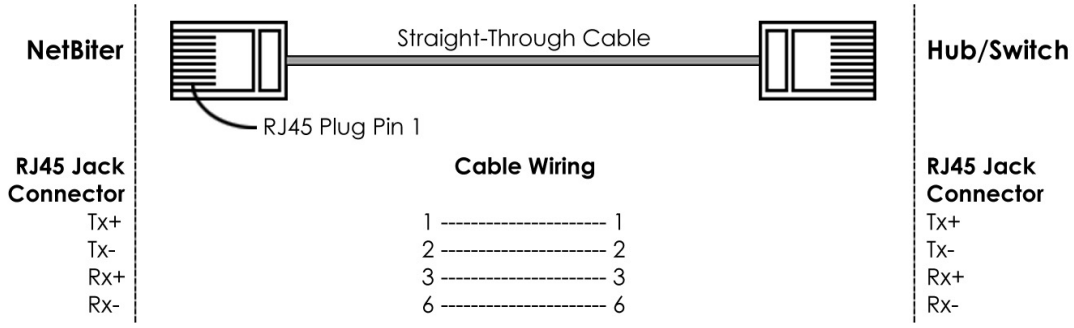
There are two methods to install the NetBiter Config utility; either download it from the IntelliCom website or use the installation CD-ROM.

- Using the CD-ROM: Run “Setup-NetBiterConfig.exe” and follow the instructions.
- From website: Download the self-extracting installation package “Setup-NetBiterConfig.exe” from http://www.intellicom.se/support and run it.

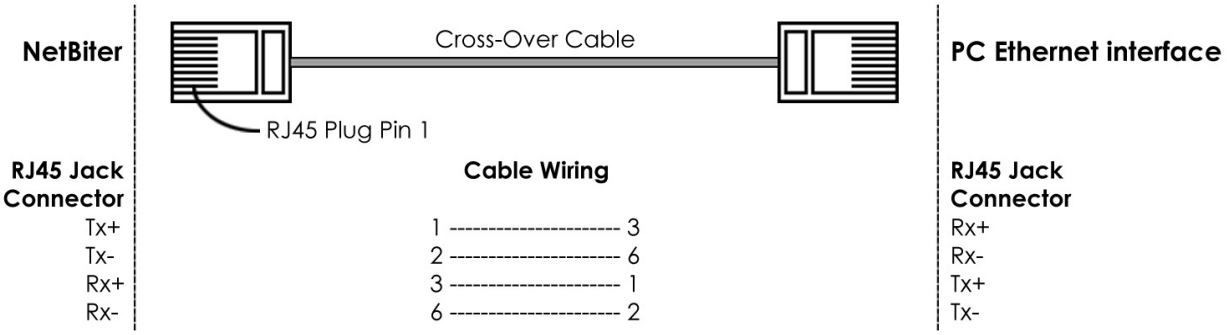
2.1.3 Scanning for connected devices

First ensure that you have connected the NetBiter units you want to install on the same Ethernet network as the PC is connected to. Use standard Ethernet cables, straight-through or crossover cable depending on how you connect to the device. See pictures below for details.

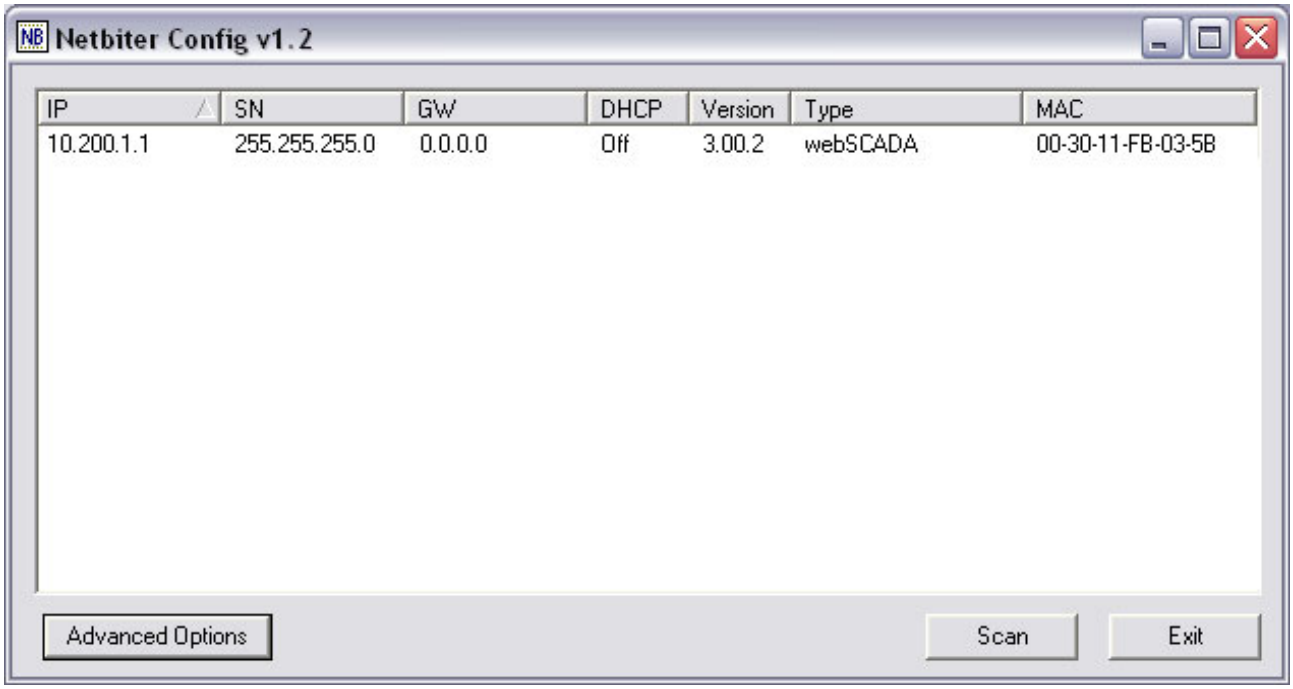
Connecting the NetBiter to a hub or Switch



Connecting the NetBiter directly to a PC



When the NetBiter Config utility is started, it will scan the Ethernet network for NetBiter devices. All detected devices will be presented in a list in the main window. If you want to force a new scan for devices, you can press the "**Scan**" button.



IP: The IP address of the NetBiter

SN: The subnet mask

GW: The default gateway

DHCP: Dynamically assigned IP address On/Off

Version: Firmware version

Type: Product type (webSCADA-Modbus)

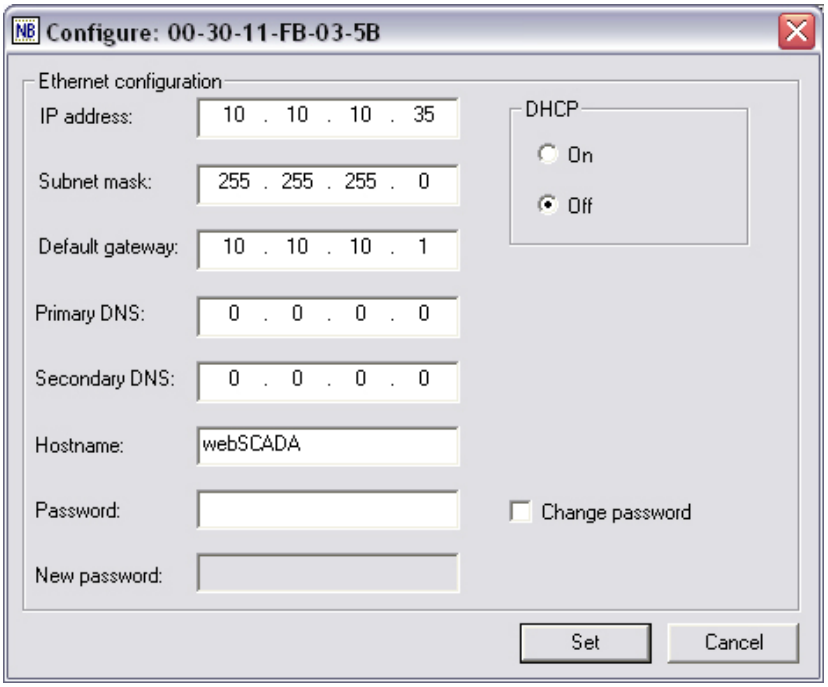
MAC: The Ethernet MAC address

Use the "Advanced Options" button to enable the NetBiter Config DHCP Server. This is useful when you have set DHCP to "On" in the NetBiter, but don't have a DHCP-server available on the network.

2.1.4 Changing IP settings

To change the IP settings on a detected device, double-click on the device you want to configure in the list of devices. This will open up a dialog where you can enter the desired IP configuration.

To obtain the necessary information about IP address, subnet mask etc. please contact your network administrator.



DO NOT SET DHCP TO "ON" IF YOU DON'T HAVE A DHCP-SERVER AVAILABLE ON THE NETWORK.

Host Name: Here you can enter a hostname of your device (**optional**).

IP Address: The IP address of the NetBiter.

Netmask: The subnet mask

Gateway: The default gateway

Primary DNS: The primary Domain Name Server (**optional**)

Secondary DNS: The secondary Domain Name Server (**optional**)

The default password for authentication of the new settings is "**admin**".

Pressing "**Set**" will cause the NetBiter device to reboot and after that the new settings will be enabled.

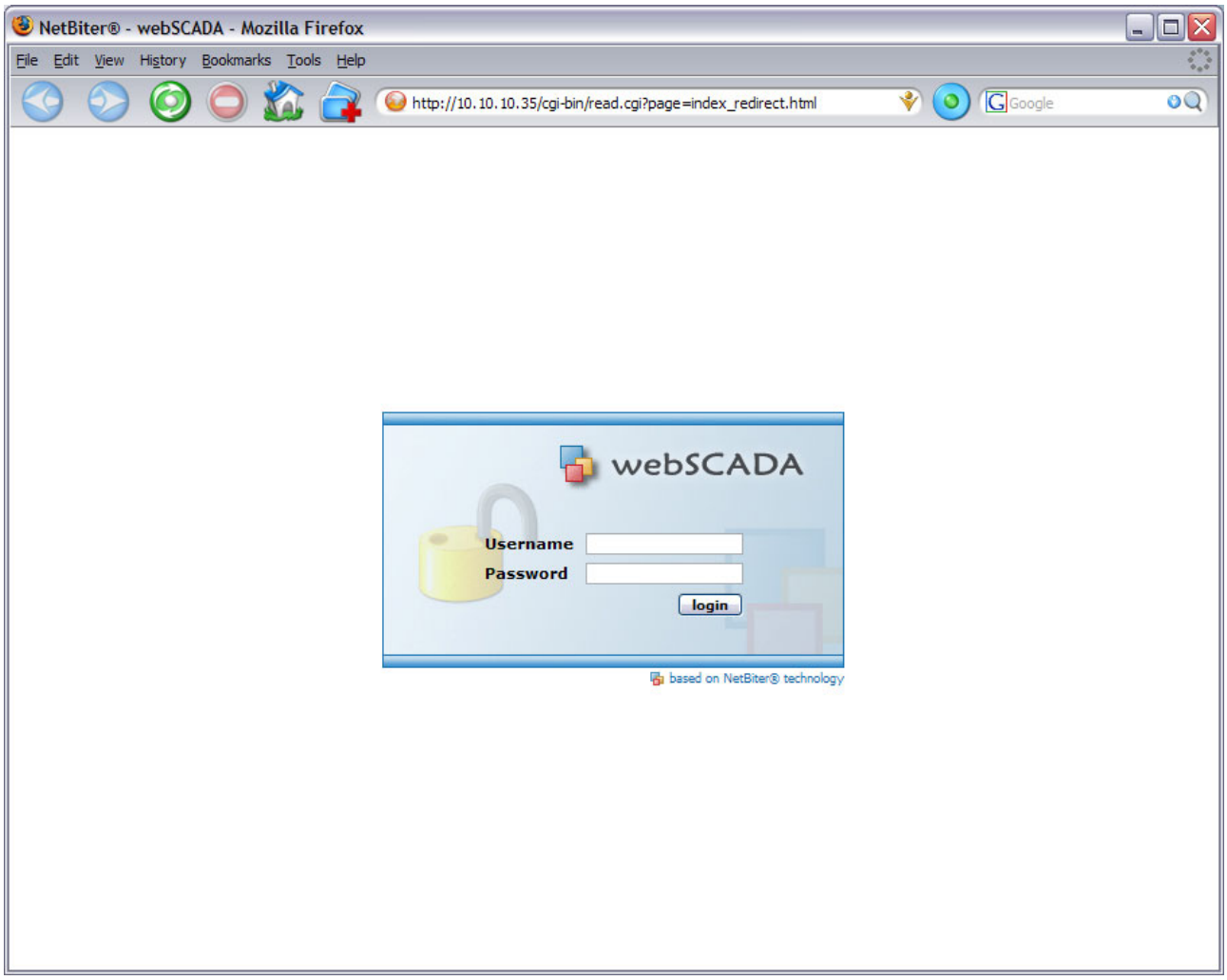
You can test the new settings by opening a web-browser and enter the IP you assigned to the device. If you selected DHCP and want to know what IP your device have been assigned, you can do a new scan with the NetBiter Config utility to view the new network configuration.

2.2 Log in

Open a web browser (Internet Explorer for example) and enter the IP address you have set on the NetBiter unit with the NetBiter Config utility. For example, if you entered the address 10.10.10.35 then you should enter the text below in the address field of the browser and press enter.

http://10.10.10.35

Now you should see the login screen:



To be able to configure the Gateway you should enter "**admin**" in the user-name box.
The default password is "**admin**".

You can later change the default password to something else (recommended).
This will be described in section Users .

If you have problems to log in and you are sure that your password is correct, make sure that "Caps Lock" is not enabled on your keyboard.

3 Web-page overview

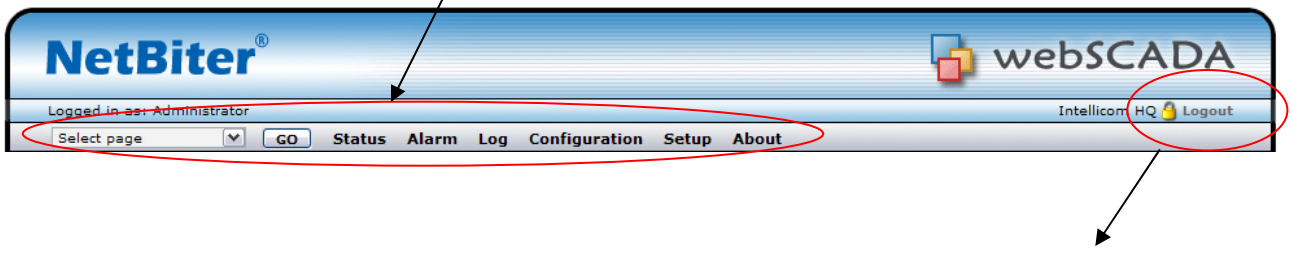
3.1 Browser requirements

The web-pages are optimized for Internet Explorer 6.0 and Mozilla Firefox. Other browsers can work as well, but the web-pages might appear differently. **The browser must be JAVA enabled, to use pages with JAVA content (like the graph page).** If it's not, please visit www.java.com to download a JAVA-plugin for your browser.

The picture below shows the welcome screen which is shown when you first log into the module.

3.2 Menu overview

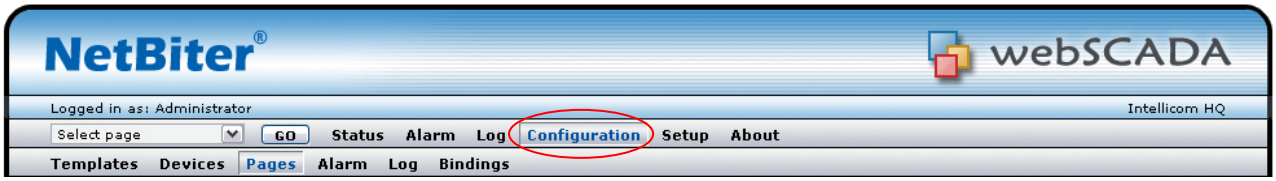
To navigate on the web-pages, use the menu items available: Select Page(**Go**), Status, Alarm, Log, Configuration and Setup.



Logout Button

3.2.1 Configuration menu

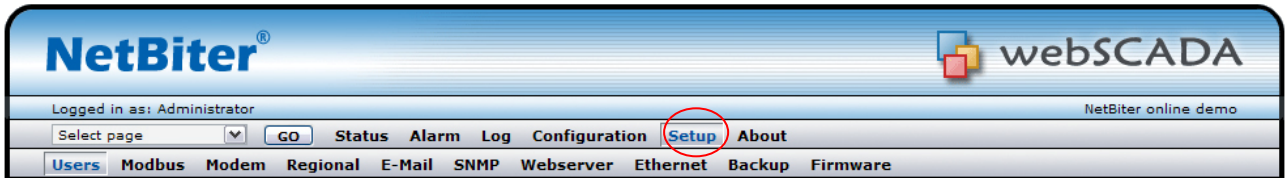
When you choose the **Configuration** menu, a sub menu will appear:



- The "**Templates**" configuration sub-menu will be used to create, edit and backup templates for your devices.
- On the "**Devices**" screen you define the devices which you connect to the webSCADA.
- On the "**Pages**" screen you create and edit the structure of the presentation web-pages and also select parameters to be presented.
- The "**Alarm**" screen can be used to enable/disable SMS/Email/SNMP alarms, and also to create and modify alarm parameters.
- On the "**Log**" configuration screen it's possible to configure the behaviour of the log-file, and also create/modify log-parameters.
- The "**Bindings**" configuration screen makes it possible to enable automatic parameter "copying" from one Modbus slave to another at a configurable interval.

3.2.2 Setup menu

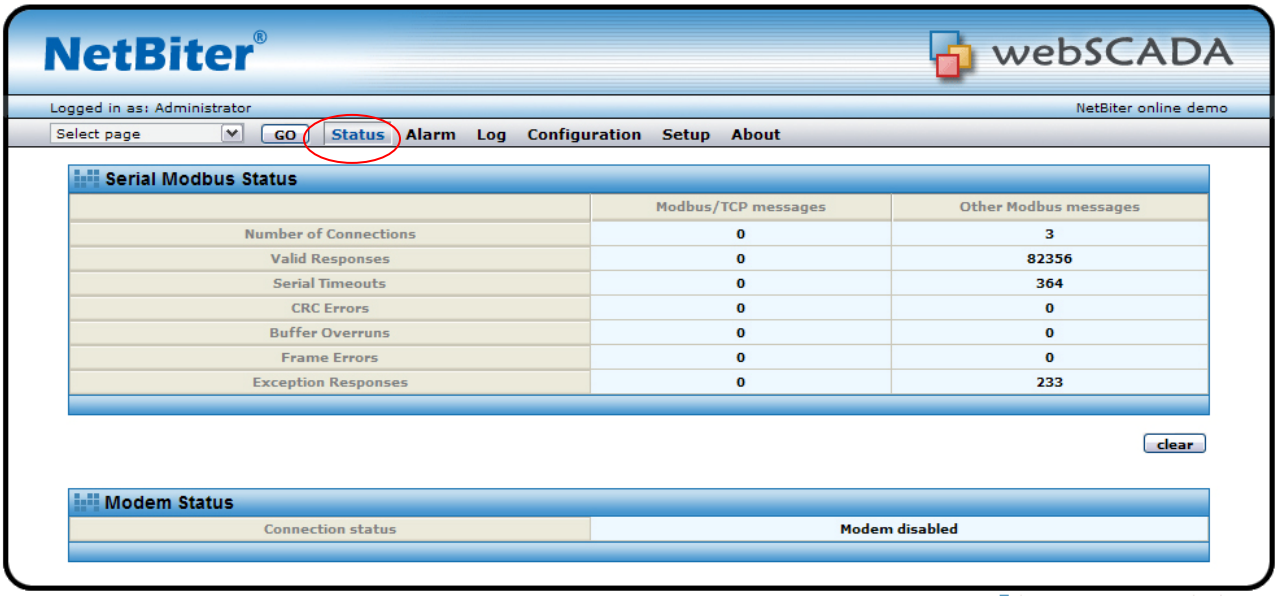
When you choose the **Setup** menu, a sub menu will appear:



- The "**Users**" screen is where all things related to user management are handled.
- The "**Modbus**" screen handles all ModbusRTU and ModbusTCP configuration.
- The "**Modem**" screen handles all modem configurations (Analogue, GSM, GPRS, dial-up, dial-in).
- The "**Regional**" settings screen configures things like date/time and generic module information.
- The "**E-mail**" screen configures all that is needed to send emails from the webSCADA.
- The "**SNMP**" screen makes it possible to configure SNMP trap properties.
- The "**Webserver**" screen can be used to define which port the webSCADA web-server should use.
- The "**Ethernet**" screen handles all TCP/IP configurations, like IP-address, DHCP, DNS etc.
- On the "**Backup**" screen it's possible to backup/restore all settings, and also do a factory reset of the webSCADA module.
- The "**Firmware**" screen can be used to download new firmware to the module.

3.3 Status

This page shows some status information about the Modbus interface. The Status screen is split into two columns, “Transparent queries” and “Internal queries”. The Transparent fields shows information about requests that originate from a ModbusTCP master attached to the gateway, and the internal fields shows information about requests that originate from either internal applications (Log/Alarm) and WebPages.



Number of connections: Indicates the number of open connections to a Modbus TCP master. Internal queries indicate number of pending queries from WebPages + the internal connection from (Alarm/Log) application.

Valid Responses: Counts valid responses from the Modbus/RTU slaves.

Serial Timeouts: The number of time-outs from attached slaves.

CRC Errors: The number of CRC errors on incoming Modbus/RTU responses.

Buffer Overruns: If an incoming Modbus/RTU response is larger than 300 bytes, this will cause the input buffer to overflow.

Frame Errors: If an incoming Modbus/RTU response has incorrect length or some other fault in the frame, this will cause a Frame Error.

Exception Responses: Counts all exception responses from the connected Modbus/RTU slaves.

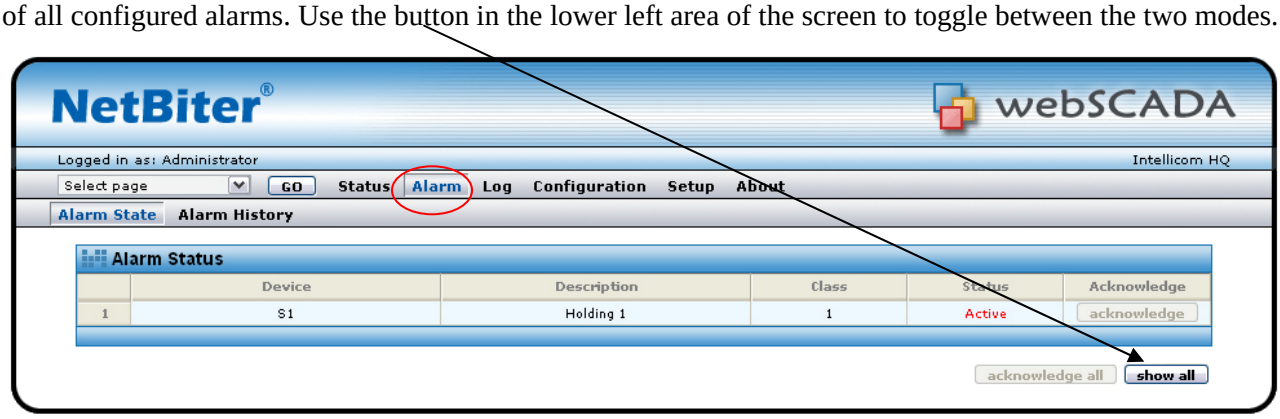
3.3.1 Modem Status

The modem status field gives information about what state an attached modem is in.

- Connecting to Internet:
  Calling Internet Service Provider and negotiate for a connection.
- Waiting for incoming connection:
  The unit is waiting for an incoming call.
- Waiting for Event/Alarm:
  The unit is in standby mode, and when an alarm or event appear it will connect to Internet.
- Connection established:
  A connection to Internet is established and data will be sent.
- Incoming connection is in progress:
  There is an incoming call and correct baud rate, username and password is being verified.
- Modem disabled:
  Not possible to connect using the modem

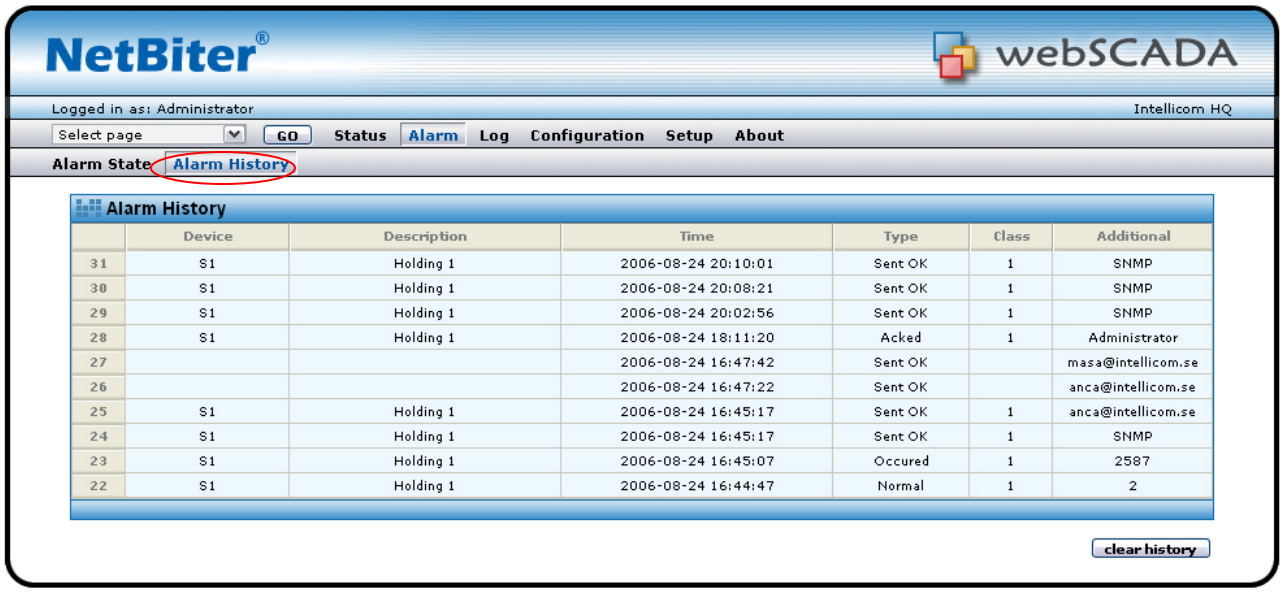
3.4 Alarm

The Alarm page shows all active and unacknowledged alarms. It is also possible to select to view the status of all configured alarms. Use the button in the lower left area of the screen to toggle between the two modes.



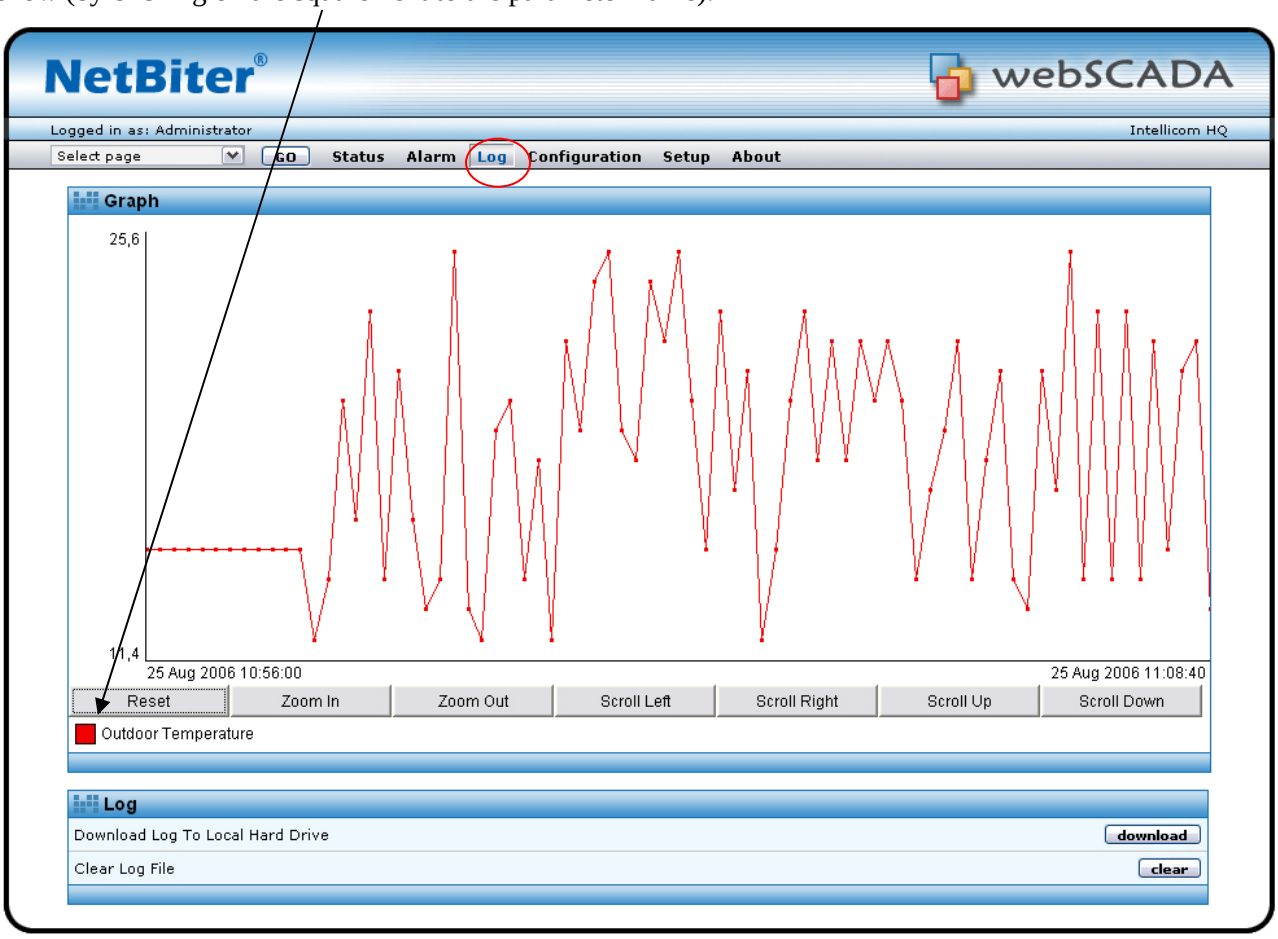
3.4.1 Alarm history

The “Alarm History” screen shows all alarms that have occurred. To clear this list, click the “clear history” button.



3.5 Log

From this page it's possible to download the log file from the webSCADA (if logging has been enabled). Simply click the "**download**" button to download/view the file, or click the "**clear**" button to remove all data from the log-file. To view the log-file as a graph, make sure that JAVA is installed on your computer. The graph will show all parameters in the log-file, but in the graph it's possible to select which parameters to show (by clicking on the square next to the parameter name).



4 Module Configuration

An important concept for the webSCADA is the usage of templates. This allows the user to define templates for different products and configurations, and then easily re-use and distribute them. A template contains properties for available parameters in a device of a certain type. These properties includes: Parameter Names, Modbus register types and addresses, data scaling and presentation.

See also Application Note **AN-1003** for more details about how to create a configuration.

(Can be downloaded from support.intellicom.se).

4.1 Work-flow

Follow these steps to get your webSCADA operational:

1 – Do all generic Setup, like assigning an IP-address (Setup/Ethernet), add/modify users (Setup/Users), configure the Modbus interface (Setup/Modbus) and set date/time etc (Setup/Regional).

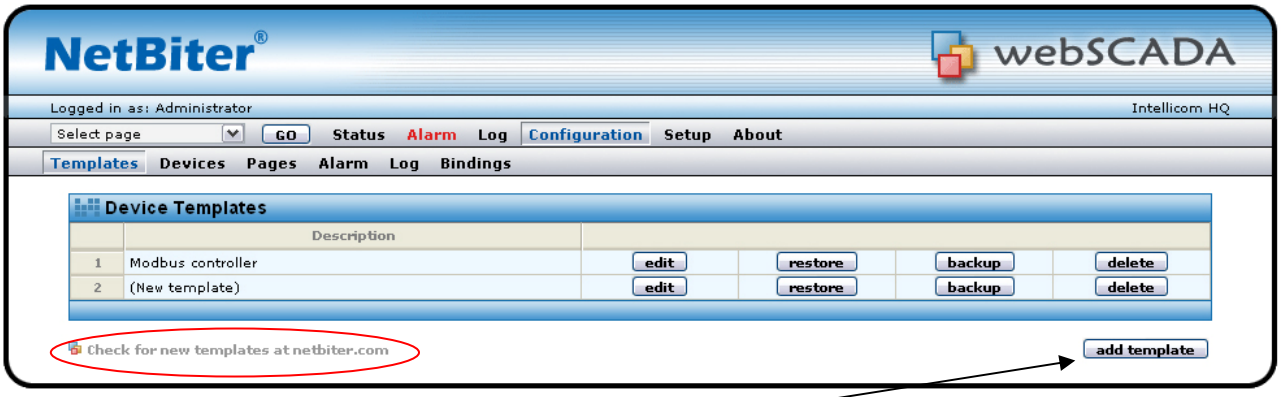
2 – Create a template (Configuration/Templates). A Template consists of one or several groups, and each group is a collection of Modbus Parameters.

3 – Define your Devices (Configuration/Devices). A Device is simply a Modbus slave, with a unique Modbus address. For each Device, you apply a Template.

4 – Create your Application! Now you can define your web-pages, alarms, log entries and bindings.

4.2 Create a template

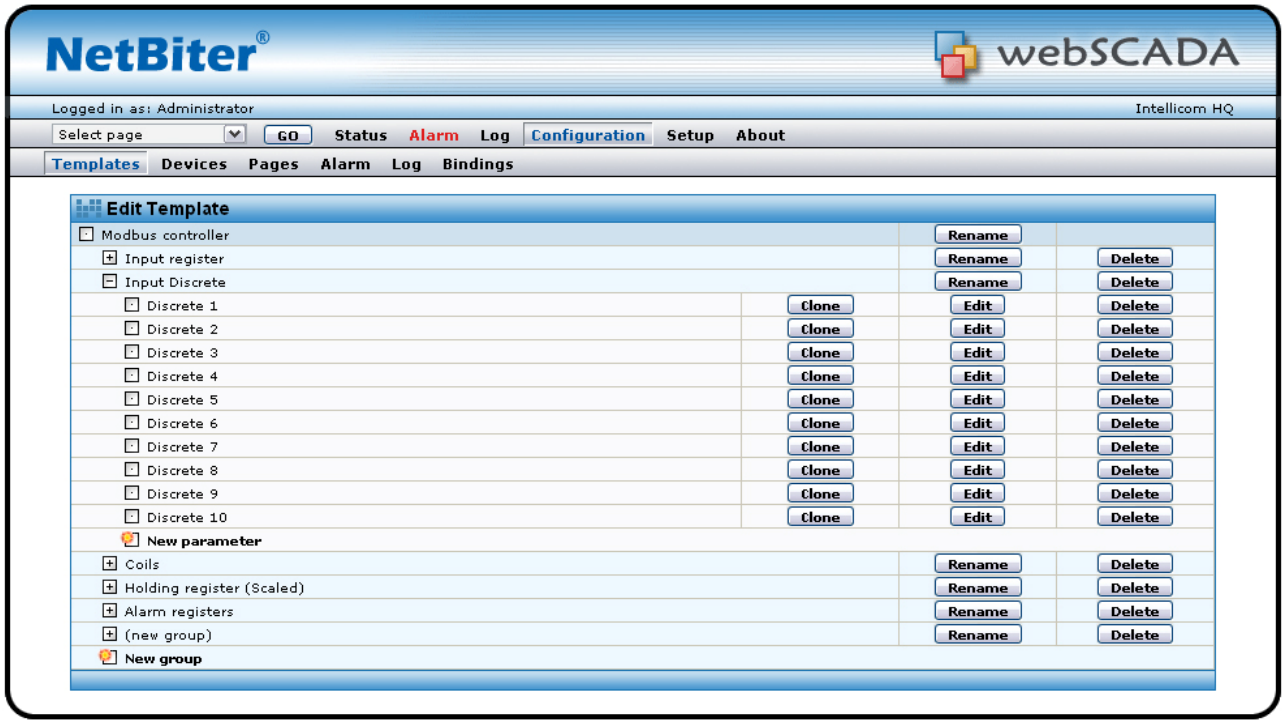
Clicking on the "Configuration/Templates" link will bring up the following screen:



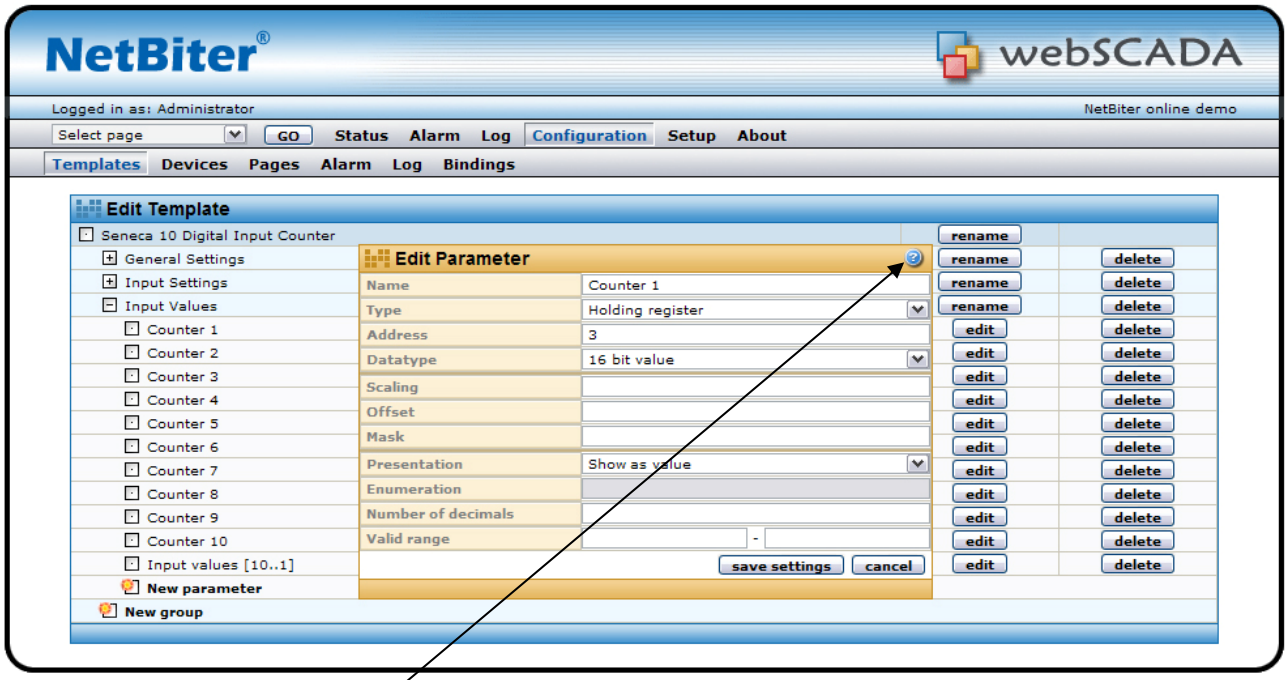
To create a template, click the "add template" button. This will create a "New template" in the list, which you now can edit. This will bring up the "Edit Templates" page where it's possible to add new groups (a collection of parameters) and new Parameters. From this page it's also possible to backup, restore and delete templates.

Also check out the IntelliCom Template page, where Templates from different manufacturers will be published.

You must always add a Group, before you can add a Parameter.



When you have created a Group, and at least one parameter, it's possible to edit the Parameter by clicking the "edit" button. This will bring up the following screen (Edit Parameter):



Click on the "?" to view the online help.

The "**Edit Parameter**" screen contains the following fields:

Name – Description of the parameter.

Type – Modbus type (Holding, Input, Coil, Discrete)

Address – Modbus address

Datatype - Defines the datatype of the Modbus register. Can be one of the following:

Unsigned 16 – 16-bit positive value
Signed 16 **–** 16-bit value, with sign

Unsigned 32 - 32-bit positive value. Most significant word (register) on **low** address.

modbus reg	i		i+1	
Int32	1(MSB)	2	3	4(LSB)

Signed 32 - 32-bit value, with sign. Most significant word (register) on **low** address.

modbus reg	i		i+1	
Int32	1(MSB)	2	3	4(LSB)

Unsigned 32 (swapped) - 32-bit positive value. Most significant word (register) on **high** address.

modbus reg	i		i+1	
Int32 (s)	3	4(LSB)	1(MSB)	2

Signed 32 (swapped) - 32-bit value, with sign. Most significant word (register) on **high** address.

modbus reg	i		i+1	
Int32 (s)	3	4(LSB)	1(MSB)	2

Float – 32-bit floating point. (IEEE-754) Most significant word (register) on **low** address.

modbus reg	i		i+1	
Float	1(MSB)	2	3	4(LSB)

Float (swapped) - 32-bit floating point. (IEEE-754) Most significant word (register) on **high** address.

modbus reg	i		i+1	
Float (s)	3	4(LSB)	1(MSB)	2

Double - 64-bit floating point. (IEEE-754) Most significant word (register) on **low** address.

modbus reg	i		i+1		i+2		i+3	
Double	1(MSB)	2	3	4	5	6	7	8(LSB)

Double (swapped) - 64-bit floating point. (IEEE-754) Most significant word (register) on **high** address.

modbus reg	i		i+1		i+2		i+3	
Double (s)	7	8(LSB)	5	6	3	4	1(MSB)	2

Scaling - The Modbus register value will be <u>divided</u> by the scale value before presented on the web-page, logged or compared with for alarm.
It will be <u>multiplied</u> with the scale value before value is written to a slave device.

Examples:

Modbus register value = 510, Scale value = 10 → 51,0 will be viewed on web-page.

Modbus register value = 5118, Scale value = 100 → 51,18 will be viewed on web-page.

Web-page input = 127,5 Scale value = 10 → 1275 will be written to Modbus register.

Offset – The Modbus register value will be subtracted with the offset value before it is presented on the web-page, logged or compared with for alarm. If scaling is also in use it is done before the offset is subtracted.

The Offset value will be added to the value before value is written to a slave device. If scaling is also in use it is done after the offset is added.

Mask - Is used to mask out specific bits from the Modbus register, on the webpage the value is presented in binary. The Modbus register will be masked (logic and) and shifted to the right before the value is presented on the web-page, logged or compared with for alarm.

Examples:

Modbus register value = 214 (D6 hex), Mask = 240 (F0 hex) → 1101 (13) will be viewed on web-page.

Presentation - Defines how a value will be represented on a page. Available options are:

Show as value
This option will read from the address and present the result at the view-page.

Writeable value
This option reads the value from the address and presents it. There will be a set button next to the value at the view-page which makes it possible to write to the address.

Show with enumeration
This option will read the value from the address and present it with the corresponding enum string (See Enum below).

Writeable value with enumeration
This option will read the value from the address and present it with the corresponding enum string. There will be a drop down next to the value at the view-page where available enum strings will be selectable. A selected value will be written to the address.

Enum - here the enum variables is defined in following format [number]=[string].
Each enum is separated by a semi colon ';' with no blank spaces.

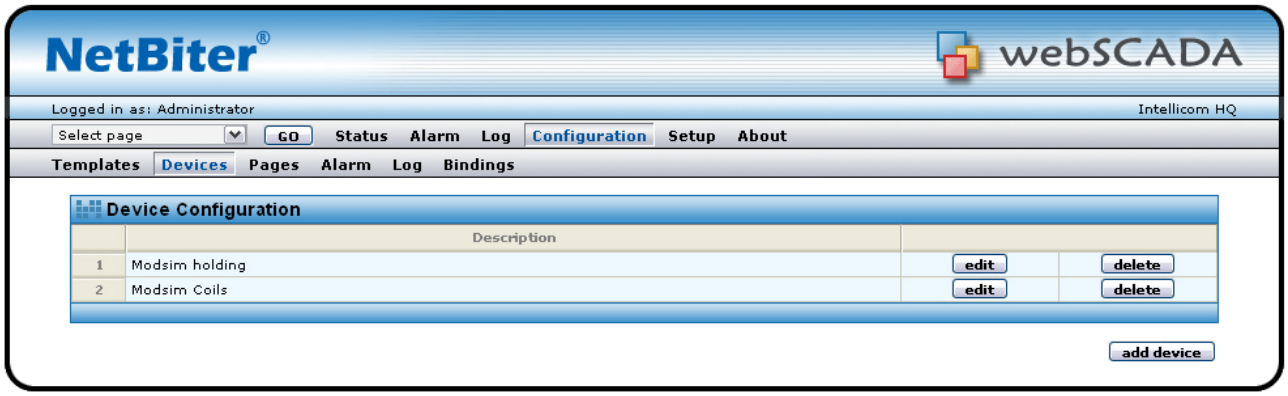
Examples:
0=Off;1=On
0=Sunday;1=Monday;2=Tuesday;3=Wednesday;4=Thursday;5=Friday;6=Saturday

Number of decimals – Defines how many decimals to use for this point.

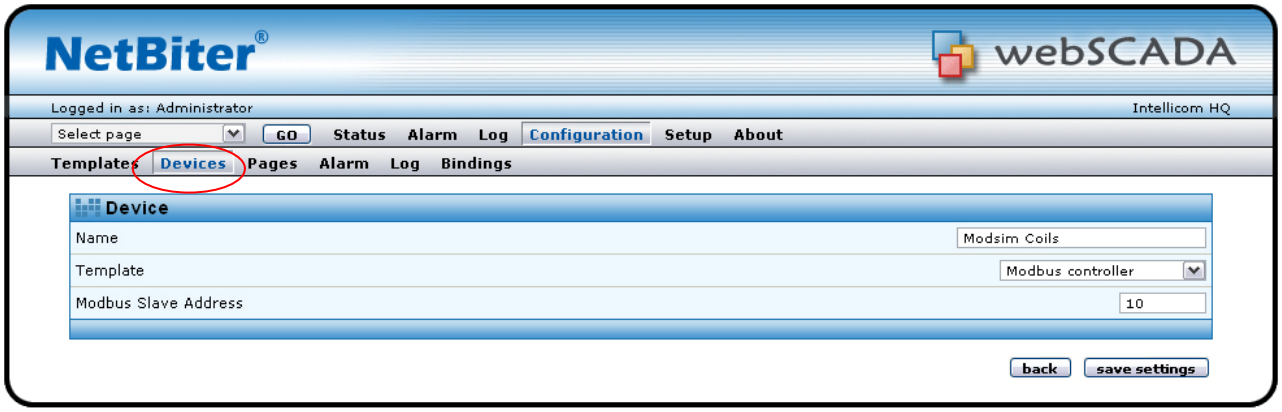
Valid range – defines min and max value for a write parameter. If a user tries to enter a value outside the range, a warning message will appear.

When you are finished with the Template, continue to the Device Configuration.

4.3 Device configuration



On the Device Configuration page, you define which Modbus slaves are attached to the webSCADA. To add a device, click the "**add device**" button. This will bring up the following screen:



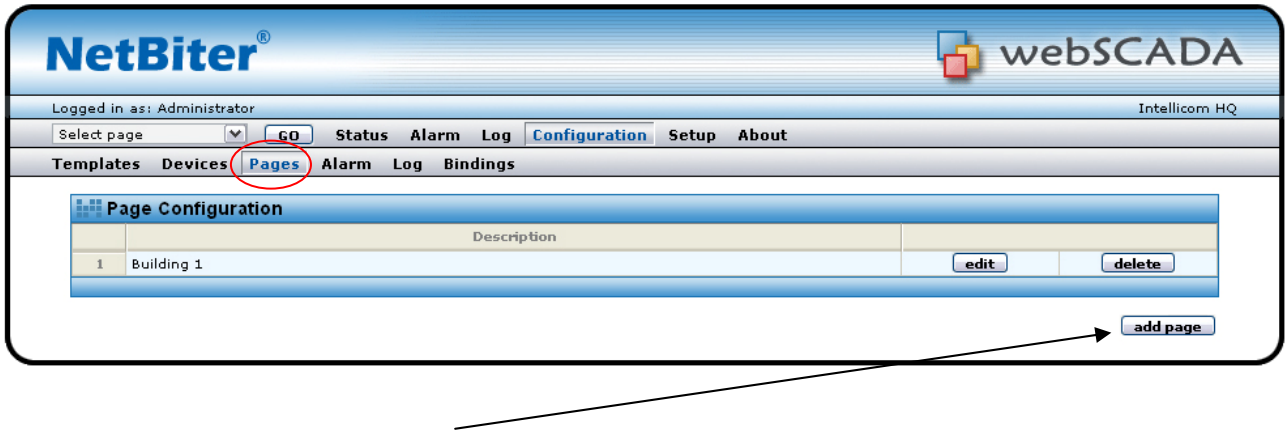
Name – A description of the device.

Template – Defines which template that should be associated with this device.

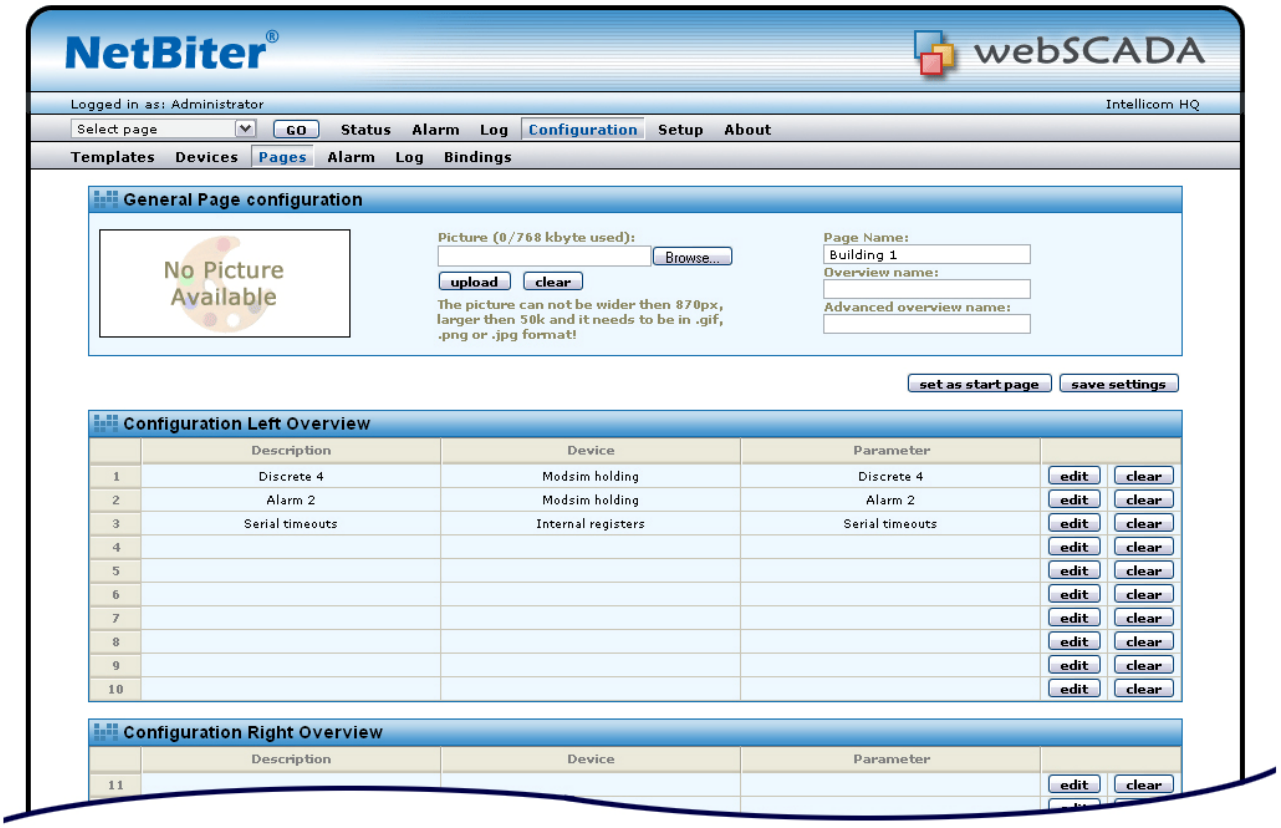
Modbus slave address – Defines the Modbus address of this device.

The next step is to create your webSCADA application, by defining the look of the web-pages and which alarms and log-parameters that should be available.

4.4 Pages



To create a new page, click the "**add page**" button. This will bring up the General Page Configuration:



On this page all page properties can be configured. A maximum of 20 Modbus points can be on each page.

Next step is to define where to display the parameters. Simply click the "edit" button on the position you want to work with.

4.4.1 Adding parameters to web-page

Now select the Device, Group and Parameter and enter a description for this parameter, and finish by clicking the "save settings" button. To check that everything is OK, go to the "Select page" menu, select the page you have been working with and hit the "**Go**" button. You can also define a "presentation format" and "presentation scaling" on this page.

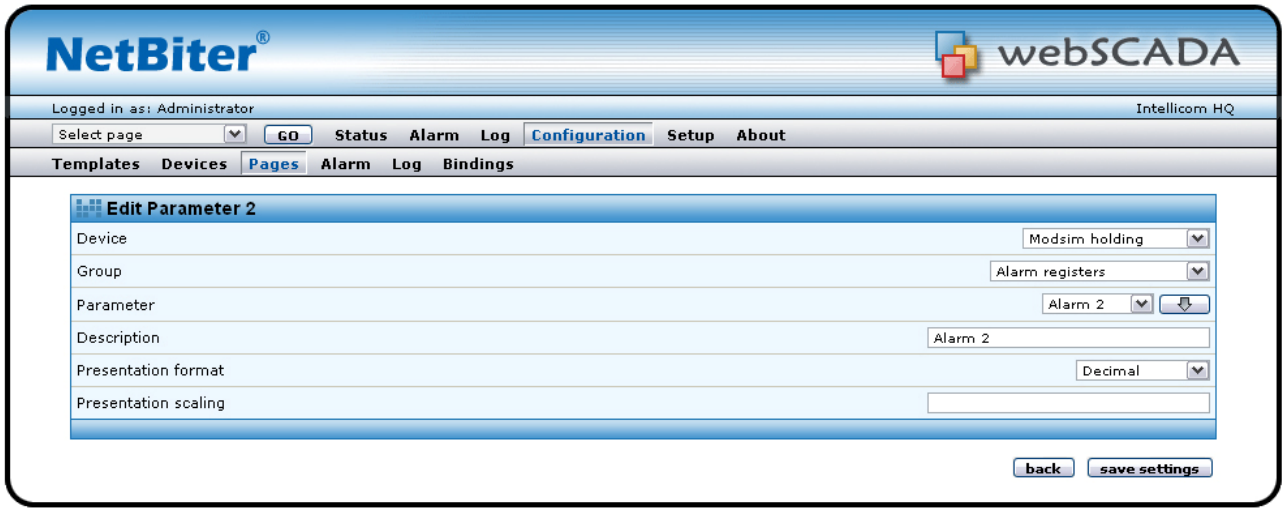
Presentation format – You can select a different presentation for a value on the presentation pages.

- Default Value is presented as it is configured in the Device template.
- Hexadecimal Value is presented in hexadecimal form.
- Binary Value is presented in binary form.

Presentation scaling – You can add an additional scaling on the value before it is presented on the web-page.

The value will be divided by the scale value before presented on the web-page. It will be multiplied with the scale value before value is written to a slave device.

It is normally better to use the scaling in the Device template because that will also include logging and alarm.



4.4.2 Picture

This option lets you choose a picture to be presented on the page. The picture must not be more than 870 pixels wide and must be in gif, jpg or png-format. The picture will be sent to the device when you press the "**Upload**" button. To remove a picture from the device, press the "**Clear**" button.

There are maximum 800kB available for pictures. On the General Page configuration section you can see how much space remains.

4.4.3 Page name

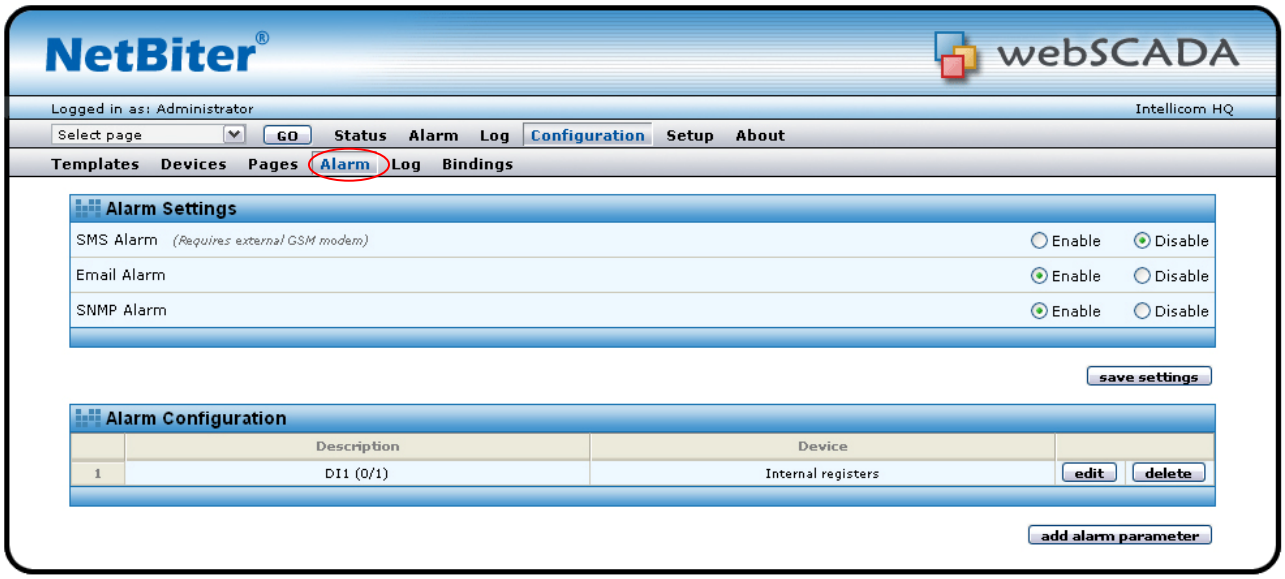
This field can be used to give the page a more descriptive name. Click the "**set as start page**" button if this page should be the first page to be presented when logging into the module.

It's also possible to change name on the Page menu (default "Overview" and "Advanced Overview").

4.5 Alarm configuration

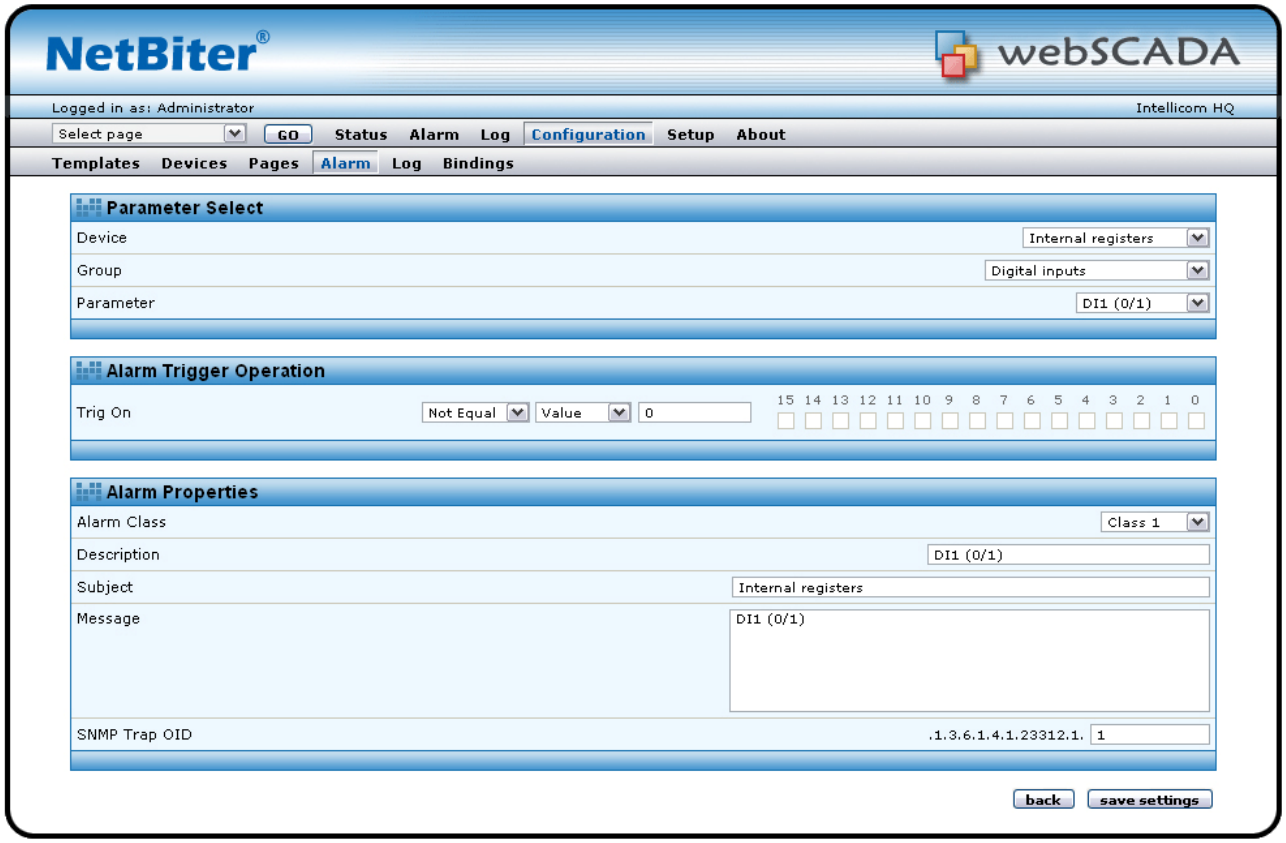
The NetBiter webSCADA can send alarm messages with email, SMS or SNMP (traps).
(SMS alarms require an external GSM modem). The alarm functionality can be enabled/disabled on the Alarm configuration page.

A maximum of 64 alarm parameters can be configured.



4.5.1 Defining alarms

To add an alarm point, click on the "**edit**" button in the Alarm Configuration list. This will bring you to the following screen. Here you need to select which parameter to use, and define the trigger operation that will activate the alarm. You also need to define some properties like alarm class (1-10), and what strings should be in the subject and message field of SMS/Email alarms.



- **Trig On** - this configures the trig condition for the alarm parameter. It's possible to trigger on a Value (Higher than, Lower than, Equal to, Not Equal to, Change of Value) or on a bit-field (Any bit, Neither bit, All bits).
- **Alarm class -** Can be used to set different priorities on the alarm (class 1-10)
- **Subject –** Defines the text to be shown as Subject in the email/SMS
- **Message –** The body of the alarm message
- **SNMP Trap OID –** the last number in the SNMP OID that will be used when sending a SNMP trap. This can be used to uniquely identify the alarm. **(Mandatory)**
  (The other part of the OID can be defined on the SNMP setup screen).

4.6 Log configuration

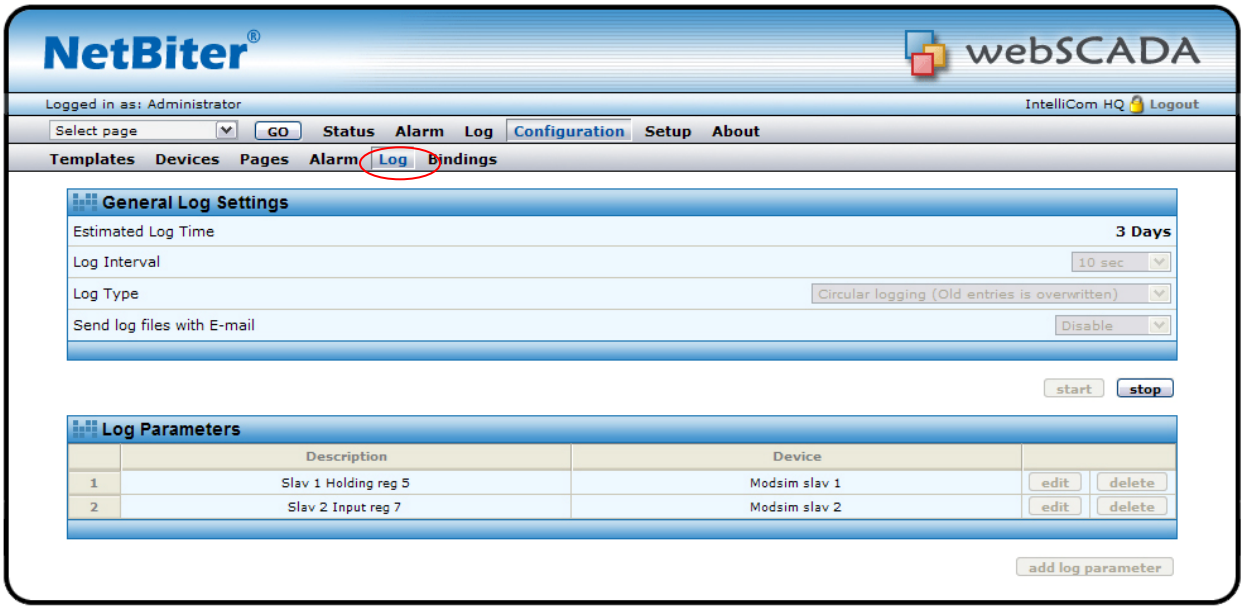
NetBiter webSCADA can be used to log Modbus registers. All data is stored in a CSV-file that can be uploaded to a computer for further analysis in e.g. Excel. A maximum of 64 parameters can be configured.

To start logging, click the "**start**" button.

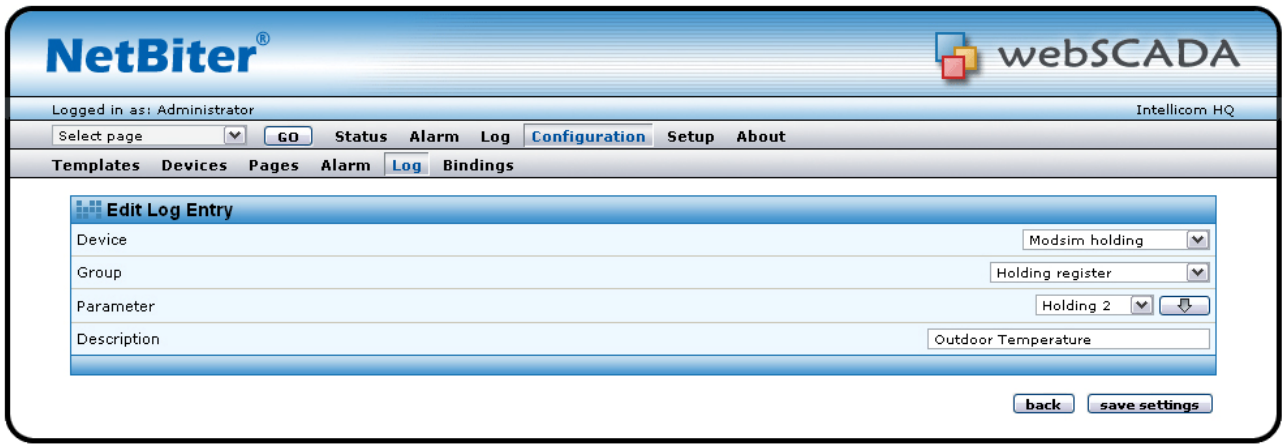
- **Estimated Log Time –** gives an estimate about how long it takes to fill the log-file.
- **Log interval –** defines the sample interval.
- **Log type –** choose whether to stop logging when the log has reached its maximum, or to overwrite old values (circular log).
- **Send log files with E-mail** – enable this if you want to send the log-files periodically with email. You can choose to send the log every hour, every day (will be sent around midnight) or every week (Sunday at midnight). You will also need to activate this function on each user that should receive the log-files.

The log-file that is stored in the NetBiter will contain historical data for a maximum of two periods as defined in the "Send log files with E-mail" property. I.e. if you set this to every day, the log-file in the NetBiter will keep a maximum of two days historical data.

See also **Setup/Regional** settings to make sure you have the correct settings for list separator and decimal symbol.



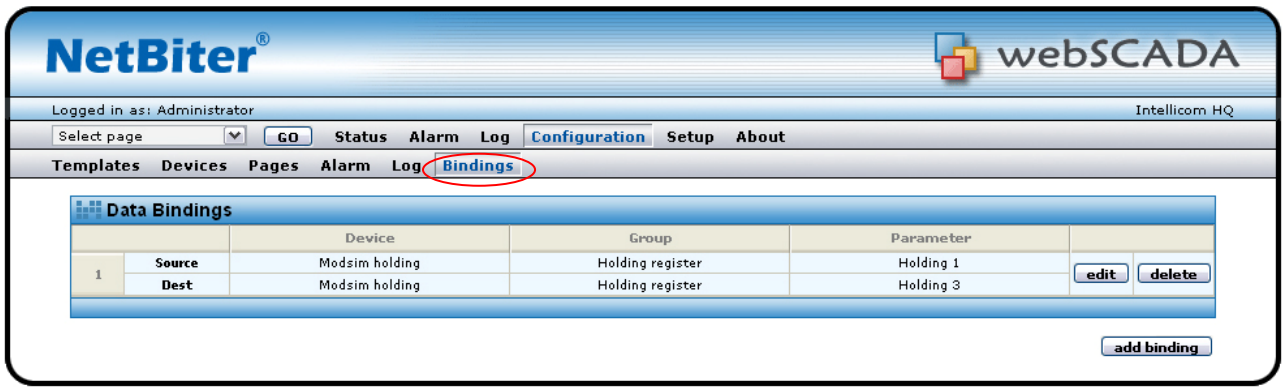
To add a log-point, click the "**add log parameter**" button, and then the "**edit**" button. This will bring you to the "Edit Log Entry" page.



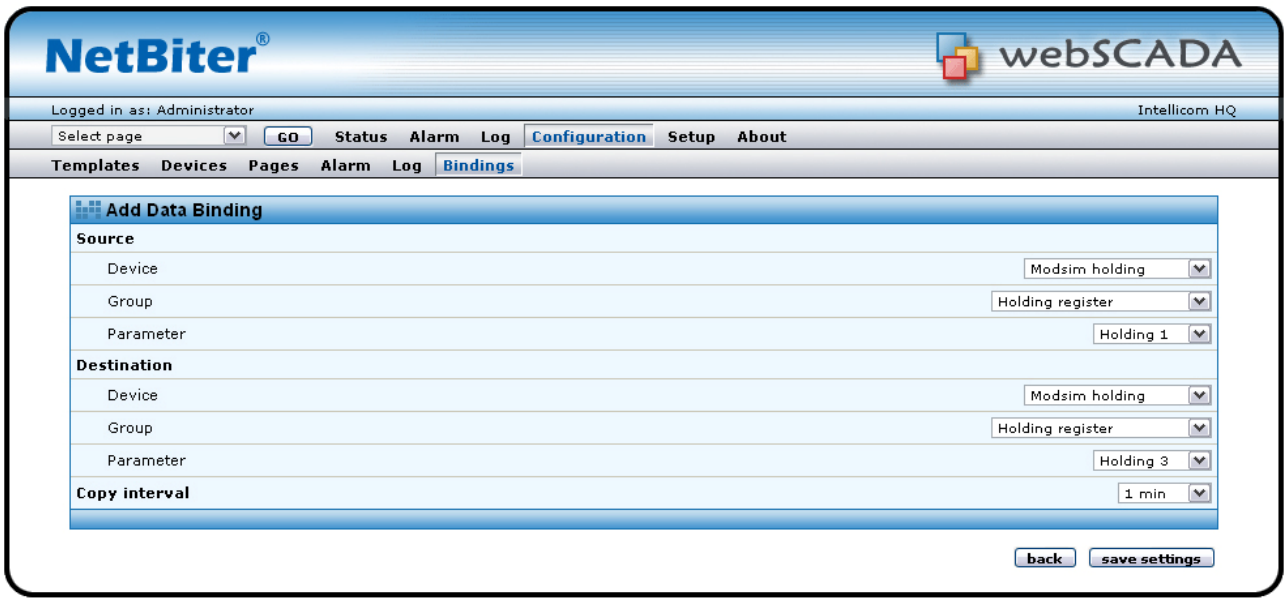
Now you can select the Device/Group/Parameter you want to log, and also enter a description for this Log Entry. To finish, click the "**save settings**" button.

4.7 Bindings

Bindings are a feature that allows you to copy parameters from one Modbus device to another. To add a binding, click the "**add binding**" button.

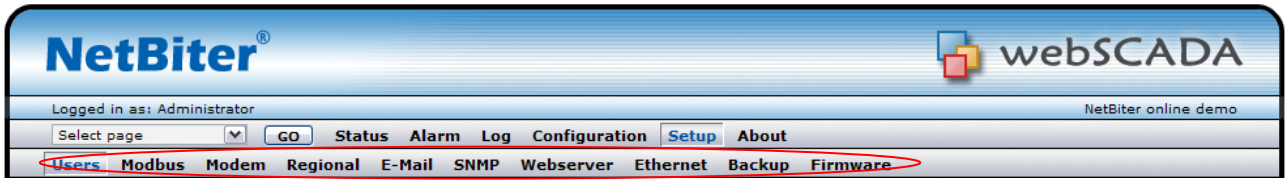


On the "Add Data Binding" screen you choose the Source and Destination parameter, and the interval for the copying of data.



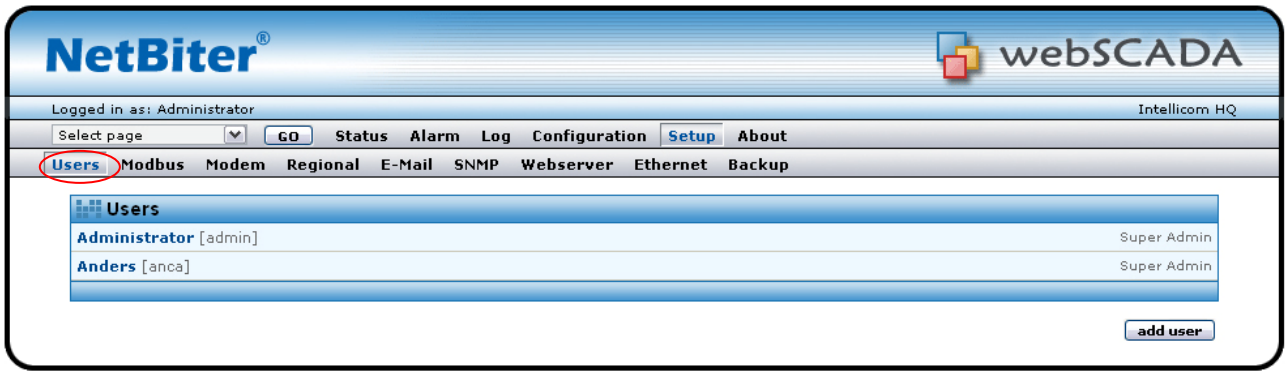
5 Module Setup

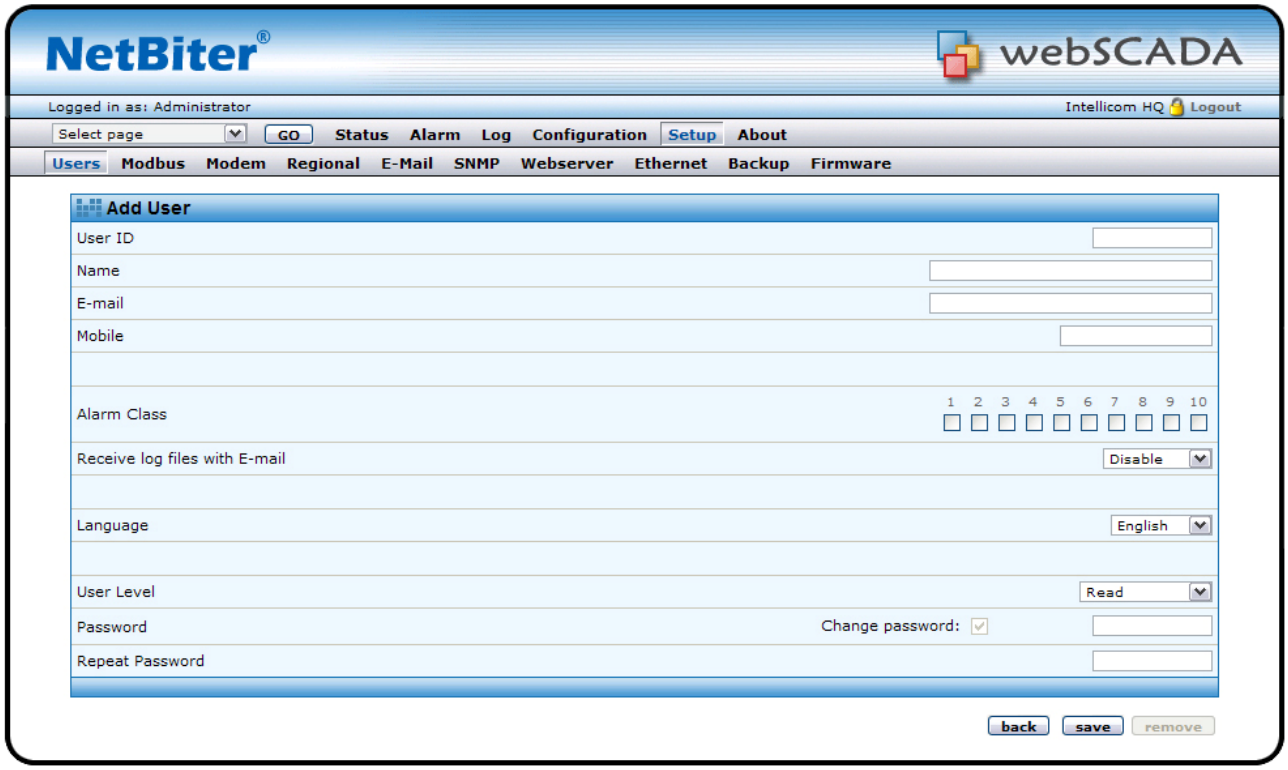
If you click on the Setup menu option, a sub menu will appear. Here you can do all necessary setup for things like user administration, modem settings and TCP/IP settings.



5.1 Users

If you press the "**Users**" link you will be transferred to the Users administration page. Here you can add, edit and remove users. To add a user, press the "**add user**" button, and to modify/remove a user click on the user you want to modify/remove.





Here you can enter the **User ID** (used on the login screen), **name**, **contact info** and a **password**.

If an e-mail address is entered, then alarms will be sent to this address (if user is configured as an alarm recipient and e-mail alarm is enabled).

If a mobile number is entered, then SMS-alarms will be sent to this number (if user is configured as an alarm recipient and SMS-alarm is enabled).

To configure a user as an alarm-recipient, enable one or more of "Alarm classes" (Class 1-10).

The user will only receive alarms that match this selection.

The "**Receive log files via E-mail**" option configures whether this user will receive logs via Email or not. See Configuration/Log (section 4.6) for more details about this function.

The language selection defines which language will be used for this user.

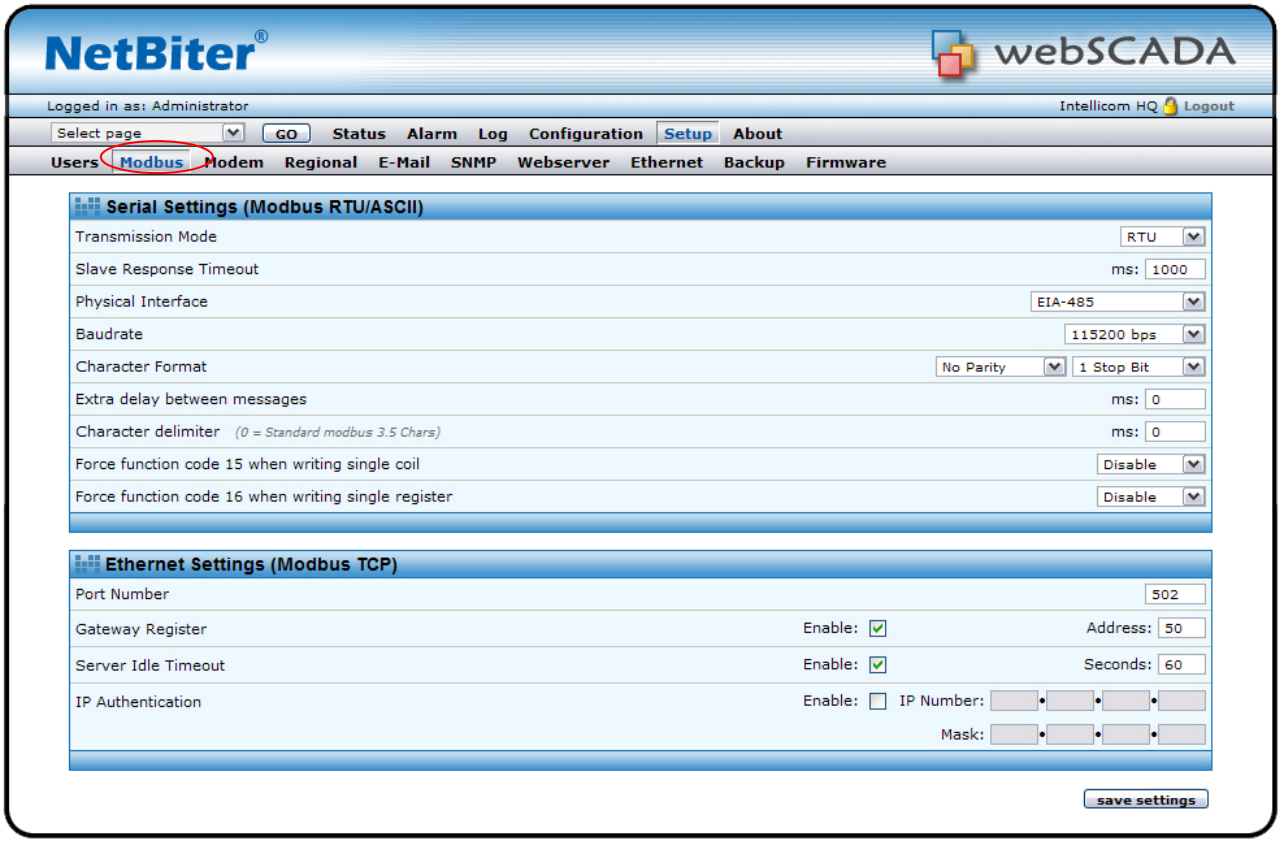
The user level defines what the user can do on the web-pages:

Read: View pages but can't do any configuration or modify Modbus Registers
Write: Can view pages and modify Modbus registers, acknowledge alarms.
Admin: Read, Write and also configure the module (templates, devices, pages, alarms, log, and bindings)
Super Admin: Read, Write, Admin and setup module like users, modem and modbus settings.

To add/edit users, you must be logged in as a user with Super admin access.

5.2 Modbus settings

If you press the Configuration/Modbus menu you will be presented with the following view:



Serial Settings (Modbus RTU/ASCII)

Transmission mode: Selects Modbus RTU or Modbus ASCII

Slave Response Timeout: The time that the module will wait for a response from a slave, before a Serial timeout will occur. (Default 1000 ms)

Physical Interface: EIA-485 or EIA-232

Baudrate: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200 bps.

Character Format: Select number of stop bits and if parity should be enabled (Odd, Even).

Delay between polls: time to delay between Modbus messages.

Character delimiter: Number of milliseconds between characters in the Modbus frame. Set to zero to use standard Modbus (3.5 characters)

Force function code 15 when writing single coil: If this option is Enabled, all writes to coils will be done with function code 15. (Useful if slaves don't support function code 05).

Force function code 16 when writing single register: If this option is Enabled, all writes to registers will be done with function code 16. (Useful if slaves don't support function code 06).

Ethernet Settings (Modbus TCP)

Port number: Which port to use for Modbus TCP communication (502 default).

Gateway Registers: The address to the gateway internal registers (if enabled). See section 5.2.1 for details about the internal registers.

Server Idle Timeout: This parameter gives the idle timeout in seconds for the Modbus/TCP connection. If the Gateway doesn't receive any Modbus/TCP query within this time the connection will be closed. (Default value is 60 seconds).

IP Authentication: This can be used to configure the IP-number that is allowed to connect to the Gateway.

It is of great importance to ensure at the time of the procedure of assigning Modbus device addresses, that there are not two devices with the same address. In such a case, an abnormal behavior of the whole serial bus can occur, the Master being then in the impossibility to communicate with all present slaves on the bus.

5.2.1 Internal Registers

If Gateway registers are enabled, queries sent to that address will not be forwarded to the Serial Modbus/RTU network; the Gateway will respond to these queries by it self.

See **Appendix B** for a list of the internal registers.

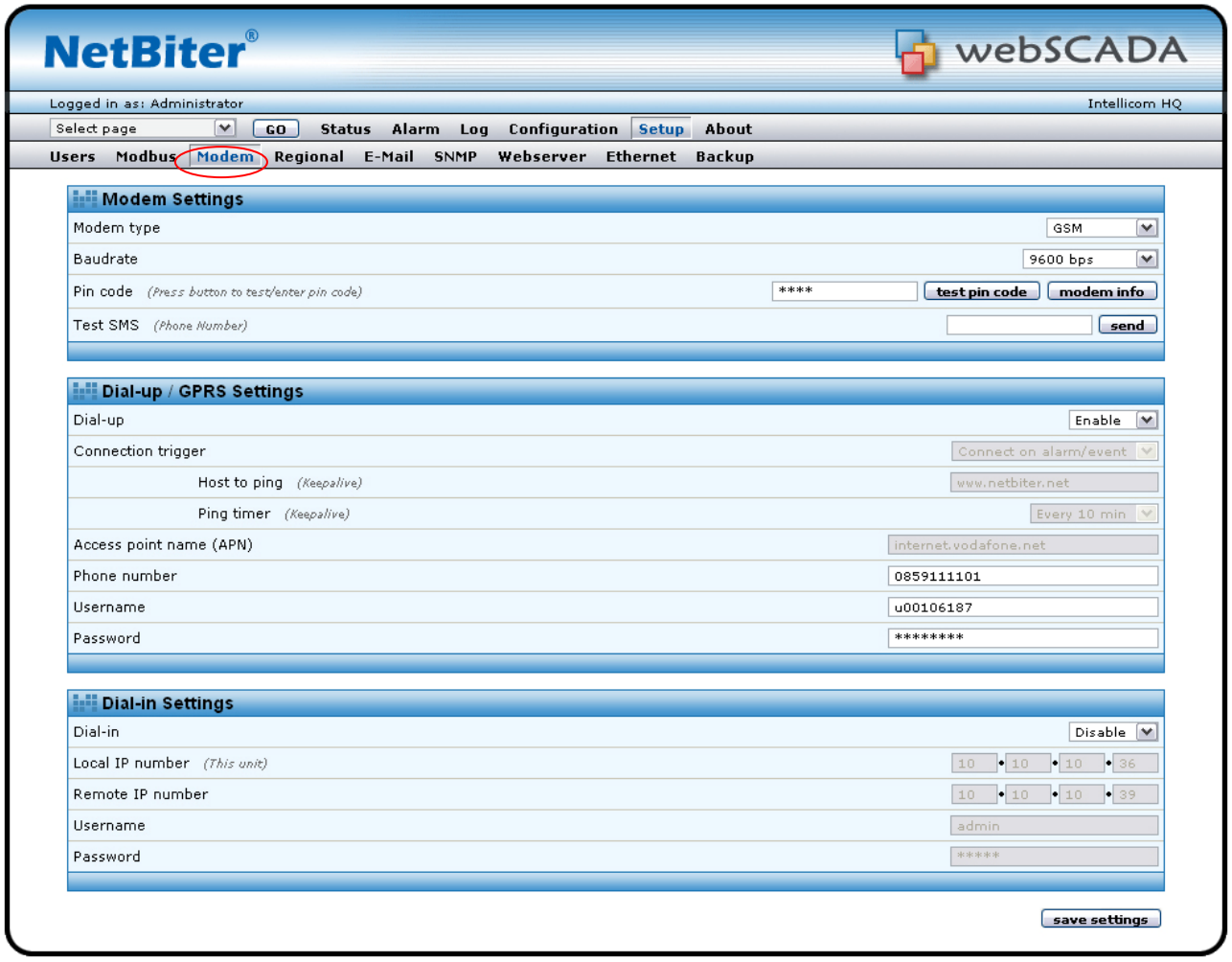
Valid Modbus commands for internal registers:

Command	Name
3	Read Holding Registers
6	Preset Single Register
16	Preset Multiple Registers

The internal registers are also available as an "internal template", i.e. the registers can be used on presentation pages and as alarms/log entries.

5.3 Modem settings

On this page you setup an external modem (optional) that can be either a GSM/GPRS modem or an analogue modem (PSTN).



5.3.1 Generic modem settings

Start with selecting the correct type of modem attached (GSM, Analogue, GPRS). Also set the desired baudrate that the webSCADA should connect to the modem with.

In this section you can also enter a PIN-code for the GSM-modem. Clicking on the “modem info” button will bring up a screen with some details about the modem (Signal strength etc).

5.3.2 Dial-up/GPRS settings

In this section you find configuration to allow the webSCADA to connect to Internet using a modem.

Connection trigger – Specifies whether the webSCADA should always be connected to Internet using the modem, or only connect when there is an alarm or event.

Host to ping – address to the Host that the webSCADA will ping when sending keep-alive messages for the GPRS connection.

Ping timer – Specifies the interval for the keep-alive messages. (Set value as high as possible to avoid unnecessary GPRS traffic).

Access Point Name (APN) – This is the gateway for all GPRS traffic. Contact your GSM/GPRS operator for information about this.

Phone number – Phone number to dial (e.g. to an Internet Service Provider, ISP).

User name – This is the username your ISP have assigned to you.

Password – Password to log into the ISP network.

5.3.3 Dial-in settings

The dial-in functionality can be used when someone wants to view the web-pages in the webSCADA over a modem-link.

Local IP-number – This is the IP-number of the webSCADA, which the remote client will see when creating the PPP-connection.

Remote IP-number – This is the IP-number that will be assigned to the remote client, when creating the PPP-connection.

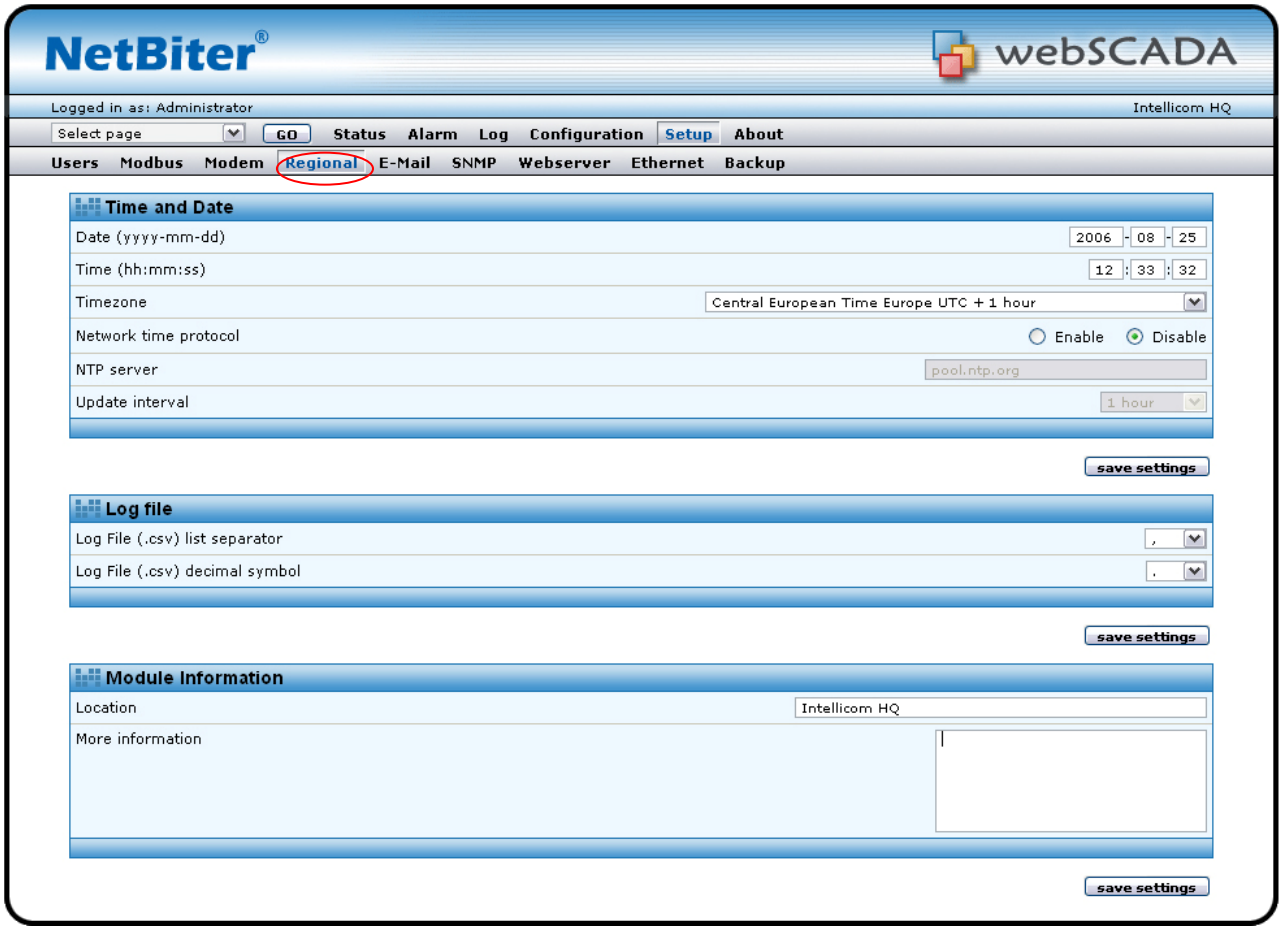
Username – This is the login that the remote client will use when creating the PPP-connection.

Password - This is the password that the remote client will use when creating the PPP-connection.

If you want to view the web-pages on a slow link (like GSM/GPRS), there is a special low-bandwidth version of the pages available. Enable this functionality on the Setup/Webserver page.

5.4 Regional

The Regional page contains configuration for time and date, generic module information and also configuration for how the log file list separator and decimal symbol should be represented.



5.4.1 Time and date

Configures the real-time clock on the module. The clock will continue to work during power-loss (max. 1 week). To use NTP (Network Time Protocol), enable it and enter an NTP-server (or use the default configuration). Also set the update interval (how often NTP will synchronise the time).

5.4.2 Numbers

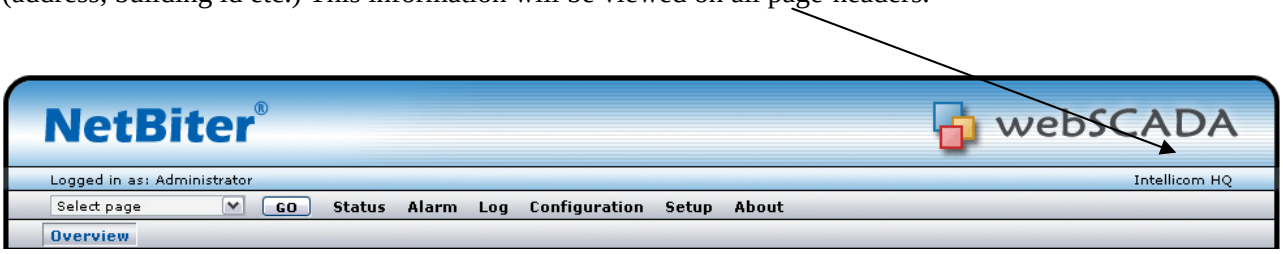
List separator - Can be either colon (,) or semi-colon (;).

Decimal Symbol – Can be either dot (.) or colon(,).

The list separator and decimal symbol should be selected so it matches the configuration on the computer where the file will be analysed.

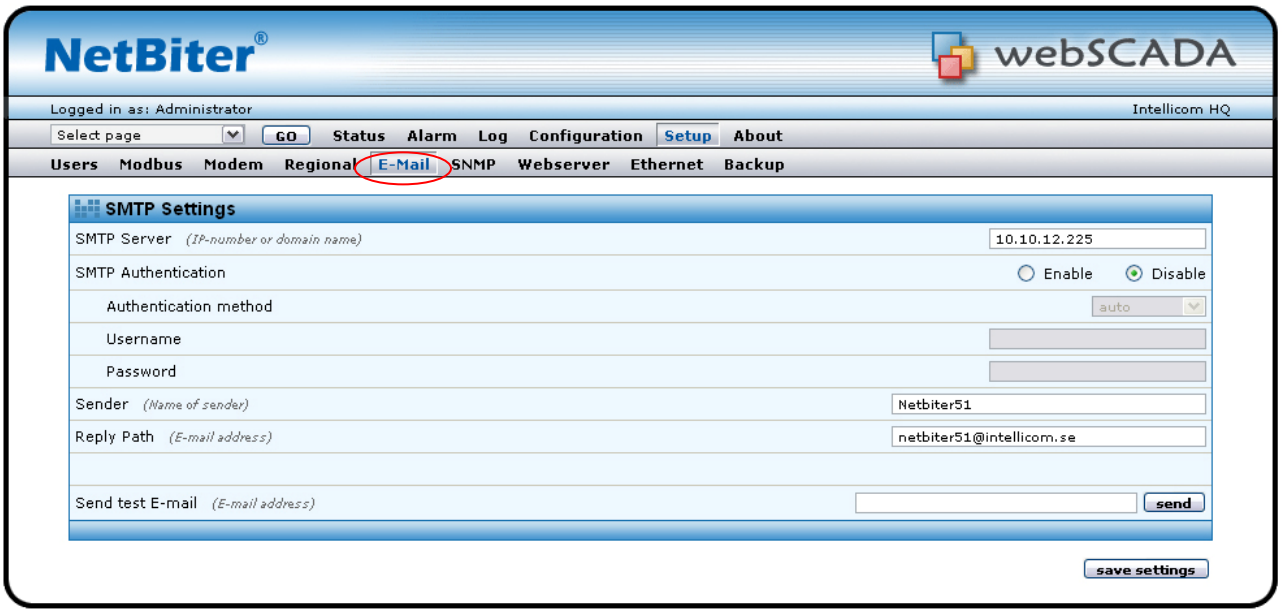
5.4.3 Module information

The "**Location**" string can be used to add information about where the module is located (address, building id etc.) This information will be viewed on all page-headers.



The "More information" field can be used to do notes about the installation.

5.5 Email Setup



The following configuration properties are available:

- **Sender** – From field in the alarm mail. Example "NetBiter"
- **Reply path** – The E-mail address to send a mail to when someone reply on an alarm mail.
- **SMTP server** – IP-number or domain name to the SMTP server that the module should use when sending E-mails. If domain name is used make sure that you have entered a DNS under the Network configuration.
- **SMTP Authentication**
  - Authentication method: Auto, plain, login or cram-MD5
  - Username
  - Password

5.5.1 SMTP Authentication

If the SMTP server require authentication you should enable SMTP Authentication. There are several types of authentication methods supported by the module:

- **auto** – The module automatically select the best method supported by the SMTP server.
- **plain** – a simple non-encrypted method supported by most SMTP servers.
- **login** – a simple non-encrypted method supported by most SMTP servers.
- **cram-md5** – a more secure login method where the username and password is encrypted. (This method is not supported by all SMTP servers).
-

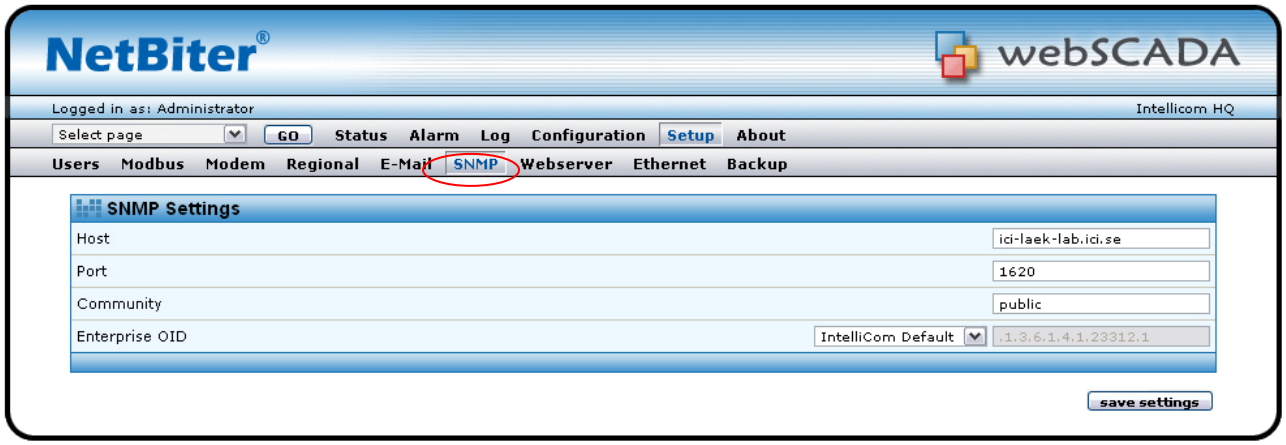
Note: auto will not work if only plain and login is supported by the SMTP server, because the module find these methods too insecure, in that case "login" or "plain" must be must be set explicit.

To verify the setup, use the Test E-mail functionality. Clicking on the "**send**" button will generate a test e-mail.

5.6 SNMP Setup

The SNMP Setup page contains configuration to be able to send SNMP traps.

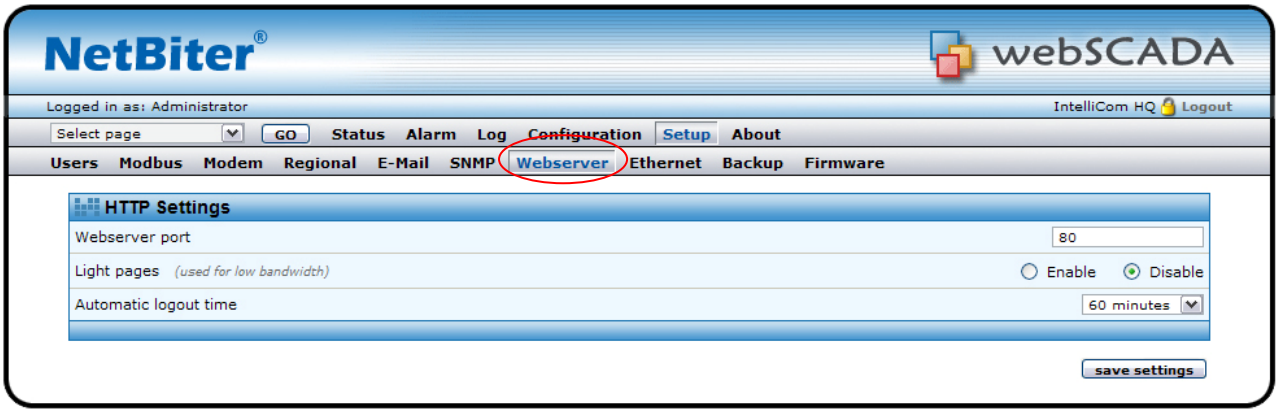
- Host – The SNMP manager to which SNMP traps should be sent
- Port – The port number on the SNMP manager to which traps should be sent
- Community – SNMP community used
- Enterprise OID – The enterprise OID (Object Identifier) that should be used in the SNMP traps sent. This is the common part of the Enterprise OID that is the same for all traps sent from the webSCADA. Use the OID setting when configuring alarms to set a unique OID for each alarm.



5.7 Web-server Setup

The Webserver Setup page contains a configuration to change the port number of the internal web-server in the webSCADA and also enable/disable the low bandwidth pages.

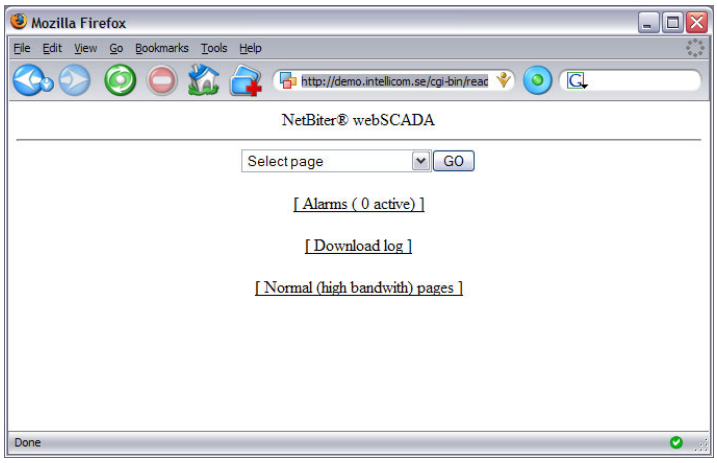
The Automatic logout time defines the time-interval before a user is logged out from the web-server.



Note: Changing the Webserver port will disable Webserver on default port 80.

5.7.1 Low bandwidth pages

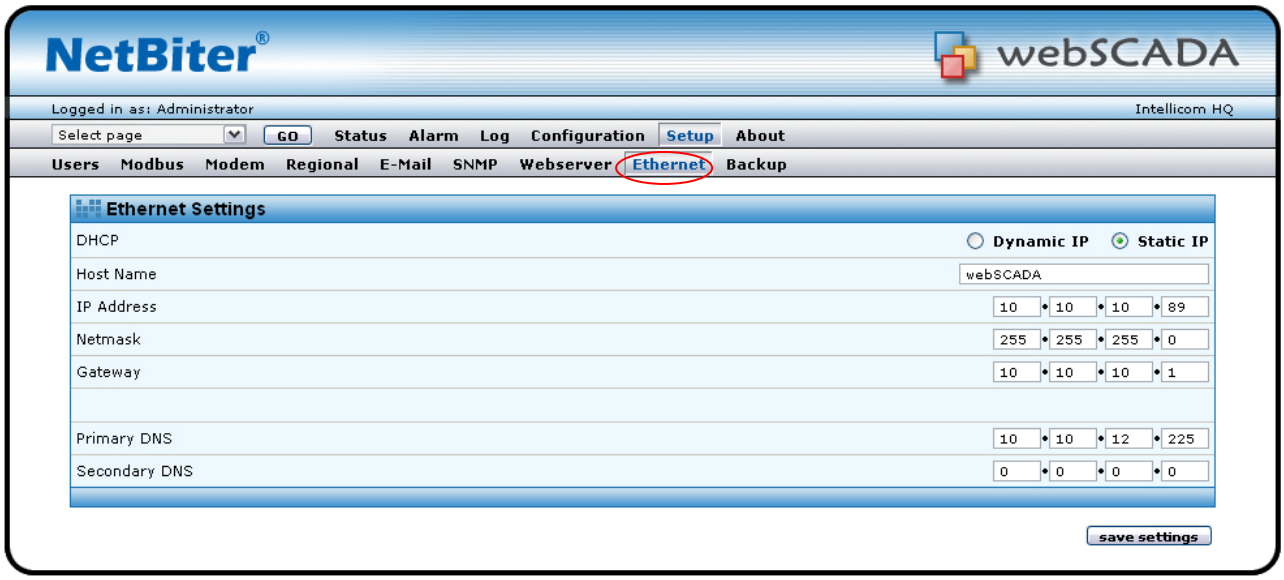
When the low bandwidth pages are enabled, the user will be presented with the following view when logging into a module:



Here it's possible to either view the parameter-page, alarms or download the log-file. It's also possible to go to the normal web-pages.

5.8 Ethernet (TCP/IP) settings

If you press the Configuration/Network link you will be presented with the following view:



On this page you can view and change the TCP/IP network settings in the module. These settings are the same as the ones set by the NetBiter Config utility.

Dynamic IP: Select this if you have a DHCP server on your network and you want the IP address be assigned automatically by the server.

DO NOT SELECT THE DYNAMIC IP OPTION IF YOU DON'T HAVE A DHCP SERVER AVAILABLE ON THE NETWORK.

Host Name: Here you can enter a hostname of your device (if E-mail alarms should be used this field must contain something)

IP Address: The IP address of the NetBiter.

Netmask: The subnet mask

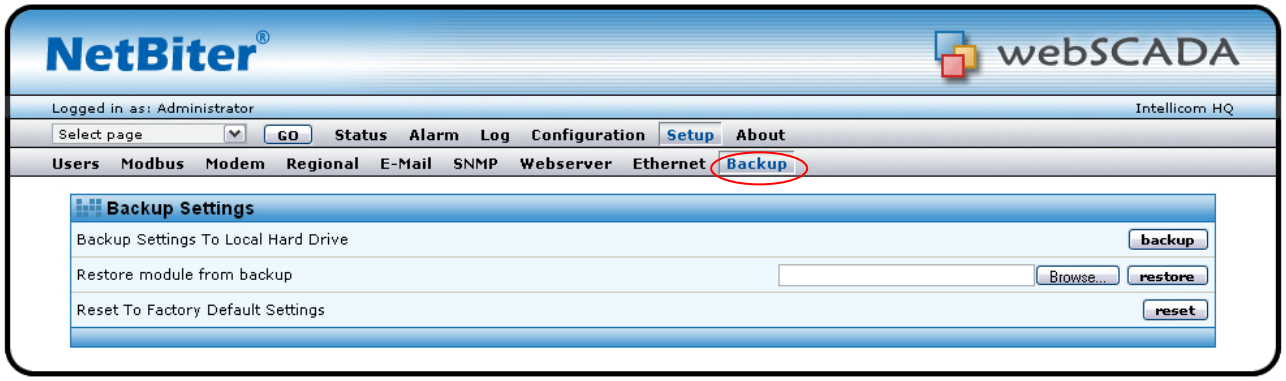
Gateway: The default gateway

Primary DNS: The primary Domain Name Server (**optional**)

Secondary DNS: The secondary Domain Name Server (**optional**)

5.9 Backup

The backup functionality makes it possible to backup and restore configurations.



By pressing the backup button you will get a backup file that can be stored locally.

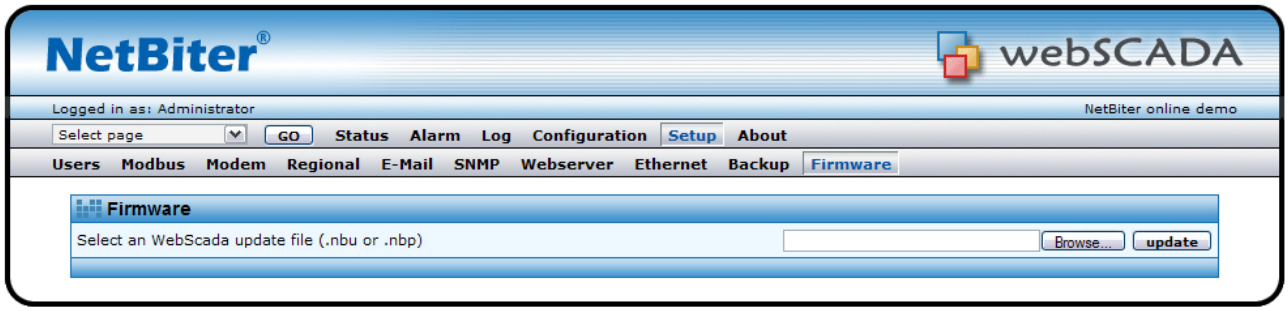
All configurations in the Module except Ethernet settings will be in the backup.

To upload a backup to a module, press the Browse button and select an .nbb file, then press restore. After restoring the configuration, you will be asked to restart the module.

To bring a module back to Factory default configuration, click the "**reset**" button.

5.10 Firmware

On the firmware page it's possible to download a new firmware image (.nbu file) or a patch file (.nbp).



APPENDIX A: SPECIFICATIONS

Ethernet connection

10Base-T or 100Base-TX (IEEE 802.3). RJ45 connector.

Serial interfaces

EIA-232 with full modem control (RTS,CTS,DCD,DTR,DSR,RI)
300-115.200bps. 9-pole DSUB connector

EIA-485, 300-115.200bps. screw connector.

Power Supply

9-30 VAC/DC (1.7W)

Temperature range

Operating : - 40- 85 °C
Storage : -40 – 85 °C

Humidity range

5-93% RH, non-condensing

Cover material

Grey plastic, LEXAN 940, self-extinguishing acc. to UL94-V0

Mounting option

DIN rail (EN 50022)

CE certification

According to EN 50 081-2:1993 and EN 61000-6-2:1999

APPENDIX B: 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
	Serial Status (Modbus/TCP)			See section (3.3)
3	Number Active Connections	0-10		Read only
4	Number Active Internal Connections	0-10		Read only
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	Exception responses	0-65535		Can be cleared
	Serial Status (Buffered messages)			
10	Valid responses	0-65535		Can be cleared
11	Serial timeouts	0-65535		Can be cleared
12	CRC errors	0-65535		Can be cleared
13	Input Buffer overruns	0-65535		Can be cleared
14	Exception responses	0-65535		Can be cleared
	Serial Status (Internal requests and Webpages)			
15	Valid responses	0-65535		Can be cleared
16	Serial timeouts	0-65535		Can be cleared
17	CRC errors	0-65535		Can be cleared
18	Input Buffer overruns	0-65535		Can be cleared
19	Exception responses	0-65535		Can be cleared
	Configuration Registers			
20	Modbus/TCP Port	1-65535		Default port number is 502
21	Gateway Modbus address	(-1)-255		
		-1	Disabled	Default
		0 - 255	Enabled	
22	Modbus/TCP idle timeout	0-65535 (seconds)		Default 60 seconds
		0	Disabled	
		1 - 65525	Enabled	
23	Baudrate	0-9		
		0	300 bps.	
		1	600 bps.	
		2	1200 bps.	
		3	2400 bps.	
		4	4800 bps.	
		5	9600 bps.	
		6	19200 bps.	Default value

Holding register	Name	Values	Options	Comment
		7	38400 bps.	
		8	57600 bps.	
		9	115200 bps.	
24	Parity	0-2		
		0	No parity	Default
		1	Even parity	
		2	Odd parity	
25	Number of Stop bits	1-2		Default 1 stop bit
26	Slave timeout time	25-65535 (milliseconds)		Default 200 ms.
27	Physical interface	0-1		
		0	EIA-485 (RJ12)	Default
		1	EIA-232 (DSUB)	
	Authentication			
28	Valid IP address 1	0-255		First byte of IP address
		0	Disabled	IP address auth disabled
		1-255	Enabled	
29	Valid IP address 2	0-255	Enabled	Second byte of IP address
30	Valid IP address 3	0-255	Enabled	Third byte of IP address
31	Valid IP address 4	0-255	Enabled	Fourth byte of IP address
32	Mask for Valid IP address 1	0-255	Enabled	First byte of mask
33	Mask for Valid IP address 2	0-255	Enabled	Second byte of mask
34	Mask for Valid IP address 3	0-255	Enabled	Third byte of mask
35	Mask for Valid IP address 4	0-255	Enabled	Fourth byte of mask