REMOTE MONITORING OPTIONS FOR ABB DRIVES, CONVERTERS AND INVERTERS

NETA-21 remote monitoring tool

User’s manual

User’s manual

NETA-21 remote monitoring tool

Table of contents

1. Safety

4. Mechanical installation

5. Electrical installation

6. Start-up

© 2020 ABB. All Rights Reserved.

3AUA0000096939 Rev H
EN
EFFECTIVE: 2020-24-06

Table of contents

1. Safety

What this chapter contains . . . 11
Use of warnings . . . 11
Safety in installation . . . 12

2. Introduction to the manual

What this chapter contains . . . 13
Applicability . . . 13
Compatibility . . . 13
Target audience . . . 13
Purpose of the manual . . . 13
Before you start . . . 14
Contents . . . 14
Terms and abbreviations used in this manual . . . 15
Terms . . . 15
Abbreviations . . . 16

3. Overview

What this chapter contains . . . 17
NETA-21 remote monitoring tool . . . 17
NETA-21-specific features . . . 18
Layout of the NETA-21 and the NEXA-21 . . . 19
Hardware and software requirements of the PC . . . 20

4. Mechanical installation

What this chapter contains . . . 21
Unpacking and examining the delivery . . . 21
Installing NEXA-21 to NETA-21 . . . 22
Installing the NETA-21 . . . 22

5. Electrical installation

What this chapter contains . . . 23
General cabling instructions . . . 23
Grounding . . . 24
Power connections . . . 24
Communication connections . . . 24
Data link connections –
Drive with the ACS-AP-x panel . . . 24
Connection over the Ethernet tool network with an Ethernet adapter module . . . 25
Data link connections –
Drive with the RDCU control unit . . . 26
Recommended fiber optic cables for DDCS . . . 27
Connection via the EIA-485 port with a Modbus/RTU adapter module . . . 28
Connecting the NETA-21 to the RS-485 network . . . 28

Switching on the bus termination 29

6. Start-up

Contents of this chapter 31
First access to the user interface 31
Connecting a local PC to the NETA-21 in the DHCP server mode 32
Logging on to the NETA-21 32
Basic settings 34
Updating the NETA-21 firmware via ABB web pages 34
Changing the password 35
Adding users 36
Setting date and time 37
Setting the language 37
Setting the location of the NETA-21 38
Defining the Ethernet network settings 38
Initializing the communication between the NETA-21 and drives online 39
Initializing the communication between the NETA-21 and ACS800 drives (or other drives with the RDCU control unit) 39

7. Program features

What this chapter contains 41
FTP/FTPS 41
HTTP 42
HTTPS 42
HTTPS certificate 42
Modbus/TCP gateway 43
Ethernet PC tool gateway 44
TCP and UDP service ports 46
In-bound network services on the NETA-21 46
Out-bound network services on the NETA-21 48
Safe deployment of NETA-21 48
Cybersecurity Disclaimer 49

8. Front page

What this chapter contains 51
Parts and components of the portal 51
All devices portlet 53
Version information 53
Application toolbar and navigation bar 54
Status icons 55
Content area 55

9. Users

What this chapter contains 57
My details 57
User management 58
Users tab 58
User properties 60
User roles 61
Tool admin 61

Drive expert . . . 62
Network admin . . . 63
Firmware admin . . . 64
User . . . 64
Guest . . . 65
FTP user account . . . 65
External account . . . 65
User interface . . . 66

10. Devices

What this chapter contains . . . 69
Devices tab . . . 69
Device front page . . . 71
Device control buttons . . . 72
Parameter browser . . . 73
Parameter properties . . . 75
Export of parameters . . . 77
Import of parameters . . . 78
Device data logger . . . 79
Data logger . . . 79
Opening a data logger . . . 81
Setting up a data logger . . . 82
Device interface settings . . . 85
Device interfaces . . . 85
DDCS tab . . . 86
Ethernet tab . . . 87
Modbus monitoring tab . . . 88
Modbus templates tab . . . 89
Add Modbus templates . . . 89
Edit Modbus templates . . . 90
Modbus/TCP gateway tab . . . 95
Panel bus tab . . . 96
Interface settings . . . 96
Modbus/TCP settings . . . 97
Ethernet settings . . . 98
Modbus settings . . . 99
DDCS settings . . . 100
Panel bus settings . . . 101
NETA-01 compatibility mode . . . 102
Activate NETA-01 compatibility mode . . . 102
NETA-01 device configuration . . . 105
Events . . . 106
Special registers . . . 107
Cache . . . 107
Exceptions . . . 108

11. Networks

What this chapter contains . . . 109
Network interfaces view . . . 109
Test interface . . . 110
Ethernet panel . . . 111
Network status panel . . . 112

Network services 112
Test SMTP settings 113
Services/firewall settings panel 113
Services settings panel 114
Proxy settings panel 114
Mail servers (outgoing) panel 115
DHCP 115
HTTP/HTTPS 116
Starting up the SMTP configuration 116
FTP/FTPS 118
Dynamic DNS 119
Using the Dynamic DNS service 119
Dial-up function 120
Using a mobile broadband connection 121

12. Events

What this chapter contains 123
Universal event list 123
Contents of the non-universal event list 125
Filtering settings by columns 125
Filtering settings through the Event filter panel 127

13. Reporting

What this chapter contains 129
Introduction to reporting 129
Configuring the NETA-21 for reporting 130
Creating an email report 132
Format of the email report 133
Creating an SD card report 134
Format of an SD card report 135
CSV-formatted reports 135
DB-formatted reports 136
Creating an FTP report 137
Format of an FTP report 140
Creating SMS report 140
Setting the report trigger 142
Setting the reported data 144
Changing the reporting name 146
Changing the default naming of signals 147
Parameter logging interval templates 148
Changing the continuous monitor interval 150
Using scripting for email reports (custom report) 151
Using scripting for SMS reports (custom report) 152
Description of the tabs under Reports 153
Settings tab 153
Devices tab 154
Parameter history logging tab 155
Report events data tab 157
Configuration events tab 158

14. Tools

What this chapter contains . . . 159
Tool firmware . . . 159
Factory tools . . . 161
IP address after a factory reset . . . 162
Packages . . . 162
Using ABB IP Configuration Tool . . . 163

15. Backup and restore

What this chapter contains . . . 165
Backing up the NETA-21 . . . 165
Restoring the NETA-21 . . . 167

16. Security

What this chapter contains . . . 169
Applicability . . . 169
Advantages . . . 169
Features . . . 169
Protocol level implementation for RADIUS . . . 170
Enabling RADIUS authentication in NETA-21 web UI . . . 171
Enable RADIUS authentication method in security settings . . . 171
Add RADIUS user account with External account user role . . . 172
Steps: . . . 172
User permissions mapping . . . 174
Troubleshooting . . . 177

17. Memory card

What this chapter contains . . . 179
Using the memory card . . . 179
Memory card status tab . . . 179
File browser tab . . . 180
Autoinst tab . . . 180
Backup tab . . . 181
Report tab . . . 181
Restore tab . . . 181

18. Battery

What this chapter contains . . . 183
About the battery . . . 183
Procedure . . . 184

19. Frequently asked questions

What this chapter contains . . . 185
How to update the NETA-21 firmware . . . 185
Before you start . . . 186
Updating the NETA-21 firmware over a remote web connection . . . 186
Updating the NETA-21 firmware locally with SD card(s) . . . 188
Copying the FMZAAvrr.NTU file to memory card . . . 188

Updating the firmware locally with an SD card 188
How to reset the factory settings /
What if I forget my password 190
How to replace the SD memory card safely 190
How to configure the logging of drive data to the SD card 190
How much logged data fits into an SD/SDHC card? 191
How to interpret the logged data from the SD card 191
How to create an FTP account 191
How to re-enable reports if time & date have been shifted backwards 191

20. Diagnostics and troubleshooting

What this chapter contains 193
LED indications 193
LED indications of the NETA-21 194
LED indications of the NEXA-21 196
Troubleshooting 196

21. Technical data

What this chapter contains 199
Hardware 200
Enclosure of the NETA-21 200
Enclosure of the NETA-21 with the NEXA-21 200
Technical data of the NETA-21 and the NEXA-21 201

Further information

1

Safety

What this chapter contains

The chapter contains the warning symbols used in this manual and the safety instructions which you must obey when you install or connect an optional module to a drive, converter or inverter. If you ignore the safety instructions, injury, death or damage can occur. Read this chapter before you start the installation.

Use of warnings

Warnings tell you about conditions which can cause injury or death, or damage to the equipment. They also tell you how to prevent the danger. The manual uses these warning symbols:

Electricity warning tells you about hazards from electricity which can cause injury or death, or damage to the equipment.

General warning tells you about conditions, other than those caused by electricity, which can cause injury or death, or damage to the equipment.

Safety in installation

These warnings are intended for all who install or connect an optional module to a drive, converter or inverter, and need to open its front cover or door to perform the work.

WARNING! Obey these instructions. If you ignore them, injury or death, or damage to the equipment can occur.

- If you are not a qualified electrician, do not do installation or maintenance work.
- Disconnect the drive, converter or inverter from all possible power sources. After you have disconnected the drive, converter or inverter, always wait for 5 minutes to let the intermediate circuit capacitors discharge before you continue.
- Disconnect all dangerous voltages connected to any control signal connectors in reach. For example, it is possible that 230 V AC is connected from outside to a relay output of the drive, converter or inverter.
- Always use a multimeter to make sure that there are no parts under voltage in reach. The impedance of the multimeter must be at least 1 Mohm.

2

Introduction to the manual

What this chapter contains

This chapter introduces this manual.

Applicability

This manual applies to the NETA-21 remote monitoring tool and the NEXA-21 extension unit for DDCS, SW version 3.22.

Compatibility

The NETA-21 remote monitoring tool is compatible with various types of ABB drives, wind turbine converters and solar inverters. For information on the compatibility, see the ordering information or the appropriate hardware manual of the product.

Note: Later in this manual, term drive substitutes for string drive/converter/inverter.

Target audience

The reader is expected to have basic knowledge of electrical fundamentals, electrical wiring practices and how to operate the drive.

Purpose of the manual

The manual provides information on installing, commissioning and using the NETA-21.

Before you start

It is assumed that the drive is installed and ready to operate before starting the installation of the NETA-21.

In addition to conventional installation tools, have the drive manuals available during the installation as they contain important information not included in this manual.

Contents

The manual consists of the following chapters:

- *Safety* presents the safety instructions which you must follow when installing a NETA-21.
- *Introduction to the manual* introduces this manual.
- *Overview* contains a short description of the NETA-21.
- *Mechanical installation* contains a delivery checklist and instructions on installing the NETA-21.
- *Electrical installation* contains the cabling and connection instructions of the NETA-21.
- *Start-up* contains instructions on how to start up the NETA-21.
- *Program features* contains feature descriptions in more detail.
- *Users* describes the user management.
- *Devices* describes how to manage device parameters and use data loggers.
- *Networks* explains how to set up and configure Ethernet network interfaces of the NETA-21.
- *Events* describes how to observe and filter events.
- *Reporting* describes how to make reporting and trend logging settings for configuring which time levels and event categories are sent out by a reporting plug-in to be monitored.
- *Tools* explains how to manage NETA-21 firmware, factory settings and software packages.
- *Backup and restore* describes the backup and restore functions of the NETA-21.
- *Memory card* describes the tabs under **Memory card**.
- *Frequently asked questions* contains how-to instructions for various tasks.
- *Diagnostics and troubleshooting* explains how to trace faults with the status LEDs on the NETA-21 and the NEXA-21.
- *Technical data* contains the technical data of the NETA-21 and the NEXA-21.

Terms and abbreviations used in this manual

Terms

Term	Explanation
Assistant control panel	Assistant control panel with an USB connector enabling a PC tool connection for common architecture drives. Assistant control panel is a generic name for ACS-AP-I and ACS-AP-S panels.
Data log	File produced by a data logger. Can be sent and stored as a report attachment.
Data logger	Data logger inside a monitored device
DDNS	Dynamic domain name system
Device	Device connected to the NETA-21 for remote monitoring and data access. In the UI devices are classified as generic devices, drives, converters or inverters. See *Device type*.
Device interface	Software component that enables access to certain types of devices
Device type	Attribute for a device that is auto-detected or set by the user. Defines the main category of the device, eg, if the device represents a rotating machine or if it just converts electrical power from one form to another.
Drive	Term drive is used instead of string drive/converter/inverter
Modbus/TCP gateway	Modbus/TCP server that relays data read requests to any device interface. Feature allows an external Modbus/TCP client to read data through the NETA-21 from any connected device.
NETA-21 remote monitoring tool	Hardware product for accessing drives remotely – typically off-site access over public Internet, local/private Ethernet or modem connection.
Network interface	Any defined interface to the connected data network
Network service	Any inbound or outbound data connection provider in the NETA-21. NTP time service and email (SMTP) are examples of outbound network services.
Parameter	Operating instruction for the drive. Parameters are typically adjusted with a control panel or a PC tool. Parameter browsing, monitoring and writing can be done also with the NETA-21.
PC tool autodiscovery	Network service which allows automatic detection of other Ethernet-based ABB products (eg, the FENA-11) in a local network. In addition, enables finding the NETA-21 in the network where the PC tool has been connected.
Portlet	Panel for text and controls within a page or tab. Some portlets can be moved around, added and removed, eg, on the front page.
Trend logging = parameter history logging	Refers to low time resolution, long-term data logging performed by the NETA-21. Trend logging is a functionality within the NETA-21 while data loggers are part of the drive functionality and merely configured with the NETA-21.
User account	A user name that in combination with a password can be used to access the NETA-21 web user interface or some other services of the NETA-21.
Web UI	Web-based user interface of the NETA-21

Abbreviations

Abbreviation	Explanation
DDCS	Distributed Drives Communication System, an optical fiber device access method for drives and inverters (for example, ACS800 and PVS800)
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol, a protocol for configuring servers in a network
FTP	File Transfer Protocol provides an unsecure way to access files in a network
FTPS	File Transfer Protocol Secure provides a secure way to access files in a network
HTTP	Hypertext Transfer Protocol is an application protocol used between data clients and web servers
HTTPS	Hypertext Transfer Protocol Secure is a combination of the HTTP and SSL/TLS protocols. Provides secure communication with web servers.
NBT NS	NBT NS is a daemon for the NetBIOS name discovery. Allows finding computers from a local network by using the NetBIOS host name.
NTP	Network Time Protocol is a protocol for synchronizing computer clocks over a network
SD	Secure Digital memory card
SDHC	Secure Digital High Capacity memory card
SMTP	Simple Mail Transfer Protocol is a protocol for sending emails
SSH	Secure Shell, a protocol for a secure remote access.
SSL/TLS	Transport Layer Security (previously Secure Sockets Layer) protocol is used to encrypt data between clients and servers
TCP	Transmission Control Protocol, used together with Internet Protocol (IP) as the transport protocol for the Internet
UI	User interface
UTC	Coordinated Universal Time is the most often used time in the world. Time zones are presented with positive or negative offsets.

3

Overview

What this chapter contains

This chapter contains a short description of the NETA-21.

NETA-21 remote monitoring tool

The NETA-21 remote monitoring tool is used for browser-based remote monitoring of ABB drives via Ethernet. Multiple drives can be connected to the network by using a panel bus or through the fiber optic channel of the NEXA-21 extension unit.

Through the NETA-21, you can:

- monitor drives
- read and adjust drive parameter values
- read status information and actual values from drives
- set up and monitor the data logger and save its content to a file
- read the contents of the fault log from monitored devices and save it to the memory
- send email messages on events
- use email for continuous monitoring of drives
- reset a fault on drives
- use an SD card for continuous monitoring of drives
- use an SD card to store all events
- use the FTP server for storing drive parameters and events
- create custom events
- create custom reports: email reports, SD card reports and FTP reports.

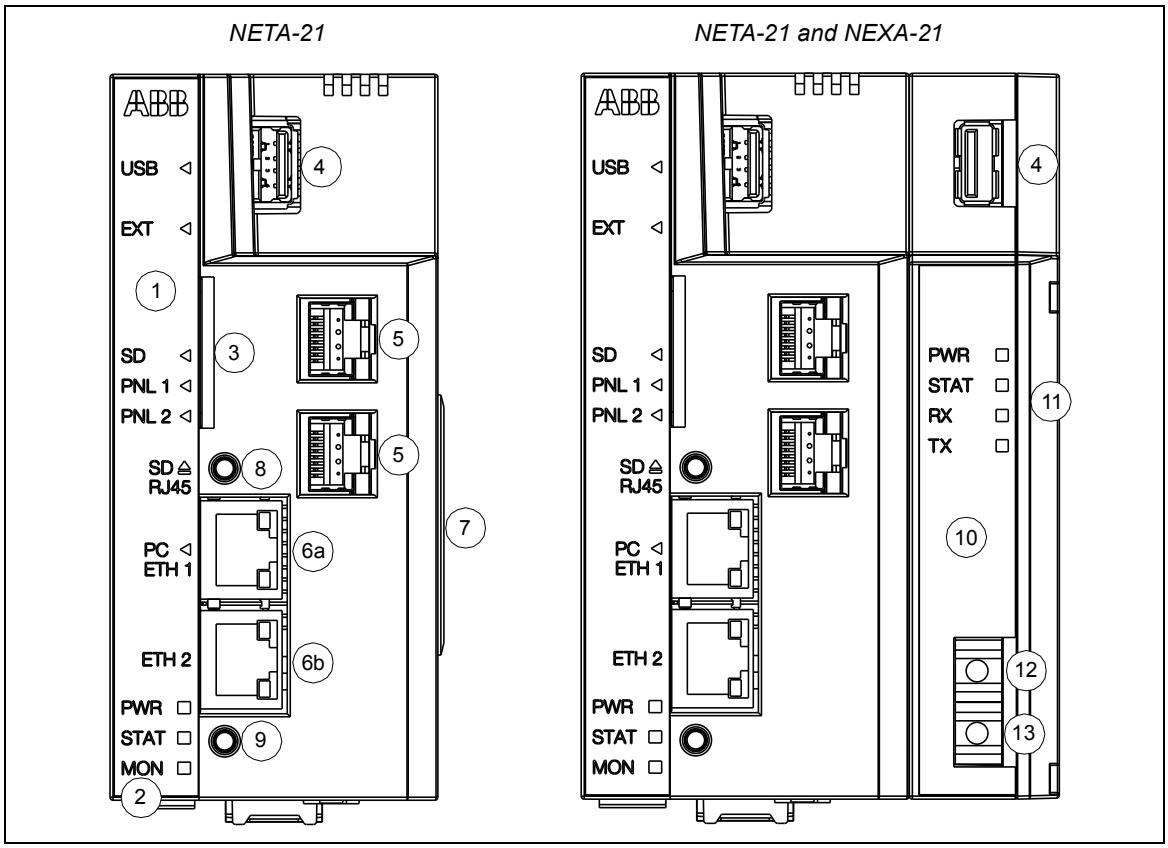
The NETA-21 is not intended for controlling or commissioning the drive. The NETA-21 provides stand-alone logging without a PC and automated data reporting to external data systems. The user interface can be accessed with any web browser including mobile devices, without the need to install any special software.

NETA-21-specific features

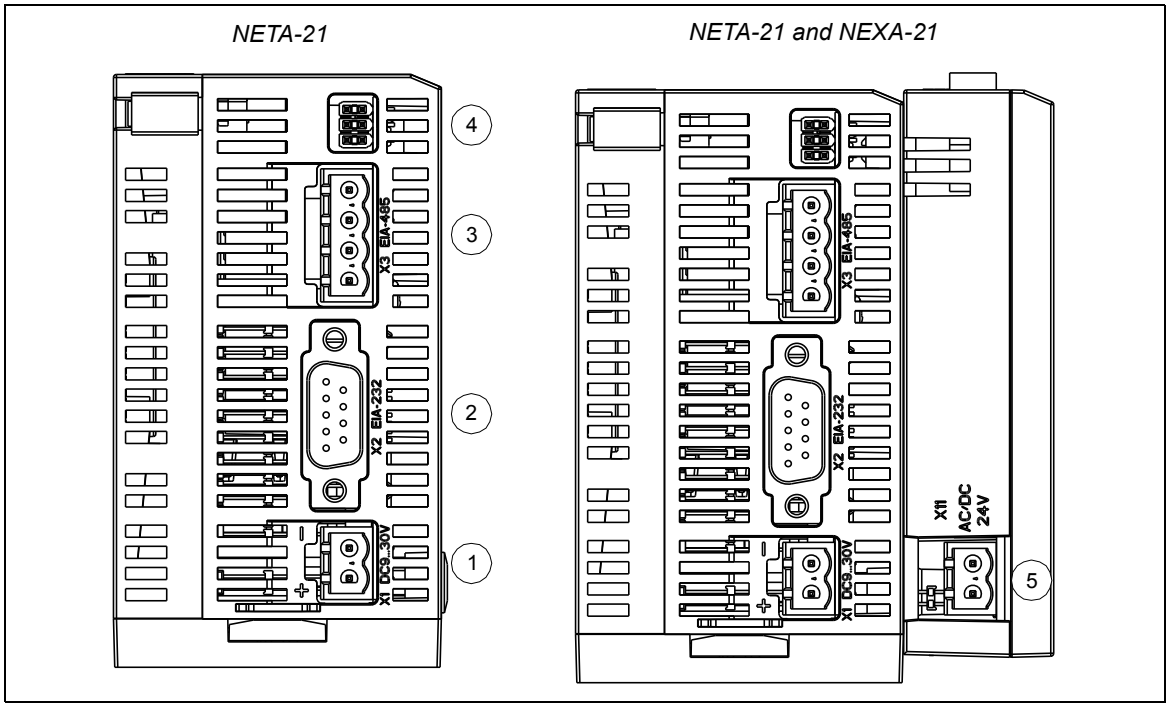
- Two network connections
  - Internal (factory line)
  - External (Internet access)
  - Automatic or fixed IP configuration
- Easy point-to-point access to the NETA-21 with a PC (no need to change the IP address of the PC)
- Email reporting of events and parameter history logs
- FTP reporting of events and parameter history logs to an external FTP server
- Storing of events and history log files to a SD memory card
- FTP and FTPS file access to an SD/SDHC memory card
- Browsing an SD/SDHC memory card via the web UI
- Different access rights for different users
- NETA-21 software upgrade locally or remotely
- Importation of the NETA-21 settings from the USB memory
- Time synchronization via an NTP server
- Full or selected backup/restore of the software
- Dynamic DNS support
- Support devices connected via:
  - Panel bus (ACSx80 series)
  - Ethernet PC tool communication (ACSx80 series)
  - DDCS with a fiber optic cable (eg, ACS800, ACS600)
  - Modbus/RTU via RS485
- Support for a USB modem
- Online monitoring with a history
- Automatic discovery the connected device
- Automatic log changes in the connected device

Layout of the NETA-21 and the NEXA-21

The following figures describe the front and bottom layout of the NETA-21 and the NEXA-21.



1	Front panel labeled with a black sticker and equipped with indicator LEDs
2	PWR, STAT, MON – power, status and monitoring indicators, see *LED indications*
3	SD – SD/SDHC memory card slot
4	USB – USB host connector for third party extensions
5	PNL 1/PNL 2 – connector providing an interface for a panel bus that can be used for communication with certain drive types
6a	PC ETH 1 – connector providing an Ethernet connection for a locally connected PC
6b	ETH 2 – connector providing an Ethernet connection for an external Ethernet network
7	Connector for the NEXA-21 unit
8	SD RJ45 – SD button is used for removing the SD/SDHC card safely and activating a DHCP server for the first access to the user interface
9	Reset button is used for rebooting the NETA-21
10	NEXA-21 provides a DDCS fiber optics connection, secondary power input and one extra USB connector
11	PWR, STAT, RX, TX – power, status and RX/TX indicators, see *LED indications*
12	Fiber optic transmitter DDCS
13	Fiber optic receiver DDCS



1	X1 10…30 V DC – power supply input
2	X2 EIA-232 connector (in reserve)
3	X3 EIA-485 connector for a Modbus network
4	Termination jumpers for the link connected to X3
5	X11 AC/DC 24V – secondary power supply input

Hardware and software requirements of the PC

The NETA-21 can be configured and used with a normal PC with:

- Ethernet network adapter
- Windows XP/Vista/7/8, Linux, MAC OS
- Internet Explorer 9+, Firefox 3.6+ (PC, Mac), Safari 5+, Chrome 10+ or Opera 11+ (PC, Mac).

  Note: Firmware versions until 2.21 have been tested with Internet Explorer 8. Firmware versions 2.22 and beyond have been tested only with Internet Explorer 9 and later.

Most mobile phone and tablet browsers are also capable of showing the NETA-21 web pages, but displayed elements are not fully optimized for the touch screen use.

Javascript and cookies must be enabled in the web browser settings before you can use the NETA-21 web interface. The NETA-21 does not require external plug-ins, such as Java or Flash.

4

Mechanical installation

What this chapter contains

This chapter contains a delivery checklist and instructions on mounting the NETA-21.

WARNING! Follow the safety instructions given in this manual and the drive documentation.

Unpacking and examining the delivery

The option package for the NETA-21 contains:

- remote monitoring tool, type NETA-21
- *NETA-21 remote monitoring tool installation and start-up guide* (3AUA0000096881 [English]).

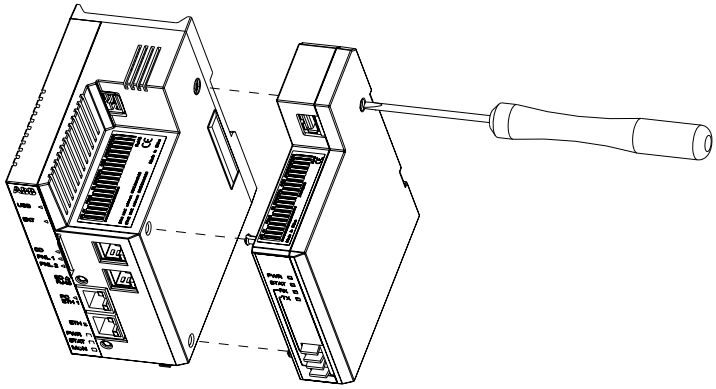
The option package for the NEXA-21 contains:

- extension unit, type NEXA-21
- NEXA-21 installation instructions sheet.

1. Open the option package.
2. Make sure the package contains all items listed above.
3. Make sure that there are no signs of damage.

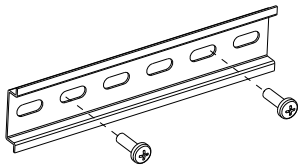
Installing NEXA-21 to NETA-21

1. Remove the plastic cap from the connector in the NETA-21.
2. Press the NEXA-21 against the NETA-21.
3. Tighten the grounding screw.
   Do not use excessive force.

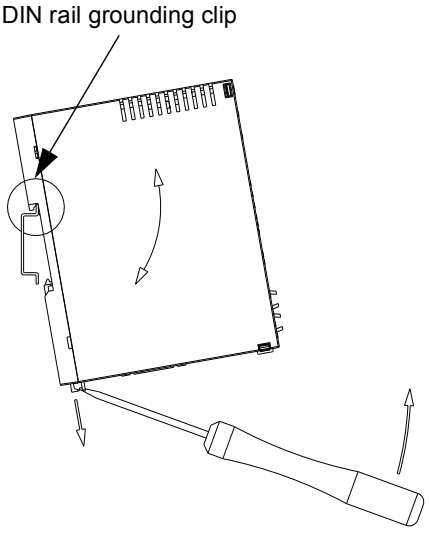


Installing the NETA-21

1. Protect the devices from the drilling dust.
2. Drill the holes for the fastening screws of the mounting rail.
3. Fasten the mounting rail.



4. Snap the NETA-21 onto the rail.



See the grounding instructions in section *Grounding*.

5

Electrical installation

What this chapter contains

This chapter contains:

- general cabling instructions
- grounding instructions
- instructions on setting the IP address
- instructions on connecting the NETA-21 to the drive and to the Ethernet network.

WARNING! Only qualified electricians are allowed to carry out the work described in this chapter. Follow the instructions in section *Safety in installation*. Ignoring the safety instructions can cause physical injury or death.

General cabling instructions

- Arrange the cables as far away from the power cables as possible.
- Avoid parallel runs with the power cables.

See chapter *Technical data* for information on cable types.

Grounding

Use a grounding clip to connect the ground of the NETA-21 to the mounting rail. Make sure that he mounting rail is grounded to a noiseless ground. If the rail is not mounted on a properly grounded base, use a separate grounding conductor. The conductor must be as short as possible and its cross-sectional area must be 6 mm^2 at least.

Do not use any solid copper conductor (only stranded wire is allowed).

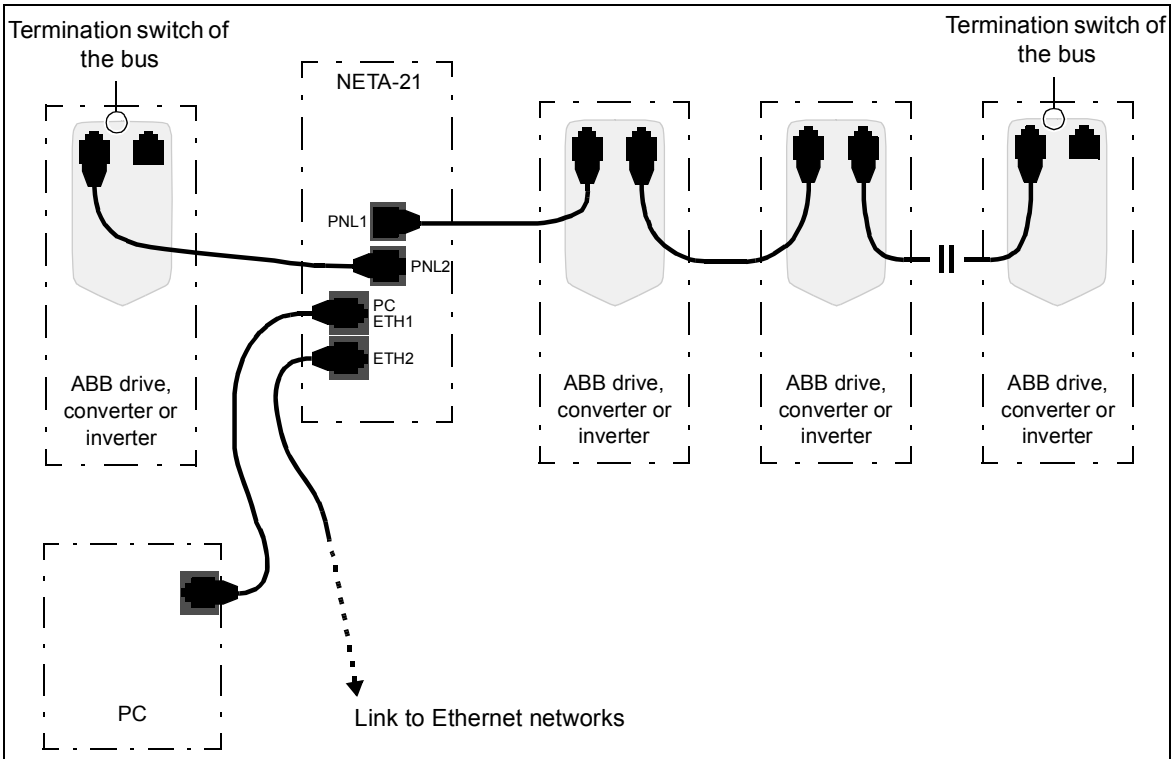
Power connections

Connect the power supply to connector X1 of the NETA-21. The NETA-21 supplies also the NEXA-21. For information on the connector type, voltage and power specification, see *Technical data of the NETA-21 and the NEXA-21*.

Note: In the NEXA-21, there is an alternative power supply input (X11), which you can use for supplying power to the NEXA-21 and the NETA-21.

Communication connections

Data link connections – Drive with the ACS-AP-x panel

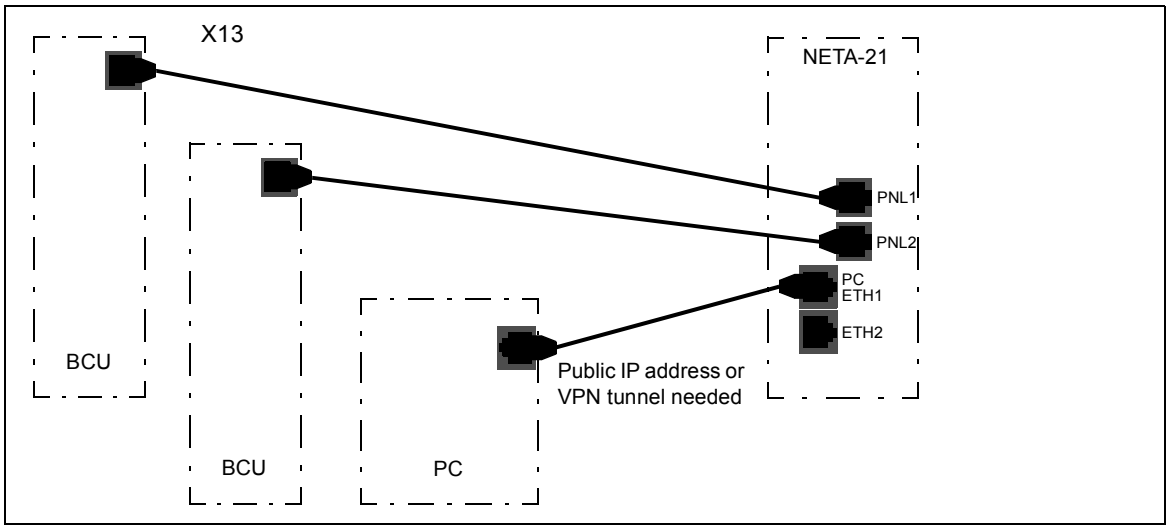


Note: The RJ45 connectors of the control panel are located in the “ceiling” of the control panel housing. Beside the left-hand side RJ45 connector in the control panel housing there is a switch that must be pushed upwards in the last drive of the chain to terminate the bus.

The maximum number of devices per panel port bus is 10.

Set a unique ID to each node on the panel bus. See the appropriate drive manual.

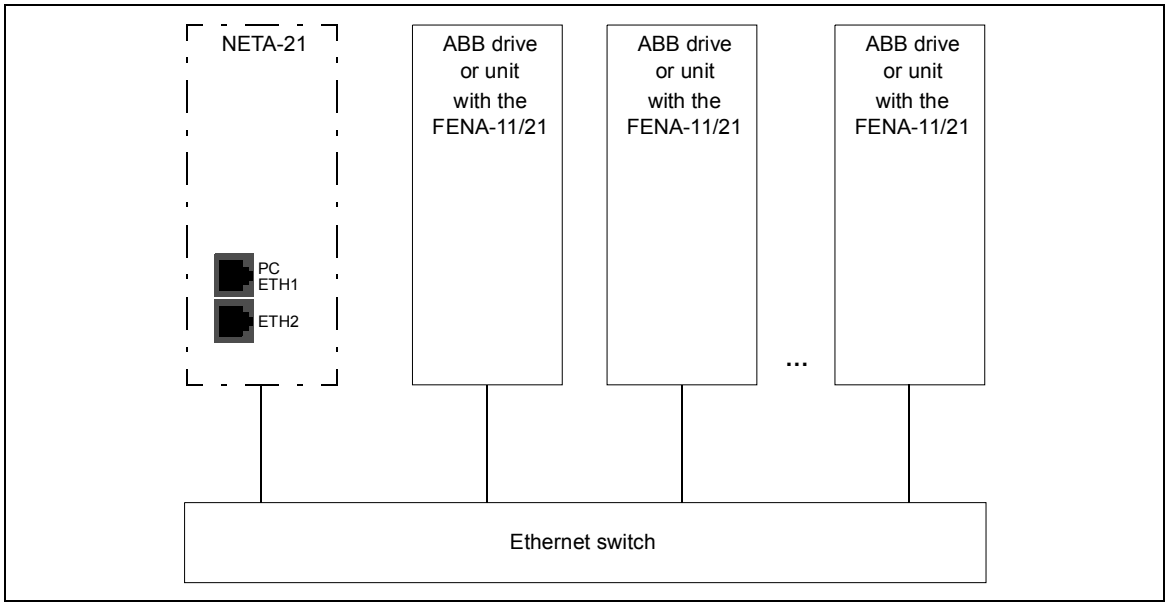
In the BCU-01/02/12/22 control unit, use connector X13 for the panel bus connection.



Connection over the Ethernet tool network with an Ethernet adapter module

In the Ethernet tool network, each drive/unit is connected to the network through a FENA-11/21 Ethernet adapter module.

Note: The Ethernet tool network is available only for ACS880 and ACS860 drive series.

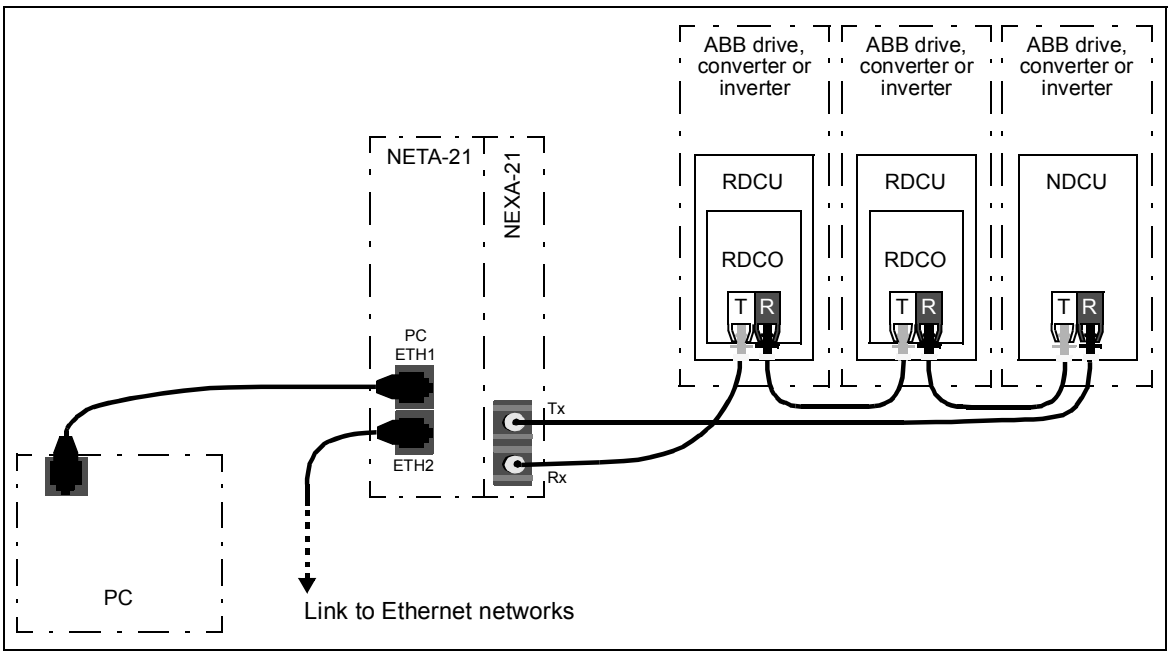


The NETA-21 detects nearby adapter modules (max. 10 pcs over Ethernet) in a local network. The automatic detection is enabled by default only via the ETH2 port. To change the settings of the automatic detection, go to **Settings –> Device interfaces –> Ethernet –> Settings –> Background scan**.

Note: If the ETH1 and ETH2 ports of the NETA-21 are connected, they must be configured to use different sub-nets (different IP addresses under non-overlapping netmasks).

Data link connections – Drive with the RDCU control unit

The figures below show the data connections in a ring and star topology when a fiber optic link is used.



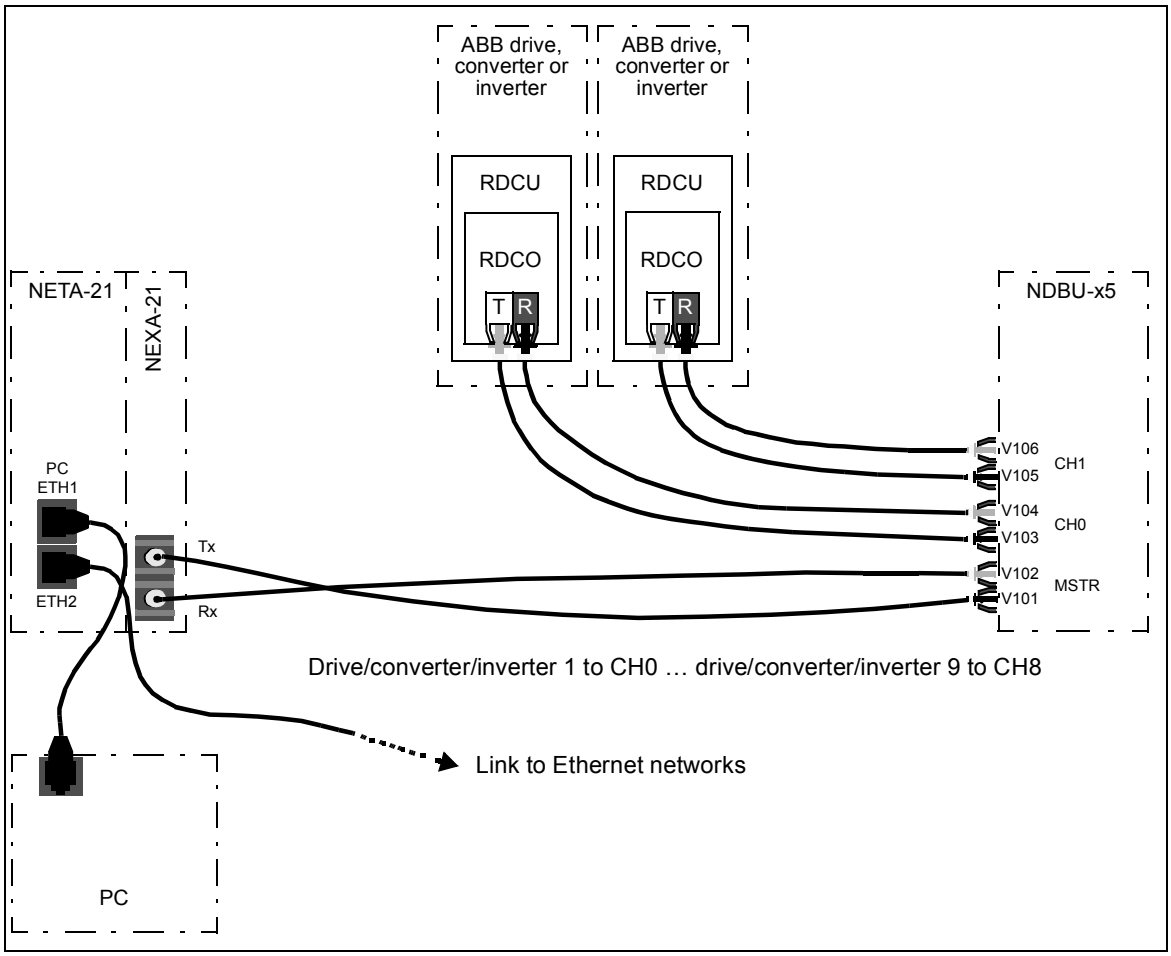
The maximum number of devices per fiber optic link is 10.

Connect the NEXA-21 primarily to fiber optic channel ch3 on the RDCO connector unit. You can connect the NEXA-21 also to ch0 if the maximum speed of the DDCS communication does not increase above 1 Mbit/s.

The default NETA-21 settings for a DDCS network are ring topology and 1 Mbit/s communication speed. With these settings, the NETA-21 can normally auto-detect drives connected to an NDBU branching unit. The NETA-21 auto-detects connected devices when the fiber is connected for the first time. If reconfiguration is needed afterwards, it can be done in the web user interface.

Note: If there are NDCU control units, use channel 4 or 3 (titled Remote diagnostics and PC channel).

Note: Use the same speed setting in the NETA-21, NDBU branching unit and drives.



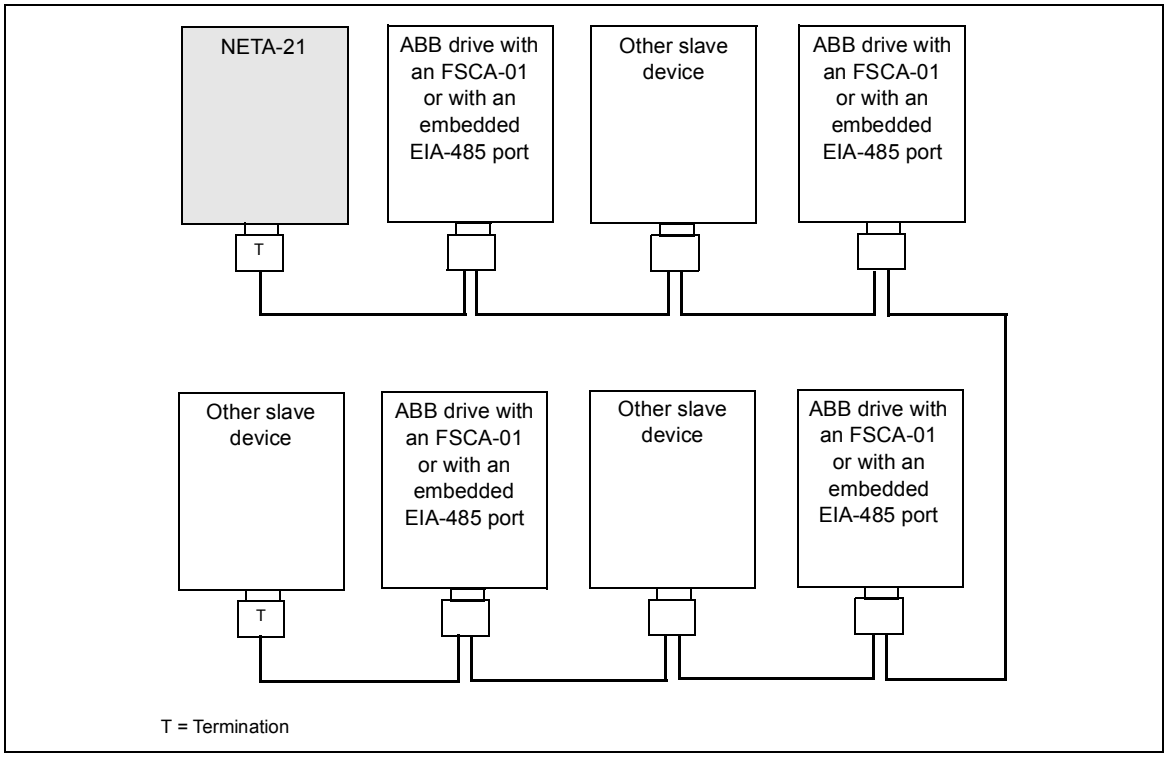
Recommended fiber optic cables for DDCS

You can use the below recommended cables as per the requirement:

- For long distances (50m, 150m, 200m) - Hard clad silica (HCS) optical fiber, a duplex cable which also includes mechanical protection.
- For short distances (2m, 20m) and for optical chains inside drive cabinets - Plastic optical fibre (POF). This zipcord duplex cable can be separated into two single core cables.

Connection via the EIA-485 port with a Modbus/RTU adapter module

A maximum of 32 monitored Modbus/RTU devices can be connected to the same EIA-485 network. The following figure is an example of an allowable topology:

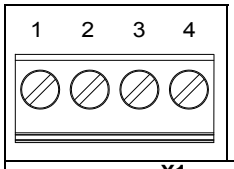


The X3 EIA-485 connector for a Modbus network is located at the bottom of the NETA-21. See the bottom layout in section *Layout of the NETA-21 and the NEXA-21*. The EIA-485 (RS-485) cabling requires a shielded dual twisted pair cable. The nominal impedance of the cable must between 100…150 ohm.

Connecting the NETA-21 to the RS-485 network

Connect the bus cable to connector X3 on the NETA-21.

The pin allocation of the X3 connector is shown below.

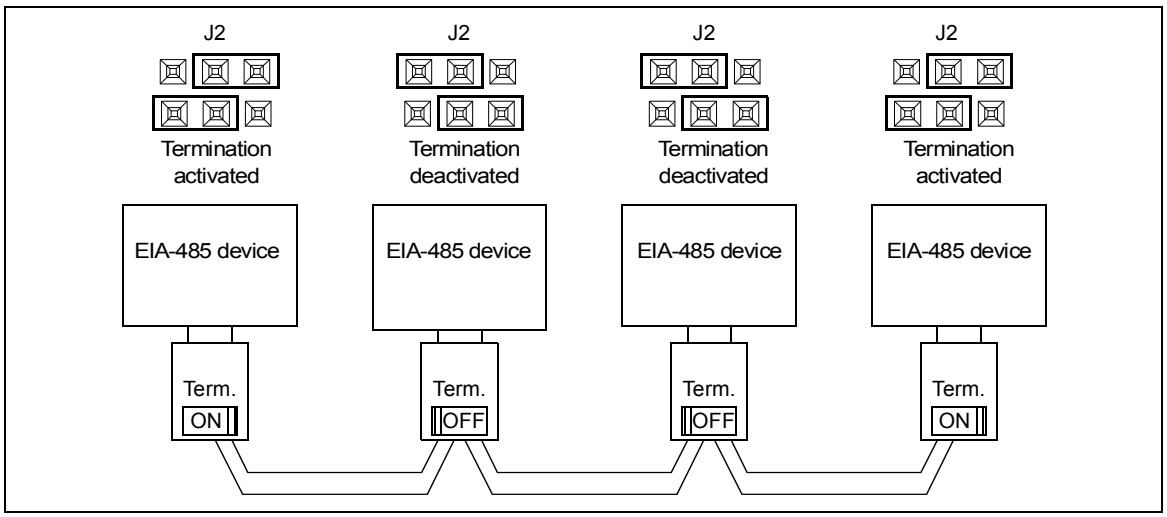


X1		Description
1	SHLD	Bus cable shield. Connected internally to a ground clip via an RC filter. Depending on the installation environment, the shielding is connected to this pin on the NETA-21 or on another location on the EIA-485 network.
2	DATA_B	Data positive
3	DATA_A	Data negative
4	GND_B	Isolated signal ground

Signals DATA_A, DATA_B and GND_B must always be connected to all communication modules and to the NETA-21.

Switching on the bus termination

To avoid signal reflection, add 120-ohm termination to the last devices at each end of the bus line.



You can use the internal resistor of RS-485/EIA-485 adapters or an external passive termination resistor. The internal termination switch activates also the pull-up and pull-down resistors.

6

Start-up

Contents of this chapter

This chapter tells you how to start the NETA-21.

First access to the user interface

This section tells you how to get access to the user interface. The NETA-21 can be used as a DHCP server for a local PC when the PC is connected to the PC ETH 1 terminal. When the DHCP server mode is activated, the NETA-21 provides an IP address to the PC for an easy connection.

The NETA-21 uses dynamic IP addressing by default. After it starts, the NETA-21 tries to get a dynamic IP address from the local Ethernet network if there is a DHCP server available. If there is no local DHCP server in the connected network, then the NETA-21 assigns itself a Zero Configuration networking address in the range of 169.254.1.0…169.254.254.255. The technology of the automatic IP address configuration is called either Link-local address assignment (RFC 3927) or Automatic Private IP addressing (APIPA).

When a local PC is connected to the PC ETH 1 connector, you can set the NETA-21 as the DHCP server in the Ethernet 1 link.

Connecting a local PC to the NETA-21 in the DHCP server mode

Note: If another device operates in the DHCP server mode, you cannot use the NETA-21 in the DHCP mode via the local Ethernet 1 network.

1. Start the NETA-21.
2. Wait until the set-up completes and the STAT LED is green.
3. Push the SD RJ45 button for 5 seconds or until the PC ETH 1 LED starts to flash green.

   The NETA-21 operates as a DHCP server via the PC ETH 1 connector.
4. Connect the PC to the PC ETH 1 connector.

   The PC gets a dynamic IP from the NETA-21.

   The PC ETH 1 LED shows that there is a connection (green blink = waiting, green = connected).

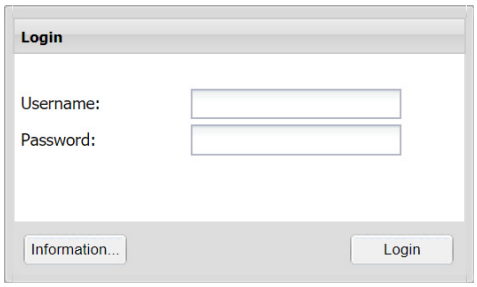
   Note: If after one minute there is no connection between the PC and the NETA-21, the DHCP server mode in the NETA-21 is set off.
5. Go to https://192.168.230.1.

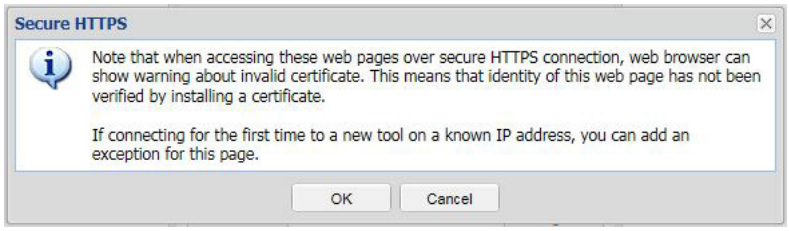
Note: If the Ethernet cable is connected to the NETA-21 before you push the SD RJ45 button, the PC does not automatically get an IP address.

Logging on to the NETA-21

1. With the web browser of you PC, navigate to https://192.168.230.1.
2. When you log on to the NETA-21 for the first time, use the default user name/password.

   Type “admin” both to the **Username** and **Password** text boxes.
   Note: A Secure HTTPS notification window appears, when you use HTTPS login. Acknowledge the instructions to continue. Since FW 3.x, HTTPS login is the default protocol.





3. Click **Login**.

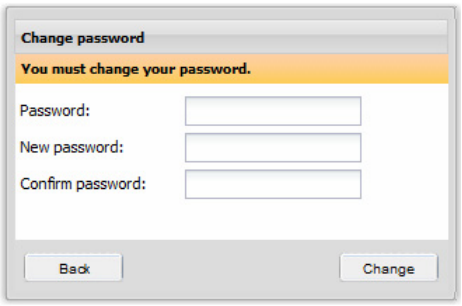
   You are redirected to the front page.

If the authentication does not succeed and you are redirected back to the Login dialog box, the following error messages may appear:

- Authentication failed. Contact system administrator for more information.
- You have logged out from the remote monitoring tool!
- Session expired; you were automatically logged out because of idle time was exceeded.
- Server (remote tool) does not respond to authorization request.
- The server was rebooted.

By clicking the **Information...** button you can get information on, for example, the serial number and MAC addresses of the Ethernet interfaces. To customize the data, go to **Settings –> User interface**.

4. Change the password.



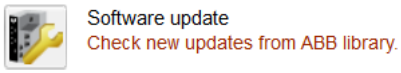
The front page of the user interface is shown. See chapter *Front page*.

You are now logged on as a tool administrator (Tool admin). See section *User roles*.

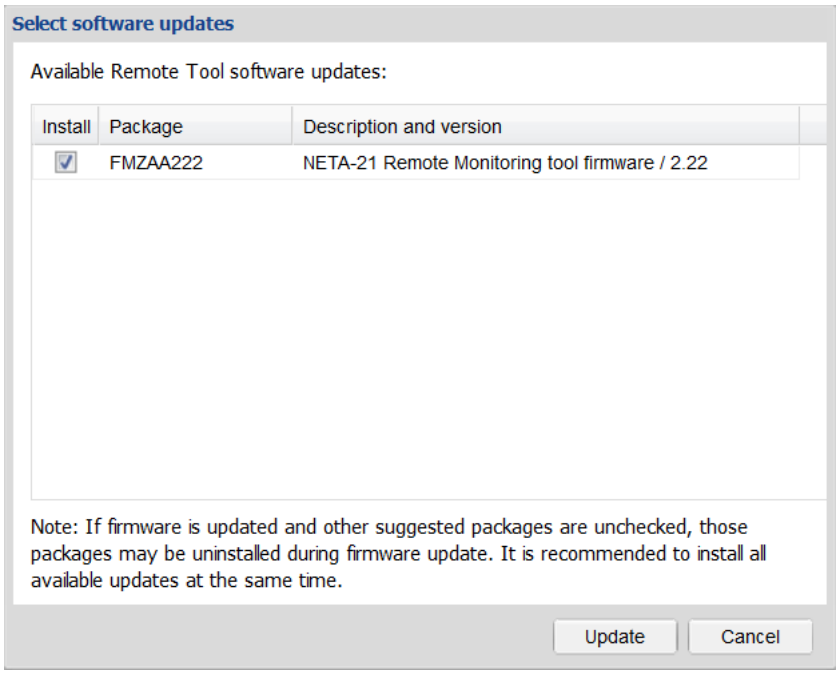
Basic settings

Updating the NETA-21 firmware via ABB web pages

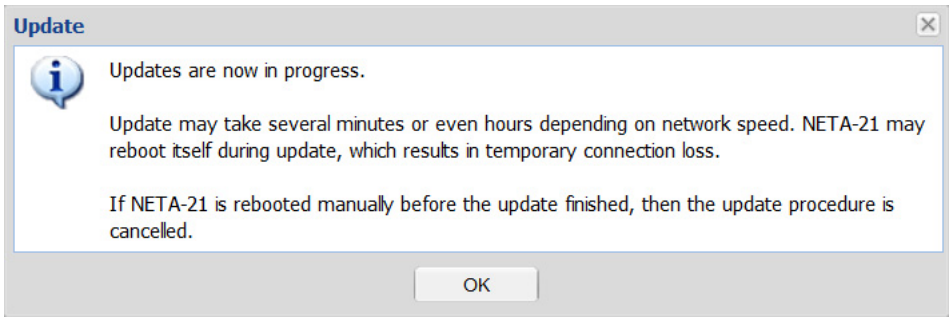
1. Go to the front page.
2. Click the **Software update** button.



The NETA-21 searches the pages for a new version of firmware or any of the installed extra packages and shows a list of available updates.

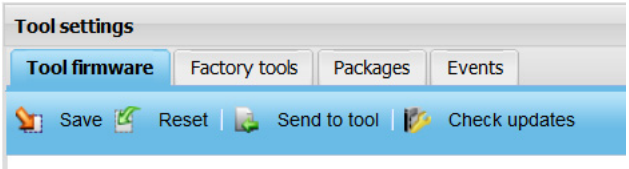


3. Select the updates you want to install and click the **Update** button.
   You get the following Update message.



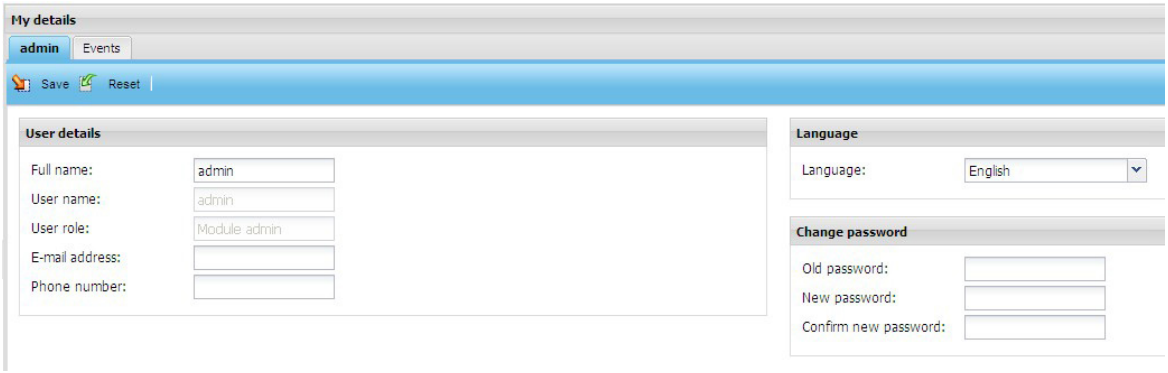
When the selected updates have been downloaded, the NETA-21 reboots.

There is an alternative way to look for available updates: Go to **Settings –> Tool settings –> Tool firmware** and click the **Check updates** button.



Changing the password

1. To change your password, go to **Settings –> My details –> Change password**.

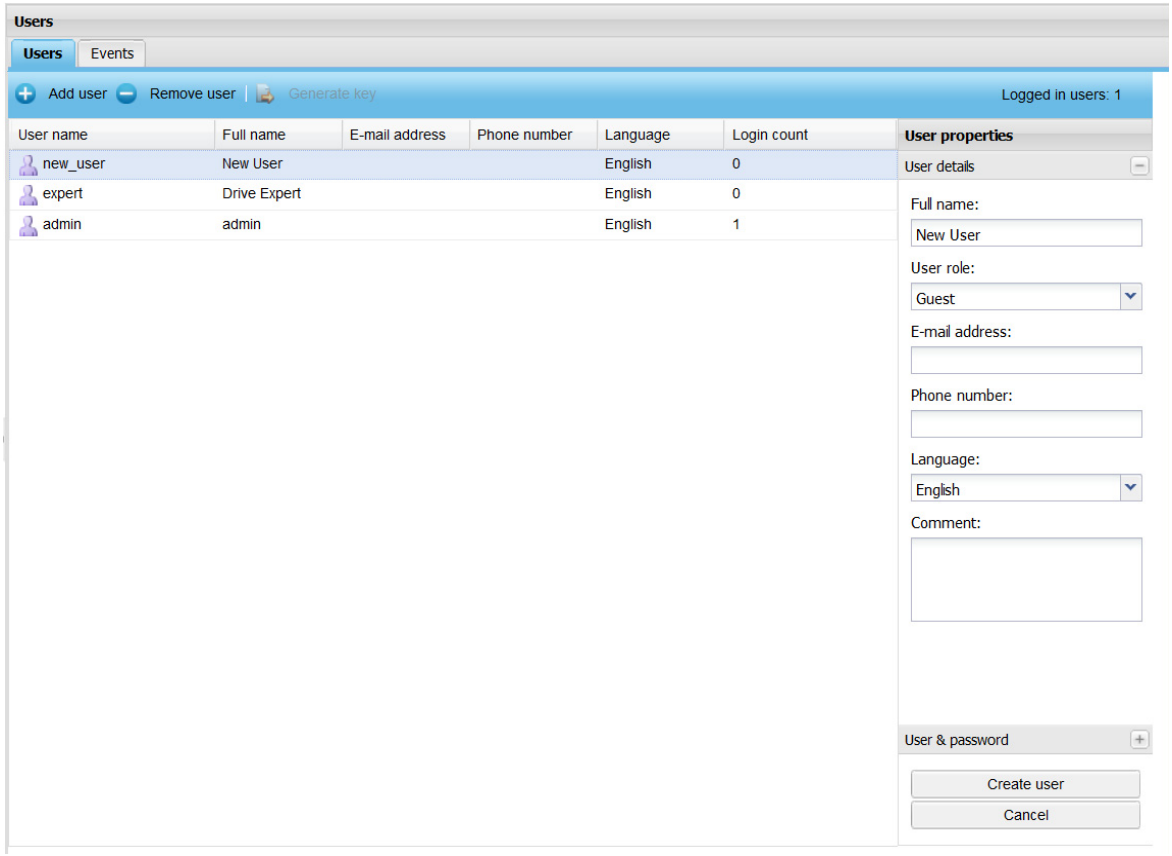


2. Type the old password to the **Old password** text box.
3. Type the new password to the **New password** text box.
4. Type the new password again to the **Confirm new password** text box.
5. Click **Save**.

Adding users

Note: You can add users only if you have the access rights of Network admin or Tool admin.

1. To add a user, go to **Settings –> Users –> Add user**.
   The **User properties** panel appears on the right-hand side of the tab.



   The components of the tab are described in section *User management*.

2. Fill in the text boxes.
   The name typed into the **Full name** text box is shown in the upper right-hand side corner of the window. The user name (login name) is created under the **User & password** sub-panel in step 4.

3. Expand the **User & password** sub-panel by clicking the heading.

4. Fill in the text boxes.
   See section *User roles*.

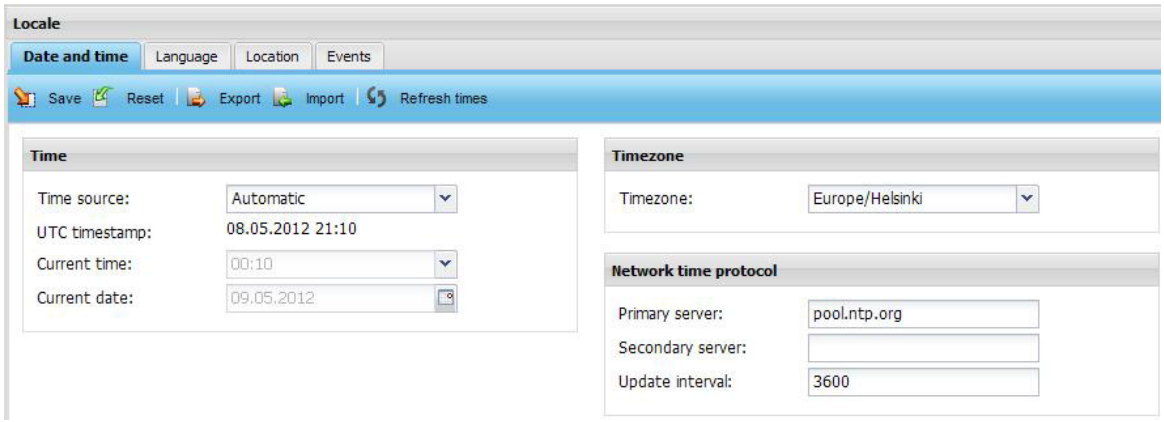
5. Click **Create user**.

Setting date and time

Note: You can change the locale settings, if you have the access rights of Drive expert, Network admin or Tool admin.

1. To set date and time, go to **Settings –> Locale –> Date and time**.

   Note: If the NETA-21 does not have the correct date and time, the stored data will also be logged with incorrect date and time stamp.



2. In the **Time source** drop-down list, select one of the following values:
   - Automatic
   - NTP (Network Time Protocol)
   - Manual
     If you select **Manual**, define the time from the **Current time** drop-down list and select the date from the calendar in the **Current date** box.
   - External
     The external software synchronizes time with NETA-21 periodically. Hence, enable External option when you use remote monitoring services.

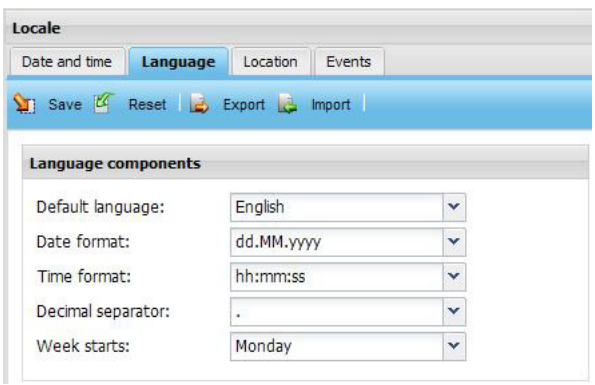
   Note: In the Automatic mode the NETA-21 tries to fetch time and date over NTP, contacting server pool.ntp.org by default.

3. Fill in other appropriate boxes.

Setting the language

Note: You can change the locale settings, if you have the access rights of Drive expert, Network admin or Tool admin. Currently only English language is available for the web UI.

To customize the date format, time format, decimal separator and the first day of the week, go to **Settings –> Locale –> Language**.

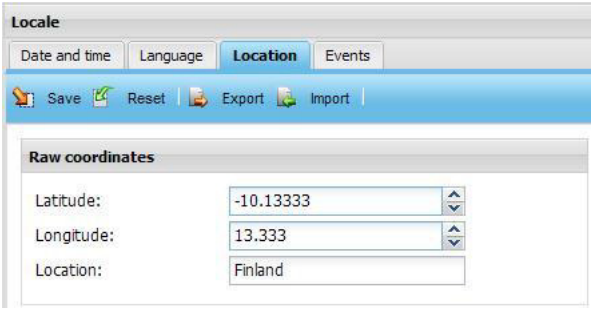


Note: The language selected on the **Language** tab is used only in the web UI of the NETA-21. Monitored devices can have their own independent language selectors.

Setting the location of the NETA-21

Note: You can change the locale settings, if you have the access rights of Drive expert, Network admin or Tool admin.

To set the location of the NETA-21, go to **Settings –> Locale –> Location**.



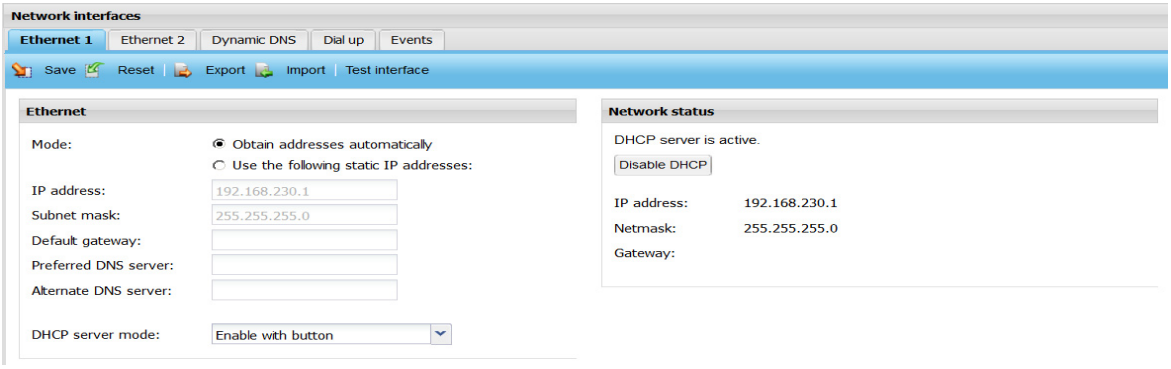
Defining the Ethernet network settings

1. Go to **Settings –> Network interface** and enable the **Obtain DNS server automatically** function.

   The NETA-21 adjusts the communication settings automatically. Individual attributes can be set separately.

   Enable the function both for local Ethernet 1 connected to the PC ETH 1 connector and external Ethernet 2 connected to the ETH 2 connector.

   Note: From firmware version 2.12 onwards, the Ethernet settings are taken into use directly after the settings have been saved. The NETA-21 shows a warning explaining that connection can be lost if the IP address of the currently active connection is changed.



2. From the DHCP server mode drop-down list, select the desired DHCP server mode. The available options are:
   - Disabled always
   - Enable with button
   - Enable during next reboot
   - Enable always
3. Check the LAN settings of your PC.

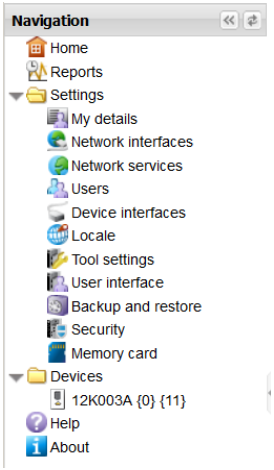
   Activate the following functions: **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

Initializing the communication between the NETA-21 and drives online

WARNING! Follow the instructions in section *Safety in installation*.

Initializing the communication between the NETA-21 and ACS800 drives (or other drives with the RDCU control unit)

1. Switch the drives on.
2. In the first drive, change the node address of channel 3 (CH3) to 1 (example: ACS800 standard control 70.02 CHANNEL 3 ADDR = 1).
3. In the second drive, change the node address of channel 3 (CH3) to 2 (example: ACS800 standards control 70.02 CHANNEL 3 ADDR = 2).
4. Give the rest of the drives a unique ID as well.
   See the appropriate drive manuals.
5. Switch the drives off to set the channel address settings.
6. Switch the NETA-21 off or disconnect the fiber optic cable from the NEXA-21 for more than 1 minute.
7. Connect the drives to the NEXA-21. See section *Communication connections*. Use either the ring or star topology.
8. Switch the drives, NETA-21 and NEXA-21 on.
9. Wait until the PWR and STAT LEDs of the NEXA-21 go green.
   Tx and Rx LEDs are yellow indicating that there is data transmission between the NETA-21 and monitored devices.
10. Log on to the UI when the STAT LED of the NEXA-21 is blinking green.
    The UI recognizes the monitored device automatically and the drive is shown in the user interface.



Note: If the NETA-21 does not detect all drives automatically, go to **Settings –> Device interfaces –> DDCS –> Rescan devices**.

11. Click **Save**.

7

Program features

What this chapter contains

This chapter describes some of the features listed in section *NETA-21-specific features* in more detail.

FTP/FTPS

FTP (File Transfer Protocol) is a simple protocol designed for transferring files.

FTP allows you to browse folders in a remote device. All normal operations are supported, eg, you can create or delete folders, and move, delete or rename files.

The main purpose of using FTP is to upload or download files between the local and remote device.

The NETA-21 supports both unencrypted and encrypted (FTPS) connection.

The unencrypted connection s disabled by default and works on port 21.

The encrypted connection supports only explicit Transport Layer Security (TLS) encryption and works on port 990.

You can enable or disable these services as well as change the default port through the Network services panel.

HTTP

The HTTP (Hypertext Transfer Protocol) is used to serve web pages using the HTML (Hypertext Markup Language) and Javascript. To use the NETA-21 web interface you need a browser supporting Javascript and cookies (see *Hardware and software requirements of the PC*). External plug-ins, such as Java or Flash, are not required.

It is recommended to use HTTP only with a direct cable connection to the NETA-21. For all other purposes it is recommended to use the secure HTTPS. To switch from HTTP to HTTPS edit the address from http://192.168.230.1 to https://192.168.230.1. You can also do this by checking the **Prefer HTTPS** check box in **Network services**.

HTTPS URLs use port 443 by default, whereas HTTP URLs use port 80 by default.

HTTPS

The Hypertext Transfer Protocol Secure (HTTPS) is a combination of the HTTP with an added encryption layer of SSL/TLS protocols to create a secure channel over an insecure network, provided that adequate cipher suites are used and that the server certificate is verified and trusted. The HTTPS is supported by all popular browsers.

Note: Although the HTTPS encrypts everything, including the URL, an eavesdropper can still observe the host name and port of the URL because they are part of TCP/IP packets to establish and maintain the connection. This means that an eavesdropper or attacker can know that a connection is taking place between the two parties, get the domain name and IP addresses, through which he can see the sites the host is connect to, the amount of time spend using a site, and the amount of information uploaded or downloaded on the particular site.

HTTPS certificate

The NETA-21 HTTPS uses a self-signed certificate which is uniquely generated per each NETA-21 tool. The factory reset of the NETA-21 can also reset the self-signed certificate and generate a new one (while, eg, a firmware update keeps the certificate unchanged).

Most browsers display a warning if they receive an invalid or a self-signed certificate. When you connect an older browser to a site with an invalid certificate the browser shows you a dialog box asking if you want to continue. Newer browsers display a warning across the entire window and also prominently display the site's security information in the address bar. Extended validation certificates turn the address bar green in newer browsers. Most browsers also display a warning when you visit a site that contains a mixture of encrypted and unencrypted content.

From the NETA-21 firmware version 2.13 onwards you can install a customized HTTPS site certificate to each NETA-21. The installation requires than an Apache 2 compatible apache.pem certificate file is generated on the PC and saved to folder "cert” in the SD memory card. Create a “cert” folder, if the “cert” folder does not exist. The customized certificate will be taken to use after a reboot or power-up of the NETA-21. A valid certificate is taken into use and removed from the memory card for security reasons.

Modbus/TCP gateway

The NETA-21 supports a subset of the Modbus/TCP protocol specification v1.1b. This allows to use a normal TCP/IP connection to access the parameters of drives.

The supported functions are:

- 03 (0x03) Read Holding Registers
- 06 (0x06) Write Single Register
- 16 (0x10) Write Multiple registers
- 23 (0x17) Read/Write Multiple registers
- 43 (0x2B) Encapsulated Interface Transport

To enable the service for selected network interfaces (by unlocking it in the NETA-21 internal firewall), go to **Settings –> Network services –> Services**.

With a normal PC and a program that supports the Modbus/TCP protocol in the same network to which the NETA-21 is connected, you can query values of parameters from the connected devices. The Modbus/TCP client configuration requires you only to specify the IP of the NETA-21 and port 502.

The Modbus protocol supports up to 247 devices. Each device is identified with an ID, a number from 1 to 247.

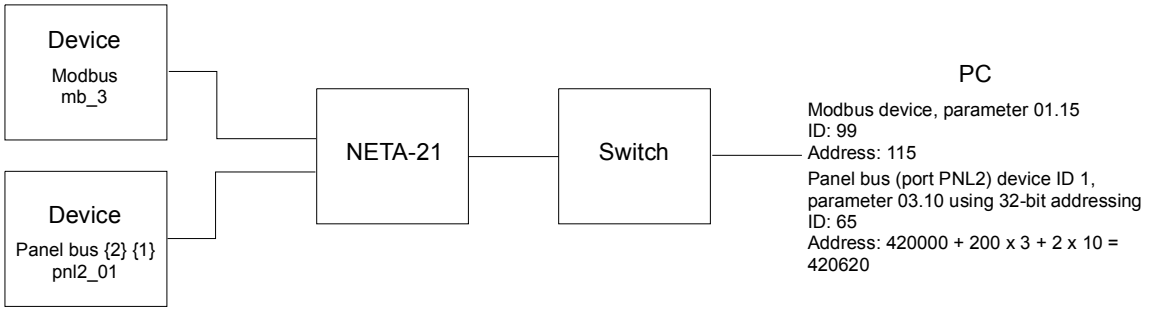
ID range	**Protocol**
1…32	DDCS fiber optics
33…64	Panel bus 1 (port PNL1)
65…96	Panel bus 2 (port PNL2)
97…128	Modbus/RTU
129…160	Ethernet tool network
161…247	Reserved

The ID used by a specific device can be determined with its internal name (shown in the **Modbus/TCP gateway** panel under **Device interfaces**). This name always ends with a number that represents the index inside the range of the IDs of the specific protocol. For example, a slave device connected through the Modbus/RTU protocol with station address 3 (device node ID mb_3) is accessible by Modbus/TCP gateway station address 99 (97+3-1).

To access a specific parameter of a given group and index, you must specify an address by calculating it according to one of the following formulas:

16-bit address = (4)0000 + 100 × group + index

32-bit address = (4)20000 + 200 x group + 2 x index



By default, the Modbus protocol returns the internal raw 16-bit value and does not specify any information about sign and scaling. Therefore, you must apply the correct ones for the specified parameter.

Note: Most Modbus/TCP master applications omit the 40000 (or 400000) from the beginning of the register numbering.

The Modbus function code 03 Read Holding Registers is supported over the Modbus/TCP gateway of the NETA-21. In firmware 2.23 you can configure the settings of the Modbus/TCP gateway. Go to **Settings –> Device interfaces**. Firmware 2.23 and above supports a read/write option. In addition, firmware 2.24 and above supports dataset access.

If any user tries to access read protected, write protected, or 'string' type drive parameters via Modbus/TCP Gateway, the error 0x02 - **Illegal Data Address** is sent to the master.

Notes:

- For security reasons, Modbus/TCP gateway connections must be used only inside a trusted network.
- Modbus/TCP gateway throughput for DDCS interface is approximately 10 ms/read, 100 parameter values per second, and 4 ms/read for datasets, provided no other interface (Panel bus, Ethernet, Modbus) is accessed simultaneously. Mixing interfaces increases response time for DDCS.
- From NETA-21 firmware version 3.00, you can enable NETA-01 compatibility mode from **Device interfaces –> Modbus/TCP gateway –> Settings –> Interface settings –> NETA-01 compatibility**. As a result, a device “NETA-01 emulation” appears, with Modbus node id 0. This device can implement customizable Modbus/TCP register to any drive with any parameter mapping.
- For better performance, set DDCS Gateway mode to Dedicated mode. In this mode, case WebUI and Reporting do not impact Modbus/TCP gateway operations.

Exception codes

NETA-21 supports the following Modbus exception codes:

Exception code	Name	Description
01h	ILLEGAL FUNCTION	The function code received in the query is not an allowable action for the server.
02h	ILLEGAL DATA ADDRESSS	User tries to access read/write protected or string type drive parameters using Modbus/TCP Gateway.

Exception code	Name	Description
03h	ILLEGAL DATA VALUE	A value contained in the query data field is not an allowable value for the server.
04h	SLAVE DEVICE FAILURE	An unrecoverable error occurred while the server was attempting to perform the requested action.
06h	SLAVE DEVICE BUSY	The server is engaged in processing a long-duration command. The client should retransmit the message later when the server is free.
0Ah	GATEWAY PATH UNAVAILABLE	NETA-21 is engaged in boot up and all services which provides Modbus/TCP gateway to drive is not completely initialized. Error code disappears after full boot up.
0Bh	GATEWAY TARGET DEVICE FAILED TO RESPOND	Internal timeout occurred when NETA-21 was forwarding Modbus/TCP request to drive interface. This can be due to ongoing operation on drive interface. For example, parameter backup operation. You can increase timeout value on Modbus/TCP gateway settings or switch to Dedicated mode in DDCS device adapter settings to avoid this error.

Ethernet PC tool gateway

WARNING! Make sure that all Ethernet PC tool gateway connections (DDCS and Panel bus) are used only inside a trusted network. Untrusted networks can cause cybersecurity threats.

Drive Composer establishes Ethernet communication only with recognized devices such as FENA-11 and FENA-21 Ethernet fieldbus adapters.

The PC tool friendly mode should be enabled in NETA-2 if NETA-21 and Drive Composer are used at the same time through Ethernet. To enable PC tool friendly mode, go to **Settings –> Device interfaces –>Ethernet/Settings –> PC tool friendly mode**.

Drive Window PC tool can connect to UDP port 61332 on NETA-21 and access connected drives through the DDCS Ethernet gateway. When a connection is active, normal DDCS communication from NETA-21 web user interface to the drive is suspended.

Note: PC tool Gateway mode causes NETA-21 to disconnect Ethernet connectivity with the drive, if it detects other PC tool traffic such as running Drive Composer Pro in nearby network.

TCP and UDP service ports

There are multiple in-bound and out-bound network services running on the NETA-21.

In-bound network services on the NETA-21

Port	Service	Purpose
21 / TCP 990 / TCP	FTP	File transfer service. Enabled by default, but FTP user accounts need to be specified in the web UI (**Settings –> Users**) before the FTP login becomes possible. Port 990 provides a file transfer service with an SSL security layer. You can use the same user accounts as for the FTP service. Explicit TLS encryption must be used in a FTPS client. (SFTP protocol is not supported). To modify the FTP and FTPS service availability, go to **Settings –> Network services**.
22 / TCP	SSH	SSH console for support and diagnostics. Each NETA-21 contains a factory user account with a random password. SSH access is not provided for NETA-21 end users. To disable the SSH service, go to **Settings –> Tool settings –> Factory tools** and deselect **Enable factory login (factory support account)**.
80 / TCP	HTTP	Web server provides the UI over the HTTP protocol. HTTP protocol access is always enabled. Recommendation to use HTTPS is shown in the tool login box.
443 / TCP	HTTPS	Secure version of the HTTP pages. To modify the HTTPS port, go to **Settings –> Network services**.
502 / TCP	Modbus/TCP	Modbus/TCP Gateway is listening on port 502. Gateway forwards Modbus/TCP data requests to any connected drive (either as DDCS fiber optics, RJ45 Panel bus or as EIA485 Modbus/RTU traffic). To modify the service availability, go to **Settings –> Network services**.
(optional) / TCP	HTTP	To specify an extra HTTP port (any higher TCP port than 1024) or a default HTTPs port, go to **Settings –> Network services**. Extra port is disabled by default.
67,68 / UDP	DHCP (client and server)	DHCP client functionality is used in both Ethernet ports by default as specified in RFC 3927 (Dynamic Configuration of IPv4 Link-Local Addresses). DHCP server can be activated only on the ETH1 port.
137 / UDP	NBT NS	Netbios (NBT) Name Service allows a name resolution from Windows XP / Windows 7 PC by typing `http://neta-21` to the address bar of the web browser (if a firewall is disabled in Windows). NBT NS service is active only on the ETH1 port by default. To modify the service availability, go to **Settings –> Network services**.
24576 / UDP	ABB Netconfig	Autodiscovery protocol used by ControlBuilder plus (IP Configuration tool) and Drive composer pro and DriveWindow 2.40 PC tools to discover ABB-specific Ethernet devices in a local network segment, by listening to and responding to UDP broadcasts. This service is also in the out-bound services list.
61332 / UDP	Ethernet GW	Ethernet gateway service is disabled by default. When enabled, the DDCS Ethernet gateway starts to wait for DriveWindow PC tool connections on this port. To enable the service, go to **Settings –> Device interfaces –> DDCS –> Settings –> Ethernet GW**.
8888 / TCP	Panel bus Ethernet GW	Ethernet gateway service is disabled by default. When enabled, the Panel bus Ethernet gateway starts to wait for Drive Composer PC tool connections on this port. To enable the service, go to **Settings –> Device interfaces –> Panel bus –> Settings –> Ethernet GW**.

Port	Service	Purpose
-	ICMP	Internet Control Message Protocol (ICMP) messages are typically used for diagnostics or control purposes. The ICMP messages are also generated in response to errors in IP operations. There is no TCP or UDP port number associated with ICMP packets.

Out-bound network services on the NETA-21

Port	Service	Purpose
21	FTP	File Transfer Protocol. Reporting option for sending CSV files over the FTP protocol to any external server. Not in use until configured.
25 / TCP (or another configured port)	SMTP(S)	Simple Mail Transfer Protocol, outgoing e-mail. Also secure version SMTPS is supported (typically TCP port 587 or 465). NETA-21 can send email out if the SMTP(S) server settings and email reporting are configured. By default, the service is not in use. Two SMTP servers are supported (primary and secondary server). Server names and outgoing port numbers can be configured in the web UI (**Settings –> Network services**). To enable the email plug-in, go to **Reports –> Settings –> Add** and select **E-mail reporting**.
80, 443	HTTP, HTTPS	Used for reporting data to external portal services. Not in use until configured.
80	HTTP	HTTP protocol is used for the Ethernet tool network slave device access, to access FENA-11/-21 fieldbus modules and BCU-xx control boards over the Ethernet tool network (typical use case in a local/private network only). Connection to supported devices established if supported devices are discovered.
123 / UDP	NTP	Network Time Service. NETA-21 sends outgoing NTP service packets to “pool.ntp.org” by default every hour. To configure the setting, go to **Settings –> Locale –> Date and time**. If no NTP server is found, the NETA-21 defaults to a manually configured clock setting.
24576 / UDP	ABB Netconfig	Autodiscovery protocol. By default the NETA-21 sends discovery broadcasts over the ETH2 interface every minute to discover other ABB devices (eg, FENA-11 or BCU-xx) in a local network segment. To modify the background scan setting, go to **Settings –> Device interfaces –> Ethernet –> Settings**.
53 / TCP, UDP	DNS	Used for Domain Name Service (DNS).

Safe deployment of NETA-21

WARNING! It is strongly recommended not to connect NETA-21 WebUI interface directly to the internet, even when you use secure HTTPS protocol. Connection to the WebUI should be protected by the customer's external firewall or VPN network. This decreases proneness to unauthorized access of NETA-21.

The NETA-21 firmware includes many extra services as follows:

- NBT NS discovery
- ABB Netconfig
- FTP
- FTPS
- HTTP
- Modbus/TCP gateway
- PC tool gateway
- NTP

Before deployment of NETA-21 cybersecurity features, you should disable all unwanted services. By default, the following services are disabled:

- PC tool gateway
- Modbus/TCP gateway
- FTP
- Modbus/TCP master (By default, no slaves are configured)

The services can be disabled as follows:

Service	Navigation	Action
ABB Netconfig	Setting **–>** Network services **–>** Services **–>** Firewall settings	Clear the check box of the desired network interface.
FTP	Setting **–>** Network services **–>** Services **–>** Firewall settings	Clear the check box of the desired network interface.
FTPS	Setting **–>** Network services **–>** Services **–>** Firewall settings	Clear the check box of the desired network interface
HTTP	Setting **–>** Network services **–>** Services **–>** Firewall settings	Clear the check box of the desired network interface **Note:** HTTP protocol can be disabled only if HTTPS port setting has the default value 443.
Modbus/TCP gateway	Setting **–>** Network services **–>** Services **–>** Firewall settings	Clear the check box of the desired network interface.
PC tool gateway	Settings **–>** Device interfaces **–>** Panel bus **–>** Settings	Set Ethernet GW to Disable.
NTP	Settings **–>** Locale **–>** Date and time	Set Time source to Manual or External.
	Network Time protocol settings	Replace public NTP server address with a local server address.

Cybersecurity Disclaimer

This product is designed to be connected to and to communicate information and data via a network interface. It is Customer's sole responsibility to provide and continuously ensure a secure connection between the product and Customer network or any other network (as the case may be). Customer shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

8

Front page

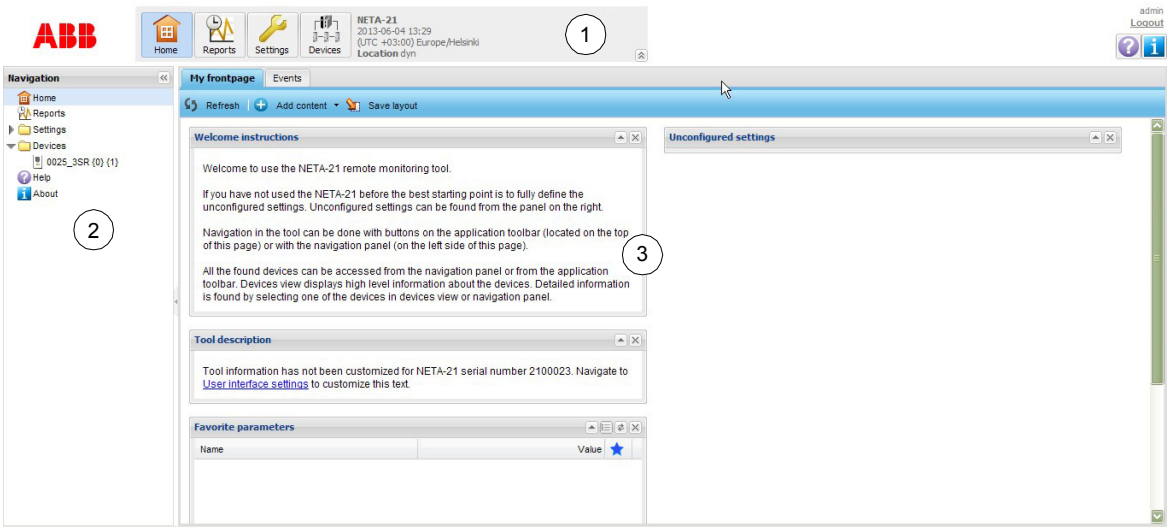
What this chapter contains

This chapter describes the front page of the web UI.

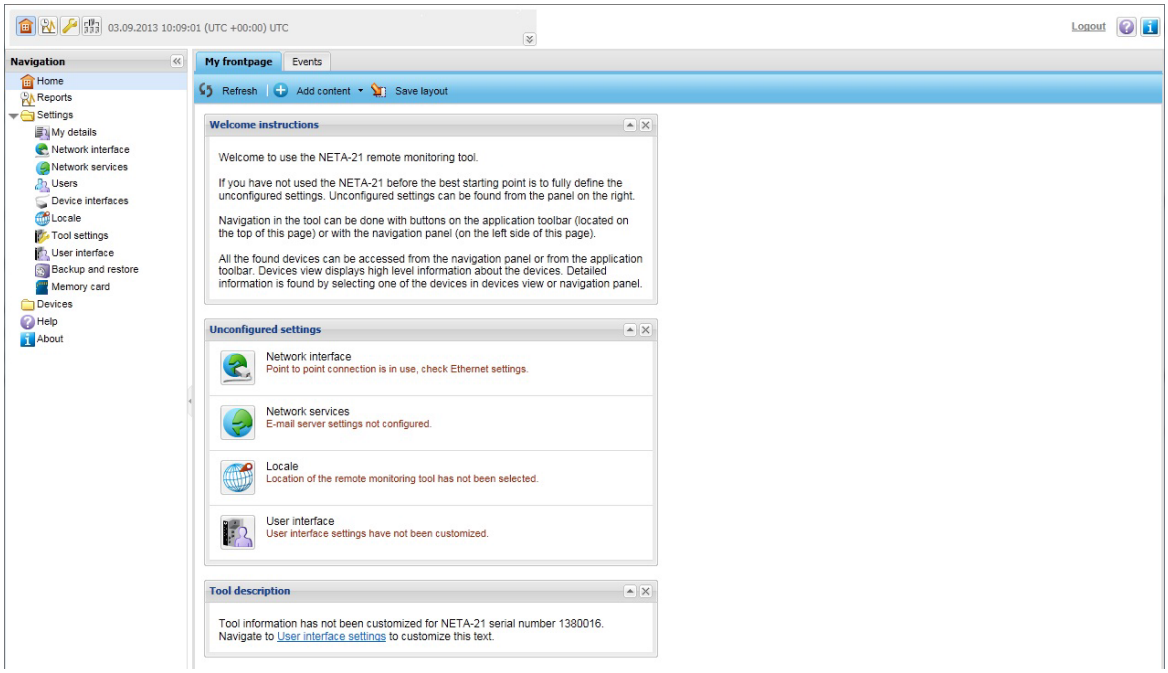
Parts and components of the portal

The front page consists of the following parts:

- application-specific toolbar (1)
- navigation bar (2)
- content area (3).

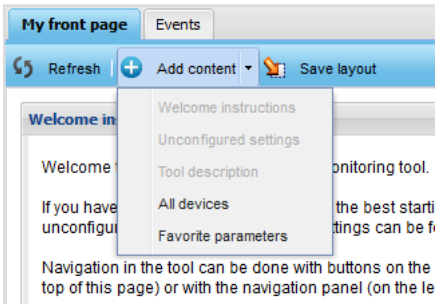


The front page is a portal where you can change the contents by adding, removing or moving around the portlets. The figure below shows a modified front page.

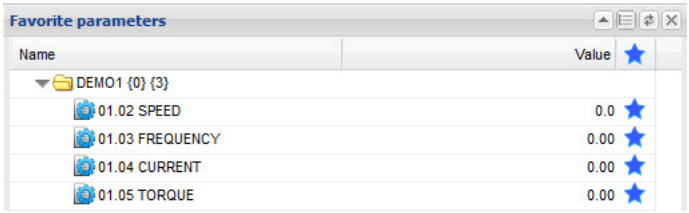


The front page contains the following components:

- **Refresh** button updates the contents of the front page.
- **Add content** button adds new portlets to the front page. The portlet can be selected from a pop-up menu. If a portlet is already selected, the corresponding menu item is disabled in the pop-up menu.



- **Save layout** button stores the current layout to be loaded when the front page is opened again.
- **Welcome instructions** portlet contains instructions for the new user. To change the instruction text, go to **Settings –> User interface**.
- **Tool description** portlet contains a description of the NETA-21. The description text can be changed from the settings.
- **Favorite parameters** portlet contains the parameters that are marked with a blue star on the **Parameter browser** tab. To refresh the values of the parameters, click the **Refresh** button on the title bar.

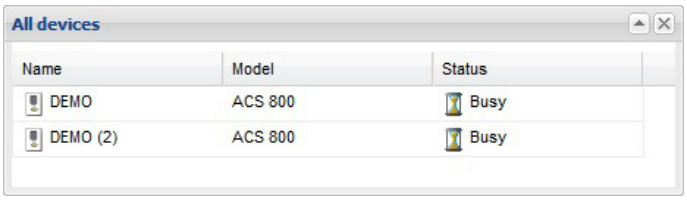


To group the parameters by drive, click the button on the title bar.

- **Unconfigured settings** portlet shows the settings categories that have not been configured or that are misconfigured. By clicking the category button you are redirected to the corresponding settings view.

All devices portlet

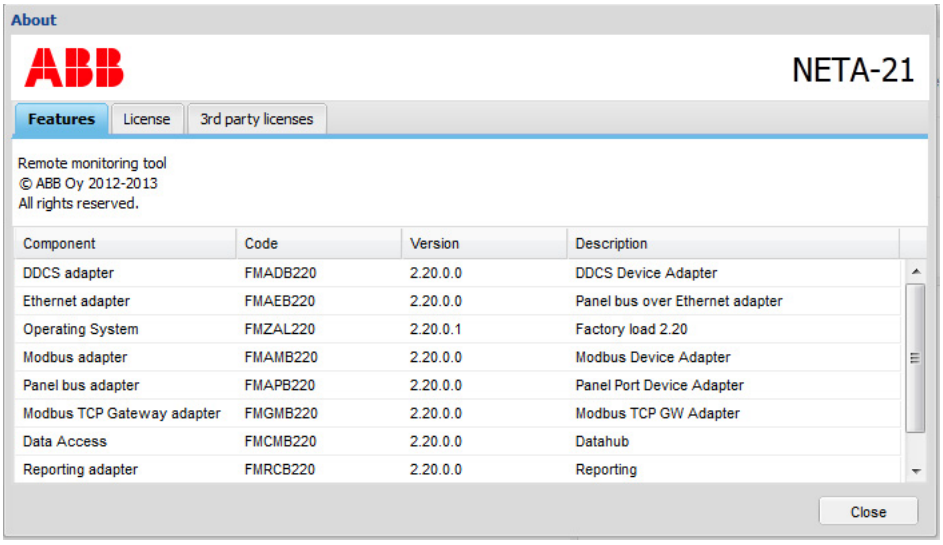
The **All devices** portlet shows all devices connected to the NETA-21. To navigate to the front page of a device, double-click the device in the list.



All portlets can be minimized or closed by clicking the icons in the right corner of the portlet title bar.

Version information

To find out the version information of the NETA-21, click **About** in the navigation bar of the user interface or the corresponding icon in the application-specific toolbar.



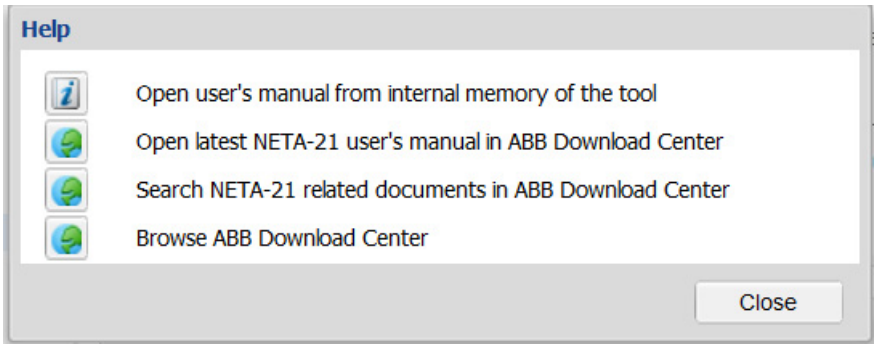
- **Features** tab shows the versions of the internal software components.
- **License** tab contains the software license agreement.
- **3rd party licenses** tab lists the third-party software licenses in this product. The third-party licenses include open source software licenses.

Application toolbar and navigation bar

The application-specific toolbar is visible in every view (excluding the login page) on the top of the user interface. The toolbar provides a quick access to the views that are used most frequently. The toolbar contains the following components:

- Tool ID field shows the identifier of the NETA-21 (default: NETA-21 <serialno>).
- Time field shows the current time and time zone of the NETA-21.
- Location field shows the location of the NETA-21.
- User name field in the upper right hand corner shows the name of the user that has logged on.
- **Logout** link logs the currently logged-on user out. The user is redirected to the login page.
- **Help** button opens the following dialog box.

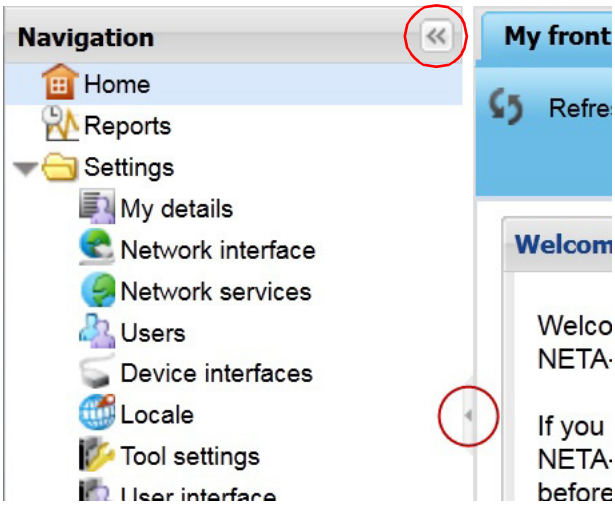
  Note: The ABB library access requires a connection to the Internet.



- **Home** button opens the front page of the user.
- **Reports** button opens the reporting view.
- **Settings** button opens the main settings view.
- **Devices** button opens a view showing all the devices connected to the NETA-21.
- Top bar can be shrunk to a smaller size by clicking the double arrow button at the bottom right corner of the gray box.

The navigation bar contains the above-mentioned navigational items and also the sub-items for the Settings and Devices items.

The navigation bar can be hidden/unhidden by clicking the small arrow between the navigation bar and the content area or the double arrow within the Navigation title bar.



Status icons

In the navigation bar and application toolbar the statuses of the devices are indicated with small icons. The following device statuses are supported:

- disconnected
- busy
- warning
- fault.

If the device is connected and functioning normally, the device is shown without any status icon.

The **Devices** button in the application toolbar can have a maximum of three different status icons simultaneously. For example, if there are two devices that are disconnected, only one icon indicating a disconnected device is shown in the **Devices** button. If there is one disconnected device and one busy device, both icons are shown in the **Devices** button. If all four statuses occur at the same time, the icons indicating the fault, disconnected and warning statuses are shown in the **Devices** button. If the status of the device is missing or cannot be read, the device is shown with the busy icon.

Content area

The application-specific tabs are shown in the content area. The view in the content area changes as soon as you have selected another application since the UI does not have to load a new HTML file from the server. However, you may have to refresh the view if the data gets out of date.

9

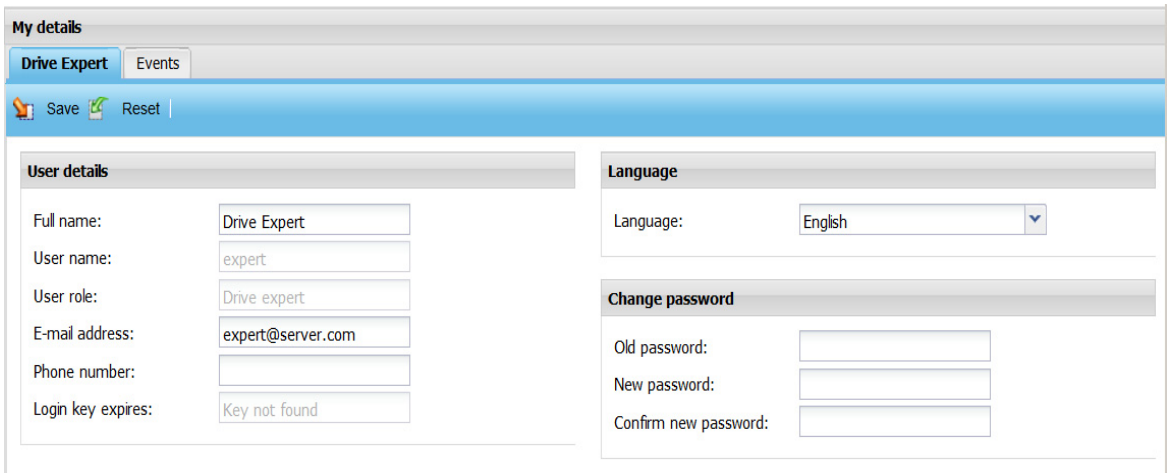
Users

What this chapter contains

This chapter describes the user management.

My details

To see the settings of a current user, go to **Settings –> My details**. On the **admin** tab, you can change your email address, phone number, language and password. You cannot change your user name or role, even if you had an administrator role.



The **admin** tab contains the following components:

- **Save** button saves the modified settings to the server.
- **Reset** button cancels the changes in the settings.
- **Full name** text box shows the full name of the current user.
- **User name** text box shows the user name of the current user.
- **User role** text box shows the user role of the current user.
- **E-mail address** text box shows the email address of the current user.
- **Phone number** text box shows the phone number of the current user.
- **Login key expires** shows the login key expiry time.
- **Language** drop-down list shows the selected language of the user interface.
  - When the language is changed, the change takes place in the user interfaces as the next view is loaded from the server.

  Note: Currently, only English language is supported.
- **Old password** text box is empty by default.
  - If you want to set a new password, the old password must be written for verification purposes.
- **New password** text box empty by default.
  - The minimum requirement for the valid password is two different characters.
- **Confirm new password** text box is empty by default.
  - You are notified if both passwords do not match or the old password is wrong or missing.

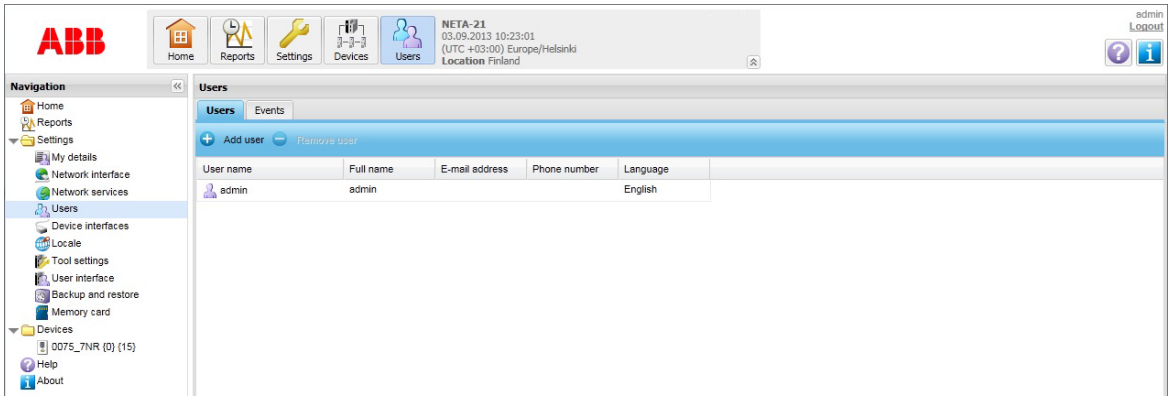
User management

You can restrict the access rights of users by choosing different roles for them. The names of the roles are descriptive, for example, Guest has the lowest level access to the NETA-21 and Tool admin can change everything in it.

Note: The NETA-21 includes a factory account for the web UI. This account is not shown in the users list. To disable the factory account, go to **Tool settings –> Factory tools** (see *Factory tools*).

Users tab

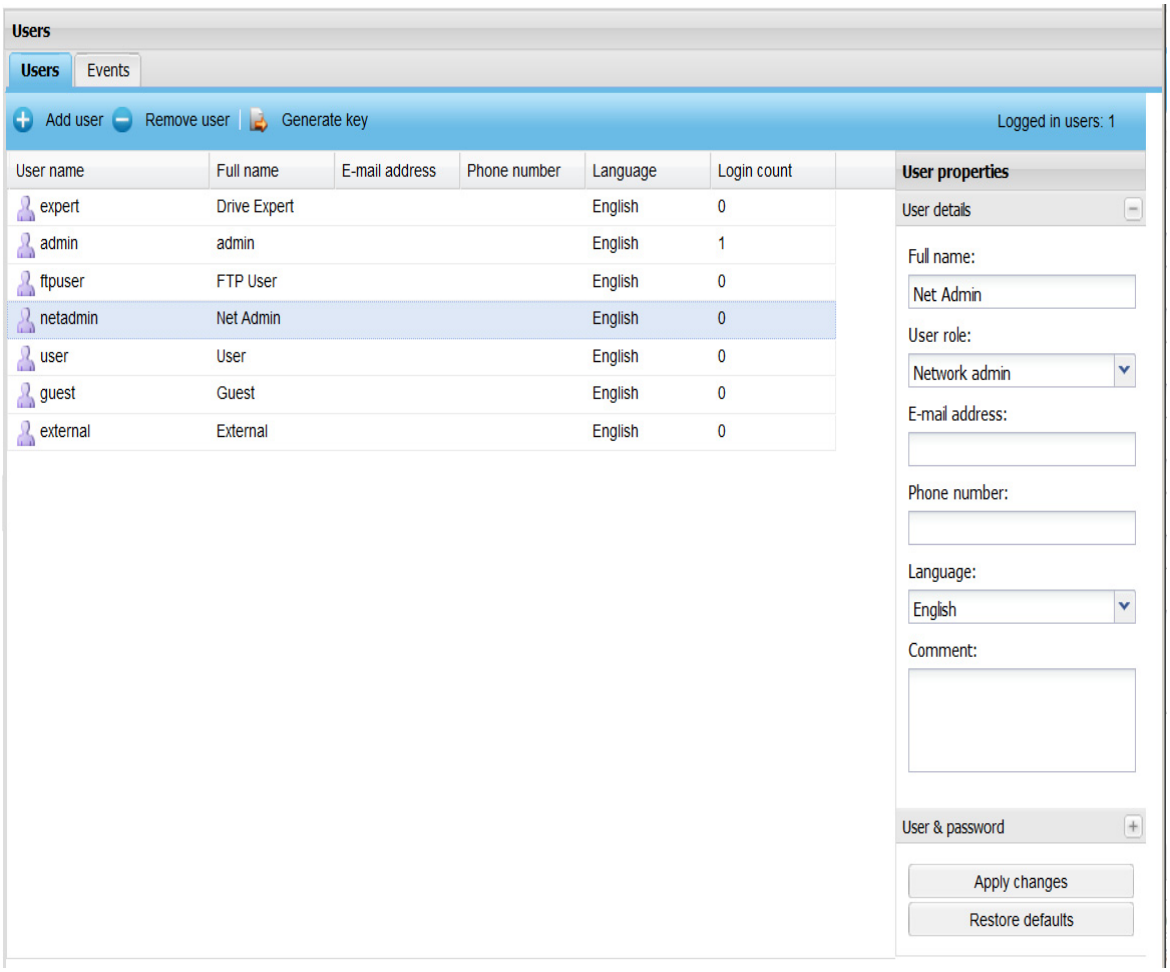
On the **Users** tab you can add, remove and modify users.



The **Users** tab contains the following buttons:

- **Add user** button inserts a new user in the list with default settings. The new user is not added to the UI until you have clicked the **Create user** button in the User properties panel.
- **Remove user** button removes the selected user from the UI. This button is disabled if no users are selected from the user list, or if the user selects itself.
- **Generate key** button creates a hash key which can be used to securely log into the tool without providing the user password.
- **Logged in users** shows the total number of active users.

User list contains existing users, which can be sorted according to different columns. When a user is selected from the list, the User properties panel appears on the right side of the tab.



The user list contains the following columns:

- **User name** shows the name which is used for logging on to the UI.
- **Full name** shows the full name of the user.
- **E-mail address** shows the email address of the user.
- **Phone number** shows the phone number of the user.
- **Language** shows the used language when the user is logged on.
- **Login count** shows the total number of logins performed by the user.

User properties

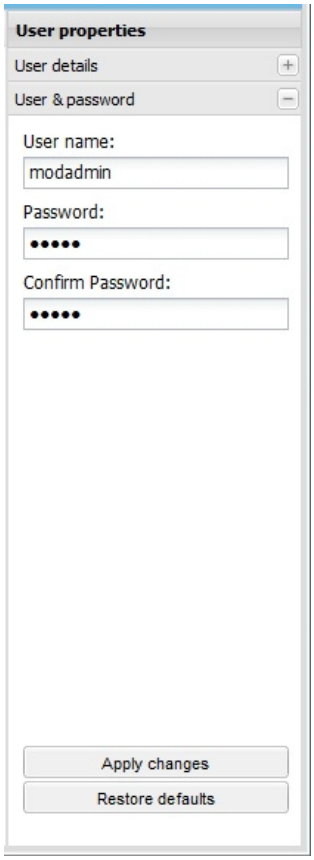
The **User properties** panel contains modifiable settings for the selected user. This panel is visible only if a user is selected from the user list. The **User properties** panel consists of two sub-panels: **User details** and **User & password**.

The **User details** sub-panel inside the **User properties** panel contains the following components:

- **Full name** text box defines the full name of the user. When you are creating a new user, the user name in the **User & password** sub-panel is generated based on the full name if you have not already modified the login name.
- **User role** drop-down list contains all the roles that can be selected for the user: See *User roles*. **Guest** is selected by default. The user cannot change his/her own role.
- **E-mail address** text box defines the email address of the user (optional).
- **Phone number** text box defines the phone number of the user (optional).
- **Language** drop-down list contains all possible languages in the UI. This defines the language used when the user logs on.
- **Comment** text box provides the administrators with an area for writing a comment on the currently selected user. The comment is not visible for the selected user (unless the user has administrator privileges).

The **User & password** sub-panel inside the **User properties** panel contains the authentication details of the user:

- **User name** text box defines the name of the user.
- **Password** text box defines the password for the user name. The password is not shown in plain text. The minimum length for a password is 2 symbols.
- **Confirm Password** text box is used for checking that the password has been typed correctly. The password is not shown in plain text.



In the lower part of the **User properties** panel there are two buttons, whose names change by the context. When you are creating a new user, there are the following buttons:

- **Create user** for saving the new user settings
- **Cancel** for canceling the creation and removing new_user (default name) from list.

When you are modifying an existing user, there are the following buttons:

- **Apply changes** for saving the modifications
- **Restore defaults** for resetting the values to a previously saved user setting.

When the new user logs on to the UI for the first time, he/she is prompted to change the password.

User roles

The user roles to be selected from the **User role** drop-down list on page *36* are the following:

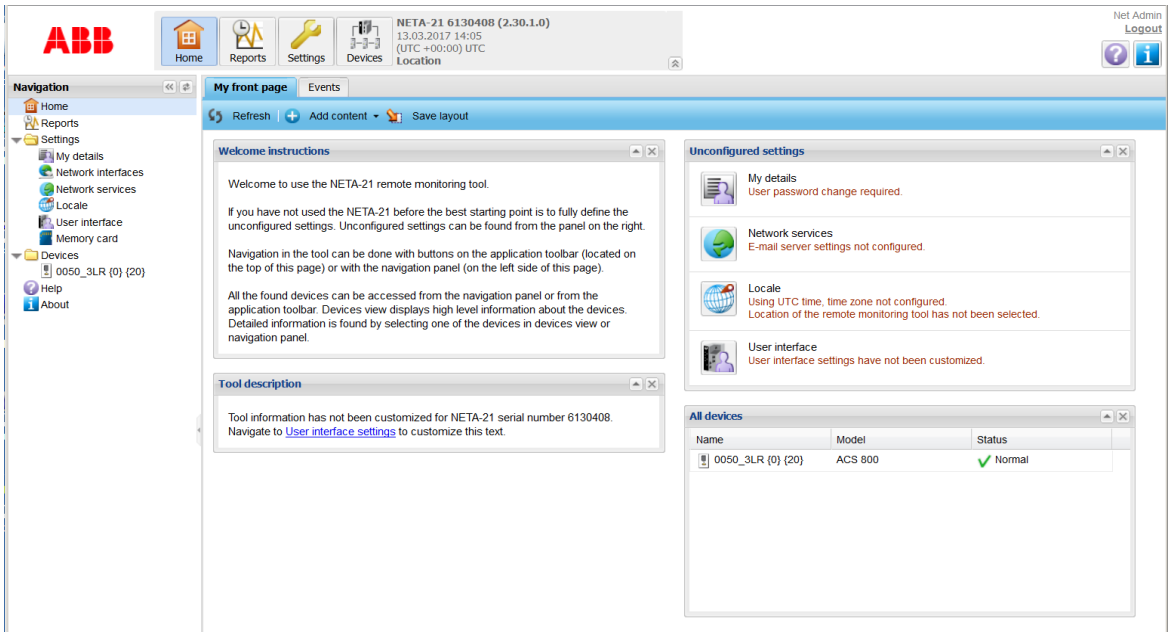
- FW admin
- Tool admin
- Network admin
- Drive expert
- User
- Guest
- FTP user account.
- External account

Tool admin

With the Tool admin role you have the full access rights to the NETA-21. In addition to the access rights listed for Drive expert and Network admin, the Tool admin role allows you to:

- add and remove NETA-21 user accounts (and modify permissions of other users)
- perform the firmware update of the NETA-21 through the SD card or PC
- back up and restore the NETA-21 firmware and NETA-21 settings to/from the SD card
- enable or disable the factory login (factory support account)
- reset the tool settings to the default settings (restore the factory settings)
- add and remove extra software packages
- change report settings.

If you log on to the UI as Tool admin, the front page appears as follows:

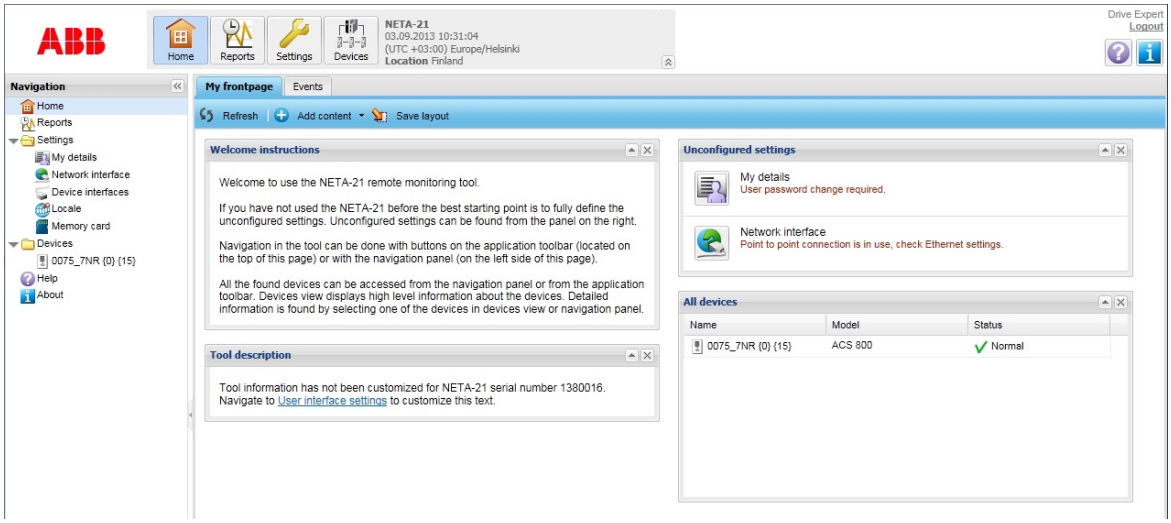


Drive expert

The Drive expert role includes the access rights of Guest and User supplemented with rights allowing you to:

- reset and rescan drives
- view network interface settings
- change locale settings
- view and change device interface settings.

If you log on to the UI as Drive expert, the front page appears as follows:



Network admin

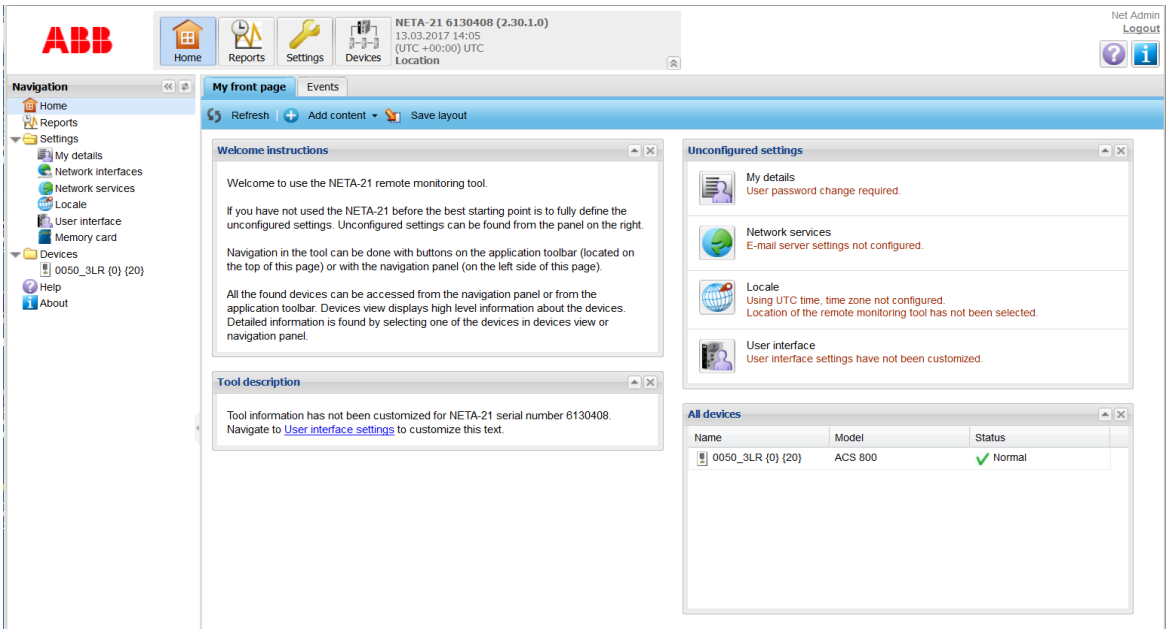
The Network admin role includes almost all the access rights of the Drive expert role plus supplemental rights allowing you to:

- change network interface settings
- view and change network service settings
- change descriptions and prompts for the UI
- change the web server session time-out
- view the memory card status and reports folder on the SD card
- monitor the IP addresses of the logged-on users through events.

As Network admin you cannot:

- view and manage user settings
- view and change NETA-21 settings
- restore settings to factory default values (software option)
- see the installed software type and version of the NETA-21
- reboot the NETA-21 (software option)
- view and change user interface settings
- back up and restore tool parameters to the internal memory or SD card
- rescan device parameters or reset an active fault
- view and change device interface settings
- write device parameters
- select parameters for trend logging
- configure and control data loggers embedded in some monitored devices
- export or import device parameters to/from a file.

If you log on to the UI as Network admin, the front page appears as follows:

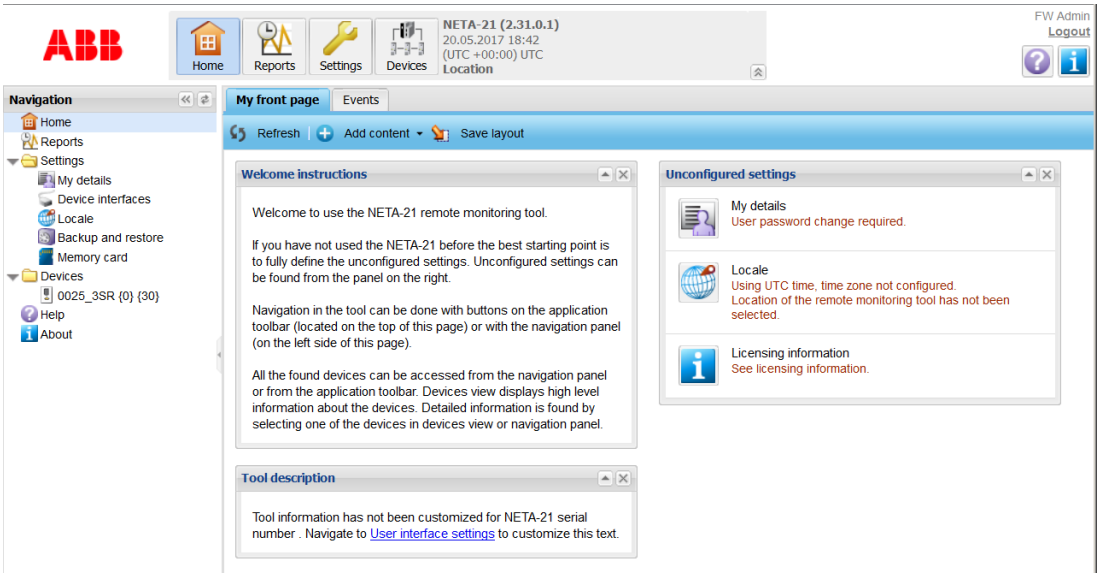


Firmware admin

The Firmware admin (FW Admin) role includes the access rights of the User role in addition with rights allowing you to:

- reset and rescan drives
- change locale settings
- view and change device interface settings
- back up and restore the NETA-21 firmware and NETA-21 settings to/from the SD card
- update the firmware of NETA-21 connected drives.

If you log on to the UI as FM Admin, the front page appears as follows:



User

With the User role you have the access rights of the Guest role supplemented with rights allowing you to:

- write drive parameters
- select parameters for trend logging
- access data logger views
- view report settings
- view locale settings
- view the memory card and its contents
- export all drive parameters to the **Events** tab and save them to a PC
- import drive parameters from the PC file to a device.

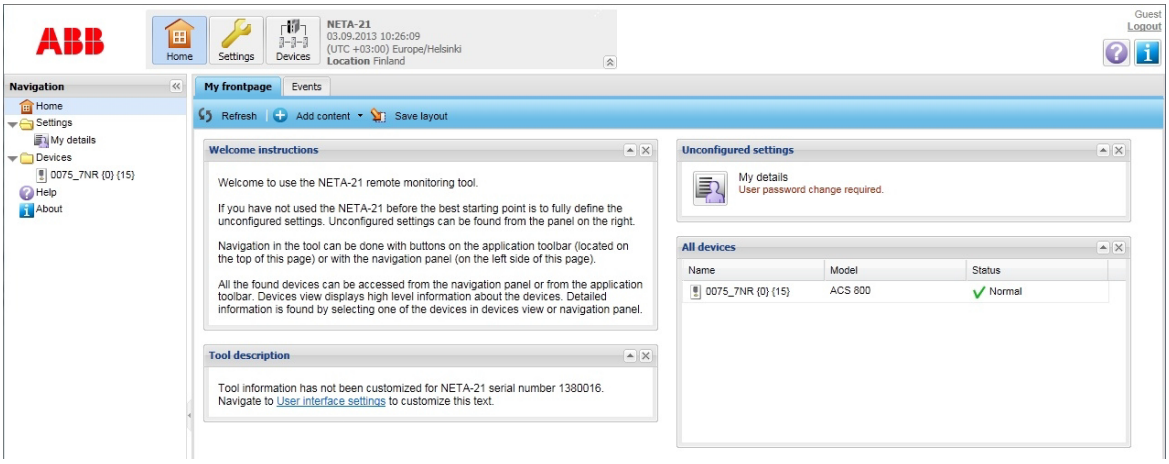
If you log on to the UI as User, the front page appears as follows:

Guest

With the Guest role you have the lowest level access rights. As Guest you can only:

- change My details settings
- view events
- read drive parameters and see the statuses of the devices.

If you log on to the UI as Guest, the front page appears as follows:



FTP user account

The FTP user account does not give access to log on to the web UI. The account can be defined to allow an FTP or FTPS access to the memory card.

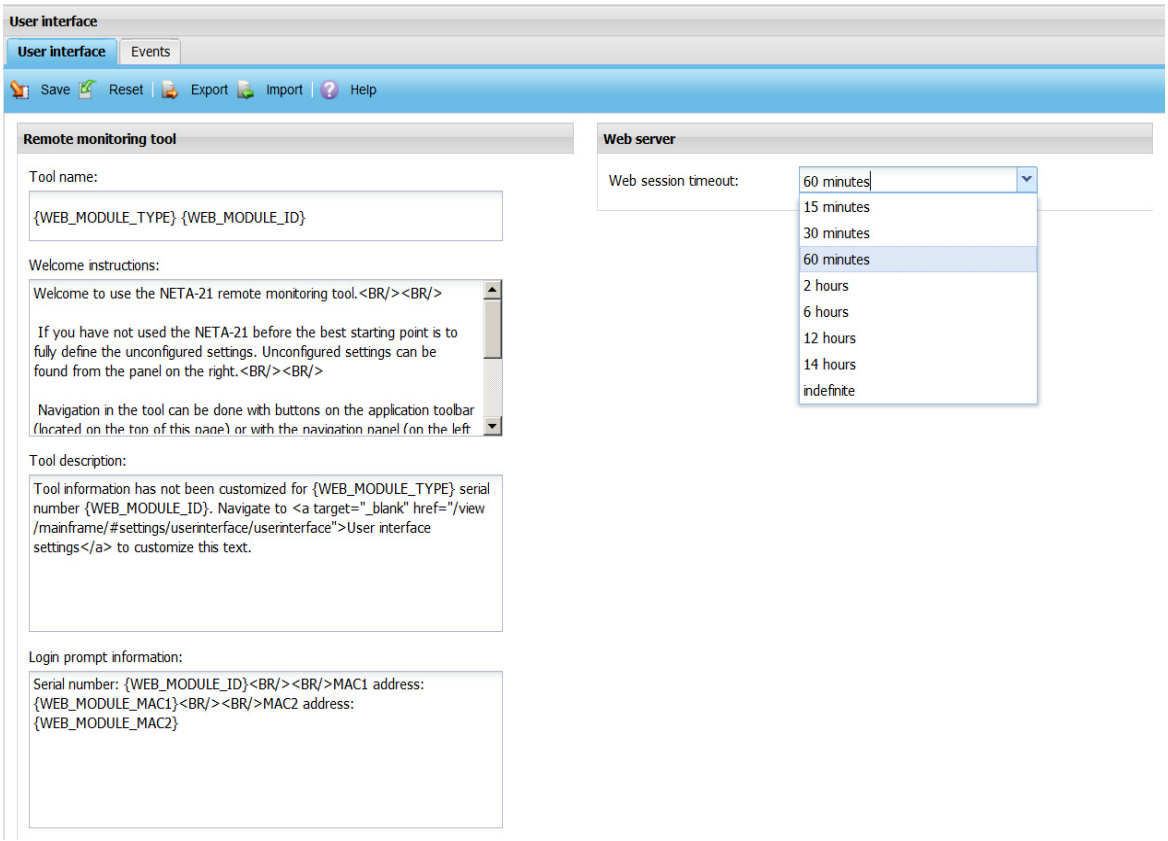
Note: The unsecured FTP protocol is disabled by default from firmware 2.22 onwards (FTPS is enabled). To enable the FTP service go to **Settings –> Network services –> Services**.

External account

For information on External account, see chapter *Security* on page *169*.

User interface

The **User interface** tab is found under **Settings**. The text boxes on the tab can contain embedded environment variables, in other words, the value of the environment variable is shown in the text. The text may contain '{VARIABLE}' where VARIABLE means the name of environment variable on the server. If text contains two braces ('{{' or '}}'), only one brace is shown in the UI.



The **User interface** tab contains the following components:

- **Save** button saves the modified settings to the NETA-21.
- **Reset** button discards all changes in the settings.
- **Export** button exports the UI settings to a local file.
- **Import** button imports the UI settings from a file to the UI.
- **Help** button opens a dialog box informing you about the embedded environment variables in the UI.
- **Tool name** text box shows the name of the NETA-21 (the default is the same as the tool type). This box may contain embedded environment variables. When you make changes in this box, the following places will be affected:
  - Web browser title shows the tool name.
  - Application toolbar shows the tool name.
- **Welcome instructions** text box contains the welcome instructions for the UI. The welcome instructions are shown on the front page after the first login. This box may contain embedded environment variables.
- **Tool description** text box contains the NETA-21 description. This text is shown on the front page after the login. This box may contain embedded environment variables.
- **Login prompt information** text box contains the information visible for all users in the login dialog box. This box may contain embedded environment variables.
- **Web session timeout** drop-down list defines the time (in minutes) when the user is logged out if there is no activity in the UI. The default value is 15 minutes. The following values can be selected:
  - 15 minutes
  - 30 minutes
  - 60 minutes
  - 2 hours
  - 6 hours
  - 12 hours
  - 14 hours
  - indefinite.

  Note: The web session expires in less than 5 minutes if the web browser is closed or the connection to the NETA-21 is lost. The **Web session timeout** setting has effect only if the web browser window is open. The time-out calculation is reset every time when the user browses around in the UI.

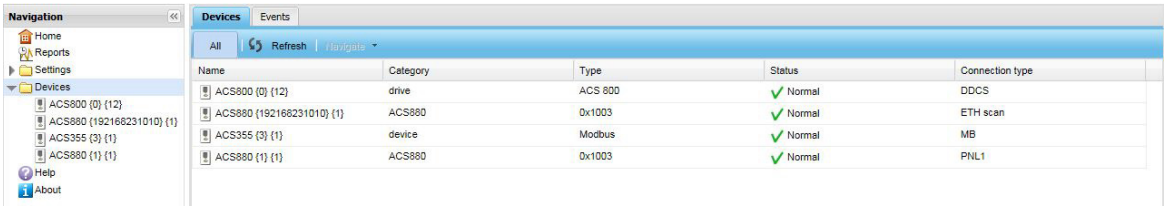
10

Devices

What this chapter contains

This chapter describes how to manage device parameters and use data loggers.

Devices tab



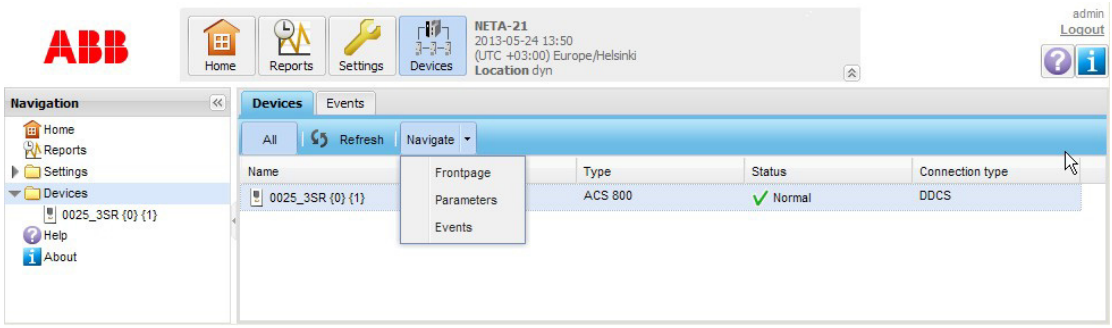
There are two tab pages under Devices:

- **Devices** tab lists all devices that are connected to the NETA-21.
- **Events** tab lists events for all detected devices.

The **Devices** tab contains the following components:

- **All** button shows all devices.
- **Refresh** button updates the device list. When the view is updated, the **Refresh** button is disabled and the icon spins indicating that the updating is in progress.

- **Navigate** button opens the front page of a selected device. This button is disabled if no device has been selected. If you click the arrow on the button and select **Parameters** or **Events**, you can go directly to the **Parameter browser** tab or the **Event** tab of the selected device.



- Device list shows all detected devices. Double-click a device to open the front page of the device. The list contains the following columns:
  - Name column contains the name and icon of the device.

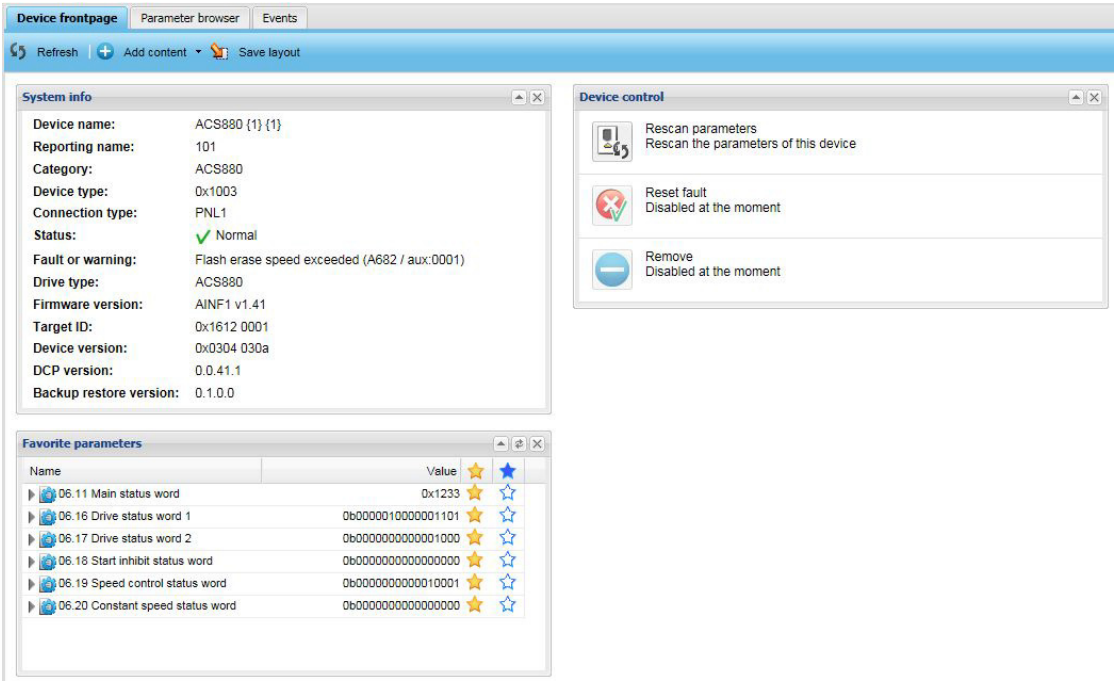
    After the device name there are two numbers in curly brackets. The first number depends on the connection type:
    0 = DDCS connection
    1 or 2 = PNL connection
    3 = Modbus connection
    Ethernet connection = IP of the device without dots.

    The second number is an ID that indicates different devices of the same connection.
  - Category column contains the category of the device.
  - Type column contains the type of the device.
  - Status column contains the connection status of the device and the corresponding icon describing the status. The status can be, for example, one of the following: Normal, Disconnected, Warning, Fault.
  - Connection type column contains the connection type of the device. The following connection types are available:
    DDCS
    ETH scan, ETH manual (Ethernet connection, either automatically scanned or manually connected)
    MB (Modbus)
    Panel bus.

Device front page

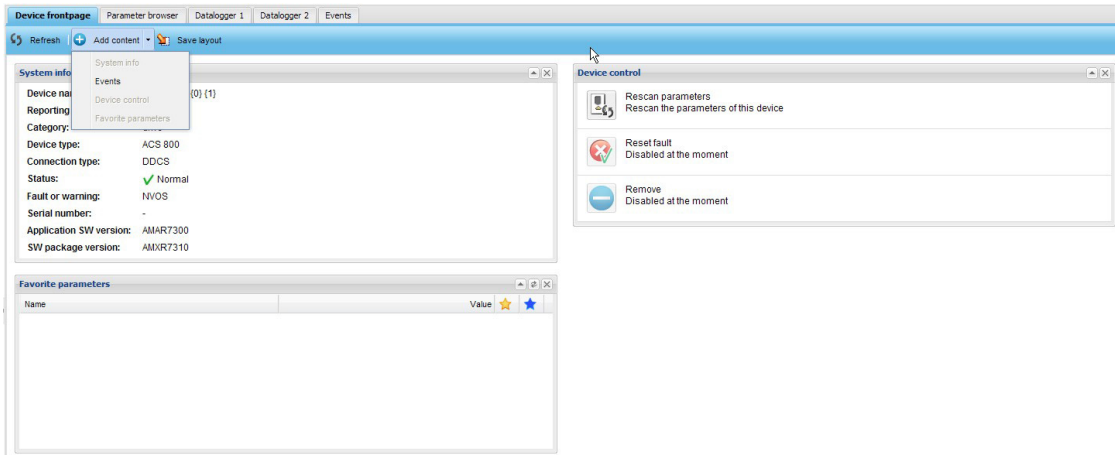
Every device has its own front page which can be customized by the administrator. Every user has the same layout. The front pages are portals where the user can move, add and remove the contents.

- Example of a device front page:



The toolbar of the front page contains the following buttons:

- **Refresh** button refreshes the contents of the view. When the view is updated, the **Refresh** button is disabled and the icon spins to indicate that the updating is in progress.
- **Add content** button adds a new portlet to the portal. If you click the arrow on the button, you get a drop-down list containing the following portlets:
  - System info
  - Device control
  - Events
  - Favorite parameters.



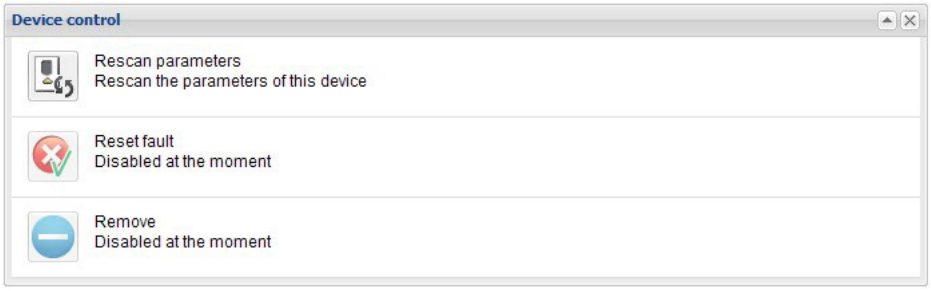
- **Save layout** button saves the layout. This button is visible only to device super users and administrators that have permissions to modify the layout.

The front page contains the following portlets:

- **System info** portlet shows read-only information about the device.
- **Device control** portlet contains means to control the device. Every option contains a title, icon and description. See section *Device control buttons*.
- **Events** portlet shows the latest events for the device. The event list contains the following columns: Name, Timestamp and Severity. The list can be sorted.
- **Favorite parameters** portlet contains the parameters that are marked with a yellow star on the **Parameter browser** tab. You can refresh the values of the parameters by clicking the **Refresh** button of the front page.

Device control buttons

There are three device control buttons in the **Device control** portlet.When you click the icon, the icon is disabled until the action has completed. If the action fails, a light-blue warning message is shown under the description. The panel may contain the following actions (the options may vary between devices):



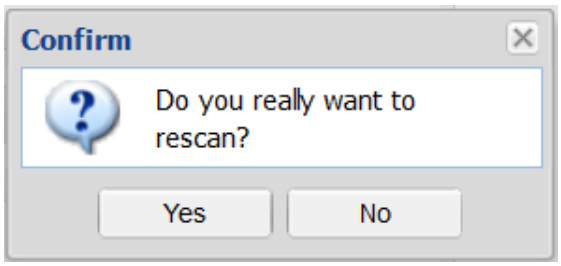
- **Rescan parameters** button

  The button is enabled when the associated drive is connected and parameter scanning is not active on any of the drives handled by the same device interface (eg, DDCS, panel bus, Ethernet, Modbus). In any other case the button is disabled.

  The automatic parameter scanning starts if all connected devices per interface (or panel port) become disconnected. Some interfaces such as Ethernet tool network may scan for nearby devices continuously in the background.

  There are situations when the parameter list of a drive and the content of the **Parameter browser** tab become unsynchronized, for example, when the parameters of a drive have been modified while it has been disconnected shortly from the NETA-21. When you reconnect the NETA-21 to the drive, use this button to resynchronize the parameters shown in the **Parameter browser** tab with the actual parameters of the drive.

  When you click the button, a dialog box appears. Click Yes to confirm rescan:



- **Reset fault** button

  The button is enabled when the associated drive is connected, there is an active fault on a drive, or when a drive has an unacknowledged fault which has already ended.

In any other case the button is disabled.

If the cause of the fault has been handled, you can reset the fault by clicking this button. If a fault condition is active or a device has a permanent fault, the fault cannot be reset via interferes.

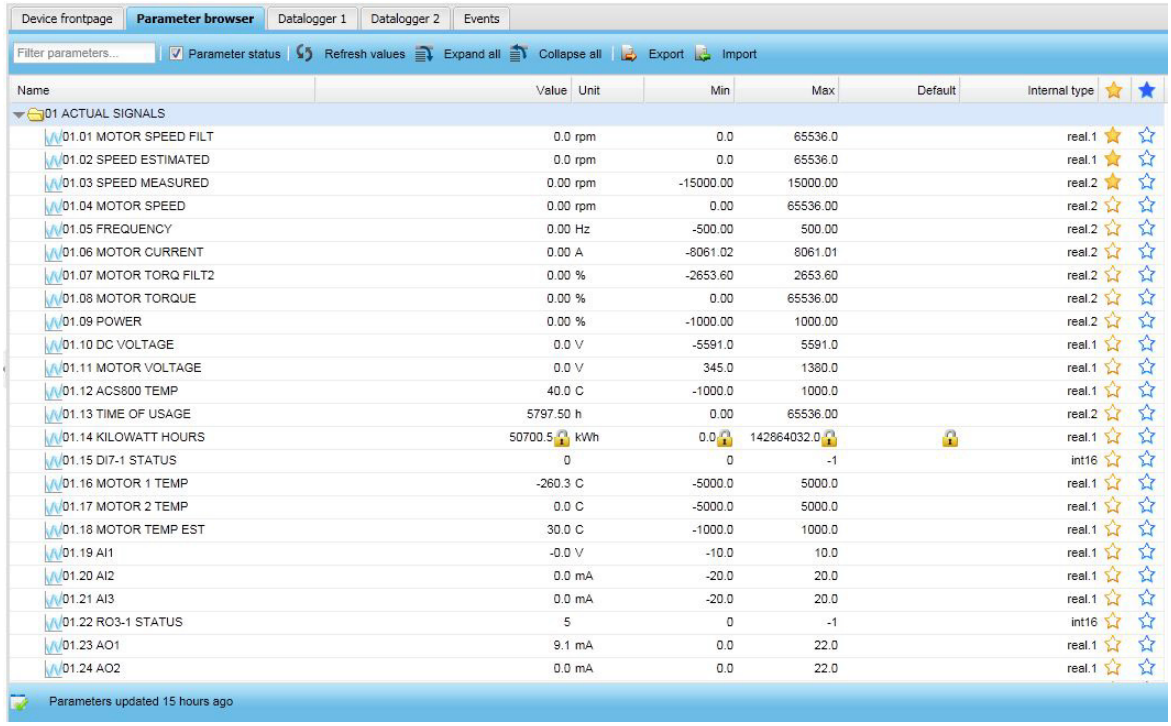
- **Remove** button

  The button is enabled when the associated drive has been disconnected from the NETA-21. Use the button to permanently delete the drive from the drive list of a device interface, for example, when the configuration of the system has changed.

  The button is disabled when the drive has been reconnected to the NETA-21.

Parameter browser

Every device has one or more parameter browser tabs that list the parameter groups and parameters of the device. You can mark favorite parameters with yellow and blue stars. Parameters marked with a yellow star are shown in the **Favorite parameters** portlet on the device front page. Parameters marked with a blue star are shown in the **Favorite parameters** portlet on the **My frontpage** tab.



The toolbar of the **Parameter browser** tab contains the following components:

- **Filter parameters…** is a text box for finding parameters from the parameter list. The parameter list is updated automatically when you type search criteria to this box.
- **Parameter status** is a check box for showing or hiding the parameter status bar of the parameter view at the bottom of the window. The status bar is visible by default.
- **Refresh values** button updates the parameter values visible in the parameter list. When the view is updated, the refresh button is disabled and the icon spins to indicate that the refreshing is in progress.

  The NETA-21 has a cached list of parameter groups and parameter names. The **Refresh values** button does not necessarily update all group names on the list, since that would take too much time. Some of the parameter data will be updated after a delay when you start browsing into the parameter groups. If it is uncertain that the parameter list is up to date or if there are strange access errors when you try to open parameter lists, the errors can be solved by reloading all device-specific data. To

reload all device-specific data, click the **Rescan parameters** control button on the device front page.

- **Expand all** button shows all parameters of all groups.
- **Collapse all** button hides all parameters and shows only the group list.
- **Export** button exports parameters to a file.
- **Import** button imports parameters to the device.

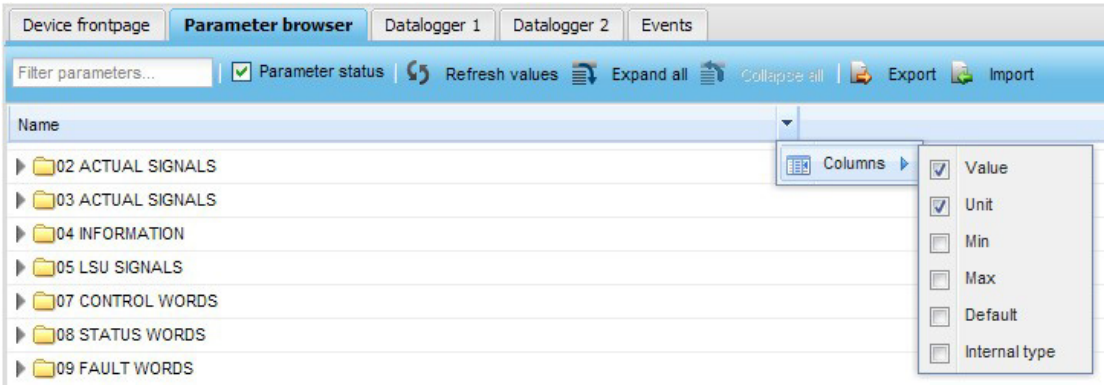
The status bar provides the following information:

- Parameters updated field shows how much time has gone since the parameter structures have been updated from the device to the NETA-21. The NETA-21 keeps a cached list of parameter structures, and someone else (a local user with a control panel, a PC tool user, or the monitored device itself) may have changed parameters after the last update. The elapsed time is shown as follows:
  - Parameters updated X days ago
  - Parameters updated X hours ago
  - Parameters updated X minutes ago
- On-going operation field shows what the device is currently doing. The operation is indicated with an icon and, for example, the following texts:
  - Parameter list is up to date
  - Refreshing parameters
  - Device is disconnected
  - Device is offline.

The parameter list is not sortable. The list contains the following columns:

- Name column shows the name of a parameter.
- Value column shows the value of a parameter. For parameters that have a decimal value, the value is shown in the hex, decimal or binary format depending on the selection made in the **Parameter properties** panel.
- Minimum, maximum and default value columns are hidden by default.

  To add columns, click the arrow on the right-hand side of an existing column:



- Unit column shows the unit of the parameter value. This field may be empty for some parameters.
- Internal type shows the data type of the parameter, either a device-specific type (eg, float2 for a float number with two decimals) or a generic type (eg, "number" or "string").

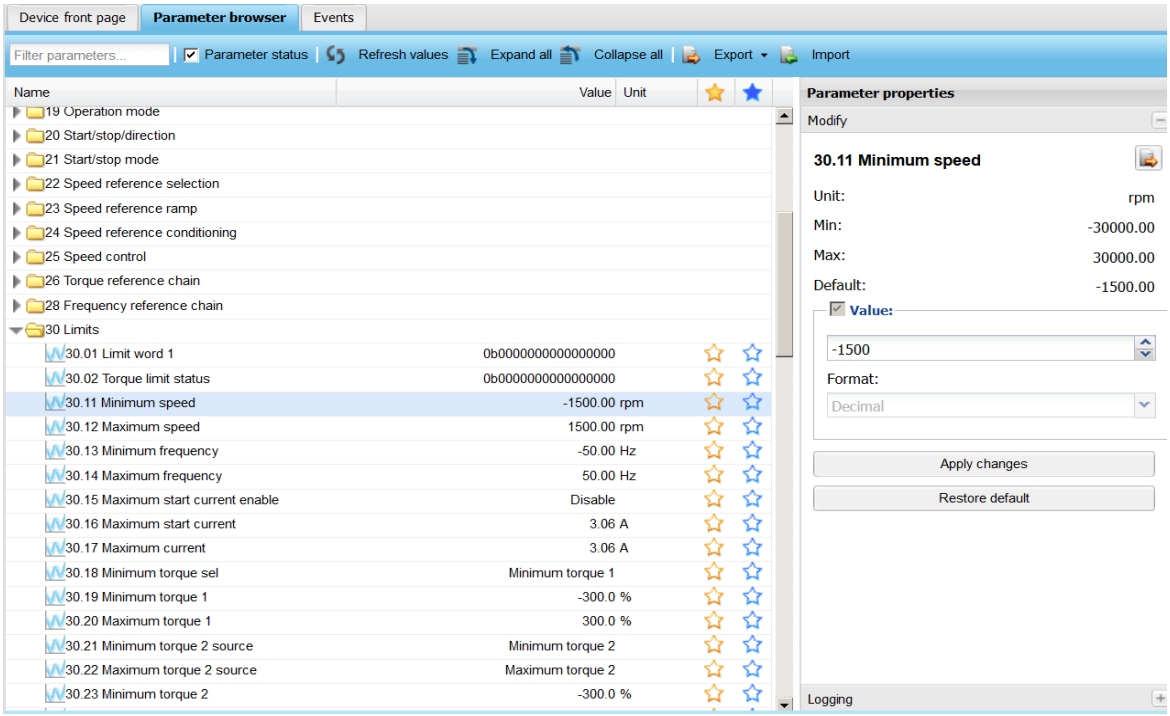
When you select a parameter from the list, an edit panel titled Parameter properties appears in the right-hand side of the tab.

Parameter properties

Open the **Parameter properties** panel by clicking a parameter in the Name column. The panel has two sub-panels that are visible one at a time.

- **Modify** panel has controls to modify the parameter value.
- **Logging** panel contains logging-specific settings and lists.

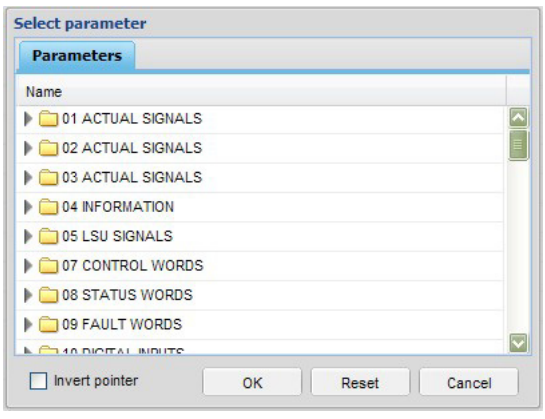
With the **Modify** sub-panel you can modify the parameter value.



The **Modify** sub-panel contains the following components:

- **Value** check box: There can be two value boxes to choose from depending on the data type of the parameter. If there are two value boxes, only one of them can be selected at a time, and the other is collapsed.

  The box may be a spin box, check box grid, drop-down list, text editor or a parameter selection control (parameter pointer or bit pointer). If there is the **Parameter** check box, click the list to open a pop-up window where you can choose a parameter or the bit of a parameter value.



Spin-boxes use the minimum and maximum value limits received from the device. You cannot type the value.

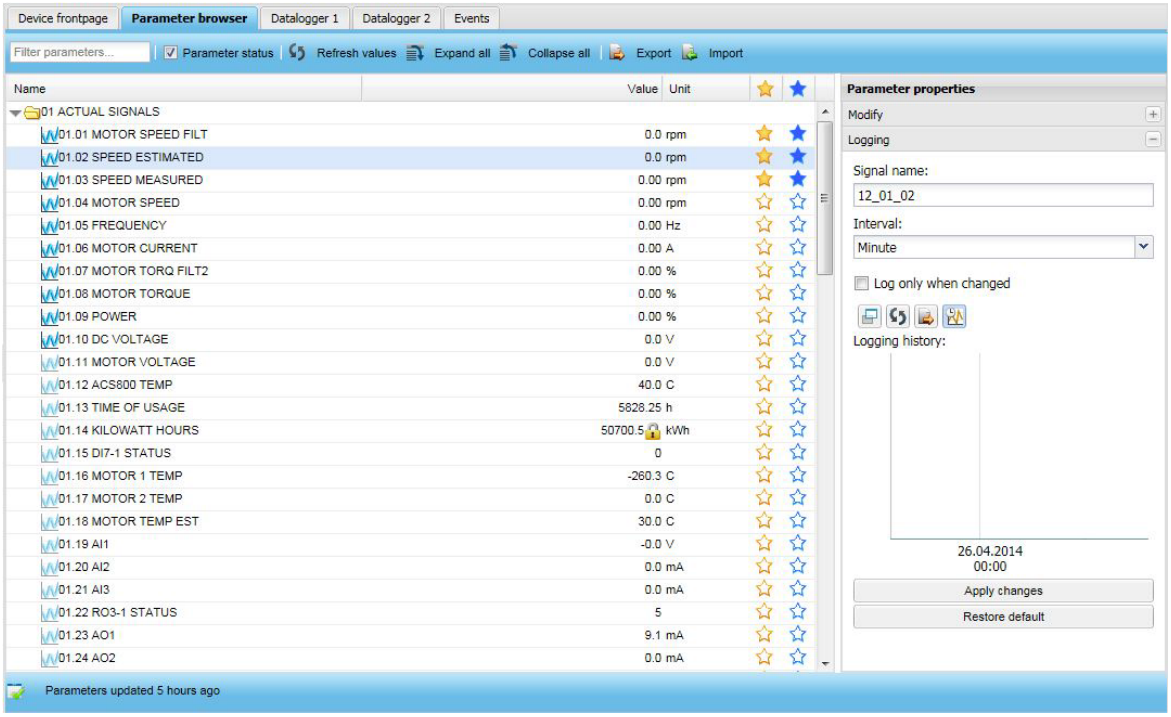
- **Format** is a drop-down list for specifying the format of a parameter value. The format can be **Decimal**, **Hex** or **Binary**.
- **Export** button exports the parameter in a text-based file.
- **Apply changes** button saves the parameter changes to the device.

  The icon of the **Refresh** button is spinning while the changes are applied to the NETA-21.
- **Restore defaults** button asks the device to restore the default value to a parameter. This button is disabled if the parameter has no default value.

Notes:

- You cannot modify the value or format of read-only parameters.
- Read-protected parameters cannot be read and appear as an empty value field.

The **Logging** sub-panel contains logging-specific settings and lists:



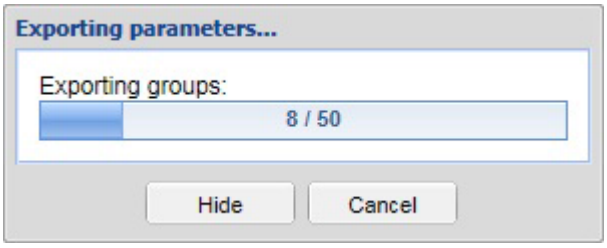
The **Logging** sub-panel contains the following components:

- **Signal name** defines the name of the parameter that is used in reporting and trend logging. The default name depends of the style selected in **Reports –> Settings –> Signal names –> Settings –> Default signal name**. You can restore the default signal name with the **Restore default** button or by storing an empty signal name.
- **Interval** drop-down list is used for selecting the logging interval for the current parameter. You can select from the following values: Minute, 5 Minutes, Hour, Day, None or Continuous monitor. To save the value, click the **Apply changes** button.
- **Log only when changed** check box is used for selecting values to be logged only when the parameter value changes. If this check box is not selected, the parameter value is logged at every interval.

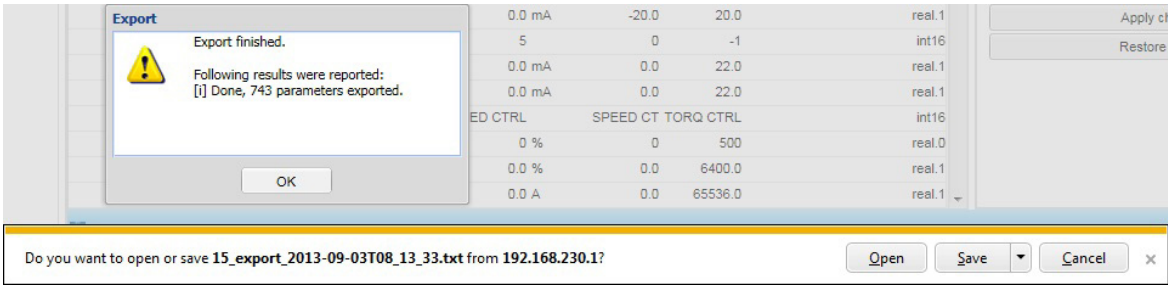
- **Open parameter logging history in a new tab** button
- **Refresh** button updates the log list/chart if new values have been logged.
- **Export the event attachment** button creates a log report file to be exported.
- **Toggle between chart and list view** button changes the view in which the logged values are displayed.
- **Logging history** shows all the logged values for the parameter in the current segment.
- **Apply changes** button saves the parameter log changes.
- **Restore default** button replaces all changes in the settings with default values.

Export of parameters

When you click the **Export** button in the toolbar the following progress pop-up window appears:



The progress pop-up window has a **Cancel** button which stops the exporting process. With the **Hide** button you can hide the exporting pop-up window. The pop-up window is shown again when you click the **Export** button.

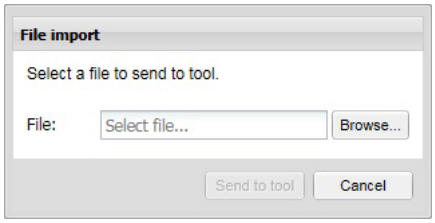


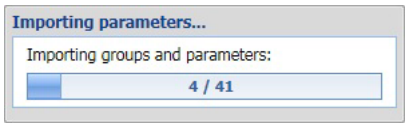
Note: Only one parameter export can be ongoing at a time. If another user has started a parameter export before you started a new export, your export may fail. In addition, you cannot start an export, if drive parameters are being scanned in background.

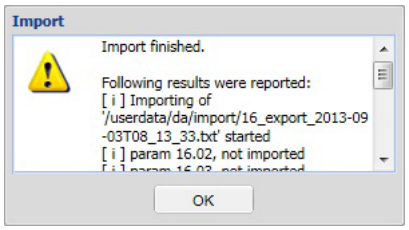
Note: The parameter export format depends on the device type and device interface. The parameter export is not available for all device interfaces.

Import of parameters

When you click the **Import** button you are asked for an import file.







The file is sent to the NETA-21 and the progress dialog box is shown. The NETA-21 supports the NETA-21, NETA-01 and DriveWindow parameter export files for importing.

Note: The format of the parameter import file is compatible with the NETA-21 parameter export files, NETA-01 parameter export files and DriveWindow 2.x parameter export .txt files (but not with DriveWindow parameter .dwp save files).

Make sure that you import/export parameters only between identical drives and device software versions.

It may be necessary to power cycle the drive and reload the device interface in the NETA-21 to see all effects of parameter changes, especially if monitored devices change their device interface node ID.

Note: The parameter import does not open a parameter lock or handle all dependencies between parameters. Sometimes it helps when you import a parameter file multiple times.

Note: For the ACS800 firmware, the parameter import restores ID run parameters if those are included in the parameter file. In addition, only visible parameters are restored.

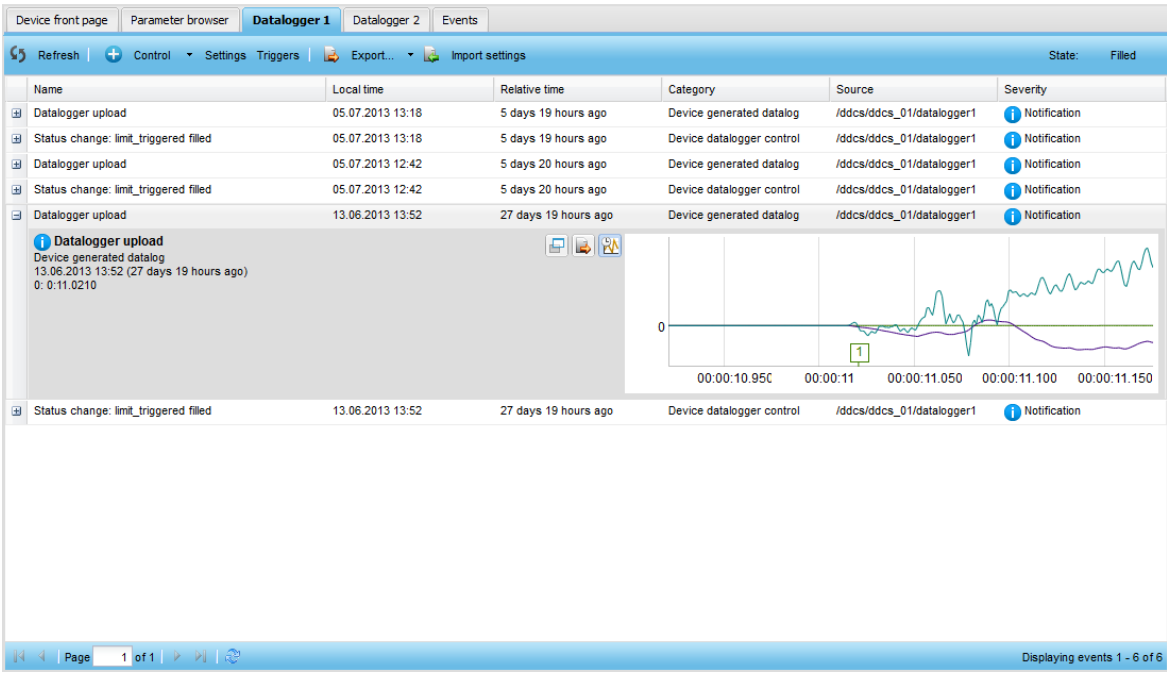
WARNING! Make sure that you can start the drive safely before using the parameter import function. Imported parameter settings must to be compatible with the specific drive. When you import specific parameter configurations you can cause the drive to start during or after the parameter import. (Control words or signals in groups <10 are not written to a drive during the parameter import).

Device data logger

Data logger

The drives connected through a DDCS protocol have a data logger or data loggers that can record data from various signals of the drive when there is no external logging mechanism active. This can be used for troubleshooting or diagnostics. Data collecting can be stopped by either a specific stop command or automatically by a triggering condition becoming true in the drive. After the data collecting has been stopped, the collected data can be read and studied.

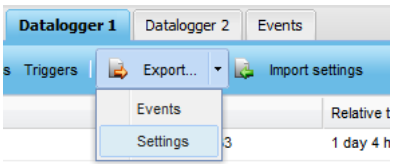
The data logger tabs contains all uploaded data logs from the drive. One drive can have multiple data loggers configured. All data loggers have an identical user interface.



The data logger tabs contain the following components:

- **Refresh** button refreshes the data logger view.
- **Control** button is a menu button that can be used to control the data logger with the following actions:
  - Start - starts the data logger.
  - Stop - stops the data logger.
  - Reset - restarts the data logger.
  - Trigger - triggers the data logger manually.
- **Settings** toggle button shows the data logger settings in the editor panel.

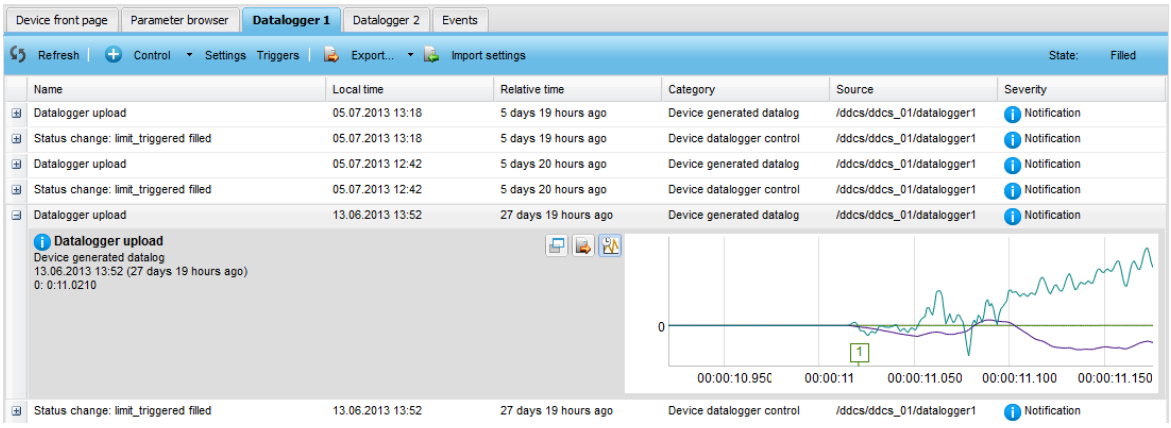
- **Triggers** toggle button shows the data logger trigger settings in the editor panel.
- **Export…** button shows a drop-down list of two options: **Events** and **Settings**.



  - **Events** option exports all collected recent data log files to a compressed .zip file that can be opened with a PC.
  - **Settings** option exports the currently opened data logger Settings and Triggers panel configurations to a file that can be loaded to a PC.
- **Import settings** button allows you to import the previously saved data logger settings and triggers from a file on a PC to a data logger in a monitored device.
- **State** defines the current state of the data logger with the following states:
  - Not initialized
  - Stopped – the data logger is not running/collecting data.
  - Started – the data logger is running/collecting data.
  - Filled – data logger upload is complete and data logger is not running/collecting data.

  The State is updated automatically every couple of seconds.

The Datalogger tabs show all uploaded data logs from the drive.



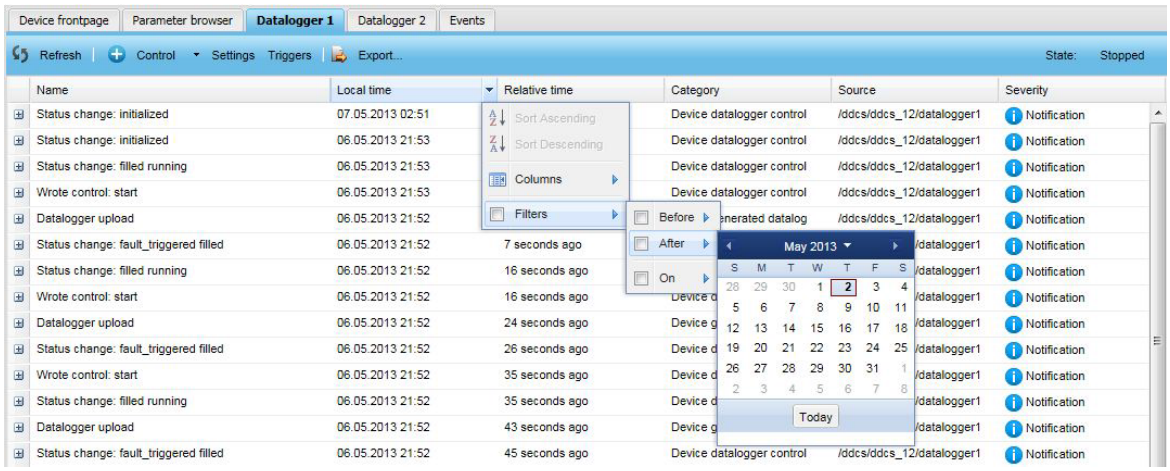
You can see the content of an entry by double-clicking the entry in the data logger list or by clicking the plus sign beside it. You can close the content of an entry by double-clicking the open entry in the data logger list or by clicking the minus sign.

The tabs contain the following columns:

- **Name** column shows the event name.
- **Local time** column shows when the event occurred. You can use the following filters **Before**, **After** or **On**.
- **Relative time** column shows how much time has passed since the event occurred.
- **Category** column defines whether the event contains a device-produced data log file (category: device generated datalog) or whether the event indicates a change in a data logger state (category: device datalogger control).

- **Source** column shows the source of the event. You can filter this field with a free text box.
- **Severity** column defines the severity (or type) of the event (Detail, Notification, Warning, Fault, Severe). You can filter this field to show only the wanted event types.

The columns can be sorted, hidden or filtered by clicking the header arrow, which appears when the cursor is over the header.



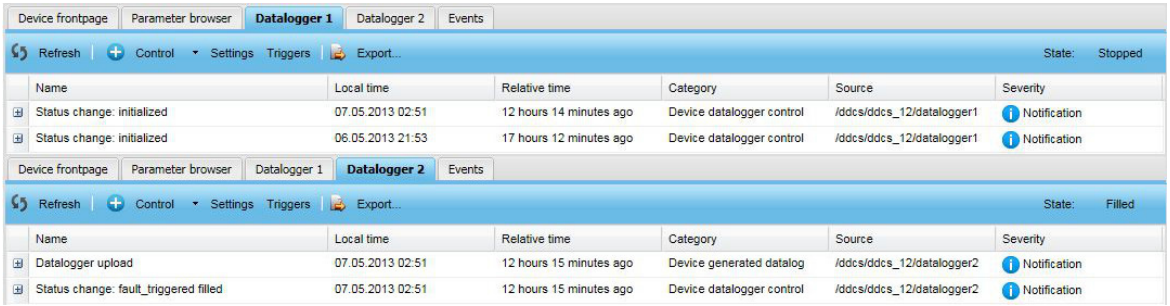
The data logger records data before and after the triggering event, depending on its settings.

For more information on the functionality of data loggers, see the drive-specific firmware manual.

Opening a data logger

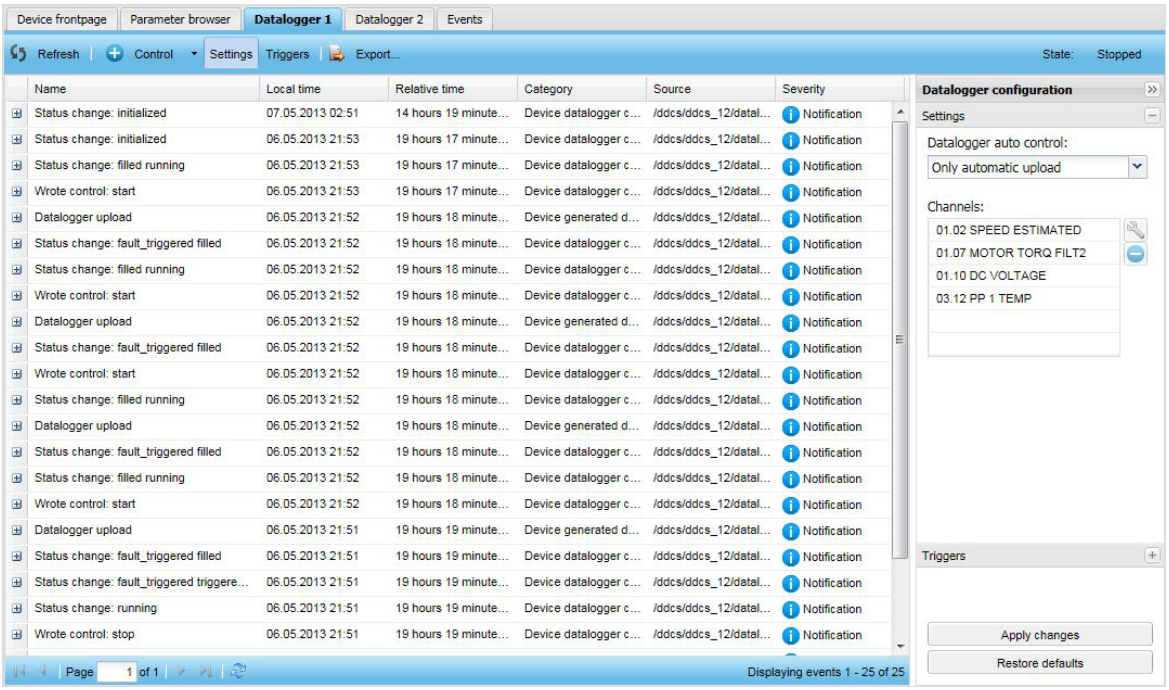
1. Log on as a user with roles other than Guest or Net Admin.
2. Click **Devices**.
3. Select the device to be monitored with a data logger.

   Note: All monitored devices do not provide data loggers. Data loggers are supported if there is one Datalogger tab or more Datalogger tabs on the device-specific page.
4. Click the **Datalogger 1** or **Datalogger 2** tab to view the system data logs.



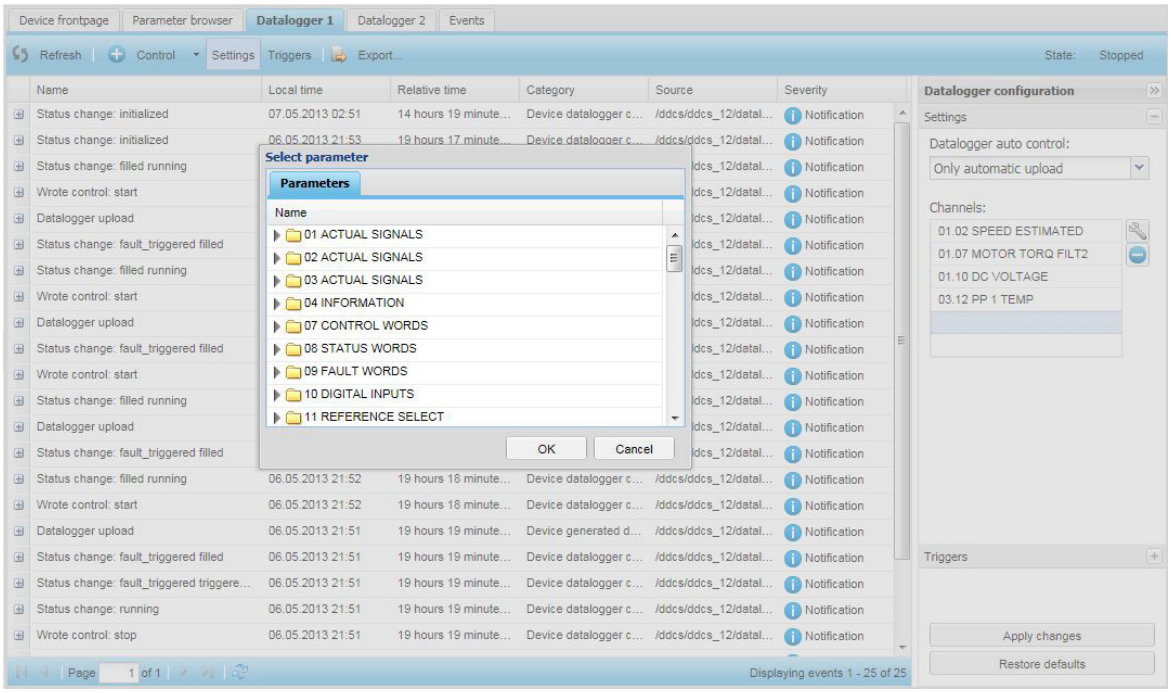
Setting up a data logger

1. Open **Datalogger 1** or **Datalogger 2** (see above).
2. Click the **Settings** button to open the **Settings** sub-panel of the **Datalogger configuration** panel in the right-hand side of the tab.

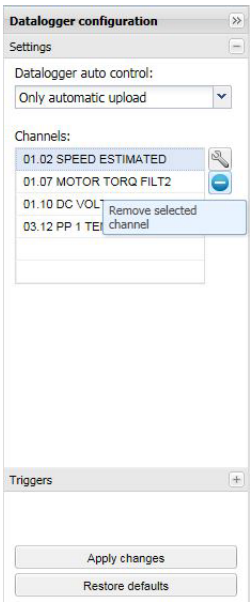


3. From the **Datalogger auto control** drop-down list select **Only automatic upload** (data logger stops after it has finished collecting data) or **Keep continuously running** (data logger is started whenever the logger is initialized or filled, even if the logger was not initially running).
4. In the Channels box click the parameter you want to add and then click the **Change selected channel** icon.
5. In the pop-up window select the new parameter you want to add to the list and click **OK**.

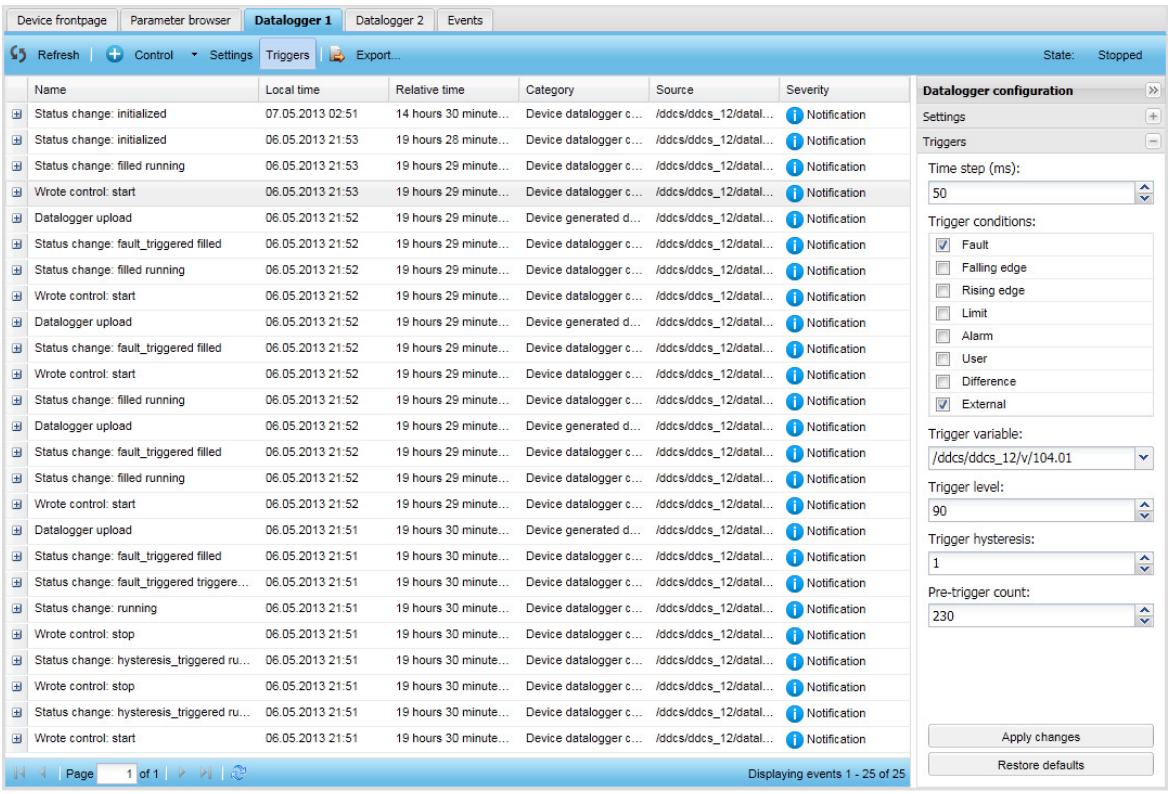
To leave the Channel box as it is, click **Cancel**.



6. Remove the unnecessary monitoring parameters by selecting them and clicking the **Remove selected channel** icon.



7. Open the **Triggers** sub-panel.

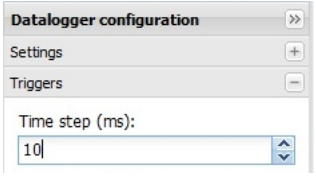


In this panel you can adjust:

- **Time step (ms):** sampling rate of the data logger in the device.
- **Trigger conditions:** multiple choices depending on the monitored device.
  Note: Configuring the “External” trigger condition to any of the dataloggers cause triggering of other loggers too.
- **Trigger variable** (parameter selection), **Trigger level** and **Trigger hysteresis**, if the selected trigger condition requires the values. For example, a limit check requires that the parameter and trigger level limit are specified.
- **Pre-trigger count**: number of the samples recorded in each data log before the triggered event occurred.

Note: The number of available ranges and trigger options vary depending on the monitored device. If the selected settings are not accepted by the monitored device when you click the **Apply changes** button, the UI restores the original settings from the monitored device to the **Triggers** panel.

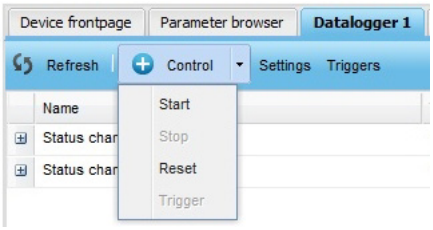
8. From the **Time step** spin box select the time interval (in milliseconds) between data readings.



9. From the **Trigger conditions** list select what device conditions will trigger the data logger to send in the collected data.

   An additional parameter value set in **Trigger variable** can be used to trigger the data logger. Use the **Trigger hysteresis** spin box to set the signal value hysteresis.

10. In the **Pre-trigger count** spin box select the number of data entries that will predate the trigger event.
11. Click **Apply changes**.
12. Click **Control** and select **Start** to start the data logger or change the **Only automatic upload** mode to the **Keep continuously running** mode in the **Settings** panel.



The State changes to Started indicating that data logger is running.

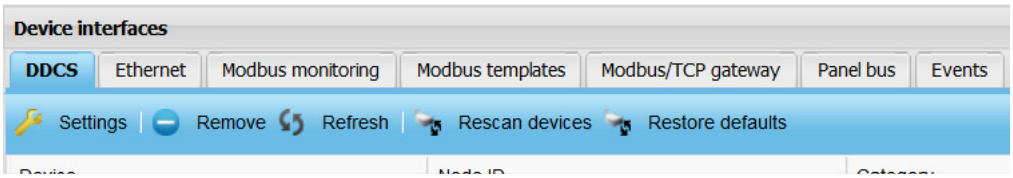
Device interface settings

Device interfaces

The Device interfaces view is meant for device expert users who want to configure the access to the monitored devices in fine detail. Device interface specific settings lets you configure communication parameters as well as fine tune device specific settings.

Normally the NETA-21 configures device interfaces automatically and auto-discovers connected monitored devices. Sometimes it is necessary to rebuild the device interface to refresh the list of monitored devices. Devices in the selected interface are presented in a generic fashion since new interfaces can be added to this view dynamically as new device interfaces.

Every connection type has its own tab.



Note: The selection of available device interfaces depends on the installed firmware version and extra packages.

The toolbars of the tabs differ but all of them have the following buttons:

- **Settings** button opens an *Interface settings* dialog box that contains settings for the selected device interface. The settings vary for every interface.
- **Refresh** button refreshes the device list in the current interface.
- **Rescan devices** button rescans a specific device interface to add/remove devices. This button is not available for every device interface. The rescanning of devices is run in the background for every device interface while no devices are connected, or when all connected devices become disconnected. Some interfaces such as Ethernet may be able to rescan for added devices in the background continuously.
- **Restore defaults** button restores the default values for settings and re-initiates the scanning of devices within the selected interface. Previously connected devices may be lost.

The device list on each tab has the following columns:

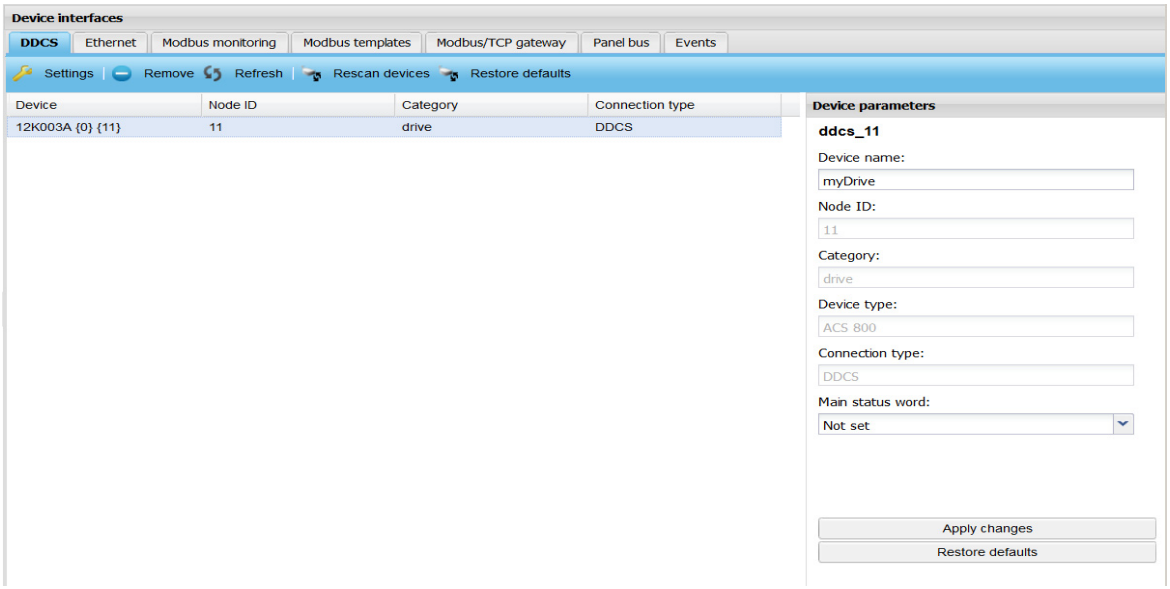
- **Device** column shows the name of device.
- **Node ID** column shows the node ID of the device interface.
- **Category** column shows the category of the device.
- **Connection type** column shows the connection type of the device.

When you select a device from the list, the Device parameters panel appears in the right-hand side of the tab. The content of the Device parameters panel is specific for each connection type, but the following components can be found in all of them:

- **Device name** box sets a custom name for the device.
- **Apply changes** button saves the modified device settings.
- **Restore defaults** button discards the changes made before the **Apply changes** command was given.

DDCS tab

The **DDCS** tab contains all the devices which use the DDCS protocol and which are connected to the NETA-21 through fiber cables (via the NEXA-21).

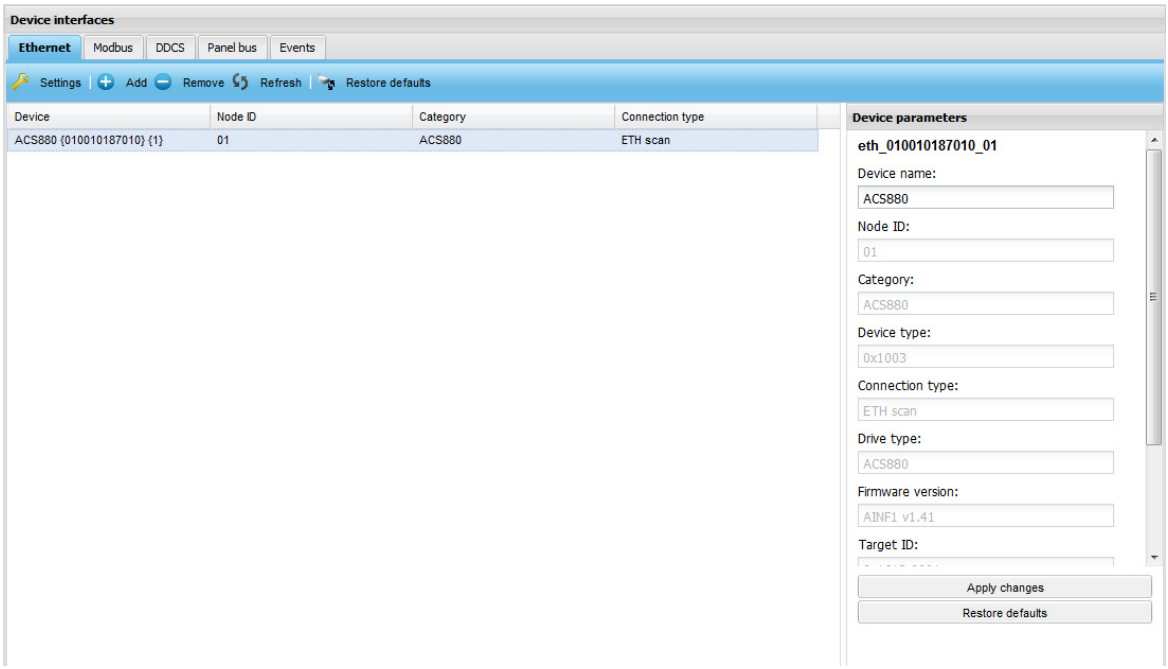


Click a device in the list to open the **Device parameters** panel where you can change the value of the Main status word to **Not set**, **Dataset 2** or **Dataset 11**.

Note: The Main status word dataset is normally auto-detected during the device detection. If a wrong value is selected, the device fault and warning statuses are not indicated correctly.

Ethernet tab

The **Ethernet** tab contains all the devices that the NETA-21 finds in its Ethernet tool network.



Note: If there is an ACS880 or ACS860 drive equipped with a FENA-11/21 adapter module in the Ethernet network, the NETA-21 and the Drive composer PC tool cannot access the FENA-11/21 at the same time. The FENA-11/21 can have only one PC tool connection at a time. The FENA-11/21 connection can be released for a PC tool by removing the specific Ethernet device from the NETA-21 device interfaces view (or by clicking the **Remove** button on a specific Ethernet device front page).

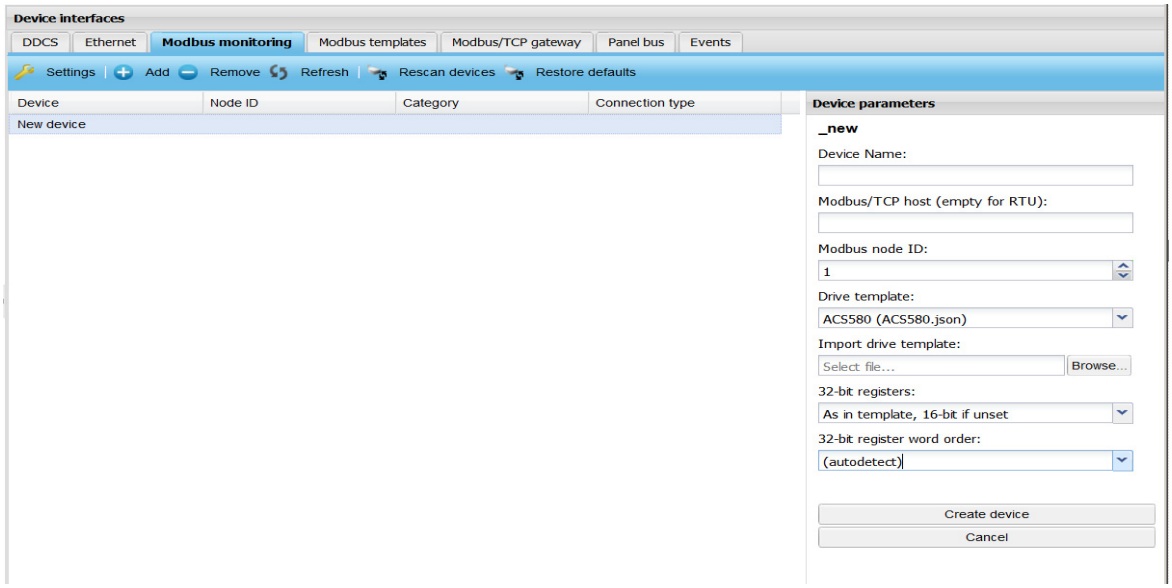
The toolbar of the **ETH** tab contains the following two extra buttons:

- **Add** button allows you to add a device to the list by specifying its IP address.
- **Remove** button removes the selected device from the list.

By default, the NETA-21 discovers devices automatically via the Ethernet tool communication connected to port ETH2. To modify the background scan settings click the **Settings** button.

Modbus monitoring tab

The **Modbus monitoring** tab contains all the devices which use the Modbus/RTU protocol and which are connected to the NETA-21 through serial port.



The toolbar of the **Modbus monitoring** tab contains the following extra buttons:

- **Add** button allows you to add a device to the list by specifying the following properties:
  - **Device Name** is a text box for the custom name of the device.
  - **Modbus/TCP host (empty for RTU)** is a text box for the IP address of the Modbus/TCP host. No value should be provided when the used protocol is Modbus/RTU.
  - **Modbus node ID** is a spin box for the node ID configured in the monitored device.
  - **Drive template** is a drop-down list for the template to be used with this device. A template is a file provided by ABB that is stored under the "template" folder in the SD card or internal memory. The template selection provides also a list of other connected drives. You can clone parameters from another device (eg, a DDCS or Panel bus connected device) into a Modbus device.
  - **Import drive template** contains the name of the imported active template. Click the Browse button to select a file.
  - **32-bit registers** is drop-down list for selecting 16-bit or 32-bit values of parameters. There are three options:

    As in template, 16-bit if unset
    As in template, 32-bit if unset
    Force all values to 32-bit
  - **32-bit register word order** is a drop-down list for selecting the most or least significant word order for 32-bit values. There are three options:

    Autodetect

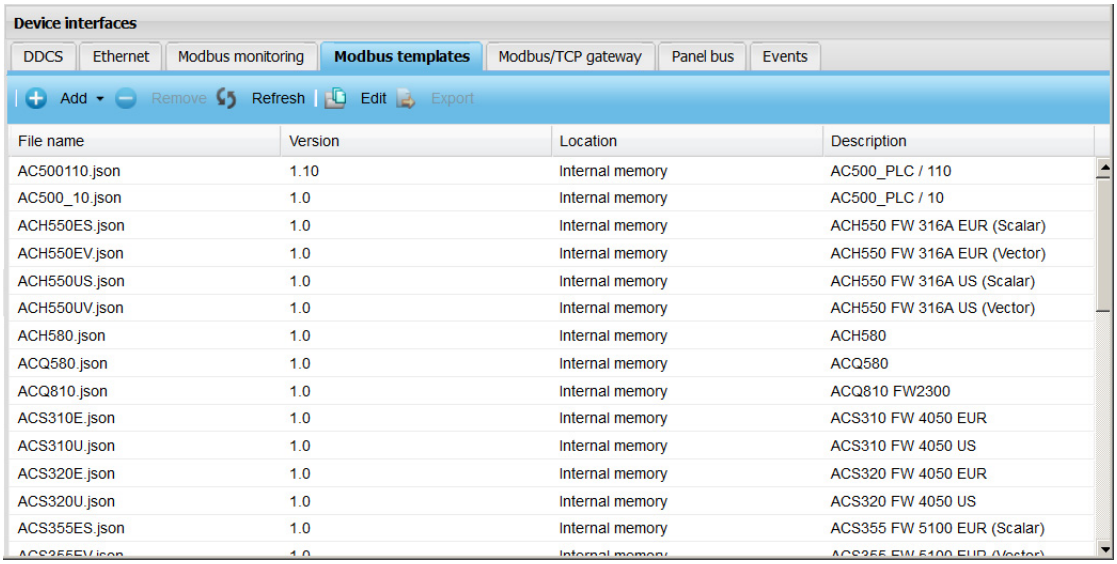
    High-low
    Low-high
- **Remove** button removes the selected device from list.
- **Rescan devices** button performs a rescan that searches for all Modbus-connected devices.

Note: The Modbus/RTU rescan uses a selected communication speed (defined in the **Interface Settings** dialog box). The rescan runs continuously in the background if all devices are disconnected.

Click a device in the list to open the **Device parameters** panel where you can change the Modbus node ID and the 32-bit register word order.

Modbus templates tab

The Modbus templates tab lists all the available templates from the internal memory and the SD card of NETA-21.



File name	Version	Location	Description
AC500110.json	1.10	Internal memory	AC500_PLC / 110
AC500_10.json	1.0	Internal memory	AC500_PLC / 10
ACH550ES.json	1.0	Internal memory	ACH550 FW 316A EUR (Scalar)
ACH550EV.json	1.0	Internal memory	ACH550 FW 316A EUR (Vector)
ACH550US.json	1.0	Internal memory	ACH550 FW 316A US (Scalar)
ACH550UV.json	1.0	Internal memory	ACH550 FW 316A US (Vector)
ACH580.json	1.0	Internal memory	ACH580
ACQ580.json	1.0	Internal memory	ACQ580
ACQ810.json	1.0	Internal memory	ACQ810 FW2300
ACS310E.json	1.0	Internal memory	ACS310 FW 4050 EUR
ACS310U.json	1.0	Internal memory	ACS310 FW 4050 US
ACS320E.json	1.0	Internal memory	ACS320 FW 4050 EUR
ACS320U.json	1.0	Internal memory	ACS320 FW 4050 US
ACS355ES.json	1.0	Internal memory	ACS355 FW 5100 EUR (Scalar)

The tool bar of the Modbus templates tab has the following buttons:

- **Add** button allows you to add more templates. You can either import a template or can clone the parameters of a connected device. See, *Add Modbus templates*.
- **Remove** button allows you to remove a template from the list of available templates and from the SD card. Only user defined templates can be removed.
- **Refresh** button updates the list of templates. This is performed after addition or removal of a template.
- **Edit** button displays the Modus Template Editor dialog box and allows you to edit the template. Before editing, templates stored in the internal memory will be saved to the SD card. See *Edit Modbus templates*.

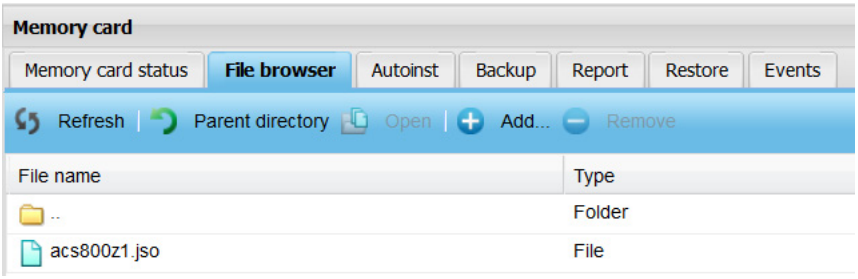
Add Modbus templates

To add new Modbus templates, perform the following:

1. Open the template directory.

   Note: Create the template directory if the template directory does not exist.

2. Click the Add button and select the template file to be uploaded. To add the template directly, copy the templates to the template directory.

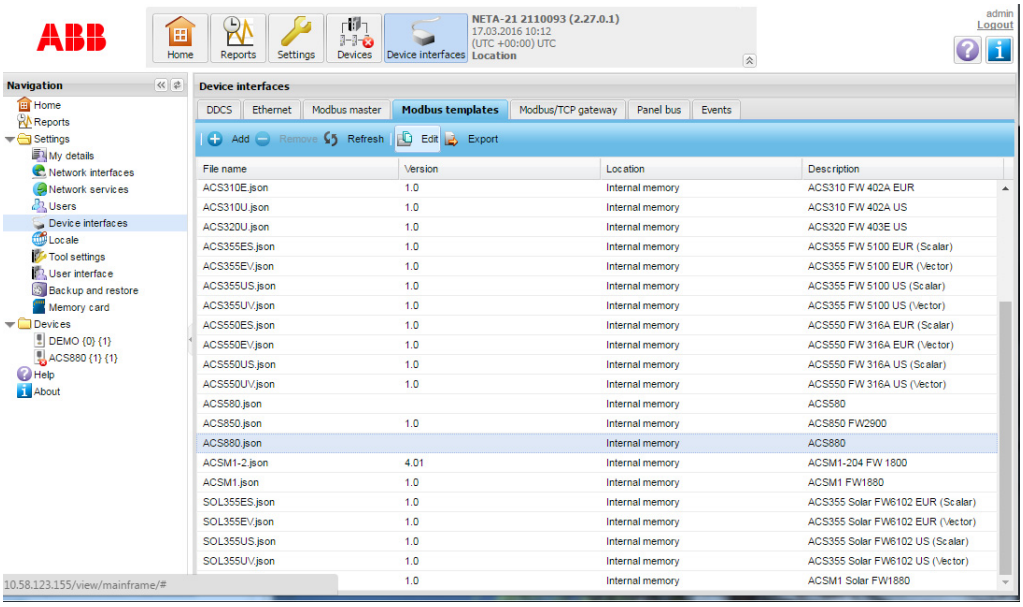


Note: The template names should be in 8.3 format. The maximum file name length is 8 characters and the maximum file extension length is 3 characters. This is due to the SD card's file system limitation.

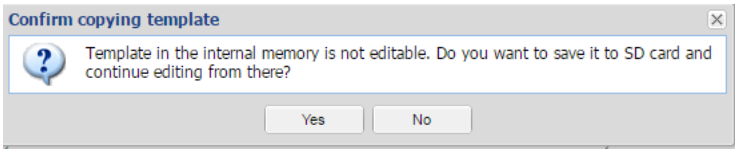
Edit Modbus templates

You can edit an existing Modbus templates or can add and edit a copy of existing default template. To edit an existing Modbus template, perform the following:

1. From the NETA-21 UI, go to **Settings -> Device interfaces -> Modbus templates** tab.
2. Select the template to be edited and click **Edit**. A Modbus template Editor dialog box is displayed.
   To edit a new template based on an existing default template, click **Export** and copy the existing template to PC. Rename the file and **Add** (see *Add Modbus templates*) it to the template directory as a new template.



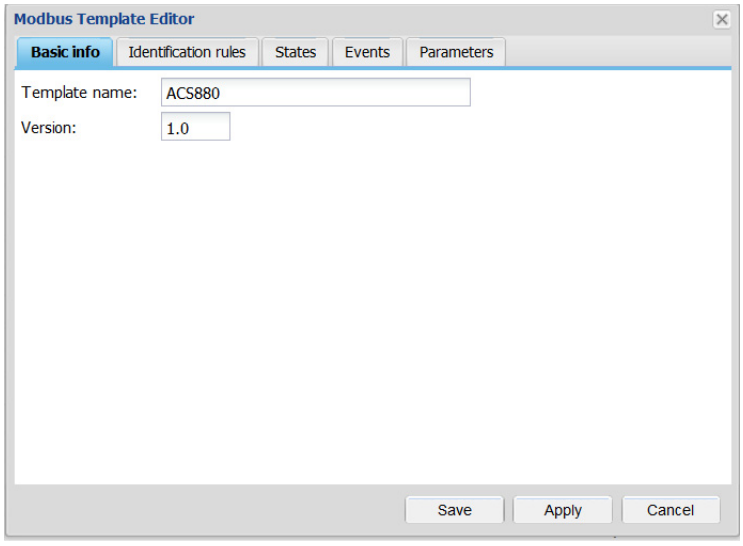
Note: If you try to edit a default template, a confirmation message is displayed to copy the template to the SD card. Click Yes to continue. Else, click No.



3. In the Modbus Template Editor, you can edit the following:
   - *Basic Info*
   - *Identification rules*
   - *States*
   - *Events*
   - *Parameters*
4. After required modification in each section, click **Apply** and then **Save** to save the changes.

   Basic Info

   Basic info includes the basic information of the templates. These are informal metadata attributes. The Basic info tab has the following components:
   - Template name - Defines the name of the template.
   - Version - Defines the version of the template.



   Identification rules

   Identification rules are used for automatically scanned Modbus/RTU devices. It is not used for node IDs that are added manually such as Modbus/TCP devices connected through fixed IP address.

   The Identification rules tab include the raw Modbus register and fixed value details. To apply the template automatically during the background scan of the Modbus/RTU devices, the register and fixed values should match.

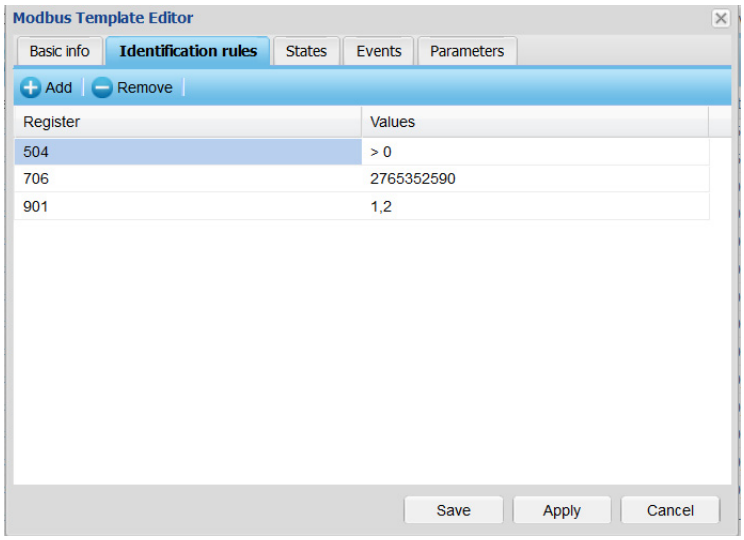
   The Identification rules tab has the following components:
   - Register - Unsigned integer. Modbus register can be 16 bit (values 1...20000) or 32 bit (over 20000). For drives automatic identification, if parameter internal type is int16 or uint16 then register is calculated as:

$$\text{register} = 100 \times \text{group} + \text{index}$$

If parameter internal type is int32 or uint32 then register is calculated as:

$$20000 + 200 \times \text{group} + 2 \times \text{index}$$

- Values - Comma separated integers, parameter internal values, and comparisons using the >, >=, <, <=, and <> operators.



Note: It is possible to list multiple registers and multiple possible identification values for each register. However, the increase in conditions makes the identification slower and further slows the automatic identification performance (Modbus background scanning). Hence, it is recommended to use maximum 3 conditions.

States

States tab includes the Modbus register information that is mapped to the Modbus template and also indicates the device status.

States tab has the following components:

- Name - Displays the device status. For example, Disconnected, fault, warning, and so on.
- Parameter - Displays the related parameter in group.index format.
- Mask - Unsigned integer. Defines the value of bitmask for comparison operation.The mask value is calculated as:

  $$\text{maskvalue} = 2^0 + 2^1 + \ldots + 2^n$$

  where 0, 1.....n are the bits in a bitword.

Note: You can enter the mask values as decimal number in different formats. For example, 123, 0x7B, 0b1111011, and so on.

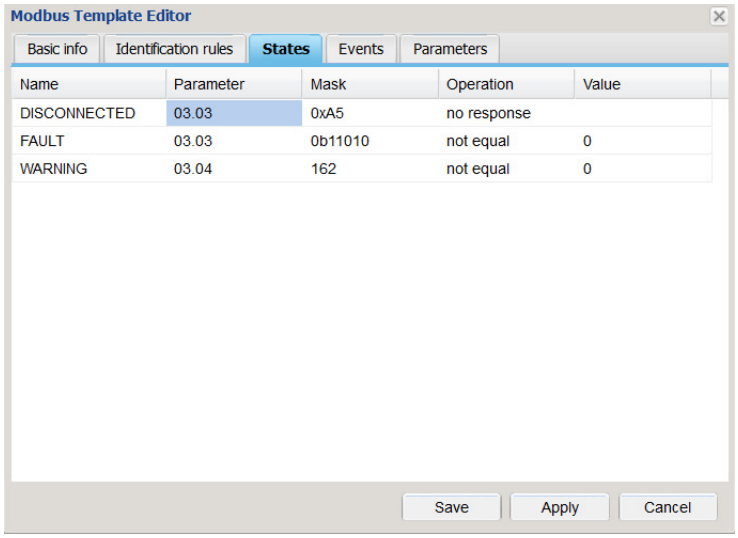
- Operation - Triggered automatically if NETA - 21 cannot read any values. The possible events and its reasons are:

Operation	Reason
No response	NETA-21 cannot read any values. Value column and mask can be empty, but the parameter must be an existing parameter which can be always read if the device is connected (preferably main statusword which is also used for fault and warning states)

Operation	Reason
Change (appears as Equal in firmware 2,27 and later)	Value is changed and is equal to specified value.
Not equal	Value not equal to specified value

Note: The operation names are not editable.

- Value - Parameter internal value (integer).

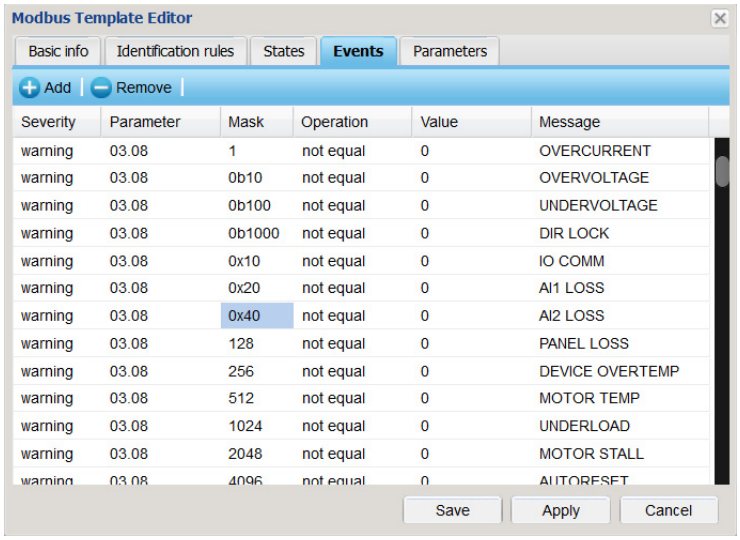


Events

Events tab provides information on the custom monitored parameters that triggers the events.

Event tab has the following components:

- Severity: Displays the severity of the event.
- Parameter: Displays the related parameter that triggers the event.
- Mask - See mask field in *States* tab.
- Operation - See Operation in *States* tab.
- Value - See Value in *States* tab.
- Message - Displays the type of event. For example, overcurrent, overvoltage, and so on.

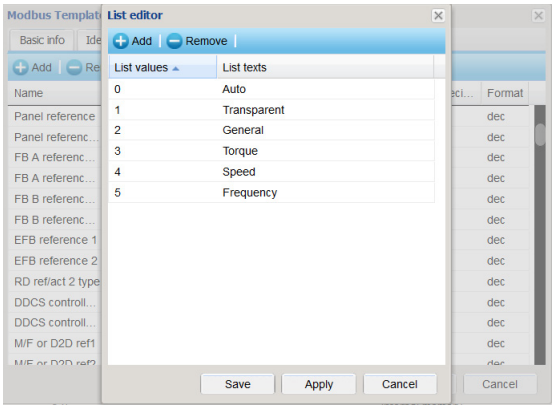


Parameters

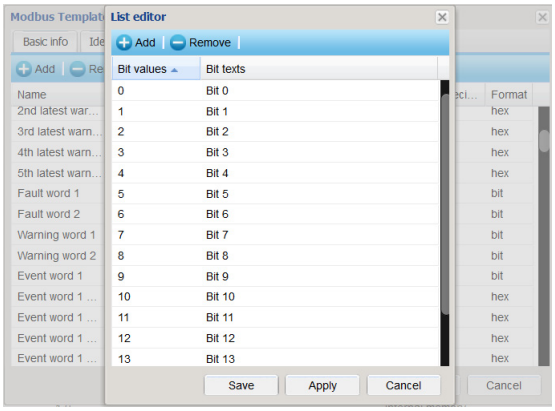
Parameters tab provides information on parameters that are mapped to the Modbus templates. You can click **Add** or **Remove** to add or remove any parameter from the list.

The parameters tab has following components:

- Name - Displays the parameter or group name that appears in the parameter browser.
- Type - Displays the type of parameter listed. The possible parameter type values are:
  - Empty: Normal parameters.
  - Group: Parameter groups
  - List: Parameters with lists. You can edit the parameter lists using **Edit list** button.



-Bitword: Parameters with bitwords. You can edit the bit values and texts using the **Edit List** button.



- Index - Displays the parameter index in group.index format. Max value is 255.255
- WP - Displays whether the parameter is write protected.
- Pointer - Allows you to enable target parameter pointer selection in web UI.
- Unit - Displays the unit that is displayed in the parameter browser.
- Internal type - Defines the parameter internal type as follows:

  U16: Unassigned 16 bit integer

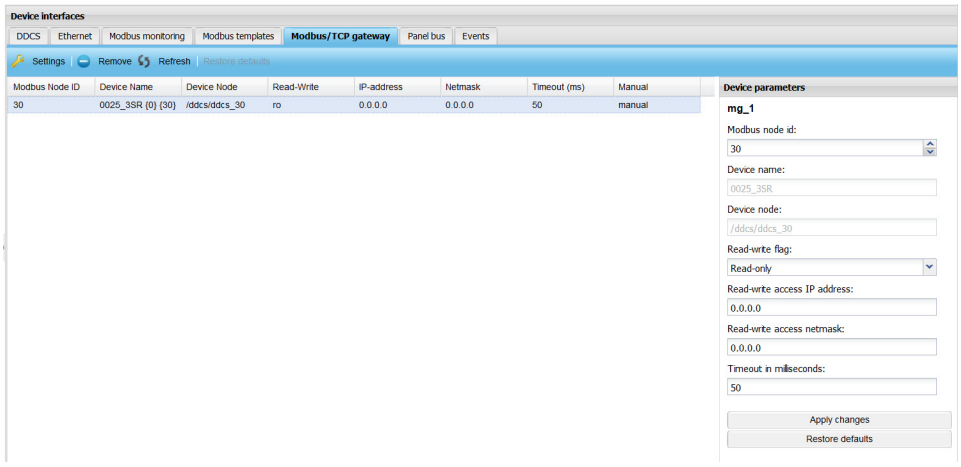
  S16: Signed 16 bit integer

  U32: Unsigned 32 bit integer

  S32: Signed 32 bit integer
- Scaling: Defines the scaling value to scale the value read from the drive
- Decimals: Displays the number of decimals displayed in the parameter browser. This is not used for any calculations.
- Format: Defines the value format. For example dec for decimal, hex for hexa decimal, and bin for binary.

Modbus/TCP gateway tab

The Modbus/TCP gateway tab contains a list of all connected drives which can be accessed through the Modbus/TCP gateway.



On selection of a drive from the list, the Device Parameters section displays settings of the selected drive as follows:

- **Modbus node id** field represents the connection specific node ID of the drive, see chapter *Modbus/TCP gateway* on page *43*.
- **Device Name** field shows the name of the drive.
- **Device Node** field shows the node id of the drive.

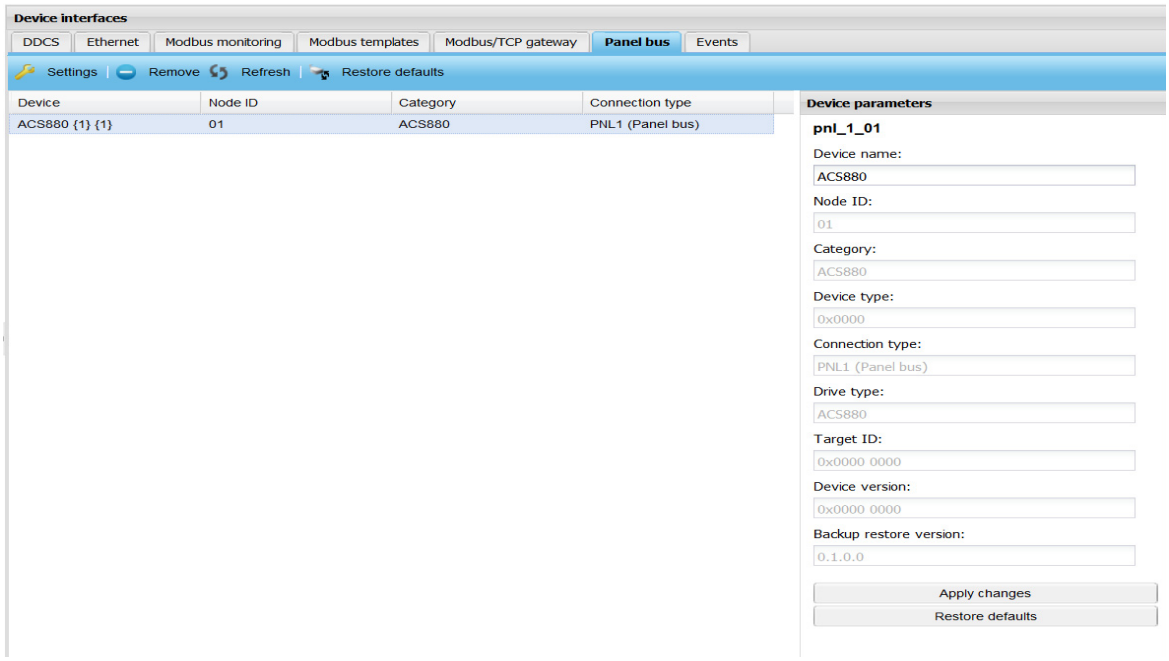
  Read-write flag is a drop-down list to select the access mode, specific to the particular drive through the gateway. There are 2 options:

  - Read-only

  - Read-write.
- **Read-write access IP address** is an edit box, where the user can specify the IP address from where the gateway accepts connections to this particular drive.
- **Read-write access netmask** is an edit box, where the user can specify the netmask of the IP address from where the gateway accepts connections to this particular drive.
- **Timeout in milliseconds** is an edit box, where the user can specify the maximum waiting time for a response after each individual request, for this specific drive.

Panel bus tab

The **Panel bus** tab contains all the devices connected to the PNL connectors.



Interface settings

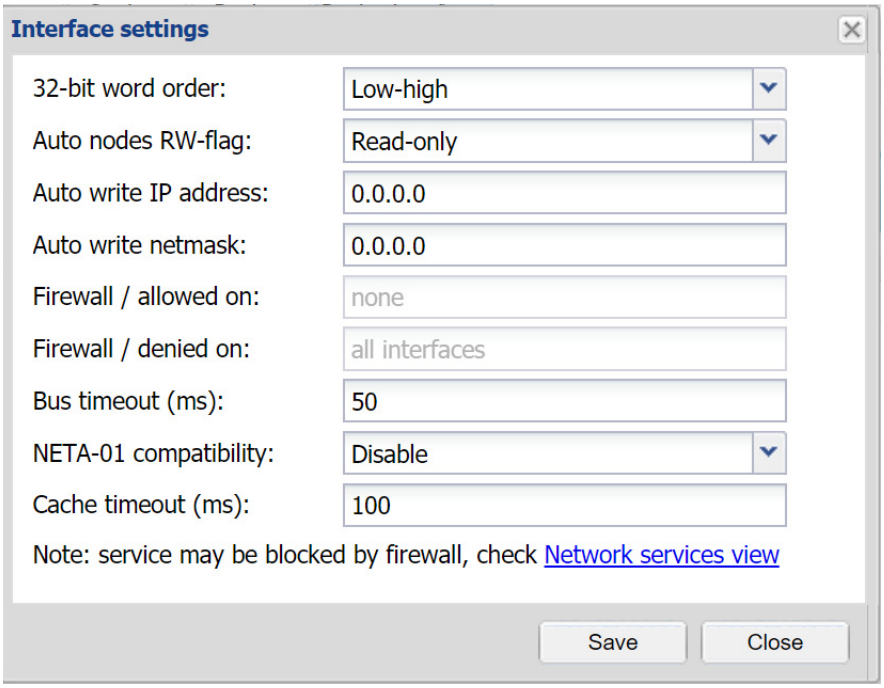
To open the Interface settings dialog box, click the **Settings** button on the toolbar. Every connection type has its own Interface settings dialog box. The following two buttons are common to each connection type:

- **Save** button saves the modified settings.
- **Close** button closes the dialog box without saving the settings.

Note: The settings depend on the configuration required by a device interface.

Modbus/TCP gateway settings

The figure below shows the Interface settings dialog box of the Modbus/TCP gateway tab.

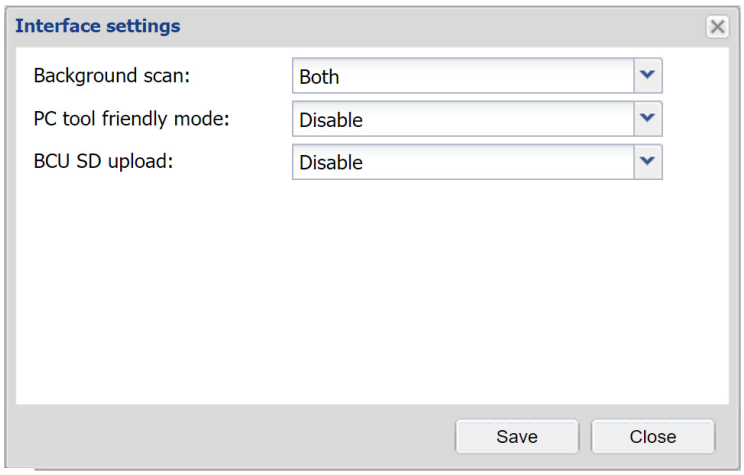


- **32-bit word order** is a drop-down list for selecting the most or least significant word order for 32-bit values. There are 2 options:
  - Low-high
  - High-low
- **Auto nodes RW-flag** is a drop-down list for enabling or disabling write access. There are 2 options:
  - Read-only
  - Read-write
- **Auto write IP address** is a text box where the IP address of the Modbus/TCP master can be specified.
- **Auto write netmask** is a text box where the netmask for Modbus/TCP master IP address can be specified.
- **Firewall / allowed on** shows the network interfaces on which Modbus/TCP gateway access is enabled. Changes can be done in **Settings -> Network services -> Firewall settings**.
- **Firewall / denied on** shows the network interfaces on which Modbus/TCP gateway access is disabled. Changes can be done in **Settings -> Network services -> Firewall settings**.
- **Bus timeout (ms)** is a text box where the user can specify the maximum waiting time for a response given to an individual Modbus/TCP request. If the response hasn't arrived in the allotted time, Modbus error 0x06 - **Slave Device Busy** is sent back to the master.
- **NETA-01 compatibility** enables NETA-01 users to use NETA-21 as a direct replacement for NETA-01. The basic NETA-01 functionalities are added to the NETA-21 firmware. See *NETA-01 compatibility mode*.
- **Cache timeout (ms)** allows to define the cache expiry time. See *Cache*.

When the master's request contains a range of values, the timeout is applied to each value separately.

Ethernet settings

The figure below shows the Interface settings dialog box of the Ethernet connection.



With the **Background scan** function you can define how the automatic device discovery works. The available options are:

- **Disabled**: Devices are not automatically discovered.
- **ETH1**: Automatic discovery works only on the first Ethernet port.
- **ETH2**: Automatic discovery works only on the second Ethernet port.
- **Both**: Automatic discovery works only on both Ethernet ports.

When the **PC tool friendly mode** is enabled, the background scan function starts with a 30 seconds delay. This time is used by PC tool (like Drive Composer) to detect a drive and connect to it.

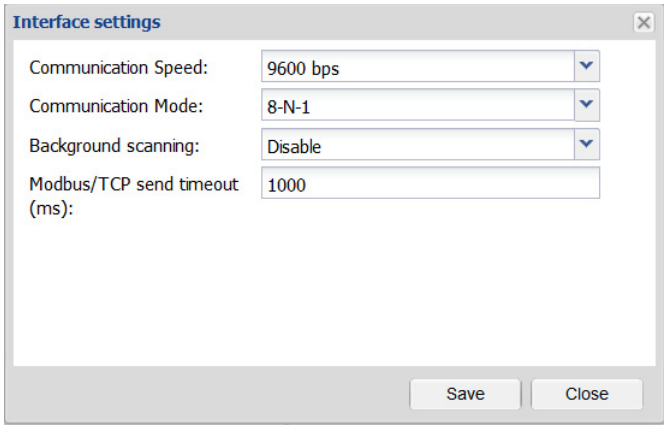
When **BCU SD upload** option is enabled, the NETA-21 uploads the additional diagnostic data generated by the drive to the SD card, for the selected period. The available options are:

- Disable
- Latest 30 days
- Latest week
- Latest one day
- Everything

For ACS580MV and ACS6080 drives, the input is BlackBox data and for ACS880 drives, the input is BCU PSL2 logger upload data.

Modbus settings

The figure below shows the Interface settings dialog box of the Modbus connection.



Communication Speed is a drop-down list for setting the speed of the Modbus communication. The available speeds are the following:

- **9600 bps**
- **19200 bps**
- **38400 bps**
- **57600 bps**
- **115200 bps**
- **230400 bps.**

Communication Mode is a drop-down list for setting the serial communication mode. The available values are the following:

- **8-N-1**: 8 None 1
- **8-E-1:** 8 Even 1
- **8-O-1**: 8 Odd 1
- **8-N-2**: 8 None 2.

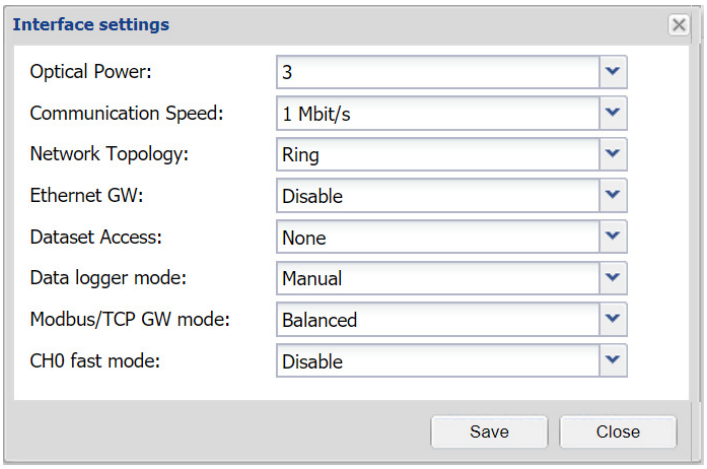
Background scanning is a drop-down list for enabling or disabling the automatic device discovery. The background scanning uses the selected communication settings. The background scanning runs every minute if there are no connected devices, or every 4 minutes if at least one device is connected.

Modbus/TCP send timeout is a text box where the user can specify the maximum waiting time for a response from individual drive. The timeout period is defined in milliseconds.

When the master requests to read or write several registers, the timeout value is applied to each response.

DDCS settings

The figure below shows the **Interface settings** dialog box of the DDCS connection.



- **Optical Power** is a drop-down list for defining the value from 1 (lowest) to 4 (highest).
- **Communication Speed** is a drop-down list for defining the value from 1 to 8 Mbit/s.
- **Network Topology** is a drop-down list where you can choose values **Star** or **Ring**.
- **Ethernet GW** is a drop-down list for enabling or disabling the Ethernet gateway for a remote DriveWindow PC tool (2.4 or later) connection. Ethernet gateway is turned off automatically when the DriveWindow stops the connection. If the connection is interrupted unexpectedly, NETA-21 keeps gateway mode active for the time specified in DriveWindow configuration (**Device Mastership -> Watchdog Timeout**). By default, the gateway mode active time is set as 60 minutes. The NETA-21 resumes normal operation after the defined time. By default, the gateway is disabled.

  Note: For security reasons, PC tool Ethernet gateway connections for DDCS must be used only inside a trusted network.
- **Dataset Access** is a drop-down list where datasets can be enabled or disabled. The options available are None, Read-only, and Read-write.
- **Data logger mode** is a drop-down list for selecting how drive data logger control mode is modified. The available options are:
  - Manual: You can navigate to **Devices** → **Datalogger** and manually configure data logger settings. You can configure start/stop/trigger for each logger or can configure specific loggers for automatic uploads individually. Manual mode is recommended for case specific drive inspection when you use NETA-21 web UI directly without the use of cloud services.
  - Automatic: In automatic mode, NETA-21 uploads logger files per each fault automatically and also auto configures datalogger signals and runs connected DDCS drive data logger. This option is recommended for cloud-connected NETA-21.
- **Modbus/TCP GW mode** defines the way how DDCS interface is shared during operation. The available options are:
  - Balanced - Processes requests from different components before Modbus/TCP Gateway requests.
  - Enhanced - Processes Modbus/TCP Gateway requests before the requests from all other components
  - Dedicated - In this mode, when NETA-21 detects a Modbus/TCP Gateway request, the Gateway gets special access to the DDCS drive. During this time, the other components (e.g. WebUI, Reporting) do not have access to read, write, or

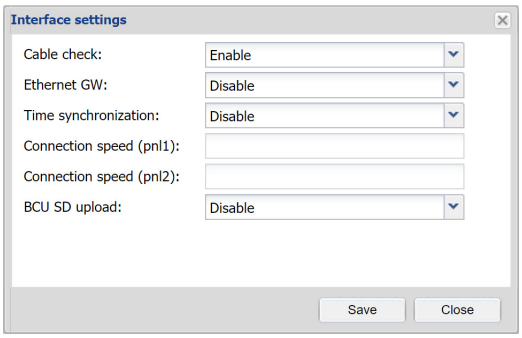
display DDCS parameter values. The device resumes the normal behavior 5 seconds after the last Gateway request.

- CH0 fast mode is intended only for fast Modbus/TCP control when cloud connection is not active on the NETA-21.
  Note: During cloud monitoring, NETA-21 should be connected to CH3 tool channel of the drive and CH0 fast mode should be disabled.

Panel bus settings

WARNING! Make sure that you do not enable this connection in an open or insecure network. Panel bus to Ethernet tool network gateway does not use HTTP encryption or authentication. Hence, this connection is not secure.

The figure below shows the **Interface settings** dialog box of the Panel bus connection.



Note: From NETA-21 firmware version 3.0, HTTP is disabled. To use HTTP gateway feature, enable HTTP in **Settings -> Network services**.

- **Cable check** is a drop-down list for enabling or disabling the function.
  - When the cable check function is enabled, the NETA-21 tries to identify the connected cable (by testing the input voltage from the drive control board). The panel bus connection scanning runs in the background only if the cable (input voltage) is detected on the PNL1 or PNL2 port.
  - When the cable check function is disabled, panel ports are scanned continuously even if the cable is not connected. If the input voltage is not available from the panel bus, this option can be used for detecting panel bus devices. When the cable check function is disabled, there is extra background CPU load in the NETA-21. The PNL1/PNL2 LEDs are red if no panel bus device cannot be detected. See *LED indications of the NETA-21*.
- **Ethernet GW** is a drop-down list for enabling or disabling the gateway mode. By default, Ethernet gateway is disabled. There are four different options to enable this feature:
  - Enable - Enables the Ethernet gateway permanently. This can weaken security and is not recommended.
    Note: While Ethernet GW is active, communication through Modbus/TCP GW does not work.
  - Enable while in use - Keeps the gateway open, as long as data is flowing through. Gateway is disabled automatically after 10 seconds of inactivity.
  - Enable 1 hour - Keeps the gateway open for 1 hour from the time it is enabled, regardless of inactivity.
  - Enable 24 hours - Keeps the gateway open for 1 day from the time it is enabled, regardless of inactivity.

Note: For security reasons, PC tool Ethernet gateway connections for Panel Bus must be used only inside a trusted network.

- **Time synchronization** is a drop-down list for enabling or disabling the function. When enabled, NETA-21 will act as a clock master for the drives connected via this interface.
- **Connection speed (pnl1)** shows the speed for the active connection.
- **Connection speed (pnl2)** shows the speed for the active connection.
- **BCU SD upload** is a drop-down list to enable or disable the BCU SD upload function. When the BCU SD upload function is enabled, the NETA-21 uploads the additional diagnostic data generated by the drive to the SD card, for the selected period. The available options in the BCU SD upload function are:
  - Disable - Disables the BCU SD upload function
  - Latest 30 days - Uploads the additional diagnostic data generated in the last 30 days.
  - Latest week - Uploads the additional diagnostic data generated in the last week.
  - Latest one day - Uploads the additional diagnostic data generated in the last one day.
  - Everything - Uploads the existing additional diagnostic data completely.

The uploaded content for ACS580MV and ACS6080 drives is the BlackBox data. For ACS880 drives, the content is the BCU PSL2 logger upload data.

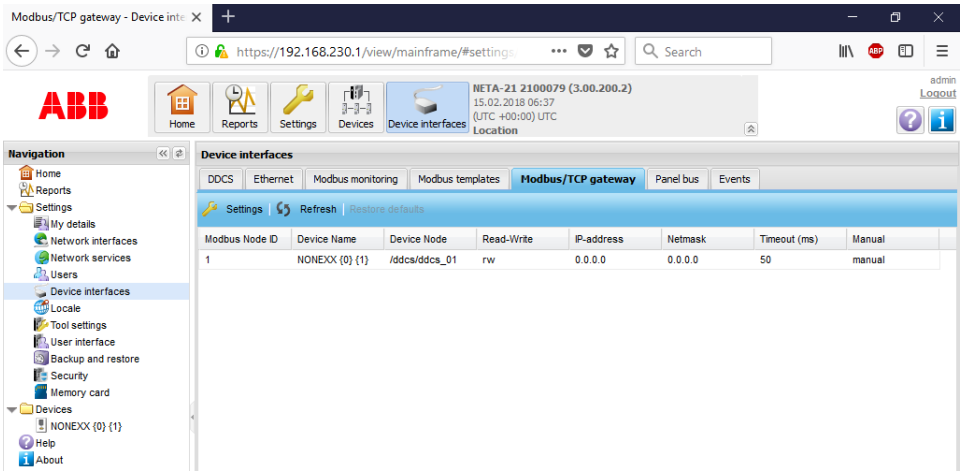
NETA-01 compatibility mode

NETA-01 compatibility mode allows NETA-01 users to use NETA-21 as a replacement for NETA-01.

Activate NETA-01 compatibility mode

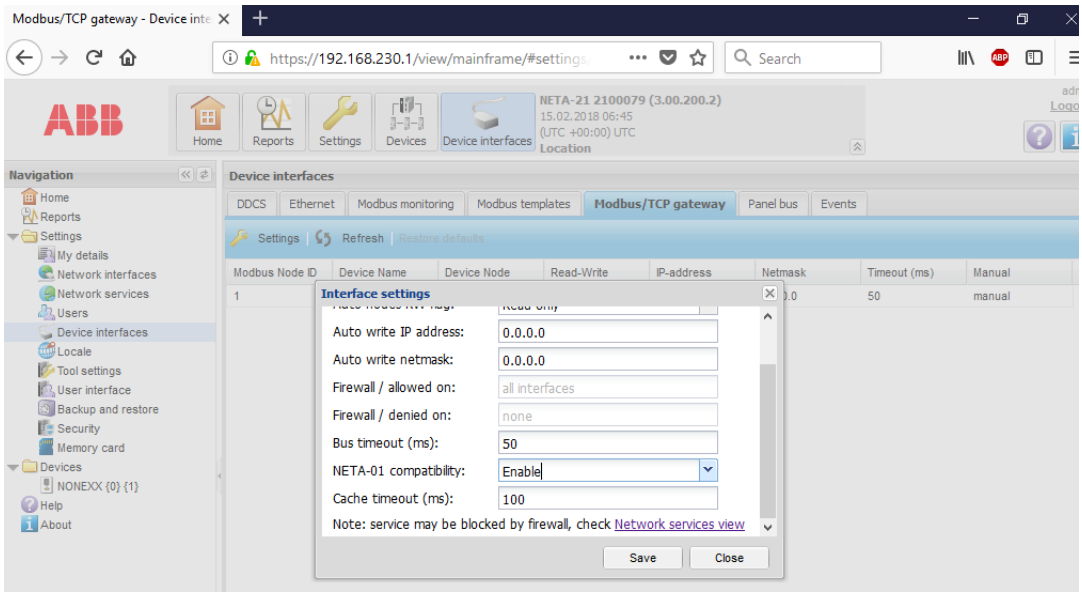
To activate NETA-01 compatibility mode,

1. From the NETA-21 UI, navigate to **Settings -> Device interfaces -> Modbus/TCP gateway** tab.

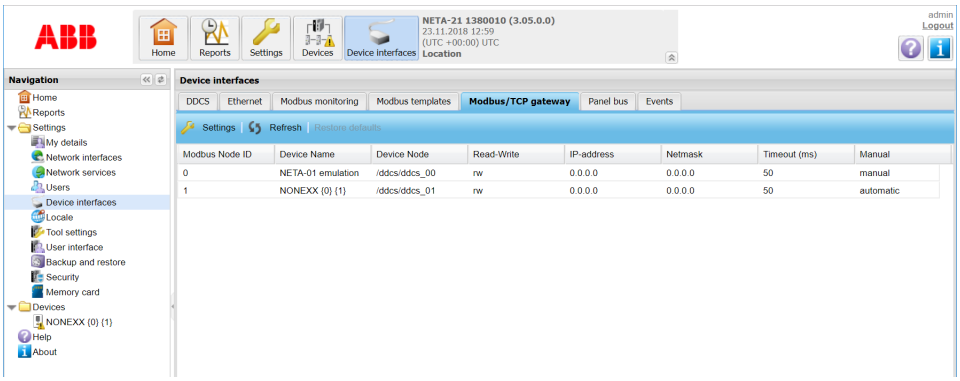


2. Click **Settings.**
   The Interface Settings window appears.

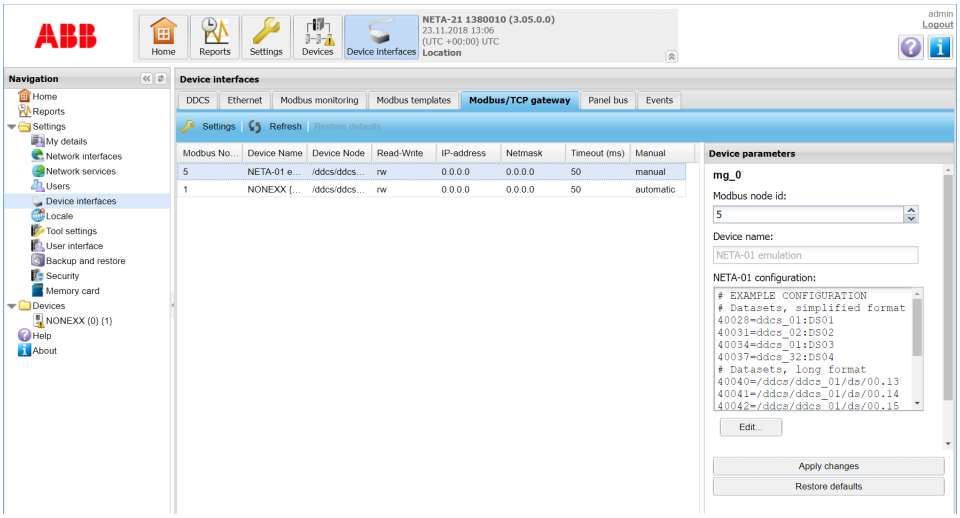
3. From the **NETA-01 compatibility** drop-down, select **Enable**.



4. Click **Save**.
   The NETA-01 compatibility mode is enabled successfully and a new virtual Modbus/TCP gateway device NETA-01 emulation with Modbus Node ID 0 appears in the device list.



5. If required, you can click on the added device and change the value of the Modbus node id. The values can range 0 to 247.



Notes:

- By default, on activation of NETA-01 compatibility mode, NETA-21 maps the NETA-01 compatibility mode to Modbus node ID 0. Other addresses can be allocated by NETA_21 specific mapping. For more information, see section *Modbus/TCP gateway tab* on page *95*.
- The Modbus device address 0 requests are processed based on the NETA-01 configuration settings. Other requests are handled normally.

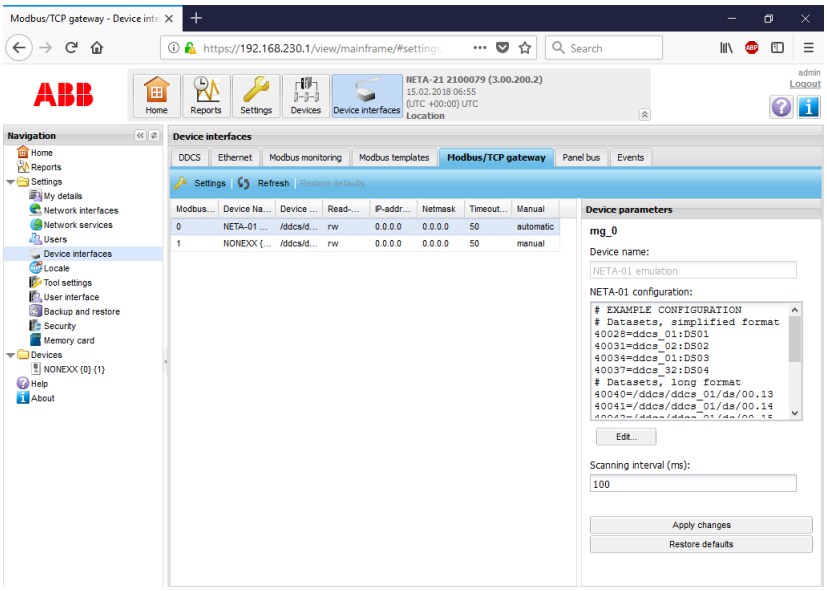
To deactivate NETA-01 compatibility mode,

1. From the NETA-21 UI, navigate to **Settings -> Device interfaces -> Modbus/TCP gateway** tab.
2. Click **Settings.**
   The Interface Settings window appears.
3. From the **NETA-01 compatibility** drop-down, select **Disable.**
4. Click **Save**.
   The NETA-01 compatibility mode is disabled successfully and the NETA-01 emulation device disappears from the device list.

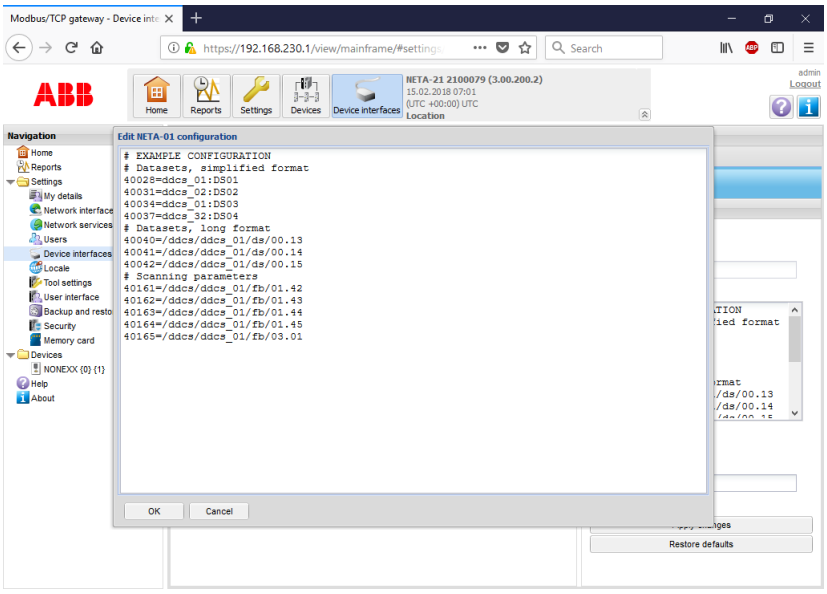
NETA-01 device configuration

NETA-01 emulation device has dedicated device parameters. To configure the NETA-01 emulation device,

1. From the **Modbus/TCP gateway**, select the **NETA-01 emulation device.** The Device parameters window appears.



2. In the **NETA-01 configuration** editor, enter the configuration code. You can also click the **Edit...** button and make the required changes in **Edit NETA-01 configuration** window..



Supported configuration formats for parameters/datasets (software versions 3.05 - 3.21)

Parameter/dataset range	Format
Starts at register 40028 or 40031 or 40034 - 40085	Simplified format, 40028=ddcs_01:DS01
Datasets/registers in NETA-01 user guide 40028 - 40087	Long format, 40028=/ddcs/ddcs_01/ds/00.01
Scanning parameters 40161 - 40205	40161=/ddcs/ddcs_01/fb/01.42

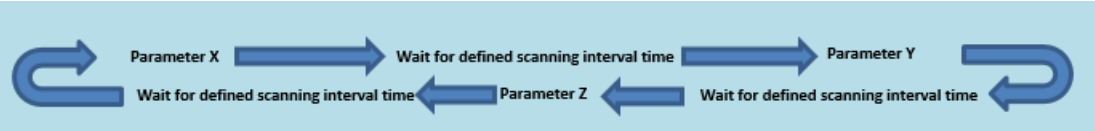
Supported configuration formats for parameters/datasets (software version 3.22 or later)

Parameter/dataset range	Format
Dataset three register group. Starting register can be selectable between 40001 - 40097 and other two registers for three values inside specified dataset.	Simplified format, 40001=ddcs_01:DS01
Dataset 4001 - 40099 single register pointing to single parameter reference inside dataset.	Long format, 40001=/ddcs/ddcs_01/ds/00.01
Scanning parameters 40101 – 49999	40101=/ddcs/ddcs_01/fb/01.42

Notes:

- For parameter/dataset range 40101 – 49999, a maximum of 200 scanning parameters can be configured.
- From software version 3.22, the configurable scanning interval range is increased from 100-1000ms to 10-1000ms.

3. Click **Apply changes.**
   The internal parser validates and saves the configuration. A notification is sent to the user if the parser rejects the configuration.
4. Enter the **Scanning interval**. The scanning interval defines the rate at which individual parameter is read from the drive to cache.The values can range from 100 to 1000 milliseconds.
   Note: The system takes 450 milliseconds to 45 seconds to update 45 scanning parameters in the cache. This depends on the scanning interval value set.



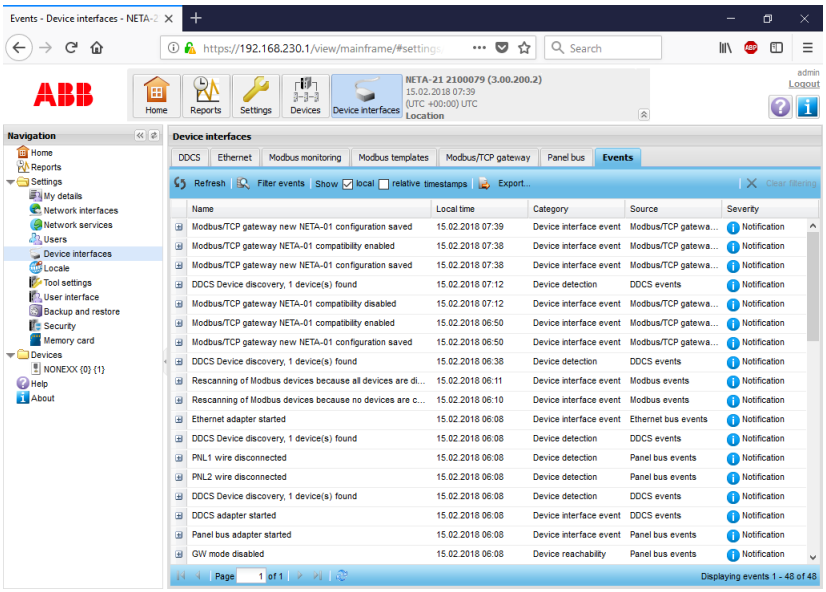
Events

Events are logged whenever:

- NETA-01 compatibility mode is enabled or disabled. Example for log messages are shown below:

Modbus/TCP gateway NETA-01 compatibility enabled.
Modbus/TCP gateway NETA-01 compatibility disabled.

- NETA-01 configuration is saved. Example for log message is shown below:
  Modbus/TCP gateway new NETA-01 configuration saved.



Special registers

When you enable NETA-01 compatibility mode, the system emulates two special registers. later, Later, the scanned parameter mapping might override these registers.

1. System status word register (address 40089)
   The value of this register toggles every 5th second between 64512 and 65024 (0xFC00 and 0xFE00).
2. System control word register (address 41113)
   NETA-21 reboots automatically, if any value is written to this register with bit3 enabled.

Cache

For scanning parameters in NETA-01 compatibility mode, a dedicated cache for up to 45 parameters (firmware versions up to 3.21) or up to 200 parameters is available (firmware version 3.22 and later). This cache is updated by the cache server in the background. Modbus read requests are served immediately and requested parameters are returned from cache. During this time, no cache misses or data expiration happens.

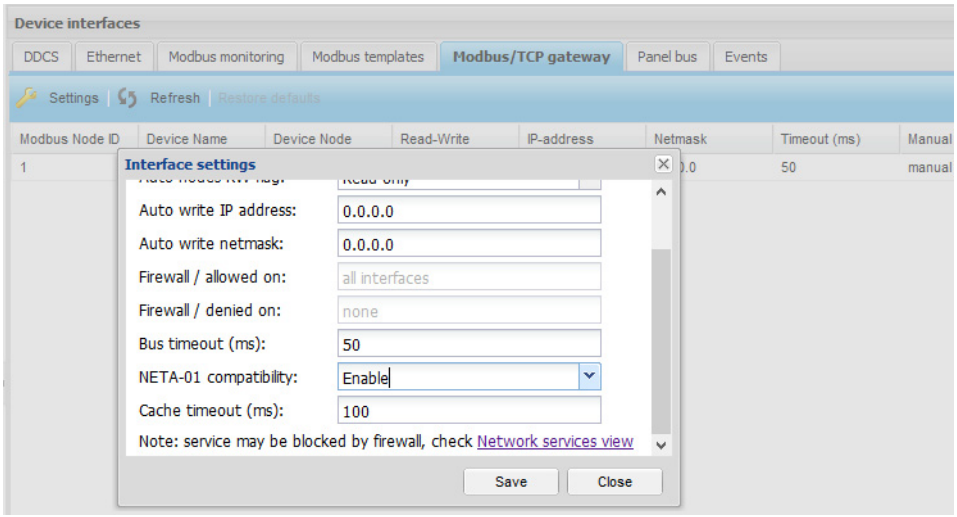
For other read requests including when NETA-21 compatibility mode is not activated, there is a common LRU (Least Recent Used) type cache that serves all dataset and non-compatibility mode scanning parameter read requests. During this time, if any cache miss or data expiry happens, the request is forwarded to the DDCS / drive.

Notes:

- Cache is not used when writing Modbus/TCP values to parameters or datasets.
- Scanned parameter range cannot overwrite Modbus/TCP. Cached datasets and NETA-21 mode mapped parameters are writable depending on the configuration. For more information, see section *Modbus/TCP gateway settings* on page *97*.

Cache timeout

You can adjust the cache expiry time. To define the cache expiry time, from Modbus/TCP gateway tab, navigate to Interface settings and in the Cache timeout (ms) field, enter the desired value. The values can range 100 to 1000 milliseconds.



The efficiency of the cache depends on the poll cycle of external request (time between requests) and the cache timeout.

The performance of the cache improves when the cache timeout is more than the polling rate. For example, if the cache timeout is 1000 ms and the polling rate is 100 ms, then the system serves 9 requests from the cache and every 10th request is forwarded to DDCS / drive. If any of the requested values is not in cache or value has expired, the whole request is forwarded to DDCS / drive.

Exceptions

- Illegal Data Address exception - Modbus address 0 register not in NETA-01 configuration
- Gateway Path Unavailable exception - Modbus address/node not found.

11

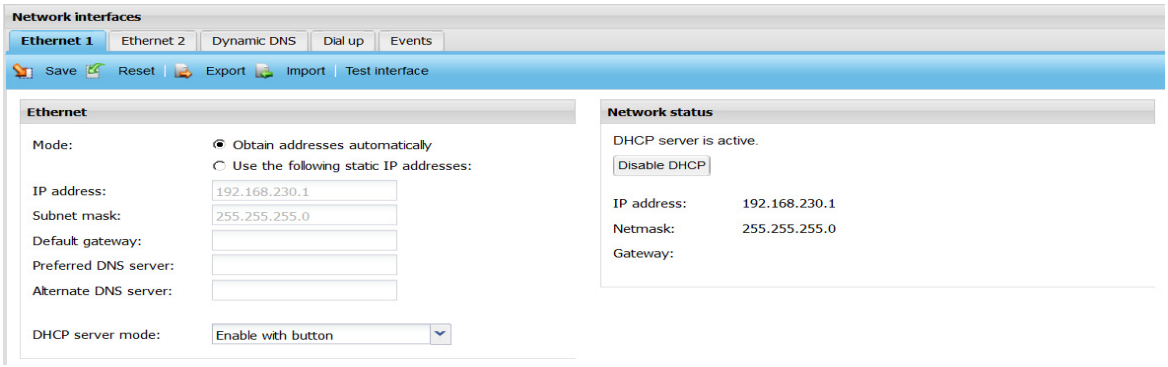
Networks

What this chapter contains

This chapter explains how to set up and configure Ethernet network interfaces of the NETA-21.

Network interfaces view

The Network interfaces view (**Settings –> Network interfaces**) is split into two interface specific tabs: **Ethernet 1** and **Ethernet 2**.



In addition to the *Ethernet panel* and *Network status panel*, the Ethernet interface tabs contain the following components:

- **Save** button saves the changes to the NETA-21. When you save the settings, they are applied to use immediately. A dialog box warns that the connection to the web pages can be lost, if the IP address of the NETA-21 is changed. You can either continue or cancel the changes.
- **Reset** button discards all changes made by the user.
- **Export** button exports the Ethernet settings to a local file.

- **Import** button imports the Ethernet settings from a file to the UI.
- *Test interface* button opens a dialog which can be used for sending a ping message to a defined address.

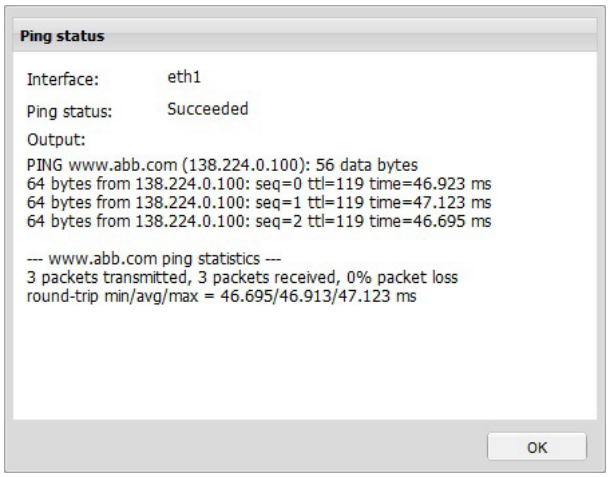
Test interface

When you click the **Test interface** button the following dialog box appears:

The **Ping server** dialog box contains the following components:

- **Server to ping** box defines the address of the server where the ping message is sent.
- **OK** button sends the ping message and opens a dialog to show the result.
- **Cancel** button closes the dialog box.

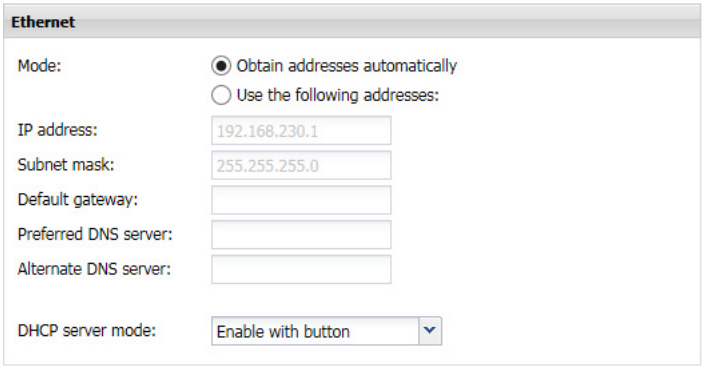
The following **Ping status** dialog box appears after the ping message has been sent:



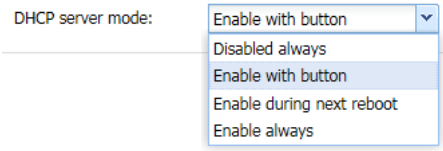
The **Ping status** dialog box contains the following components:

- **Interface** field shows the interface that was used for sending the ping message.
- **Ping status** field shows whether the sending of the message has failed or succeeded.
- **Output** field shows the console output for sending the message.
- **OK** button closes the dialog box.

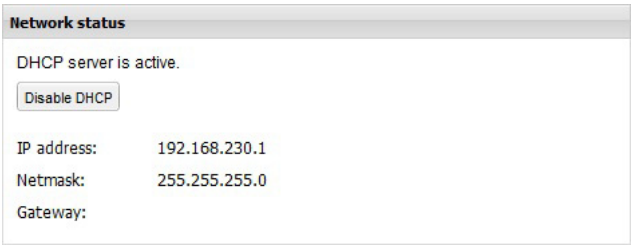
Ethernet panel



- **Mode** has two options for selecting either an automatically obtained or a static IP address:
  - **Obtain an IP address automatically** option disables the IP address, Subnet mask and Default gateway boxes. This is the default setting. When this mode is selected, the NETA-21 tries to retrieve its IP address from the DHCP server. If the DHCP address retrieval fails, the NETA-21 defaults to a “zeroconf” IP address in format 169.254.x.y where x and y are randomly selected numbers.
  - **Use the following IP addresses** option requires you to configure the fixed static IP address settings by filling in the following boxes: IP address, Subnet mask, Default gateway, Preferred DNS server and Alternate DNS server.
  - **DHCP server mode** (only on the **Ethernet 1** tab from firmware 2.22 onwards) can always be disabled or enabled, or enabled for the next boot up. Option **Enable with button** is the same as by default: If you press the SD/RJ45 button for 5 seconds, you activate the DHCP server on the ETH1 port. If another DHCP server is detected in a local network, the NETA-21 does not activate its DHCP server.



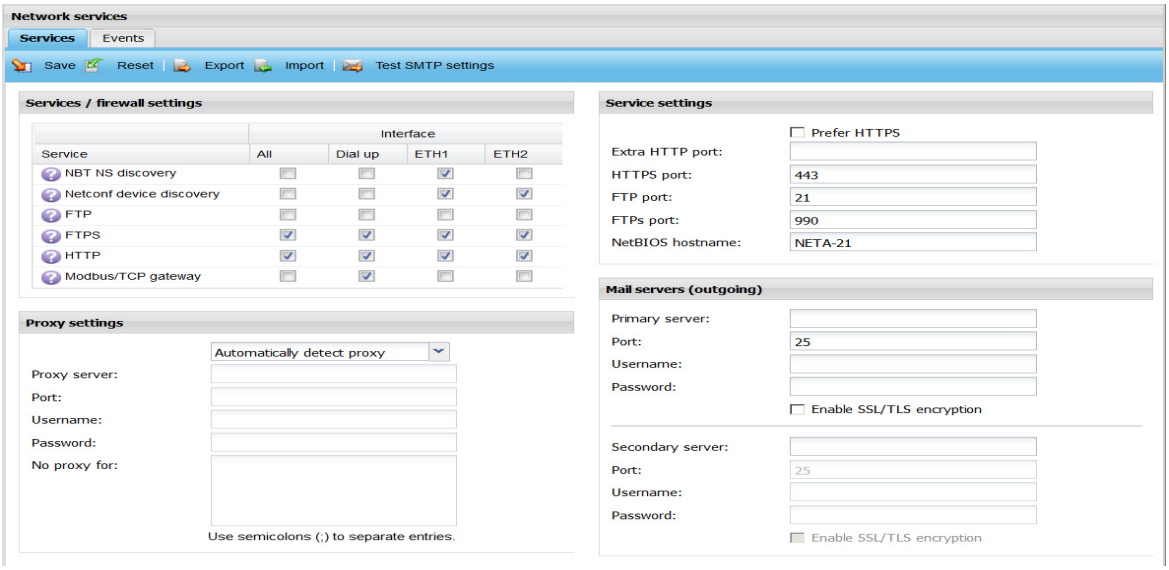
Network status panel



- **Disable DHCP** button disables the DHCP server mode. The button is visible only when the DHCP mode has been activated with the SD RJ45 button.
- **IP address** field shows the currently used IP address for the interface. If the field is empty, no IP address has been defined. If the link status is "down", a message indicating this is shown instead. This field cannot be modified.
- **Netmask** field shows the current network mask. If the field is empty, no mask has been defined. This field cannot be modified.
- **Gateway** field shows the default gateway for the specific interface. This field cannot be modified in the Network status panel.

Network services

The **Network services** view (**Settings –> Network services**) shows the connectivity of the NETA-21 with outside world over Ethernet.



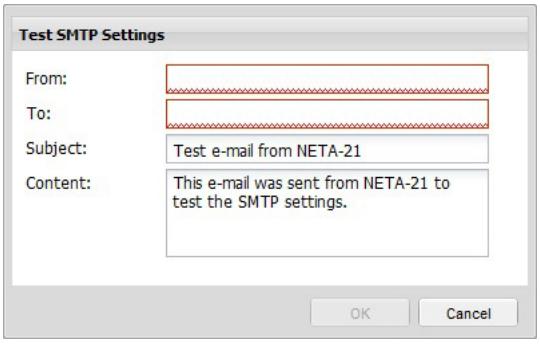
For example, time services are located in the Locale settings view. Some of the out-bound reporting services such as email and FTP are configured in the **Report** view.

The **Services** tab contains the following components:

- **Save** button saves the changes to the NETA-21.
- **Reset** button discards all changes made by the user and restores the default settings.
- **Export** button exports the visible settings to a local file.
- **Import** button imports the settings from a file to the UI.
- *Test SMTP settings* button asks you for an email address. The UI uses the visible SMTP settings to send a test email to the specified email address.

The *Services/firewall settings panel*, *Services settings panel* and *Mail servers (outgoing) panel* are described below.

Test SMTP settings

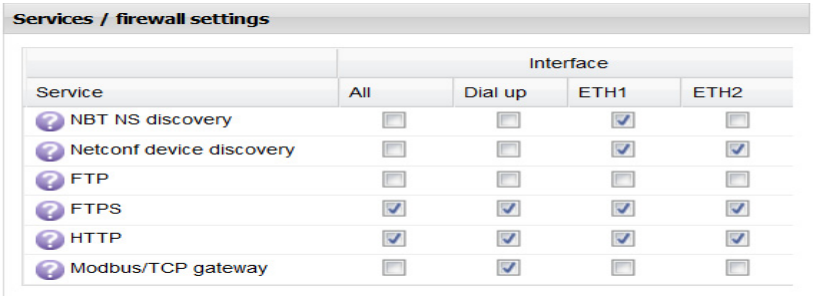


The **Test SMTP settings** dialog box contains the following components:

- **From** text box defines the email address of the sender.
- **To** text box defines the email address of the receiver.
- **Subject** text box defines the subject for the email message.
- **Content** text box defines the content for the email message.
- **OK** button closes this dialog box and sends an email to the receiver.
- **Cancel** button closes this dialog box.

Services/firewall settings panel

The **Services/firewall settings** panel has one service defined in every row. You can enable or disable the service per each interface. You can also select the service to be enabled for all interfaces.

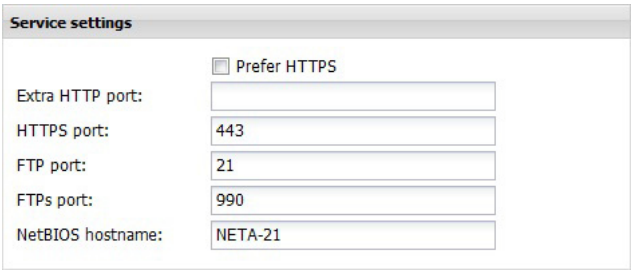


The list has the following columns:

- **Service** column has every available service listed. After the service name there is an icon. By clicking the icon a popup dialog box or a tooltip is opened providing more details about the service.
- **Interface** column has multiple sub-columns. All interfaces are below this column.
- **All** column is always visible and enabled. The column has a check box which is selected if the service has been enabled for all interfaces.
  - When the **All** check box is selected all other check boxes in the interface column are selected as well (in the same row). The **All** check box disables any firewall limits and allows the service to be reached over any network connection.
  - When the **All** check box is not selected all other check boxes in the interface column are unselected as well (in the same row).
- **Interface X** column shows what services are selected for the current interface. It is possible that there is no interface X column since the available interfaces depend on

the tool configuration and type. There may be multiple interface X columns containing a check box.

Services settings panel



The **Services settings** panel contains the following components:

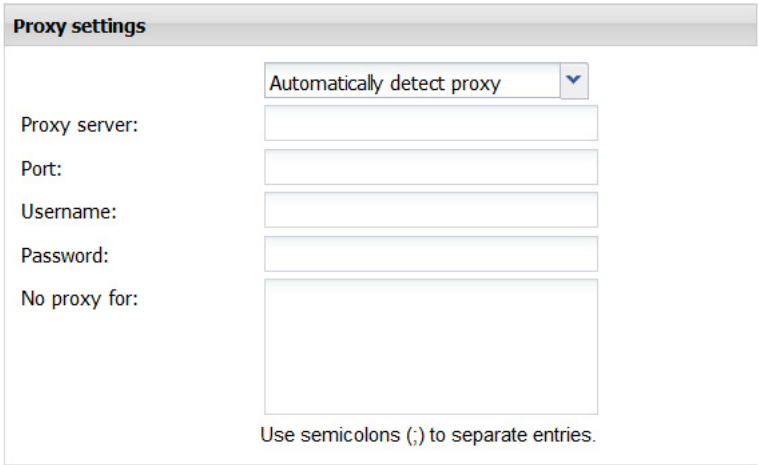
- **Prefer HTTPS** is a check box for defining that HTTPS is used when possible.

  If prefer the Prefer HTTPS check box is selected, the UI login page forwards users always to the HTTPS protocol version of the login page.
- **Extra HTTP port** is a text box for defining an additional HTTP port. If this box is empty, no additional port is used.

  Note: The NETA-21 provides the HTTP version of the web pages always in port 80.
- **HTTPS port** is a text box for defining the HTTPS port. The default value is 443.
- **FTP port** is a text box for defining the FTP port. The default value is 21.
- **FTPs port** is a text box for defining the FTPS port. The default value is 990.

  Note: In the NETA-21 the FTPS client program is configured to use Explicit TLS encryption.
- **NetBios hostname** is a text box for defining the host name for the NetBios service, which facilitates the access to the NETA-21 with a local name instead of an IP address in some local network environments. The default value is "NETA-21".

Proxy settings panel



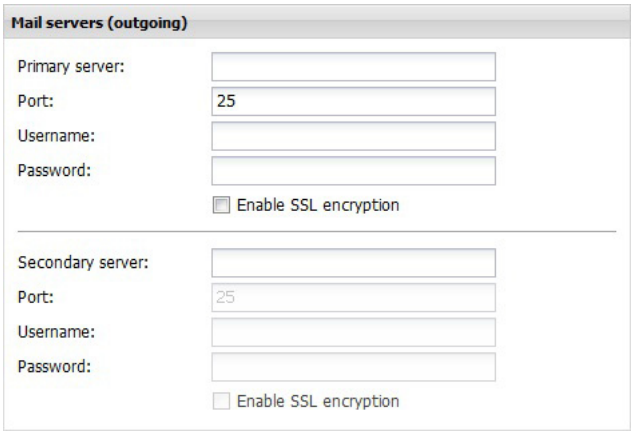
The **Proxy settings** panel contains the following components:

- A selection list to set the preferred proxy server operating mode. The options available are:
  - Automatically detect proxy
  - Do not use any proxy
  - Specify proxy manually

If the user selects to configure the proxy server manually, the desired settings can be specified in the following fields.

- **Proxy server** is a text box for defining the address of the server.
- **Port** is a text box for defining the port of the server.
- **Username** is a text box for defining the user name to access the proxy server.
- **Password** is a text box for the password to access the proxy server.
- **No proxy for** is a text box to list all the IP addresses or domains which can be accessed directly, without contacting the proxy server.

Mail servers (outgoing) panel



The **Mail servers (outgoing)** panel contains the following components:

- **Primary server** is a text box for defining the primary server for the SMTP service.
- **Secondary server** is a text box for defining the secondary server for the SMTP service.
- **Port** is a text box for defining the SMTP port for the SMTP service. The default value is 25. Both primary and secondary mail servers have their own ports to be configured.
- **Username** is a text box for defining the user name for the SMTP service. Both primary and secondary mail servers have their authentication settings to be configured. The Username and Password boxes can be left empty if the SMTP server does not require authentication.
- **Password** is a text box for defining the password for the SMTP service. Both primary and secondary mail servers have their authentication settings to be configured.
- **Enable SSL encryption** is a check box for enabling the SSL encryption for the SMTP service. Both primary and secondary mail servers have their encryption settings to be configured.

DHCP

For instructions on setting up a DHCP server, see *Connecting a local PC to the NETA-21 in the DHCP server mode*.

HTTP/HTTPS

Make sure that you use a firewall or VPN connection, when you use HTTP. HTTP is a non-secure protocol and it is recommended to use it only when HTTPS protocol cannot be used. Non-secure protocol can cause unauthorized access to NETA-21.

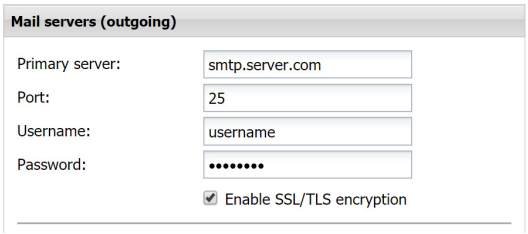
HTTP and HTTPS are the protocols used to display the web pages for user interface of the NETA-21.

Note: From NETA-21 firmware version 3.0, by default, HTTP is disabled. If required, you can enable HTTP in **Settings -> Network services**.

Starting up the SMTP configuration

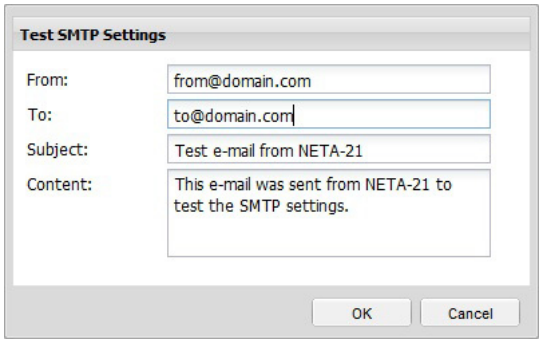
1. Make sure that the NETA-21 is able to access the specified SMTP server over Ethernet.
2. Go to **Settings –> Network services –> Mail servers (outgoing)** and set the appropriate server settings.

Make sure that the “Enable SSL encryption” is always enabled. Disabling this security feature can cause proneness to cybersecurity attacks and unauthorized access to mail servers.

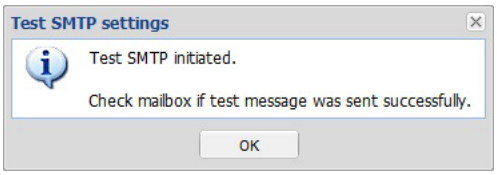


Note: By default, from NETA-21 firmware version 3.00, the "Enable SSL encryption" check box is enabled.

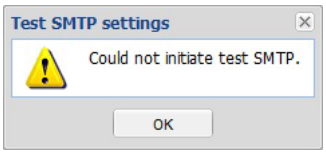
3. To check the SMTP settings, click **Test SMTP settings**, type the test email addresses and click **OK**.



If the test succeeds, the following message is shown.



If the test fails, the following message is shown.



If the SMTP settings are correctly configured, the email reporting process is successfully set up and it is possible to send reports with the NETA-21. See *Reporting*.

FTP/FTPS

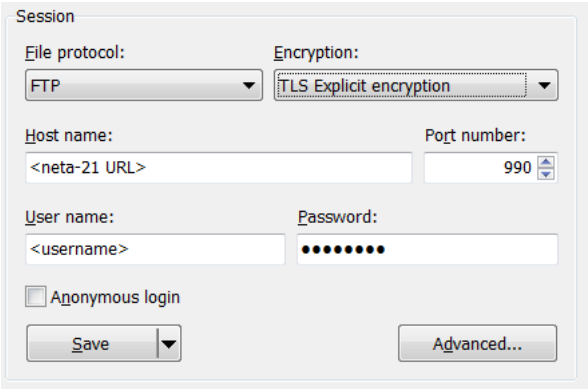
With the NETA-21 you can access the content of the SD memory card remotely if you use the FTP protocol either through an encrypted or an unencrypted channel.

It is highly recommended to use secure FTPS protocol always. FTP uses insecure protocol which transmits data and passwords without any encryption. This can increase proneness to cybersecurity attacks and unauthorized access.

Go to **Settings –> Network services** to enable FTP. You can enable either the encrypted (FTPS) or unencrypted (FTP) connection. FTPS is enabled by default.

You have to create an FTP user account to be able to log on to the FTP connection.

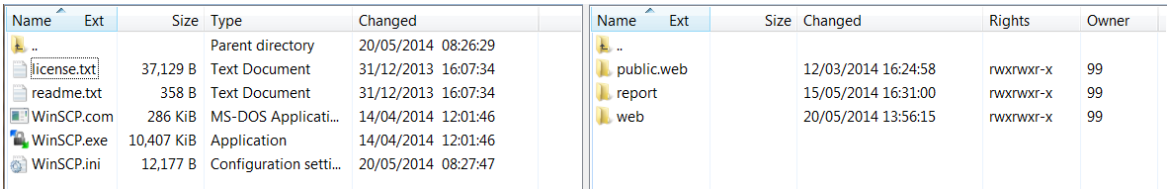
You must have an FTP client to be able to connect to the NETA-21. The following screenshots are taken from WinSCP, but you can have another client, too.



When you configure the FTP connection, you have to specify the protocol, the URL (or IP address) of the NETA-21 and the username and password of the FTP account.

If you choose the FTP protocol with No encryption, the default port number is 21. If you choose the FTP protocol with TLS Explicit encryption, the default port number is 990. You can customize the ports under **Network services**.

When you have logged on to the FTP connection, the you see two panes listing the files on a local computer and the content of the SD memory card.



You can move files from one pane to another with the drag and drop feature.

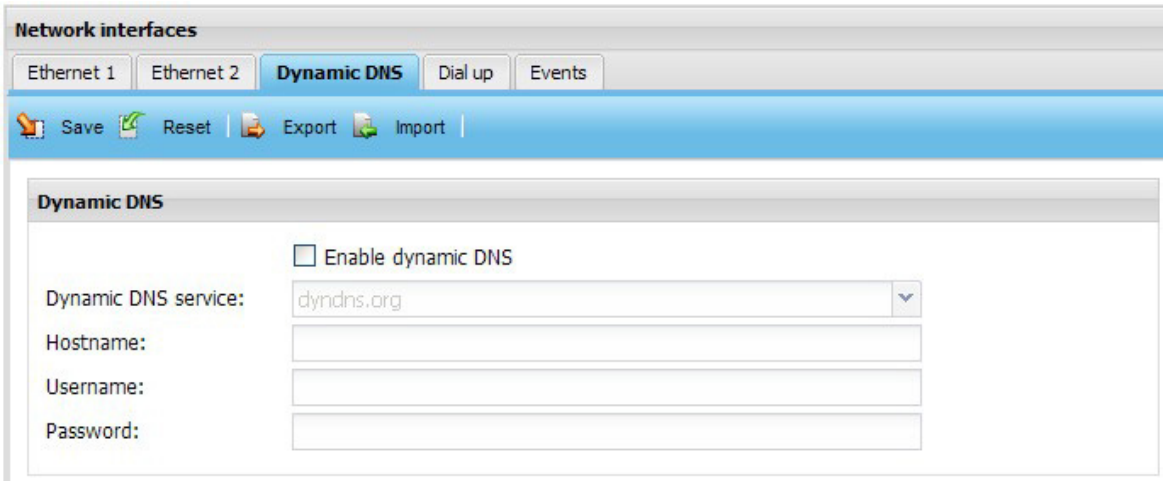
Dynamic DNS

The NETA-21 provides support for the Dynamic domain name system (DDNS).

The Dynamic DNS service is useful when you have to access the NETA-21 with a dynamic IP, for example, when the NETA-21 is located in an isolated region where the only network access is through a 3G modem.

Using the Dynamic DNS service

1. Go to **Settings –> Network interfaces –> Dynamic DNS**.



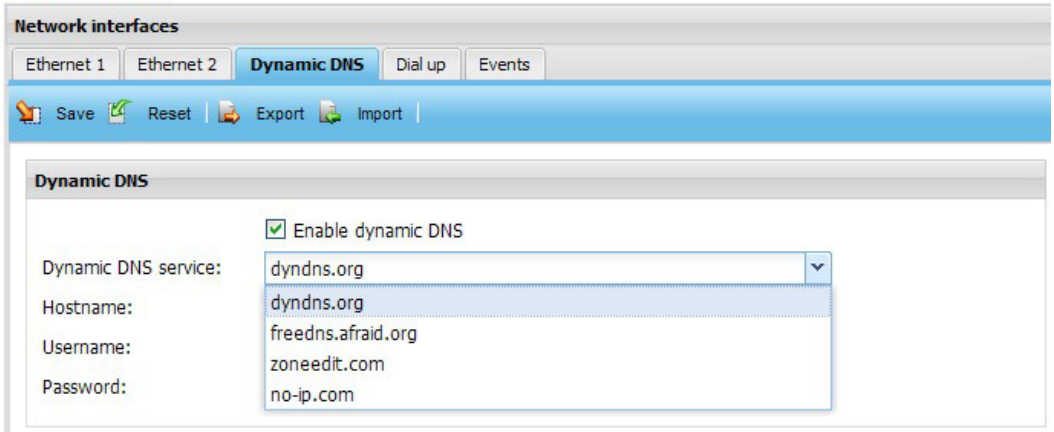
The toolbar of the **Dynamic DNS** tab contains the following buttons:

- **Save** button saves the user configuration to the NETA-21.

  No external file is generated.
- **Reset** button discards all changes you have made and resets the fields to default values.
- **Export** button exports the DDNS settings to a local file.
- **Import** button imports the previously exported DDNS settings from a file to the UI.

2. Select the **Enable dynamic DNS** check box.
3. Fill in the following text boxes:
   - **Dynamic DNS service:** contains a list of all DNS service providers that can be used.

     After you have registered to one of the supported Dynamic DNS service providers, you get a host name, user name and password.



- **Hostname:** is the name assigned to the NETA-21.
  Host name must be registered at the selected service provider.
- **Username:** defines the user name for the DDNS service.
- **Password:** defines the password for the DDNS service.

Now you can access the NETA-21 web interface by using the registered host name.

For example, if you have registered to the dyndns.org service with host name “my-neta-21”, you can access the NETA-21 with address “my-neta-21.dyndns.org”.

Dial-up function

In isolated regions, the mobile broadband may be the only way to have an Internet connection. With the dial-up function you can use a USB 3G modem for establishing an Internet connection to the NETA-21 via the USB port (see section *Layout of the NETA-21 and the NEXA-21*).

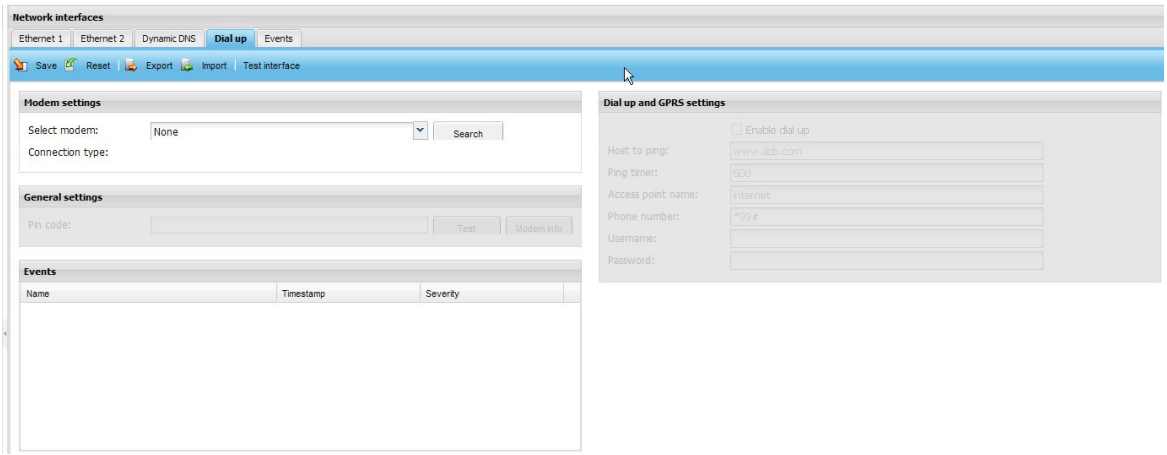
Note: The NETA-21 searches for connected modems via the USB. The modems connected to the USB port of the NEXA-21 are not detected. The modem must support either GPRS, EDGE or 3G connections.

The following USB modem models are verified to function correctly with NETA-21:

- Huawei E153
- Huawei E3131 (non-HiLink version)
- Huawei K3715
- Telewell HSPA USB 3G modem
- Vodafone K4505
- ZTE K3565-Z
- D-Link DWM-222 4G LTE USB adapter.

Other modems may be detected by the NETA-21 but have not been tested for compatibility. For example, the connection establishment may not be reliable with untested modems. The USB modems acting as an Ethernet adapter to a PC (USB modems which provide a web UI) are not compatible with the NETA-21.

The dial-up function is located on the **Dial up** tab under **Network interfaces**.



The toolbar contains the following buttons:

- **Save** button saves the changes to the NETA-21.
- **Reset** button discards all changes you have made.
- **Export** button exports the modem settings to a local file.
- **Import** button imports the modem settings from a file to the UI.
- **Test interface** does the ping test with a defined URL.

The **Modem settings** panel contains the following components:

- **Select modem** is a drop-down list for selecting the installed modem.
- **Connection type** shows the connection type of a modem.
- **Search** button detects the installed USB modems.

The **General settings** panel contains the following components:

- **Pin code** text box is for the PIN of a SIM card.
- **Test** button verifies the PIN.
- **Modem info** button provides additional information about the modem.

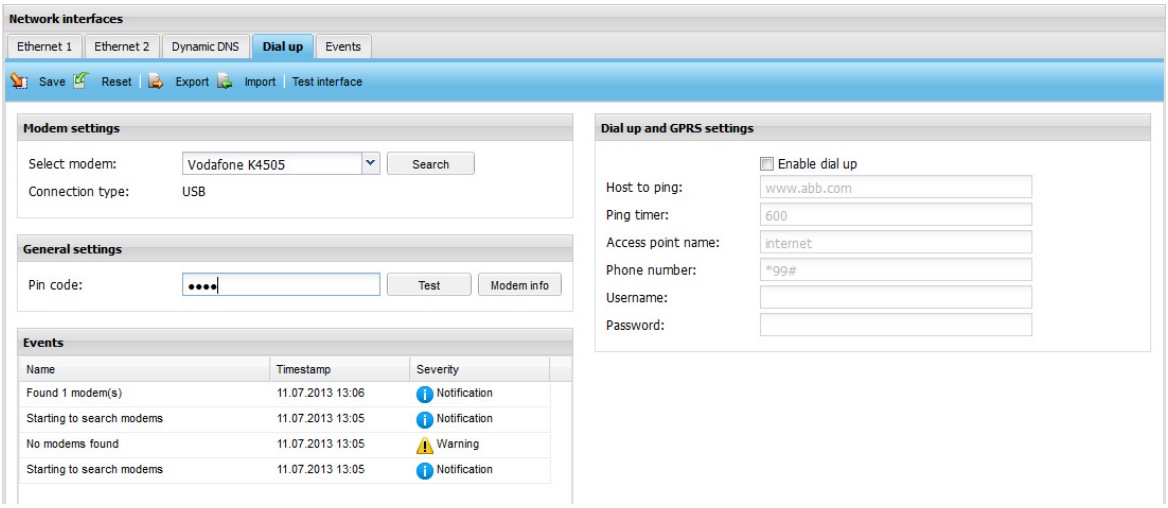
The **Dial up and GPRS settings** panel contains the following components:

- **Enable dial up** is a check box for selecting the dial-up function.
- **Host to ping** is a text box for the defined URL needed in a ping test.
- **Ping timer** is a text box for defining the PING operation delay.
- **Access point name** is a text box for defining the access point name of the provider to access the Internet
- **Phone number** is a text box for a phone number.
- **Username** is a text box for the user name needed if the modem service is enabled.
- **Password** is a text box for the password needed if the modem service is enabled.

Using a mobile broadband connection

1. Plug the USB 3G modem into the USB port.
   Note: If a USB cable is used to connect USB modem to NETA-21, make sure that the length of the USB cable does not exceed 3 meters.
2. Go to **Settings –> Network interfaces –> Dial up**.
3. Select the modem from the **Select modem** drop-down list.

If the modem is not already available in the list, click the **Search** button.



4. Select the **Enable dial up** check box.
5. Type all necessary information in the **Dial up and GPRS settings** panel.
6. Click the **Save** button.
7. Click the **Events** tab to check that the Internet connection has been established.

12

Events

What this chapter contains

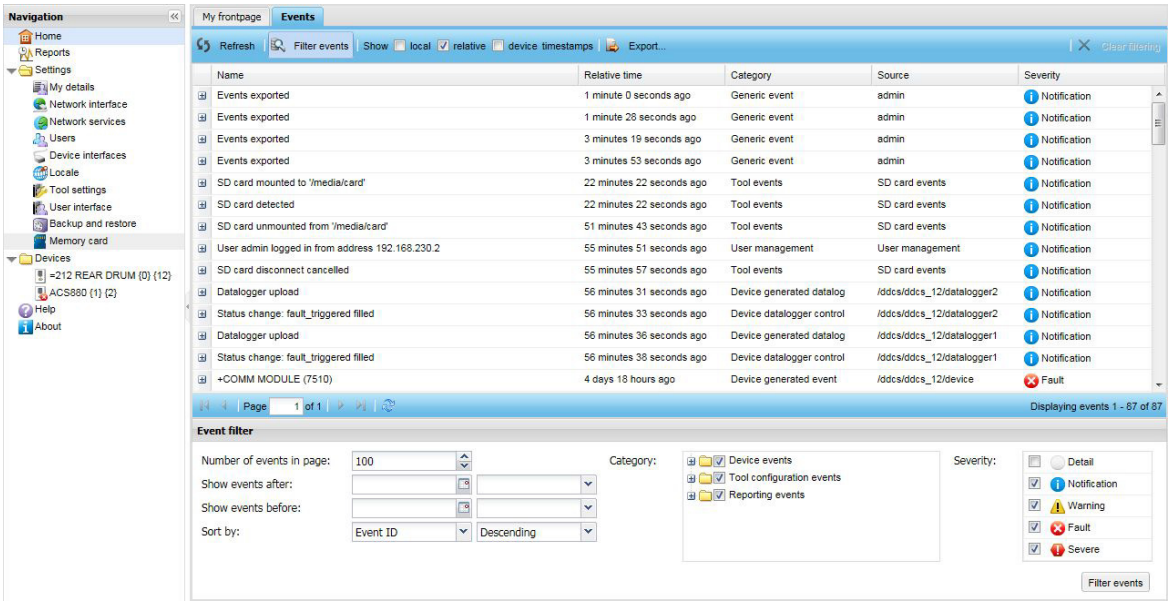
This chapter describes how to observe and filter events.

Universal event list

The **Event** tab is virtually omnipresent in the UI. The contents of the tab may vary slightly in different views. The following figure shows the **Event** tab under **Home**. This tab shows all events.

The past events of the monitored device are grayed out.

By default all events are sorted by the occurrence of the event. Device events, however, are sorted by the device-specific time.



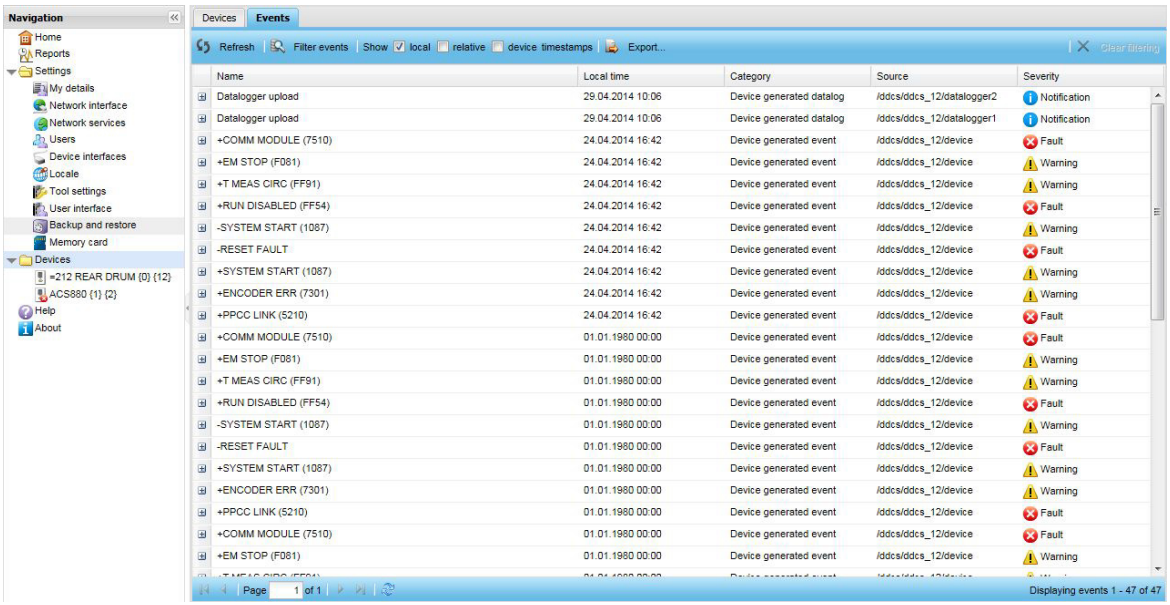
The tab contains the following components:

- **Refresh** button updates the contents of the tab.
- **Filter events** button opens and closes the **Event filter** panel at the bottom of the view.
- **Show local/relative/device timestamp** check boxes add columns showing the local/relative/device time for the events:
  - **Local time** column shows all time values according to the local time of the NETA-21
  - **Relative time** column shows all time values in a relative format, for example 3 days 3 hours ago
  - **Device time** shows all time values according to the time set in the device.
- **Export** button exports all the events and data logger data to a .ZIP file.
- **Clear filtering** button clears any filtering that has been performed for the event list. This button will be disabled if no events have been filtered. Filtering is available by clicking on event list column titles.

  Note: Filtering is applied only on the web browser side and for the visible (usually 100 latest) events only. Filtering can empty the event list even if there were matched events in the event storage of the NETA-21 (in an older event history).

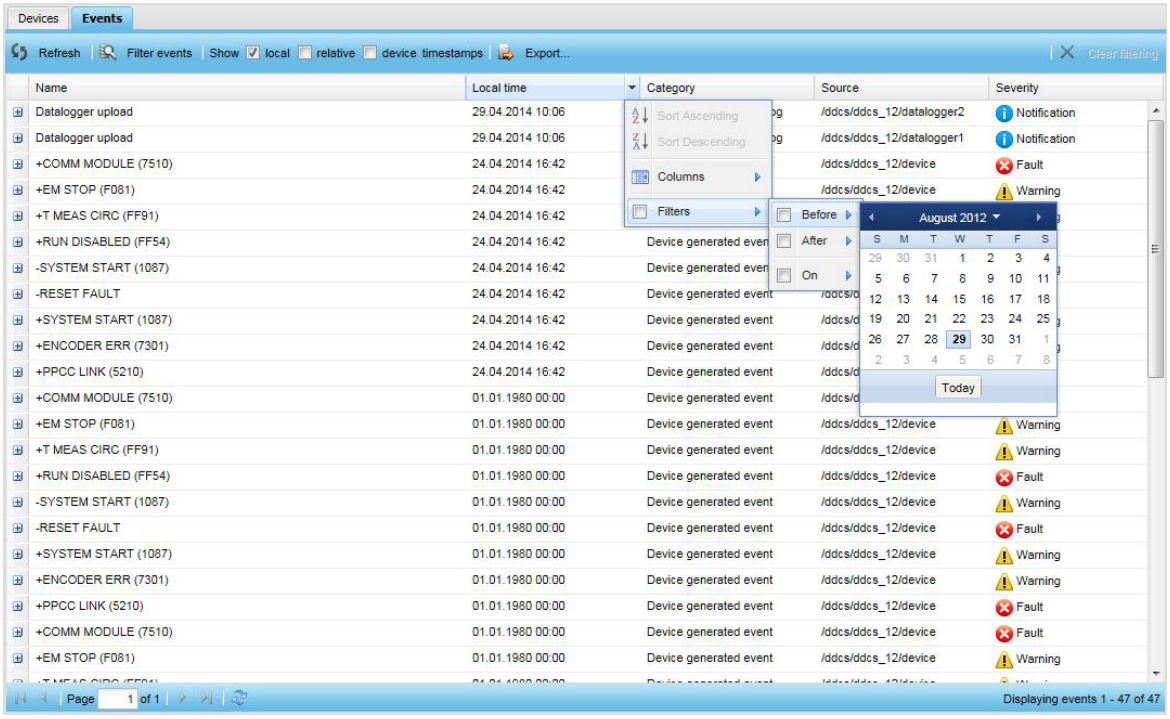
Contents of the non-universal event list

The non-universal event lists do not show all events. For example, the **Event** tab under **Devices** shows only device-related events.



Filtering settings by columns

The filtering criteria can be set separately for each column. In the heading row of the event list there are arrow icons opening a menu for setting the filtering criteria for each column.

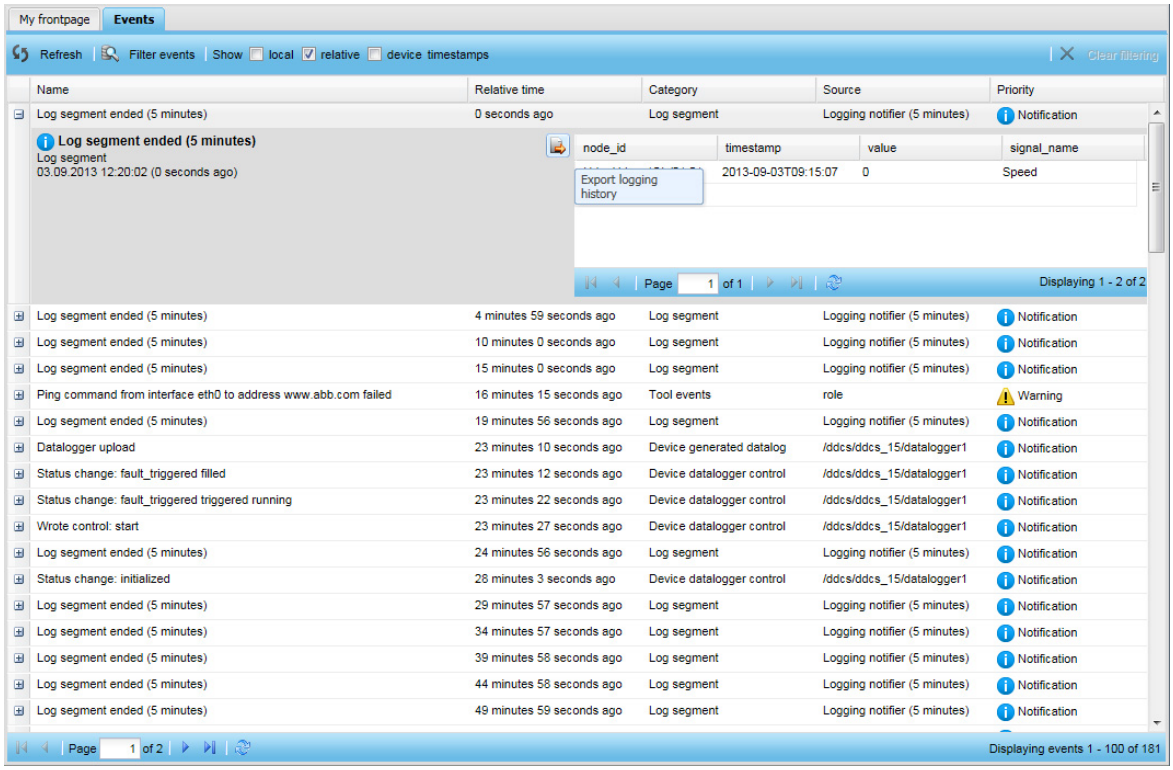


The event list contains the following column headings:

- **Event ID** column shows the event ID number. The column can be sorted with a numeric filter (less or more than or equal to the event ID number). The column is not visible by default.
- **Name** column shows the event name. A balloon icon is shown if the event contains comments. The column can be sorted with a search text box.
- **Local time** column shows when the event has happened. Device events are synchronized with the NETA-21 clock.
- **Relative time** column shows how much time has passed since the event has happened. You can use the following filters: **Before**, **After** or **On**.
- **Device time** column shows the event time from the device itself.

  The device time can represent a run time counter for some drives. The device time is only available for faults and warnings originating from a monitored device.
- **Category** column shows the event category. The column can be sorted with a search text box.
- **Source** column shows the source of the event. The column can be sorted with a search text box.
- **Severity** column defines the severity (or type) of the event. The menu has the following filtering criteria: **Detail**, **Notification**, **Warning**, **Fault** and **Severe**.

If there is an attachment for the event, the attachment can be exported by clicking the icon with an orange arrow.

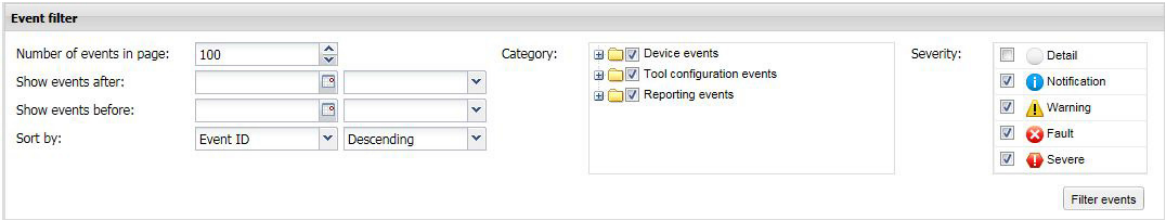


To select the page, use the toolbar at the bottom of the **Event** tab.

Filtering settings through the Event filter panel

The event list can be sorted by defining the filtering criteria with the **Event filter** panel.The **Event filter** panel is opened by clicking the **Filter events** button.

Note: The **Event filter** panel provides more accurate search results than column filter and search options, because it initiates a search within the web UI server. Column filters only search within the visible data items (for example the 100 latest events).



The **Event filter** panel contains the following components:

- **Number of events in page** spin box defines the number of events shown in a single page. The values can range from 10 to 200. The default value is 100.
- **Show events after** has two boxes with which the date and time can be defined for events occurring after the selected timestamp. The boxes can be empty.
- **Show events before** has two boxes with which the date and time can be defined for events occurring before the selected timestamp. The boxes can be empty.
- **Sort by** drop-down lists define the sorting column and sorting direction. The default setting is Event ID in ascending order. The latest added events appear at the top of the event list, even if the event timestamps are not in chronological order.

  The first **Sort by** drop-down list contains the following items:
  - Event ID
  - Starting time
  - Category
  - Severity.

  The second drop-down list contains the following items:
  - Ascending
  - Descending.
- **Category** box contains all available categories with check boxes. The categories have sub-categories. The categories are selected and unselected by clicking the check boxes. Under **Settings** the **Category** box in the **Event filter** panel shows only the pre-defined categories. In general all the categories are shown and selected by default.
- **Severity** box contains the types of events with check boxes. The icon representing the severity of the event is shown next to the text. By default, all types are selected except **Detail**. If no type is selected, the types are not prioritized at all. The box contains the following types:
  - Detail
  - Notification
  - Warning
  - Fault
  - Severe
- **Filter events** button makes the query to the server. After the query has succeeded, the **Event filter** panel is hidden and the list of events is updated. If events do not fit to

a single page, the toolbar at the bottom of the **Event** tab can be used for changing pages.

13

Reporting

What this chapter contains

This chapter describes how to make reporting and trend logging settings for configuring which time levels and event categories are sent out by a reporting plug-in.

The tabs under **Reports** are described from left to right.

Introduction to reporting

With the NETA-21, reporting means that parameter values or event data of a drive or several drives connected to the NETA-21 are sent periodically to the users. The NETA-21 reporting provides many ways to save or send the report. The NETA-21 supports the following reporting methods:

- Email reporting – reports are sent via email
- SD card reporting – reports are saved to an SD card
- FTP reporting - reports are transferred to an FTP server.
- SMS reporting - reports are sent as SMS messages.

The NETA-21 can be configured to send reports based on triggers. The triggers can be time intervals, values of some parameters or drive events such as faults or warnings.

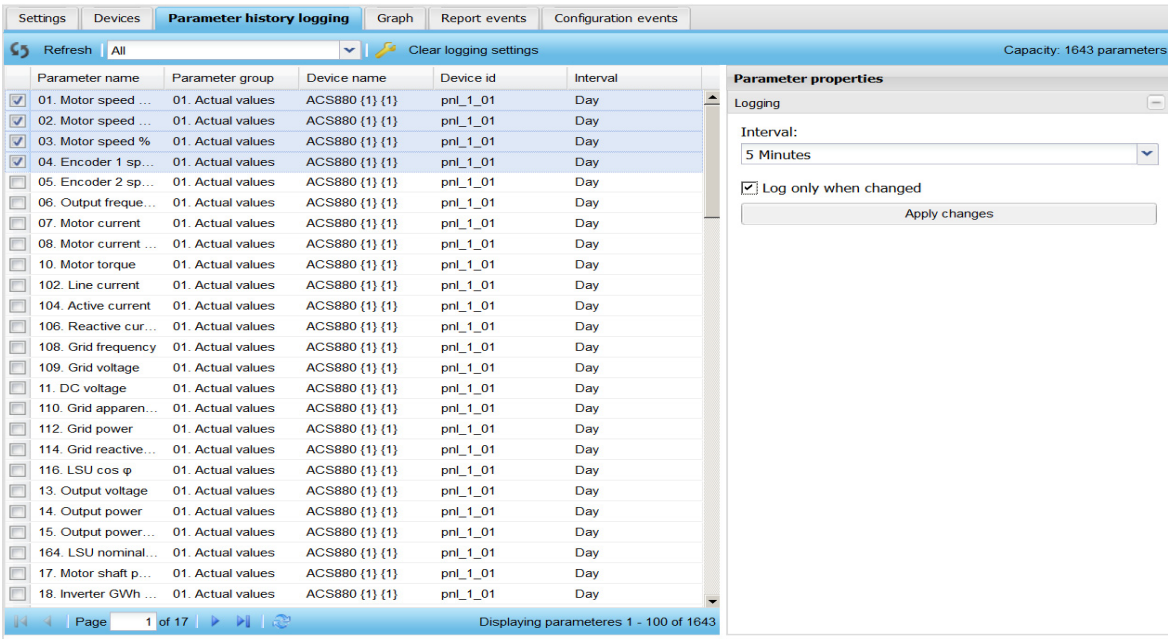
For example, it is possible to save all or some parameter values periodically to an SD card or to upload them to an FTP server. In addition, you can configure the NETA-21 to send emails when a drive enters a faulted state. By default the NETA-21 stores all changed parameters and drive events to an SD card daily.

In email reporting it is possible to create a custom report format.

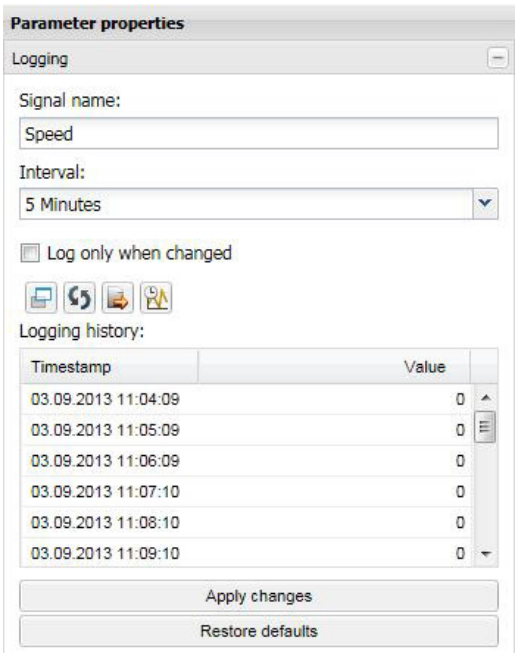
Configuring the NETA-21 for reporting

To configure the NETA-21 for reporting, specify the logging intervals of the parameters needed in the report:

1. Go to **Reports –> Parameter history logging**.



2. Click a parameter and select the interval in the **Parameter properties** panel.



The following intervals are available:

- Day
- Hour
- 5 Minutes
- Minute
- Continuous monitor
- None (in other words, no logging)

The Continuous monitor logging interval was added in firmware 2.20.

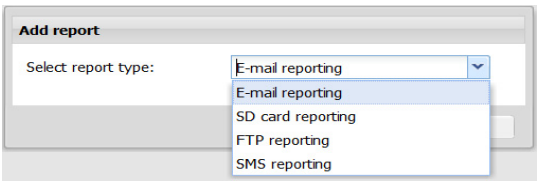
If you want to set the intervals for several parameters simultaneously, go to **Reports –> Parameter history logging –> Parameter properties –> Interval**. For more information, see *Parameter logging interval templates*.

Creating an email report

To be able to use the email reporting, you must configure the SMTP settings. See section *Network services*.

Make sure that you have set the logging intervals for the parameters (**Reports –> History logger**). If you have not set the logging intervals for the parameters, the reports will have no data.

1. Go to **Reports –> Settings** and click the **Add** button.
2. Select **E-mail reporting** from the drop-down list.

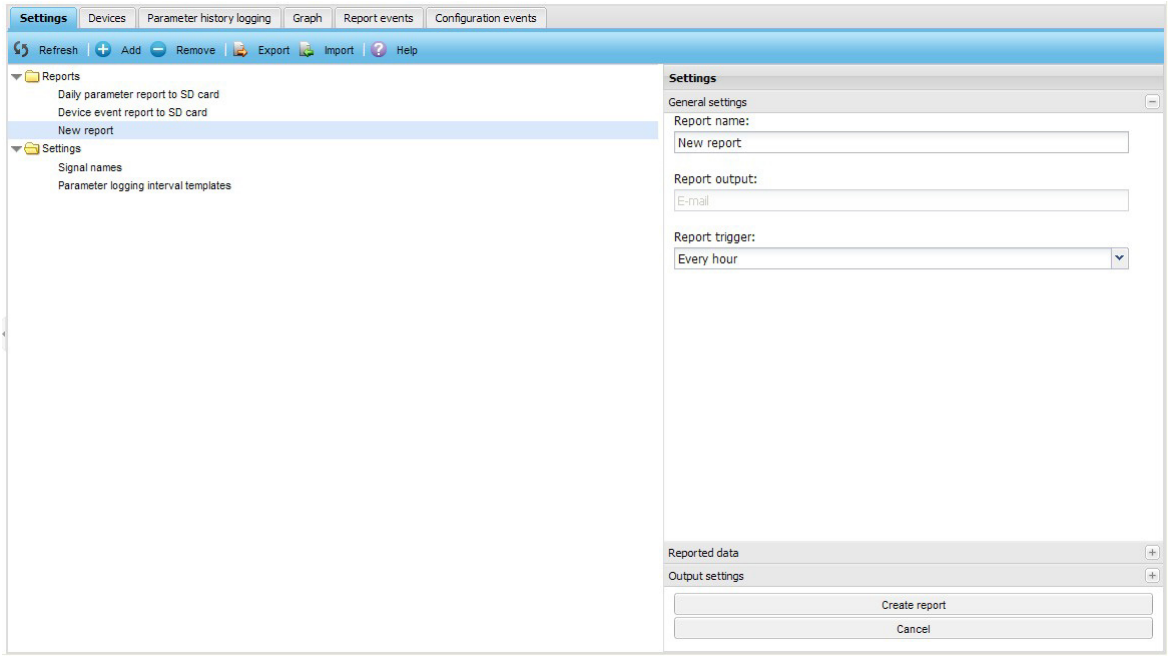


   Now the new report has been added to the list of reports.

3. Define the general settings of the report, such as report name and reporting trigger. See section *Setting the report trigger*.
4. When you have named the report and selected the trigger, click the **Reported data** sub-panel.

   Here you can select the data to be reported. See *Setting the reported data*.

5. Click the **Output settings** sub-panel and define the settings.



- **Enable report** is a check box for enabling the email reporting.
- **Report output format** is a list for defining the template used in the report.
- **From address** is a text box for defining the sender.

- **To address** is a tex box for defining the email recipient.

  To send an email to several recipients, separate the email addresses with a comma or semicolon.
- **E-mail subject** is a text box for defining the subject of the email.
- **Site identifier (default: serial no. of tool)** is a text box for defining the identifier used in the reports.

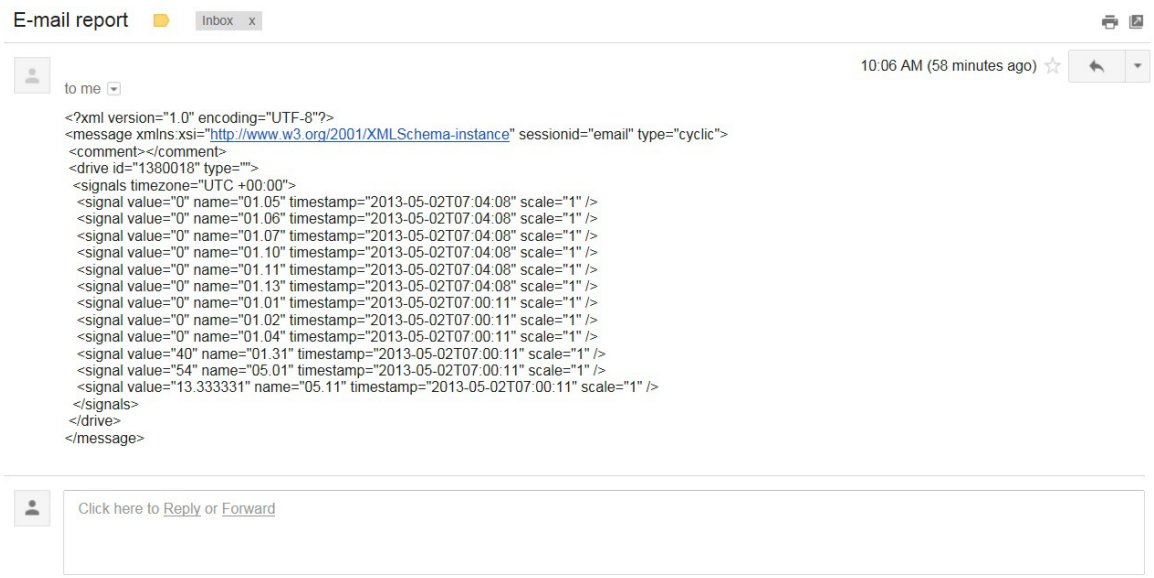
6. Click the **Create report** button.

   To check that the report has been successfully sent, go to **Reports –> Report events**. If no report has been sent, check the network and email settings.

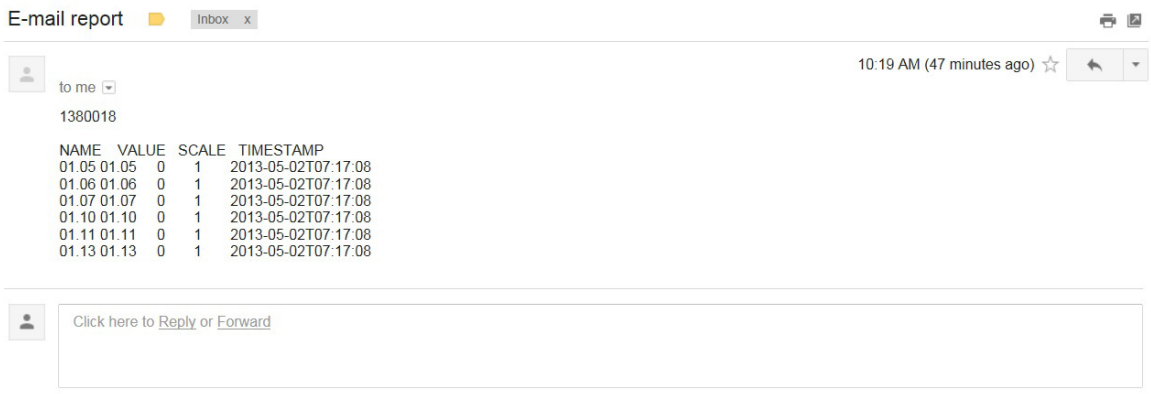
Format of the email report

The reported data is shown in the email message body.

If you have selected an XML format, the email report looks like the following example:



If you have selected a plain text format, the email report looks like the following example:



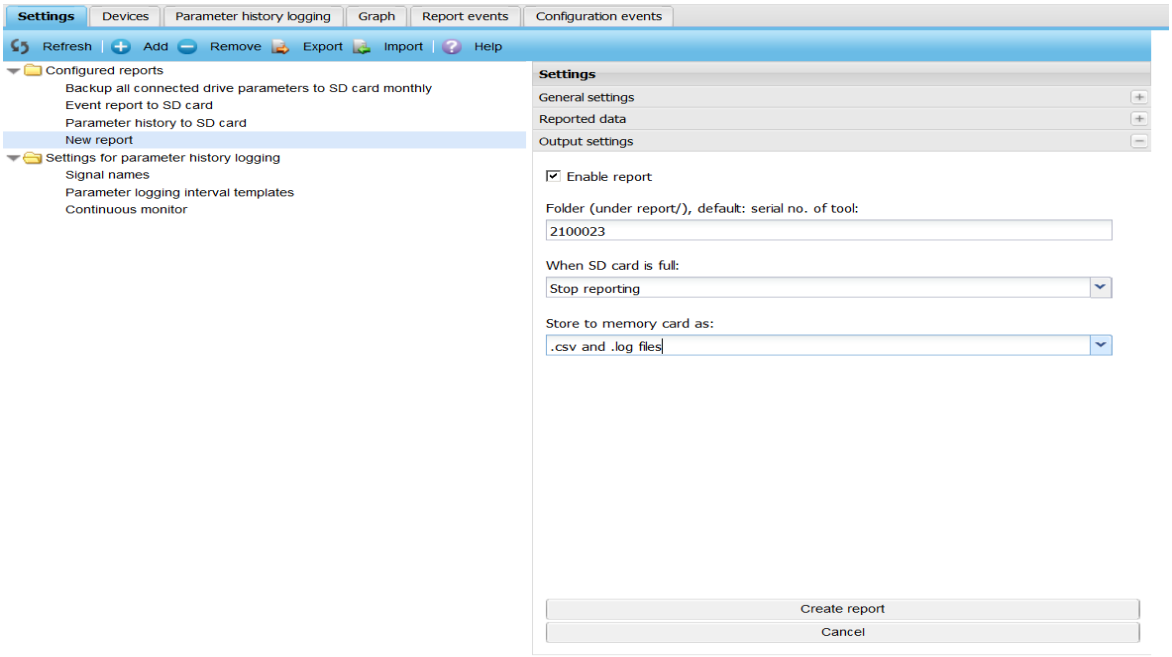
You can create a custom format by using the report scripting section in an email report. For more information, see section *Using scripting for email reports (custom report)*.

Creating an SD card report

The NETA-21 contains three default reports: **Parameter history to SD card**, **Event report to SD card** and **Backup all connected drive parameters to SD card monthly**. These reports update values.db and events.db databases to the SD card when new data is logged (before firmware 2.22, .csv and .log files were stored daily by default). You can modify or remove pre-defined reports or define additional reports to the SD card.

Make sure that you have set the logging intervals for the parameters (**Reports –> History logger**). If you have not set the logging intervals for the parameters, the reports will have no data.

1. Go to **Reports –> Settings** and click the **Add** button.
2. Select **SD card reporting** from the drop-down list.
   Now the new report has been added to the list of reports.
3. Define the general settings of the report, such as report name and reporting trigger. See section *Setting the report trigger*.
4. When you have named the report and selected the trigger, click the **Reported data** sub-panel.
   Here you can select the data to be reported. See *Setting the reported data*.
5. Click the **Output settings** sub-panel and define the settings.



- **Enable report** is a check box enabling the SD card reporting.
- **Folder path** is a text box for specifying the location of the reports on the SD card. If there is no folder, it will be created automatically. The default folder path is the serial number of the NETA-21.
- **Cleaning of SD card** is a list for enabling the cleaning of an SD card when the SD card is full or, alternatively, for stopping the reporting.

- **Store to memory card as** is a selection list for specifying the formats to save reported data and events. The available options are:

  .csv and.log files

  .db database (SQLite)

6. Click the **Create report** button.

   To check that the report has been successfully sent, go to **Reports –> Report events**.

   Note: If the report does not appear on the SD card, check that the SD card is not full.

Format of an SD card report

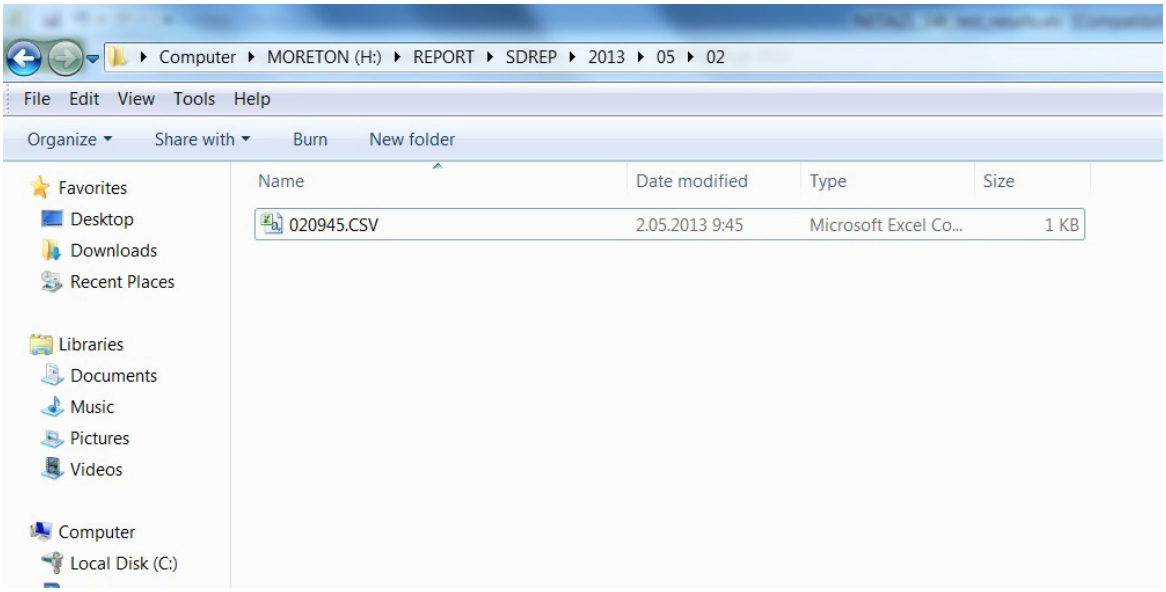
SD card reports can be stored in the CSV or SQLite format.

From firmware version 2.22 onwards, the SD card reports are in the SQLite format. SQLite files with parameter values have extension .DB and event data reports have extension .log (or .evt in earlier firmware revisions prior to firmware revision 2.20).

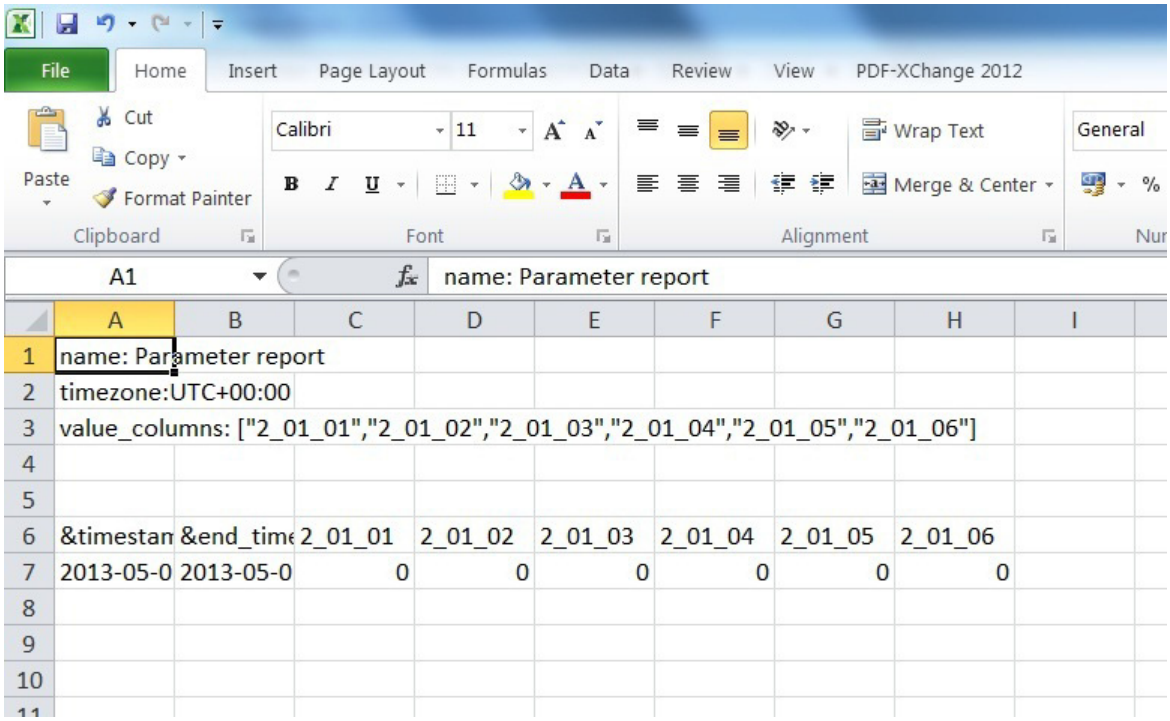
Until firmware version 2.21, the SD card reports were in the CSV format. CSV files with parameter values have extension .CSV.

CSV-formatted reports

Each report is created in a sub-folder of the folder specified in the Output settings sub-panel. The folder structure is: SD:/report/Folder path in Output settings/Year/Month/Day/. The report file names on the SD card follow format <ddhhmm>[_<n>] where <ddmmss> indicates the day of the month, hours and minutes. An optional numeric posfix "_1", "_2", "_3" ... "10", "11" ... "99" is added if multiple log files are written during one minute.



The SD card report for logged data looks like in the following example. An event report looks similar except that there are more event-specific columns beginning with an ampersand “&”.



DB-formatted reports

SQLite files have extension .db. You can view the content of the files with any SQLite file viewer, for example, with **SQLite Database Browser**. You can also use **SQLite Manager** as an extension for the Firefox web browser.

The SQLite file looks different for an events report and a parameters report.

The SQlite file of an events report is always stored to a file named events.sb and contains the following kind of data:.

event_id	timestamp	original_time	end_time	archived_timestamp	category_id	category	severity	text_id	text	content	code	description	attachment_path	source	device_id	acked
1	2017-01-2...			2014-05-15T07:38:0...	2	Data Ac...	2	da_start	Core mo...	['2.22.0.0']				Data Ac...		0
2	2017-01-2...			2014-05-15T07:38:0...	31	Device i...	2	Panel bu...	Panel bu...	[]				Panel bu...	interface	0
3	2017-01-2...			2014-05-15T07:38:0...	31	Device i...	2	DDCS a...	DDCS a...	[]				DDCS ev...	interface	0
4	2017-01-2...			2014-05-15T07:38:0...	30	Device d...	2	PNL2 wir...	PNL2 wir...	[]				Panel bu...	interface	0
5	2017-01-2...			2014-05-15T07:38:0...	30	Device d...	2	PNL1 De...	PNL1 De...	[]				Panel bu...	interface	0
6	2017-01-2...			2014-05-15T07:38:0...	30	Device d...	1	New dev...	New dev...	[]				Panel bu...	interface	0
7	2017-01-2...			2014-05-15T07:38:0...	13	User ma...	2	um_li_succ	User ad...	['admin',...				User ma...		0
8	2017-01-2...			2014-05-15T07:38:0...	31	Device i...	2	Ethernet...	Ethernet...	[]				Ethernet...	interface	0
9	2014-05-1...			2014-05-15T07:38:0...	15	Network...	2	ntp_minus	Time an...	['847901...				Operatin...	locale	0

The SQLite file of a parameters report contains three tables: **parameters, sqlite_sequence** and **value_cache**.

The **parameters** table contains the list of parameters stored in the report.

id	node_id	signal_name
1	/pnl/pnl_1_01/v/01.01	101_01_01_motor_speed_used
2	/pnl/pnl_1_01/v/01.02	101_01_02_motor_speed_estimated
3	/pnl/pnl_1_01/v/01.04	101_01_04_encoder_1_speed_filtered
4	/pnl/pnl_1_01/v/01.05	101_01_05_encoder_2_speed_filtered

The **value_cache** table contains the values read for the parameters.

rowid	parameter_id	timestamp	value	type
1	4	1484944921955000	0	2
2	3	1484944921921000	0	2
3	2	1484944921887000	0	2
4	1	1484944921722000	0	2
5	4	1484944982235000	0	2
6	3	1484944982201000	0	2
7	2	1484944982167000	0	2
8	1	1484944982132000	0	2

Note: The timestamp column indicates time in microseconds since the 1st of January 1970 (so called Unix time except with microsecond precision).

Creating an FTP report

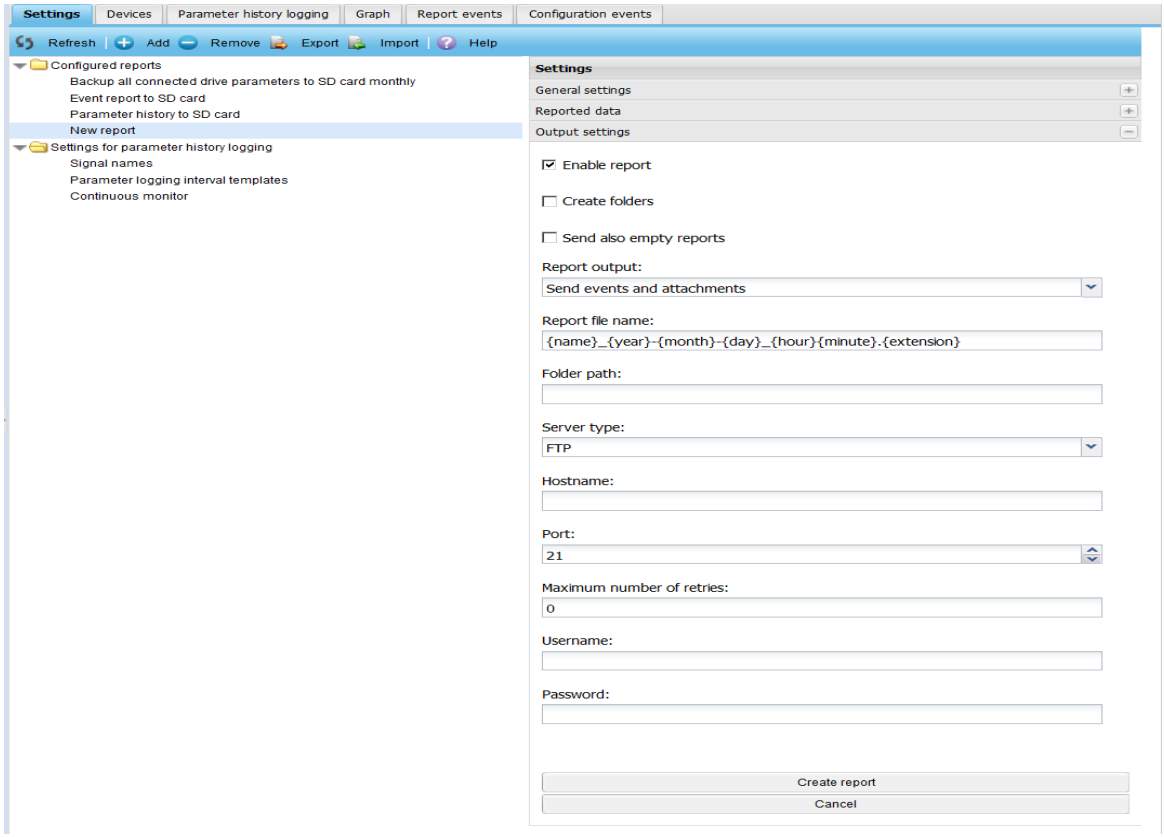
Make sure that you have set the logging intervals for the parameters (**Reports –> History logger**). If you have not set the logging intervals for the parameters, the reports will have no data.

1. Go to **Reports –> Settings** and click the **Add** button.
2. Select **FTP reporting** from the drop-down list.

   Now the new report has been added to the list of reports.
3. Define the general settings of the report, such as report name and reporting trigger. See section *Setting the report trigger*.
4. When you have named the report and selected the trigger, click the **Reported data** sub-panel.

Here you can select the data to be reported. See *Setting the reported data*.

5. Click the **Output settings** sub-panel and define the settings.



- **Enable report** is a check box enabling the FTP reporting.
- **Create folders** is check box for enabling the creation of a new folder.
- **Send also empty reports** is a check box to allow sending of reports even when there hasn't been any change to report.
- **Report output** is a selection list which specifies content of the report. Available options are:

  Send events and attachments

  Send only events

  Send only attachments
- **Report file name** is a text box for defining file name of the report.
- **Folder path** is a text box for defining the path to the folder in which the report is created.

It is highly recommended to use secure FTPS protocol always. FTP uses insecure protocol which transmits data and passwords without any encryption. This can increase proneness to cybersecurity attacks and unauthorized access.

- **Server type** is a selection list to specify the type of the server where the reports will be sent. Available options are:

  FTP
  FTPS
- **Hostname** is a text box for the address of the host provider.
- **Port** is a list for setting the port via which the FTP connection is carried out.
- **Number of retries** is a list for defining the number of retries during communication breaks.
- **Username** is a text box for the name of the account user.
- **Password** is a text box for the password needed to a verified connection.

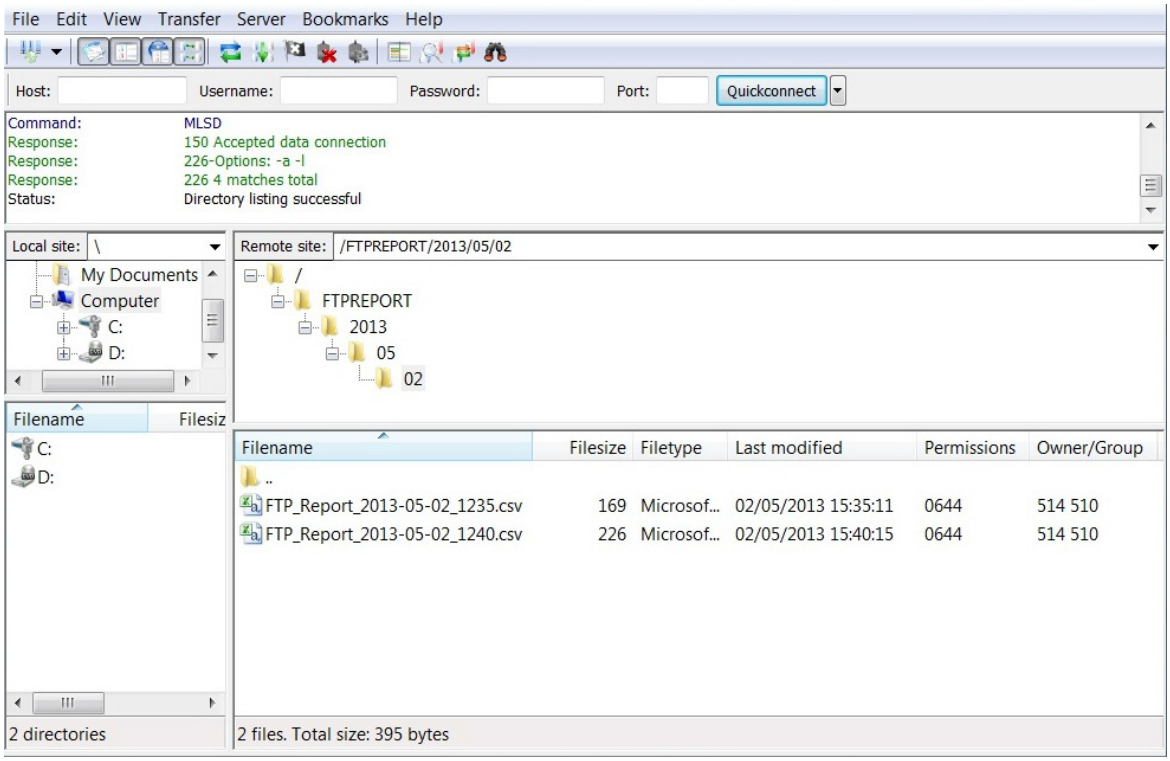
6. Click the **Create report** button.

   To check that the report has been successfully sent, go to **Reports –> Reported data**.

Format of an FTP report

The FTP reports are in the CSV format. CSV files with parameter values have extension .CSV and event data reports have extension .log (or .evt prior to firmware revision 2.20).

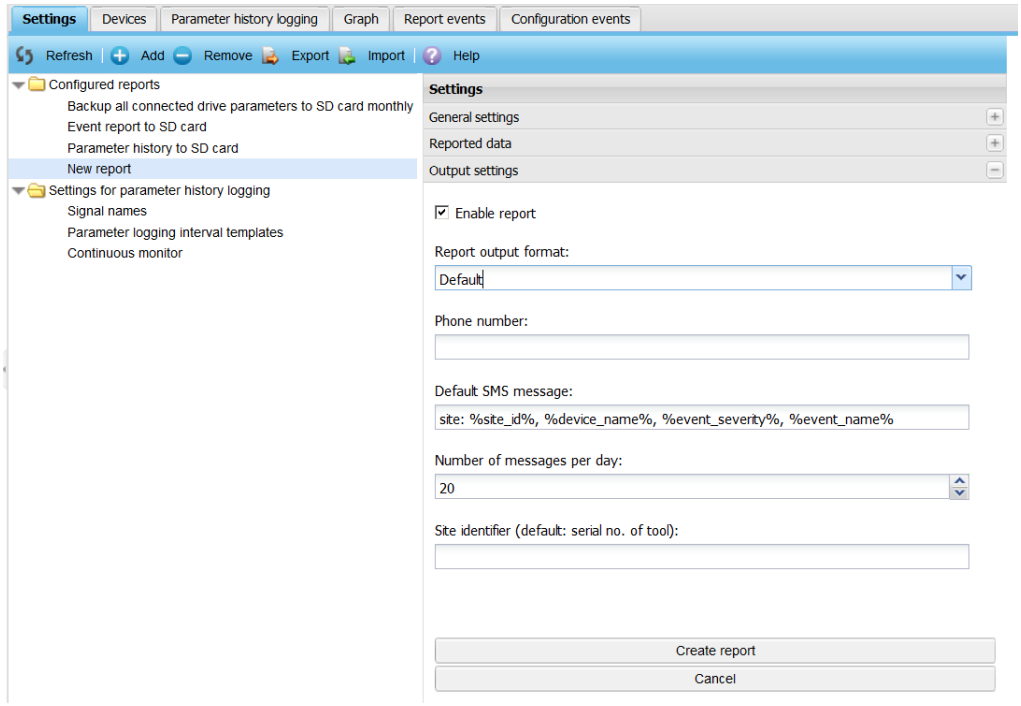
Each report is created in a sub-folder of the folder specified in the Output settings sub-panel. The folder structure is: /Folder path in Output settings/Year/Month/Day/. Each report has a unique name with a time stamp.



Creating SMS report

Make sure that you have set the logging intervals for the parameters (**Reports –> History logger**). If you have not set the logging intervals for the parameters, the reports will have no data.

1. Go to **Reports –> Settings** and click the **Add** button.
2. Select **SMS reporting** from the drop-down list.
   The new report is added to the list of reports.
3. Define the general settings of the report, such as report name and reporting trigger. See section *Setting the report trigger*.
4. Click the **Reported data** sub-panel and select the data to be reported. See *Setting the reported data*.
5. Click the **Output settings** sub-panel and define the settings.



- **Enable report** is a check box to enable the SMS reporting.
- **Report output format** is a selection list which specifies the format of the report. Available options are:

  Default

  Custom - Enables report scripting. For details about Report scripting, see chapter *Using scripting for SMS reports (custom report)* on page *152*.
- **Phone number** is a text box to specify the phone number to which reports needs to be sent.
- **Default SMS message** is a text box to specify the format of the report message. The default message uses certain variables from the predefined SMS report script.
- **Number of messages per day** is a list to define the maximum number of SMS messages per day, which is limited to 100.
- **Site identifier** is a text box to define the optional name for the site. By default, the serial number of NETA-21 is added as site identifier.

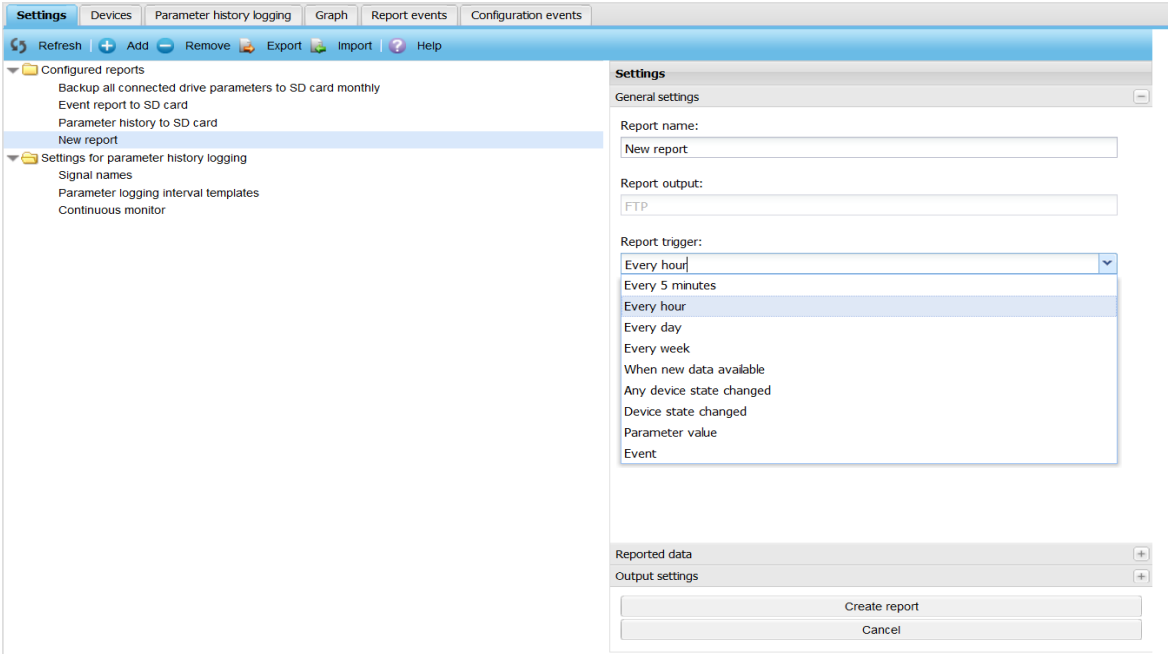
6. Click the **Create report** button.

To check that the report has been successfully sent, go to **Reports –> Report events**.

If no report has been sent, check the network and SMS settings.

Setting the report trigger

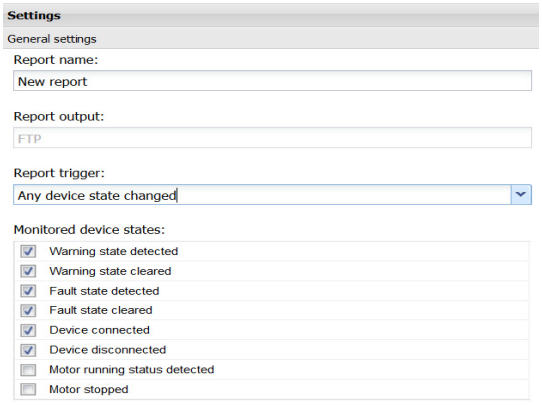
1. To define the report trigger, go to **Reports –> Settings –> Reports –> New report –> General settings**.



2. From the **Report trigger** list, select the frequency for the report generation:
   - Every 5 minutes
   - Every hour
   - Every day
   - Every week
   - When new data available

     Parameter has a new value or there is a new event.
   - Any device state changed

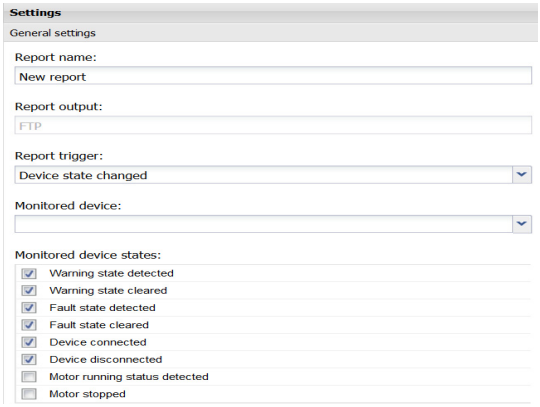
     Status of any of the drives has changed.



Note: You can select the statuses to be monitored.

- Device state changed

  Status of a particular drive has changed.

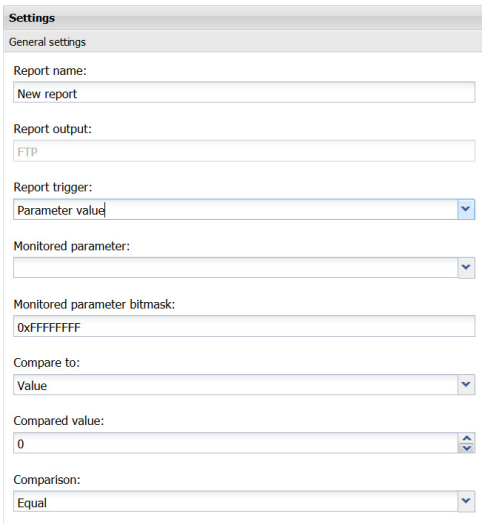


  Note: You can select the drive to be monitored.

- Parameter value

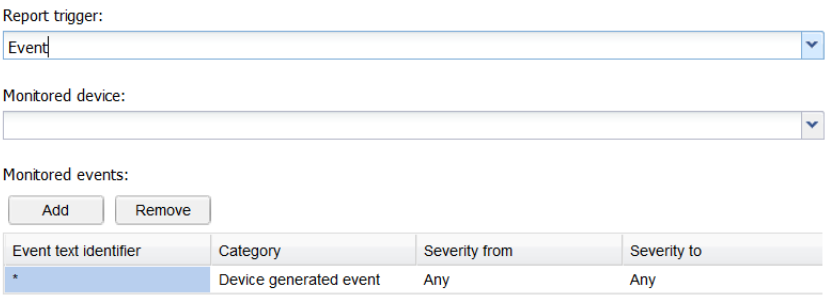
  Value or another parameter can be specified as a basis for comparison.

  Bitmask is ANDed to the original value before comparison.



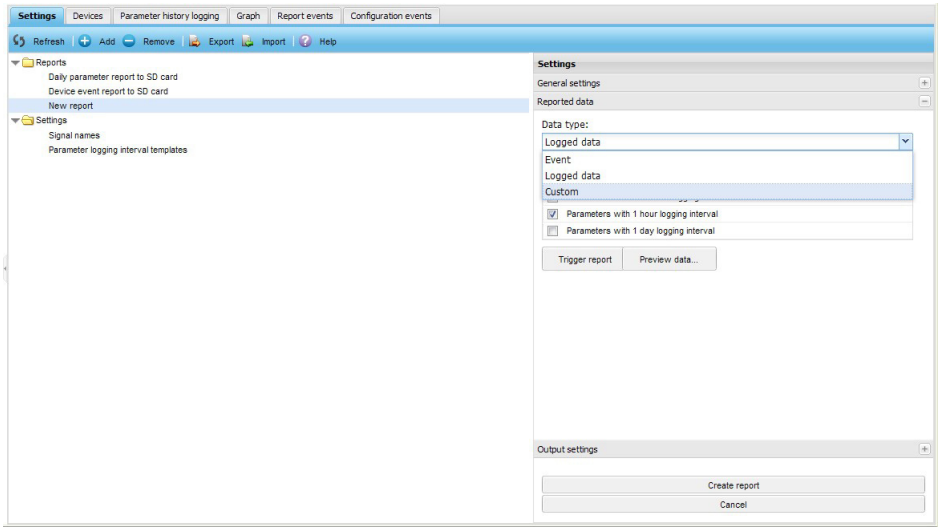
- Event

  Name, category and severity of an event can be specified as a basis for comparison.



Setting the reported data

1. To define the data type for the reports, go to **Reports –> Settings –> Reports –> New report –> Reported data**.
2. From the **Data type** drop-down list, select the desired data type.



The available Data type options are:

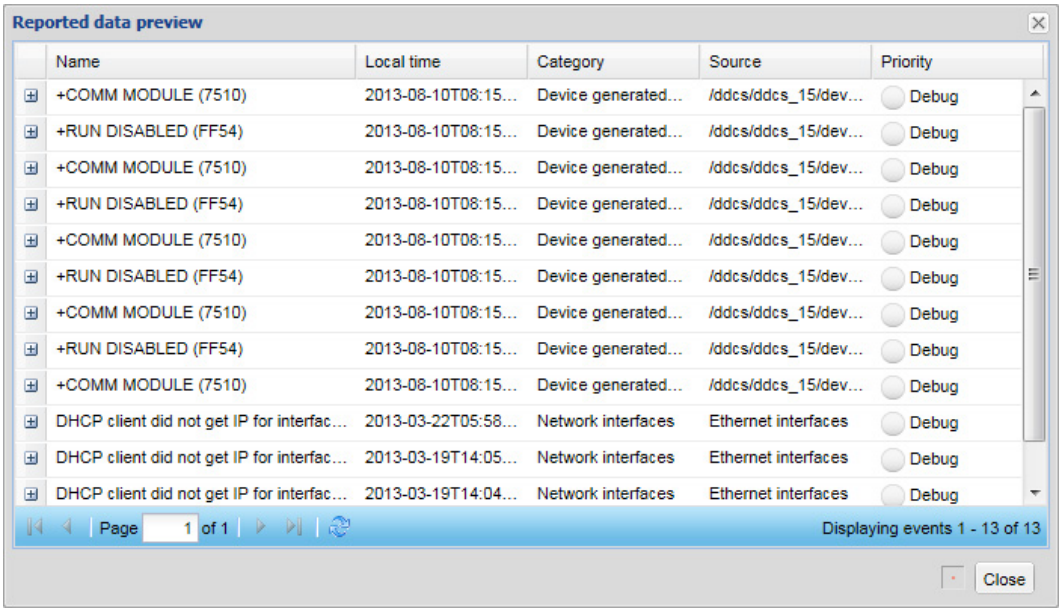
- **Event** - To report events according to severity and category.
- **Logged data** - To report all parameters according to the logging interval defined in section *Configuring the NETA-21 for reporting*.
- **Custom -** To specify the custom data from the **Reported custom data** list.

From the **Reported custom data** drop-down list, select the desired Reported custom data type:

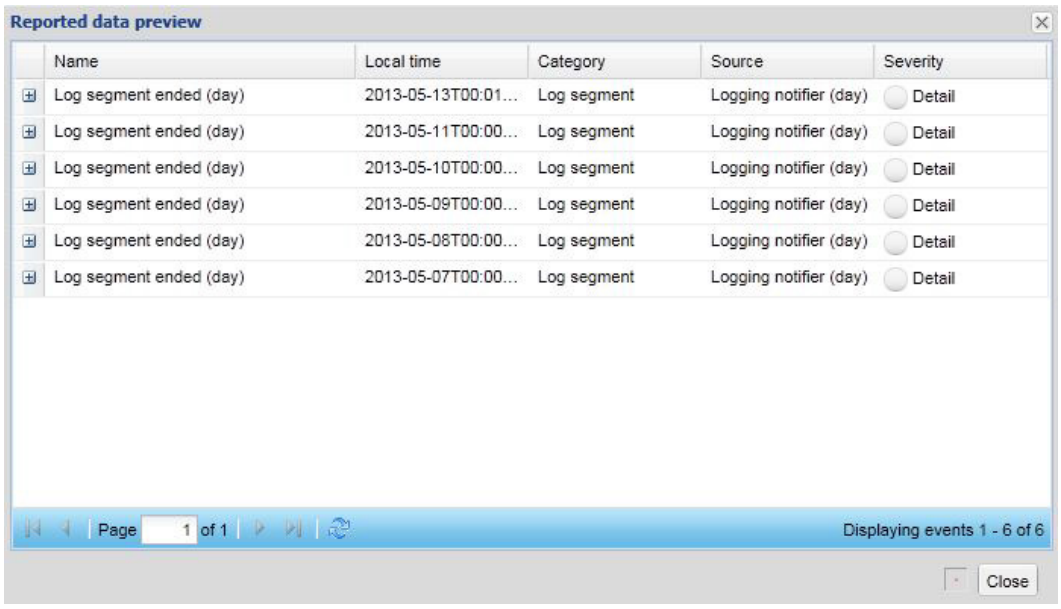
The available options are:

- **Customized report script** - To report an event of a given severity with a specified name every time the event occurs, and optionally allows you to define your own reporting script.
- **Parameter export** - To report all parameters of a particular drive.
- **Parameter export of all devices** - To report all parameters of all connected drives.
- **Import settings** -To restore the settings defined with the backup and restore function, see chapter *Backup and restore* on page *165*.
- **APBU upload** -To report the selected logger (First, Last, User) data from the APBU logger at the given node id.

3. To preview the contents of the report, click the **Preview data…** button.
   - On selecting the data type **Event**, the content of the report appears as shown in the below figure:



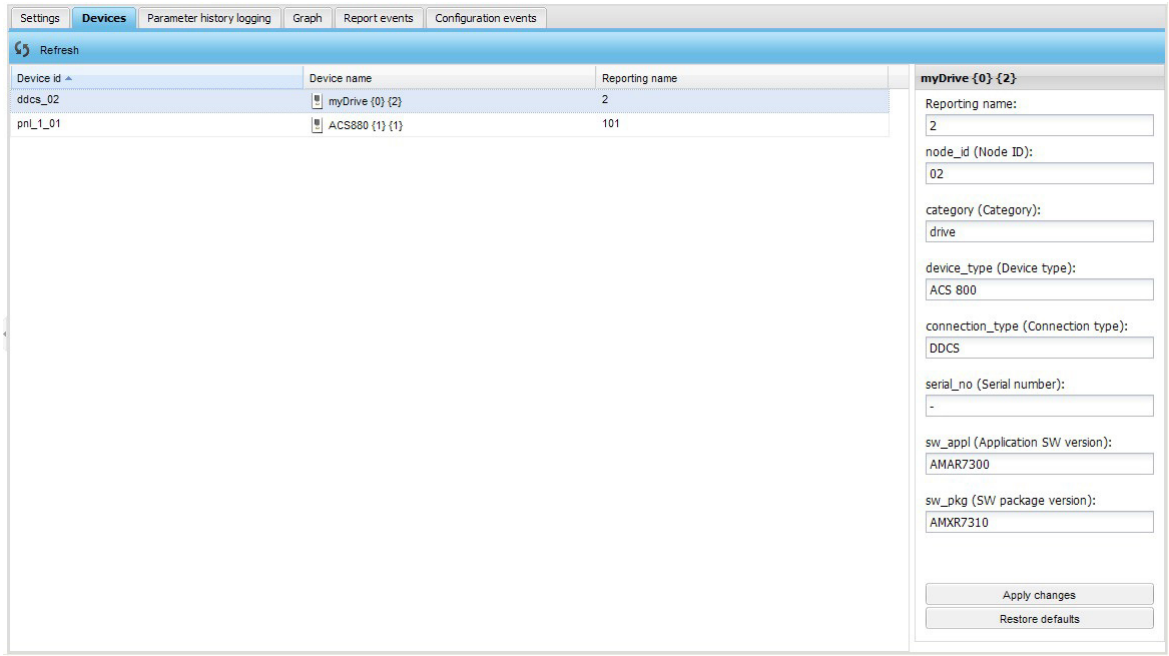
   - On selecting the data type **Logged data**, the content of the report appears as shown in below figure:



Changing the reporting name

You can customize the reporting name for each connected device. The reporting name and the optional reporting name are added as a prefix to the logged signal names, if you have selected so (**Reports –> Settings –> Signal names –> Settings,** see *Changing the default naming of signals*).

1. Go to **Reports–> Devices** and click the row of the device which you want to rename.
2. Type the new name to the **Reporting name** text box.
3. Click **Apply changes**.



To update the device list, click the **Refresh** button.

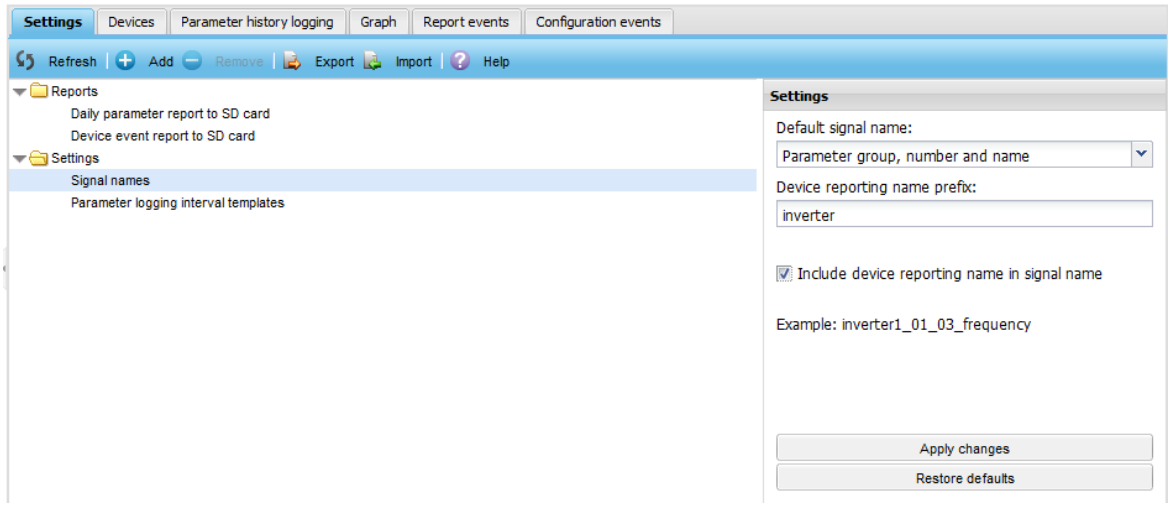
From firmware version 2.20 onwards, you can customize also other device-specific reporting attributes, for example the serial number and device type. Editable attributes depend on a specific device.

Changing the default naming of signals

There are two locations where you can manually name each trend-logged parameter value: Parameter browser tab under each monitored device and **History logging** tab under **Reports**.

If you have not typed in any customized name for the trend-logged variables, the default naming is used for the parameters.

1. To define how the NETA-21 names the trend-logging variables by default, go to **Reports –> Settings–> Signal names –> Settings**.



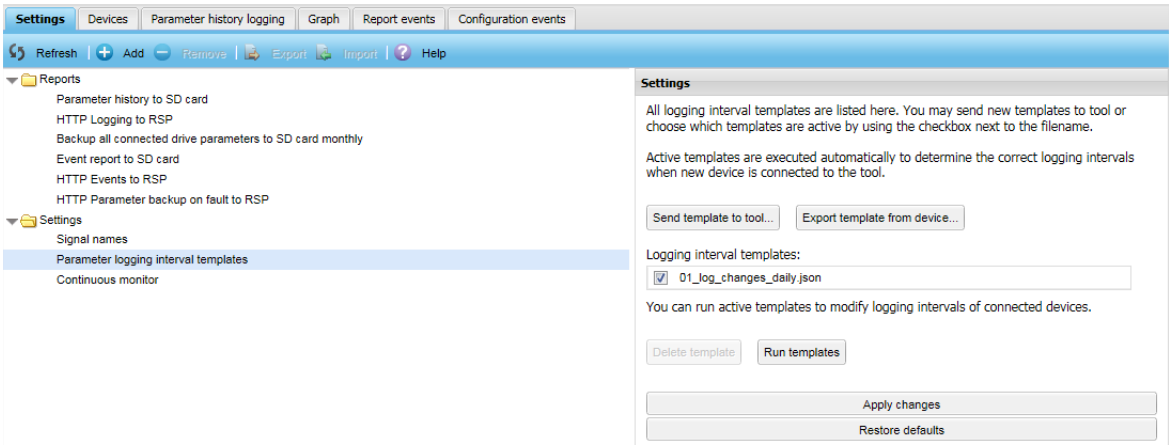
2. From the **Default signal name** list, select one of the following options:
   - **Group and parameter number** provides the parameter with a name such as "03_02" (default setting prior to firmware version 2.20)
   - **Parameter name** provides the parameter with a name such as "main_status_word"
   - **Parameter group, number and name** is a combination of the two options above, for example, 03_03_main_status_word (default setting from firmware revision 2.20 onwards).
3. Optionally, define a prefix for each device reporting name in the **Device reporting name prefix** text box.
4. If you select the **Include device reporting name in default signal name** check box, the device reporting name set under **Devices** tab is prefixed to the signal name.

   The example of the default name is shown in the **Settings** panel.

Parameter logging interval templates

Use log intervals (**Reports –> Settings –> Parameter logging interval templates -> Settings –> Logging interval templates)** to modify the logging intervals of multiple parameters simultaneously instead of modifying the logging interval of parameters one by one via the **Parameter history logging** tab.

With the log intervals function you can also bulk-change certain other attributes related to parameters and reporting such as the reported parameter names and only the **Log only when changed** selection on the parameter specific logging settings. All available logging interval templates are matched to all connected monitored device parameters when the **Apply changes** button is clicked. Templates are applied to newly connected devices also when any new monitored device is connected to the NETA-21 (and after the device interface has been reset to the default settings).



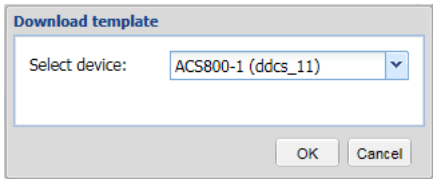
Use the **Send template to tool…** button to save a new template file to the NETA-21.

Under the **Logging interval templates** heading you can see the list of saved templates. If you click the **Run templates** button, you can check some of the saved templates.

The **Delete template** button deletes the currently focused template file from the NETA-21.

The **Run templates** button runs the selected templates (all template files on the Logging interval templates list which have been selected).

From firmware 2.22 onwards there is also a button to option **Export template from device…** which shows a pop-up window with a drop-down list of all connected drives:



Select a device and click **OK** to export the currently selected configuration settings for the parameter logging from the connected device into a file on a PC. The file can be edited and imported (sent) to other NETA-21 tools.

A sample content of a logging interval template file is shown below:

```
{
    "device_attributes": {
        "<attribute>": "<attribute_value>",
        "<attribute>": "<attribute_value>"
        …
    },
    "rules": [
        {
            "param_id": "<param_value>",
            "unit": "<unit_value>",
            "interval": "<interval_value>",
            "signal_name": "<signal_value>",
            "log_only_when_changed": <log_value>
        }, …
    ]
}
```

- **device_attributes** is a list of drive attributes that determine the drives to which the template is applied.
  - Possible attributes are: **category** for the category of the device, **sw_pkg** for the SW package, **sw_appl** for the SW application.
  - Values for these attributes are usually shown on the device front page and you can use wild cards, for example, *(asterisk).
  - If you do not specify any attributes, the template is applied to all devices.
- **rules** is a list of rules that define the parameters and values.
- **param_id** defines the index of the logged parameter, eg, "12.34
- **unit** defines the engineering unit of the monitored parameter, eg, "V" or "mA"
- either **param_id**, **unit** or both rules must be specified or the specific rule will not be applied to any parameter.
- **interval**, **signal_name** and **log_only_when_changed** specify values that are applied to the log interval of time, signal name and the **Log only when changed** selection of the previously specified parameters.
  - **interval** can be one of these values: “monitor”, “minute”, “5minutes”, “hour”, “day” and “none”.
  - **signal_name** can be any valid string.
  - **log_only_when_changed** is true or false.
- from firmware 2.23 onwards, you can set **fallback** to true or false. By default the fallback is false. If the fallback is set to true and there is a parameter that does not fit to the primary interval (interval attribute), the NETA-21 tires to set the logging interval of a matching parameter to the next available (lower frequency) interval during the template run. It is possible that all intervals are fully used, in which case the parameter is not logged at all.
- from firmware 2.23 onwards, **priority** can be set to 1 or 2 (default: 2) and the setting is used to define whether the parameter interval setting overrides the intervals in other templates.

The following is an example of the logging intervals template that applies an interval of 1 minute to parameter 01.01:

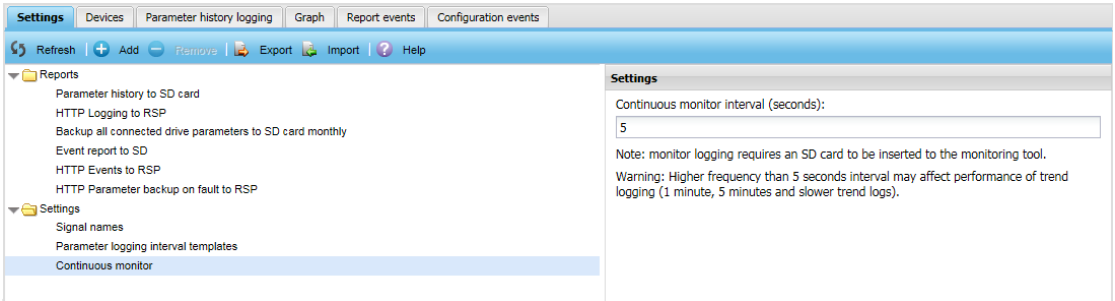
```
{
    "device_attributes": {
        "category": "drive"
    },
    "rules": [
        {
            "param_id": "01.01",
            "interval": "minute"
        }
    ]
}
```

The following is an example of the logging intervals template where the reported signal name of parameter 01.01 is changed to “percentage” only when the unit of the parameter is %:

```
{
    "device_attributes": {
        "category": "drive"
    },
    "rules": [
        {
            "param_id": "01.01",
            "unit": "%",
            "signal_name": "percentage"
        }
    ]
}
```

Changing the continuous monitor interval

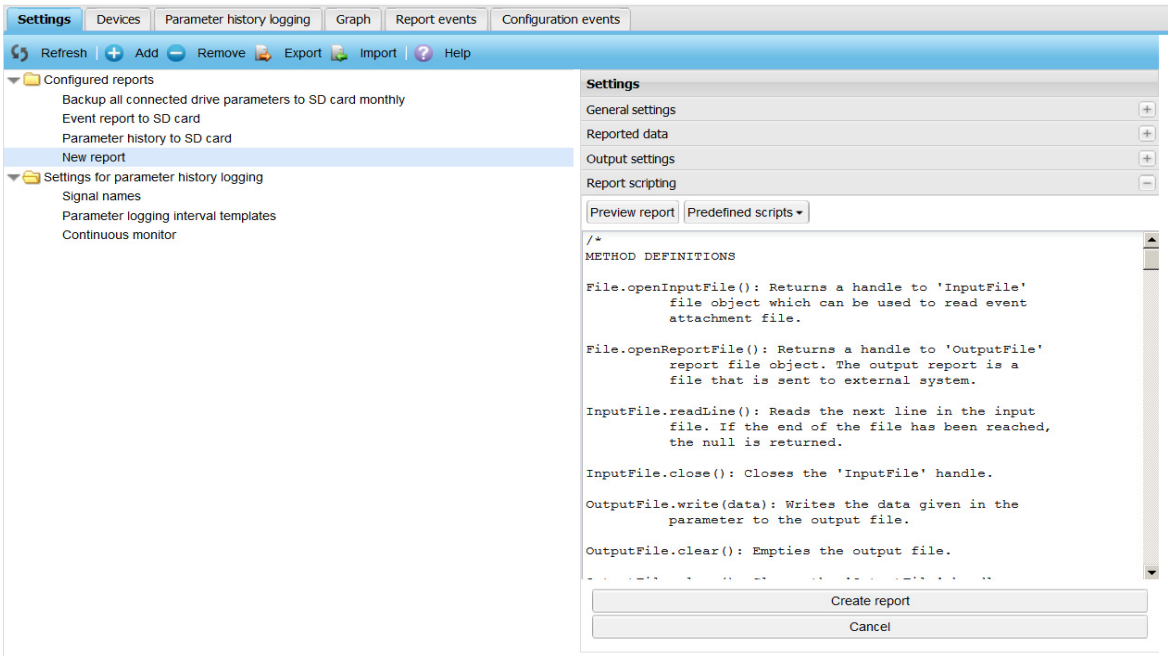
In firmware 2.23 you can configure the default interval for continuously monitored parameters (default: 5 s). You can set the value between 1 s and 30 s. To configure the interval of Continuous monitor logging, go to **Reports -> Settings -> Continuous monitor -> Settings**.



Using scripting for email reports (custom report)

To see the scripting panel of email reports:

1. Go to **Reports –> Settings –> Configured Reports –> New report –> Settings -> Output settings**.
2. Select **Custom** from the **Report output format** drop-down list.
3. Click **Report scripting** sub-panel.



The **Report scripting** sub-panel contains the following components:

- **Preview report** button displays a Preview dialog box which contains a report generated by the currently visible script. The report is generated by using a predefined data. If the script contains an error, an error is displayed in the preview dialog box.
- **Predefined scripts** is a drop-down list with three options: **Custom report**, **XML report** and **Plain text report**. If you select a predefined script from the list, the script editing text box shows that specific predefined script.
- Script editing text box contains a script which is used for generating parameter and event reports. If you have modified the content of a predefined script and want to restore the predefined script, select an appropriate form from the drop-down list and click **Restore defaults**.

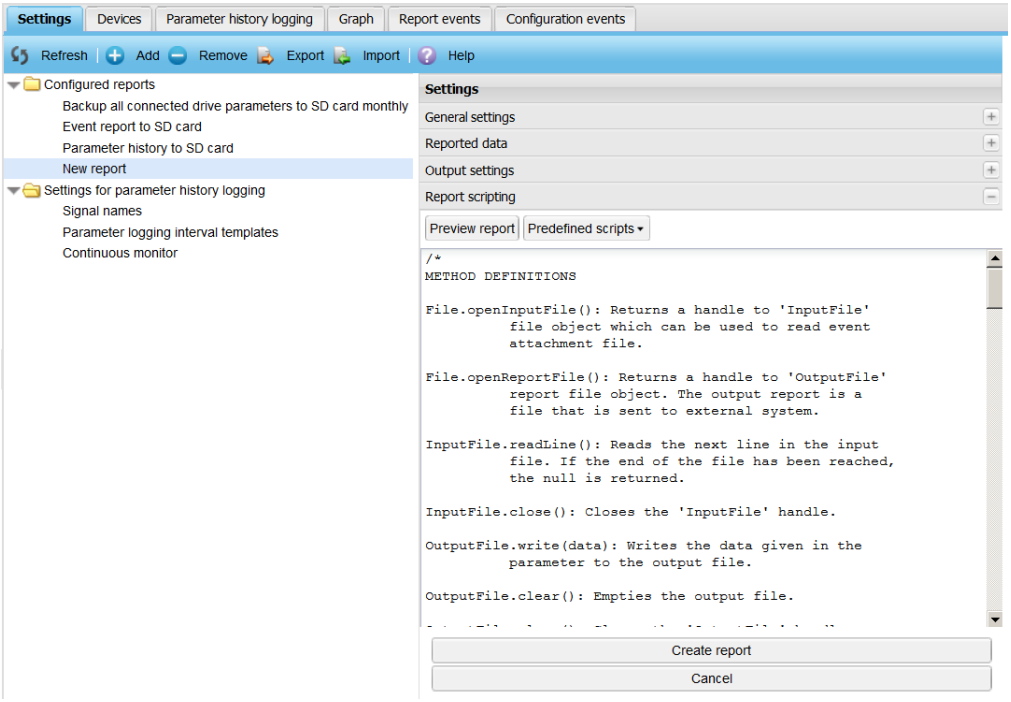
Notes:

- JavaScript language is used to form the email output. You can modify the report scripting code and can use the template scripts to produce XML and CSV formatted outputs.
- Editing an invalid JavaScript code can lead to interruption in reporting. If the reporting freezes completely as a result of an invalid script, you need to restart the NETA-21. Before restarting the NETA-21, choose a pre-defined reporting template and save the report settings.
- You need to use the provided code templates as detailed programming guide on the report scripts is not available.

Using scripting for SMS reports (custom report)

To see the scripting panel of SMS reports:

1. Go to **Reports –> Settings –> Configured Reports –> New report –> Settings -> Output settings**.
2. Select **Custom** from the **Report output format** drop-down list.
3. Click the **Report scripting** sub-panel.



The **Report scripting** sub-panel contains the following components:

- **Preview report** button displays a Preview dialog box which contains a report generated by the currently visible script. The report is generated by using a predefined data. If the script contains an error, the error is displayed in the preview dialog box.
- **Predefined scripts** is a drop-down list and includes **SMS report** option. On selecting the predefined script, the script is displayed in the script editing text box.
- Script editing text box contains the script which is used for generating reports. If you have modified the content of a predefined script and want to restore the predefined script, select the appropriate form from the drop-down list and click **Restore defaults**.

The JavaScript language is used to format the email output. You can modify the report scripting code. Editing of an invalid JavaScript code can lead to stoppage of all reporting. If the reporting freezes completely as a result of an invalid script, you may have to restart the NETA-21. Before restarting the NETA-21, choose a pre-defined reporting template and save the report settings.

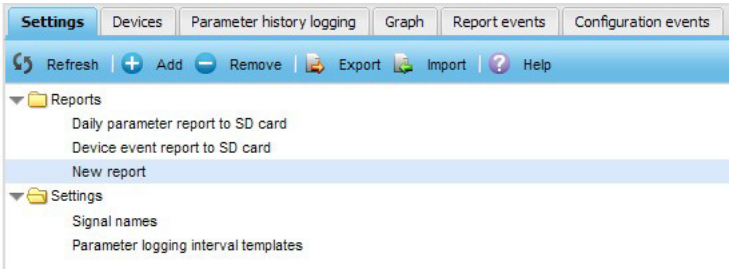
Use the provided code templates, since there is no detailed programming guide on the report scripts available.

Description of the tabs under Reports

There are five tabs under Reports: **Settings**, **Devices**, **Parameter history logging**, **Reported data** and **Configuration events**.

Settings tab

You can define which reporting plug-in is used in reporting when a log segment ends. For information on the customizable reports, see *Introduction to reporting*, *Creating an email report*, *Creating an SD card report* and *Creating an FTP report*.



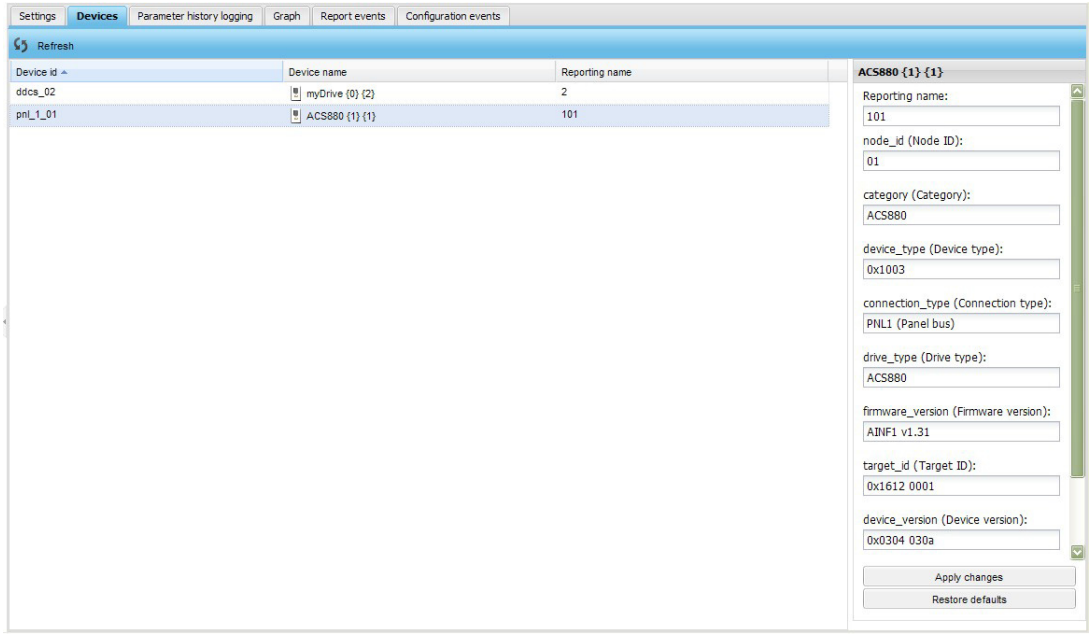
The **Settings** tab contains the following components:

- **Refresh** button refreshes the contents of the parameter list.
- **Add** button adds a new report to the list of reports. The button is enabled only when the **Reports** folder is selected.
- **Remove** button removes the selected report.
- **Export** button downloads the saved settings of the selected report.
- **Editor panel** means the area appearing on the right-hand side of the **Settings** tab when you have selected one of the items on the left-hand side of the **Settings** tab.
- **Import** button imports a report from a file to the NETA-21. If the imported report has the same name as an existing report in the NETA-21, then the report in the NETA-21 is overwritten with the file.
- **Help** button opens a dialog box providing information about the settings of the view.
- **Tree structure** shows all active reports and available settings. When an item is selected, the **Settings** panel appears on the right-hand side of the **Settings** tab.

Devices tab

On the **Devices** tab, you can see all connected devices. There are the following three columns:

- **Device id**: the internal name of a device.
- **Device name**: the name assigned to a device.
- **Reporting name**: the name used in reports for a device.

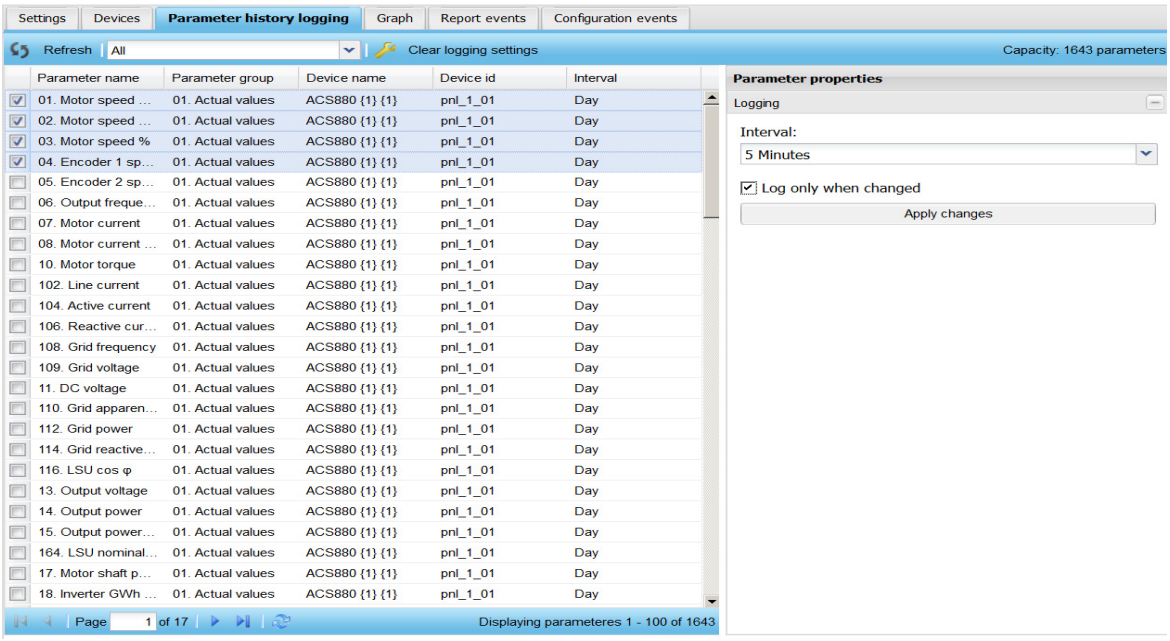


If you click a device, you can customize the reporting name of the device in a right-hand side panel. From firmware version 2.20 onwards, you can customize also other device-specific reporting attributes.

Use the **Refresh** button to refresh the device list.

Parameter history logging tab

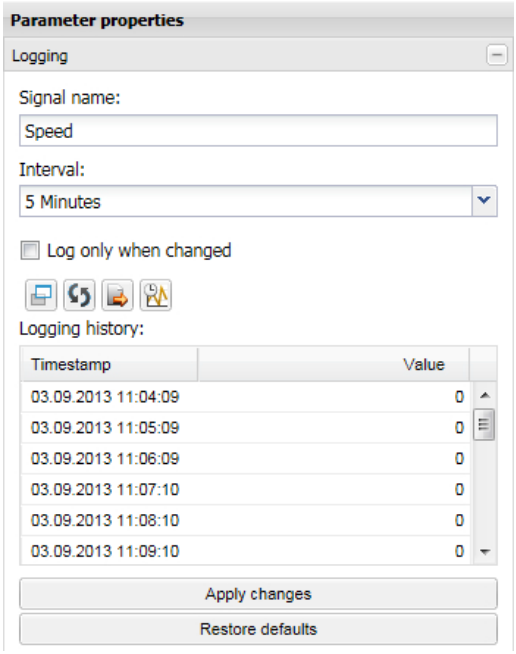
The **Parameter history logging** tab shows the drive signals to be reported. By default all signals are checked for changes daily. Only changes are saved and reported to the SD card.



The tab contains the following components:

- **Refresh** button refreshes the contents of the parameter list.
- **Interval selection** drop-down list shows the logging intervals.When you select an interval, the contents of the parameter list are updated. The following intervals are available:
  - All
  - Minute
  - 5 minutes
  - Hour
  - Day
  - Continuous monitor.
- **Capacity** shows the number of parameters in the selected interval. The maximum number of allowed monitored parameters per time interval are as follows:
  - 1 minute – max. 100 parameters
  - 5 minutes – max. 500 parameters
  - 1 hour – max. 1000 parameters
  - Day – max. 10000 parameters
  - Continuous monitor – max. 20 parameters.

- **Parameter list** shows all parameters in the selected interval. Multiple parameters can be selected at the same time. If at least one parameter is selected, the parameter properties panel is shown. The following columns exist:
  - Parameter name
  - Parameter group
  - Device name
  - Device id
  - Interval.
- In the **Parameter properties** panel you can customize the logged signal name and logging interval and select that logging is done either always or only when the signal value has changed.



There are different ways to select multiple parameters:

- With the check boxes on the left of the parameters; add or remove parameters one by one by clicking the check boxes
  - To cancel the selection, click anywhere else in the row.
- With the Ctrl key; press the Ctrl key and click the rows you want to select.
- With the SHIFT key; hold down SHIFT and click the first and last rows of the selection.

To change the interval of parameters, select the parameters, choose the appropriate interval from the drop-down list and click **Apply changes**. If you select multiple parameters, you cannot edit the signal name and the signal logging history is not shown.

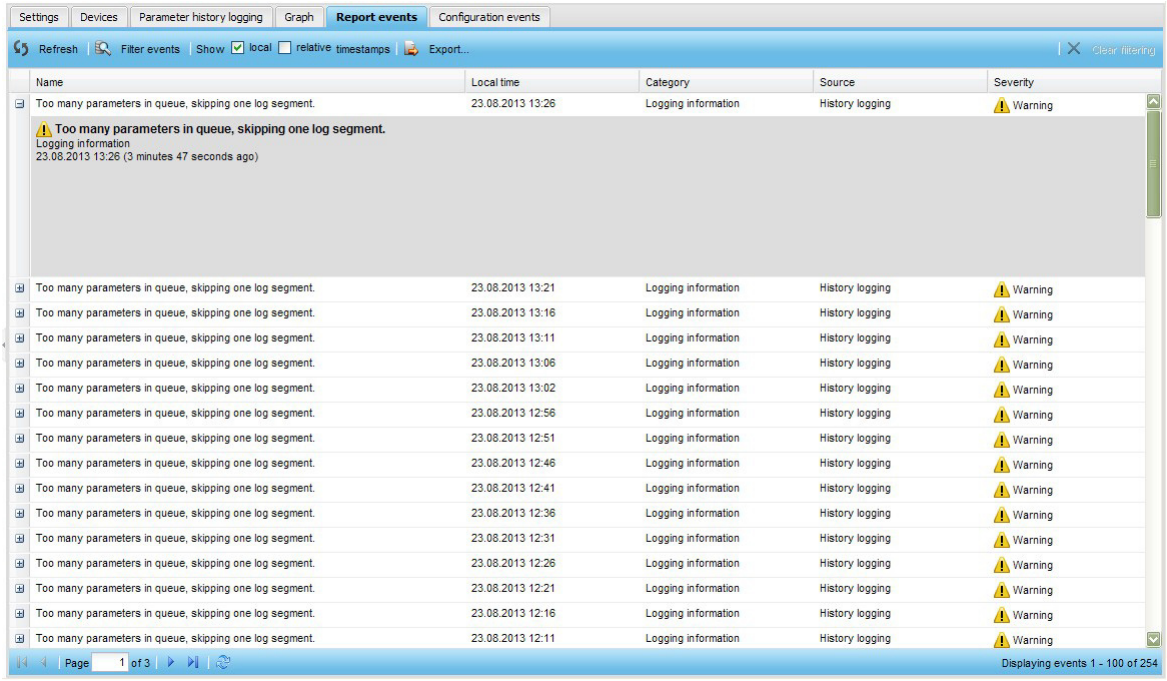
The available intervals are:

- Minute
- 5 minutes
- Hours
- Day
- None
- Continuous monitor.
    - In firmware 2.21 the logging interval for Continuous monitor is 1second. In firmware 2.23 the logging interval is adjustable between 1 … 30 s and the default value is 5 seconds.

The signals are logged only if their values have changed. If the **Log on when changed** check box is unchecked, the values are logged even if they have not changed.

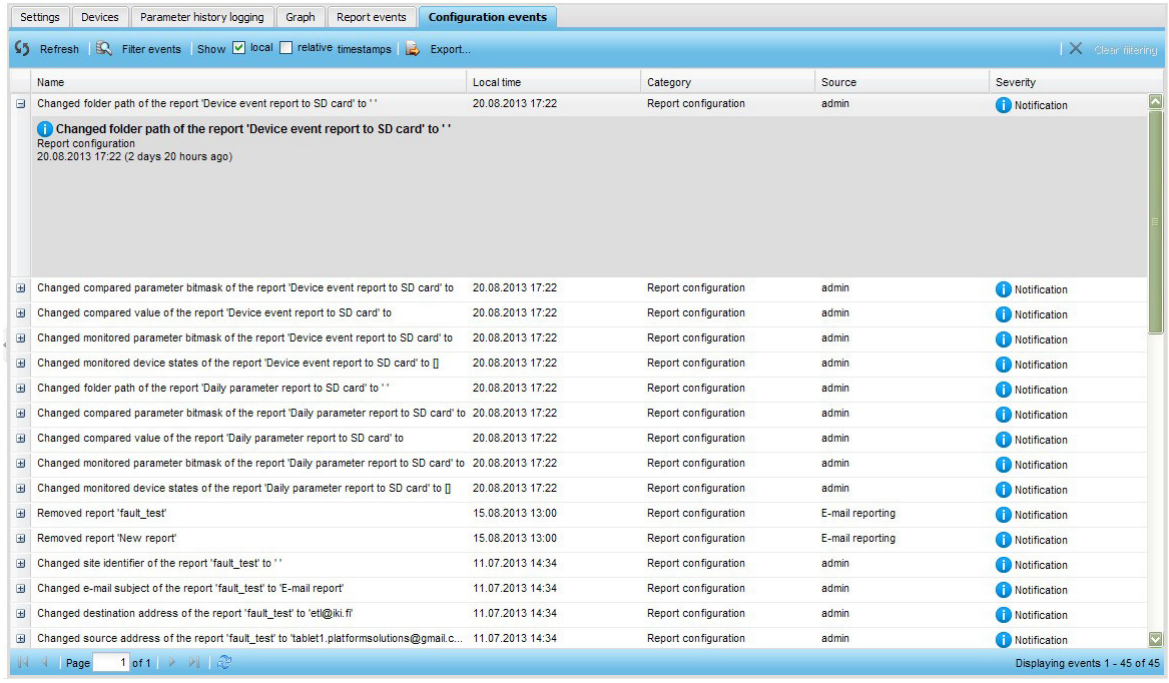
Report events data tab

To see all sent reports and those errors that may have occurred after reports have been created and sent, go to **Reports –> Report events**. The reports are sent to the email address defined in section *Creating an email report*.



Configuration events tab

To see all the modifications made to reporting settings, go to **Reports –> Configuration events**. The events can be filtered and sorted.



14

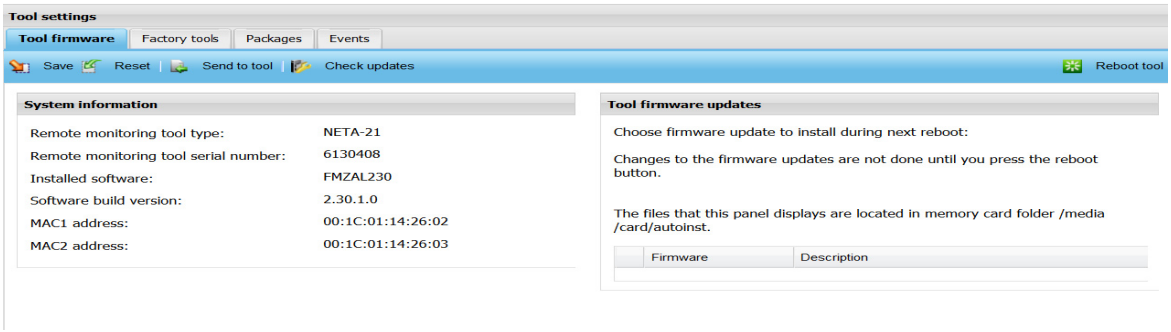
Tools

What this chapter contains

This chapter explains how to manage NETA-21 firmware, factory settings and software packages and introduces other useful tools.

Tool firmware

The **Tool firmware** tab (**Settings –> Tool settings**) shows the installed firmware version of the NETA-21 and enables to update the firmware of the NETA-21.



Note: The NETA-21 firmware updates require an SD card with a minimum of 200 MB free space.

The **Tool firmware** tab contains the following components:

- **Save** button saves the firmware update settings to the NETA-21.
- **Reset** button discards all changes made to the firmware update settings.
- **Send to tool** button opens a file browser for sending a firmware file to the memory card. Firmware files to be uploaded must have the following name format:

FMZAAvrr.NTU, where vrr represents a 3-digit version number (letters can be in upper or lower case).

- **Check updates** button connects to ABB Download Center and checks for new NETA-21 firmware releases. If a new version is found, it is downloaded and installed to the device.
- **Reboot tool** button reboots the NETA-21, which triggers the software update if new and selected firmware upgrade exists in the memory card. You are prompted to reboot the NETA-21 after clicking the **Reboot** button.
- **System information** panel shows tool-specific information. The panel contains the following fields: Remote monitoring tool type, Remote monitoring tool serial number, Installed software, Software build version, MAC1 address and MAC2 address.
- **Tool firmware updates** panel shows all available firmware updates on the SD card. The changes are saved and firmware installation settings are modified when you click the **Save** button. The unchecked firmware files whose version number is not greater than the version number of the currently installed firmware file are blacklisted and not installed during the next reboot.
- **Firmware** column shows the file name of the file. The column contains also a check box for defining whether the firmware update should be installed in the next reboot (if the file is not checked, then NETA-21 does not try to install it). The check box is disabled if the firmware is older than the current firmware or if it is the current firmware.
- **Description** column shows the status of the firmware update. The following conditions may be seen:
  - *Old firmware* is shown if the currently installed software is newer.
  - *Currently installed* is shown if the file version equals to the currently installed software.
  - *Non-installable* is shown if the running OS version is factory-loaded (FMZALvrr) and the same version as the update package (FMZAAvrr).
  - *Installation failed* is shown if the number of the running OS version is smaller and updating has failed.
  - *Not chosen to be installed* is shown if the number of the running OS version is smaller and the file is not checked.
  - *Install on next reboot* is shown if the number of the running OS version is smaller than the number of the currently installed firmware version. The NETA-21 tries to install the OS during the next reboot.

Factory tools

Factory tools tab provides an option to reset the NETA-21 to factory settings, and an option to disable (or keep enabled) the factory support account.

The **Factory tools** tab contains the following components:

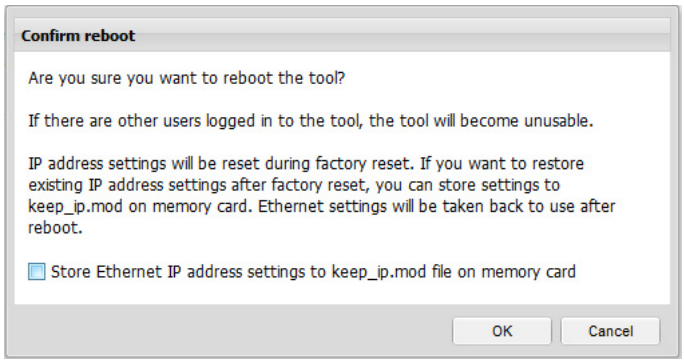
- **Save** button saves the settings. If the restore factory settings check box is selected, you are prompted to reboot the NETA-21.
- **Reset** button discards all changes made to the settings.
- **Export** button exports the settings to a local file.
- **Import** button imports the settings from a file to the UI.
- **Reboot** button reboots the NETA-21.
- **Enable SSH** is a check box for enabling or disabling secure shell service on TCP port 22.
- **Enable factory login** is a check box for enabling or disabling the web UI factory support user (user account "_factory"). Each NETA-21 has an individual factory user account for remote service and support purposes. You can disable the factory user account completely by unselecting this option.

  Note: The factory user account can be disabled if strict security is needed, but the deletion of the account affects the installation of extra software packages and remote support functionalities. In addition, if this option is disabled, the IP address will not work after a system has fully rebooted. The NETA-21 contains a factory support account for the web UI and for SSH remote connections. Factory account passwords are unique to each NETA-21.
- **Disable extra package installation (ips) from external media (USB, SD card)** is a check box for enabling or disabling external package (*.ips) installation from external media such as USB drives or SD card.
- **Disable settings import from external media (USB, SD card)** is a check box for enabling or disabling device settings (*.baj) package installation from external media, such as USB drives or SD card.

  Note: After changing the check box status, you should restart NETA-21 for the changes to take effect.
- **Restore factory settings** is a check box for removing all user data from the NETA-21 during the next reboot. To restore the factory settings, select this check box, save the settings using the **Save** button and finally click the top-right corner **Reboot tool** button.

IP address after a factory reset

From firmware 2.22 onwards, the NETA-21 shows the following dialog box when you want to reboot the NETA-21:

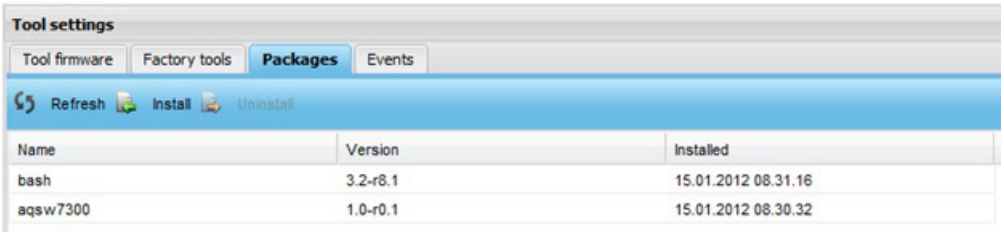


If you select **Store Ethernet IP address settings to keep_ip.mod file on memory card**, the NETA-21 tries to keep any previously defined fixed IP address configuration over a reset. The current network interface configurations are saved to a file on the SD memory card. The freshly initiated (factory resetted) firmware should be able to read the previous network interface configurations and take those into use. The keep_ip.mod and any existing restore.log or restore.n21 files should be removed from the SD memory card root folder after a factory reset to optimize the boot-up mode and to enable similar functionality in future.

Packages

The **Packages** tab enables to install and uninstall packages from the NETA-21. All core packages are filtered from the list so that you cannot uninstall any vital packages from the NETA-21.

You must have a Tool admin role (administrator) to access this view. This tab can only be used to install signed packages with an IPS file extension.



The **Packages** tab contains the following components:

- **Refresh** button refreshes the package list.
- **Install** button opens a file selector for an IPS package. After a file has been selected, the file is sent to the NETA-21 and installed. IPS packages are signed extra software packages provided by ABB.
- **Uninstall** button is enabled only if a package has been selected from the package list. When you click the button, you are asked to confirm the uninstallation before the NETA-21 starts uninstalling the package.
- **Package list** shows all installed packages in the NETA-21 excluding all packages that are necessary to the functioning. The package list contains the following columns: Name, Version and Installed.

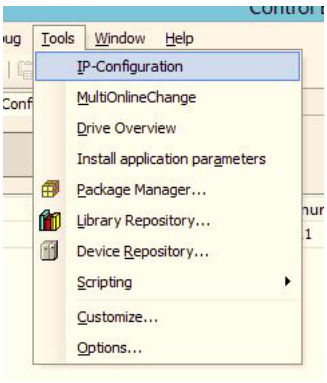
Using ABB IP Configuration Tool

ABB IP Configuration Tool detects all the NETA-21 remote monitoring tools in the network. The tool can be downloaded separately from www.abb.com, but it also comes bundled with ABB Control Builder Plus, the IEC 61131-3 programming environment for ABB PLCs and drives.

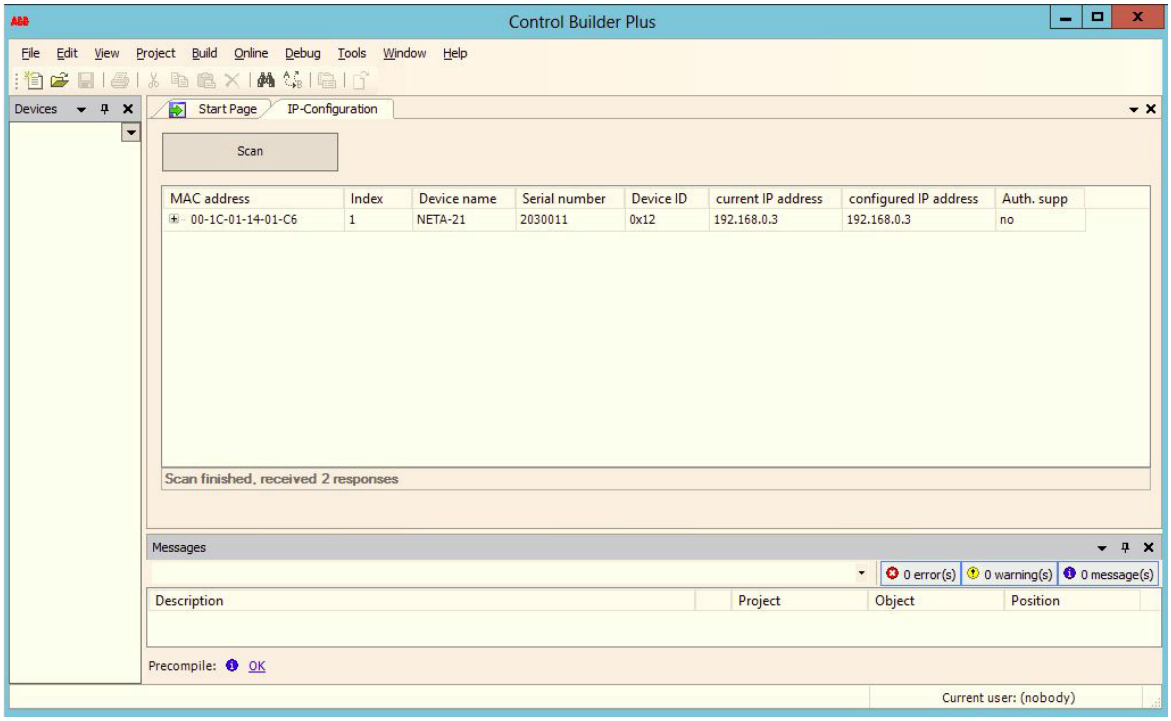
Use the tool, for an example, when you no longer know the IP address of the NETA-21 or when you do the initial set-up.

If you have the ABB Control Builder Plus 2.3.0 build 312 or newer installed, do as follows:

1. Launch the tool from **Tools –> IP-Configuration**.



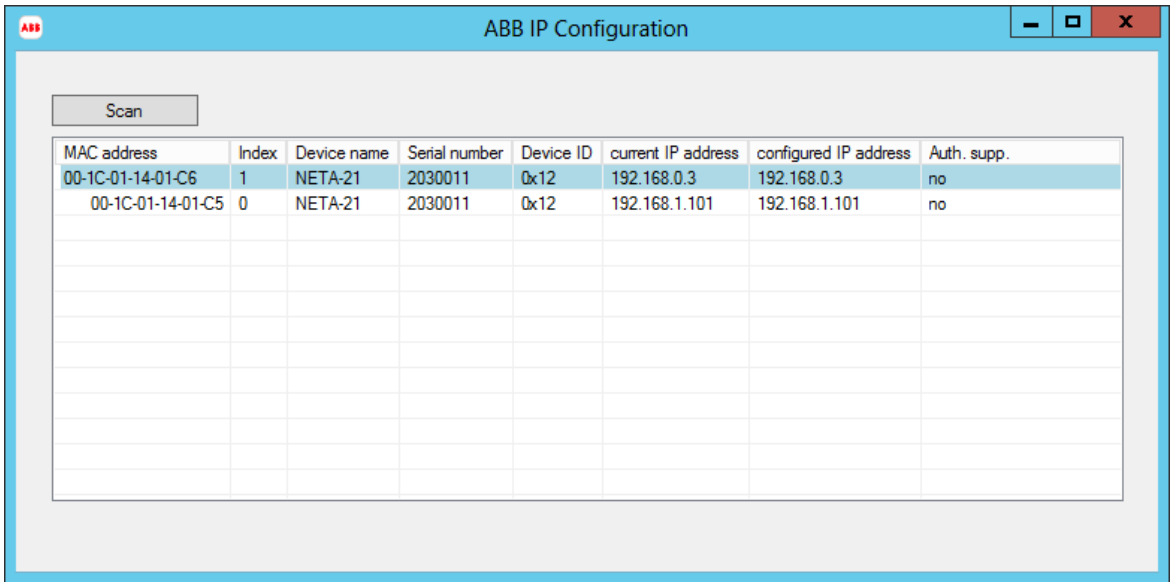
2. Start the scanning process by clicking the **Scan** button:



If no devices are found, make sure that your firewall does not interfere with the scanning process. Disable your firewall and try again.

All devices found during the scanning process are presented in a table where each device is in a separate row. In addition to the IP addresses of the device you can also see the MAC address, device name, serial number and device ID information.

In older Control Builder Plus 2.3.0 builds (for example build 252), ABB IP Configuration Tool is a separate program. Go to **Start –> ABB –> ABB IP Configuration**. However, the older version of ABB IP Configuration Tool gives the same information:



15

Backup and restore

What this chapter contains

The backup and restore function enables the replication of the NETA-21 settings to another similar type of remote monitoring tool. There are two main backup types: full system backup and backup of the selected settings only.

Backing up the NETA-21

1. Go to **Settings –> Backup and restore** and select the backup type.

Note: You must have an SD/SDHC card installed into the SD slot to create a backup. The SD card must have a minimum of 200 MB free space to enable the backup/restore functions. Backup and restore files are stored in the BACKUP folder on the SD card.

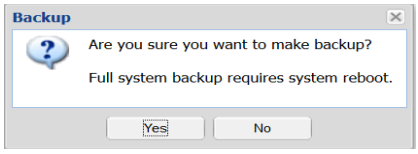
Create backup creates a backup according to the selected backup type.

Full system backup enables a full system backup of the NETA-21. The NETA-21 is rebooted before the backup file can be downloaded. After the NETA-21 goes back online, you must log on to the NETA-21. After you have logged on to the NETA-21, the **Backup** tab is shown and the NETA-21 starts sending the backup file to the PC.

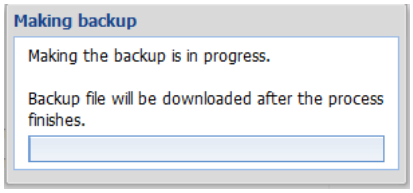
Settings backup enables a backup of selected data categories. You can select the following data categories:

- Device information
- Device interface settings
- Network service settings
- Users
- Locale settings
- User interface settings
- Logging settings
- Reporting settings

2. Click the **Create backup** button.
   The following dialog box appears.



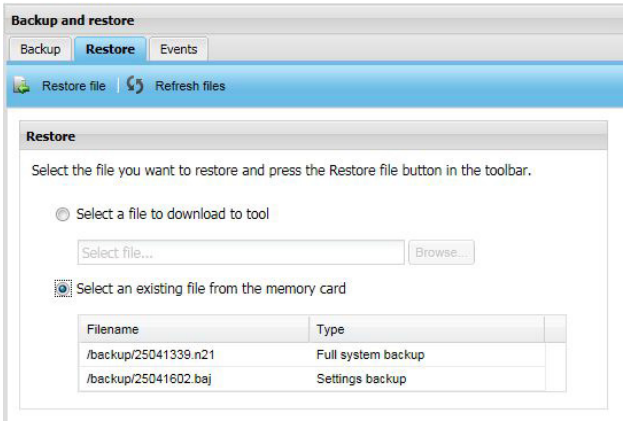
If you have chosen the **Settings backup** type, the Making backup pop-up window appears.



3. If a reboot is required after a backup has been created, log on to the NETA-21 to enable downloading when the system is back online.

Restoring the NETA-21

1. Go to **Settings –> Backup and restore –> Restore**.

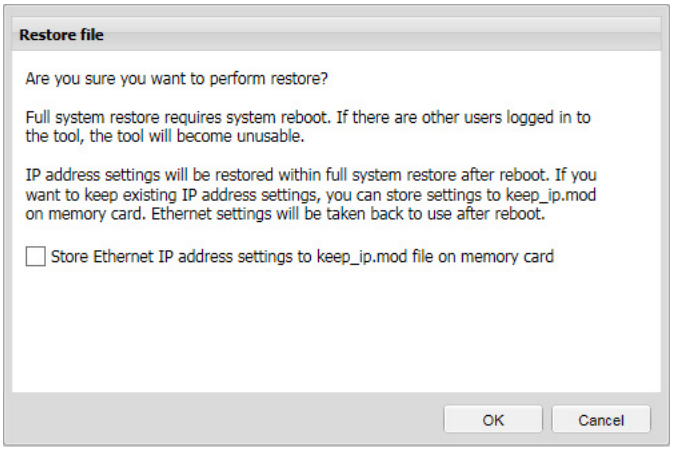


   The **Restore file** function restores a selected file. If restoring requires rebooting (full system restore), you are prompted to reboot the system. If you choose to reboot the NETA-21, the reboot view is shown. When the server goes back online, you are redirected to the **Login** window and eventually back to the **Restore** tab.

   To restore the files stored in the SD card, select the **Select an existing file from the memory card** check box.

2. Click the **Restore file** button.

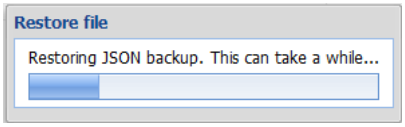
   The following dialog box appears.



   If you select **Store Ethernet IP address settings to keep_ip.mod file on memory card**, the NETA-21 tries to keep any previously defined fixed IP address configuration over a firmware restoration. The current network interface configurations are saved to a file on the SD memory card. The freshly initiated (factory resetted) firmware should be able to read the previous network interface configurations and take those into use, if the restored firmware is 2.22 or later.

   The keep_ip.mod and any existing restore.log or restore.n21 files should be removed from the SD memory card root folder after a system has rebooted to optimize the boot-up mode and to enable similar functionality in future.

If the file is a Settings backup file, a progress dialog box appears showing the status of the settings importation.



Note: If the restore file contains different network interface settings (for example IP addresses for Ethernet interfaces), the connection to the web UI can be lost after the restore function has been started. The new IP address settings depend on the file restored to the NETA-21.

16

Security

What this chapter contains

This chapter describes about the RADIUS (Remote authentication Dial-In User Service) authentication feature in NETA-21.

Applicability

The central RADIUS authentication feature is available from firmware version 2.30 or later.

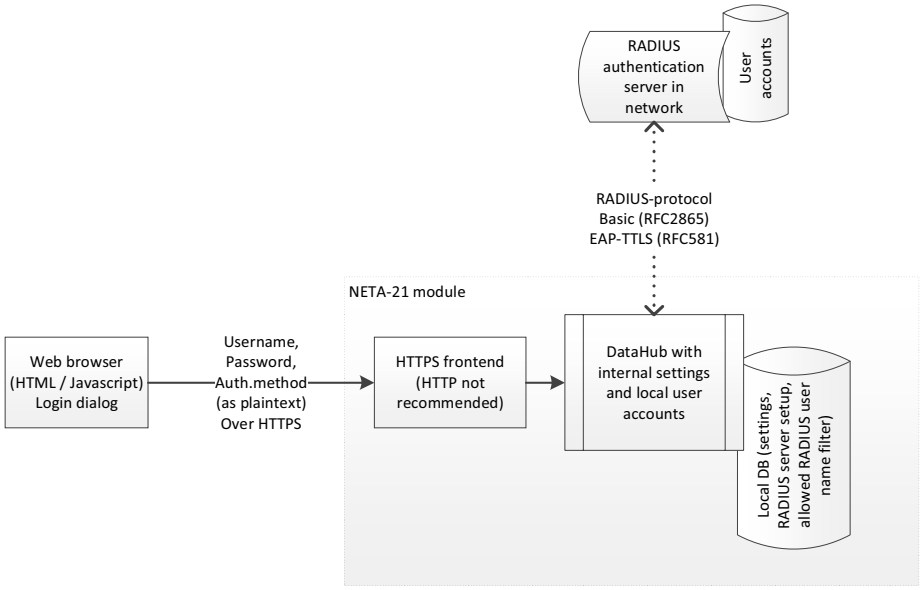
Advantages

On a large network each NETA-21 does not need to have user accounts and passwords defined separately for all users. Instead, with the RADIUS authentication feature, the user accounts and password policies can be managed centrally. This helps to increase the cyber security of the web interface.

Features

The RADIUS authentication supports two protocol variants:

- Basic/RFC2865
- EAP-TTLS (RFC5281)



Notes

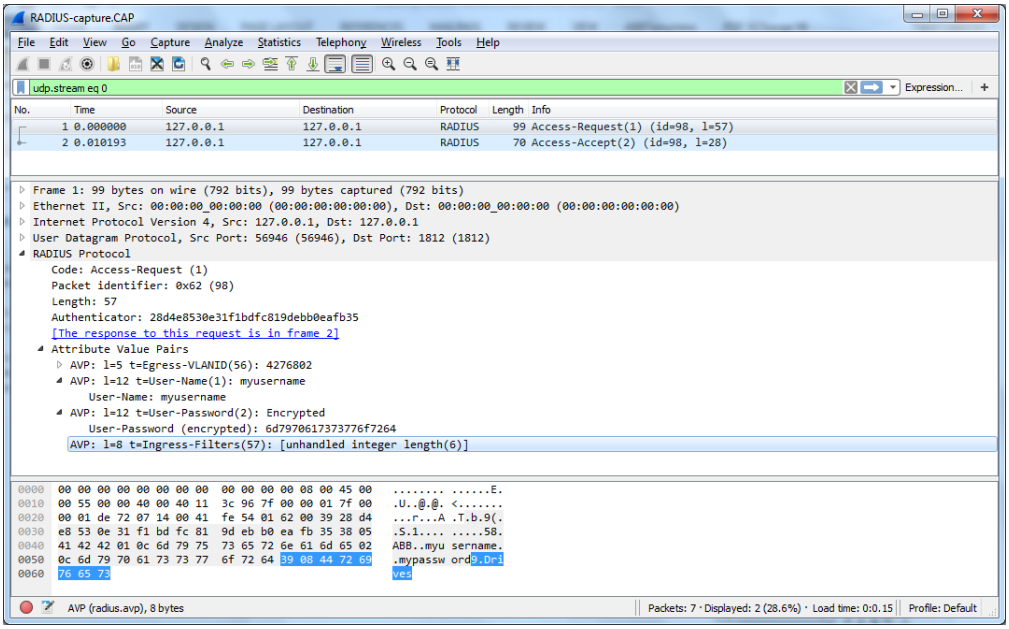
- The external user and password information is transmitted as plain text during RADIUS login. Use HTTPS login as an alternative to HTTP.
- The local logins does not perform hashing of the password in external RADIUS login. Hence, HTTPS / TLS encryption is used for password encryption.
- Local user accounts can be left active on side of the external RADIUS user accounts. Local accounts should have strong passwords. In cases when RADIUS server is unreachable (e.g. due to lost network connection), local login will be enabled once per failed RADIUS login even if the local logins are disabled.

Protocol level implementation for RADIUS

On protocol level, NETA-21 sends a RADIUS access request to RADIUS server with attributes as follows:

Attribute name	Attribute ID	Value
Vendor-ID	56	“ABB” (ID 100)
Vendor-Sub-Type	57	“Drives” (ID 101)

Example of RADIUS Access-Request packet sent by NETA-21 is shown in the below figure:



Receiving of RADIUS Access-accept leads to:

- Checking of attributes in response packet
- Mapping of attributes (in customizable Javascript code) to NETA-21 web interface permissions
- Login as the specified external type user.

Enabling RADIUS authentication in NETA-21 web UI

You can enable RADIUS authentication as follows:

- *Enable RADIUS authentication method in security settings*

  or
- *Add RADIUS user account with External account user role*

Enable RADIUS authentication method in security settings

1. From the NETA-21 web U, navigate to **Settings -> Security.**
2. In the **Login methods** panel, enable the RADIUS Login method.
3. Choose the RADIUS login method as Default.
4. If required, modify limit of Concurrent sessions in the **Login settings** panel. By default, the number of concurrent sessions is set as 10. The value can be changed to any value between 1 and 100.

   Notes:
   - Factory user can use one session in the background.
   - Key based authentication is not available for common use in 2.30 firmware.
5. Verify the settings on the **RADIUS settings** panel as follows:

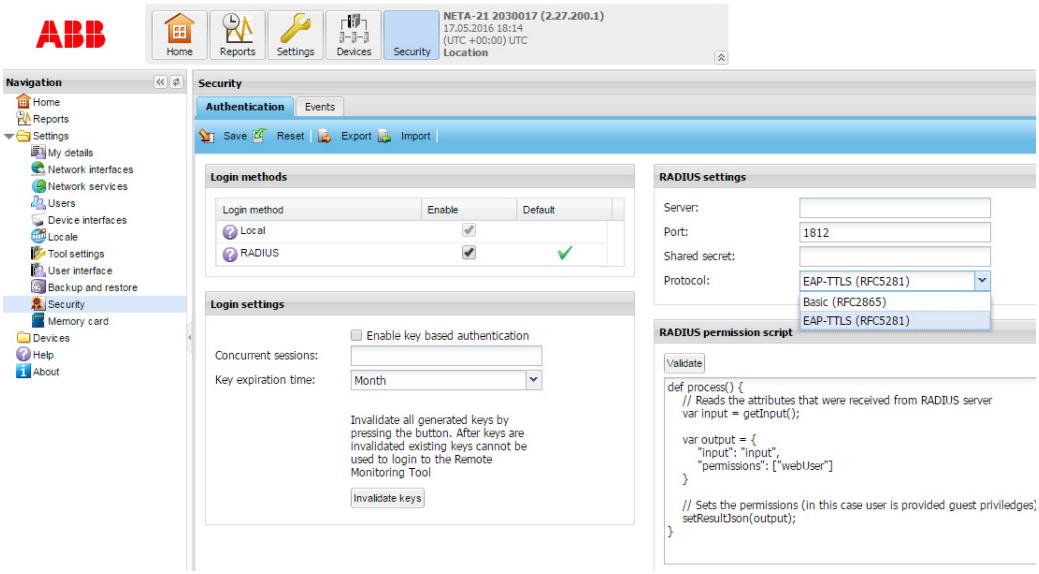
   Server - IP address or domain name of the RADIUS server

   Port - RADIUS server port (UDP port)

   Shared secret - RADIUS shared secret

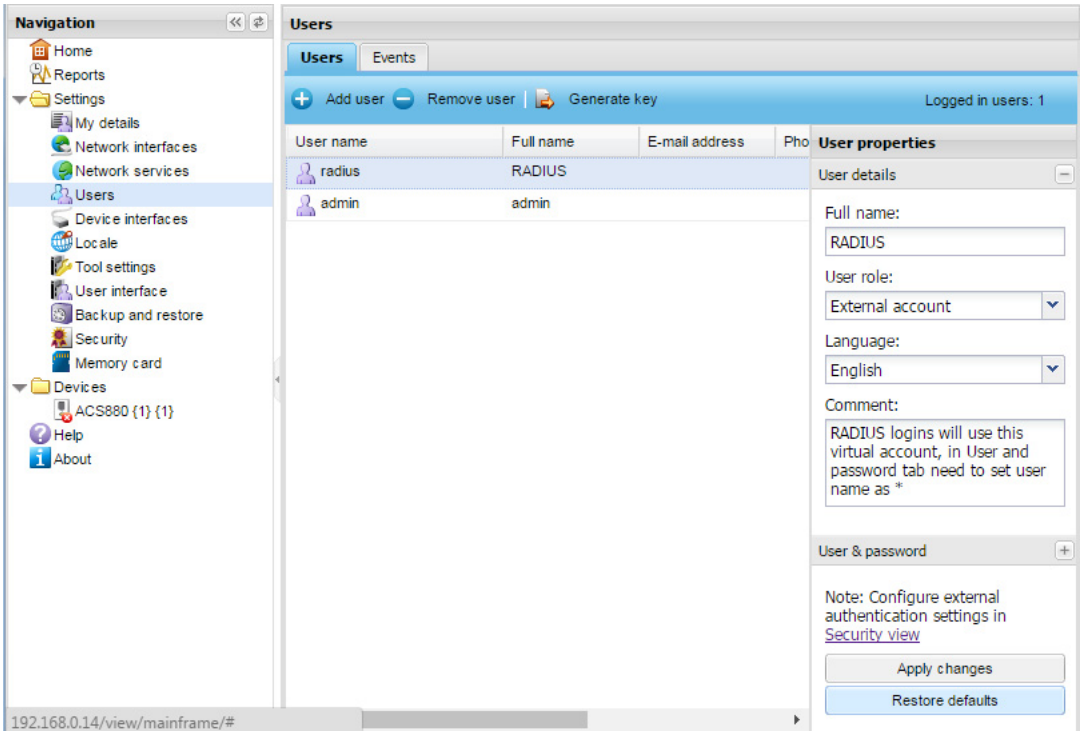
Protocol - Select one of the options:

- **Basic (RFC2865)** – authentication backend component implemented with pyRad.
- **EAP-TTLS (RFC5281)** – authentication backend is eapol-test (part of wpa-supplicant).



Add RADIUS user account with External account user role

This option allows you to define desired full name and external user name.



Steps:

1. Navigate to **Settings -> Users,** and click **Add user.**
2. In the **User details** section, complete the below details:
   Full name - Enter desired name

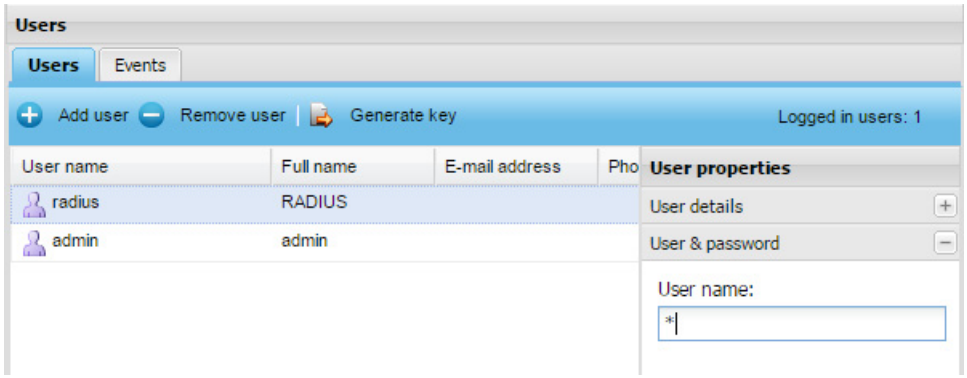
User role - Select External account from the drop down

Language - Select the desired language

Comment - Provide comments if required.

Notes:

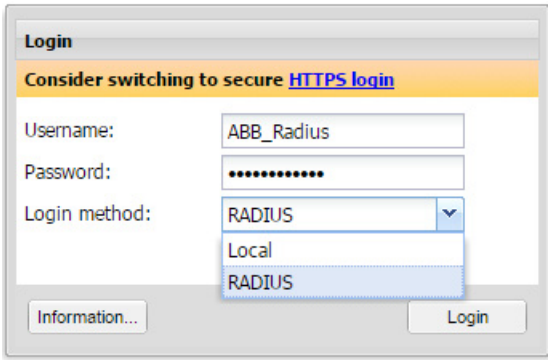
- Local user accounts will be left active in addition to the external RADIUS user accounts.
- Local accounts should have strong passwords.
- When RADIUS server is unreachable due to network unavailability or other reasons, local login will be enabled once per failed RADIUS login even if the local logins are disabled in Security settings.



3. In the **User & password** section, enter the desired user name in the User name field.
   The below patterns are allowed for User name:

Pattern	Login user	Example
*	Any valid user	johdoe john.doe@example.com \\JDOE
*@example.com	Any user at specific domain	john.doe@example.com
user name	Only one specific user	johndo john.doe@example.com

4. After the above changes, the **Login** dialog box displays the option to login with RADIUS login method.

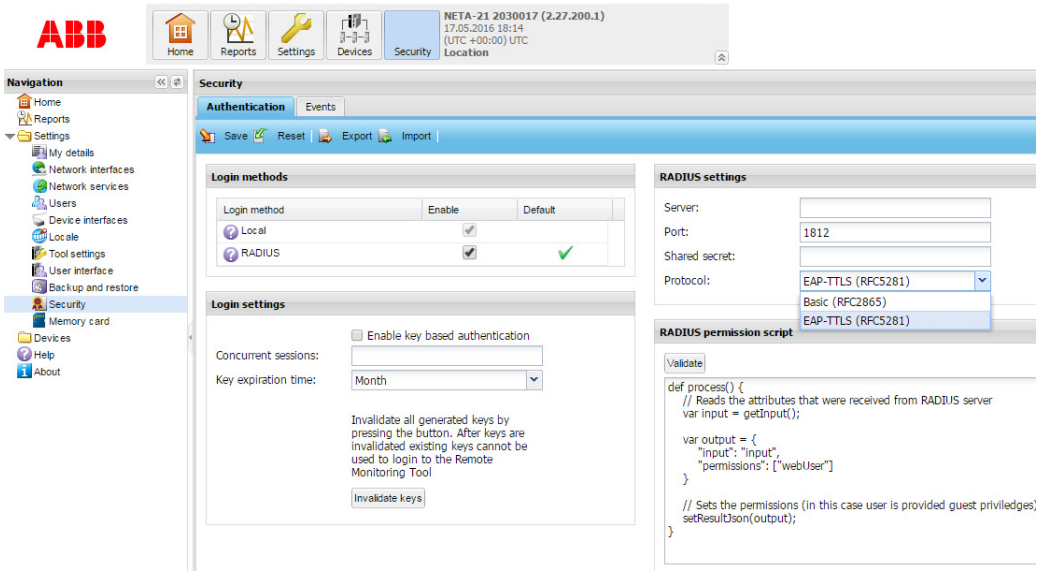


User permissions mapping

You can configure RADIUS permissions script to modify user permissions based on the parsed RADIUS server response. For example, user level attribute or similar server specific setting.

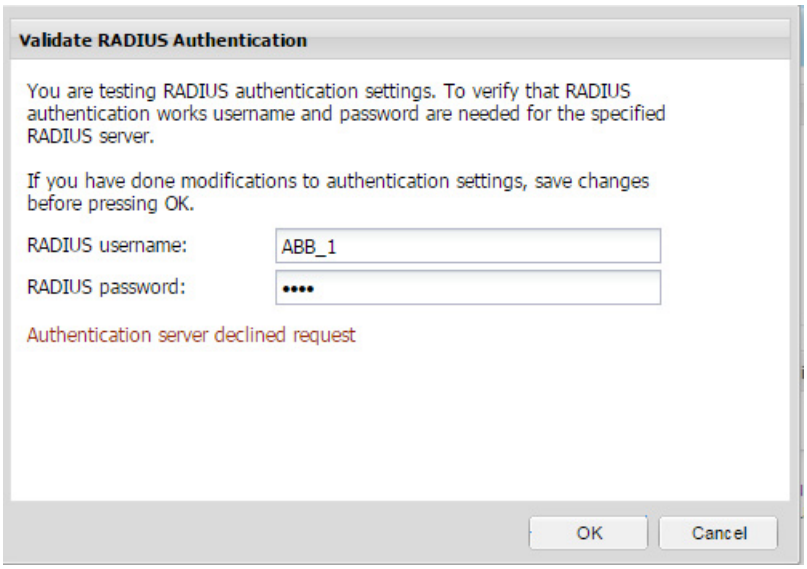
To configure RADIUS permissions script, perform the following steps:

1. Navigate to **Settings -> Security -> RADIUS permissions script.**
2. Configure the RADIUS permissions script (Javascript, interpreted with PyV8 inside NETA-21).



3. If required, click **Validate** to validate the script and test the RADIUS login. On validation, RADIUS permissions script gets the RADIUS Access-Accept attributes as an input object with key/value pairs. On successful validation, the desired array of NETA-21 permissions are generated.

   If the validation fails, an error message is displayed.



Available functions in the scripts are:

Function	Parameters	Description
getInput()		RADIUS Access-Accept attributes as an input object with key/value pairs
getInput()	Error message (any text)	Debug aid for **Validate** function of RADIUS permission script on Security settings dialog box, to show customized errors for recognizing specific issues in authorization. User-specified errors are not shown in login dialog box of NETA-21, instead, an Authorization error is shown.
setResultJson(obj)	Array of permission strings	Must be called at the end of the script to generate valid permissions for the user (empty return results in Authorization error). See below for examples of different typical permission sets, which are in NETA-21 web interface hidden behind user “roles” such as Guest, User, Drive expert, Tool, and admin
log(text)	Message	Not visible in web interface, only for command line debugging tests

If the response is successful, the RADIUS response and parsed permissions array is returned. The permissions that affect functionalities of the NETA-21 will be available for the logged in user.

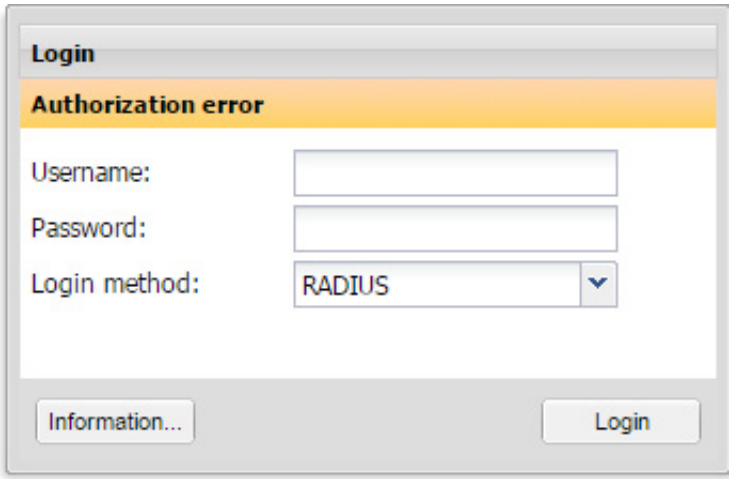
Following are examples of available user access levels:

```
var accessLevelPermissions = [
    // Guest
    [   "webUser", "deviceViewer"
"
    ],
    // User
    [   "webUser", "settingsViewer", "moduleGuest",
        "moduleUser", "deviceViewer", "deviceUser",
        "fileView", "reportViewer"
    ],
    // Drive expert
    [   "webUser", "settingsViewer", "settingsManager",
        "systemLogViewer", "moduleGuest", "moduleUser",
        "moduleSuperUser", "networkUser", "deviceViewer",
        "deviceUser", "deviceSuperUser", "deviceAdmin",
        "fileView", "fileStore", "reportViewer"
    ],
    // Drive expert
    [   "webUser", "settingsViewer", "settingsManager",
```

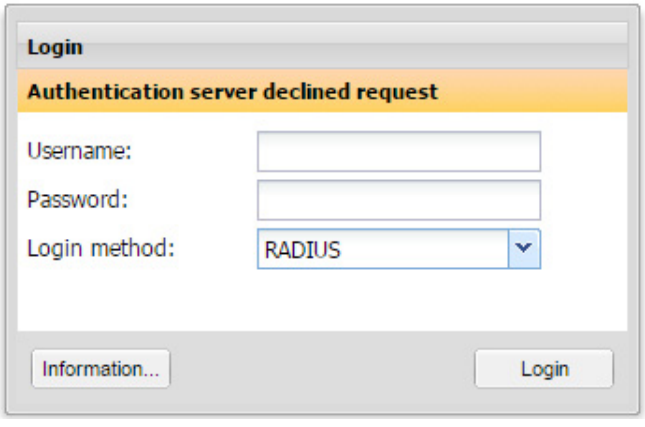
```
        "systemLogViewer", "moduleGuest", "moduleUser",
        "moduleSuperUser", "networkUser", "deviceViewer",
        "deviceUser", "deviceSuperUser", "deviceAdmin",
        "fileView", "fileStore", "reportViewer"
    ],
     // Tool admin
    [   "webUser", "settingsViewer", "settingsManager",
        "systemLogViewer", "moduleGuest", "moduleUser",
        "moduleSuperUser", "moduleAdmin", "networkUser",
        "networkSuperUser", "networkAdmin", "deviceViewer",
        "deviceUser", "deviceSuperUser", "deviceAdmin",
        "fileView", "fileStore", "reportViewer",
        "reportManager"
    ]
```

If the RADIUS request fails, one of the following errors is displayed:

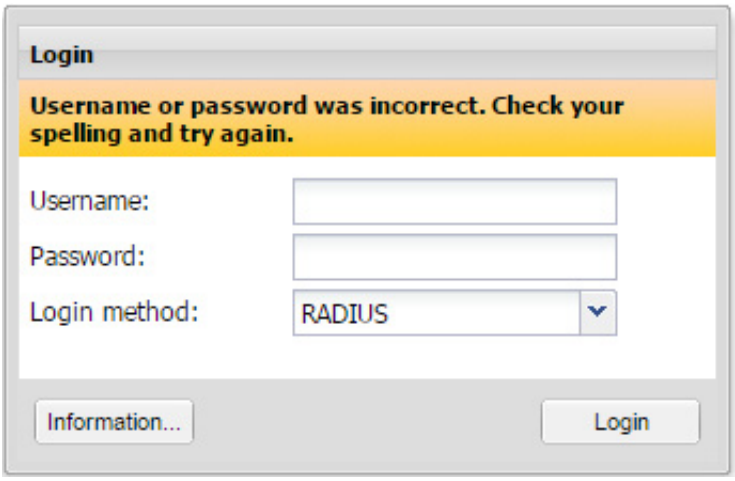
- Authentication server does not respond
- Authentication server declined request
- Authorization error



- Authentication timed out



- User name or password was incorrect This error is displayed if external user account does not exist for the mentioned user name.



You can resolve the errors using the suggestions in *Troubleshooting* section.

Troubleshooting

If an error occurs during RADIUS login, perform the following steps:

Error Message	Cause	What to do
User name or password was incorrect	**External user** name filter did not let the user name to attempt login via RADIUS.	Make sure that the user with role **External account** and **name** is created. In the login dialog box, make sure that login method **RADIUS** was selected.
Authentication server does not respond	RADIUS server is not reached.	In Security settings, check the IP address and availability of the RADIUS server.
Authentication timed out	High system load or long delays in network traffic.	Check network access. Retry multiple times **Note:** In general, RADIUS authentication takes 20 seconds, and login times out after 60 seconds.
Authorization error	User name or Password is wrong. RADIUS permissions script failed to run or returned zero permissions for the user account.	Check user accounts. Check the RADIUS permissions script.
Authentication server declined request	RADIUS server declined in-coming connection.	Check RADIUS server and firewall settings.

17

Memory card

What this chapter contains

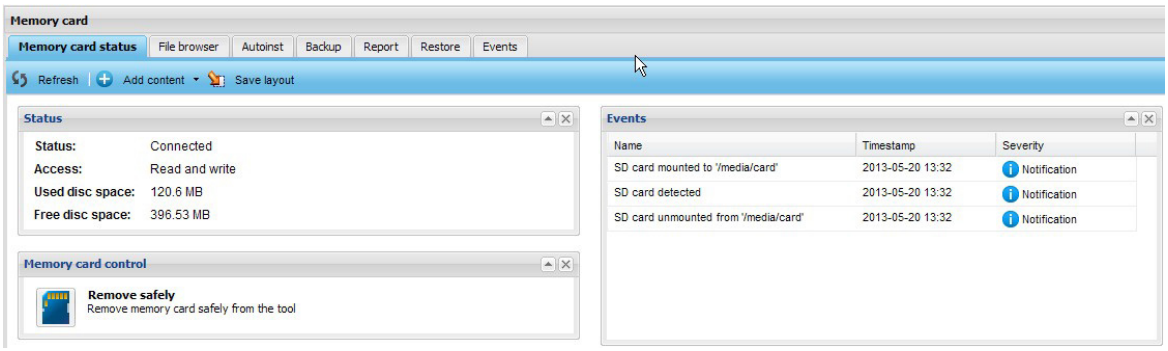
This chapter describes the tabs under **Memory card**.

Using the memory card

To observe and manage the data on the memory card, go to **Settings –> Memory card**. Use the memory card for collecting, for example, log files, backup files, device manuals and restore archives.

Memory card status tab

The **Memory card status** tab shows actual data about the memory card: status, access type and space status.

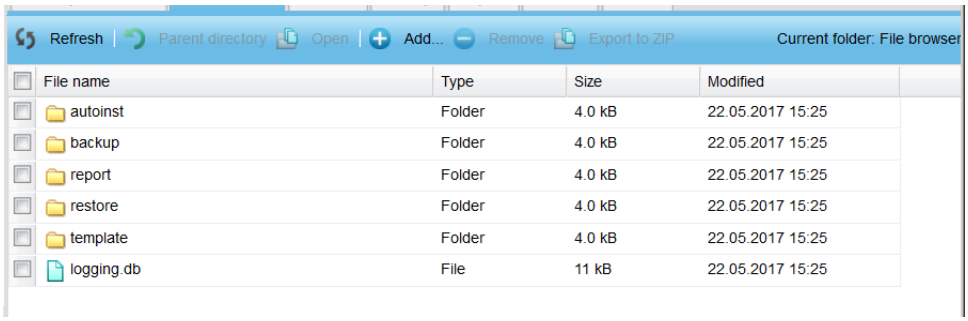


In general, the toolbar contains the following buttons:

- **Refresh** button refreshes the memory card data in the current interface.
- **Add content** button adds the portals: **Status**, **Memory card control** and **Events**.
- **Save layout** button stores the current layout settings to the NETA-21 memory.

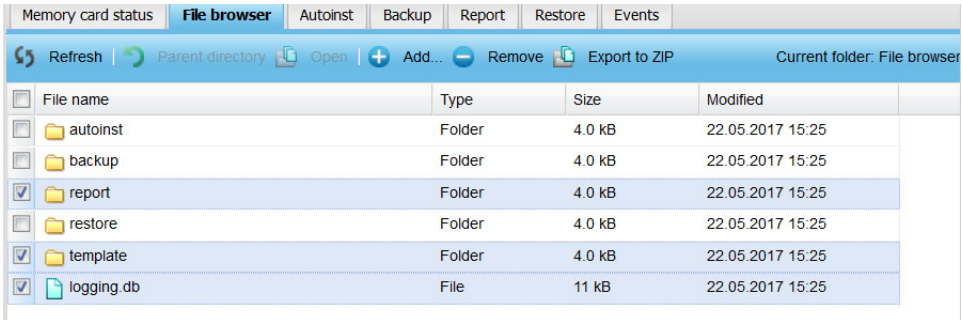
File browser tab

The **File browser** tab shows the files in the memory card. You can see this tab only if your role is Tool admin.



In general, the toolbar contains the following buttons:

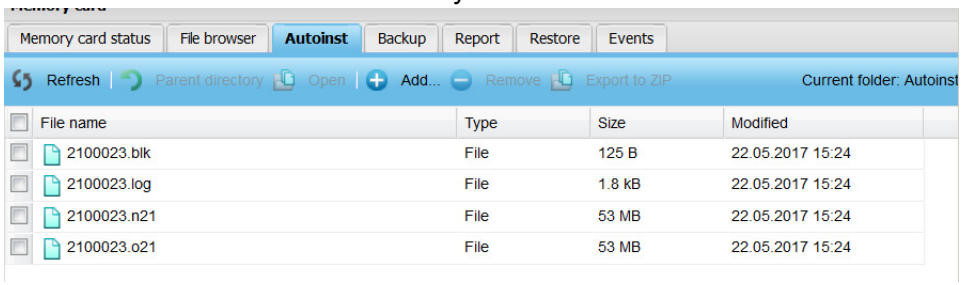
- **Refresh** button refreshes the list of files in the current folder.



- **Parent directory** button navigates to the parent folder.
- **Open** button opens the selected file.
- **Add…** button copies a file from the PC to the memory card.
- **Remove** button deletes the selected file or folder (only an empty folder can be deleted).
- **Export to ZIP** button collects all selected files and folders to a ZIP archive, which can be downloaded at the end of the process.

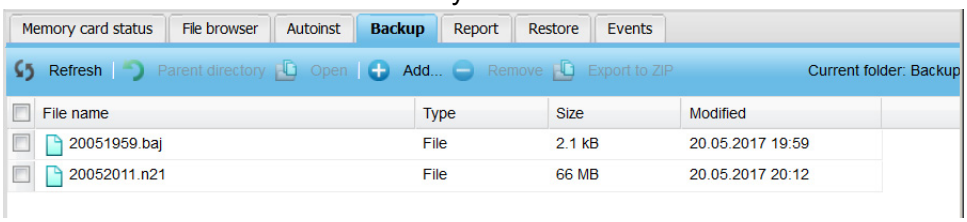
Autoinst tab

The **Autoinst** tab works the same way as the **File browser** tab but it uses the “autoinst” folder as a root folder in the memory card.



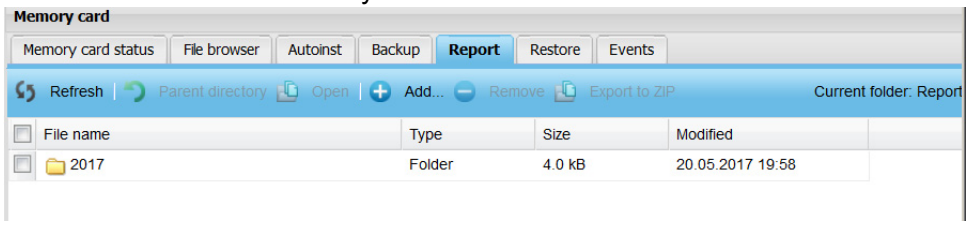
Backup tab

The **Backup** tab works the same way as the **File browser** tab but it uses the backup folder as a root folder in the memory card.



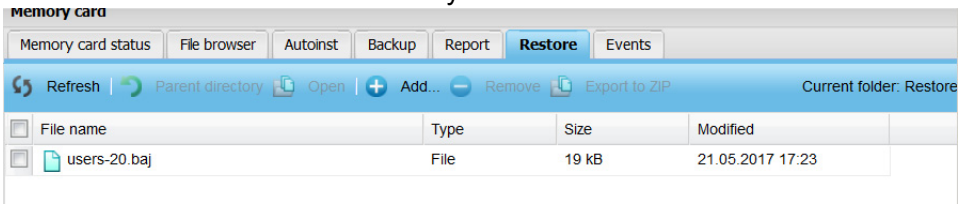
Report tab

The **Report** tab works the same way as the **File browser** tab but it uses the report folder as a root folder in the memory card.



Restore tab

The **Restore** tab works the same way as the **File browser** tab but it uses the restore folder as a root folder in the memory card.



18

Battery

What this chapter contains

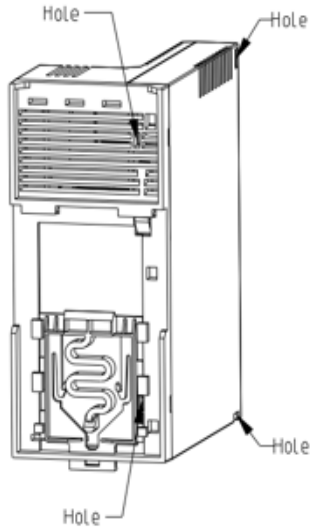
This chapter describes the procedure to remove and install NETA-21 battery.

About the battery

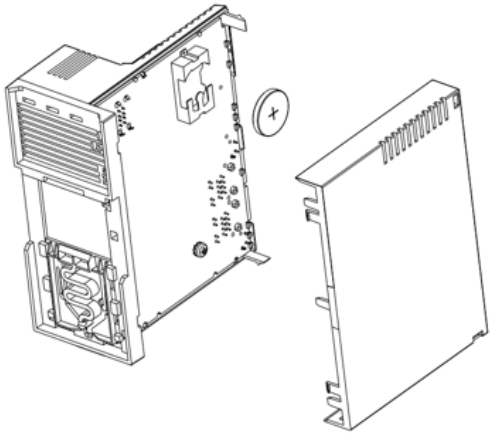
NETA-21 uses CR 2032 3V lithium battery. It is recommended to change the battery every 5 years.

Procedure

1. Remove the top cover.



2. Use a non-metallic tool and remove the existing battery.
3. Insert the new battery. Make sure that the negative pole of the battery faces towards the socket.



19

Frequently asked questions

What this chapter contains

This chapter contains how-to instructions for various tasks.

How to update the NETA-21 firmware

The following sections show how to update the NETA-21 firmware with an SD memory card. The NEXA-21 does not require any firmware updates.

In brief:

- With firmware 2.02 or any of the later releases:

  Put the update file on the root of the SD card, and the NETA-21 applies the update (or full system restore.n21) on the next reboot. The update takes about 5 minutes. LEDs STAT and SD are blinking during the update.
- With firmware 2.01 and earlier releases:

  Only the .NTU update mechanism over the web UI is supported. See section *Updating the NETA-21 firmware over a remote web connection* on page *186*.

For instructions on how to update several NETA-21 units at the same time locally with an SD card, see section *Updating the NETA-21 firmware locally with SD card(s)* on page *188*.

Notes:

- From firmware version 2.00 onwards, you can update all delivered NETA-21 units.
- The firmware update keeps all previous settings of the NETA-21. This means that a remotely connected NETA-21 stays reachable after the firmware update.
- Do a factory reset after major firmware updates, especially when you upgrade the NETA-21 firmware from version 2.11 or older releases, or when you upgrade the NETA-21 firmware more than one minor version number The factory reset restores the network settings.

Before you start

You must have NETA-21 update file FMZAAvrr.NTU where vrr stands for version and subversion numbers, for example in FMZAA221.NTU firmware version 2.21.

You must have an SD memory card:

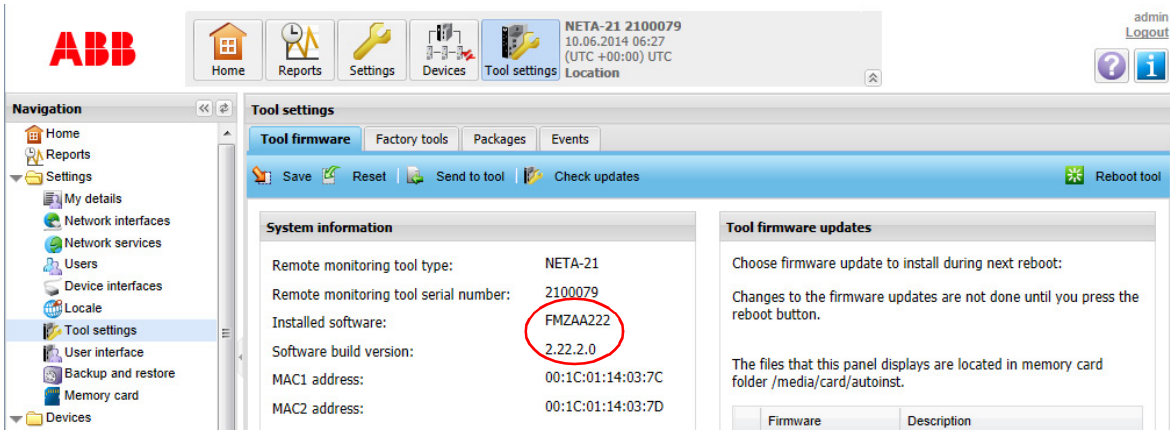
- Minimum size 512 MB, maximum size 32 GB
- Minimum of 200 MB free disk space
- Formatted with the FAT or FAT32 file system
- Read-writable (not write protected).

You can use the default SD cards included in each shipped NETA-21.

The firmware update has no effect if the existing software is already up to date. The firmware update can be done between minor versions such as 2.12.x.y and 2.13.x.y but not between patch versions of the same minor version such as 2.13.0.0 and 2.13.1.0. Thus, the firmware update from 2.12.2.0 to 2.13.1.0 succeeds because the minor version number is updated.

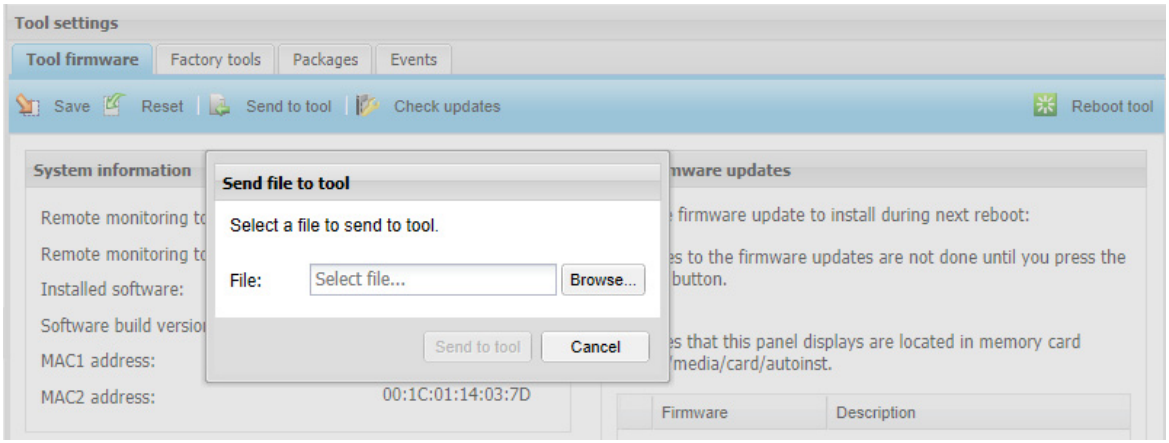
Updating the NETA-21 firmware over a remote web connection

1. Log on to the NETA-21 and go to **Settings –> Tool settings**.
   Tool firmware tab is visible. The **System information** panel on the **Tool firmware** tab shows the currently installed software version.



2. Click the **Send to tool** button.

The following dialog box appears.



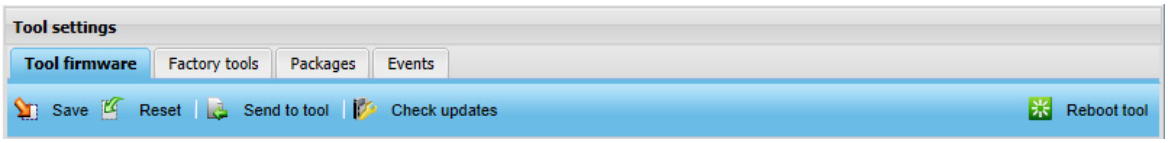
3. Click the **Browse…** button.
4. Choose the FMZAA…NTU file and click the **Open** button.
5. Click the **Send to tool** button.

   A process indicator shows how the uploading proceeds.

   The uploading takes few minutes, depending on the network speed.

   Note: If you have a slow network, we recommend you to use the FTP protocol or copy the file manually to the SD card.

   The file appears in the **Tool firmware updates** panel on the right-hand side of the **Tool firmware** tab. The latest available version is selected.
6. Click the **Reboot tool** button.

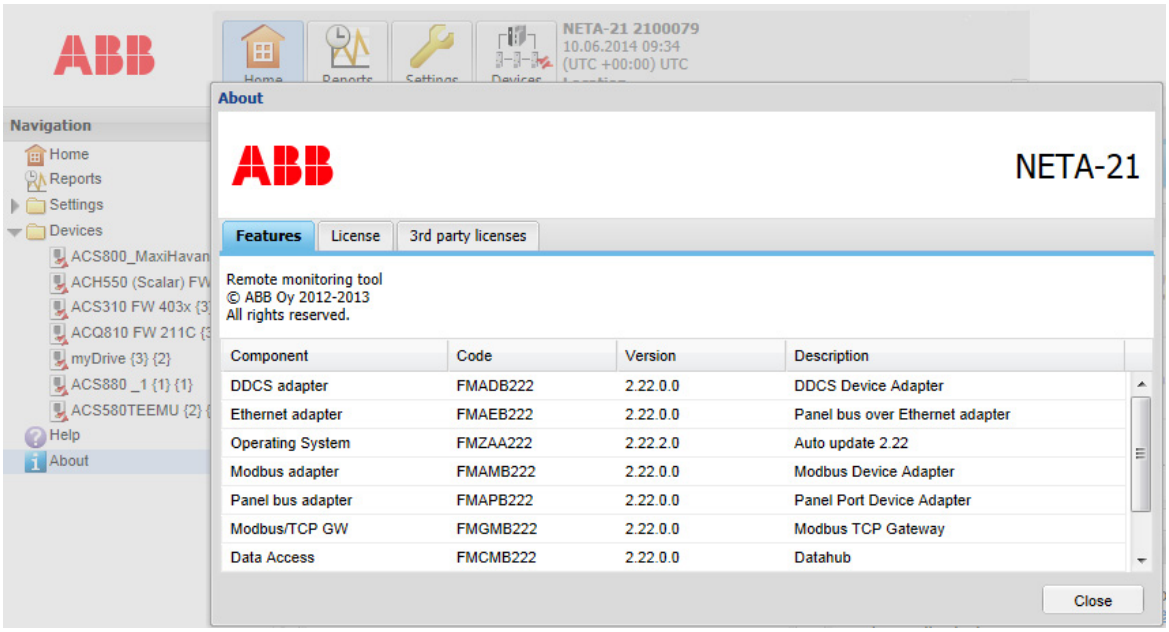


   Confirm that you want to reboot the tool.

   The rebooting takes about 5 minutes. If the **Login** dialog box does not appear in 10 minutes, reopen the web browser.

   Note: If you are access the NETA-21 with a local PC Ethernet connection, you must push the SD RJ45 button and reconnect the Ethernet cable to re-enable the DHCP server mode at this stage.
7. Log on to the web UI again.
8. To check that the update has been installed successfully, click **About** in the navigation bar of the user interface or the corresponding icon in the toolbar.

The **About** dialog box shows various software component versions. the Operating System version number is the most interesting one.



Note: If the installation of the new firmware has failed, the firmware is unselected and the description says "Do not install during next reboot". If the firmware update has succeeded, the firmware file is grayed out in the **Tool firmware updates** list. After a successful update, files can be cleaned up from the SD card (**Settings –> Memory card**). The already installed firmware update is located in folder "autoinst". Folder "backup" contains a full system backup image file which is automatically created before the firmware update. The size of the system backup image file is 50 MB … 200 MB.

Updating the NETA-21 firmware locally with SD card(s)

Use the local update method if you want to update multiple NETA-21 units in a batch or if you do not want to spend extra time accessing the web UI before and after rebooting the NETA-21. When the local updates are completed, we recommend you to reset the NETA-21 to factory default settings.

Copying the FMZAAvrr.NTU file to memory card

1. Insert the SD memory card into the PC.
2. Create a folder on the SD memory card and name it "autoinst" (without the quotes).

   Note: From release 2.02 onwards, you can skip this step and copy the file to the SD card root.
3. Copy the FMZAAvrr.NTU file (eg, FMZAA213.NTU) from the PC to the “autoinst” folder on the SD memory card.
4. Remove the card from the PC and insert it to the NETA-21.

Updating the firmware locally with an SD card

1. Make sure that NETA-21 has been switched off.
2. Insert the SD memory card with firmware update files into the SD memory card slot of the NETA-21.
3. Switch on the NETA-21 and wait about 5 minutes.

The time required by the operation depends on the speed of the SD memory card and the amount of data in the NETA-21, because the NETA-21 takes a full system back-up of all stored internal data to the SD memory card.

4. Do not switch off the NETA-21 or remove the SD memory card until the STAT LED on the NETA-21 has turned green.

   If power is lost during the update, the NETA-21 reverts to the previous system configuration and blacklists the attempted update. In this case, you have to retry to update the firmware via the web user interface or remove the blacklisted firmware from the autoinst folder.

   Do not remove the SD memory card permanently. If you do not insert the SD memory card back, the NETA-21 can be caught in an infinite restart loop indicated by LEDs flashing on and off every 2 minutes. If the restart loop condition does not fix itself in 10 minutes, the NETA-21 requires factory SW programming.

   If the STAT LED does not turn green, restart the NETA-21. Do not remove the SD memory card. Wait 5 minutes for the NETA-21 to restart the software update.

5. Switch off the NETA-21 when the STAT LED has been green for 1 minute.

6. Verify the update results from the log files on the SD card.

   After you have updated the software, there will be some log files and backups generated on the SD memory card. You can remove the log files and backups now or later over a remote connection.

   In folder autoinst/ on the SD memory card there are two new files per each updated NETA-21:

   - <serialno>.N21 - backup file
   - <serialno>.LOG - log file

   … where <serialno> is the 7-digit serial number of the NETA-21 tool, part of the same serial number as in the barcode label. (For example, if the barcode label serial number is B1500012WS, the log file is 1500012.LOG).

   The following is an example of a successful NETA-21 SW update log file. The timestamps at the beginning of each line specify when the operation was done (yyyyMMddThh:mm, log level, Moreton-autoupdate: message text).

```
20111228T06:19:52, 2, Moreton-autoupdate: Found valid update
file, starting update.
20111228T06:19:52, 2, Moreton-autoupdate: Starting backup.
20111228T06:21:04, 2, Moreton-autoupdate: Backup done.
20111228T06:21:04, 2, Moreton-autoupdate: Starting flashing.
20111228T06:21:22, 2, Moreton-autoupdate: Flashing done.
20111228T06:21:22, 2, Moreton-updater: Rebooting.
20111228T06:21:31, 2, Moreton-autoupdate: Continuing to init
for finishing the update.
```

How to reset the factory settings / What if I forget my password

If you have forgotten the NETA-21 password, do as follows:

1. Name any .n21 full system backup image as a restore.n21 image or use a restore.n21 image provided by ABB.

   Full system restore.n21 files are available from ABB Download Center.
2. Put the file in the SD memory card root folder.
3. Boot the NETA-21 up with the SD memory card inserted.

   A full system restoration also makes a full system backup of the previous system installation (which can be used to analyze the system afterwards).

A faster way to reset all settings to default values is to trigger a direct factory reset. This option removes all data permanently. Do as follows:

1. When you have switched off the NETA-21 after a software update, connect a straight-through Ethernet (Cat5 or higher) cable between the PNL1 and PNL2 ports.

   Note: Crossover Ethernet cables cannot be used.
2. When you switch on NETA-21, press the “RESET" button near the PWR and STAT LEDs. Press the button continuously for 5...10 seconds.
3. Wait until the PNL1 and PNL2 LEDs turn yellow. This may take 20...30 seconds.
4. When the PNL1 and PNL2 LEDs have turned yellow, remove the cable between the PNL ports immediately (within a minute).
5. When you have removed the cable, the NETA-21 resets to factory defaults and reboots.

   The reset function is complete within 10…20 seconds and indicated by all LEDs (except PWR) going off and then going on again.
6. Switch off the NETA-21.

   You can switch off the NETA-21 either right after it has rebooted, or wait until the STAT LED has become green again (factory settings have been re-initialized when the STAT LED has turned green).

How to replace the SD memory card safely

There are two buttons on the front panel of the NETA-21:

- SD RJ45 (eject) button for ejecting the SD memory card and discovering devices
- “Reset" button (no name indicated beside the button)

To eject th SD memory card safely, press the SD RJ45 button for a minimum of 1 second but no longer than 2 seconds. The SD LED turns from green to blinking red/green. When the LED has stopped blinking and there is a constant yellow light, you can remove the SD card. If you did not eject the SD card after trying for 1 minute or if a process blocked the access to safely remove the memory card, the SD LED turns green.

How to configure the logging of drive data to the SD card

To configure the logging of specific drive parameters manually, see the description of the **Logging** sub-panel in section *Parameter properties* or *Parameter history logging tab*.

By default all logged parameters and all occurred events are stored to events.db and values.db files on the SD memory card. You can adjust the storage interval and switch to the .csv / .log file storage, see section *Creating an SD card report*.

How much logged data fits into an SD/SDHC card?

2 weeks to 1 year with a default SD card, up to 10 years with the largest available SD memory card, depending on the configuration.

How to interpret the logged data from the SD card

See section *Format of an SD card report* for the report file syntaxes.

How to create an FTP account

Create the FTP and FTPS accounts in the same way as web UI accounts. Set the user role to "FTP user". You can use the FTP and FTPS accounts only for accessing files on the SD memory card.

The usage of the FTP and FTPS services may require modifications in the firewall settings. Go to **Settings –> Network services –> Services** to see if the FTP/FTPS services have been opened over the specific network interfaces.

How to re-enable reports if time & date have been shifted backwards

If time and date of the NETA-21 have been shifted backwards, it can happen that both logging and reporting of the previously defined reports stop, until the time again flows over the previous point when data was sent out the last time.

To re-enable reporting and to reset the internal timestamp/pointer of the last reported data, open the specific report for editing in the Reports view and apply changes to that report or just save the report settings.

20

Diagnostics and troubleshooting

What this chapter contains

This chapter explains how to trace faults with the status LEDs on the NETA-21 and the NEXA-21.

LED indications

The NETA-21 is equipped with 13 bi/tricolor diagnostic LEDs. The NEXA-21 is equipped with four bi/tricolor diagnostic LEDs. The LEDs are described below.

LED indications of the NETA-21

Name	Color	Function
USB	Off	No USB mass storage devices attached
	Green	USB mass storage device attached and mounted.
	Blinking green	Device attached, initialization in progress
	Yellow	Device can be removed.
	Red	Unidentified error when settings are imported from an USB memory device.
	Blinking red	Initialization failed. Unsupported file system on a USB stick. Only FAT file systems with 8.3 character filenames are supported. Basically, NTFS-formatted USB sticks and external hard disks are not supported.
EXT	Off	No NEXA-21 connected
	Green	NEXA-21 found and initialized
	Blinking green	NEXA-21 support is being initialized (when the NETA-21 boots up)
	Red	NEXA-21 malfunctions
	Blinking red	NEXA-21 not supported
SD	Off	No SD/SDHC card
	Green	Card attached and taken into use
	Blinking green	Card attached and initialization in progress
	Yellow	Card can be safely removed
	Blinking yellow	Card attached, removal in progress
	Blinking yellow	**Together with the blinking red STAT LED:** System waits for confirmation of reboot operation or network override
	Red	Card error, for example write protection prevents from writing data to the card
	Blinking red	Card initialization failed. Unsupported card type, for example, SDXC (extra capacity) cards and MMC cards are not supported.
PNL 1/ PNL 2	Off	No devices (no wire) connected to the PNL port
	Green	All devices connected, identified and commissioned
	Blinking green	Manual or automatic discovery of devices in progress
	Yellow	Communication OK, but device connectivity limited. All devices are ready to be unplugged/disconnected.
	Red	Communication error caused the panel port network initialization to fail. Unknown device in the network, or something is interfering the network and preventing proper detection of monitored devices.
	Blinking red	Unsupported device is found in the network, or there are too many devices in the network to be monitored

Name	Color	Function
PC ETH 1	Off	PC not connected. If an Ethernet cable is connected to the PC ETH 1 port but no one uses the NETA-21, the LED remains blank.
	Green	Connection set up and in operation, for example, DHCP is active and at least one PC has got an IP-address
	1/2-second blinking green	• NETA-21 provides IP addresses for local devices. Activate the DHCP server mode by pressing the SD RJ45 button for five seconds. • When a PC is connected and the NETA-21 has provided an IP address for it, the LED turns steady green. **Note:** The DHCP server functionality remains enabled until the NETA-21 is restarted or until the DHCP server is disabled in the web UI (**Settings –> Network interfaces –> Ethernet 1**).
	1-second blinking green	At least one user has been logged on to the user interface
	Blinking yellow	Factory-level access/operation. Firmware update in progress. **Note:** System status (STAT LED) blinks during the firmware update.
PWR	Off	Power off
	Green	Power on
	Yellow	Timed power off or standby. NETA-21 can go to the standby mode as a protective measure (eg, if the environmental temperature is too high). To wake up the NETA-21, press the SD RJ45 button.
STAT	Green	System in operation, OK
	Yellow	System starts up, services not yet fully operational
	1/4-second blinking yellow	System waits for a confirmation of the reboot operation or network override. • If you reboot the NETA-21 by pressing the reset button for 5 seconds when the NETA-21 is running, the STAT LED starts blinking. Confirm the reboot operation by pressing the SC RJ45 button. If you do not confirm the reboot operation, it stops after a 1-minute delay. • You can override the network settings by pressing the SD RJ45 button for 10 seconds when the NETA-21 powers up. If you keep pressing the button for about 20 seconds, the STAT LED starts blinking, which indicates that you can release the button. If you do not release the SD RJ45 button within one minute (or if the button is locked to the “ON” position), the default network settings are not restored.
	1-second blinking yellow	Firmware update in progress
	Blinking red	Error occurred during the start-up of the NETA-21. If the start-up fails, the NETA-21 restarts itself automatically after a few seconds. During the reboot operation, all LEDs excluding the PWR LED flash before the STAT LED turns yellow again. If the yellow STAT LED and blinking red STAT LED alternate and the STAT LED does not turn green, the start-up of the NETA-21 fails continuously. Try resetting the NETA-21 to factory settings.
MON	Blinking green	NETA-21 sends data (eg, email) to an external destination.
	Blinking red	NETA-21 fails to send data (eg, email) to an external destination. Log on to the web user interface and go to **Reports –> Events** for error details.

LED indications of the NEXA-21

Name	Color	Function
PWR	Off	NEXA-21 not controlled by the NETA-21 or the NETA-21 boots up
	Green	NEXA-21 detected by the NETA-21 and the NEXA-21 turned on
STAT	Green	System in operation, OK. DDCS drives commissioned. Communication with drives OK.
	Yellow	System reboots, the NEXA-21 temporarily out-of-order
	Blinking yellow	Limited connectivity. Devices not found.
	Red	Internal error. DDCS network not physically OK, or no devices detected.
	Blinking red	Incompatible device in DDCS. NEXA-21 has lost connection to a configured device. **Note:** DDCS is running.
RX	Off	Not receiving data
	Yellow	Receiving data
TX	Off	Not transmitting data
	Yellow	Transmitting data

Troubleshooting

Problem	Cause	Solution
The STAT led of the NEXA-21 turns red after the NETA-21 has been powered up.	DDCS devices are not detected.	Do as follows: Check that the DDCS wiring is connected the right way around. Disconnect optical fibers for over 30 seconds and then reconnect the fibers. The 30-second disconnection initiates the device rescanning. Log on to the NETA-21 web user interface. Go to **Settings –> Device interfaces**, select the DDCS tab and click **Restore defaults**. Confirm the restoration by clicking the same button again.
The newly connected devices do not appear in the UI.	Automatic rescanning is done only if all devices per interface have been disconnected for 1 minute or longer.	EITHER: Disconnect wires for 1 minute and then reconnect. OR: In the UI, go to **Settings –> Device interfaces**, select the interface specific tab, and click button **Rescan devices**.

Problem	Cause	Solution
The disconnected old devices remain in the UI and do not disappear.	Disconnected devices must to be manually removed. An automatic removal would affect customized device settings, such as reporting settings.	The solution depends on the device interface. Try one of the following: 1. Go to **Settings –> Device interfaces** and select the specific device interface. Click button **Rescan devices**. 2. If devices still reside in the UI, go to the front page of the disconnected device. Check the Device control panel and click the **Remove device** button if such a button is available.
Web pages behave erratically or the login is prevented after the tool firmware update.	The web browser cache contains an old version of the user interface.	Try refreshing the whole page. Try pressing the shift key on the keyboard during refreshing, to reload all script files. If that does not help, clear all temporary Internet files or the cached web content using browser specific menus, and try to log on to the NETA-21 again.
When the web page is zoomed with a tablet or mobile phone only part of the screen area is usable.	The content zooming with touch screen devices is not fully supported.	Zoom to the desired level and tilt the phone/tablet screen (90 degrees to the horizontal or vertical position) to readjust screen frames.

21

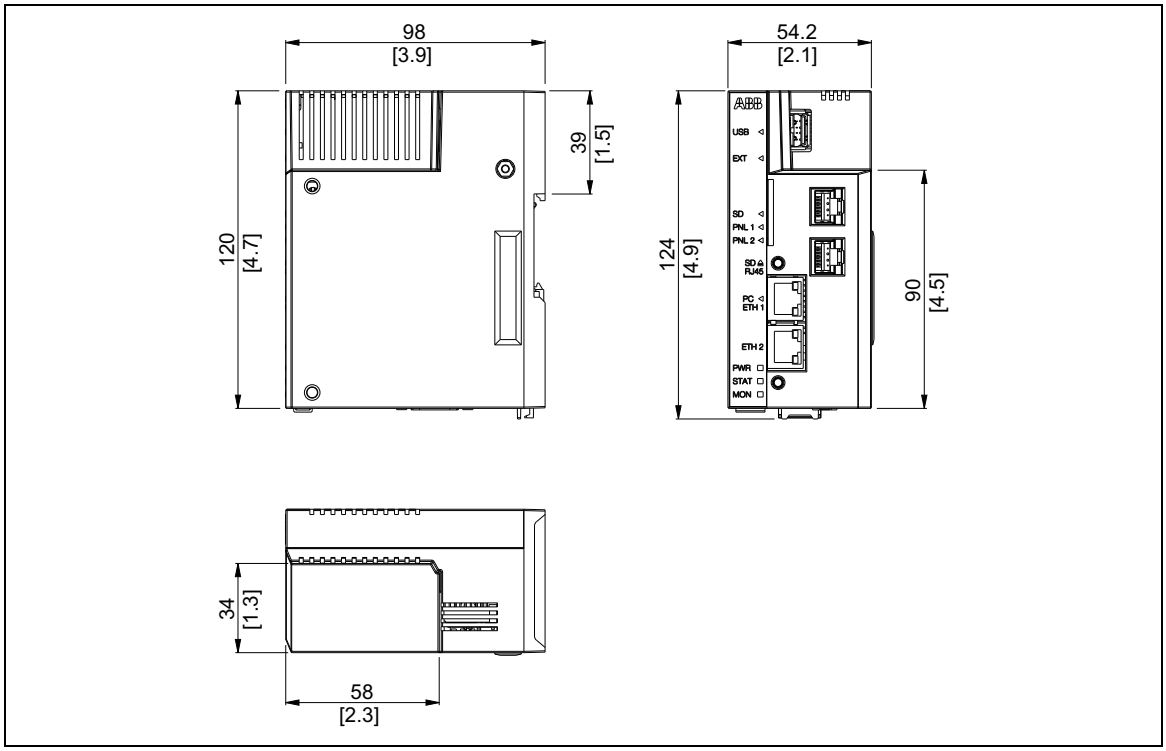
Technical data

What this chapter contains

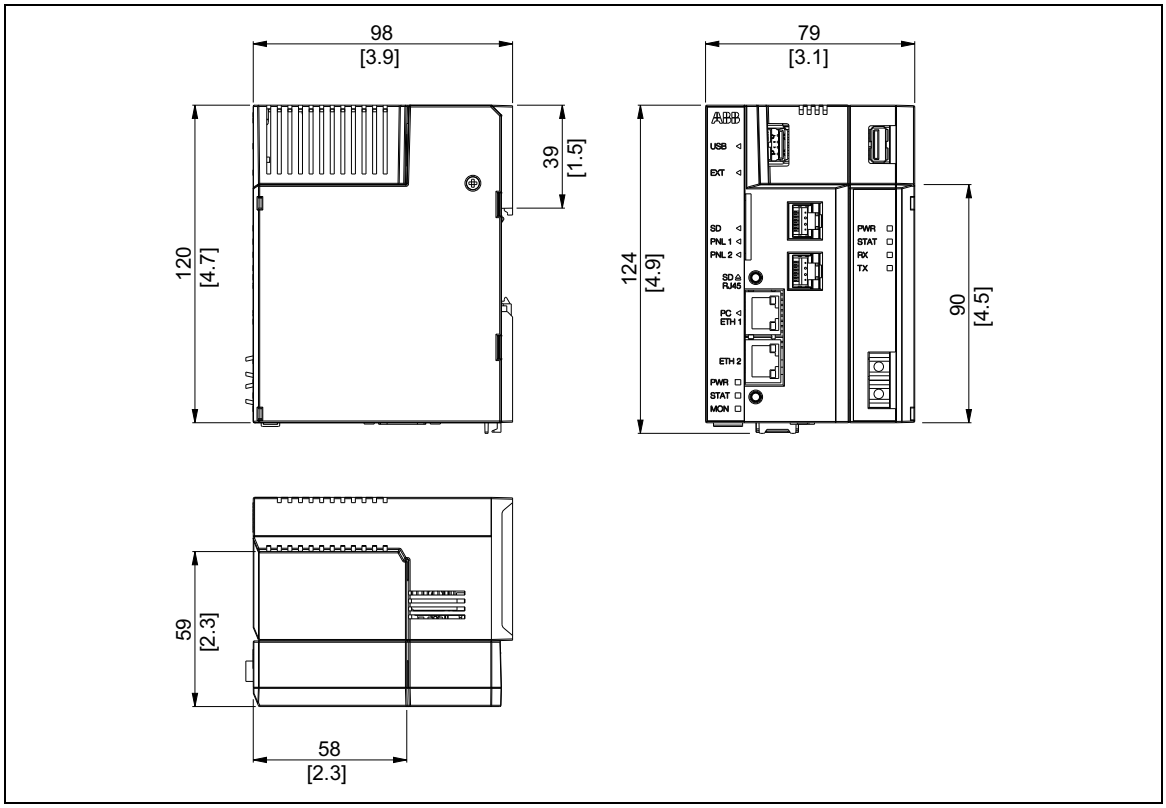
This chapter contains the technical data of the NETA-21 and the NEXA-21.

Hardware

Enclosure of the NETA-21



Enclosure of the NETA-21 with the NEXA-21



Technical data of the NETA-21 and the NEXA-21

Mounting	On a 35-mm / 1.4-inch DIN rail
Degree of protection	IP20
Ambient conditions	Applicable ambient conditions specified for the drive in its manuals are in effect. • Operating temperature: -5…+60 °C / -23…+140 °F (free air circulation)
Indicators	9 + 4 bi/tricolor LEDs
Connectors	Power supply input (X1) • Signal level: 10 … 30 V DC, max. 2 A (typical: 200mA @ 24 V / 500 mA @ 12 V) • Connector type: Shrouded header for the wire plug, 2 pins, pitch 5.00 mm / 0.19 inch Panel bus port 1 (PNL 1) and 2 (PNL 2) • Bus voltage: 5 V • Signal level: EIA-485 • Communication protocol: Panel bus over EIA-485 • Cable type: Ethernet CAT5, straight • Connector type: Shielded 8P8C modular jack (RJ45) • Maximum segment length: 100 m / 328 ft Ethernet port 1 (ETH 1) and 2 (ETH 2) • Media: 10Base-T / 100Base-TX (10 Mbit/s or 100 Mbit/s) • Cable type: Shielded twisted pair (STP), both straight-through and crossover cables are supported (HP Auto-MDIX). • Connector type: Shielded 8P8C modular jack (RJ45) • Termination: Internal • Maximum segment length: 100 m / 328 ft EIA-232 Port (X2) • Physical layer: EIA-232, galvanic isolated • Connector type: D-sub 9-pin male EIA-485 Port (X3) • Bus voltage: 5 V • Medium: Shielded twisted pair cable, impedance 100…150 ohm • Serial communication type: Asynchronous, half-duplex RS-485 • Physical layer: EIA-485, galvanic isolated • Communication protocol: Modbus • Connector type: Shrouded header for the wire plug, pitch 5.00 mm / 0.19 inch • Maximum length: 1200 m / 3 937 ft SD/SDHC connector • Supports up to a 32-GB SD/SDHC card USB host ports • PHY Interface: USB2.0 • Connector type: Shielded USB Type A Fiber optic transmitter/receiver DDCS • Media: Fiber optic cable (max. 10 Mbit/s) • Protocol: Distributed Drives Communication System (DDCS) • Connectors: Dark gray – receiver; gray – transmitter
Power supply	• Primary power supply input: 10…30 V DC, max. 3 A • Secondary power supply input: AC/DC 24 V ± 10%, max. 1 A (rms). For redundant power supplies via extension modules. • Power supply output: 5 V, 700 mA for external option modules. Short circuit protected.
General	• Battery replacement interval: 5 years at 25 °C / 77 °F • Complies with EMC standards IEC 61000-6-2 and IEC 61000-6-4 • All materials are UL-approved

Further information

Product and service inquiries

Address any inquiries about the product to your local ABB representative, quoting the type designation and serial number of the unit in question. A listing of ABB sales, support and service contacts can be found by navigating to abb.com/searchchannels.

Product training

For information on ABB product training, navigate to new.abb.com/service/training.

Providing feedback on ABB Drives manuals

Your comments on our manuals are welcome. Navigate to new.abb.com/drives/manuals-feedback-form.

Document library on the Internet

You can find manuals and other product documents in PDF format on the Internet at abb.com/drives/documents.

abb.com/drives

3AUA0000096939H

© Copyright 2020 ABB. All rights reserved.
Specifications subject to change without notice.

3AUA0000096939 Rev H (EN) 2019-24-06