NETSILON 9 / 11

User manual

This document refers to the following products:

907 910	Netsilon 9 AC
907 911	Netsilon 9 DC
907 912	Netsilon 9 AC+DC
907 913	Netsilon 9 AC+AC

This document refers to the following products:

907 915	Netsilon 11 AC
907 916	Netsilon 11 DC
907 917	Netsilon 11 AC+DC
907 918	Netsilon 11 AC+AC

Bodet
www.bodet-time.com

BODET TIME & SPORT
1 rue du Général de Gaulle
49340 TREMENTINES - France
Tél. support France: 02 41 71 72 99
Tel.: +33 (0) 2 41 71 72 33

afaq ISO 9001 Qualité AFNOR CERTIFICATION
afaq ISO 14001 Environnement AFNOR CERTIFICATION
Usine de Trémentines

Ref: 608552J

On receipt, ensure that the product has not been damaged during transportation and report any concerns to the carrier.

TABLE OF CONTENTS

SAFETY INFORMATION

The following icons are used to indicate risks or sources of danger when installing, using and maintaining this product.

Symbol	Description
i	*IEC60417 - 1641* Operating instructions
+	*IEC60417 - 5002* Positioning of cell
⏚	*IEC60417 - 5017* Class I
⏚	*IEC60417 - 5018* Functional earthing
⏚	*IEC60417 - 5019* Protective earth (ground)
⎓	*IEC60417 - 5031* Direct current
~	*IEC60417 - 5032* Alternating current
≂	*IEC60417 - 5033* Both direct and alternating current
ϟ	*IEC60417 - 5036* Dangerous voltage
⧈	*IEC60417 - 5172* Class II equipment
⚠ UV	*IEC60417 - 6040* Caution, ultraviolet radiation
⚠ ☼	*IEC60417 - 6041* Caution, visible radiation
⚠ ϟ	*IEC60417 - 6042* Caution, risk of electric shock
⧈ ⏚	*IEC60417 - 6092* Class II equipment with functional earthing
⚠ IR	*IEC60417 - 6151* Caution, infrared radiation
🔌	*IEC60417 - 6172* Disconnect all power sources
🗑	*IEC60417 - 6414* Waste Electrical and Electronic Equipment (WEEE)
⚠	*IEC60417 - 0434b* Caution
3~	*IEC60417 - 5032-1* Three-phase alternating current
3N~	*IEC60417 - 5032-2* Three-phase alternating current with neutral conductor
⏻	*IEC60417 - 5009* Power, Stand-by
⚠ ☼	*IEC60417 - 6069* Caution, very bright light

1. GENERAL INFORMATION

Thank you for choosing the BODET Netsilon 9 / 11 time server. This product has been carefully designed for your satisfaction, according to the rules of our ISO9001 and ISO14001 quality system.

We recommend that you read this manual carefully before using the product for the first time.

Retain this manual throughout the lifespan of your product so that you can refer to it when necessary.

Failure to observe these instructions may cause irreversible damage and invalidate the warranty. In that case, BODET cannot be held liable. The product is guaranteed for 3 years, excluding damage caused by power surges (lightning, etc.) in the absence of a Bodet GNSS surge protector on the installation.

Non-contractual data. BODET reserves the right to make certain functional, technical or aesthetic changes to the devices without prior notice.

This manual is subject to change without notice. To obtain the latest version of this documentation, please refer to our website: www.bodet-time.com.

Note: depending on your configuration (e.g option cards, NTP and/or GNSS synchronisation, etc.), some functions introduced in this user manual may not be available on your Netsilon time server.

1.1 Use of the instructions

Different user profiles may be required to install or use this product.

According to the task to be performed and the proficiency level of the user, we recommend as follows:

- Basic user:
  Read through this manual in its entirety before installing and configuring Netsilon.
- Trained and qualified user:
  Read through this manual from Chapter **2. Installation.**
- If Netsilon is already operational:
  In order to change a specific setting or gain a better understanding of its characteristics and functions, read this manual from Chapter **3. Commissioning**. Use the search function, click on a PDF bookmark or use the table of contents.
- In the event of technical problems please refer to chapter **8. Support.**

Key to symbols:

ℹ : indicates advice, a recommendation or any other noteworthy information relating to the use of Netsilon.

⚠ : indicates that special attention needs to be paid.

⚡ : indicates that misuse or failure to follow the instructions could result in an electrical danger. This information must be taken into account when installing or using Netsilon.

1.2 Introduction

Netsilon is a time server designed to distribute a high-precision time signal.

Compact and modular, the Netsilon time server combines the precision of a master clock and a secure approach of data networks:

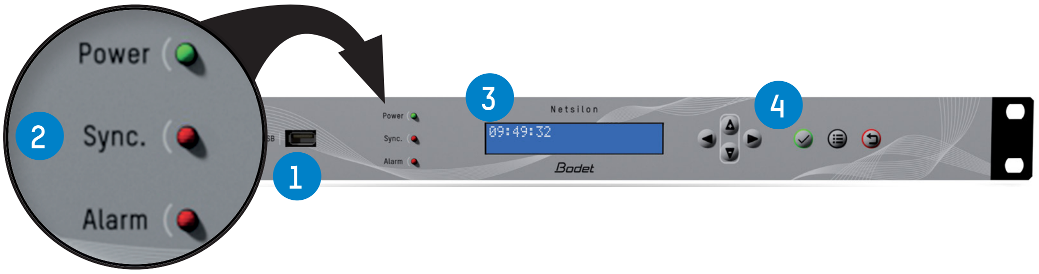
- High-precision internal clock regulated by its own OCXO quartz.
- Order of priority for the different synchronisation references.
- Modular design allowing a wide variety of input/output signals (up to four option cards).
- Network security management: enable/disable encryption, authentication and access protocols.
- Alarm information in the form of SNMP traps and e-mails.

Four versions are available, depending on the power supply:

- Netsilon 9 AC
- Netsilon 9 DC
- Netsilon 9 AC+DC
- Netsilon 9 AC+AC
- Netsilon 11 AC
- Netsilon 11 DC
- Netsilon 11 AC+DC
- Netsilon 11 AC+AC

1.3 Netsilon presentation

1.3.1. Front panel

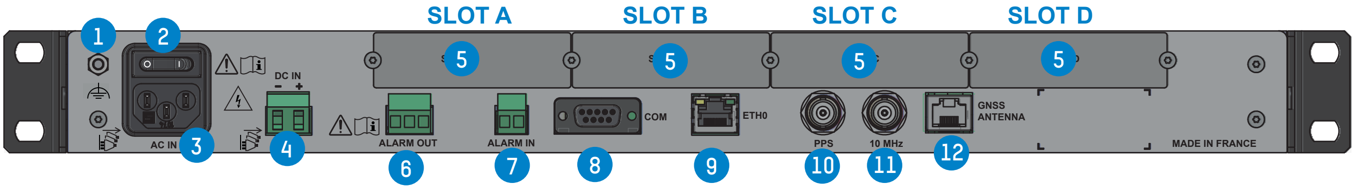


The Netsilon front panel contains:

- a USB[1] port 1,
- three status LEDs for power supply, synchronisation and alarms (Power, Sync and Alarm) 2.
  See chapter **8.1 Status of LEDs on the front panel**
- a two-line LCD display 3,
- control keys 4 for initial setup (full setup from the web server).

1.3.2. Rear panel

- **NETSILON 9 / 11 (AC+DC)**

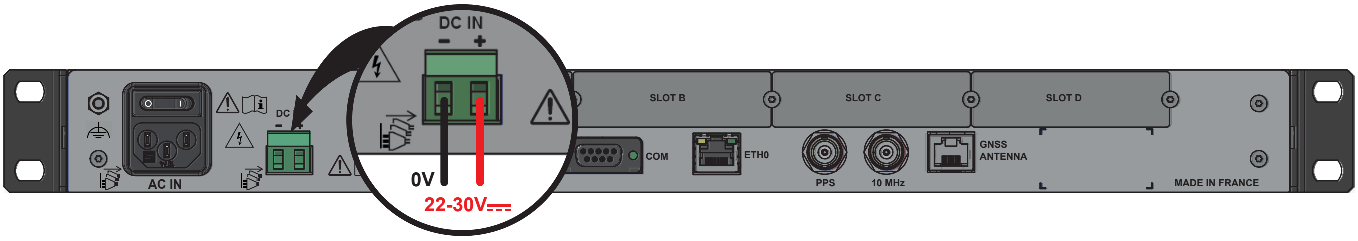


1 Functional earthing terminal ⏚: can be attached to the cabinet frame (optional).
The protective earth is provided by the IEC male connector 3.

2 On/Off switch.

3 AC IN mains connector. IEC 320 power inlets.

4 DC IN direct current power supply terminal block (3.81 mm terminal block).



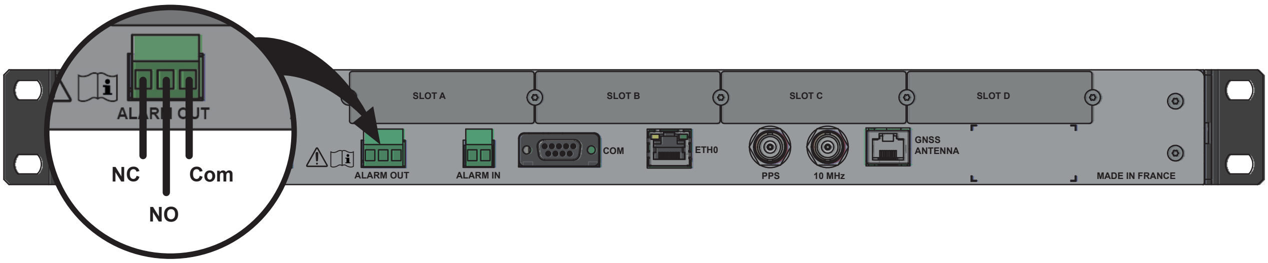
5 Slots for option cards:

- NETWORK option card (RJ45), ref. 907 920. Maximum 2 option cards [Slot A or B or C].
- NETWORK option card (SFP), ref. 907 921. Maximum 2 option cards [Slot A or B or C].
- PTP option card (RJ45 + SFP), ref. 907 922. Maximum 1 option card (Slot A or B or C or D].
- IRIG OUTPUT option card, ref. 907 930. Maximum 4 option cards [Slot A or B or C or D].
- IRIG INPUT option card, ref. 907 947. Maximum 1 option card [Slot A or B or C or D].
- ASCII option card, ref. 907 926. Maximum 4 option cards [Slot A or B or C or D].

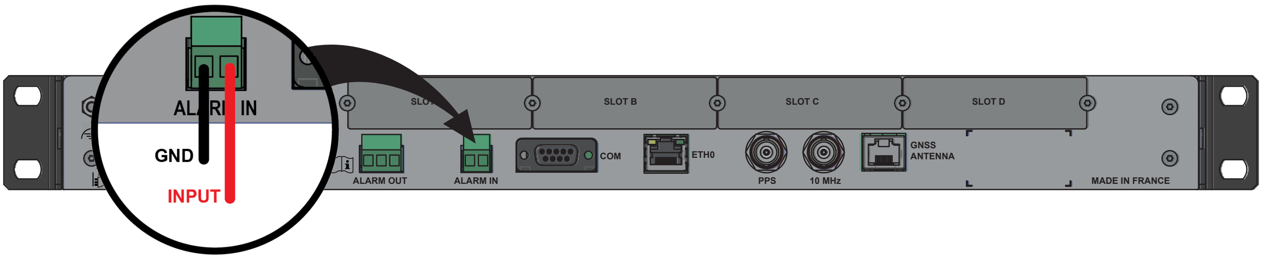
The option cards are installed in our production factory. For subsequent installation, please refer to the option card installation guide (ref: 608511).

[1] *Netsilon supports USB keys formatted to FAT16/FAT32 and NTFS.*

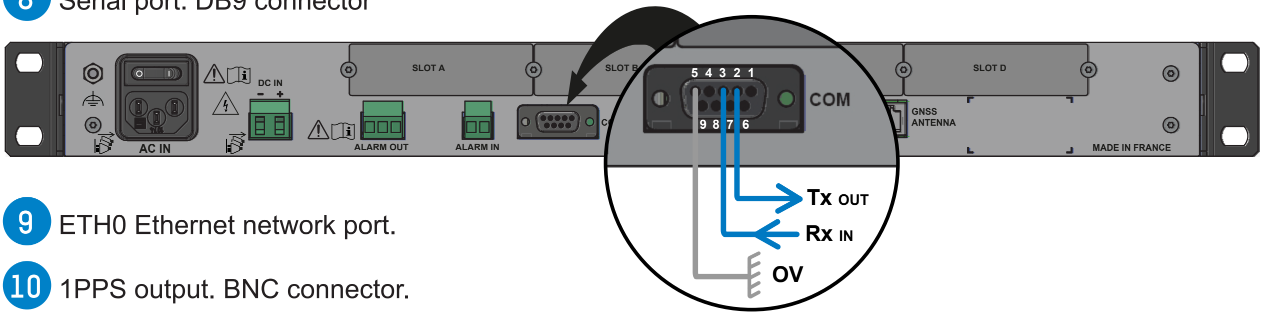
6 Common/Normally-Closed/Normally-Open relay contact output.
If contact Normally-Open: no alarms / if contact Normally-Closed: alarms.



7 Alarms input: interfaces with the dry contact of the client equipment.



8 Serial port. DB9 connector



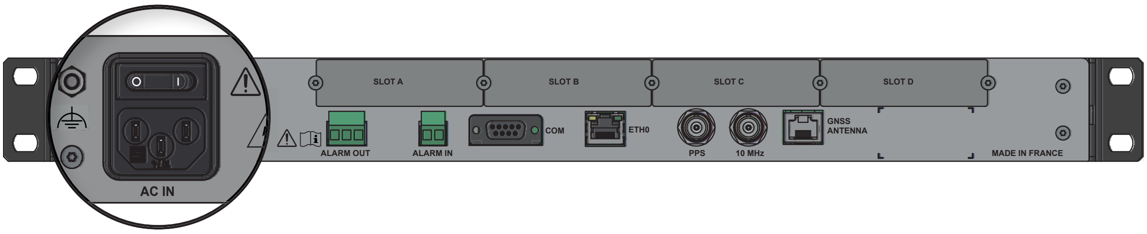
9 ETH0 Ethernet network port.

10 1PPS output. BNC connector.

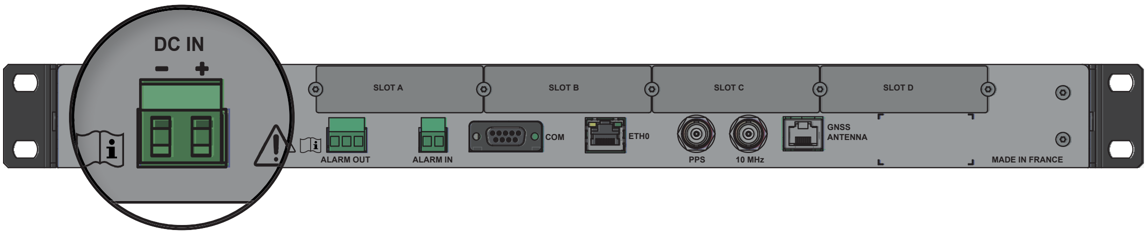
11 10 MHz output. BNC connector

12 GNSS antenna. RJ45 socket.

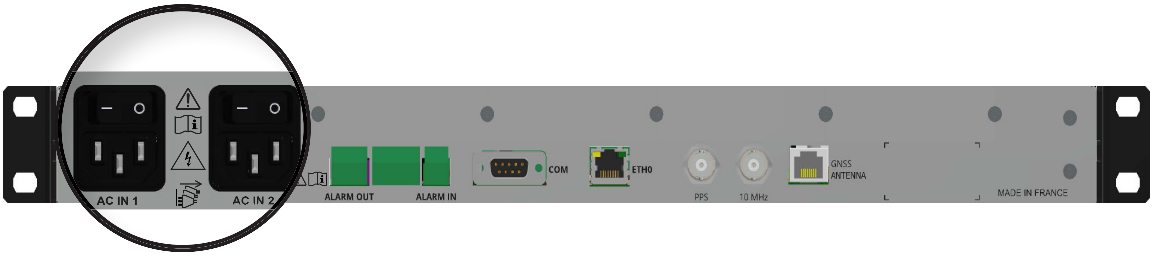
> NETSILON 9 / NETSILON 11 (AC)



> NETSILON 9 / NETSILON 11 (DC)



> NETSILON 9 / NETSILON 11 (AC+AC)



1.4 Specifications

1.4.1. *Accuracy*

	Typical values - Netsilon 9	Typical values - Netsilon 11
Accuracy[1]	$1x10^{-11}$	$1x10^{-11}$
Stability[2]	$1x10^{-9}$/day	$1x10^{-9}$/day
Holdover[3]	**15** µs (after 24 hours)	**2.5** µs (after 24 hours)

[1] *average after 24 hours with GPS signal*

[2] *average after 2 weeks with GPS signal*

[3] *typical value, after a 2-week GPS synchronisation at constant temperature*

1.4.2. *Connections for time synchronisation and broadcasting*

	Standard	Option
Inputs	GNSS NTP	NTP PTP IRIG
Outputs	NTP 10 MHz 1PPS	NTP PTP Coded time: NMEA 0183,... IRIG

1.4.3. *Mechanical characteristics*

Construction	Metal case – 1 U rack – 19”
Operating temperature	0°C to +50°C
Relative humidity at 40°C	0-90 % non-condensing
Protection index	IP20
Weight	2.5 kg
Dimensions	442 x 264 x 44.2 mm

1.4.4. *Electrical characteristics*

Power supply	AC : 100-240V∼ / 50-60Hz / 1.9-0.8A DC: 22-30V⎓ / 3.2-1.9 A AC+DC | Redundant power supplies, AC+AC | characteristics above.
Consumption	20 W (without option card)
Alarm input	Alarm IN Dry contact input, potential-free contact. $I_{IN} \leq 10$ mA
Alarm output	Alarm OUT NC-NO-C relay. Maximum current: 1A/50V⎓, 1A/30V∼
MTBF	100,000 hours

1.4.5. *Communications*

Network port	RJ45, 10/100/1000-BaseT (Gigabit)
Panel	USB- USB socket (can be disabled) for saving and updating the firmware. Keyboard (lockable) and LCD screen for network configuration.
Serial interface	COM - RS232 - DB9 connector

1.4.6. Network characteristics

PROTOCOLS

NTP V2, V3, V4	Compliant with RFC 1305 and 5905. Supports Unicast, Broadcast, Multicast, Anycast, MD5 authentication + MD5 integrity, peering and Autokey.
Maximum number of NTP requests per second: All Ethernet ports combined	7000
Maximum number of NTP clients (typical)	32 000
SNTP V3, V4	Compliant with RFC 1769, 2030, 4330 and 5905
TIME PROTOCOL	Compliant with RFC 868
DAYTIME PROTOCOL	Compliant with RFC 867

COMMUNICATION

HTTP/HTTPS	Compliant with RFC 2616 (management of signed certificates)
SSH	SSH v1.3, SSH v1.5, SSH v2 (OpenSSH)

MANAGEMENT

IP	IPv4, IPv6: Dual stack
VLAN	802.1Q standard (single/multi)

SERVICES

DHCP	DHCPv4, DHCPv6, Autoconf & Slaac
SMTP	Mail forwarding

SUPERVISION

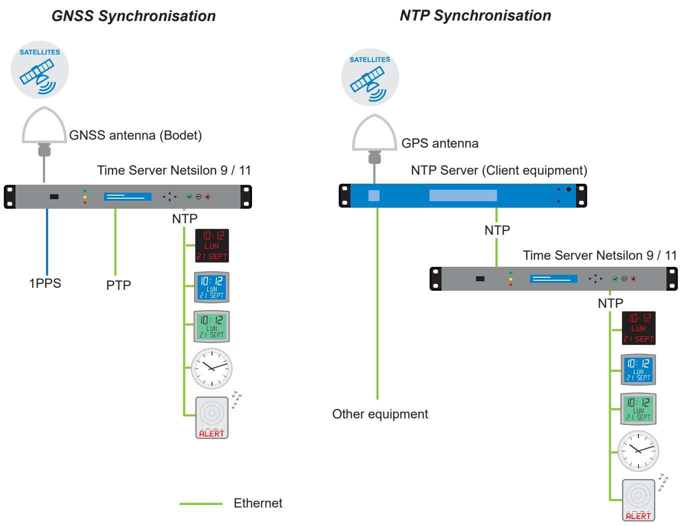
Alarm	SNMP traps, email and relay contact
SNMP	v1 (RFC 1157), v2c (RFC 1901-1908) and v3 (RFC 3411-3418) (traps + agents)
Syslog	Event log services
Relay contact / External input	Sending and receiving of alarms (Alarm OUT / Alarm IN)

1.4.7. Security features

- Enable/disable protocols,
- Authentication via 802.1x protocol,
- Redundancy via LACP protocol,
- Protection by single authentication (login + password) or authentication via LDAP / Radius,
- DES and AES encryption,
- SHA1, MD5 authentication,
- SSL/TLS: securing exchanges via computer network,
- SCP: secure copy of Netsilon files via a SSH session,
- SFTP: secure transfer of Netsilon files via a SSH session.

1.4.8. Synchronisation sources

Two synchronisation sources are available for the Netsilon 9 / 11: the BODET GNSS antenna or an NTP server present on the computer network.



2. INSTALLATION

This chapter provides an overview of the steps to be followed to install a Netsilon 9 or Netsilon 11.

Several factors must be taken into account when installing Netsilon 9 / 11:

1) The type of power supply: AC, DC, AC+DC, AC+AC
2) The type of installation: integration of a Netsilon 9 / 11 into an existing Ethernet network or new installation (ensure cable accessibility).
3) A PC connected to the Ethernet network with a web browser[1] such as Google Chrome®, Mozilla Firefox, Microsoft Edge or Internet Explorer® is required.

If Netsilon 9 / 11 is equipped with option cards, they must be configured from the web server, once network configuration is complete (via the ETH0 port).

2.1 Checking the package

Carefully unpack the time server and check the contents of the package. This must include:

- The Netsilon 9 or 11 unit, with its option cards,
- The two brackets for mounting in a 19” rack,
- A quick start guide.
- A safety instructions manual.

2.2 Security

This product has been carefully designed for your satisfaction according to the rules of our ISO9001 and ISO14001 quality system.
Before installing and configuring Netsilon, carefully read the various safety instructions.
Ensure that you observe the safety warnings and precautions at all times during the installation, operation and maintenance of your product.

⚠ **This device should be installed and maintained by qualified personnel, trained on BODET equipment.**

The device is connected to the mains. The installation must comply with the IEC 364 standard.

2.2.1. Installing the equipment

The installation and maintenance of this device must be performed by accredited personnel. This product must not be installed by untrained and unauthorised users/operators.
The electrical installation of this equipment must comply with the electrical standards in force in the country where the product is used.
This equipment is not suitable for use in places likely to receive children.

2.2.2. Opening the equipment

There are no user-serviceable parts inside this equipment. Please contact BODET customer support if the equipment needs to be repaired.
Do not open the product except when adding or replacing option cards and changing battery:

- ⚡ **Caution, risk of electric shock. Disconnect all power sources.**
- **Never open the product as long as power supplies indicated by the symbol are connected.**
- ⚠ **Ensure that all power supply sources are removed from the device before installing the option cards.**

The ON/OFF switch is of functional type. It is not a power supply disconnect switch. Disconnect the power supply and relay circuits before any intervention.

2.3 Mechanical rack installation

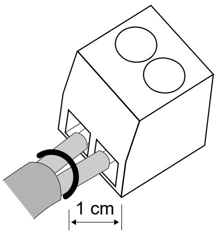
The Netsilon time server should be installed in a 19” rack or cabinet, using the two brackets supplied.

ℹ **We recommend that you install Netsilon in a secure location.**

[1] *It is recommended to have the latest version of the browser used.*

2.4 Electrical installation

All cables must be securely attached to the chassis before being connected to the various terminal blocks in order to prevent traction on connections. Furthermore, conductors on the same circuit must be attached to each other close to the terminal block to avoid reduced isolation should one of the terminals become loose.



The equipment must only be connected to the power supply once it has been securely mounted in the 19” destination rack.

2.4.1. *Power supply*

Power supply management according to version:

- Netsilon 9 / 11 (100-240V∼): mains power supply only.
  - Connect the power cord to the AC IN connector at the rear of the device.
- Netsilon 9 / 11 (22-30V⎓): direct current only.
  - Connect a DC cable and observe the polarity indicated at the rear of the device.
- Netsilon 9 / 11 (100-240V∼ + 22-30V⎓): mains power supply and/or direct current power supply.
  - Connect the power cord to the AC IN connector and/or a DC cable, being careful to observe the correct polarity indicated at the rear of the device.
- Netsilon 9 / 11 (100-240V∼ + 100-240V∼): dual mains power supply.
  - Connect the power cord(s) to the AC IN connector(s) at the rear of the device.

The functional earthing terminal can be attached to the cabinet frame (optional).

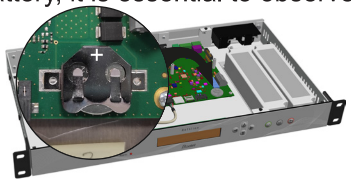
The DC IN power supply must be protected upstream by a 6.3 AT fuse.

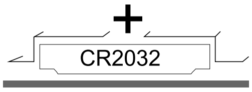
When several Netsilon units are powered by the same power supply, protect each DC IN input with a separate 6.3 AT fuse.

Be careful to observe the correct polarity indicated at the rear of the device.

2.4.2. *Backup battery - CR2032*

When replacing the CR2032 battery, it is essential to observe the polarity as indicated on the slot of the battery.





Caution:

- **There is a risk of explosion if the battery is replaced by a battery of incorrect type. Use only batteries recommended by the manufacturer.**
- **Dispose of used batteries in accordance with the instructions given on our website.**
- **The accumulator must not be swallowed, risk of chemical burns.**
- **Always keep new and discharged accumulators out of reach of children.**
- **This product contains a battery or a button accumulator. If swallowed, the battery or button accumulator can cause severe internal burns which may be fatal.**
- **If you suspect that an accumulator may have been ingested or inserted anywhere in the body, you must seek medical attention.**

2.4.3. *Ethernet*

The ETH0 Ethernet port, accessible on the rear panel of the device, enables easy connection to routers, switches or hubs.
1) Use a shielded CAT. 5E or CAT. 6 Ethernet cable (RJ45).
2) Connect the Ethernet network cable to the RJ45 connector on the Netsilon rear panel.

The product is commissioned by activating the ON/OFF switch on the rear panel of the device.
The Bodet company strongly recommends connecting and using Netsilon exclusively on a private network (VLAN).

2.4.4. *Alarm relay circuits*

For the relay circuits, provide protection by means of a fused disconnect switch or a circuit breaker of 1A maximum. Maintenance must be performed with power off. Disconnect the power supply and relay circuits under hazardous voltage.

3. COMMISSIONING

Netsilon configuration is performed exclusively on the web server. In order to be able to access the web server, it is necessary to configure the ETH0 port via the front panel keypad and the LCD screen.

⚠ **In order not to disrupt Netsilon synchronisation with the other products present on the network, it is important to maintain identification of the time server.**

There are two solutions for accessing the web server:

- With DHCP server: automatic assignment of an IP address.
- Without DHCP server: manual assignment of a fixed IP address via the control panel in the Netsilon network menu.

3.1 Factory configuration

The default configuration settings have been selected to facilitate initial configuration. A single account is activated when shipped from the factory.

- Default user account of the web server:
  - Username: bodetadmin
  - Password: admin49

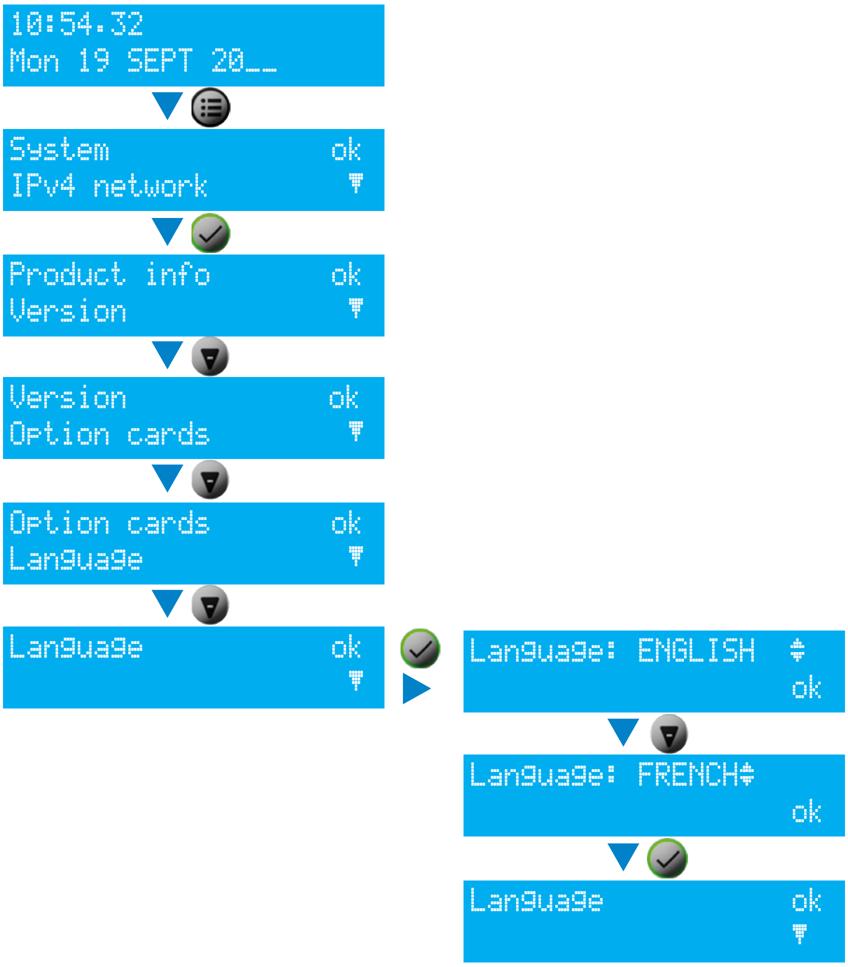
This account cannot be deleted. However, it is strongly recommended to change the password (see chapter 4.2.1.1 Changing the password of the default account).

When first running Netsilon, the default settings are as follows:

Functionalities	Default status	Means of configuration
Control panel & LCD screen	Unlocked	Control panel (technician menu) + web server
	Language: English	Web server
	Rotation of information: time, network, synchronisation and system status	Web server
USB port	Enabled	Web server
ETH0 Ethernet port	Services: HTTP: ON HTTPS: ON DNS: ON Console: ON SSH: ON	Web server
	IP address not given	Control panel + web server

3.2 Choosing the LCD screen display language

The network settings for configuration of the ETH0 port (assignment of an IP address) can be read or configured via the Netsilon control panel. It is necessary to first select the product’s display language:



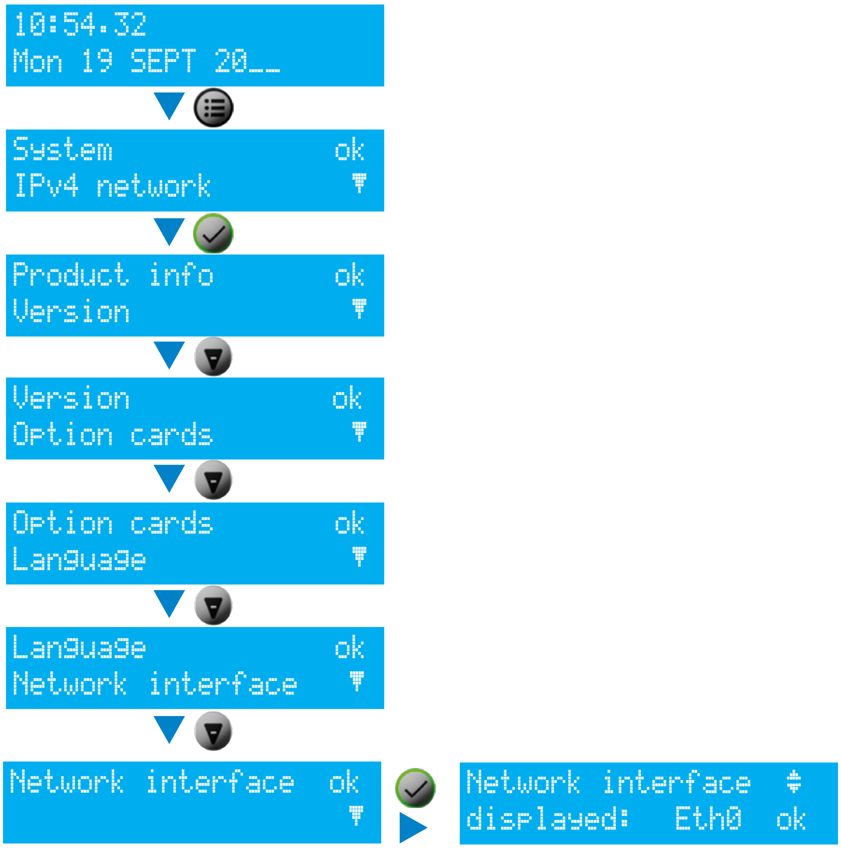
```
10:54.32
Mon 19 SEPT 20__

System              ok
IPv4 network

Product info        ok
Version

Version             ok
Option cards

Option cards        ok
Language

Language            ok

Language: ENGLISH
                    ok

Language: FRENCH
                    ok

Language            ok
```

Selection of available languages: English, French, Italian, Dutch, German and Spanish

Exit the menu by pressing the button.

3.3 Choosing the network interface

As the product is connected to the network, select the network interface concerned on the LCD screen:



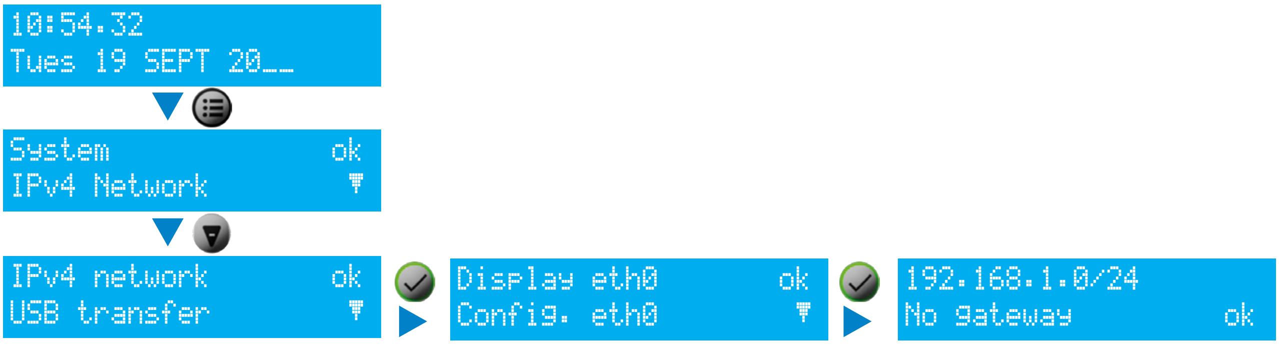
```
10:54.32
Mon 19 SEPT 20__

System              ok
IPv4 network

Product info        ok
Version

Version             ok
Option cards

Option cards        ok
Language

Language            ok
Network interface

Network interface   ok

Network interface
displayed:  Eth0    ok
```

Eth0 flashes. Select the interface using the keyboard navigation buttons.

3.4 Configuration with a DHCP server

1) On start up, the Netsilon 9 / 11 time server waits for automatic assignment of an IP address by the DHCP server. This may take a few minutes.

2) Once assigned, this IP address is shown on the LCD screen. By default, the LCD screen alternately displays several settings. To read the IP address on the LCD screen, consult the network menu using the Netsilon control panel and the LCD screen:



```
10:54.32
Tues 19 SEPT 20__
```

```
System          ok
IPv4 Network
```

```
IPv4 network    ok
USB transfer
```

```
Display eth0    ok
Config. eth0
```

```
192.168.1.0/24
No gateway      ok
```

3) Enter the IP address as seen on the LCD screen into the web browser (Google Chrome®, Mozilla Firefox, Microsoft Edge or Internet Explorer®).

4) See chapter **4. Configuration on web server.**

192.168.1.0/24 is the IP address with CIDR notation.

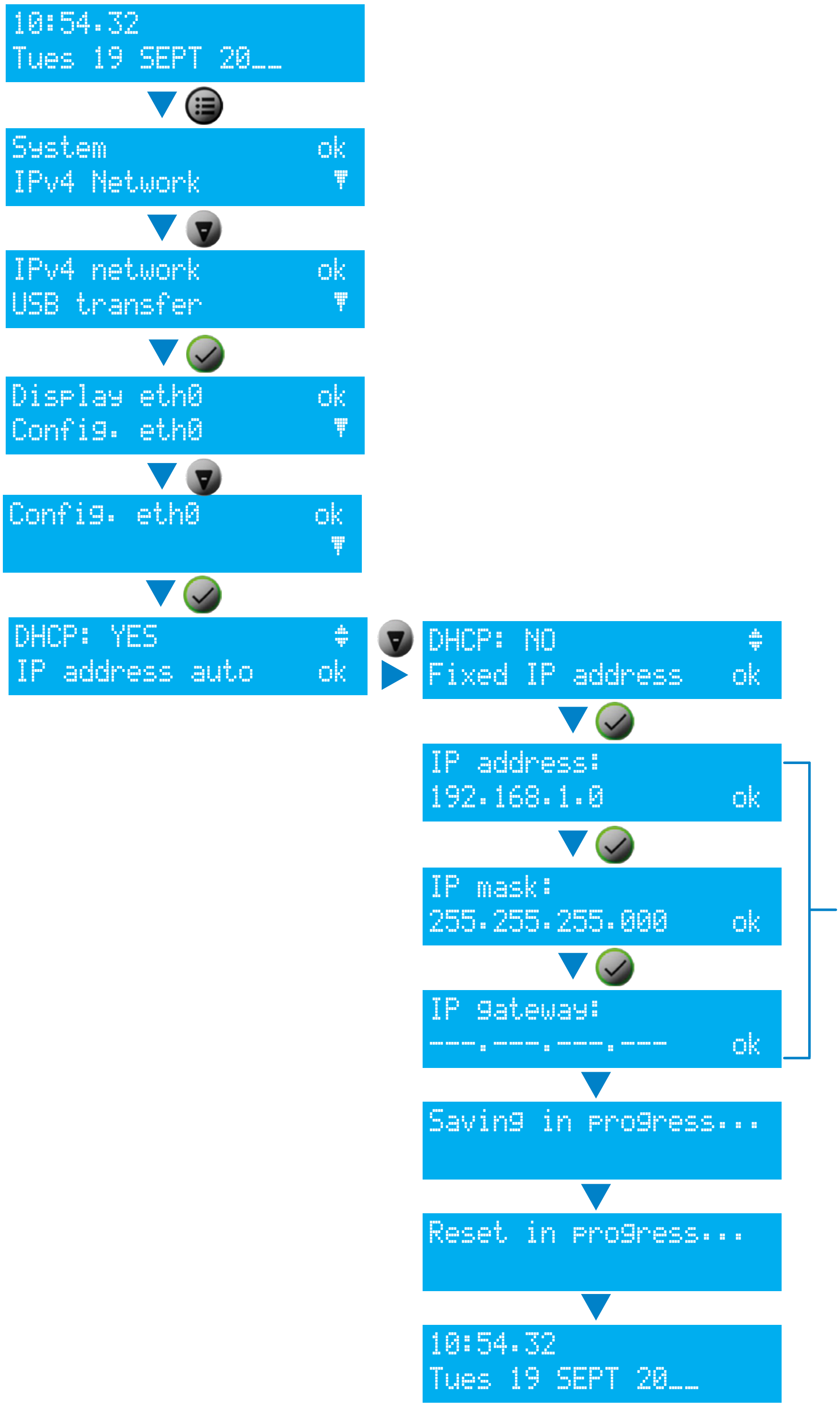
3.5 Configuration without a DHCP server

Without automatic assignment of an IP address by a DHCP server, it is necessary to manually assign a fixed IP address.

To manually configure the Netsilon network settings, enter the following three parameters:

- IP address assignment
  - This is a unique address assigned to Netsilon by the network administrator. Ensure that the chosen address is available. Ensure that the chosen address is available.
- Subnet mask
  - The subnet mask defines the number of bits taken by the IP address. The number of bits used in the network mask may range from 8 to 30 bits.
- Gateway
  - The gateway address is required if communication with Netsilon is made outside the local network. By default, the gateway is disabled.

To configure these three parameters, use the Netsilon network menu, via its control panel:



```
10:54.32
Tues 19 SEPT 20__
```

```
System          ok
IPv4 Network     ▼
```

```
IPv4 network    ok
USB transfer     ▼
```

```
Display eth0    ok
Config. eth0     ▼
```

```
Config. eth0    ok
                 ▼
```

```
DHCP: YES        ⇕
IP address auto ok
```

```
DHCP: NO         ⇕
Fixed IP address ok
```

```
IP address:
192.168.1.0     ok
```

```
IP mask:
255.255.255.000 ok
```

```
IP gateway:
---.---.---.--- ok
```

```
Saving in progress...
```

```
Reset in progress...
```

```
10:54.32
Tues 19 SEPT 20__
```

Enter the values with the ▼ and ▲ keys.
Note: these values are determined by the network administrator.

4. CONFIGURATION VIA WEB SERVER

The order of the chapters corresponds to the steps to be completed as part of an initial commissioning. It is important to observe this order to ensure correct deployment of the system.

An administrator profile is required to modify the web server parameters presented in this chapter. To view rights according to the profile used, please refer to **Annex 3: rights according to profile**.

To access the Netsilon web server, follow these steps:

1) Note the Netsilon IP address.

2) Open a web browser page.

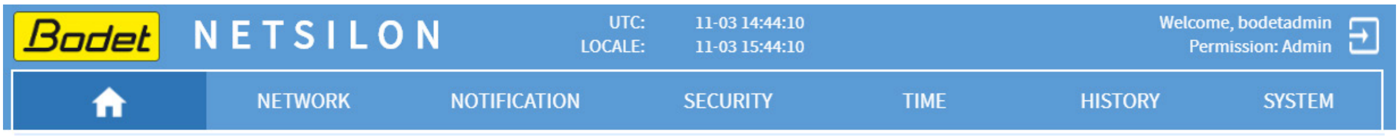
3) Enter the IP address into the browser's address bar.

4) Enter the username and default password to access the web server. As a reminder:

- Username: bodetadmin
- Password: admin49

4.1 Start-up

4.1.1. Presentation of the main menu



UTC: 11-03 14:44:10
LOCALE: 11-03 15:44:10

Welcome, bodetadmin
Permission: Admin

⌂ : dashboard which can be used to view the status of synchronisation, sources, alarms, power supplies, outputs and unacknowledged alarms.

NETWORK : configuration of interfaces, static routes and network services.

NOTIFICATION : configuration of alarms, alarm thresholds, SNMP traps, SMTP and Syslog.

SECURITY : local or centralised user management (LDAP, RADIUS), SNMP agents, SSH, HTTP/HTTPS services, certificates and keys..

TIME : configuration of synchronisations (configuration, status and priority of sources), outputs, Time zone and time scales (TAI/UTC offset, Leap Second Manual).

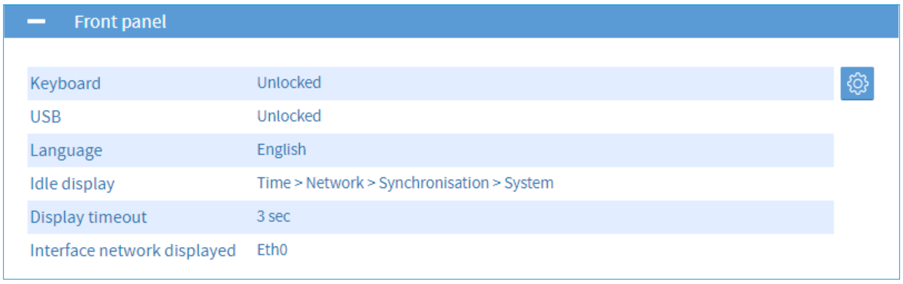
HISTORY : consultation of GNSS, NTP, PTP, IRIG (depending on the options selected) and oscillator statistics, NTP logs, Syslog logs and acknowledgement of alarms.

SYSTEM : configuration of the system, the LCD screen display, consultation of firmware versions, online help and system tools (upgrade and backup, restarting, option card versions and log exporting).

4.1.2. Configuring the Netsilon front panel

To configure the interface (LCD display, USB port and control panel), follow these steps:

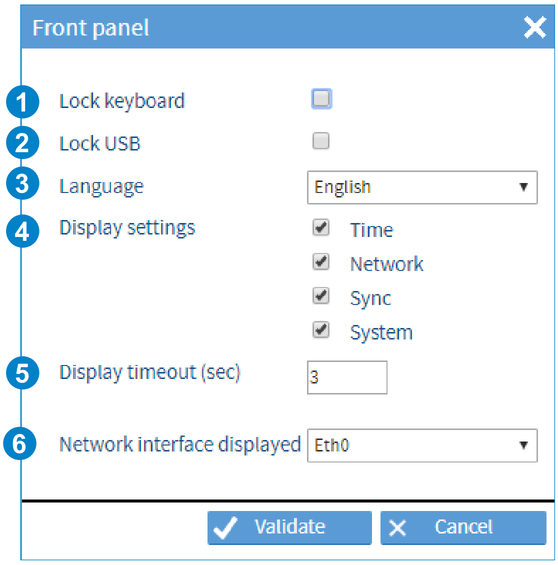
1) SYSTEM MENU > General > Front panel:



Front panel

Keyboard	Unlocked
USB	Unlocked
Language	English
Idle display	Time > Network > Synchronisation > System
Display timeout	3 sec
Interface network displayed	Eth0

2) Click on ⚙, the following window will appear:



Lock keyboard ☐

Lock USB ☐

Language: English

Display settings: ☑ Time ☑ Network ☑ Sync ☑ System

Display timeout (sec): 3

Network interface displayed: Eth0

3) Perform the desired configuration:

1 Can be used to lock the Netsilon control panel when the box is checked.

- This function can be used to prevent any misuse by a third party.

2 Can be used to disable the operation of the USB port located on the panel when the box is checked.

- This function can be used to prevent the insertion of a USB key containing malicious files by a third party.

3 Can be used to select the language displayed on the Netsilon LCD screen.

- By default: English
- Available languages: English, French, Spanish, German, Dutch, Italian.

4 Can be used to select the scrolling parameters displayed on the LCD standby screen:

- **Time**
  - Local time and date.
- **Network**
  - IP address
  - Subnet mask
  - Gateway.
- **Synchronisation**
  - Display of source(s) of synchronisation (primary and/or secondary).
- **System**
  - Display of system status (synchronised, holdover, change of reference between primary and secondary synchronisation, non-synchronised and autonomous). In order to understand these statuses, refer to **Annex 1: synchronisation**.

5 Can be used to set the scrolling display time between each element (Time, Network, Synchronisation and System) in seconds. The default time is three seconds, but can be programmed between three and ten seconds.

6 Choice of the network interface for displaying and configuring parameters on the display.

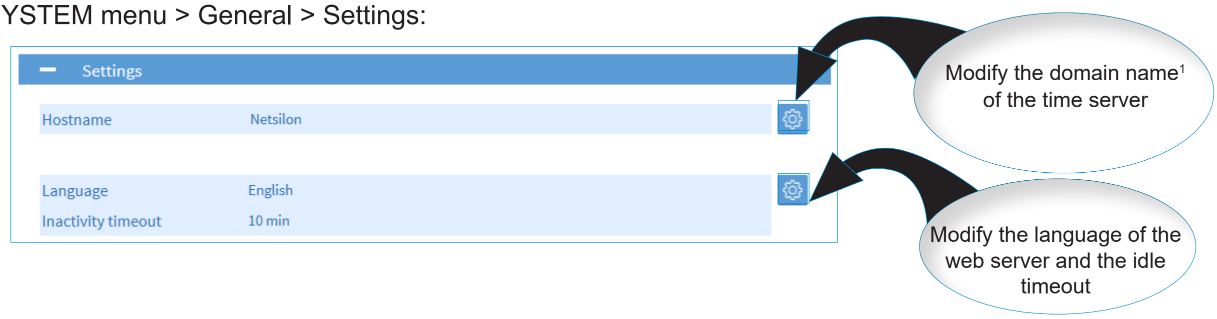
4) Click on ✓ Validate to apply the changes.

4.1.3. *Changing the language*

To make the configuration easier, it is recommended to select the language you are the most comfortable with:

To choose the web server display language, follow these steps:

1) SYSTEM menu > General > Settings:



Settings

Hostname	Netsilon
Language	English
Inactivity timeout	10 min

Modify the domain name[1] of the time server

Modify the language of the web server and the idle timeout

2) **English is the default language.** It is also possible to set the period of time after which the web server will disconnect and return to the login page.

After configuring each parameter, click on Save **to apply the changes.**

4.2 Managing users

4.2.1. *Local management*

Entering an incorrect username or password will generate an alarm (if enabled).

There is an automatic disconnection timeout, after which the user will be logged out and any unsaved changes may be lost. By default, the inactivity timeout is 10 minutes.
(can be changed to between 5 and 30 minutes)

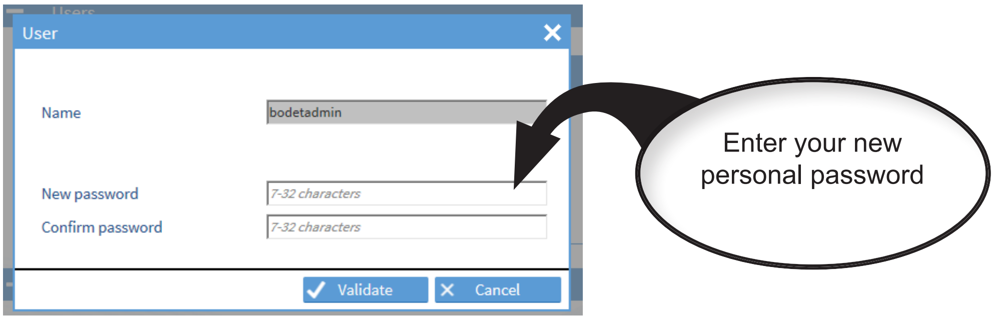
4.2.1.1 Changing the password

As a reminder, it is strongly recommended to change the default password before beginning Netsilon configuration.

To change the default administrator account password, follow these steps:

1) SECURITY menu > User management > Local users

2) Click on Change my password , the following window will appear:



User

Name	bodetadmin
New password	*7-32 characters*
Confirm password	*7-32 characters*

Enter your new personal password

3) Click on ✓ Validate to apply the changes.

The password can be entered using the following parameters:

Authorised alphabet: A-Z + a-z + 0-9 + special characters: !#$%&()*+,-./ :; «<=>?@[]^_{|}~µ§ with a total of 94 symbols (including 32 special characters). Please note that the SSH or RS232 client must be configured in UTF8 (to support the µ and § characters).

Netsilon offers SHA-512 password encryption. It is also recommended to enable HTTPS for extra security.

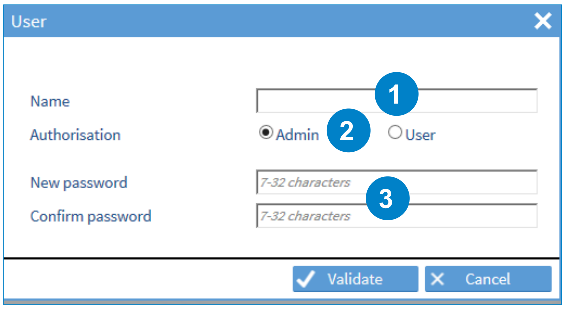
[1] *The domain name must be unique. Once changed, this will lead to regeneration of the Autokey certificate.*

4.2.1.2 Creating or modifying an account

To create a new account, follow these steps:

1) SECURITY menu > User management > Local users

2) Click on + to add an account, and the following window will appear:



User ✕

Name

Authorisation ● Admin ○ User

New password 7-32 characters

Confirm password 7-32 characters

✓ Validate ✕ Cancel

1 Enter a username between 5 and 32 characters

2 Select a profile type

3 Enter a password between 7 and 32 characters

3) Click on ✓ Validate to apply the changes.

Netsilon can manage up to 20 users. The use of duplicate users is not allowed.
The username can be entered using the following parameters:
Authorised alphabet: a-z, A-Z, 0-9, -_.@

Please refer to Annex 3 to see the differences between administrator and user profiles.

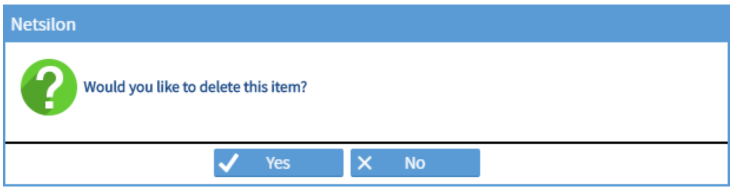
4.2.1.3 Deleting an account

To delete an account, follow these steps:

1) SECURITY menu > User management > Local users

2) Click on the account to be deleted (in order to select it)

3) Click on − to delete the account, and the following window will appear:



Netsilon

Would you like to delete this item?

✓ Yes ✕ No

3) Click on ✓ Yes to confirm.

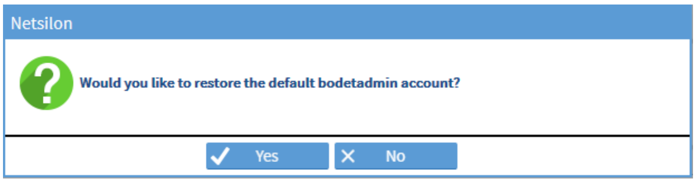
It is impossible to delete the default administrator account.

4.2.1.4 Restoring the default password

In order to restore the default administrator account password, follow these steps:

1) SECURITY menu > User management > Local users

2) Click on Restore default admin account , and the following window will appear:



Netsilon

Would you like to restore the default bodetadmin account?

✓ Yes ✕ No

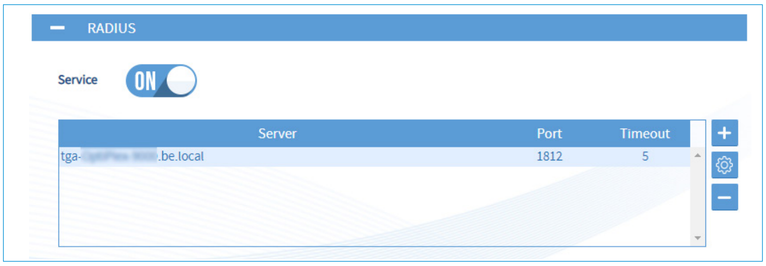
3) Click on ✓ Yes to apply the changes.

4.2.2. Centralised management

4.2.2.1 RADIUS service

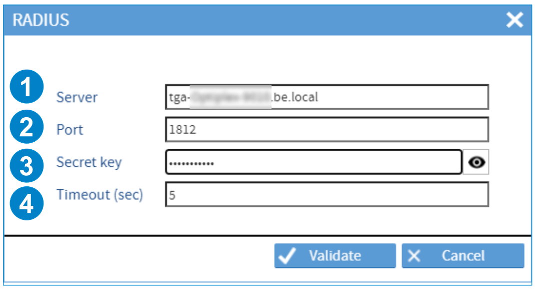
RADIUS authentication (Remote Authentication Dial-In User Service) implies the use of an external server allowing centralised management of users to log in to Netsilon. The login password entered by the user is stored in a RADIUS server on the network. Client/server exchanges are secured via a shared secret key.
To enable and configure a RADIUS server:

1) SECURITY Menu > User management > RADIUS
Enable the service using the ON button.



Server	Port	Timeout
tga-[redacted].be.local	1812	5

2) Add a RADIUS server by clicking on +, and the following window will appear:



RADIUS

1 Server: tga-[redacted].be.local
2 Port: 1812
3 Secret key: ••••••••••
4 Timeout (sec): 5

3) Enter the RADIUS server information:
(Possibility to add up to five servers maximum)

1 Enter the IP address or the host name,
2 Enter the RADIUS port number (default network port: 1812),
3 Enter the shared security key (MD5 cryptographic hash) with Netsilon, (6 to 64 characters)
4 Enter the timeout (waiting time before communication with Netsilon), (programmable from 3 to 60 seconds)

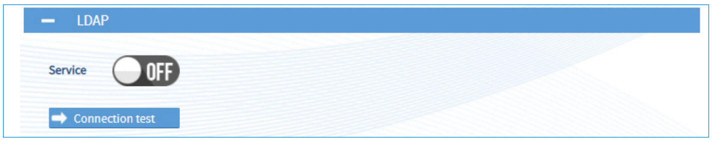
It is strongly recommended to use different user names between those used via the RADIUS server and those used locally. Do not duplicate users (declaration of local accounts in RADIUS and vice versa). In local and RADIUS, the following users are not allowed: «radius_user», « radius_users».

4.2.2.2 LDAP service

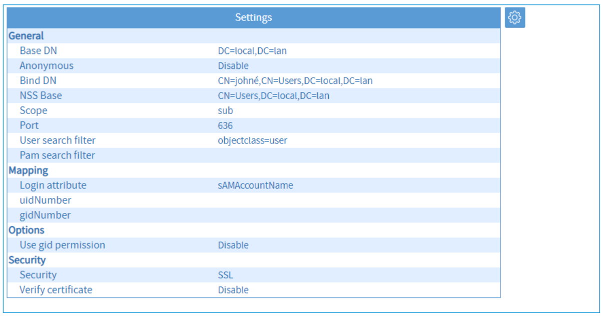
LDAP authentication (Lightweight Directory Access Protocol) implies the use of an external server allowing centralised management of users to log in to Netsilon. The login password entered by the user is stored in an LDAP server on the network. This protocol gives access to information databases on the network's users using directory interrogation. Access to the data stored in the database is secured through encryption and authentication mechanisms.

To enable and configure the LDAP service:

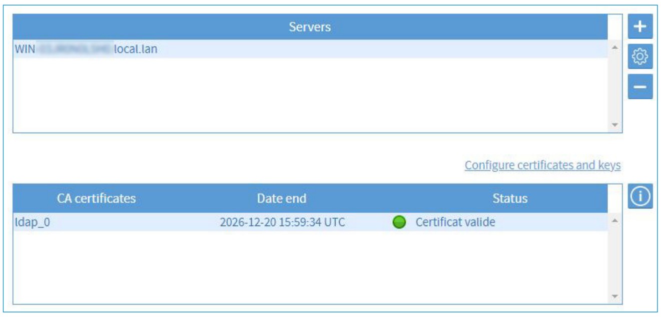
1) SECURITY Menu > User management > LDAP
Enable the service using the ON button. Enabling/disabling the service causes a restart of the product.



At the end of the configuration, click on Connection test to ensure that the configuration is consistent (valid connection to the server). This test button is only functional if the service is disabled.



Settings	
General	
Base DN	DC=local,DC=lan
Anonymous	Disable
Bind DN	CN=johné,CN=Users,DC=local,DC=lan
NSS Base	CN=Users,DC=local,DC=lan
Scope	sub
Port	636
User search filter	objectclass=user
Pam search filter	
Mapping	
Login attribute	sAMAccountName
uidNumber	
gidNumber	
Options	
Use gid permission	Disable
Security	
Security	SSL
Verify certificate	Disable

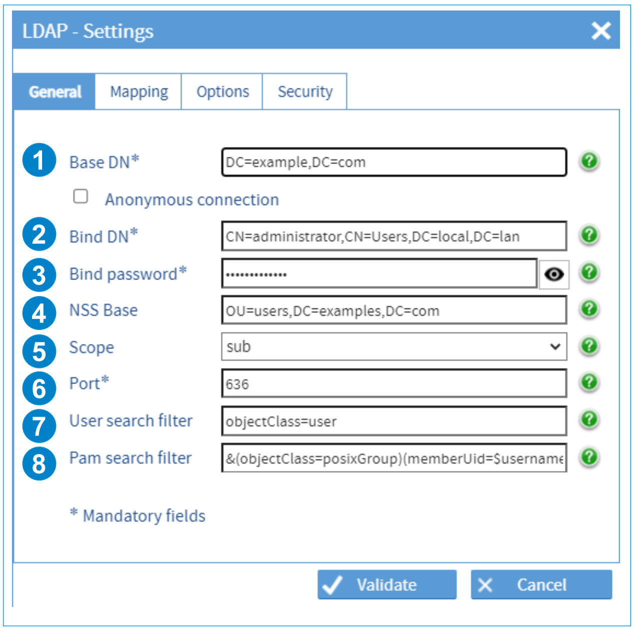


Servers
WIN [redacted] local.lan

Configure certificates and keys

CA certificates	Date end	Status
ldap_0	2026-12-20 15:59:34 UTC	● Certificat valide

2) To make the settings, click on ⚙, and the following window will appear:



LDAP - Settings

1 Base DN* DC=example,DC=com

□ Anonymous connection

2 Bind DN* CN=administrator,CN=Users,DC=local,DC=lan

3 Bind password* ••••••••••••••

4 NSS Base OU=users,DC=examples,DC=com

5 Scope sub

6 Port* 636

7 User search filter objectClass=user

8 Pam search filter &(objectClass=posixGroup)(memberUid=$username

* Mandatory fields

3) Fill in the various fields to configure the settings:

Tab - General

1 Base DN (Distinguished Name): enter the name of the search base containing the server directories to be queried for an authentication match. Typically, this is the top level of the LDAP directory tree. DN is the identifier of an LDAP entry (path in the tree).

2 Bind DN (Distinguished Name to bind server with): Enter a user on the LDAP server authorised to search the LDAP directory (in its entirety or partially). The function of the Bind DN is to query the directory with filtering requests in order to authorise or not the authentication of users.
This field is hidden if the Anonymous connection function is enabled.

3 Enter the password corresponding to the Bind DN user authorised to search the directory. This field is hidden in the case of an “anonymous connection”.
The button 👁 allows the password to be viewed only when entered.

4 Enter the search base settings (DN) to indicate the entry point of the users search.

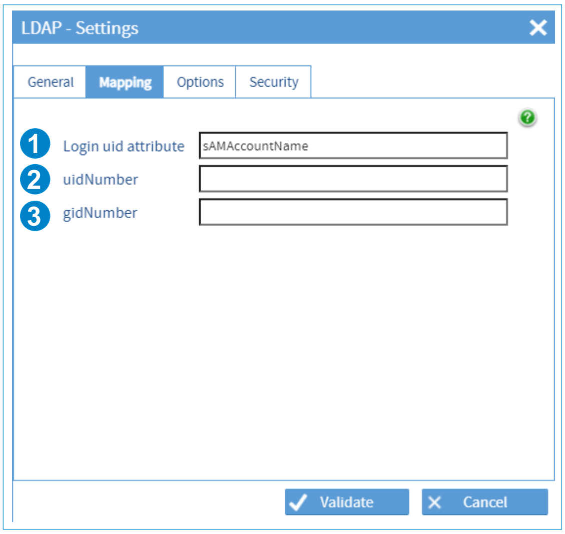
5 Choose an LDAP search scope, among “Sub”, “One”, and “Base”:
- Sub: the entire search base (all entries) is concerned,
- One: only the entries immediately subordinated to the entry specified as the search base are concerned,
- Base: only the entry specified as the search base is concerned.

6 Choose the LDAP service port number according to the security settings.
Default standard ports: Disabled: 389, StartTLS: 389, SSL: 636.

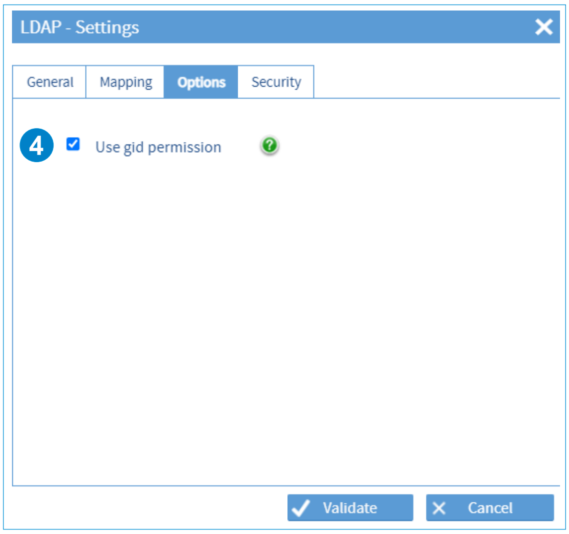
7 Enter a search filter to select the entries to be returned in a search operation.

8 Enter an additional filter, if the user matches the filter rules, access is granted, otherwise access is denied. Example: &(objectClass=posixGroup)(memberUid=$username)(cn=group01).

Tab - Mapping / Options



1 Login uid attribute: sAMAccountName
2 uidNumber:
3 gidNumber:



4 ☑ Use gid permission

If one or several variables do not exist in your LDAP server database in the user account section, the connections will be impossible. However, it is possible to map the following variables “Login uid attribute”, “uidNumber” and “gidNumber” to other variables.

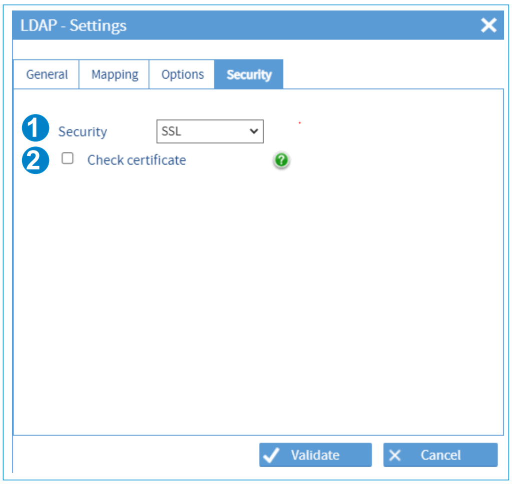
1 Variable corresponding to the login attribute used during the connection. For example, this variable can be mapped to sAMAccountName in the case of an Active Directory server (Microsoft).

2 uidNumber is a user identifier. Users must have a uidNumber whose value must exceed or equal 1050. When mapping to another attribute, make sure that the value exceeds or equals 1050 by user.
uidNumber can be declared manually by user in the case of an Active Directory server (Microsoft).

3 gidNumber is a group identifier that must exceed or equal 1 in the case of a Netsilon authentication. When mapping to another attribute, make sure that the value exceeds or equals 1 by user.

4 If the option is not activated, users must have a gidNumber which exceeds or equals 1, which will allow them to access Netsilon with the administrator rights.
If the option is activated, Netsilon checks the gidNumber of the user to grant it rights:
- gidNumber = “111”: users will be granted administrator rights.
- gidNumber = “112” or a value that exceeds or equals 1: users will be granted user rights.

Tab - Security



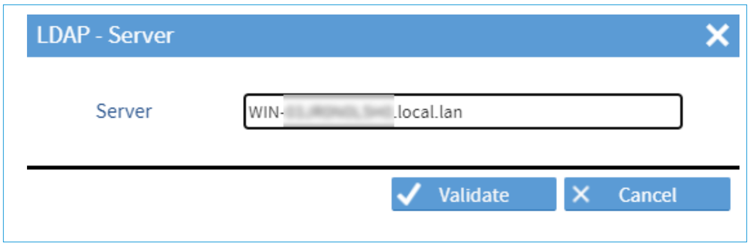
1 Security: SSL
2 □ Check certificate

1 Choose the security option: disabled, SSL (encryption of exchanges/passwords),StartTLS.
This involves a TCP port number switch.

2 Check to enable certificate verification.
If enabled, the server certificate is required.
By default, if no certificate is provided (or a faulty one), the session is automatically terminated.

Adding a certificate allows to generate an encryption and avoid a clear link.
Verification of the certificate allows the authenticity of the server to be checked.
To add a certificate, see chapter 4.10 Certificate and key management.

4) Add an LDAP server by clicking on +, and the following window will appear:
(Possibility to add up to five servers maximum)



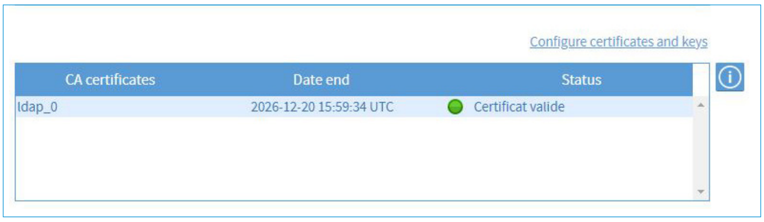
LDAP - Server

Server: WIN-[redacted].local.lan

Enter the IP address or host name of the LDAP server.

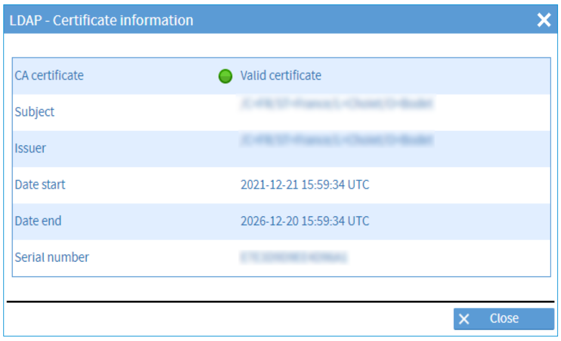
For certificate validation, it is mandatory to indicate the full host name of the LDAP server.
It is strongly recommended to use different user names between those used via the LDAP server and those used locally.
Do not duplicate users (declaration of local accounts in LDAP and vice versa).

5) Click on ⓘ to view the certificate information that may have been imported from the certificate menu and on configure certificates and keys to access this menu.



Configure certificates and keys

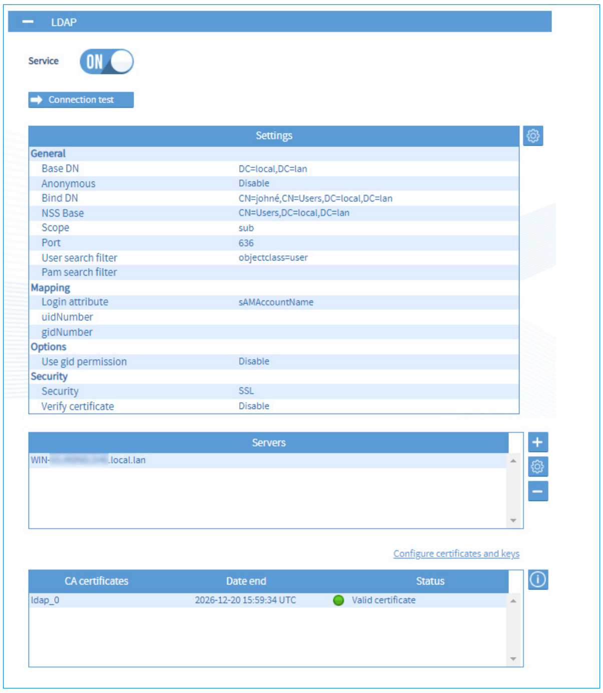
CA certificates	Date end	Status
ldap_0	2026-12-20 15:59:34 UTC	● Certificat valide



LDAP - Certificate information

CA certificate	● Valid certificate
Subject	[redacted]
Issuer	[redacted]
Date start	2021-12-21 15:59:34 UTC
Date end	2026-12-20 15:59:34 UTC
Serial number	[redacted]

The following are examples of typical LDAP service configurations:



LDAP

Service: ON

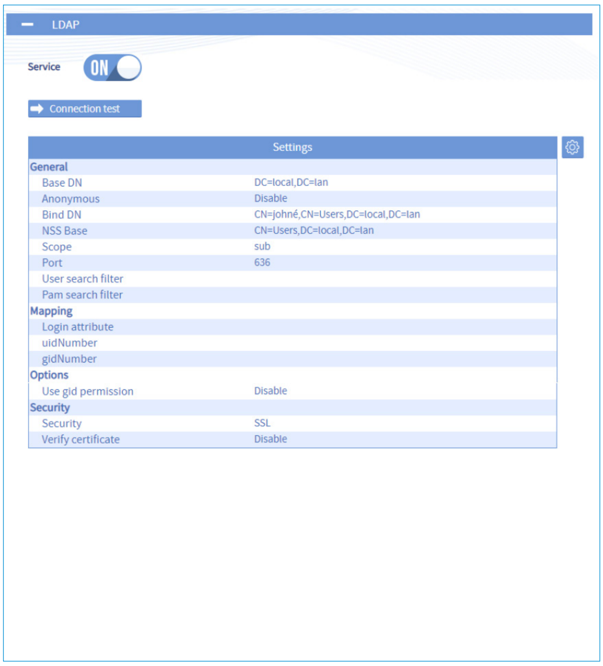
Settings	
General	
Base DN	DC=local,DC=lan
Anonymous	Disable
Bind DN	CN=johné,CN=Users,DC=local,DC=lan
NSS Base	CN=Users,DC=local,DC=lan
Scope	sub
Port	636
User search filter	objectclass=user
Pam search filter	
Mapping	
Login attribute	sAMAccountName
uidNumber	
gidNumber	
Options	
Use gid permission	Disable
Security	
Security	SSL
Verify certificate	Disable

Servers
WIN-[redacted].local.lan

Configure certificates and keys

CA certificates	Date end	Status
ldap_0	2026-12-20 15:59:34 UTC	● Valid certificate

Windows Active directory server in secure mode



LDAP

Service: ON

Settings	
General	
Base DN	DC=local,DC=lan
Anonymous	Disable
Bind DN	CN=johné,CN=Users,DC=local,DC=lan
NSS Base	CN=Users,DC=local,DC=lan
Scope	sub
Port	636
User search filter	
Pam search filter	
Mapping	
Login attribute	
uidNumber	
gidNumber	
Options	
Use gid permission	Disable
Security	
Security	SSL
Verify certificate	Disable

OpenLdap linux server

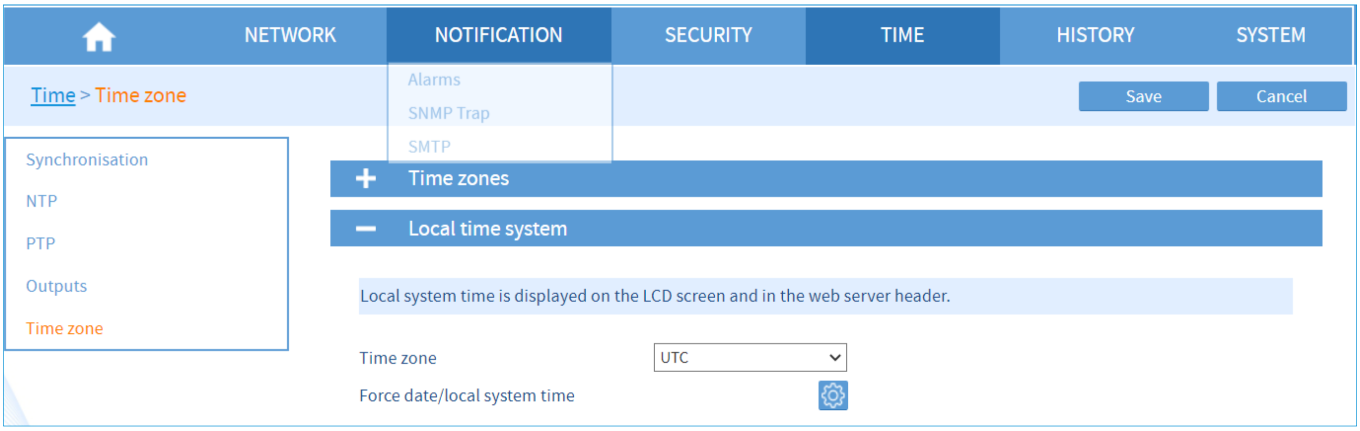
4.3 Configuring the time zone

The time zone section enables centralised time zone creation and time scale management. Each output can be defined in a time zone, defined earlier in this chapter.

4.3.1. *Defining the local time system and date*

The local time should only be changed when replacing the CR2032 battery.

For the local time system and date, follow these steps:
1) TIME menu > Time zones > Local time system.



Time > Time zone

＋ Time zones

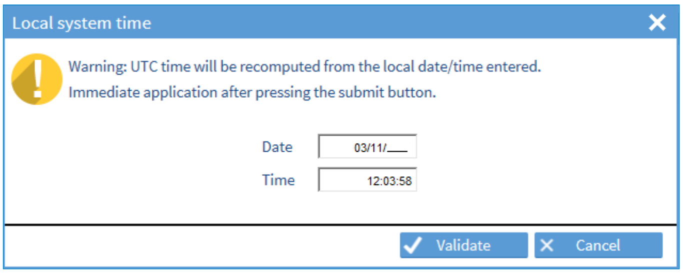
－ Local time system

Local system time is displayed on the LCD screen and in the web server header.

Time zone: UTC

Force date/local system time ⚙

2) Click on ⚙, and the following window will appear:



Local system time

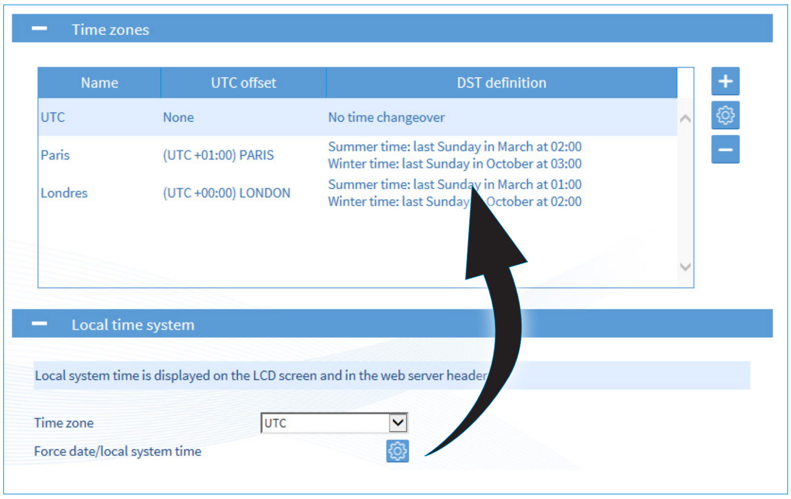
Warning: UTC time will be recomputed from the local date/time entered.
Immediate application after pressing the submit button.

Date: 03/11/____

Time: 12:03:58

3) Manually change the time and date.

4) Select the time zone from the drop-down menu. Time zones previously added are shown:



－ Time zones

Name	UTC offset	DST definition
UTC	None	No time changeover
Paris	(UTC +01:00) PARIS	Summer time: last Sunday in March at 02:00 Winter time: last Sunday in October at 03:00
Londres	(UTC +00:00) LONDON	Summer time: last Sunday in March at 01:00 Winter time: last Sunday in October at 02:00

－ Local time system

Local system time is displayed on the LCD screen and in the web server header.

Time zone: UTC

Force date/local system time ⚙

The local time is the time displayed on the LCD screen.

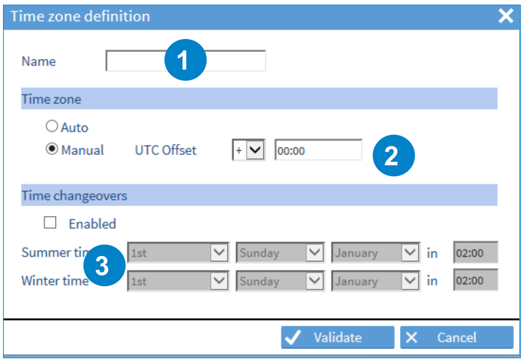
4.3.2. *Creating a time zone manually*

To create a time zone, follow these steps:

1) TIME menu > Time zone > Time zones.

The UTC reference is present by default.

2) Click on + to create a zone, then tick **Manual**, and the following window will appear:



1. Enter the name of the time zone.
2. Define the time offset as compared to the UTC reference. The drop-down menu can be used to assign a positive or negative offset. Enter the desired hours and minutes for this offset. The maximum manual offset is limited to -12hrs/+14hrs.
3. If the zone is subject to a time change: enable then enter the desired time changes.

It is possible to select a periodic day in a month or to define a date.

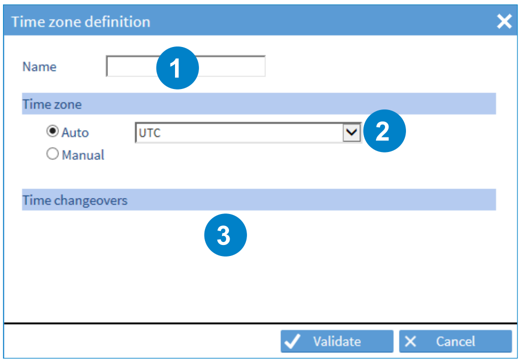
4.3.3. *Creating a time zone automatically*

To add a time zone, follow these steps:

1) TIME menu > Time zone > Time zones.

The UTC reference is present by default.

2) Click on + to add a time zone, and the following window will appear:



1. Enter the name of the new time zone.

2. Select the time zone from the drop-down menu:

UTC OFFSET	CITIES
UTC-10:00	HAWAI
UTC-08:00	LOS ANGELES
UTC-07:00	DENVER
UTC-06:00	CHICAGO
UTC-05:00	NEW YORK
UTC-04:00	FORT-DE-FRANCE
UTC-03:00	CAYENNE
UTC-01:00	AZORES
UTC+00:00	LONDON
UTC+01:00	PARIS
UTC+01:00	TUNIS
UTC+02:00	HELSINKI
UTC+03:00	MOSCOW
UTC+03:00	SAINT-DENIS

UTC+04:00	ABU DHABI
UTC+05:30	CALCUTTA
UTC+07:00	BANGKOK
UTC+08:00	SINGAPORE
UTC+09:00	TOKYO
UTC+09:30	ADELAIDE
UTC+10:00	SYDNEY
UTC+11:00	NOUMEA

3 Time changes are indicated in accordance with the chosen time zone.

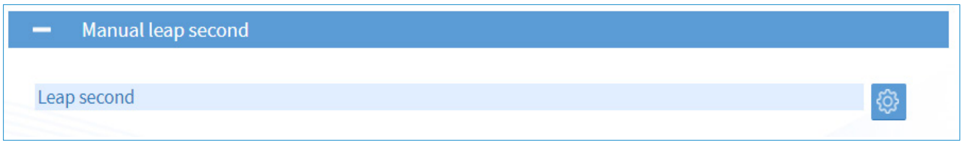
It is possible to create up to 20 time zones (including UTC).
The UTC time zone cannot be deleted.

4.3.4. Programming a manual Leap Second

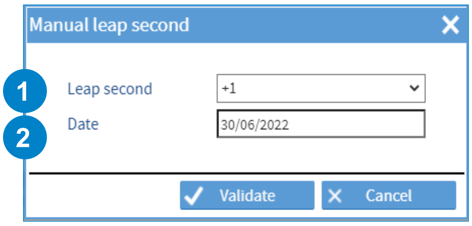
If the programming of a Leap Second is planned and if Netsilon is synchronised from a source that does not manage this information (e.g IRIG synchronisation), then it must be entered manually in Netsilon.
Without this information, it will be not transmitted to the NTP clients and a time jump of one second will be effective after the Leap Second has passed.
If Netsilon is PTP Master, the TAI / UTC offset will not be updated.

To program a manual Leap Second, follow these steps:

1) TIME menu > Time zone > Manual leap second



2) Click on ⚙ to define the Leap Second, and the following window will appear:



Manual leap second

1 Leap second: +1

2 Date: 30/06/2022

1 Enter the Leap Second value: +/- 1 second.

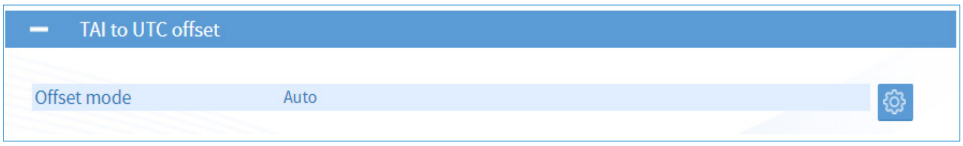
2 Enter the date of the Leap Second: **programming for the 30/06 or the 31/12 is mandatory.**

If the Leap Second information is managed by the synchronisation source used, it is always possible to program a manual Leap Second. This one takes over and ensures that Leap Second is applied.
The manual Leap Second is erased as soon as it is passed.

4.3.5. Set TAI / UTC offset

If the synchronisation source used does not provide the Leap Second information (e.g: IRIG) and if Netsilon broadcasts in TAI, this value must be entered manually in Netsilon.
The TAI/UTC offset is particularly dedicated to the particular case of IRIG synchronisation when Netsilon is also PTP master (see chapter 4.5.5 IRIG INPUT option card).

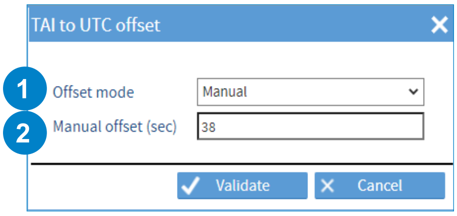
To manually enter the TAI/UTC offset, follow these steps:
1) TIME menu > Time zone > TAI to UTC offset



TAI to UTC offset

Offset mode Auto

2) Click on ⚙ to configure the offset management, and the following window will appear:



TAI to UTC offset

1 Offset mode: Manual

2 Manual offset (sec): 38

1 Define the offset mode: automatic/manual.
If the synchronisation source provides the number of Leap Second, the choice of the automatic mode is recommended. If not, choose the manual mode.

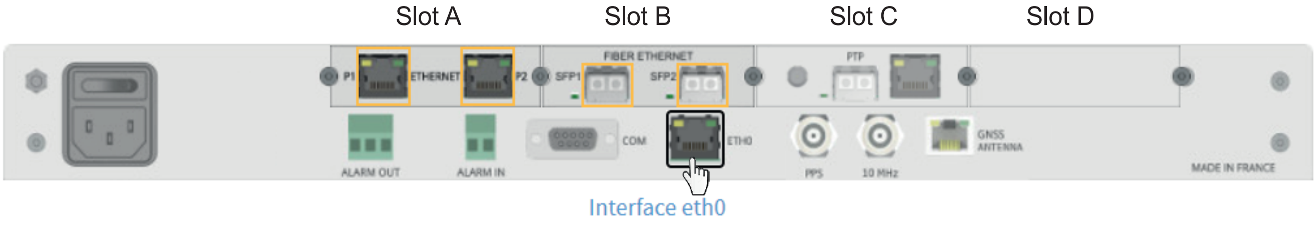
2 Enter the offset value (available in manual mode only).

When passing a manually programmed Leap Second, the TAI/UTC manual offset will change accordingly (+/-1).

4.4 Configuring the computer network

1) Click on the NETWORK to configure the network interfaces.

As for network interface configuration, navigation is interactive: move the mouse over the connector of the interface to be configured, then click on it:

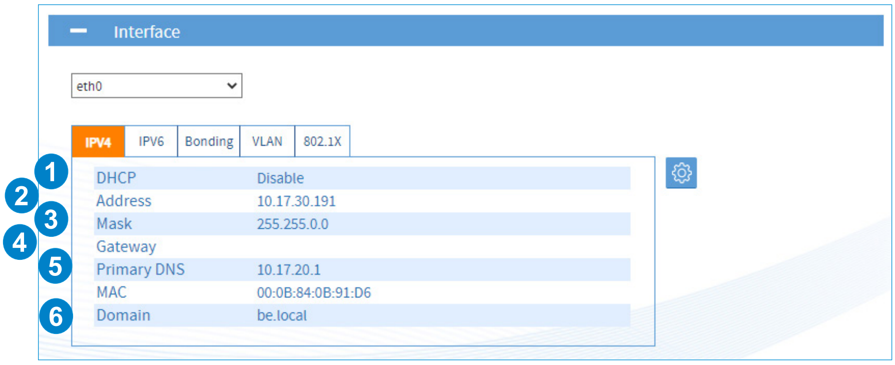


4.4.1. *Network interface configuration*

To configure a network interface, follow these steps:

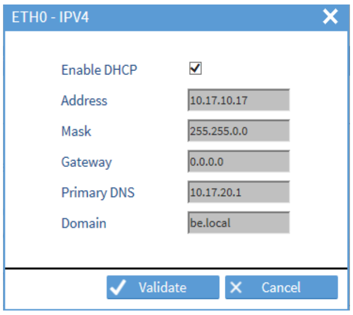
1) NETWORK menu > Interfaces > ETHx interface:

IPv4 settings:



DHCP	Disable
Address	10.17.30.191
Mask	255.255.0.0
Gateway	
Primary DNS	10.17.20.1
MAC	00:0B:84:0B:91:D6
Domain	be.local

2) Click on ⚙, and the following window will appear:

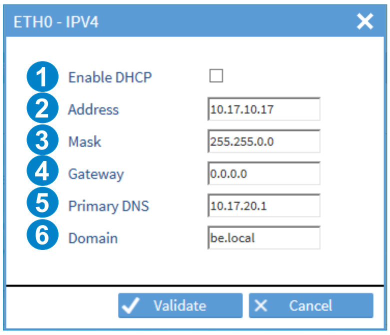


Enable DHCP	☑
Address	10.17.10.17
Mask	255.255.0.0
Gateway	0.0.0.0
Primary DNS	10.17.20.1
Domain	be.local

3) Configure the various parameters:

1 With a DHCP server: check the box. The IP address and network settings will be assigned automatically.

2 Without a DHCP server: manually enter the fixed IP address for this network port.



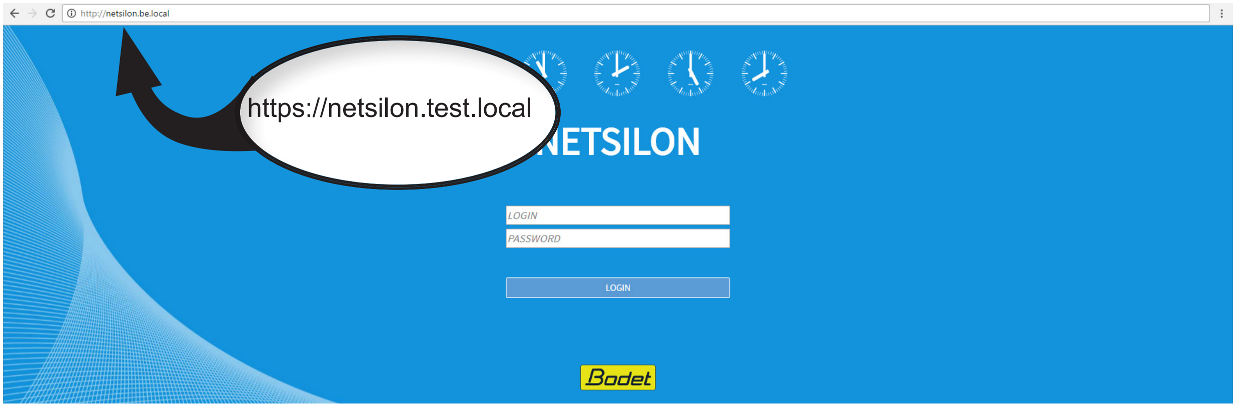
Enable DHCP	☐
Address	10.17.10.17
Mask	255.255.0.0
Gateway	0.0.0.0
Primary DNS	10.17.20.1
Domain	be.local

3 Enter the subnet mask in order to define the IP addresses of products which will be able to communicate with Netsilon.

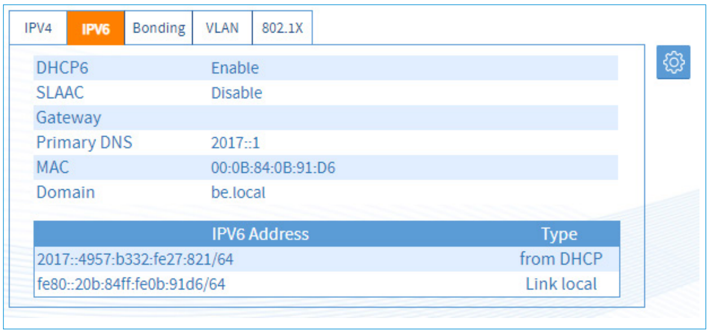
4 Enter the gateway if a product is outside the local network (LAN).

5 Enter the address of the primary DNS in order to assign a domain name.

6 Enter the domain name extension in order to access the product's web server from the DNS.
e.g: if the name of the product is "Netsilon" (see chapter **4.1 Start-up**)
Example of access to the web server using the domain name:



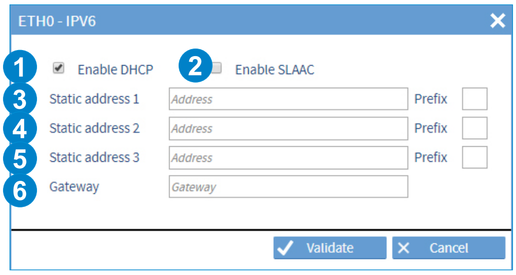
IPv6 settings:



DHCP6	Enable
SLAAC	Disable
Gateway	
Primary DNS	2017::1
MAC	00:0B:84:0B:91:D6
Domain	be.local

IPV6 Address	Type
2017::4957:b332:fe27:821/64	from DHCP
fe80::20b:84ff:fe0b:91d6/64	Link local

1) Click on ⚙, and the following window will appear:



☑ Enable DHCP   □ Enable SLAAC

Static address 1	Address	Prefix	
Static address 2	Address	Prefix	
Static address 3	Address	Prefix	
Gateway	Gateway		

1 Enable DHCP (statefull) to assign the IP address and network settings automatically.

2 Enable SLAAC (stateless with DHCP) to assign automatically an IP address to Netsilon. It also allows to retrieve the gateway.

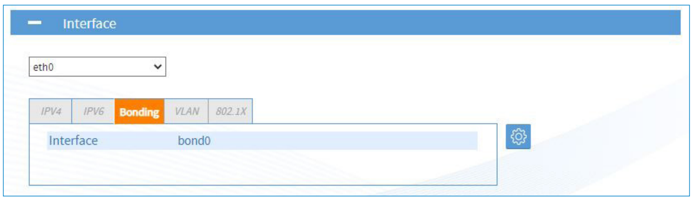
The activation of the DHCP (in addition to the SLAAC) allows to obtain DHCP options (e.g: DNS, Domine) in addition to the IP address set by the SLAAC process (no IP assignment by DHCP in this mode). The DHCP is activated by default. It is possible to combine "static"/"DHCP"/"SLAAC" modes.

3 4 5 Fixed IP addresses. Enter the prefix defined by the network administrator.

6 Network gateway defined by the network administrator. (Caution: at least one static address is required for the gateway to be taken into account).

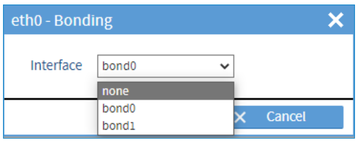
Bonding (Ethernet redundancy):
The bounding allows to link several network interfaces (at least one Network option card must be available in Netsilon) to a group called "bond". This port redundancy provides security in the event of a network interface failure, as the time server remains accessible and available via one or several other interfaces from the group (bond). Two operating modes are available for each bond.
To assign an interface to a bond, then choose its operation mode:

1) Select an interface and click on the "Bonding" tab,



Interface bond0

2) Click on ⚙, the following window opens:



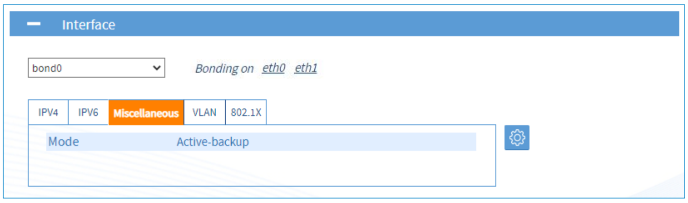
Interface bond0

3) Select the assignment of the interface to the desired group (bond) using the drop-down list.

When an interface is assigned to a bond, its configuration will be that of the bond to which it belongs. The configuration of a bond is similar to that of an Ethernet port.
When an interface is attached to a bond, the 802.1x settings of the interface that is becoming a bond are reset. When the bond is removed (no interface attached to the bond), the 802.1x settings of the bond are reset.

4) Repeat these steps for all interfaces to be assigned to a bond,

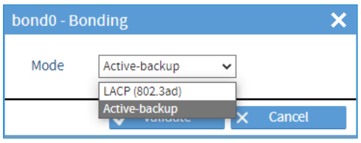
5) Configure the operating mode of the bond by selecting it and clicking on the"Miscellaneous" tab:



Bonding on eth0 eth1

Mode Active-backup

6) Click on ⚙, the following window opens:



Mode Active-backup

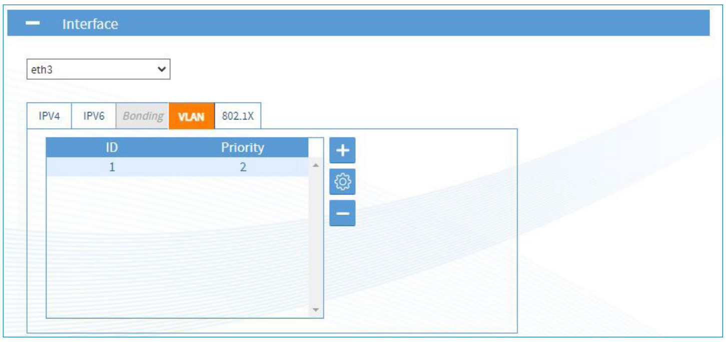
7) Choose the operating mode of this bond using the drop-down list:
Active-backup: one physical interface from the group carries all network traffic of the group. The other physical interfaces are then passive. If the active interface loses the connection, one of the passive interfaces of the group takes it over.
LACP: all interfaces of the group are aggregated together and work dynamically, which increases the level of security in the event of a failure. This operating mode implies that the other network equipment support LACP.

On an Ethernet bond, the limiting element being the CPU, doubling the bond will not increase the bandwidth. A maximum of 2 bonds is possible in total.

VLAN (virtual local area network):
VLANs reinforce computer security of networks by providing logical segmentation inside an extensive physical network. Each VLAN has its own broadcast domain.
Netsilon uses “VLAN tagged” with an assignment to the virtual local networks via the use of a tag in the message packet frame. The tag contains the ID of the virtual local network (VID) and allows the switch to determine in which VLAN the communication is taking place. The properties of the tag allow 4094 different VLANs to be supported.
In Netsilon, VLAN support allows a network port (or bond) to be attached through which data will flow to one or several designated VLANs (VLAN ID).

In order to link a network port (or a bond) to one or several VLANs:

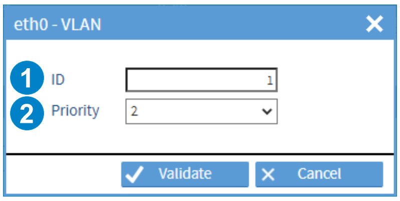
1) Select the parent Ethernet port (or bond), then click on the"VLAN" tab:



eth3

ID	Priority
1	2

2) Click on + or ⚙ to add or configure a VLAN interface, the following window opens:



ID: 1
Priority: 2

1 Enter the VLAN ID (from 1 to 4094).

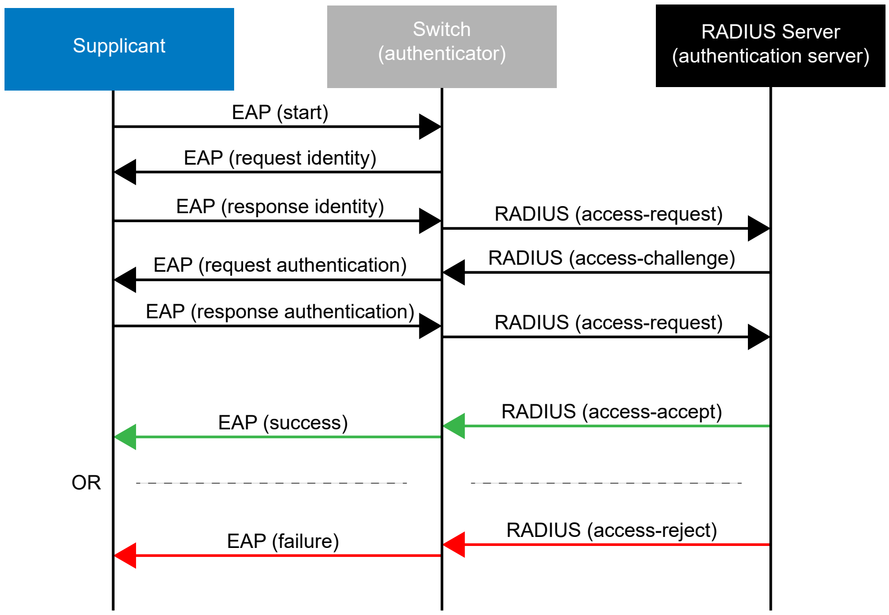
2 Select a priority index (from 0 to 7) to optimise message traffic (quality of service).

It is possible to make up to 20 assignments distributed over the different interfaces without limitation.
This will be shown as: [eth/bond].[VLAN ID] in the interface list.
It is possible to configure the VLAN interfaces (IPV4/IPV6).

802.1x authentication protocol:
The 802.1x protocol allows controlling device access to network infrastructures through an authentication process for devices that want to connect to the network.

The authentication process occurs in the following way:
1. The device (called supplicant) that seeks to join the network connects to its entry point through a switch (called authenticator).
2. The switch activates a port which only carries 802.1x frames and asks the device to identify itself.
3. In response, the device sends its ID to the switch which forwards this information to a RADIUS-type authentication server (called authentication server).
4. The RADIUS server receives the device’s ID and asks it to prove its identity by providing a password or a certificate.
5. The device provides the requested authentication data to the RADIUS server which controls the validity of the transmitted information.
6. If the information provided by the device is valid, the RADIUS server instructs the switch to allow network access to the device. Otherwise, access is denied and the device remains on a quarantine network.

The following diagram summarises the frames exchanged during the authentication process:



The Extensible Authentication Protocol (EAP) manages the transport of identification information according to the client/server mode. It manages the transport of authentication protocols so as to secure all communications.

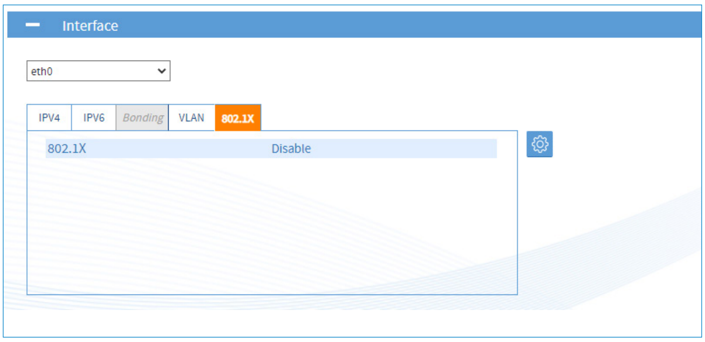
Netsilon supports the following authentication protocols:

Authentication protocols	Associated internal authentication
EAP-PWD	
EAP-MD5	
EAP-TLS	
EAP-TTLS	PAP MSCHAP MSCHAPv2 MSCHAPv2 no EAP CHAP MD5 GTC
EAP-PEAP	MSCHAPv2 MD5 GTC
EAP-FAST	MASCHAPv2

In order to configure the 802.1x protocol on Ethernet interfaces or bonds:

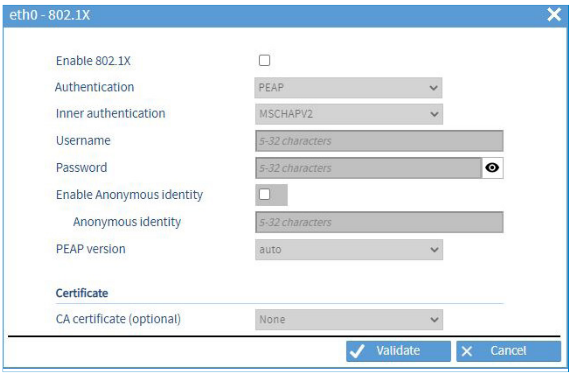
VLAN inherits the configuration of the Ethernet interface or the associated bond.

1) Select an Ethernet interface or a bond, and click on the"802.1x" tab:



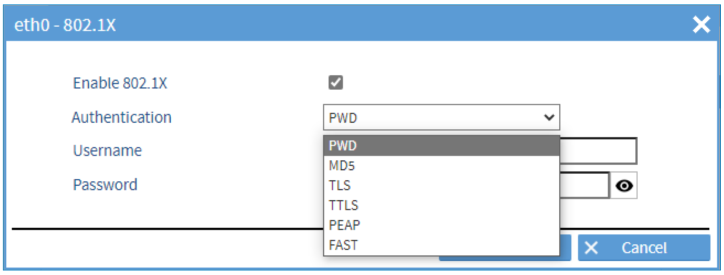
802.1X Disable

2) Click on ⚙, the following window opens:



Enable 802.1X	☐
Authentication	PEAP
Inner authentication	MSCHAPV2
Username	5-32 characters
Password	5-32 characters
Enable Anonymous identity	☐
Anonymous identity	5-32 characters
PEAP version	auto
Certificate	
CA certificate (optional)	None

3) Activate the 802.1x protocol by checking the activation box, then choose the authentication protocol type:

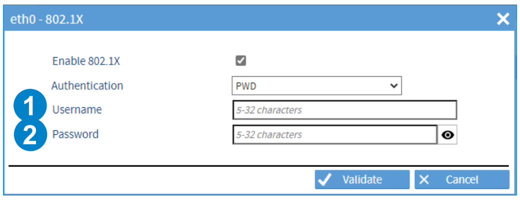


Enable 802.1X	☑
Authentication	PWD
Username	
Password	

The "Authentication" field refers to the protocol used to secure the 802.1x connection between the supplicant and the authenticator and identify the supplicant using its identity or user name.

4) Set the parameters according to the chosen authentication protocol:

- PWD: authentication by password.

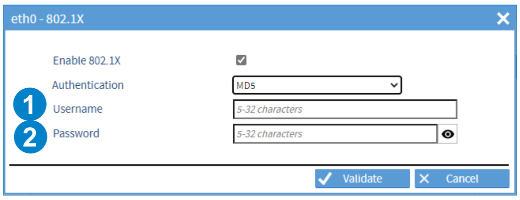


Enable 802.1X	☑
Authentication	PWD
Username	5-32 characters
Password	5-32 characters

1 Enter the user name of the supplicant (Netsilon).

2 Enter the password.
This will be verified by the authentication server.

- MD5: authentication of the device (supplicant) through a challenge-response protocol (with the authentication server) with the MD5 hash function.

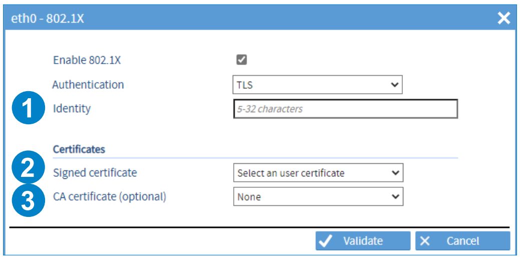


Enable 802.1X	☑
Authentication	MD5
Username	5-32 characters
Password	5-32 characters

1 Enter the user name of the supplicant (Netsilon).

2 Enter the password. This will be hash-protected and verified by the authentication server.

- TLS: mutual authentication of the device (supplicant) and the server through the use of certificates.



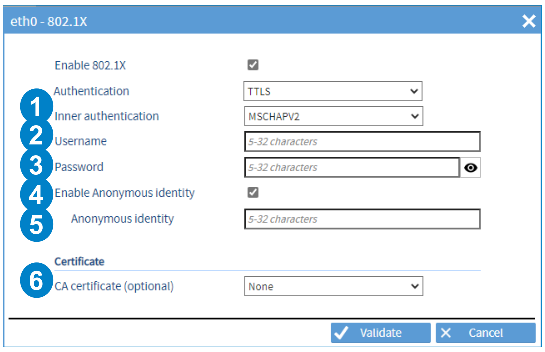
Enable 802.1X	☑
Authentication	TLS
Identity	5-32 characters
Certificates	
Signed certificate	Select an user certificate
CA certificate (optional)	None

1 Enter the supplicant ID (Netsilon).

2 Select a signed certificate (mandatory).
This certificate must be previously added in the certificates and keys section in the "Signed certificates" tab,
See chapter **4.10 Certificate and key management.**

3 Select a CA certificate (optional).
This certificate must be previously added in the certificates and keys section in the "CA certificates" tab,
See chapter **4.10 Certificate and key management.**

- TTLS: authentication by encapsulating a TLS session in 2 phases: authentication of the server to the device (supplicant) through the use of a certificate to create a secure TLS tunnel for data exchange between the 2 parties during the second phase. During the second phase, the client is authenticated to the server using an internal authentication mechanism (PAP, MSCHAPv2...), through the secure tunnel. By doing so, the identity of the supplicant is protected during the authentication phase.



eth0 - 802.1X

Enable 802.1X	☑
1 Authentication	TTLS
Inner authentication	MSCHAPV2
2 Username	5-32 characters
3 Password	5-32 characters
4 Enable Anonymous identity	☑
5 Anonymous identity	5-32 characters
Certificate	
6 CA certificate (optional)	None

Note: 5
If the "@" character is used, then the Anonymous identity must be in the form of a domain name containing a dot
(for example: @example.com).

1 Choose the internal authentication mechanism.
This mechanism allows Netsilon authentication using its password. The password will be transmitted according to the form of the selected encryption mechanism (MD5, MSCHAP...).

2 Enter the user name of the supplicant (Netsilon).

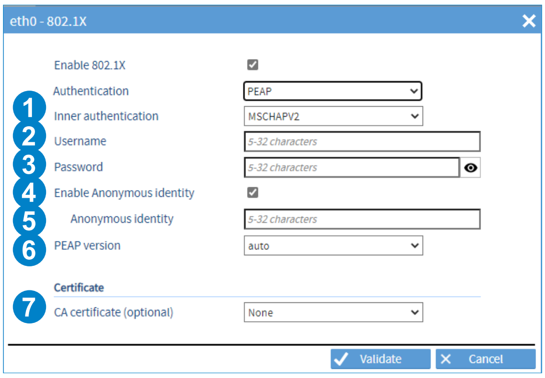
3 Enter the password.
This will be verified by the authentication server.

4 To protect the user name of the supplicant (Netsilon) during the first identification phase, when the connection between Netsilon and the switch (authenticator) is not yet secured by the TLS tunnel, an "Anonymous identity" can be used instead.
If the "Anonymous identity" parameter is not selected, the user name is used during the first phase.

5 Enter the "Anonymous identity" (not related to the user name and the password for authentication).

6 Select a CA certificate (optional).
This certificate must be previously added in the certificates and keys section in the "CA certificates" tab,
See chapter **4.10 Certificate and key management.**

- PEAP: two-phase operation, similar to TTLS. The server first authenticates to the device (supplicant) using a certificate to create a secure TLS tunnel between the two parties. Then, the server authenticates the device within the secure tunnel using an internal authentication method (MSCHAPv2, MD5...).



eth0 - 802.1X

Enable 802.1X	☑
Authentication	PEAP
1 Inner authentication	MSCHAPV2
2 Username	5-32 characters
3 Password	5-32 characters
4 Enable Anonymous identity	☑
5 Anonymous identity	5-32 characters
6 PEAP version	auto
Certificate	
7 CA certificate (optional)	None

Note: 5
If the "@" character is used, then the Anonymous identity must be in the form of a domain name containing a dot
(for example: @example.com).

1 Choose the internal authentication mechanism.
This mechanism allows Netsilon authentication using its password. The password will be transmitted according to the form of the selected encryption mechanism (MSCHAPv2, MD5,...).

2 Enter the user name of the supplicant (Netsilon).

3 Enter the password.
This will be verified by the authentication server.

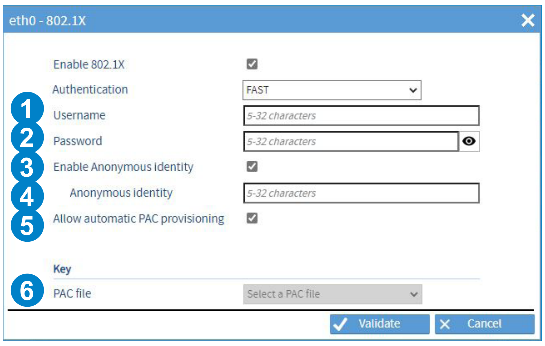
4 To protect the user name of the supplicant (Netsilon) during the first identification phase, when the connection between Netsilon and the switch (authenticator) is not yet secured by the TLS tunnel, an "Anonymous identity" is used instead.
If the "Anonymous identity" parameter is not selected, the user name is used during the first phase.

5 Enter the "Anonymous identity" (not related to the user name and the password for authentication).

6 Choose the PEAP version according to the compatibility.
Possibility to set the parameter to automatic.

7 Select a CA certificate (optional).
This certificate must be previously added in the certificates and keys section in the "CA certificates" tab,
See chapter **4.10 Certificate and key management.**

- FAST: authentication via a secure TLS tunnel using a Protected Access Credential (PAC) dynamically generated by the authentication server.



eth0 - 802.1X

Enable 802.1X	☑
Authentication	FAST
Username	5-32 characters
Password	5-32 characters
Enable Anonymous identity	☑
Anonymous identity	5-32 characters
Allow automatic PAC provisioning	☑

Key

PAC file	Select a PAC file

Note: 4

If the “@” character is used, then the Anonymous identity must be in the form of a domain name containing a dot
(for example: @example.com).

1 Enter the user name of the supplicant (Netsilon).

2 Enter the password.
This will be verified by the authentication server.

3 To protect the user name of the supplicant (Netsilon) during the first identification phase, when the connection between Netsilon and the switch (authenticator) is not yet secured by the TLS tunnel, an “Anonymous identity” is used instead.
If the “Anonymous identity” parameter is not selected, the user name is used during the first phase.

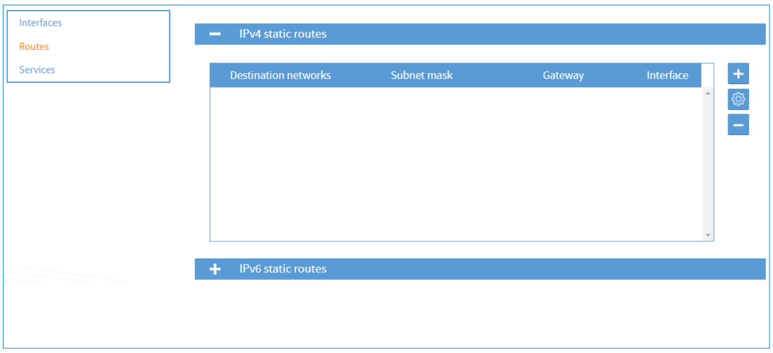
4 Enter the “Anonymous identity” (not related to the user name and the password for authentication).

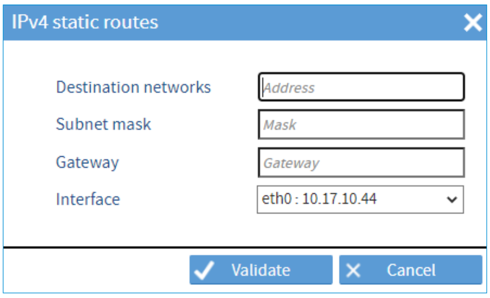
5 Allow automatic PAC provisioning during exchanges.
The user does not need to provide one.

6 Select a PAC file if the “Allow automatic PAC provisioning” option is not activated.
This PAC file must be previously added in the certificates and keys section in the “public keys” tab,
See chapter **4.10 Certificate and key management.**

4.4.2. *Configuration of IPv4/IPv6 static routes*

To configure static routes:
1) NETWORK menu > Routes





IPv4 static routes

Destination networks	Address
Subnet mask	Mask
Gateway	Gateway
Interface	eth0 : 10.17.10.44

2) Click on + and a window will appear, then fill in the various parameters required to configure the routing:
- Destination networks,
- Subnet mask (or prefix for IPv6),
- Gateway.

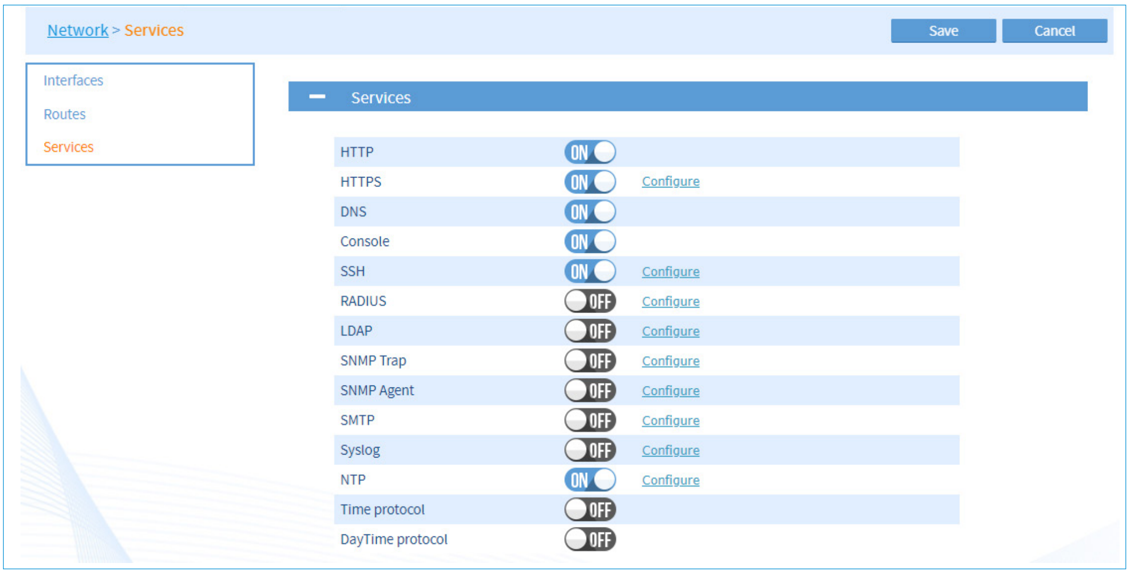
3) Choose the Ethernet interface, the bond or the VLAN.

It is possible to add up to 50 routes in IPv4 and 50 routes in IPv6.
The gateways (default routes) must be declared in the interfaces.
In the case of completely isolated networks, it is required to declare a single default route in an interface and declare the other remote networks as static routes.

4.4.3. *Managing network services*

To manage network services, follow these steps:

1) NETWORK menu > Services



Services

HTTP	ON	
HTTPS	ON	Configure
DNS	ON	
Console	ON	
SSH	ON	Configure
RADIUS	OFF	Configure
LDAP	OFF	Configure
SNMP Trap	OFF	Configure
SNMP Agent	OFF	Configure
SMTP	OFF	Configure
Syslog	OFF	Configure
NTP	ON	Configure
Time protocol	OFF	
DayTime protocol	OFF	

It is possible to enable or disable network services individually.

For some services, previous configuration is necessary. Hyperlinks (Configure) can be used to access the configuration pages for services requiring configuration.

General information on network services is introduced later in this chapter. To obtain further information on the configuration of each network service, see the detailed chapter.

› HTTP - HTTPS

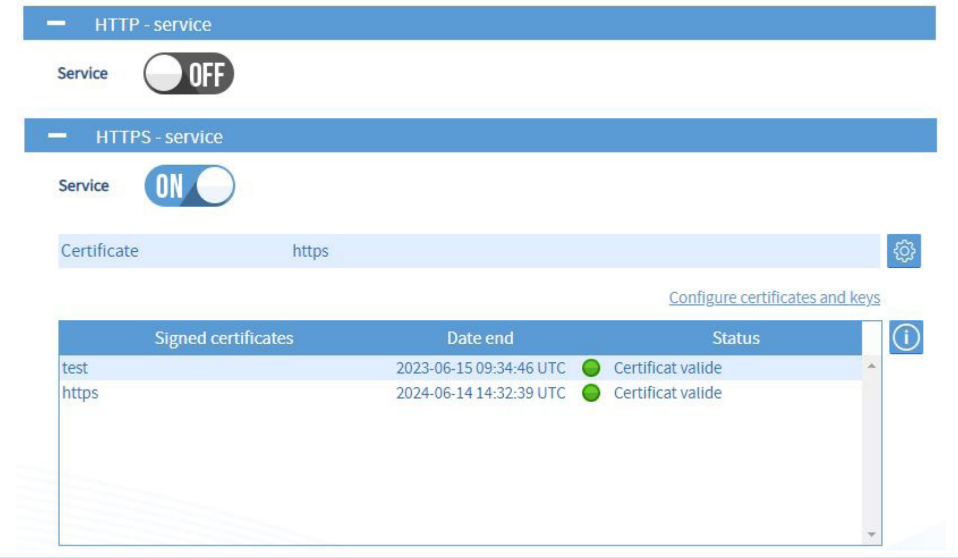
HTTPS (Hypertext Transfer Protocol Secure) is a communication protocol used to access a secure web server. If HTTPS is included in the URL instead of the usual HTTP, the message will be sent to a secure entry port on the server.

The HTTPS protocol enables secure management of access to the web server for Netsilon configuration.

The SSL certificate is required in order for the connection to be secure with Netsilon (HTTPS).

It is possible to choose between a certificate signed by an external Certification Authority (CA) and a self-signed certificate.
Each Netsilon generates an auto-certified SSL certificate. The certificate is automatically renewed after 10 years. The certificate is renewed four days before it expires.

To configure this setting, click on Configure:



HTTP - service

Service: OFF

HTTPS - service

Service: ON

Certificate: https

Signed certificates	Date end	Status
test	2023-06-15 09:34:46 UTC	● Certificat valide
https	2024-06-14 14:32:39 UTC	● Certificat valide

This menu allows you to choose the certificate to be used (self-signed or signed by an external Certification Authority) and to consult the information of external certificates.

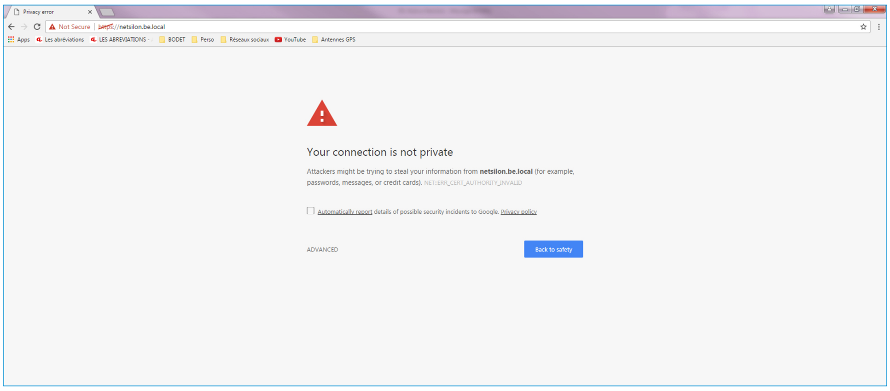
Certificates are added from the Certificates and keys menu.
See chapter 4.10 Certificate and key management.

⚠ **When a service is modified (HTTP or HTTPS) or when the certificate is modified, the product returns to the web server access page.**

To use the secure connection, HTTP to HTTPS redirection is performed automatically:

1) In the browser's address bar, enter: https://NameOfProduct.Domain.

2) Example : https://netsilon.be.local :

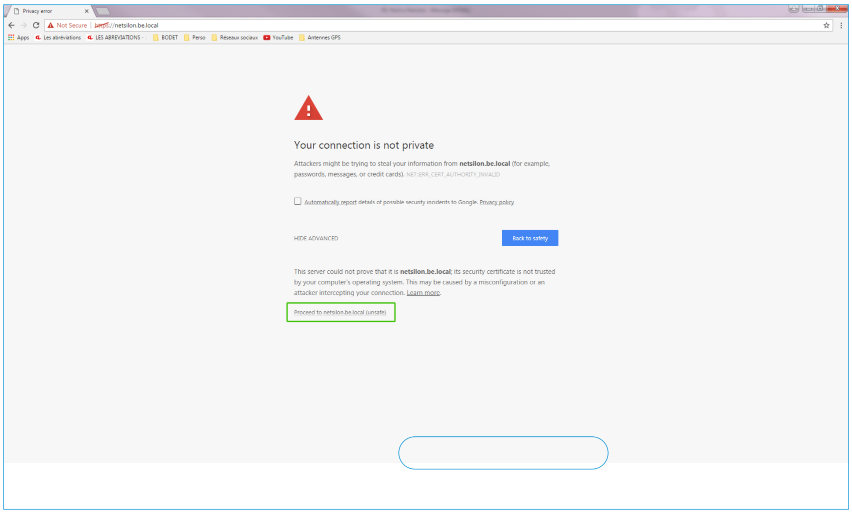


Your connection is not private

Attackers might be trying to steal your information from **netsilon.be.local** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

3) Go to the browser's advanced settings, then click on "proceed to netsilon.be.local":



Your connection is not private

Attackers might be trying to steal your information from **netsilon.be.local** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

This server could not prove that it is **netsilon.be.local**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

Proceed to netsilon.be.local (unsafe)

The connection is secure, even if "https" is crossed and in red. This warning only indicates that the certificate has not been authenticated by a certified organisation.

Bodet recommends the use of the "https" mode to optimise security when accessing the Netsilon web server.

› DNS

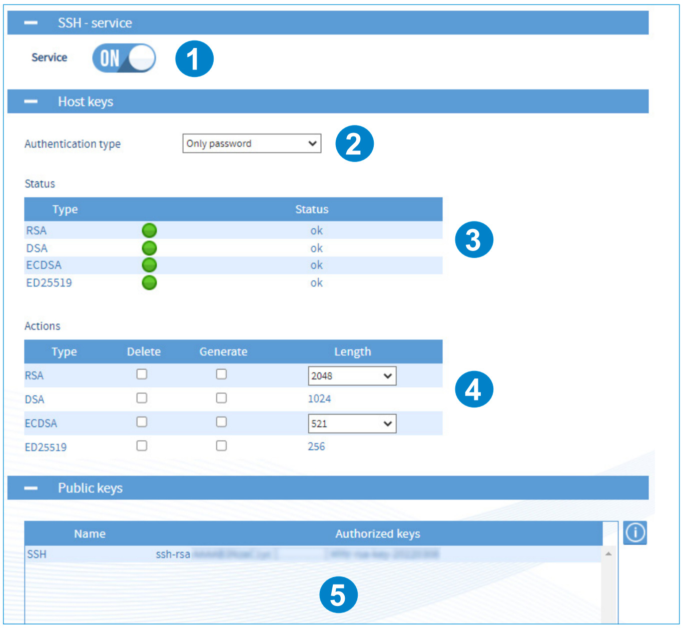
The DNS (Domain Name System) is a protocol which can be used to associate a domain name, known as Hostname (e.g. www.netsilon.com) with an IP address. However, if queried by a host on the destination server, only its IP address will be sent in order to determine precisely the identity of the synchronisation server.
The Hostname is defined in SYSTEM > General > Settings.

› CONSOLE

On the serial port, the configuration of Netsilon (basic settings) can be modified using command sets.
To configure the serial port, **see chapter 6. Configuration by console** - basic configuration.

› SSH

On the Ethernet port, the configuration of Netsilon can be modified using command sets.
To configure this setting, click on Configure:



Authentication type: Only password

Status

Type		Status
RSA	🟢	ok
DSA	🟢	ok
ECDSA	🟢	ok
ED25519	🟢	ok

Actions

Type	Delete	Generate	Length
RSA	□	□	2048
DSA	□	□	1024
ECDSA	□	□	521
ED25519	□	□	256

Name	Authorized keys
SSH	ssh-rsa [redacted]

1 Activation of the SSH service

2 Authentication by:
- Only password: authentication by password only
- Only public key: authentication by public key only.
- Public key or password: authentication by password or public key.

3 Types of keys supported:
- RSA: 1024/ 2048/4096 bits
- DSA: 1024 bits (fixed)
- ECDSA: 256/384/521 bits
- ED25519: 256 bits (fixed)

4 Allows to generate or delete the certificates of each type of key. To generate a new certificate, the old one must be deleted. **If the user deletes the RSA and DSA certificates without generating new ones, the SSH function will not work.**

5 View a public key. To add a key, you must save in a file the public key generated by the utility program (e.g.: PuTTY key generator) then import it in Netsilon. See chapter 5.2 **Authentication by public key**

› RADIUS

The RADIUS (Remote Authentication Dial-In User Service) protocol is a standard authentication protocol based on a client/server system defining access for remote users to a network.

Click on Configure then refer to chapter **4.2.2.1 RADIUS service**

› LDAP

The LDAP (Lightweight Directory Access Protocol) protocol is used to access information about users on a network by querying directory services.

Click on Configure then refer to chapter **4.2.2.2 LDAP service**

› SNMP

SNMP (Simple Network Management Protocol) is a protocol for supervision of network devices. There are two entities: an SNMP manager and agents (e.g. Netsilon).

Traps

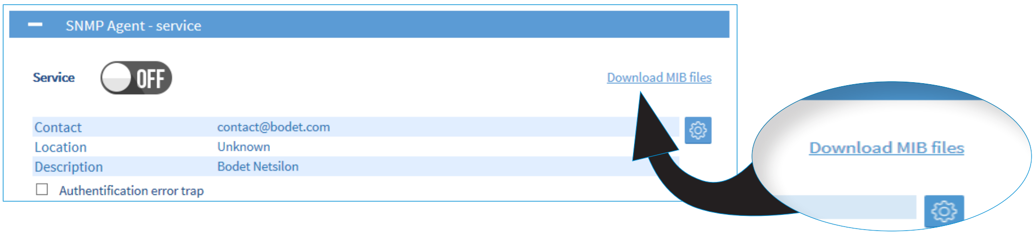
SNMP traps are messages sent using the SNMP protocol from a monitored device to a monitoring server.

The monitoring server must have the necessary features in its configuration in order to understand the received event. For this purpose, it must have a database containing the MIB files.

Click on Configure then refer to chapter **4.9.2 SNMP trap configuration.**

Downloading the MIB file

The MIB file can be obtained in SECURITY > SNMP Agent > SNMP Agent - Service:



Contact	contact@bodet.com
Location	Unknown
Description	Bodet Netsilon

□ Authentification error trap

The downloaded file is in ZIP format.

Agents

The agents are responsible for transmitting messages related to the management of the equipment in SNMP format.

Click on Configure then refer to chapter **4.11 System supervision.**

› SMTP

SMTP (Simple Mail Transfer Protocol) is used to transfer electronic messages (alarms) in a computer network.
An SMTP server is a service which listens on port 25. Its primary purpose is to route emails to a recipient.
Click on Configure then refer to chapter **4.9.1 SMTP configuration.**

› SYSLOG

Syslog is a standard protocol for sending system log events from devices on a network to a dedicated server that will centralise this information for future analysis.
It is also possible to use this service to archive events locally.

Click on Configure then refer to chapter **4.9.4 Syslog configuration**

› NTP

Network Time Protocol (NTP) is a client/server protocol for time synchronisation on IP networks.
The NTP service can be enabled or disabled. When NTP is disabled, no NTP data will be sent to the network. When enabled, the NTP service operates in Unicast mode by default.
All parameters can be changed to configure specific NTP applications: NTP client, NTP servers, NTP peers, NTP key and NTP autokey.

Click on Configure then refer to chapter **4.6 NTP synchronisation.**

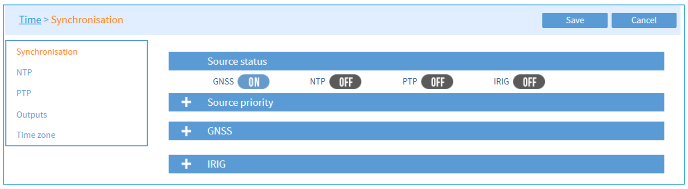
› TIME PROTOCOL and DAYTIME PROTOCOL

Activating these parameters allows Netsilon to send the UTC time and date (not configurable) to multiple devices on the computer network.

4.5 Choosing synchronisation sources

To choose the synchronisation source(s), follow these steps:

1) TIME menu > Synchronisation



GNSS ON NTP OFF PTP OFF IRIG OFF

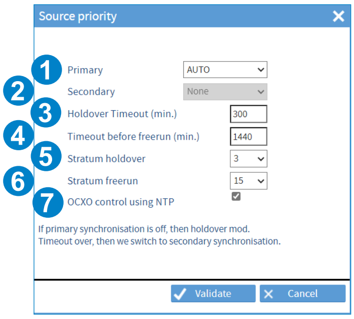
4.5.1. *Status of sources*

An overview is provided. This area shows if the available synchronisation sources have been activated.

4.5.2. *Priority of sources*

The priority of synchronisation sources can be used to define the priorities between each available source, in order to enable Netsilon to transmit a continuous, accurate time signal.

In order to establish a priority among the synchronisation sources and to configure settings: click on ⚙, and the following window will appear:



Primary: AUTO
Secondary: None
Holdover Timeout (min.): 300
Timeout before freerun (min.): 1440
Stratum holdover: 3
Stratum freerun: 15
OCXO control using NTP: ☑

If primary synchronisation is off, then holdover mod.
Timeout over, then we switch to secondary synchronisation.

1 5 possible choices: AUTO - GNSS - NTP - PTP- IRIG (PTP and IRIG: only if the corresponding card is installed).
In Auto mode, Netsilon automatically chooses the most reliable (best quality) source and switches automatically between sources (if a source is lost).
In Primary/Secondary mode, it attempts synchronisation with the primary source. If there is no synchronisation after several minutes (timeout depending on the source - GNSS: 5 minutes, PTP: 10 minutes, NTP: 15 minutes, IRIG: 10 minutes), there is a switch to the secondary source. If the primary synchronisation is restored, it automatically switches back to the primary source. If loss of synchronisation with the primary source occurs, it switches to the secondary source after the holdover timeout.

2 5 possible choices: None - GNSS - NTP - PTP- IRIG.

3 Holdover is a status in which the timer server continues to transmit a time signal without the presence of a synchronisation source. By default, the holdover value is set to 300 minutes (5 hours). This depends on the environment in which Netsilon is used and on user requirements in terms of time signal precision. This value is sufficiently large to mask any mini-outages of the synchronisation source, but sufficiently low to ensure a high-quality time signal. The value of the “Holdover timeout” can be set from 1 to 14400 minutes (10 days).

4 Once the Holdover timeout has expired, and without a return of the primary synchronisation source or a secondary source to take over, a new period is activated before reaching the “freerun” state, where the accuracy of the time zone is no longer guaranteed. This is the “Timeout before freerun”. This value can be set up to 43200 minutes (30 days).

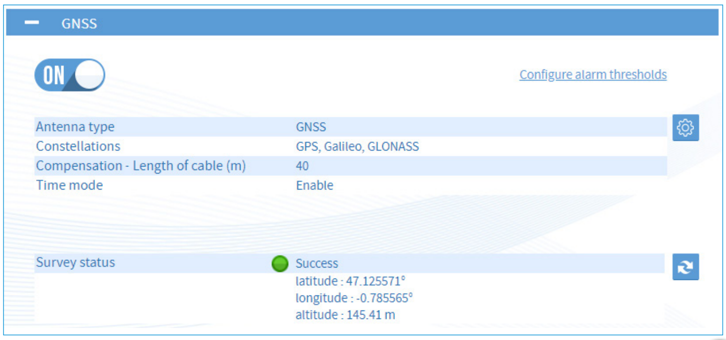
5 6 The “Stratum holdover” and “Stratum freerun” fields set the stratum of the Netsilon NTP server, not the local source. The server stratum when unsynchronised (following the “holdover” or “freerun” status) can be set between 1 and 15. By default: Stratum holdover = 3 / Stratum freerun = 15.
The stratum of the local source is therefore one level lower.
Example:
Stratum holdover = 3
Local source = 2
Netsilon NTP server (for client synchronisation) = 3

7 Control of the OCXO oscillator from an NTP source. If the primary synchronisation is GNSS and the secondary source NTP, the oscillator is slaved to the GNSS source first (better accuracy).

See chapter **9 Annex 1: Synchronisation** for an overview of the different synchronisation scenarios.

4.5.3. Satellite receivers

Enable GNSS synchronisation using the ON button.



GNSS

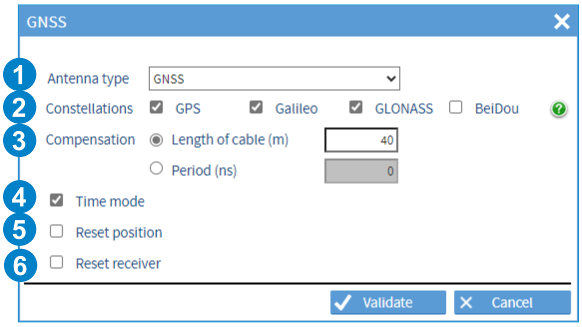
ON

Configure alarm thresholds

Antenna type	GNSS
Constellations	GPS, Galileo, GLONASS
Compensation - Length of cable (m)	40
Time mode	Enable

Survey status ● Success
latitude : 47.125571°
longitude : -0.785565°
altitude : 145.41 m

1) Click on ⚙ to select the type of antenna and the constellation(s). The button ? lists the authorised GNSS combinations.



GNSS

1 Antenna type: GNSS

2 Constellations ☑ GPS ☑ Galileo ☑ GLONASS ☐ BeiDou ?

3 Compensation ● Length of cable (m) 40

○ Period (ns) 0

4 ☑ Time mode

5 ☐ Reset position

6 ☐ Reset receiver

1 Choice of the type of antenna: GNSS or Secure GNSS (anti-jamming and anti-spoofing);
If the GNSS secure antenna is chosen, an option is provided to exclude GNSS synchronisation in the event of spoofing detection. In that case, the server will automatically use another synchronisation source.
Any change of antenna (example: replacement a GNSS antenna by a Secure GNSS) must be carried out cold and requires the device to be restarted.

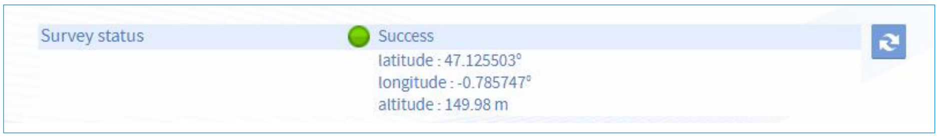
2 Choice of constellations depending on possible combinations.
As for the Secure GNSS antenna, it is possible to select all the constellations simultaneously.
It is necessary to select at least 2 constellations in order to detect a spoofing attack.

3 There are two options for compensation:

- Select the GNSS antenna cable length,
- Indicate the compensation value directly (useful when using the standard RF GNSS antenna interface).

Below is the period calculation for the standard RF GNSS interface:
D: total period in ns
L1: Ethernet cable length (time server / antenna interface control box)
L2: coaxial cable length (antenna interface control box / RF antenna)
D = L1. C1+ L2. C2
C1 = 5.8 ns/m
C2 depends on the coaxial cable. For an LMR-400 type cable, C2 = 4 ns/m
C2 can also be calculated using the cable manufacturer’s data with the formula below:
C2 = 1/ (0.3 . v) where v is the cable velocity (e.g. 0.66 for 66%)

4 “Time mode” is selected by default. This will improve PPS precision by working in fixed position. This mode is only advisable when using PPS generated by the time server.
The position of the antenna is determined automatically using the “survey” procedure.
The “survey” status will show one of the following values:
- Unknown / In progress (with time elapsed since starting) / Success / Aborted
If the survey status is "Success", the position of the antenna is given. (MSL altitude = Mean Sea Level)



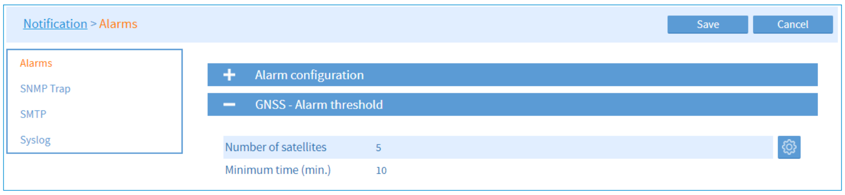
Survey status ● Success
latitude : 47.125503°
longitude : -0.785747°
altitude : 149.98 m

If “time mode” is not selected: time and position.

5 “Reset position” is only accessible in “time mode” and is used to restart the “survey” procedure to automatically determine the position of the antenna (e.g. if the position of the antenna has been altered).

6 "Reset receiver” is used to restart the GNSS receiver if required.

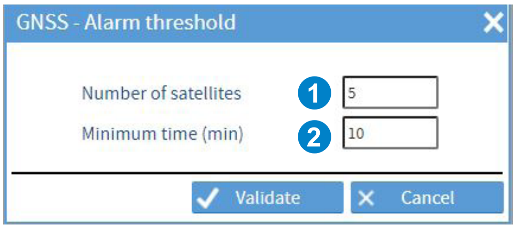
1) To set the alarm threshold, click on the link Configure alarm thresholds, and the following window will appear:



Notification > Alarms

Number of satellites 5
Minimum time (min.) 10

2) Click on ⚙, and the following window will appear:



GNSS - Alarm threshold

Number of satellites 1 5
Minimum time (min) 2 10

1 Set the number of satellites to define the alarm threshold (between 3 and 8).

2 Set the duration after which the alarm is notified.

For example:
- GPS constellation
- Duration set to 10 minutes
If less than 5 satellites are counted over a 10-minute period, an alarm will be notified.

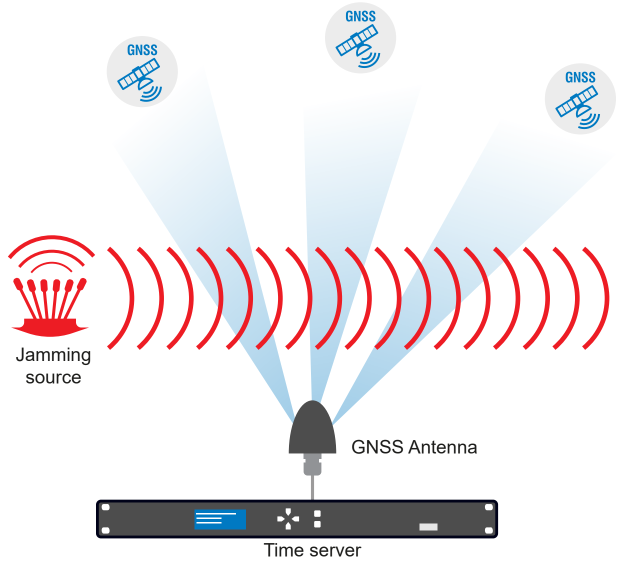
By default, the alarm threshold is activated for five satellites and a duration of 10 minutes.

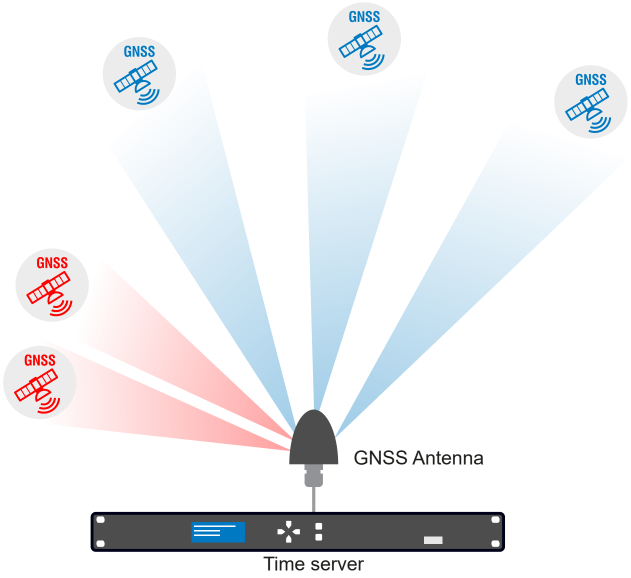
4.5.4. *Jamming and spoofing of GNSS signals*

GNSS satellites operate from the Earth's orbit. The transmitted signal is extremely weak when it reaches the earth's surface. This low signal strength near the receivers makes the use of GNSS signals sensitive to intentional (malicious) or unintentional interference.
There are mainly 2 types of interference: spoofing and jamming.

Jamming is the presence of a spurious signal that prevents the GNSS receiver from decoding the true satellite signal.

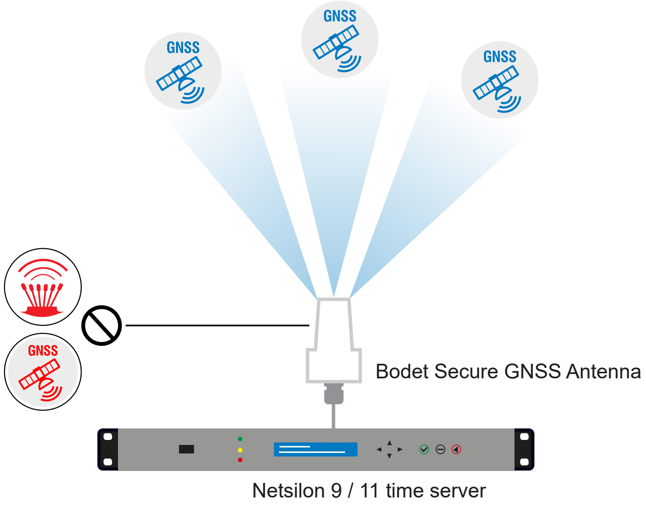
Spoofing is the intentional transmission of fake GNSS signals to divert users from their real position. Spoofing requires sophisticated equipment to recreate satellite signals.
Spoofing is more difficult to detect than jamming.



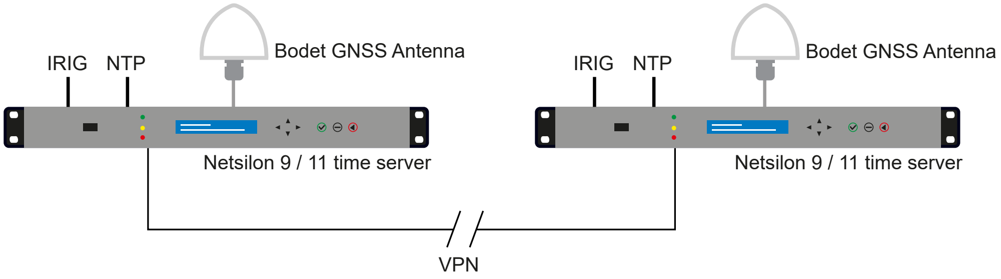


In order to prevent these risks, several options are available:

Option 1: Secure GNSS antenna (Secure GNSS)
This BODET antenna offers an additional layer of security against jamming and spoofing attempts, due to its design and the use of advanced detection algorithms.

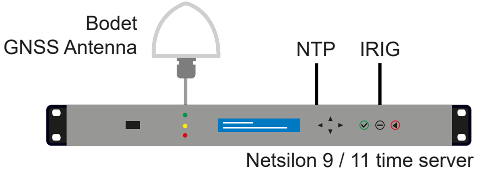


Option 2: remote installation
Jamming and spoofing attempts are made more complex with 2 geographically distant sites to attack.



2 time servers installed on 2 different sites synchronise together (via NTP, PTP or IRIG) over a private network (VPN) This option assumes that the 2 Bodet time servers are in automatic mode (choice of the source) and have 3 independent synchronisation sources each.

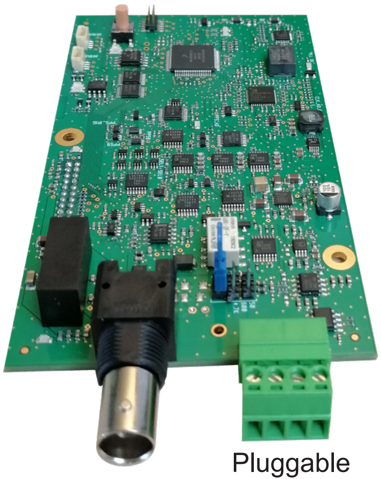
Option 3: a multi-source installation
The time server uses several synchronisation sources and makes comparisons to choose the most reliable one. In the event of jamming and loss of GNSS signals, the timer server can automatically switch to another source.



This option assumes that the Bodet time server is in automatic mode (choice of the source) and has 3 independent synchronisation sources.

4.5.5. IRIG INPUT option card (ref. 907 947)

The IRIG INPUT option card makes it possible to synchronise Netsilon from an IRIG signal.

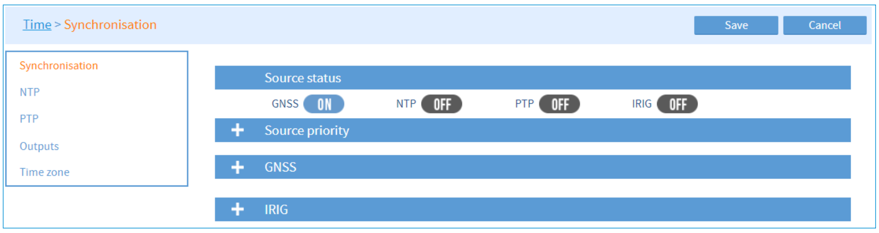


BNC connector

Pluggable
Terminal
block

To set up the IRIG input, follow these steps:

1) TIME menu > Synchronisation > IRIG



Time > Synchronisation

Save Cancel

Synchronisation
NTP
PTP
Outputs
Time zone

Source status

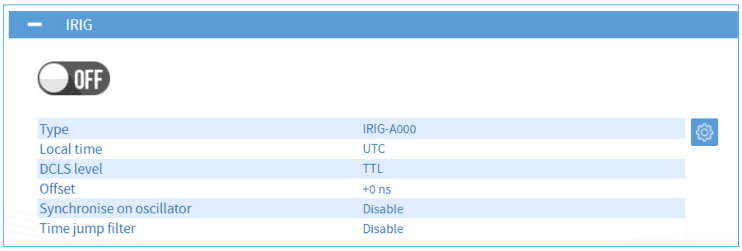
GNSS ON NTP OFF PTP OFF IRIG OFF

+ Source priority

+ GNSS

+ IRIG

2) Enable the synchronisation using the ON button.

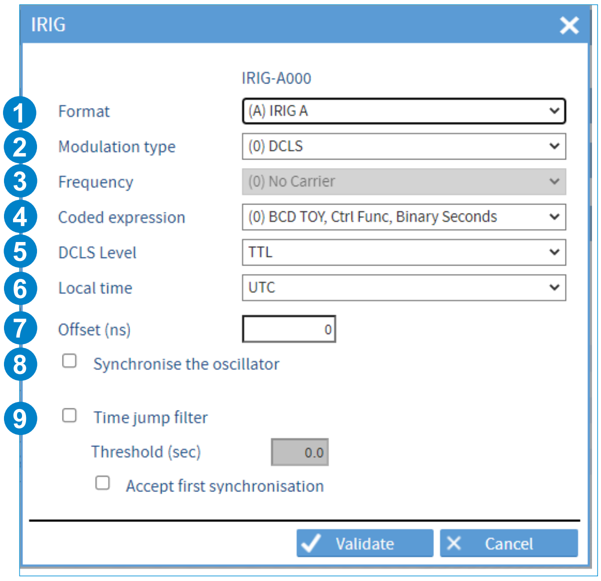


− IRIG

OFF

Type	IRIG-A000
Local time	UTC
DCLS level	TTL
Offset	+0 ns
Synchronise on oscillator	Disable
Time jump filter	Disable

3) Click on ⚙, and the following window will appear:



IRIG ✕

IRIG-A000

1 Format (A) IRIG A

2 Modulation type (0) DCLS

3 Frequency (0) No Carrier

4 Coded expression (0) BCD TOY, Ctrl Func, Binary Seconds

5 DCLS Level TTL

6 Local time UTC

7 Offset (ns) 0

8 □ Synchronise the oscillator

9 □ Time jump filter

Threshold (sec) 0.0

□ Accept first synchronisation

✓ Validate ✕ Cancel

1 Choose the input format, according to the signal source: IRIG A/B/E/G, AFNOR 87500.
The IRIG formats are defined by different pulse rates.

Format	Pulse rate	Interval
IRIG A	1000 PPS	1 ms
IRIG B	100 PPS	10 ms
IRIG E	10 PPS	100 ms
IRIG G	10000 PPS	0.1 ms

2 Choose the type of modulation of the input signal:
- (0) DCLS (DC Level Shift): pulse width coding,
- (1) AM (Amplitude Modulated): amplitude-modulated sine wave carrier.

3 Choose the modulation frequency.
It depends directly on the format and the type of modulation previously chosen.

Modulation frequency
(0) No carrier (DCLS)

(1) 100 Hz
(2) 1 kHz
(3) 10 kHz
(4) 100 kHz

4 Choose the coded expression. It depends directly on the format and the type of modulation previously chosen. This defines the data structure in the IRIG signal.

Coded expressions
(0) BCD TOY, Ctrl Func, Binary Seconds
(1) BCD TOY, Ctrl Func
(2) BCD TOY
(3) BCD TOY, Binary Seconds
(4) BCD TOY/Year, Ctrl Func, Binary Seconds
(5) BCD TOY/, Ctrl Func
(6) BCD TOY/Year
(7) BCD TOY/Year, Binary Seconds

5 Choose the transmission mode (TTL or RS422) depending on the interface with the IRIG source and the type of cable used for the connection with Netsilon (DCLS formats).

6 Time zone used by the IRIG source. Declare the corresponding time zone in Netsilon beforehand if necessary: TIME menu > Time zone > Time zones.

7 Offset used to compensate the IRIG signal transmission delay between the source and Netsilon (cable length). Depending on the quality of the signal, an offset may occur between the top generator of the signal and the synchronisation.
Compensation management is not available with the IRIG E.

8 Option enabling the Netsilon's OCXO oscillator to be slaved to the IRIG signal.
This requires superior signal quality. If the signal quality decreases, the oscillator may switch to the "tracking" or "holdover" state. If the oscillator is slaved, the synchronisation time may be longer.
The IRIG E format does not allow the oscillator to be slaved.

9 The "Time jump filter" is a filter that allows to compensate a momentary time shift of the IRIG signal generator with the time zone, by switching to another synchronisation source beyond a certain threshold set by the user (programmable value from 0.7 to 900 s).
Example: an IRIG signal generator momentarily provides a time signal shifted by 10 seconds from the time zone. If the threshold allowed by the user is 8 seconds, Netsilon detects the anomaly and rejects this source. Depending on the configuration, there will be a switch to another available synchronisation source or a switch to the "holdover" state and then "freerun".
If the threshold value is low, the initial synchronisation may be difficult. In this case, enable the "Accept first synchronisation" option. This disables filtering for the first synchronisation only.
By default, if filtering is disabled, the maximum offset allowed is 15 minutes.

> **Particular case of IRIG synchronisation if Netsilon is PTP Master:**

ℹ **If Netsilon is a PTP master, the OCXO oscillator must imperatively be slaved to the IRIG synchronisation. This requires a high quality signal. See 8 to enable the slaving option.**

⚠ **The IRIG signal delivers a UTC time signal without any indication on the number of Leap Seconds, while the PTP protocol broadcasts TAI (International Atomic Time). It is therefore necessary to know the TAI/UTC offset.**

It is therefore mandatory to manually enter in Netsilon:
- the current offset between TAI and UTC (TAI to UTC offset),
- the information of the next Leap Second so that it can be taken into account automatically.

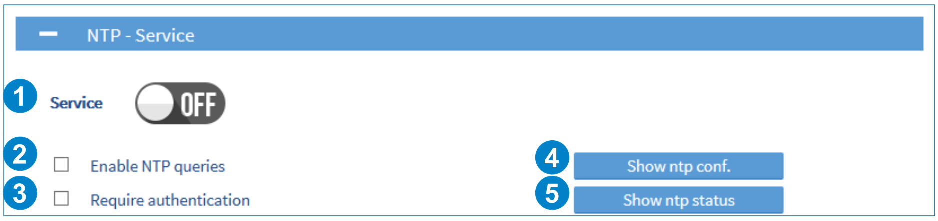
Refer to chapters **4.3.5 Set the TAI/UTC offset** and **4.3.4 Programming a manual Leap Second** to make these entries.

4.6 NTP

4.6.1. NTP service

To enable the NTP service, proceed as follows:

1) TIME menu > NTP > NTP service



Service OFF

□ Enable NTP queries

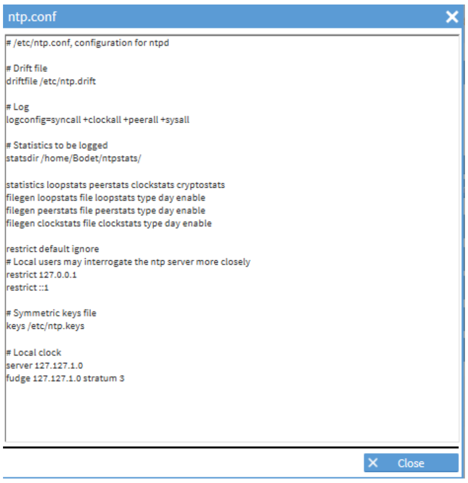
□ Require authentication

1 Service ON/OFF button.

2 Check this box to query the NTP server remotely. Authorisation of mode 6 and 7 NTP packets (remote information queries).

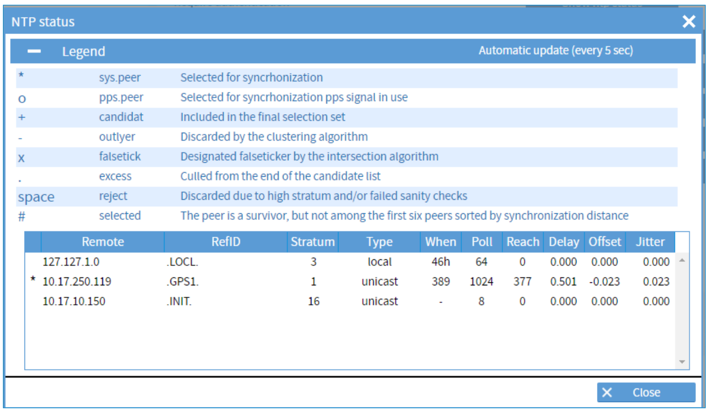
3 Check this box to force authentication with a symmetric key or autokey. Without this authentication, synchronisation is impossible.

4 ntp.conf can be used to display the configuration file (for information purposes, in read-only mode):



```
# /etc/ntp.conf, configuration for ntpd

# Drift file
driftfile /etc/ntp.drift

# Log
logconfig=syncall +clockall +peerall +sysall

# Statistics to be logged
statsdir /home/Bodet/ntpstats/

statistics loopstats peerstats clockstats cryptostats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

restrict default ignore
# Local users may interrogate the ntp server more closely
restrict 127.0.0.1
restrict ::1

# Symmetric keys file
keys /etc/ntp.keys

# Local clock
server 127.127.1.0
fudge 127.127.1.0 stratum 3
```

5 Can be used to display the NTP status, for example:



*	sys.peer	Selected for syncrhonization
o	pps.peer	Selected for syncrhonization pps signal in use
+	candidat	Included in the final selection set
-	outlyer	Discarded by the clustering algorithm
x	falsetick	Designated falseticker by the intersection algorithm
.	excess	Culled from the end of the candidate list
space	reject	Discarded due to high stratum and/or failed sanity checks
#	selected	The peer is a survivor, but not among the first six peers sorted by synchronization distance

	Remote	RefID	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
	127.127.1.0	.LOCL.	3	local	46h	64	0	0.000	0.000	0.000
*	10.17.250.119	.GPS1.	1	unicast	389	1024	377	0.501	-0.023	0.023
	10.17.10.150	.INIT.	16	unicast	-	8	0	0.000	0.000	0.000

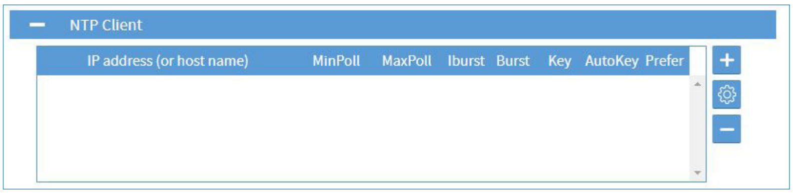
To find out the meaning of a parameter, hover over the text with the PC mouse.

4.6.2. NTP client

In client mode: Netsilon synchronises on an NTP server in unicast.

To add an NTP synchronisation source, follow these steps:

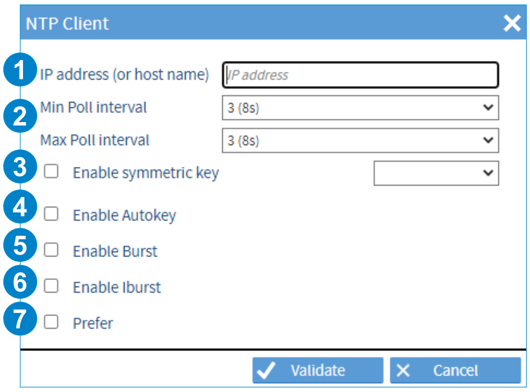
1) TIME menu > NTP > NTP client:



NTP Client

IP address (or host name)	MinPoll	MaxPoll	Iburst	Burst	Key	AutoKey	Prefer

2) Add an NTP server by clicking on +, and the following window will appear:
(Possibility to add up to 10 servers maximum.)



NTP Client

1 IP address (or host name): IP address

2 Min Poll interval: 3 (8s)

Max Poll interval: 3 (8s)

3 □ Enable symmetric key

4 □ Enable Autokey

5 □ Enable Burst

6 □ Enable Iburst

7 □ Prefer

1 Enter the IP address (or the hostname) of the NTP server.

2 Poll interval: this is the period of time in seconds, between two queries. The value shown in the NTP configuration status table (see previous page) will be lower than the minimum value in order to enable quick synchronisation.

Once synchronisation is complete, this value will increase in order to reduce network traffic and load on time servers.

- Chosen range:
  - Automatic.
  - from 3 (8 seconds) to 17 (36 hours 24 minutes and 32 seconds).

3 Enable and select a pre-defined symmetric key.

4 Before enabling this parameter, enter the autokey.

5 The Burst option should be enabled when the server can be reached. It activates the sending of 8 packets with an interval of 16 seconds between the first and the second, then two seconds for the rest. This option improves the stability of exchanges.

6 The iBurst option can be used to synchronise the server more quickly as soon as it starts up.

⚠ **Bodet recommends using iBurst as it enables the rapid provision of an active NTP service.**

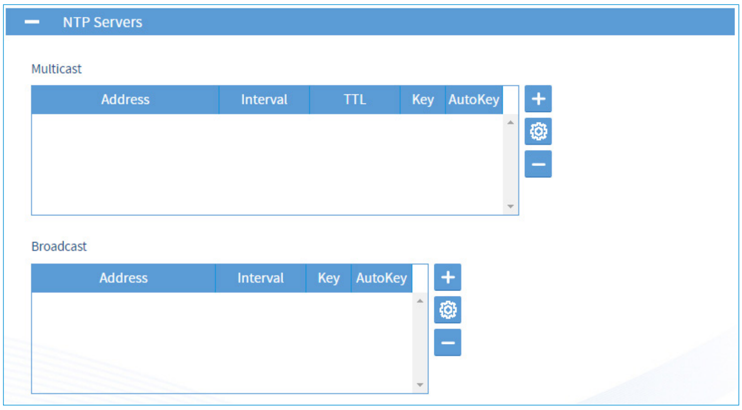
7 This parameter takes N-1 stratum servers as a reference base. This value can apply to a reference source such as GPS. If this option is checked for Netsilon, the user believes that this server is stable and nearby, and that it serves as a priority reference.

4.6.3. NTP servers

In server mode: Netsilon broadcasts the time in multicast, broadcast or unicast.

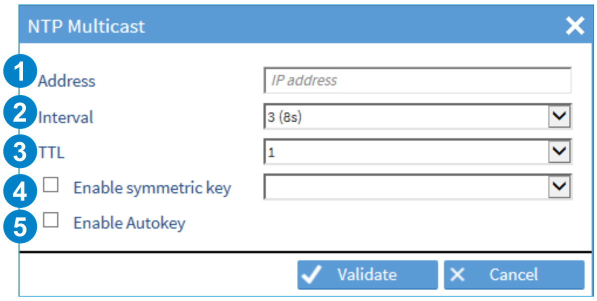
To enable the NTP Servers mode, follow these steps:

1) TIME menu > NTP > NTP servers:

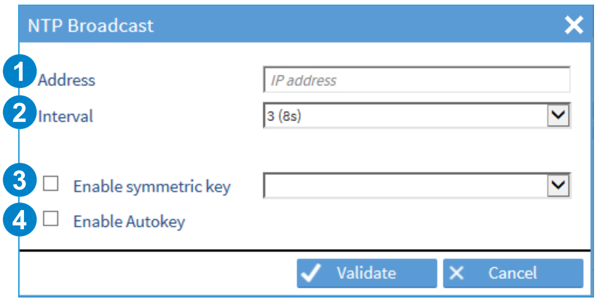


2) Select the communication mode: multicast or broadcast.

3) Add an NTP server by clicking on +, and the following window will appear:
(Possibility to add up to 5 servers in multicast and broadcast)



Address: IP address
Interval: 3 (8s)
TTL: 1
□ Enable symmetric key
□ Enable Autokey



Address: IP address
Interval: 3 (8s)
□ Enable symmetric key
□ Enable Autokey

1 Enter the IP address of the NTP client.

2 Poll interval: this is the period of time in seconds between two queries. The value shown in the NTP configuration status table (see previous page) will be lower than the minimum value in order to enable quick synchronisation.

Once synchronisation is complete, this value will increase in order to reduce network traffic and load on the time servers.

- Chosen range:
  - Automatic.
  - from 3 (8 seconds) to 17 (36 hours 24 minutes and 32 seconds).

3 Values: 1, 32, 64, 96, 128, 160,192 and 224. TTL indicates the time during which a data item is to be retained, or the time during which a data item should be cached.
The initial value of 1 is used by some protocols to ensure that the packets are not routed beyond a segment.

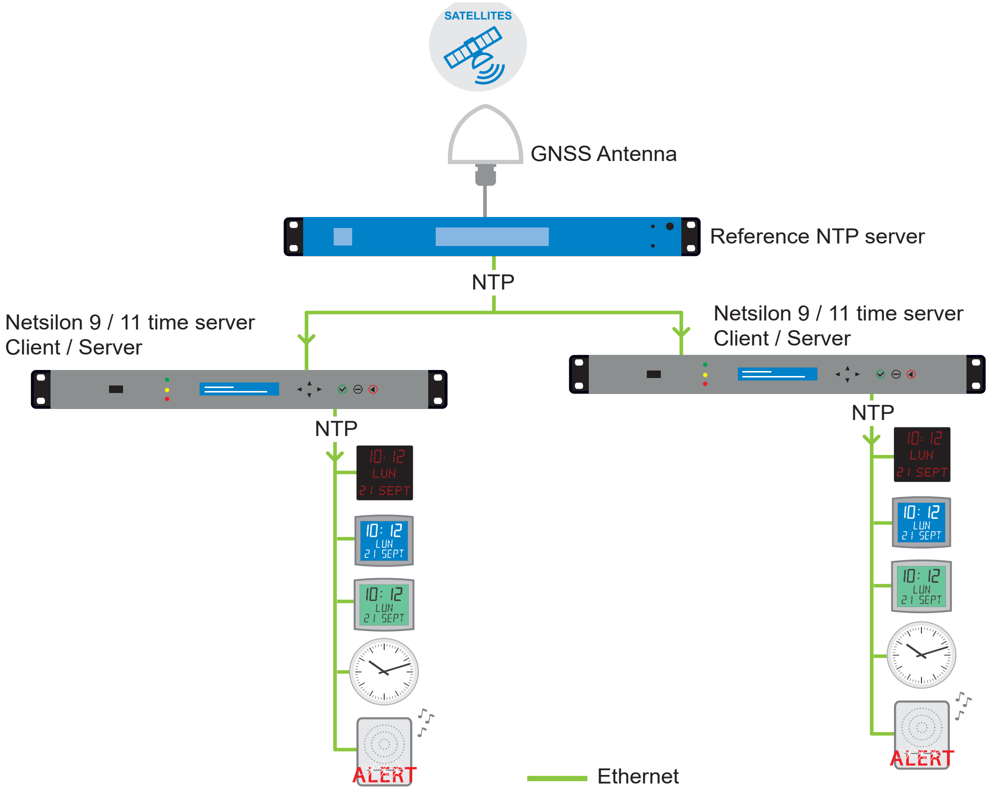
4 Before enabling this parameter, enter the autokey.

5 The Burst option should be enabled when the server can be reached. It activates the sending of 8 packets with an interval of 16 seconds between the first and the second, then two seconds for the rest. This option improves the stability of exchanges.

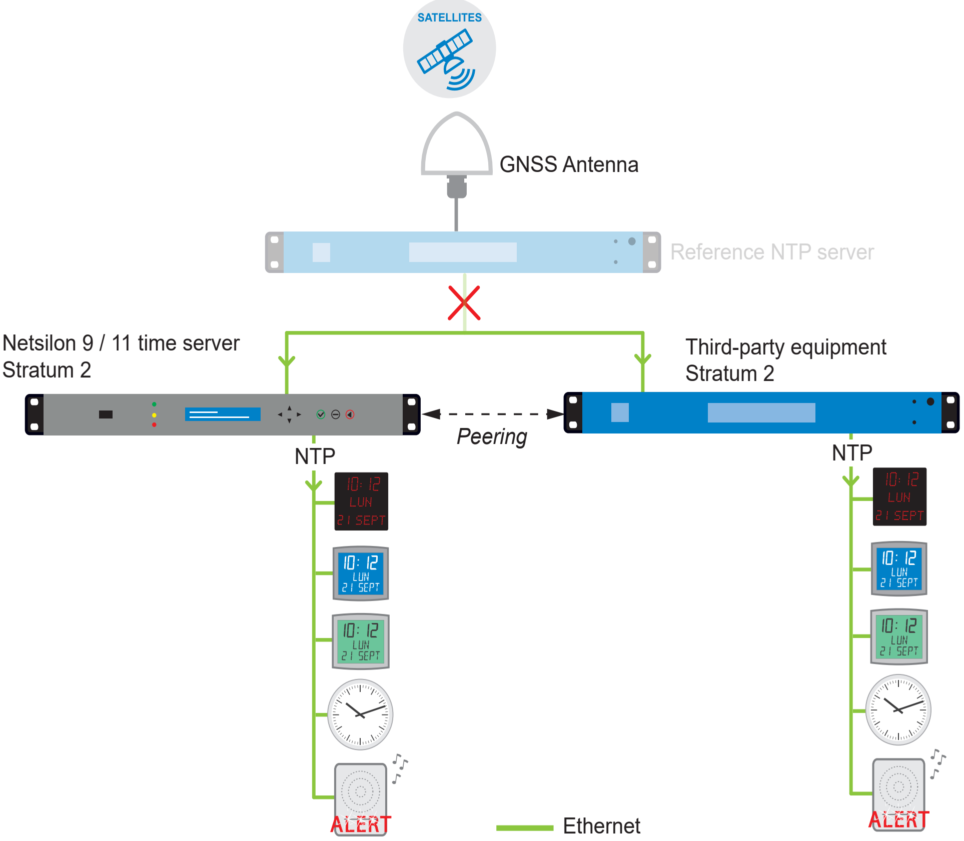
4.6.4. NTP peers

NTP peer is defined between two or more time servers. If neither of them is authorised (at the same hierarchical level) to know the time, both will work to obtain an identical synchronisation.

Scenario 1: the reference server transmits the time signal

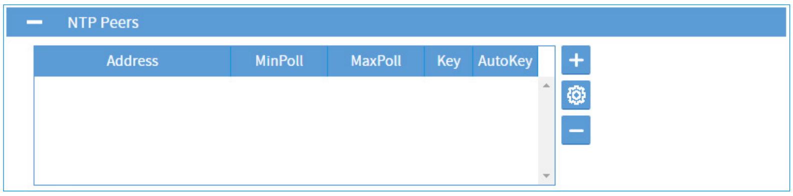


Scenario 2: the reference server no longer transmits the time signal, the third-party device synchronises on Netsilon or vice-versa:



To enable the NTP Peers mode, follow these steps:

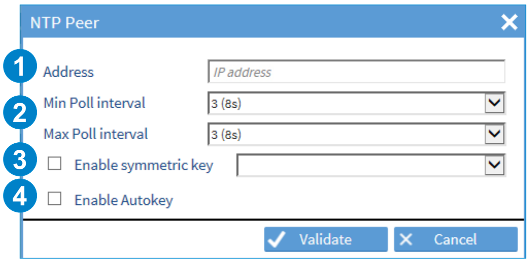
1) TIME menu > NTP > NTP peers:



NTP Peers

Address	MinPoll	MaxPoll	Key	AutoKey

2) Add an NTP server by clicking on +, and the following window appears:
(Possibility to add up to five servers maximum)



NTP Peer

1 Address: IP address

2 Min Poll interval: 3 (8s)

Max Poll interval: 3 (8s)

3 ☐ Enable symmetric key

4 ☐ Enable Autokey

1 Enter the IP address of the NTP client.

2 Poll interval: this is the period of time in seconds between two queries. The value shown in the NTP configuration status table (see previous page) will be lower than the minimum value in order to enable quick synchronisation.

Once synchronisation is complete, this value will increase in order to reduce network traffic and load on time servers.

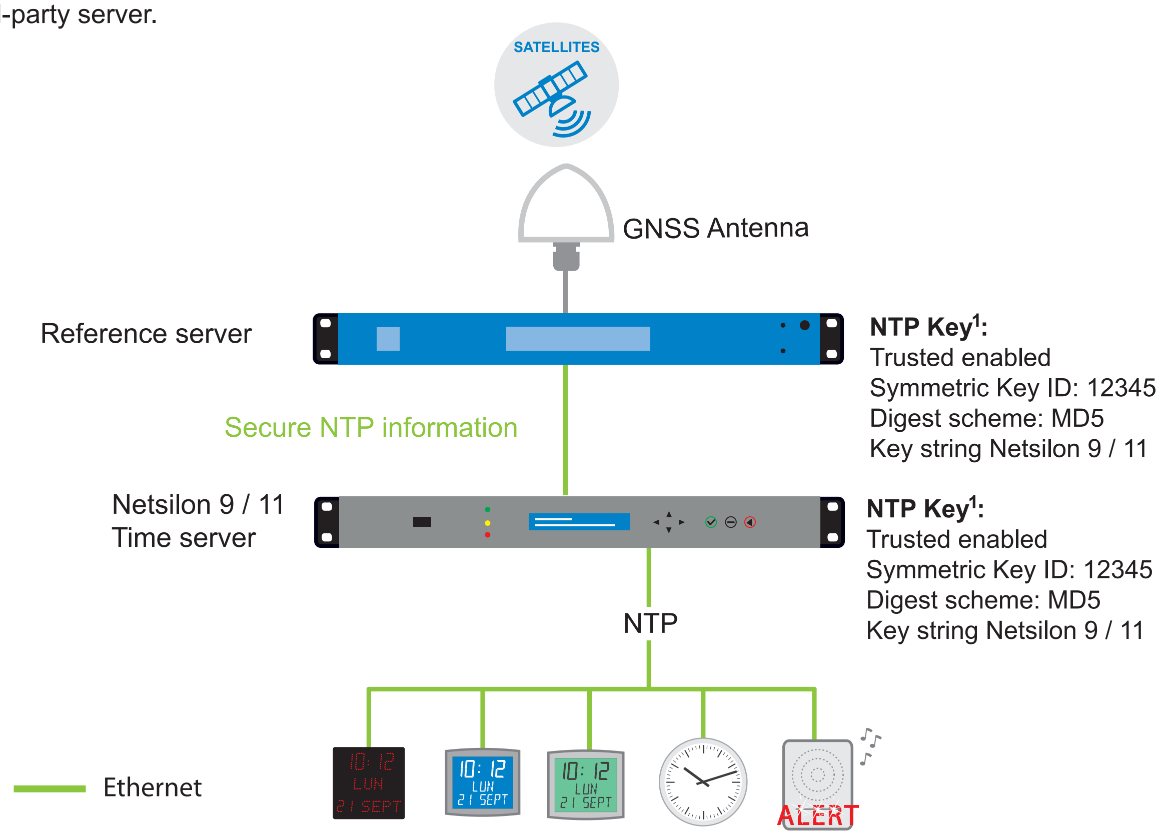
- Chosen range:
  - Automatic.
  - from 3 (8 seconds) to 17 (36 hours 24 minutes and 32 seconds).

3 Values: 1, 32, 64, 96, 128, 160,192 and 224. TTL indicates the time during which a data item is to be retained, or the time during which a data item should be cached.
The initial value of 1 is used by some protocols to ensure that the packets are not routed beyond a segment.

4 Before enabling this parameter, enter the autokey.

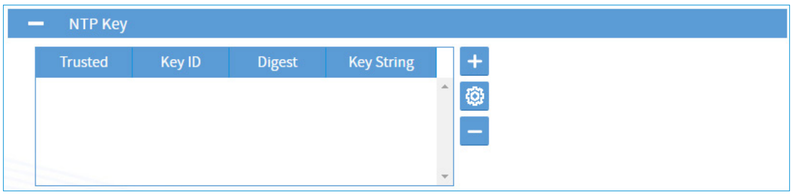
4.6.5. NTP key

The NTP key enables secure communication between a server and an NTP client in order to prevent intrusion by a third-party server.



To enable the NTP key mode, follow these steps:

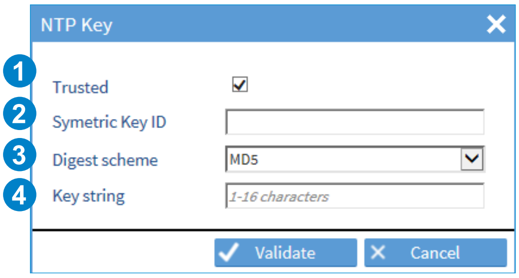
1) TIME menu > NTP > NTP key:



NTP Key

Trusted	Key ID	Digest	Key String

2) Add an NTP key by clicking on +, and the following window will appear:
(possibility to add up to 15 NTP keys maximum)



NTP Key

1 Trusted ☑

2 Symetric Key ID

3 Digest scheme MD5

4 Key string 1-16 characters

1 Check this box to use authentication with a trusted key (by default, the NTP service only takes trusted keys into account). The principle involves assigning and checking if the key for each network device intended to communicate with Netsilon is correct.

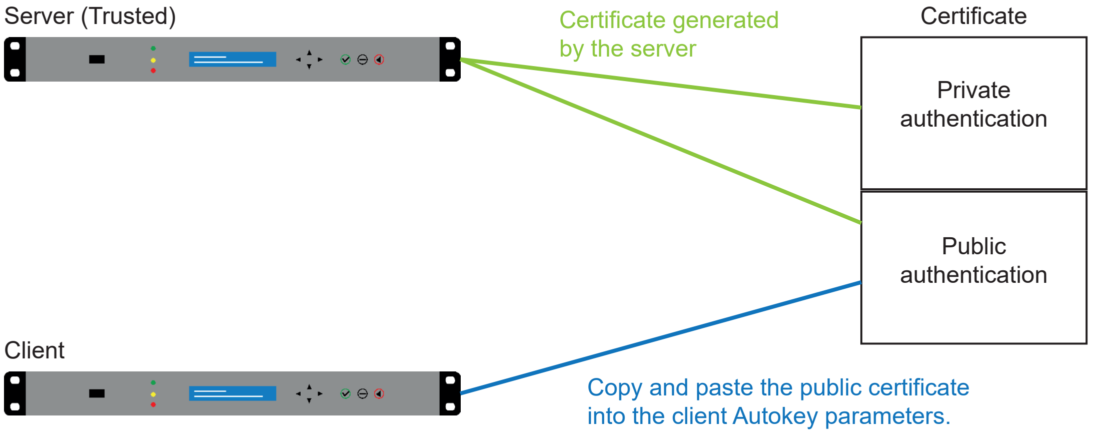
2 Enter a number between 1 and 65534. Netsilon supports MD5 authentication by default. This function assigns a authenticator, consisting of a key and an MD5 message at the end of each request. This ensures that the NTP transmission comes from a trusted NTP server or client.

3 Choose the authentication from the following list:

- MD5
- SHA
- SHA1
- MDC2
- RMD160
- MD4

4 Enter a key between 1 and 16 characters (speical and non-alphabetic characters not allowed. E.g.: !, $, #, %)

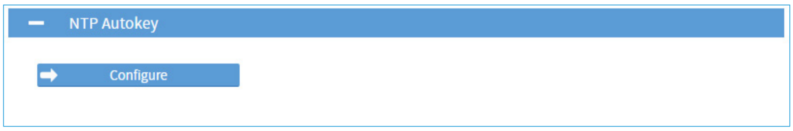
4.6.6. NTP Autokey


Server (Trusted)
Certificate generated by the server
Certificate
Private authentication
Public authentication
Client
Copy and paste the public certificate into the client Autokey parameters.

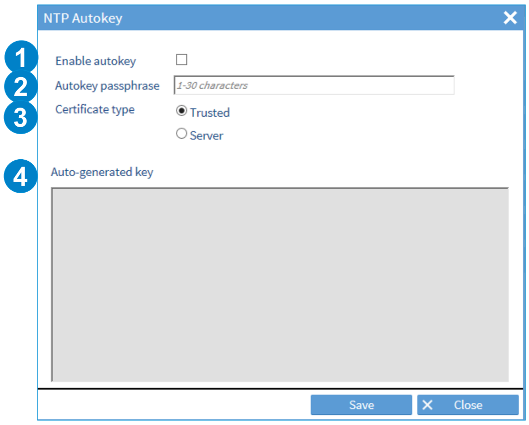
Remember that the devices must have different host names.

To enable the NTP autokey mode, follow these steps:

1) TIME menu > NTP > NTP Autokey:



2) Click on Configure, and the following window will appear:



Enable autokey □

Autokey passphrase 1-30 characters

Certificate type ● Trusted ○ Server

Auto-generated key

1 Check the box to enable and define the autokey.

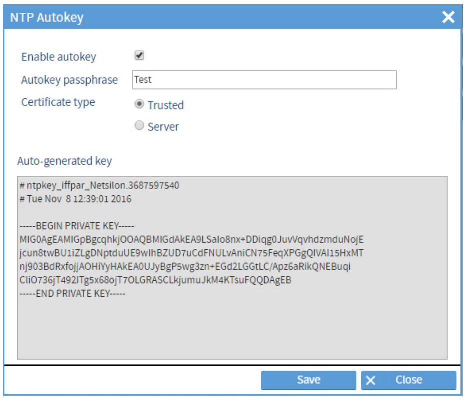
2 Set the passphrase, within the 30-character limit.

3 Before a server can be designated as a client or a server, it must be designated as Trusted. When designating a server as Trusted, select Trusted, then save. A certificate is then generated for the network.

4 Certificate. This certificate is to be copied and pasted in the NTP Autokey parameters of the client servers.

For example :

The certificate is valid for one year, but is automatically renewed every month.



Enable autokey ☑

Autokey passphrase Test

Certificate type ● Trusted ○ Server

Auto-generated key

```
# ntpkey_iffpar_Netsilon.3687597540
# Tue Nov  8 12:39:01 2016

-----BEGIN PRIVATE KEY-----
MIG0AgEAMIGpBgcqhkjOOAQBMIGdAkEA9LSalo8nx+DDiqg0JuvVqvhdzmduNojE
jcun8twBU1iZLgDNptduUE9wlhBZUD7uCdFNULvAniCN75FeqXPGgQIVAI15HxMT
nj903BdRxfojjAOHiYyHAkEA0UJyBgP5wg3zn+EGd2LGGtLC/Apz6aRikQNEBuqi
CliO736jT492ITg5x68ojT7OLGRASCLkjumuJkM4KTsuFQQDAgEB
-----END PRIVATE KEY-----
```

4.6.7. NTP Anycast

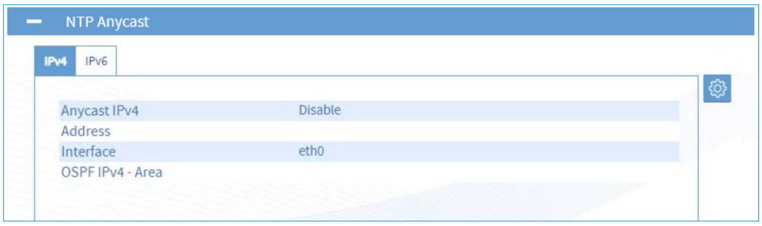
Anycast is applied to the NTP protocol to establish reliable communication between the client and the server (server redundancy).

The network (router / switch) must support the OSPF protocol.

The clocks (clients) send a query to the servers. The Anycast OSPF switch will select the server that responds fastest in order to pass the information on to the clients.

To enable the NTP anycast mode, follow these steps:

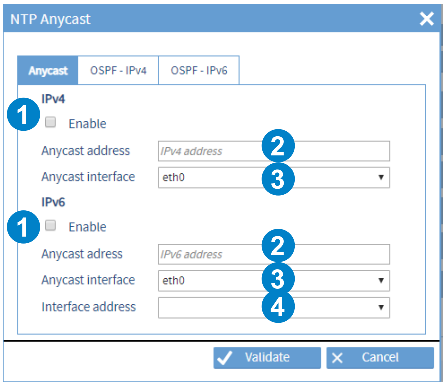
1) TIME menu > NTP > NTP Anycast:



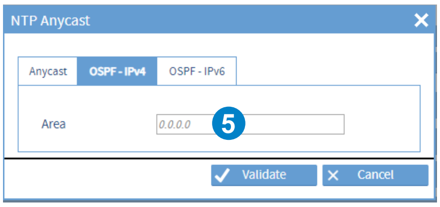
Anycast IPv4	Disable
Address	
Interface	eth0
OSPF IPv4 - Area	

Anycast only starts if the product is synchronised.
It will shut down if synchronisation is lost.

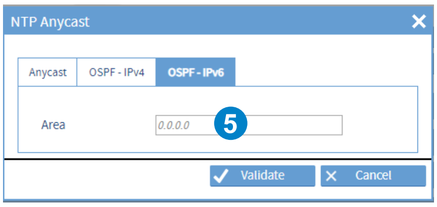
2) Click on ⚙, the following window opens:



IPv4
□ Enable
Anycast address: IPv4 address
Anycast interface: eth0
IPv6
□ Enable
Anycast adress: IPv6 address
Anycast interface: eth0
Interface address:



Area: 0.0.0.0



Area: 0.0.0.0

1 Enable/disable the NTP Anycast mode.

2 Enter the Anycast address.

3 Select the network interface to which the network cable is connected. Contact the network administrator.

4 Select the interface address.

5 Enter the "Area" address (must be identical to the one configured in your OSPF Anycast Switch). Contact the network administrator.

The IPv6 Anycast needs an IPv4 address on the ETH which manages the Anycast. (The IPv4 address is used as router-ID).

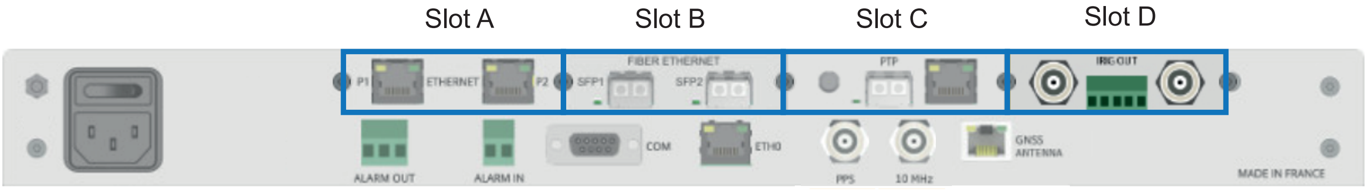
4.7 Time distribution

Time distribution can be carried out in several ways:

- NTP by using the Ethernet RJ45 and/or Ethernet SFP option cards,
- PTP,
- IRIG.
- ASCII : coded time NMEA 0183,...

Option cards can be selected in two ways:

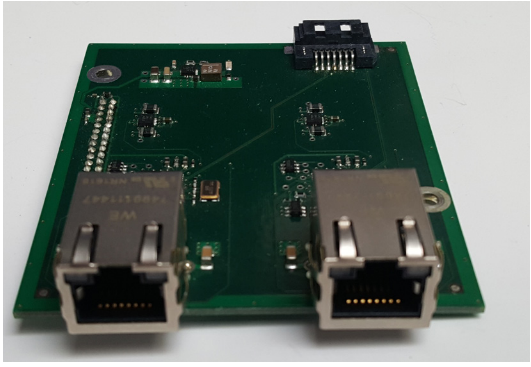
- In dynamic mode: hover the mouse over the desired option card, then click. The menu dedicated to this option card is shown on the screen.
- Click on the + button of the desired option card.



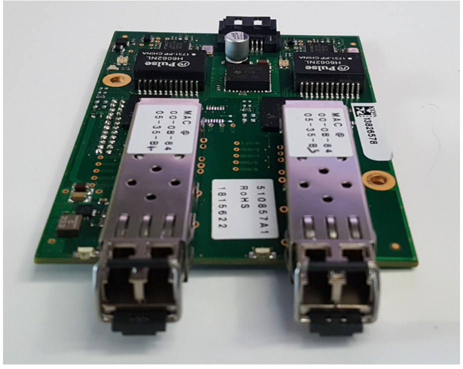
Ethernet option cards (RJ45 and/or SFP) can only be installed in slots A, B or C.

See chapter 4.4 for configuring the Ethernet cards.

4.7.1 ETHERNET option cards (RJ45 ref: 907 920) (SFP ref: 907 021)



RJ45



SFP

The network option card can be used to synchronise several independent Ethernet networks.

To configure a network output, see chapter **4.4.1 Network interface configuration.**

The mechanical installation is performed in our factory. For any subsequent installation, please refer to the option card installation guide available at www.bodet-time.com.

The labels containing the MAC address of each port are placed in the line of the RJ45 connector.

When inspecting a fibre optic connector, always ensure that no light source is left on. There is a risk of serious eye injury.

4.7.2. PTP option card (ref: 907 922)

PTP (Precision Time Protocol - IEEE1588) is an Ethernet protocol that achieves a high level of time accuracy in the nanosecond range. Unlike NTP, PTP uses the physical layer to achieve this level of accuracy by time-stamping and transmitting the time stamp when sending frames over the network. PTP also allows two devices to be synchronised in time, frequency and phase.

This protocol is governed by a Master-Slave operation of the clocks present on the network. Some of them, due to their configuration and their best synchronisation characteristics, are alternatively eligible to the status of Master Clock and broadcast SYNC time synchronisation messages to the slaves. The time interval between the transmission of two synchronisation frames by the Master Clock is called Sync Interval. The Master Clock must itself be synchronised by receiving a time signal from a constellation (GPS, Glonass, Galileo...).

To define the Master Clock, there is an algorithm called BMCA (Best Master Clock Algorithm) whose parameters are adjustable by the user.

Here are the BMCA criteria for choosing the Master Clock:

1. Priority 1 (adjustable by the user): 8-bit value which gives a priority index (the lower is the value, the higher is the priority)
2. Clock Class: class of the clock (reliability of the time source, depending on its status: synchronised to a constellation, holdover...) which gives it a priority index,
3. Clock Accuracy: the range of accuracy between the clock and UTC (from the synchronisation constellation) in nanoseconds,
4. Clock Variance: the stability of the clock,
5. Priority 2 (adjustable by the user): 8-bit value which gives a priority index in the event of failure of the other criteria (the lower is the value, the higher is the priority),
6. ClockIdentity: unique identifier of each clock (MAC of the interface)

The BMCA is present in each PTP device so that all of them choose the same Master Clock. Clocks that are eligible for the Master clock status but which do not have this role to play at the current time (because they do not have the best synchronisation characteristics) go into “passive” mode.

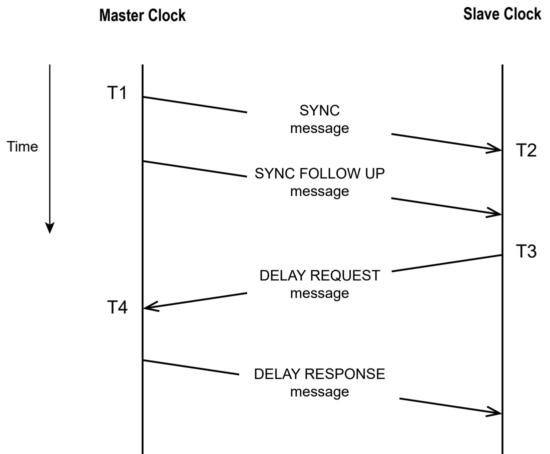
Periodically, the clocks eligible for the Master Clock status broadcast an ANNOUNCE message on the network to the Slaves with its parameters and synchronisation characteristics. The time interval between the transmission of two of these messages is called Announce Interval. When the Slaves receive this ANNOUNCE message, the BMCA sets the Master Clock for all Slaves, which will then synchronise to it.

The extreme precision of this protocol is also due to the fact that the propagation delay of a PTP frame through the network (and therefore the induced delay generated) is constantly corrected by a calculation algorithm.

At the start of a SYNC synchronisation frame from the Master Clock to the Slaves, either the frame is time-stamped directly by the output port of the device (One Step mode) of the Master Clock, or a second FOLLOW UP message immediately follows the SYNC message to give its transmission time (Two Step mode).

After receiving the SYNC message, the Slaves send a DELAY REQUEST message to the Master Clock which responds with a DELAY RESPONSE message.

These exchanges of time-stamped messages between Master and Slaves allow the propagation delay and offset to be measured. Then, a correction is applied by a calculation algorithm so that Master and Slave are synchronised.



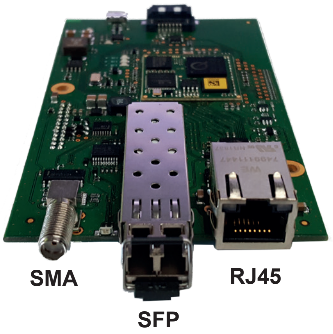
Master / Slave messages

To ensure a high level of accuracy on a network carrying PTP frames, specific switches must be used. There are two types of switches:

› The **Boundary Clock** (BC) which synchronises with the Master Clock (thus becoming its Slave) but becomes Master for the Slaves to which it acts as a relay on the network,

› The **Transparent Clock** (TC) allows PTP frames from the Master Clock to pass through, adding a time correction to take into account the transit time through its device.

The PTP protocol requires a suitable network architecture (switch, routers, etc) to guarantee a high level of accuracy.



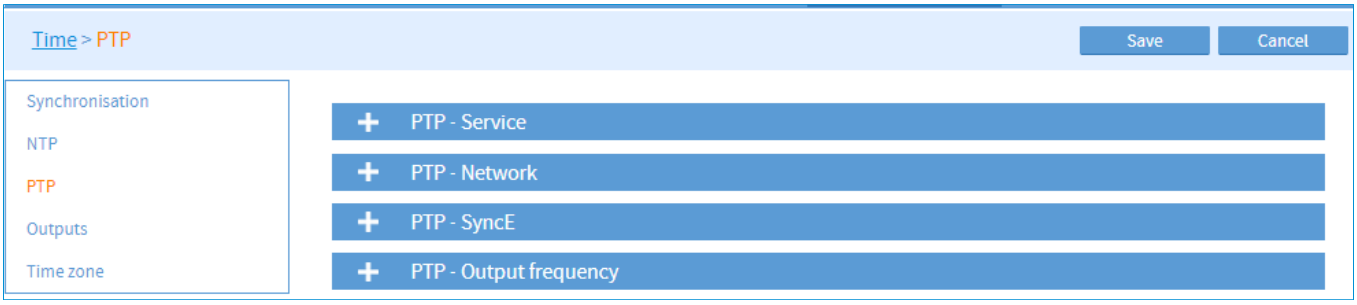
The PTP option is only operational for a GNSS reception. The master mode only operates with a GNSS reception but does not operate if the GNSS reception is only based on the GLONASS constellation.

Ethernet Interface Combo Port:
- 1 x 10 / 100 / 1000BASE-T RJ45
- 1 x GBIT SFP

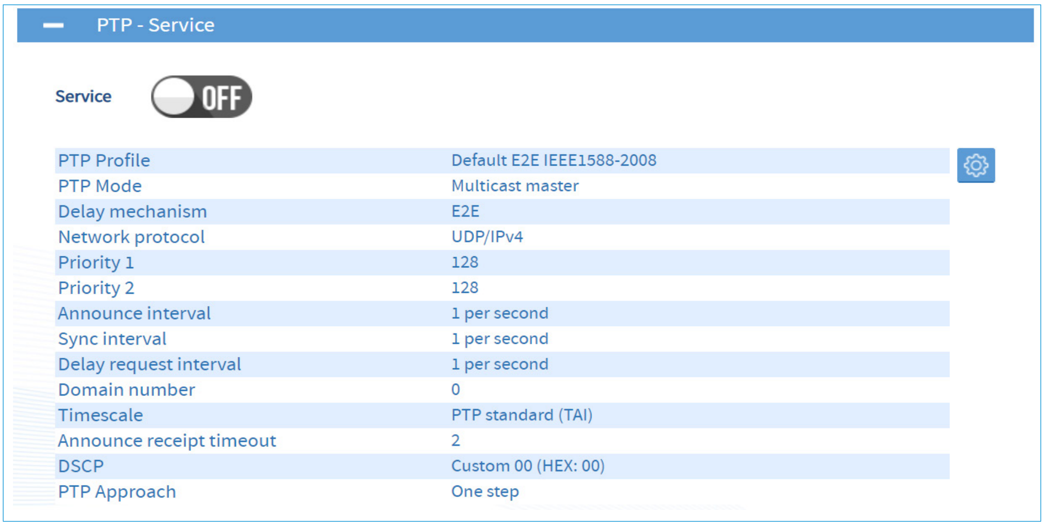
Customisable frequency output on SMA connector.

To set up the PTP output, follow these steps:

1) TIME menu > PTP

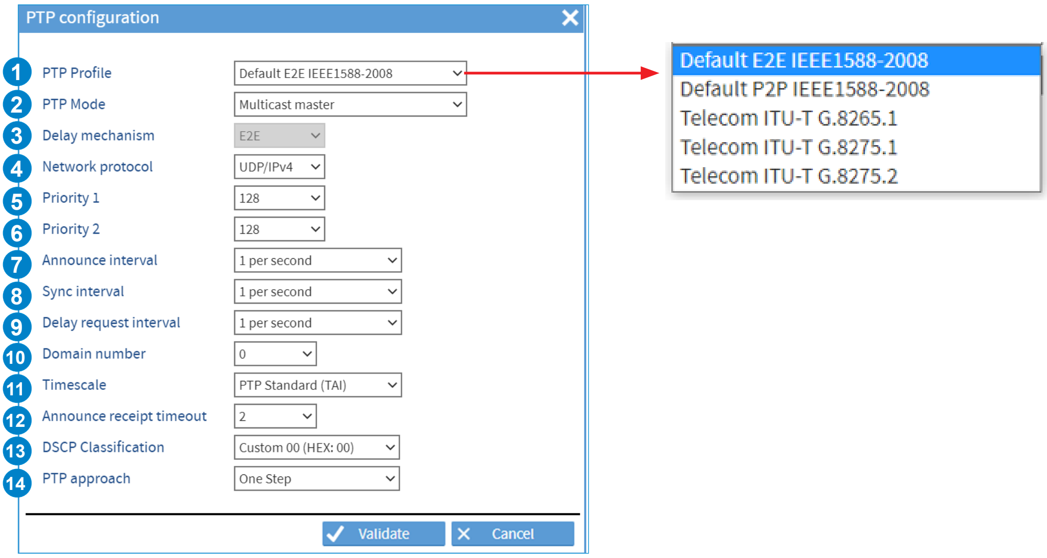


2) Enable the service using the ON button.



PTP Profile	Default E2E IEEE1588-2008
PTP Mode	Multicast master
Delay mechanism	E2E
Network protocol	UDP/IPv4
Priority 1	128
Priority 2	128
Announce interval	1 per second
Sync interval	1 per second
Delay request interval	1 per second
Domain number	0
Timescale	PTP standard (TAI)
Announce receipt timeout	2
DSCP	Custom 00 (HEX: 00)
PTP Approach	One step

3) Click on ⚙, and the following window will appear:



PTP configuration

1. PTP Profile: Default E2E IEEE1588-2008
2. PTP Mode: Multicast master
3. Delay mechanism: E2E
4. Network protocol: UDP/IPv4
5. Priority 1: 128
6. Priority 2: 128
7. Announce interval: 1 per second
8. Sync interval: 1 per second
9. Delay request interval: 1 per second
10. Domain number: 0
11. Timescale: PTP Standard (TAI)
12. Announce receipt timeout: 2
13. DSCP Classification: Custom 00 (HEX: 00)
14. PTP approach: One Step

1 PTP Profile: choose the “PTP profile” which will define:

- The algorithm parameters for choosing the best Master Clock on the network (BMCA),
- Parameters for configuring and sending data frames,
- The way to determine the delay time of data frames (End-to-end or Peer-to-Per).

The following PTP profiles are supported:

- Default E2E IEEE 1588-2008,
- Default P2P IEEE 1588-2008,
- Telecom ITU-T G8265.1
- Telecom ITU-T G8275.1
- Telecom ITU-T G8275.2

The Telecom “PTP profiles” meet specific needs of telecommunication networks by using a particular BMCA (Best Master Clock Algorithm). The product supports telecom profiles. However, its compliance with telecom standards, which in addition to the protocol impose accuracy constraints (e.g. On MTIE and DTEV), has not been checked.

The use of the P2P profile requires the presence of a network (machines, switch, routers...) supporting this type of measurement mechanism. The P2P mechanism is not available in unicast mode (PTP mode).

2 PTP mode: choose the role and synchronisation mode on the network.
The possibilities of synchronisation depend on the “PTP profile” previously chosen.

	Delay mechanism	Multicast	Unicast	IPv4	IPv6	802.3
		Choice		Choice		
Default E2E IEEE1588-2008	E2E	√	√	√	√	√*
Default P2P IEEE1588-2008	P2P	√		√	√	√
Telecom ITU-T G.8265.1	E2E		√	√	√	
Telecom ITU-T G.8275.1	E2E	√				√
Telecom ITU-T G.8275.2	E2E		√	√	√	

* only in multicast

› **Multicast mode:** Data frames are sent from the Master to the Slaves via a Multicast broadcast address dedicated specifically to the PTP protocol. Only the Slaves that are listening on this address receive data packets.

› **Unicast mode**: Point-to-point connection between the Master and the Slaves via a unique IP address for each slave clock on the network. The Master sends the data packets for each Slave. This connection mode requires more resources from the Master and generates more traffic.

Some routers may block the multicast mode.

3 Delay mechanism: choose the mechanism for measuring the delay period.
It is essential to know the SYNC message transit time from the Master to the Slaves in order to measure and correct the network latency and provide correct time information. The way of measuring the delay of data packets through the network depends on the choice of the “PTP Profile”. There is a difference between Default E2E

(End-to-end) and Default PTP (Peer-to-Per) profiles since there are two different mechanisms for measuring the delay period of a message.

›E2E: the packet delay time is directly determined by an exchange of direct requests over the network from the Master to the Slaves.

›P2P: The packet delay time is determined between two consecutive network elements (switch...) and then successfully added together to give the total delay time from the Master to the Slaves.

4 Network protocol: choose the network protocol between UDP IPv4, IPv6 and IEEE 802.3. It is recommended to use UDP IPv4 / IPv6 protocols which are used in most network environments.

5 Priority 1: choose a value. This value which can be set to 8 bits is the main parameter that allows to define the best Master Clock on the network between several eligible ones (BCMA algorithm). The default value is 128 and can vary between 0 and 255. The lower is the value, the higher is the priority.

6 Priority 2: choose a value. This value which can be set to 8 bits is the fifth parameter (out of six) that allows to define the best Master Clock on the network between several eligible ones (BMCA algorithm).The default value is 128 and can vary between 0 and 255. The lower is the value, the higher is the priority.

7 Announce interval: choose the time interval at which the clocks eligible for the status of Master Clock send the ANNOUNCE message, including their synchronisation and accuracy parameters on the network. Depending on the quality of the transmitted values and the priorities set within its algorithm, the BMCA defines the Master Clock.

8 Sync interval: choose the time interval for sending a synchronisation frame. The higher is the number of frames, the better is the accuracy. However, this overloads the network. There is therefore a compromise to be found between accuracy and load on the network traffic.

9 Delay request interval: Choose the time interval for sending a request from the Slaves to the Master Clock to determine the delay time of the data packets.

10 Domain number: choose the domain number. It is possible to define several domains within the same network. Each domain will have its own Master Clock and Slaves.

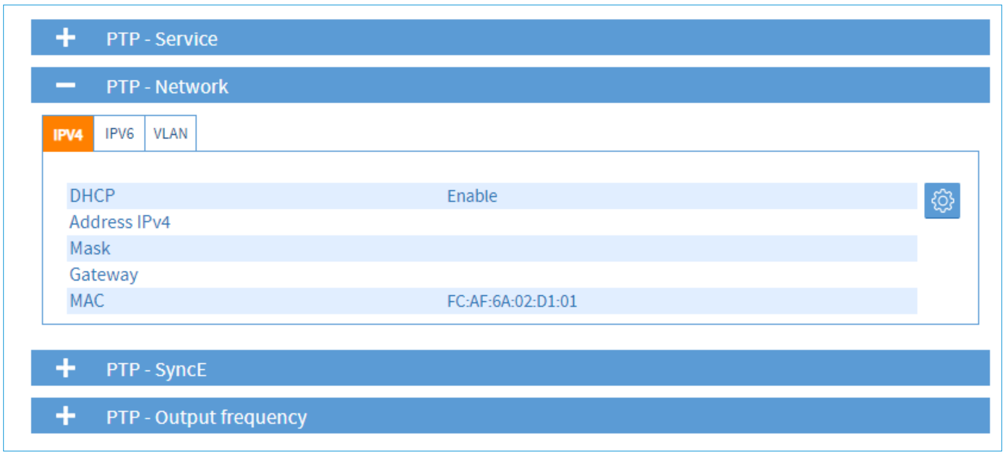
11 Timescale: choose the time scale. By default, the International Atomic Time (TAI) is selected. It is based on the definition of the second developed using the atomic clock and is not affected by leap seconds. Nevertheless, the offset for calculating UTC is transmitted in the PTP frames.
The arbitrary time scale (UTC=0) can only be used for testing purposes. With this scale, the slave clocks will not be able to calculate the correct UTC time.

12 Announce receipt timeout: choose a value which defines the delay before a slave disconnects from the master without receiving an ANNOUNCE message from it. This value is a multiplier.
Example: if the Announce Interval is 2 seconds and the Announce receipt timeout is 3, the time interval before expiration is 6 seconds.

13 DSCP classification: choose a profile. This allows to prioritise PTP frames.
DSCP (Differentiated Services Code Point) is a network architecture that defines a mechanism for ordering and controlling network traffic, while providing quality of service (carrying a type of traffic under the best possible conditions, in terms of availability, throughput...) by distinguishing between services and data using a code.
The DSCP allows to identify and prioritise PTP frames in the event of network overload to ensure the accuracy of critical systems.

14 PTP approach: choose the operation mode.
PTP sends periodic SYNC messages from the Master to the Slaves with a precise time stamping. To do this, depending on the hardware used, there are two possibilities:
› In One Step mode, the SYNC message is sent and time stamped directly from the Master's output port (due to its physical layer) to the Slaves.
› In Two Step mode, the SYNC message is sent from the Master to the Slaves without a time stamp included in the message. A second message called FOLLOW UP immediately follows the first message to timestamp it.

4) Setting up the PTP Network:

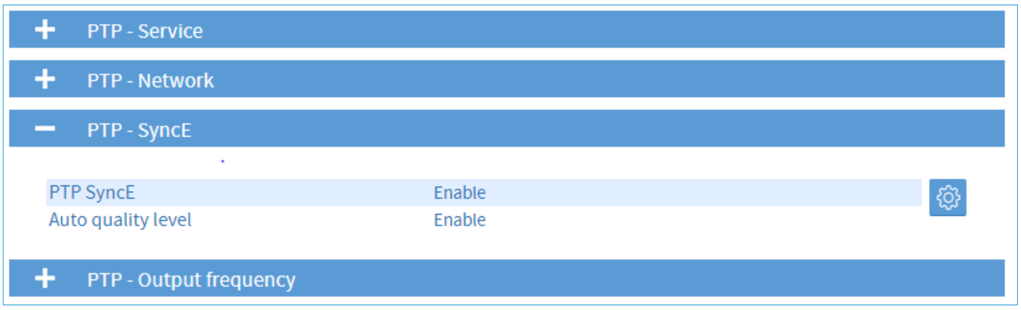


DHCP Enable
Address IPv4
Mask
Gateway
MAC FC:AF:6A:02:D1:01

Operating in IPv4: fixed IP configuration or DHCP service
Operating in IPv6: local link address (with IPv4 address: fixed IP or DHCP service enabled)
VLAN tagging support: optimised traffic management (VLAN ID + priority index).

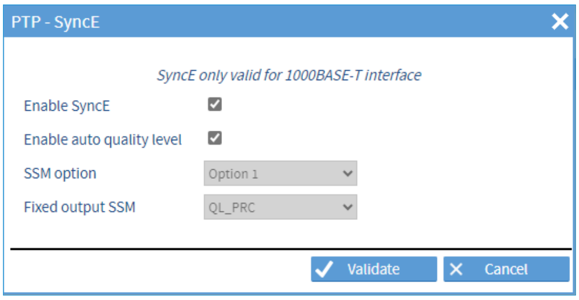
5) Configure PTP SyncE.

SyncE (Synchronous Ethernet) is a protocol for making easier the flow of clock signals over the Ethernet physical layer by ensuring reliable and synchronous propagation of the Master Clock signal to the slave clocks in a network. Enabling this service allows to gain a better accuracy.



PTP SyncE Enable
Auto quality level Enable

By clicking on ⚙, the following window appears:

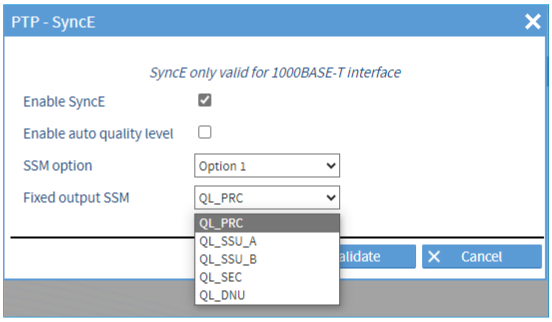


SyncE only valid for 1000BASE-T interface

Enable SyncE ☑
Enable auto quality level ☑
SSM option Option 1
Fixed output SSM QL_PRC

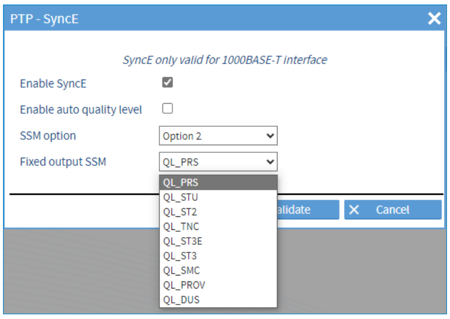
It is recommended to leave the “Enable auto quality level” option checked.

When “Enable auto quality level” is disabled, 2 SSM options are available with the following choices:



SyncE only valid for 1000BASE-T interface

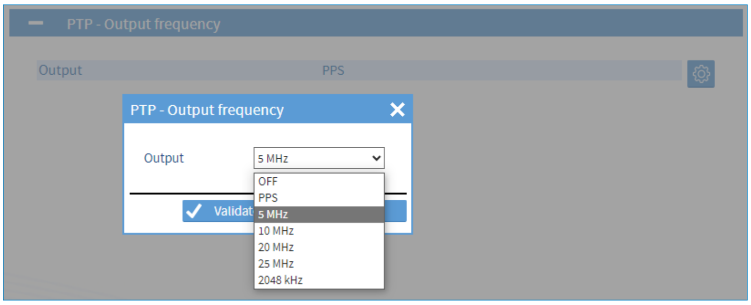
Enable SyncE ☑
Enable auto quality level ☐
SSM option Option 1
Fixed output SSM QL_PRC



SyncE only valid for 1000BASE-T interface

Enable SyncE ☑
Enable auto quality level ☐
SSM option Option 2
Fixed output SSM QL_PRS

6) Setting up the Frequency output.



PTP - Output frequency

Output PPS

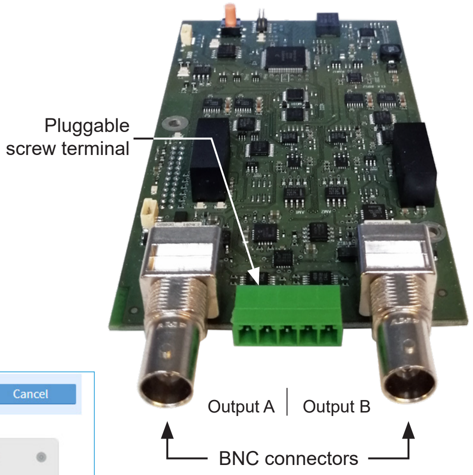
PTP - Output frequency

Output: 5 MHz

OFF
PPS
5 MHz
10 MHz
20 MHz
25 MHz
2048 kHz

- The SMA frequency output is always linked to the master.
    - o Master mode: the frequency and the phase of the 1pps are the image of the Netsilon time zone.
    - o Slave mode: the frequency and the phase of the 1pps are the image of the master’s Time zone to which the option is synchronised.

4.7.3. IRIG OUTPUT option card (ref: 907 930)

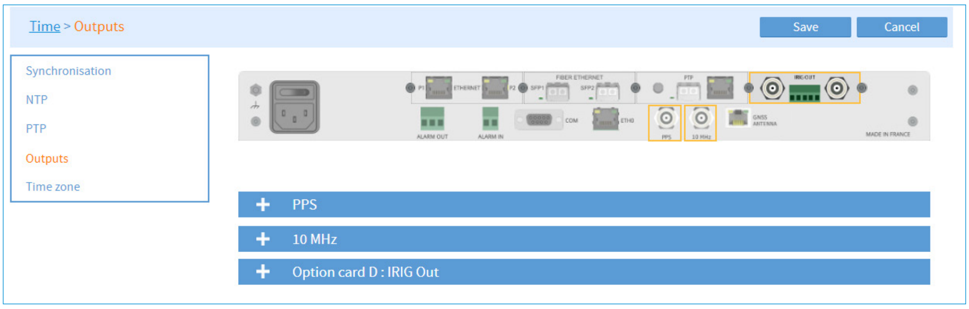


The IRIG OUTPUT option card has 2 independent outputs that generate IRIG signals for synchronising equipment.

These two independent outputs allow generating 2 different IRIG formats and managing 2 time zones.

To set up the 2 IRIG outputs, follow these steps:

1) TIME menu > Outputs > IRIG OUT



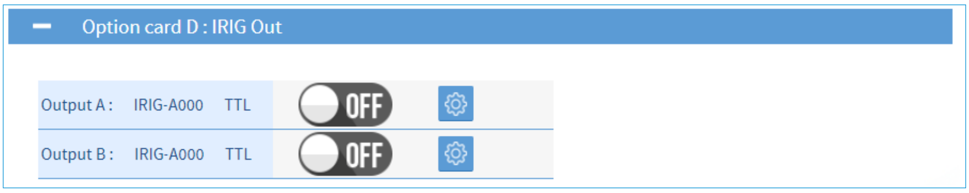
Time > Outputs

+ PPS

+ 10 MHz

+ Option card D : IRIG Out

2) Enable the outputs of the option card with the ON button corresponding to each output.

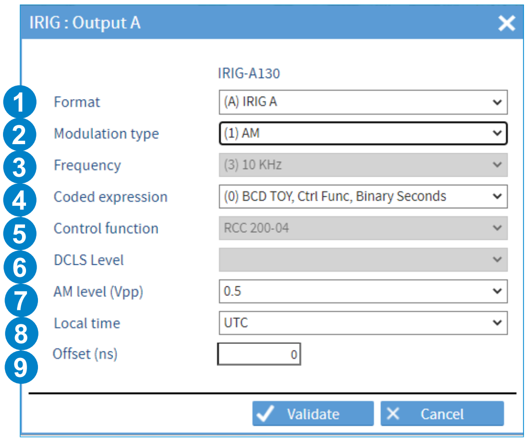


Option card D : IRIG Out

Output A : IRIG-A000 TTL OFF

Output B : IRIG-A000 TTL OFF

3) Configure each output, click on the ⚙ buttons, and the following window will appear:



IRIG : Output A

IRIG-A130

1	Format	(A) IRIG A
2	Modulation type	(1) AM
3	Frequency	(3) 10 KHz
4	Coded expression	(0) BCD TOY, Ctrl Func, Binary Seconds
5	Control function	RCC 200-04
6	DCLS Level	
7	AM level (Vpp)	0.5
8	Local time	UTC
9	Offset (ns)	0

1 Choose the output format: IRIG A/B/E/G, AFNOR 87500.
The IRIG formats are defined by different pulse rates.

Format	Pulse rate	Interval
IRIG A	1000 PPS	1 ms
IRIG B	100 PPS	10 ms
IRIG E	10 PPS	100 ms
IRIG G	10000 PPS	0.1 ms

2 Choose the type of modulation of the output signal:
- (0) DCLS (DC Level Shift): pulse width coding,
- (1) AM (Amplitude Modulated): amplitude-modulated sine wave carrier.

3 Choose the modulation frequency of the output signal.
It depends directly on the format and the type of modulation previously chosen.

Modulation frequency
(0) No carrier (DCLS)
(1) 100 Hz
(2) 1 kHz
(3) 10 kHz
(4) 100 kHz

4 Choose the coded expression. It depends directly on the format and the type of modulation previously chosen.
This defines the data structure in the IRIG signal.

Coded expressions
(0) BCD TOY, Ctrl Func, Binary Seconds
(1) BCD TOY, Ctrl Func
(2) BCD TOY
(3) BCD TOY, Binary Seconds
(4) BCD TOY/Year, Ctrl Func, Binary Seconds
(5) BCD TOY/, Ctrl Func
(6) BCD TOY/Year
(7) BCD TOY/Year, Binary Seconds

5 “Control Function” is a series of bits available for optional transmission of additional information in the output IRIG signal (e.g. current year).
Netsilon is compatible with the RCC 200-04 standard.

6 Choose the transmission mode (TTL or RS422) for DCLS formats depending on the type of cable used between Netsilon and the device receiving the IRIG signal.

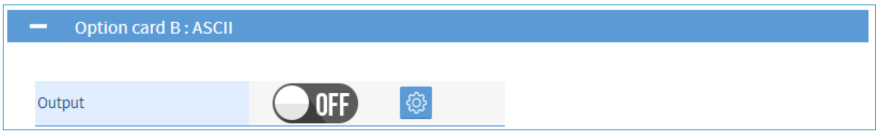
7 Choose the signal voltage for AM formats in order to compensate for possible interference or long transmission distance with the device receiving the signal.

8 Time zone of the output IRIG signal.
The time zone must be previously added in Netsilon (except if it is UTC):
TIME menu > Time zone > Time zones.

9 Offset used to compensate for the IRIG signal transmission delay between Netsilon and the receiving device (depending on the cable length). **Compensation management is not available with the IRIG E.**

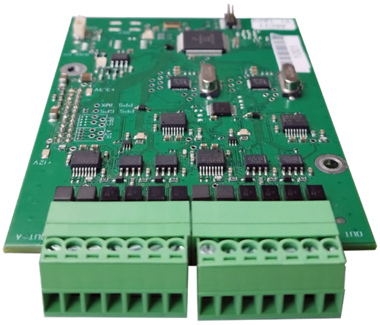
4.7.4. ASCII option card (ref: 907 924)

The ASCII option card distributes the time in coded time to a RS232, RS422 and RS485 serial interface.
To set up ASCII outputs, follow these steps:
1) TIME menu > Outputs > ASCII option card:



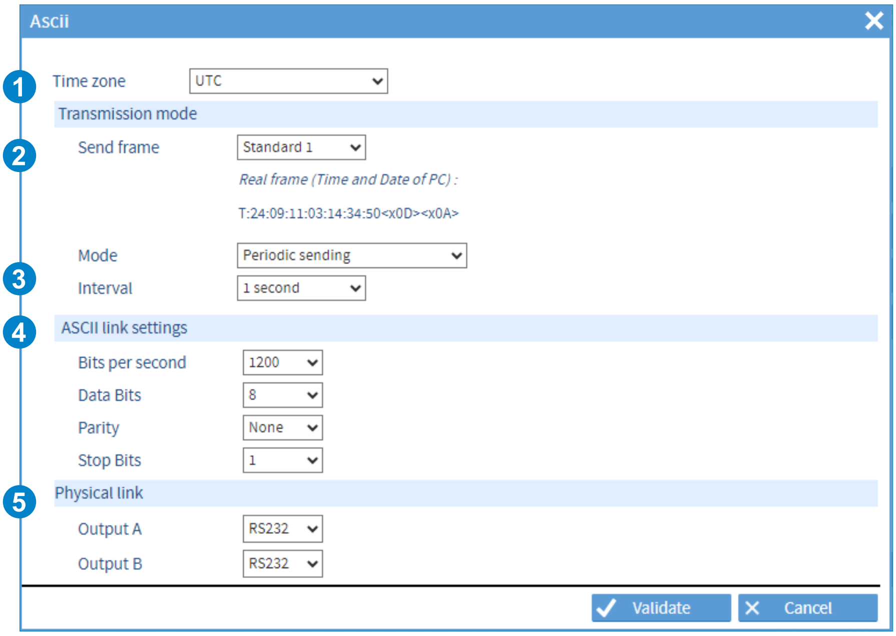
Option card B : ASCII

Output: OFF ⚙



2) Activate the outputs using the ON button, then save.

3) Click on ⚙ to carry out the configuration, and the following window opens:



Ascii

1 Time zone: UTC

Transmission mode

2 Send frame: Standard 1

Real frame (Time and Date of PC) :

T:24:09:11:03:14:34:50<x0D><x0A>

Mode: Periodic sending

3 Interval: 1 second

4 ASCII link settings

Bits per second: 1200

Data Bits: 8

Parity: None

Stop Bits: 1

5 Physical link

Output A: RS232

Output B: RS232

1 Time zone of the ASCII output signal.
The time zone must have been previously added in Netsilon (except if it is UTC):
TIME menu > Time base > Time zones.

2 Choose the coded expression. This defines the nature of the data included in the ASCII signal.

	Content of the message	Example
Standard 1	T:YY:MM:DD:ND:HH:MM:SS “x0D””x0A”	T:08:10:09:04:15:12:30<CR><LF>
Standard 2	“x02” 00 DoW DD/MM/YY HH:MM:SS “0D”	02 00 Thu 09/10/08 15:12:30<CR>
ZDA GGA GPS simulation	$GPZDA,HHMMSS.00,DD,MM,YYYY,00,00 *”checksum””x0D””x0A” $GPGGA,HHMMSS.000,0000.0000,N,00000.0000,W,1,12,0.00,000.0,M,00.0,M,, *”checksum””x0D””x0A”	$GPZDA,082613.00,02,04,2025,00,00*6B <CR><LF> $GPGGA,082613.000,0000.0000,N,00000.0000,W,1,12,0.00,000.0,M,00.0,M,,*73<CR><LF>
Prog.	%01: day of the month %02: month %03: year %04: hour %05: minute %06: second %07: day of the week %08: Sign of time difference %09: Hour of time difference %10: Minutes of time difference %11: Season %31: Frame ID %32: Checksum	« TIME :%04 :% :05% :%06 » at 12h30 and 12 seconds will be « TIME :12 :30 :12 »

3 Choose the frame transmission mode and the associated setting.
- Transmission on request following a “T”, “? “ or programmable (Prog.) request.
- Periodic transmission with an interval of 1 second, 30 seconds, 1 minute, 10 minutes or 1 hour.

4 ASCII link settings:
- Bits per second: 1200 to 57600 bauds,
- Data bits: 7 or 8 bits,
- Parity: none, even or odd,
- Stop bits: 1 or 2 bits.

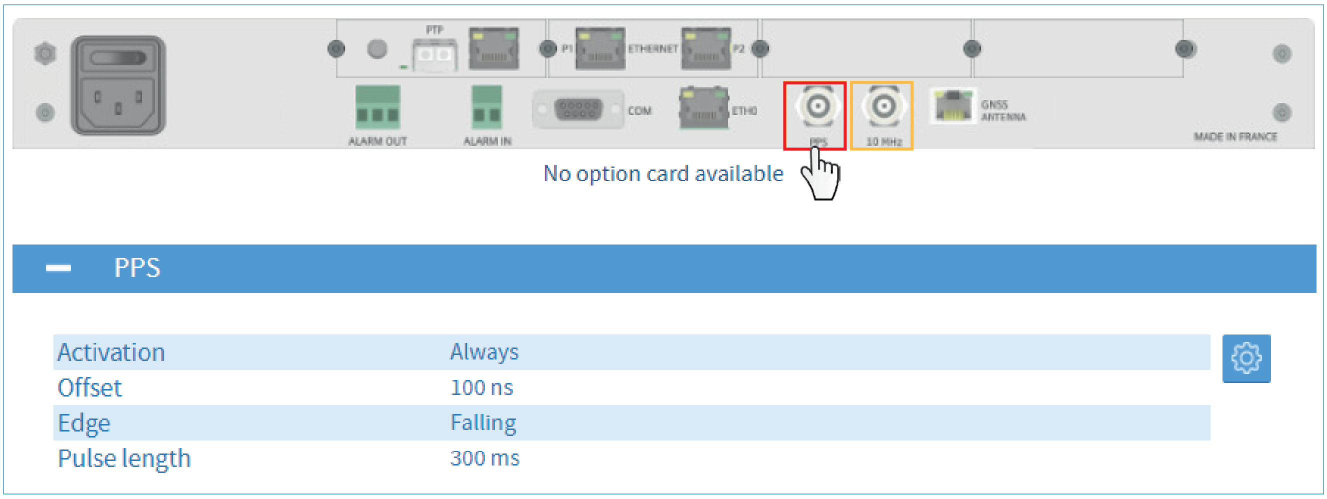
5 Choose the type of RS232/422/485 physical link:
- Output A
- Output B.

4.8 1PPS and 10 MHz outputs

4.8.1 1PPS output

The 1PPS output on the BNC connector emits one high-precision pulse per second.

1) TIME menu > Outputs > Mouse pointer on the 1PPS output:

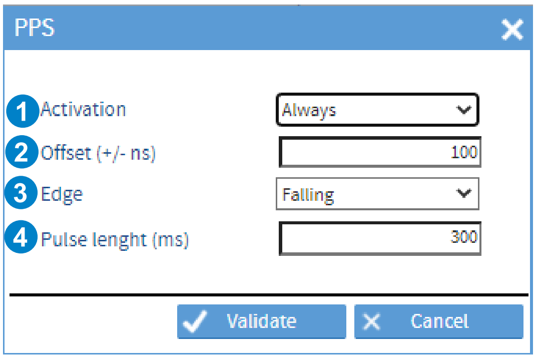


No option card available

PPS

Activation	Always
Offset	100 ns
Edge	Falling
Pulse length	300 ms

To set up the 1PPS output, click on ⚙. The following window is displayed:



PPS

1 Activation: Always

2 Offset (+/- ns): 100

3 Edge: Falling

4 Pulse lenght (ms): 300

1 Activation: - Always (by default)
- Sync or Holdover
- Sync
- Never

2 Offset (+ /-ns): enter the value manually between -500 000 000 and 500 000 000 (default value: 100 ns) An offset on the 1PPS output has no impact on the PTP master synchronisation.

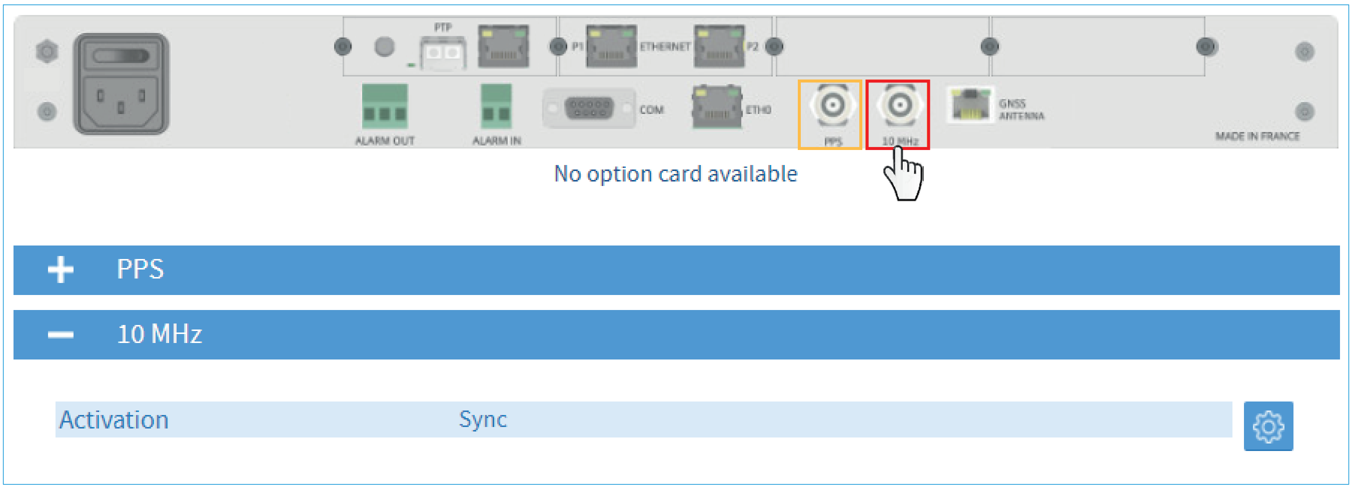
3 Edge: - Falling
- Rising

4 Pulse duration (ms): enter the value manually between 1 and 800 (default value: 300 ms).

4.8.2 10 MHz output

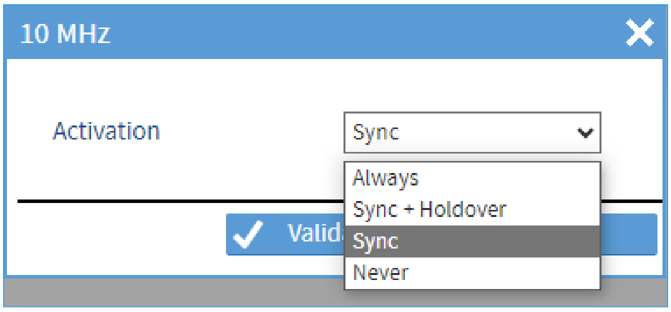
The 10 MHz output on the BNC connector emits a 10 MHz sinusoidal signal. The 1PPS output and the 10 MHz output are linked.

1) TIME menu > Outputs > Mouse pointer on the 10 MHz output:



Activation Sync

Click on ⚙ to set up the 10 MHz output. The following window opens:



Activation: Sync

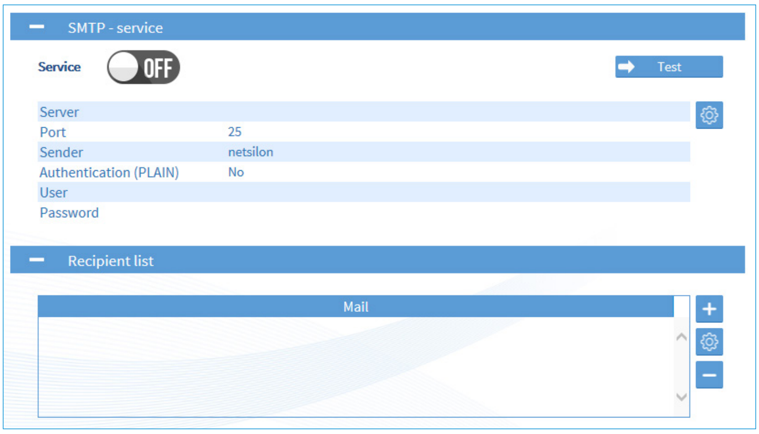
- Always
- Sync + Holdover
- Sync
- Never

Activation: - Always
- Sync or Holdover
- Sync (by default)
- Never

4.9 Management of notifications

4.9.1. SMTP configuration

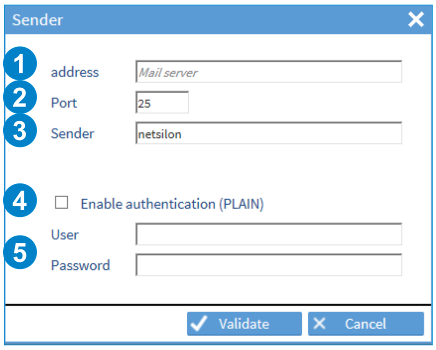
To register an SMTP server in order to send emails, follow these steps:
1) NOTIFICATION menu > SMTP:



Server	
Port	25
Sender	netsilon
Authentication (PLAIN)	No
User	
Password	

Click on ➡ Test to test the service directly (without having to generate a fault on the device).

2) In SMTP - service, click on ⚙, and the following window will appear:



address Mail server
Port 25
Sender netsilon
☐ Enable authentication (PLAIN)
User
Password

1 Enter the IP address of the receiving server (50 characters max.)

2 Enter the communication port. Port: 5 digits (65535 max.).

3 Enter the name of the sender of the emails. i.e the name given to Netsilon.

4 Check the box to enable authentication (Plain type).

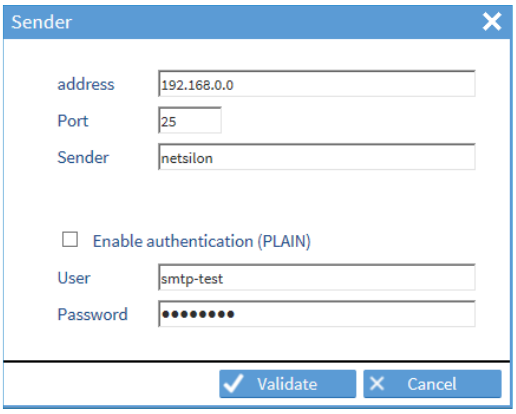
5 Enter user parameters (user / password: 50 characters max).

Refer to the next page to see a configuration example.

Configuration example:

1) Enter the sender’s parameters:

SMTP SERVER		
IP address of the SMTP server	192.168.1.254	
Port:	**25**	
Users	**e-mail**	**password**
Admin	admin@serveurtest.com	testservice
smtp-test	**smtp-test@serveurtest.com**	**testservice**
netsilon1	netsilon1@serveurtest.com	testservice



Sender

address 192.168.0.0

Port 25

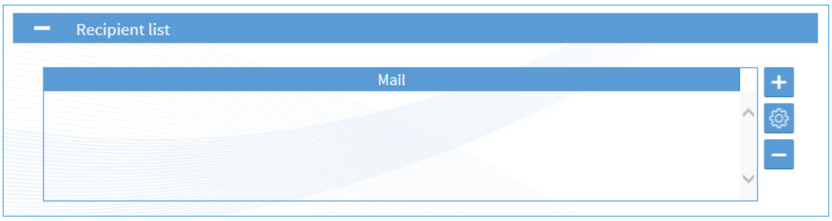
Sender netsilon

□ Enable authentication (PLAIN)

User smtp-test

Password ••••••••

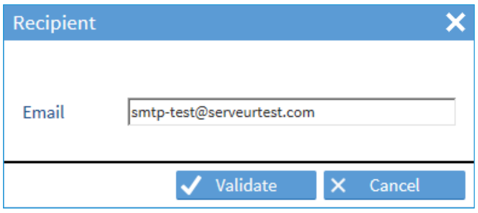
2) Enter the list of recipients:
(5 recipients max).



Recipient list

Mail

3) Click on + to add the e-mail address:
(50 characters max)



Recipient

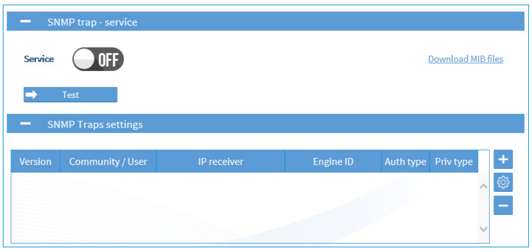
Email smtp-test@serveurtest.com

4) Enable the service using the ON button, then save.

4.9.2. SNMP trap configuration

To configure trap reception, follow these steps:

1) NOTIFICATION menu > SNMP Trap:



SNMP trap - service

Service OFF

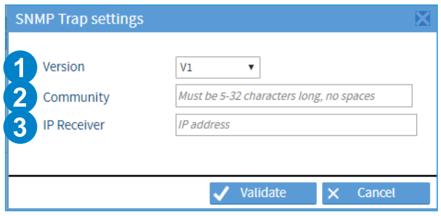
SNMP Traps settings

Version	Community / User	IP receiver	Engine ID	Auth type	Priv type

Click on Test to test the service directly (without having to generate a fault on the device).

Version V1 or V2C:
(5 accounts maximum)

2) Click on +, the following window will appear:



SNMP Trap settings

1 Version V1

2 Community *Must be 5-32 characters long, no spaces*

3 IP Receiver *IP address*

① Select the supported SNMP version: V1, V2C or V3.

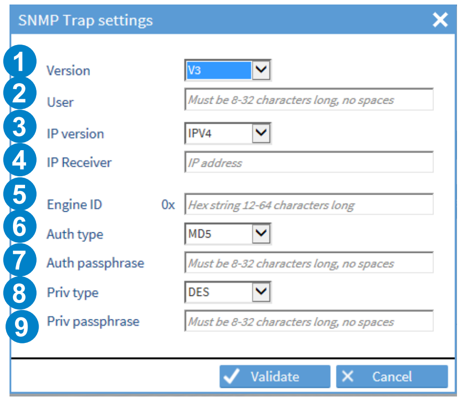
② Enter a community name between 5 and 32 characters with no spaces.

③ Enter the IP address of the trap destination server.

3) Click on ✓ Validate .

4) Enable the service using the ON button, then save.

Version V3:
(5 accounts maximum)



SNMP Trap settings ✕

① Version		V3
② User		Must be 8-32 characters long, no spaces
③ IP version		IPV4
④ IP Receiver		IP address
⑤ Engine ID	0x	Hex string 12-64 characters long
⑥ Auth type		MD5
⑦ Auth passphrase		Must be 8-32 characters long, no spaces
⑧ Priv type		DES
⑨ Priv passphrase		Must be 8-32 characters long, no spaces

① ③ ④ Please refer to the previous screenshot.

② Enter the name of the user (between 8 and 32 characters with no spaces).

⑤ Enter the ID of the SNMP engine.

⑥ Select the type of authentication (MD5 or SHA) or no authentication (NoAuth).

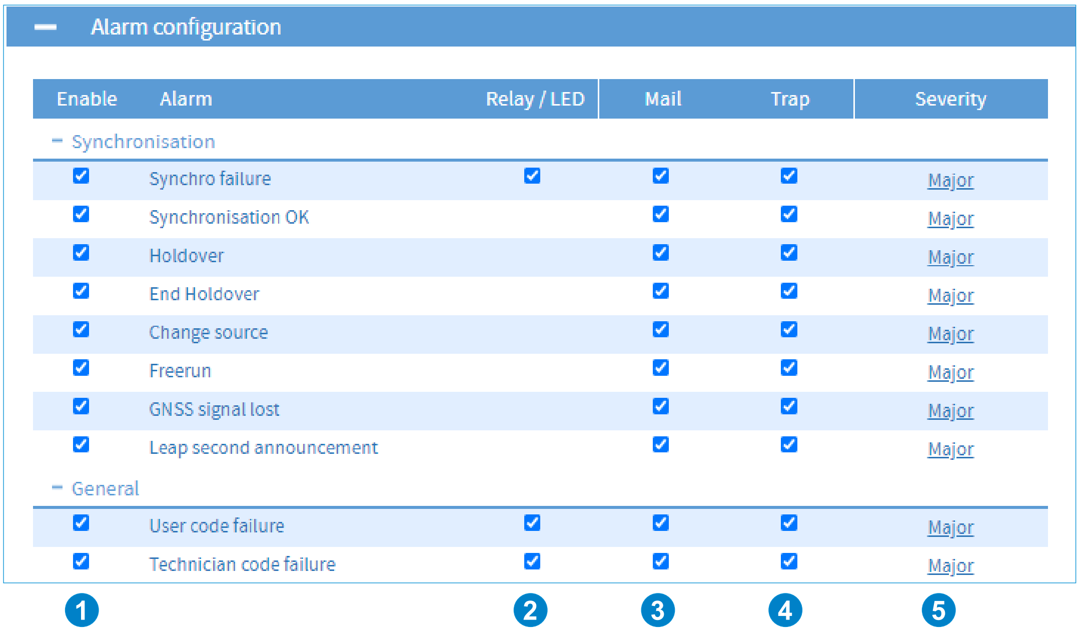
⑦ Enter the authentication passphrase (between 8 and 32 characters with no spaces).

⑧ Select the encryption type (DES or AES128) or no encryption (NoPriv).

⑨ Enter the encryption passphrase (between 8 and 32 characters with no spaces).

4.9.3. Configuration of alarms

To define the notification mode and criticality of alarms, follow these steps:
1) NOTIFICATION menu > alarms:



− Alarm configuration

Enable	Alarm	Relay / LED	Mail	Trap	Severity
	− Synchronisation				
☑	Synchro failure	☑	☑	☑	Major
☑	Synchronisation OK		☑	☑	Major
☑	Holdover		☑	☑	Major
☑	End Holdover		☑	☑	Major
☑	Change source		☑	☑	Major
☑	Freerun		☑	☑	Major
☑	GNSS signal lost		☑	☑	Major
☑	Leap second announcement		☑	☑	Major
	− General				
☑	User code failure	☑	☑	☑	Major
☑	Technician code failure	☑	☑	☑	Major

1 Check the box to enable alarm selection.

2 Check the box for the alarm to be identified by the LED on the front panel of Netsilon and notified via a relay contact.

3 Check the box for the alarm to be sent by e-mail (please refer to chapter **4.9.1 SMTP configuration**).

4 Check the box for the alarm to be sent in trap format (please refer to chapter **4.9.2 SNMP trap configuration**).

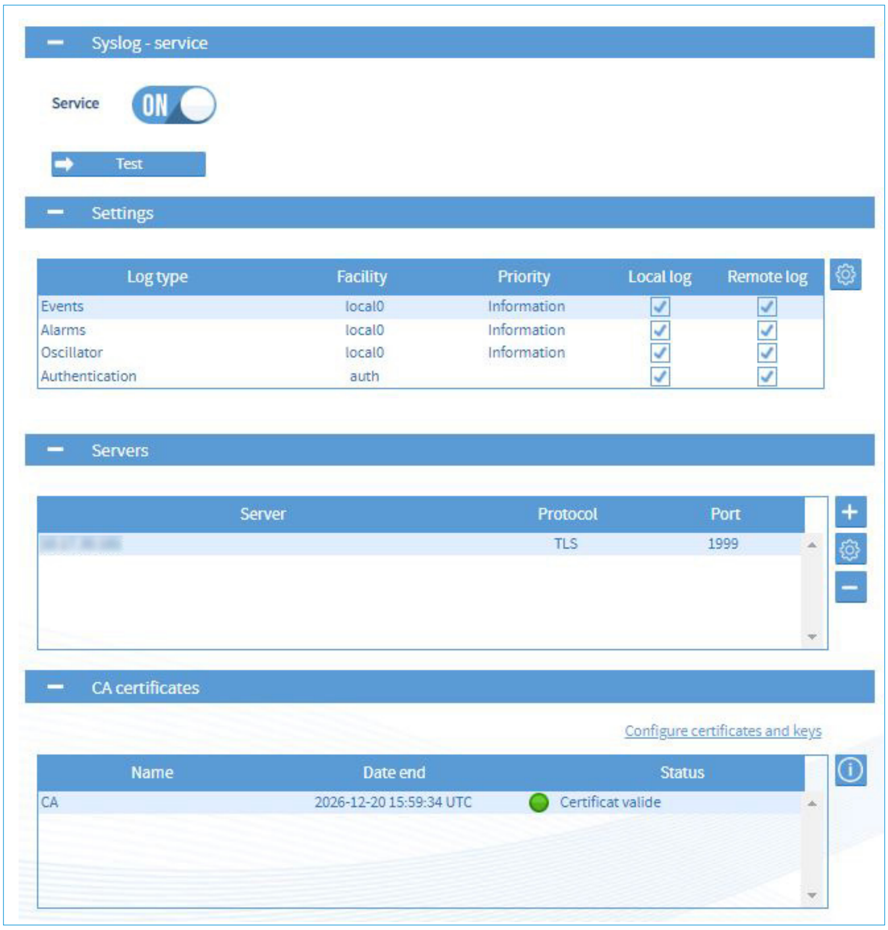
5 Choose the alarm criticality level: minor, major or critical.

Alarms are monitored and acknowledged in the history section, see chapter 4.12.9 Alarm history.

4.9.4. Syslog configuration

To configure the Syslog service, follow these steps:

1) NOTIFICATION menu > Syslog:
2) Enable the service using the ON button,



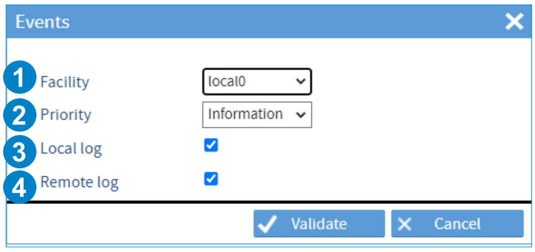
Log type	Facility	Priority	Local log	Remote log
Events	local0	Information	☑	☑
Alarms	local0	Information	☑	☑
Oscillator	local0	Information	☑	☑
Authentication	auth		☑	☑

Server	Protocol	Port
[redacted]	TLS	1999

Name	Date end	Status
CA	2026-12-20 15:59:34 UTC	● Certificat valide

Click on Test to test the service (a Syslog message is sent even if “Events” are not validated).

3) To configure each type of log (Events, Alarms, Oscillator, Authentication), select it and click on ⚙, the following window will appear:



1 Facility: local0
2 Priority: Information
3 Local log: ☑
4 Remote log: ☑

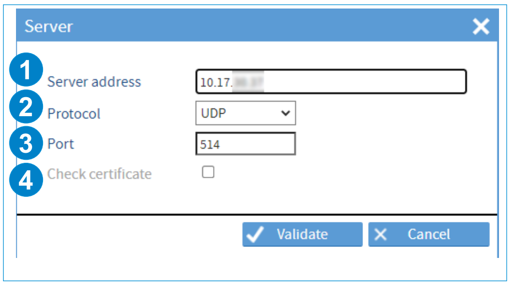
1 Choose a category for the type of message / system that caused the event (Free local use). For "Auth", the facility option is not adjustable since it is standardised by the Syslog protocol.

2 Choose the severity index of the message.

3 Check to enable log local storage.

4 Check to enable sending the log to a Syslog server. This server needs to be added.

4) Add a Syslog server by clicking on +, and the following window will appear:
(Possibility to add up to five servers maximum)



Server

1 Server address: 10.17.[redacted]

2 Protocol: UDP

3 Port: 514

4 Check certificate: □

1 Enter the address or the host name of the Syslog server.

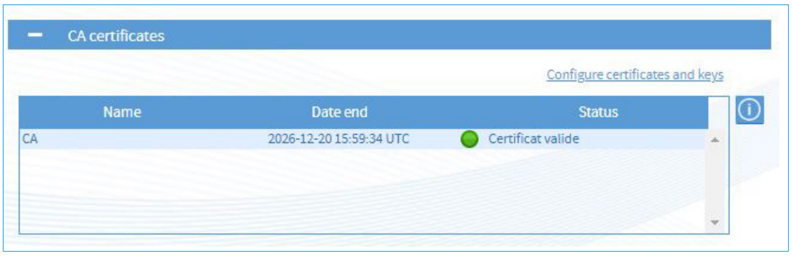
2 Choose the client/server communication protocol (UDP/TCP/TLS).

3 Enter the network port.

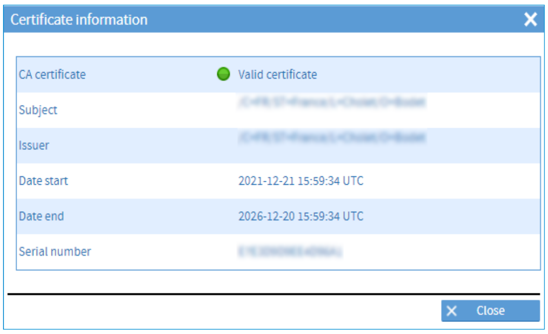
4 Enable certificate verification (TLS only).

Adding a certificate allows to generate an encryption and avoid a clear link.
Verification of the certificate allows the authenticity of the server to be checked.
To add a certificate, see chapter 4.10 Certificate and key management.

5) Click on ⓘ to view the certificate information that may have been imported from the certificate menu and on configure certificates and keys to access this menu.



Name	Date end	Status
CA	2026-12-20 15:59:34 UTC	● Certificat valide



Certificate information

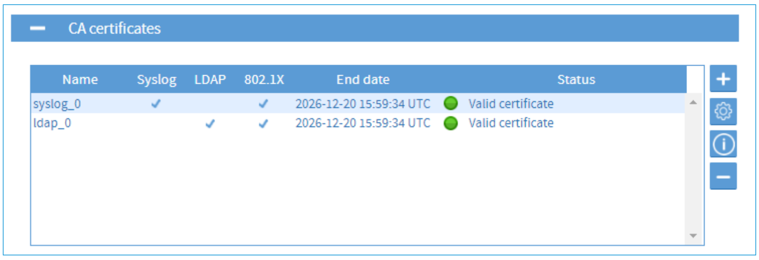
CA certificate	● Valid certificate
Subject	[redacted]
Issuer	[redacted]
Date start	2021-12-21 15:59:34 UTC
Date end	2026-12-20 15:59:34 UTC
Serial number	[redacted]

4.10 Certificate and key management

This menu allows importation of certificates and public keys in Netsilon.

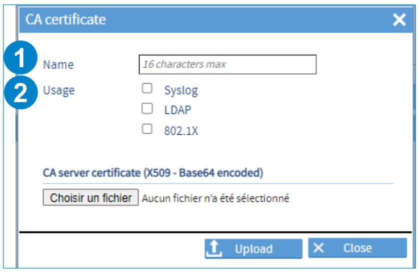
4.10.1. Importing CA certificates

To add CA certificates:
1) SECURITY menu > Certificates and keys > CA certificates



Name	Syslog	LDAP	802.1X	End date	Status
syslog_0	✓		✓	2026-12-20 15:59:34 UTC	● Valid certificate
ldap_0		✓	✓	2026-12-20 15:59:34 UTC	● Valid certificate

2) Click on +, a window opens:



Name: 16 characters max

Usage:
□ Syslog
□ LDAP
□ 802.1X

CA server certificate (X509 - Base64 encoded)

Choisir un fichier Aucun fichier n'a été sélectionné

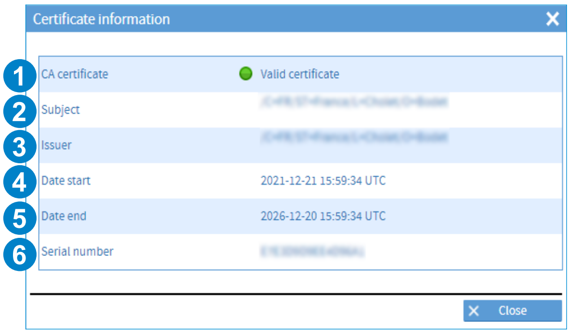
1 Enter a certificate name (16 characters maximum).

2 Select the use cases of the certificate: Syslog, LDAP, 802.1x (TLS, TTLS, PEAP).

3) Select the certificate and click on Upload to import it.

The certificates must be in X.509 Base64 format. As a reminder, an X.509 format certificate begins with «---BEGIN CERTIFICATE---» and ends with «---END CERTIFICATE---».
The number of CA certificates is limited to 40.
A maximum of 5 CA certificates can be assigned for the Syslog service and 5 CA certificates for the LDAP service. The same CA certificate cannot be added twice.

4) Click on ⓘ to see the information of the imported certificate:



CA certificate	● Valid certificate
Subject	[redacted]
Issuer	[redacted]
Date start	2021-12-21 15:59:34 UTC
Date end	2026-12-20 15:59:34 UTC
Serial number	[redacted]

1 Validity of the certificate.

2 CSR author (Certificate Signing Request).

3 Certificate issuer (Certification authority).

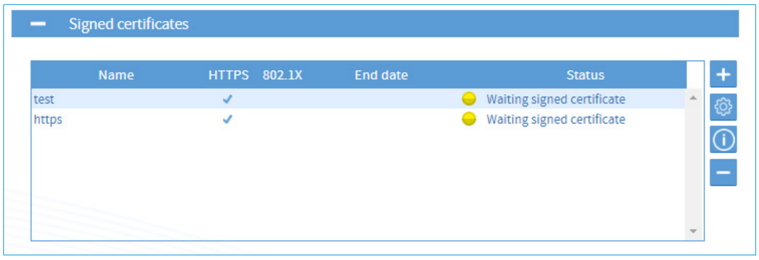
4 Start date of validity of the certificate.

5 End date of validity of the certificate.

6 Serial number of the certificate.

4.10.2. Importing signed certificates

To add signed certificates:
1) SECURITY menu > Certificates and keys > Signed certificates

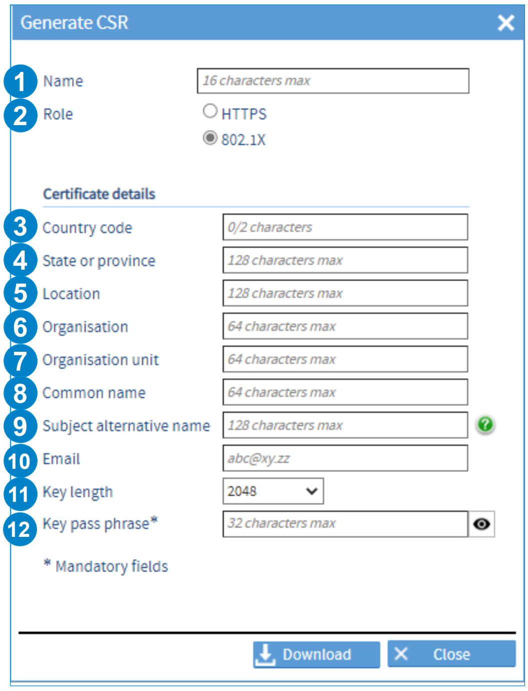


− Signed certificates

Name	HTTPS	802.1X	End date	Status
test	✓			● Waiting signed certificate
https	✓			● Waiting signed certificate

To import signed certificates, a Certificate Signing Request (CSR) is required beforehand. This CSR must be signed by the Certification Authority. Then, the signed certificate can be imported into Netsilon. It is not possible to import a private key directly. It is recommended to consult the Certification Authority to find out which fields are required in the X509 certificate request.

2) Click on + to generate a CSR, a window opens:



Generate CSR

1 Name: 16 characters max
2 Role: ○ HTTPS ● 802.1X

Certificate details

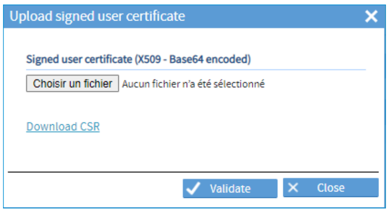
3 Country code: 0/2 characters
4 State or province: 128 characters max
5 Location: 128 characters max
6 Organisation: 64 characters max
7 Organisation unit: 64 characters max
8 Common name: 64 characters max
9 Subject alternative name: 128 characters max
10 Email: abc@xy.zz
11 Key length: 2048
12 Key pass phrase*: 32 characters max

* Mandatory fields

1. Enter a name for the CSR (16 characters maximum, a-z, A-Z, 0-9).
2. Select the use case of the signed certificate requested from the Certification Authority.
3. Enter your country code (2 characters maximum, a-z, A-Z, 0-9). See: https://www.ssl.com/country-codes/
4. Enter your state or province (128 characters maximum, a-z, A-Z, 0-9, space).
5. Enter your location (128 characters maximum, a-z, A-Z, 0-9, space).
6. Enter the legal name of your organisation (64 characters maximum, a-z, A-Z, 0-9, space).
7. Enter the name of your organisation unit (64 characters maximum, a-z, A-Z, 0-9, space).
8. Enter the full name (FQDN) of the domain to be secured (64 characters maximum, a-z, A-Z, 0-9, space, _.+@*:,-).
9. Enter alternative domain names to be secured (128 characters maximum, a-z, A-Z, 0-9, space, _.+@*:,-)
10. Enter a contact email address (128 characters maximum, a-z, A-Z, 0-9, _.+@-).
11. Select the private key length (1024, 2048 or 4096 bits).
12. Enter a mandatory private key protection password for 802.1x (From 5 up to 32 characters maximum, a-z, A-Z, 0-9, _.:#*?@+!-/).

3) Click on Download to download the CSR to be sent to the Certification Authority for signature. It is recommended to check the content of the CSR / X509 certificate request generated and if necessary, to apply a template when signing in order to meet internal constraints.

4) Import into Netsilon the signed certificate corresponding to the CSR issued by click on ⚙, a window opens:



Upload signed user certificate

Signed user certificate (X509 - Base64 encoded)

Choisir un fichier Aucun fichier n'a été sélectionné

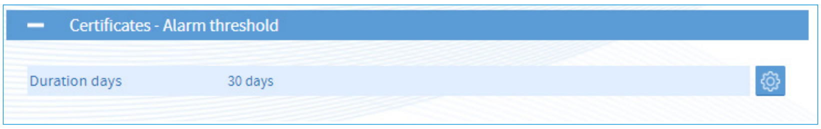
Download CSR

The certificates must be in X.509 Base64 format. As a reminder, a X.509 format certificate begins with «---BEGIN CERTIFICATE---» and ends with «---END CERTIFICATE---».
The number of signed certificates is limited to 20.

5) Click on ⓘ to see the information of the imported certificate.

4.10.3. Certificate expiration (CA and signed certificates)

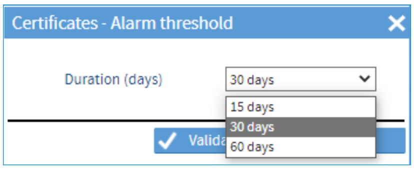
It is possible to set an alarm to inform of upcoming certificate expiry.
1) NOTIFICATION menu > Alarms > Certificates - Alarm threshold



Certificates - Alarm threshold

Duration days 30 days

2) Click on ⚙, a window opens:



Certificates - Alarm threshold

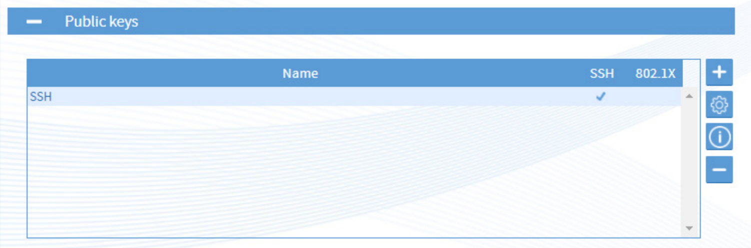
Duration (days): 30 days

- 15 days
- 30 days
- 60 days

3) Select the time before which the certificate expires for an alarm to be displayed.

4.10.4. Importing public keys

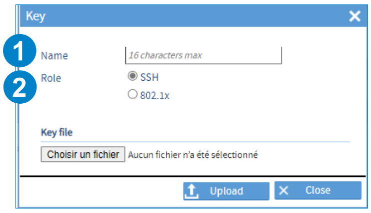
To add public keys:
1) SECURITY menu > Certificates and keys > Public keys



Public keys

Name	SSH	802.1X
SSH	✓	

2) Click on + to add a public key, a window opens:



Key

Name: *16 characters max*

Role: ● SSH ○ 802.1x

Key file

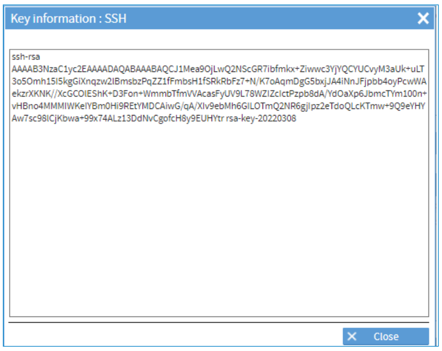
Choisir un fichier Aucun fichier n'a été sélectionné

1 Enter the public key name.

2 Select the use case of the public key.

3) Select the key and click on Upload to import it.

4) Click on ⓘ to see the imported key:



Key information : SSH

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCJ1Mea9OjLwQ2NScGR7ibfmkx+Ziwwc3YjYQCYUCvyM3aUk+uLT
3o5Omh15I5kgGiXnqzw2lBmsbzPqZZ1fFmbsH1fSRkRbFz7+N/K7oAqmDgG5bxjJA4iNnJFjpbb4oyPcwWA
ekzrXKNK//XcGCOIEShK+D3Fon+WmmbTfmVVAcasFyUV9L78WZIZcIctPzpb8dA/YdOaXp6JbmcTYm100n+
vHBno4MMMIWKeIYBm0Hi9REtYMDCAiwG/qA/XIv9ebMh6GILOTmQ2NR6gjIpz2eTdoQLcKTmw+9Q9eYHY
Aw7sc98ICjKbwa+99x74ALz13DdNvCgofcH8y9EUHYtr rsa-key-20220308
```

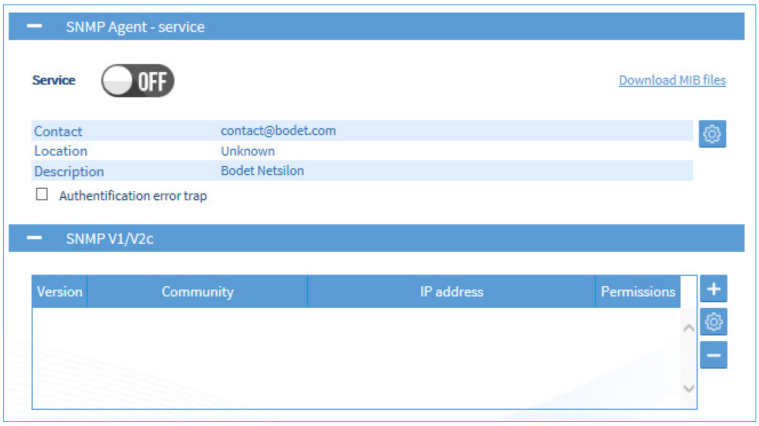
The number of keys is limited to 20.

4.11 System supervision

4.11.1. SNMP agent

› ENABLING THE SNMP AGENT (EXAMPLE V1)

1) SECURITY menu > SNMP agent:



SNMP Agent - service

Service OFF

Download MIB files

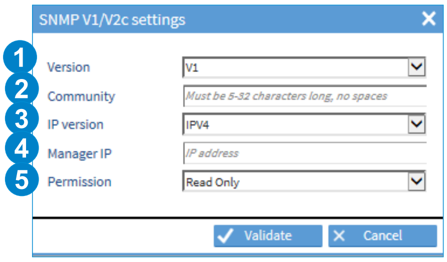
Contact contact@bodet.com
Location Unknown
Description Bodet Netsilon

□ Authentification error trap

SNMP V1/V2c

Version	Community	IP address	Permissions

2) Click on +, the following window will appear:



SNMP V1/V2c settings

1 Version: V1
2 Community: Must be 5-32 characters long, no spaces
3 IP version: IPV4
4 Manager IP: IP address
5 Permission: Read Only

1 Select the SNMP version.

2 Enter a community name between 5 and 32 characters with no spaces.

3 Choose the IP communication version: IPV4.

4 Enter the IP address of the server.

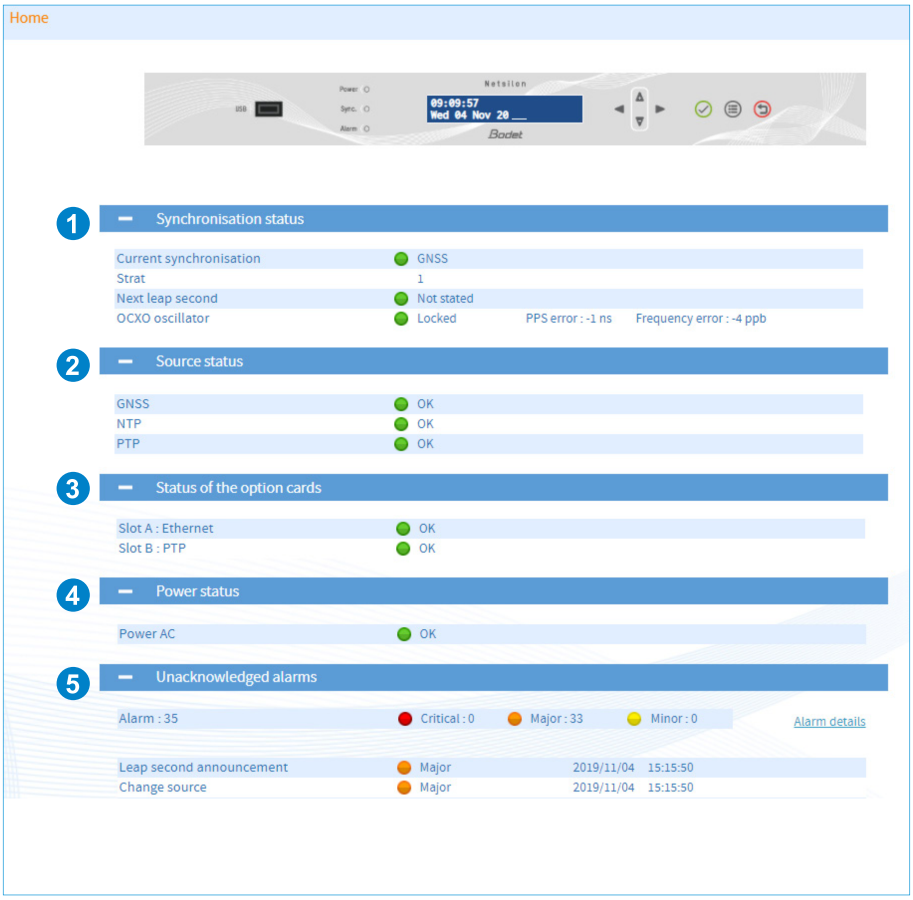
5 Choose the permission: read only or read/write.

3) Enable the service using the ON button, then save.

4.12 System monitoring

4.12.1 Homepage

The homepage is a consultation page:



Synchronisation status

Current synchronisation	● GNSS		
Strat	1		
Next leap second	● Not stated		
OCXO oscillator	● Locked	PPS error : -1 ns	Frequency error : -4 ppb

Source status

GNSS	● OK
NTP	● OK
PTP	● OK

Status of the option cards

Slot A : Ethernet	● OK
Slot B : PTP	● OK

Power status

Power AC	● OK

Unacknowledged alarms

Alarm : 35	● Critical : 0	● Major : 33	● Minor : 0	Alarm details

Leap second announcement	● Major	2019/11/04	15:15:50
Change source	● Major	2019/11/04	15:15:50

1 This menu displays the current synchronisation status:

- The current synchronisation status and the synchronisation source used:
  - Green = synchronisation OK
  - Red = no synchronisation.
- The stratum level: level in relation to the synchronisation source (satellite).
- Announcement of the next leap second.
- Oscillator status: Locked / Tracking / Holdover / Freerun.

2 This menu shows the status of the synchronisation sources:

- The name of the source and its status.

This list is dynamic and depends on the number of existing outputs on the product.

3 This menu displays the status of the outputs:

- The name of the output and its status.

This list is dynamic and depends on the number of existing outputs on the product.

4 This menu displays the power supply status:

- The name of the power supply (AC power supply, DC power supply, AC+DC power supply, AC+AC power supply) with a colour for the status:
  - Green: power supply OK.
  - Red: (in the case of a dual power supply) = error in one of the power supplies.

This list is dynamic and depends on the number of existing power supplies on the product.

5 This menu displays the list of alarms requiring acknowledgement from the user.

- The link provides alarm details (History > Alarms).
- The name of the alarm, its status (major or minor), the date and UTC time.

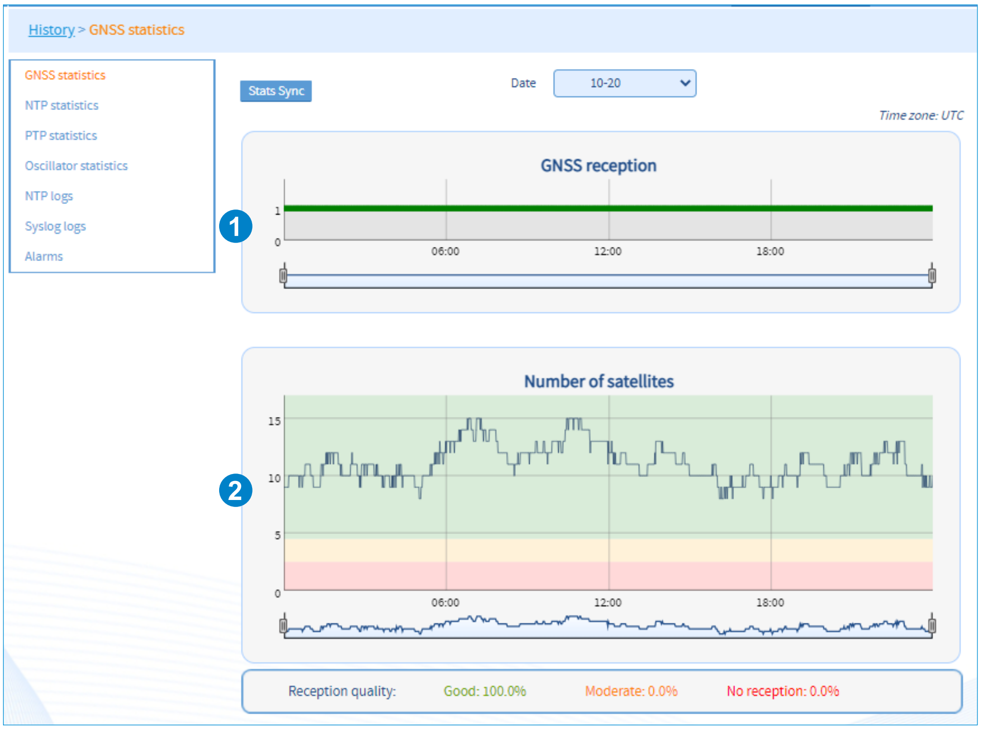
This list is dynamic and depends on the alarms notified.

4.12.2. GNSS statistics

To see the Netsilon GNSS synchronisation statistics, follow these steps:

1) HISTORY menu > GNSS statistics

2) Select the date using the drop-down menu:



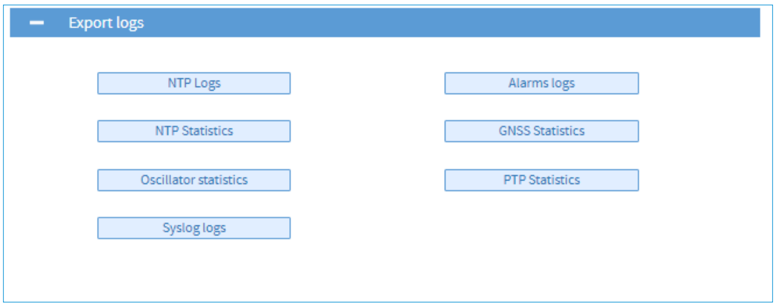
1 The status of the GNSS reception is symbolised by two status levels:

- 0: GPS reception frame but no synchronisation (waiting period to check if the source is reliable).
- 1: GPS frame reception.

2 Graph showing the number of satellites detected according to the time. Three colours indicate the quality of signal reception:

- Red: 0 to 2 satellites - no reception or poor reception quality.
- Orange: 2 to 4 satellites - moderate reception quality.
- Green: 4 to 12 and more satellites - good reception quality.

These statistics can be exported. To do so, open “Export logs” and click on GNSS Statistics.

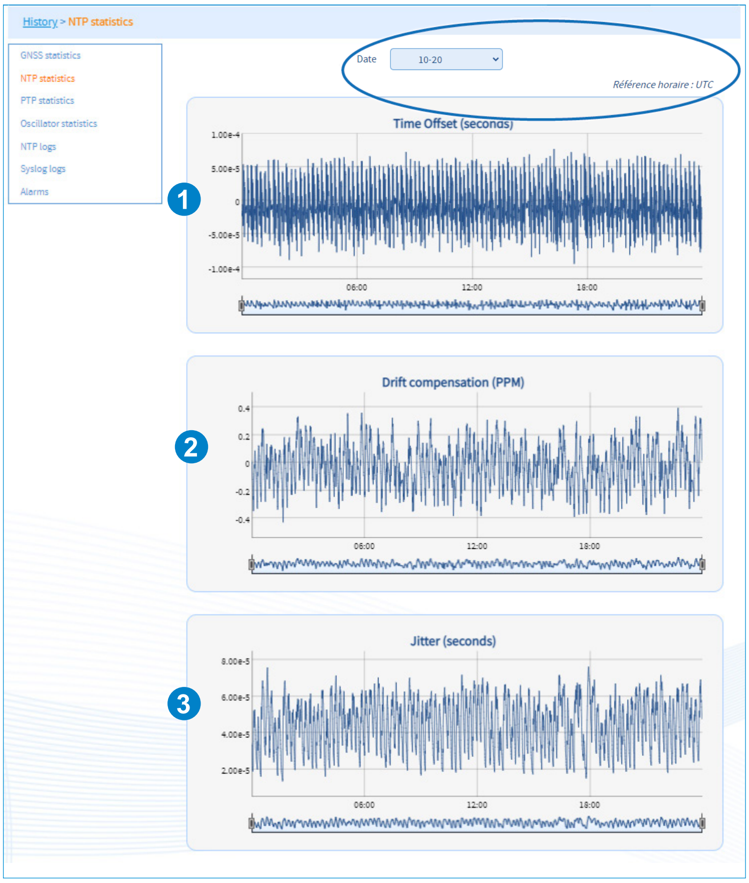


4.12.3. NTP statistics

To see Netsilon NTP synchronisation statistics, follow these steps:

1) HISTORY menu > NTP statistics

2) Select the date using the “Date” drop-down menu:



Date 10-20

Référence horaire : UTC

1 Time offset: time offset in relation to the reference synchronisation source.

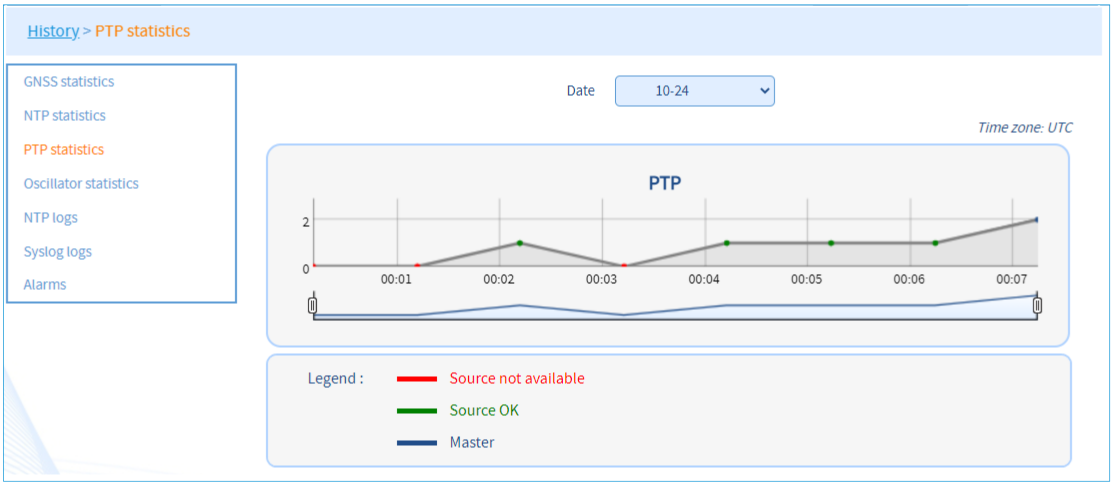
2 Drift compensation: gradual correction of the Netsilon oscillator in relation to the source. The idea is to move closer to the synchronisation source in a gradual manner (without any time jump).

3 Jitter: offset of the source around the reference.

4.12.4. PTP statistics

To see Netsilon PTP statistics, follow these steps:

1) HISTORY menu > PTP statistics



Date 10-24

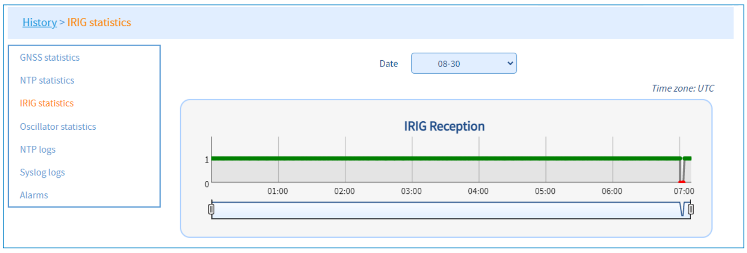
Time zone: UTC

Legend :
🟥 Source not available
🟩 Source OK
■ Master

4.12.5. IRIG statistics

To see Netsilon IRIG synchronisation statistics, follow these steps:

1) HISTORY menu > IRIG statistics



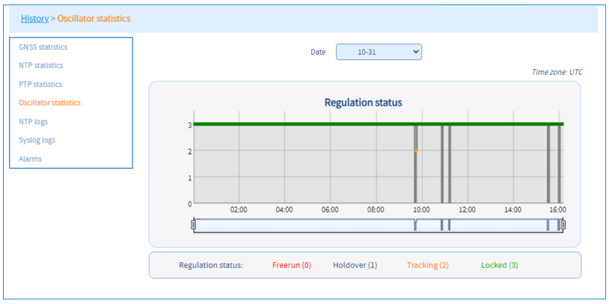
Date 08-30

Time zone: UTC

4.12.6. Oscillator statistics

To see the Netsilon oscillator statistics, follow these steps;

1) HISTORY menu > Oscillator statistics



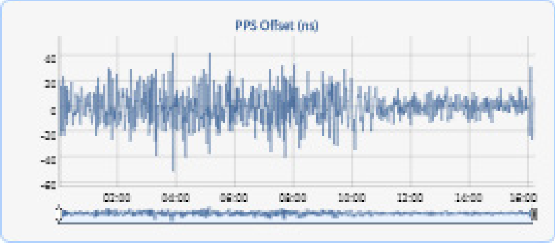
Date 10-31

Time zone: UTC

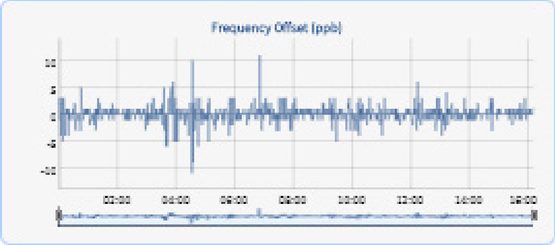
Regulation status: Freerun (0) Holdover (1) Tracking (2) Locked (3)

When the product starts up, the oscillator is in Freerun status (as if it had never been slaved). Then, it searches for the PPS signal to slave itself and switches to the Tracking status (tracking the PPS signal). Once it has been successfully slaved to the PPS, the oscillator locks on this signal (Locked status). If the PPS signal is lost, it switches to the Holdover status, then to the Freerun status when its own time zone is not longer reliable enough.

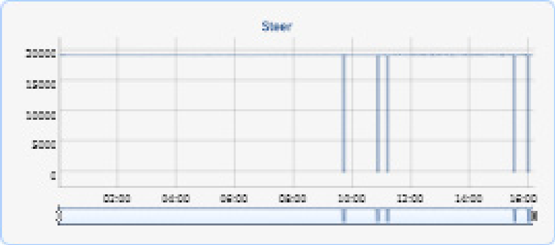
1PPS error in ns.
(PPS_Out in comparison to
the reference 1PPS)



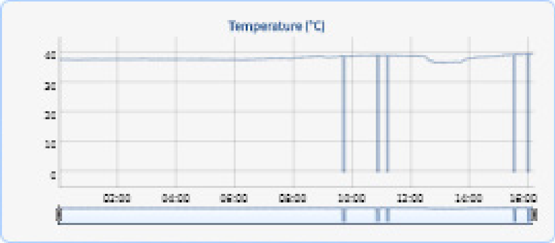
Oscillator frequency
error in ppb



Correction applied
to the oscillator

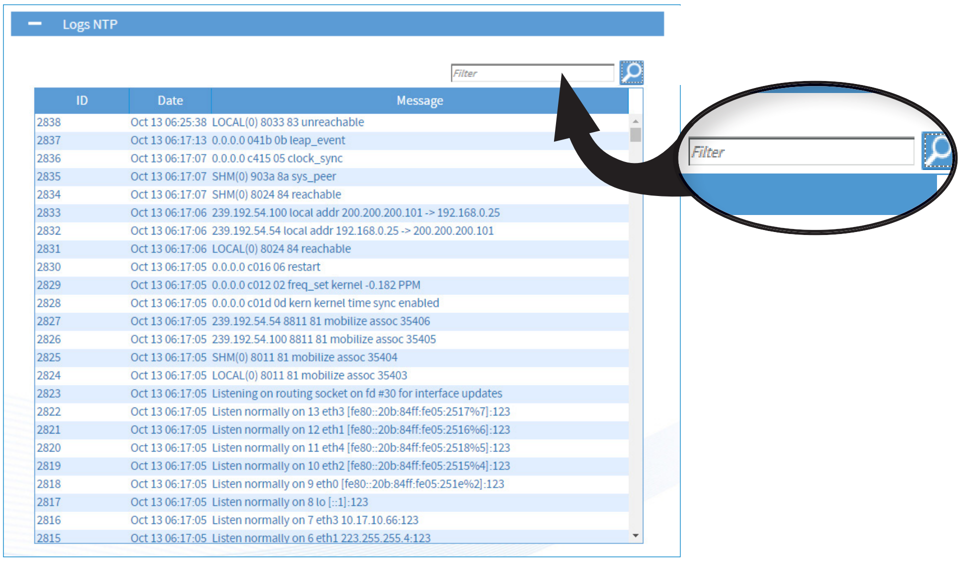


Ambient temperature
of the oscillator



4.12.7. NTP log

To see the Netsilon log records, proceed as follows:
1) HISTORY Menu > NTP logs:



ID	Date	Message
2838	Oct 13 06:25:38	LOCAL(0) 8033 83 unreachable
2837	Oct 13 06:17:13	0.0.0.0 041b 0b leap_event
2836	Oct 13 06:17:07	0.0.0.0 c415 05 clock_sync
2835	Oct 13 06:17:07	SHM(0) 903a 8a sys_peer
2834	Oct 13 06:17:07	SHM(0) 8024 84 reachable
2833	Oct 13 06:17:06	239.192.54.100 local addr 200.200.200.101 -> 192.168.0.25
2832	Oct 13 06:17:06	239.192.54.54 local addr 192.168.0.25 -> 200.200.200.101
2831	Oct 13 06:17:06	LOCAL(0) 8024 84 reachable
2830	Oct 13 06:17:05	0.0.0.0 c016 06 restart
2829	Oct 13 06:17:05	0.0.0.0 c012 02 freq_set kernel -0.182 PPM
2828	Oct 13 06:17:05	0.0.0.0 c01d 0d kern kernel time sync enabled
2827	Oct 13 06:17:05	239.192.54.54 8811 81 mobilize assoc 35406
2826	Oct 13 06:17:05	239.192.54.100 8811 81 mobilize assoc 35405
2825	Oct 13 06:17:05	SHM(0) 8011 81 mobilize assoc 35404
2824	Oct 13 06:17:05	LOCAL(0) 8011 81 mobilize assoc 35403
2823	Oct 13 06:17:05	Listening on routing socket on fd #30 for interface updates
2822	Oct 13 06:17:05	Listen normally on 13 eth3 [fe80::20b:84ff:fe05:2517%7]:123
2821	Oct 13 06:17:05	Listen normally on 12 eth1 [fe80::20b:84ff:fe05:2516%6]:123
2820	Oct 13 06:17:05	Listen normally on 11 eth4 [fe80::20b:84ff:fe05:2518%5]:123
2819	Oct 13 06:17:05	Listen normally on 10 eth2 [fe80::20b:84ff:fe05:2515%4]:123
2818	Oct 13 06:17:05	Listen normally on 9 eth0 [fe80::20b:84ff:fe05:251e%2]:123
2817	Oct 13 06:17:05	Listen normally on 8 lo [::1]:123
2816	Oct 13 06:17:05	Listen normally on 7 eth3 10.17.10.66:123
2815	Oct 13 06:17:05	Listen normally on 6 eth1 223.255.255.4:123

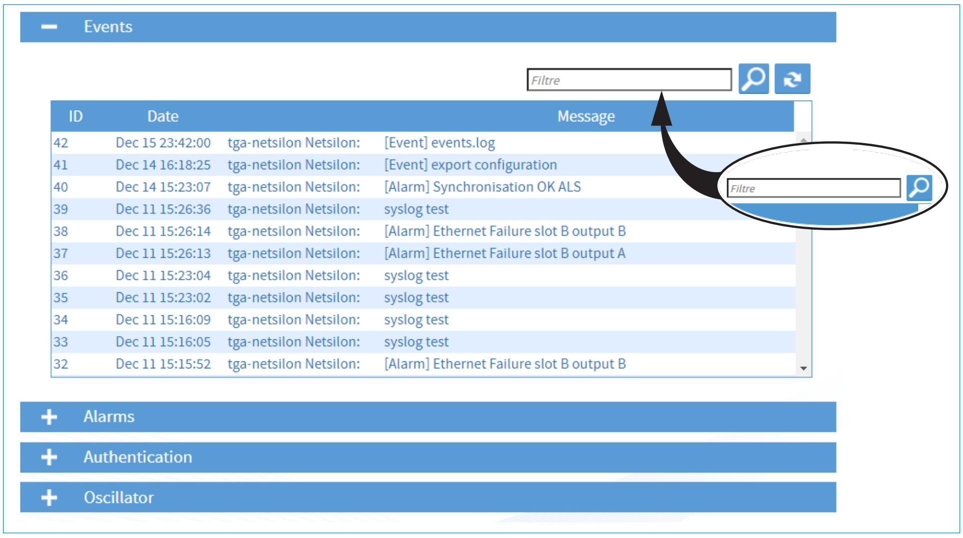
This log contains saved information. It is a standard log generated by the NTP protocol.

It is possible to perform a search on this log using the search bar.

4.12.8. Syslog log

To see the Syslog log, follow these steps:

1) HISTORY Menu > Syslog logs



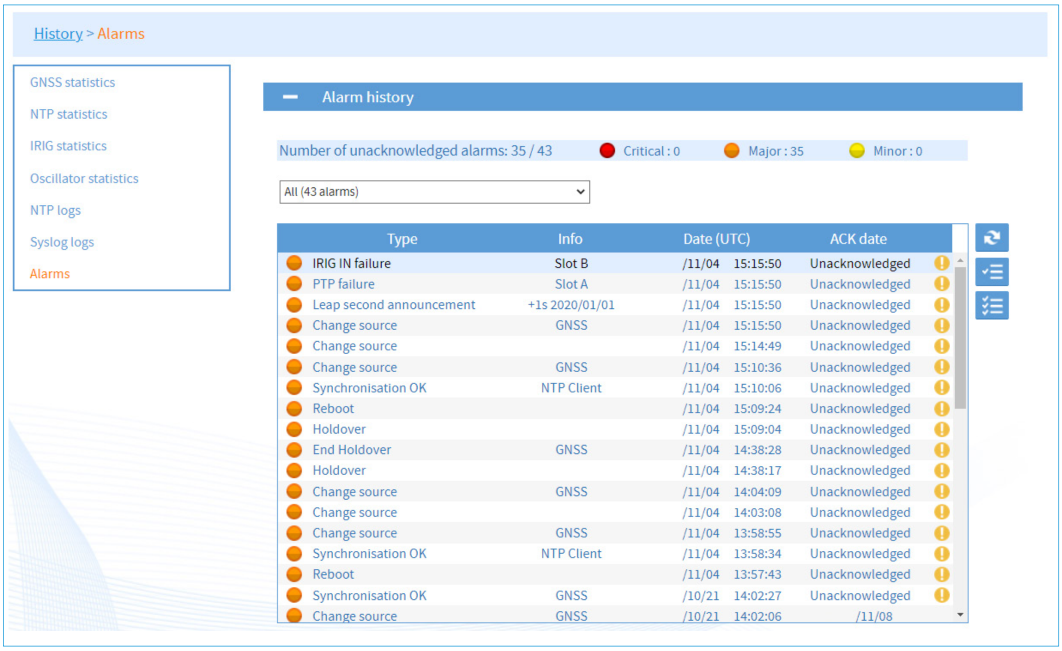
ID	Date		Message
42	Dec 15 23:42:00	tga-netsilon Netsilon:	[Event] events.log
41	Dec 14 16:18:25	tga-netsilon Netsilon:	[Event] export configuration
40	Dec 14 15:23:07	tga-netsilon Netsilon:	[Alarm] Synchronisation OK ALS
39	Dec 11 15:26:36	tga-netsilon Netsilon:	syslog test
38	Dec 11 15:26:14	tga-netsilon Netsilon:	[Alarm] Ethernet Failure slot B output B
37	Dec 11 15:26:13	tga-netsilon Netsilon:	[Alarm] Ethernet Failure slot B output A
36	Dec 11 15:23:04	tga-netsilon Netsilon:	syslog test
35	Dec 11 15:23:02	tga-netsilon Netsilon:	syslog test
34	Dec 11 15:16:09	tga-netsilon Netsilon:	syslog test
33	Dec 11 15:16:05	tga-netsilon Netsilon:	syslog test
32	Dec 11 15:15:52	tga-netsilon Netsilon:	[Alarm] Ethernet Failure slot B output B

This log reports all the information for each type of log. It is a standard log generated by the Syslog protocol.

It is possible to perform a search on this log using the search bar.

4.12.9. Alarm history

To see the history of alarms and acknowledge them, follow these steps:
1) HISTORY menu > Alarms:

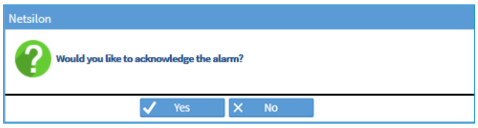


Number of unacknowledged alarms: 35 / 43 ● Critical : 0 ● Major : 35 ● Minor : 0

All (43 alarms)

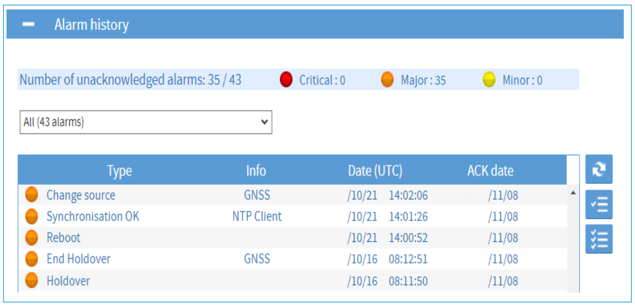
	Type	Info	Date (UTC)		ACK date	
●	IRIG IN failure	Slot B	/11/04	15:15:50	Unacknowledged	!
●	PTP failure	Slot A	/11/04	15:15:50	Unacknowledged	!
●	Leap second announcement	+1s 2020/01/01	/11/04	15:15:50	Unacknowledged	!
●	Change source	GNSS	/11/04	15:15:50	Unacknowledged	!
●	Change source		/11/04	15:14:49	Unacknowledged	!
●	Change source	GNSS	/11/04	15:10:36	Unacknowledged	!
●	Synchronisation OK	NTP Client	/11/04	15:10:06	Unacknowledged	!
●	Reboot		/11/04	15:09:24	Unacknowledged	!
●	Holdover		/11/04	15:09:04	Unacknowledged	!
●	End Holdover	GNSS	/11/04	14:38:28	Unacknowledged	!
●	Holdover		/11/04	14:38:17	Unacknowledged	!
●	Change source	GNSS	/11/04	14:04:09	Unacknowledged	!
●	Change source		/11/04	14:03:08	Unacknowledged	!
●	Change source	GNSS	/11/04	13:58:55	Unacknowledged	!
●	Synchronisation OK	NTP Client	/11/04	13:58:34	Unacknowledged	!
●	Reboot		/11/04	13:57:43	Unacknowledged	!
●	Synchronisation OK	GNSS	/10/21	14:02:27	Unacknowledged	!
●	Change source	GNSS	/10/21	14:02:06	/11/08	

- To refresh this list, click on ↻.
- There are two ways to acknowledge the alarms:
  - individually by selecting the alarm to be acknowledged and clicking on ✓☰.
  - all alarms at once by clicking on ☑☰.
- Confirm by clicking on “Yes”



Would you like to acknowledge the alarm?

Once acknowledged, the exclamation mark ! disappears from the relevant alarm line. :



Number of unacknowledged alarms: 35 / 43 ● Critical : 0 ● Major : 35 ● Minor : 0

All (43 alarms)

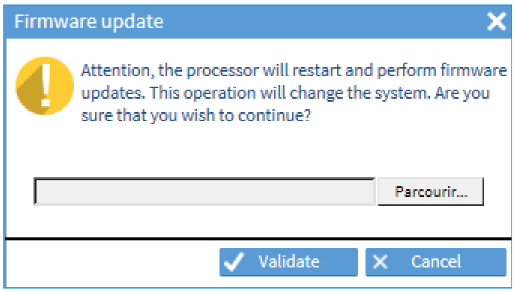
	Type	Info	Date (UTC)		ACK date
●	Change source	GNSS	/10/21	14:02:06	/11/08
●	Synchronisation OK	NTP Client	/10/21	14:01:26	/11/08
●	Reboot		/10/21	14:00:52	/11/08
●	End Holdover	GNSS	/10/16	08:12:51	/11/08
●	Holdover		/10/16	08:11:50	/11/08

The Reboot alarm is sent approx. 10 seconds after the reboot to allow time for the network to be set up.

4.13 System tools

4.13.1. Firmware update

To update the Netsilon firmware, follow these steps:
1) SYSTEM menu > Tools > Update and backup.
2) Click on Update firmware, and the following window will appear to select the file to import:


Firmware update

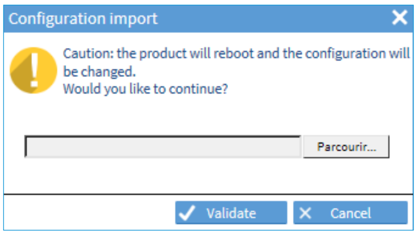
Attention, the processor will restart and perform firmware updates. This operation will change the system. Are you sure that you wish to continue?

The latest version of the firmware is available at www.bodet-time.com

4.13.2. Loading and saving a configuration

To save a configuration, follow these steps:
1) SYSTEM menu > Tools > Update and backup.
2) Click on Save configuration, a file named «export.nets» will download to your PC.

To load a configuration, follow these steps:
1) SYSTEM menu > Tools > Update and backup.
2) Click on Upload configuration, and the following window will appear to select the file to import:


Configuration import

Caution: the product will reboot and the configuration will be changed.
Would you like to continue?

The file to be imported must have a "FileName.nets" extension.

Why saving a configuration?
Exporting a configuration allows you to save the various parameters defined in Netsilon.

During any reconfiguration of Netsilon, you can simply import the saved file to retrieve all the settings previously configured.

Saving a configuration allows you to save precious time when restoring the system.

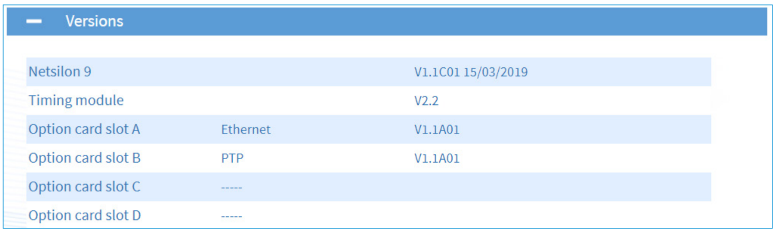
Having previously saved your Netsilon configuration means it is no longer necessary to configure it manually and follow the steps to obtain the same configuration.

To see the saved settings, please refer to Annex 4: saved settings.

4.13.3. Firmware version and online help

To see the firmware version of Netsilon and the option cards, proceed as follows:

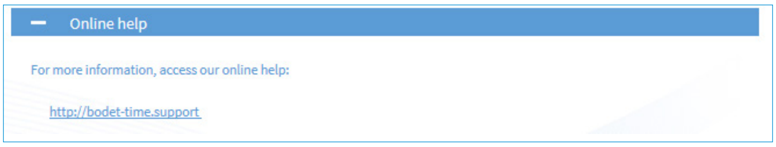
1) SYSTEM menu > General > Versions:



Netsilon 9		V1.1C01 15/03/2019
Timing module		V2.2
Option card slot A	Ethernet	V1.1A01
Option card slot B	PTP	V1.1A01
Option card slot C	-----	
Option card slot D	-----	

To access the product user manual, proceed as follows:

1) SYSTEM menu > General > Online help:



For more information, access our online help:

http://bodet-time.support

4.13.4. Firewall

Netsilon has an onboard firewall whose configuration changes automatically in line with the services confirmed by the client. Therefore, there is no configuration at client level.

Only the ports corresponding to the activated services are open.

Pings are authorised but are limited to protect against ICMP flood attacks (request saturation). SSH connections are authorised (if enabled) but are limited to protect against brute force attacks (testing all possible password combinations).

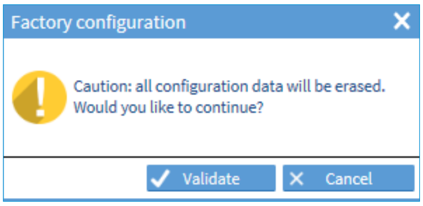
4.13.5. Factory configuration

To reset Netsilon to factory configuration, follow these steps:

1) SYSTEM menu > Tools > Update and backup.

2) Click on Factory configuration , and the following window will appear:

All configurations will be lost in the event of a factory configuration reset.



Caution: all configuration data will be erased.
Would you like to continue?

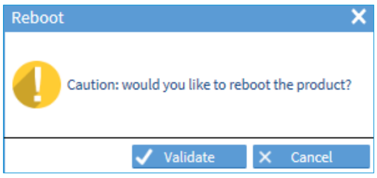
The link to the web server will be broken because the IP address is lost: it is necessary to reconfigure the network settings to access the web server (refer to chapter **3. Commissioning** and perform the operations described).

4.13.6. Restarting or switching off Netsilon

To restart Netsilon, follow these steps:

1) SYSTEM menu > Tools > Restart.

2) Click on Restart , and the window opposite will appear:

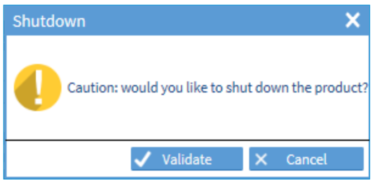


Caution: would you like to reboot the product?

To switch off Netsilon, follow these steps:

1) SYSTEM menu > Tools > Restart.

2) Click on Shut down , and the window opposite will appear:



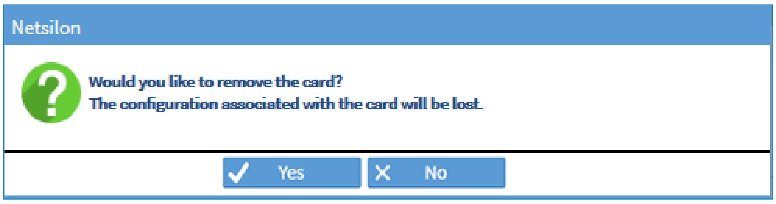
Caution: would you like to shut down the product?

The product is switched off, but the power supply is still on: the green POWER LED is on and the LCD screen remains in standby mode.

4.13.7. Removing an option card

If an option card is physically removed from Netsilon, it must also be removed from the web server so as not to generate false alarms.

To remove an option card from the Netsilon software, follow these steps:
1) SYSTEM menu > Tools > Option cards.
2) Select the option card to be removed.
3) Click on −, and the following window will appear:



Would you like to remove the card?
The configuration associated with the card will be lost.

If this removal is performed while the option card is still present, it will be re-detected when the user returns to this menu.

4.13.8. Exporting logs and statistics

To export Netsilon logs and statistics, follow these steps:
1) SYSTEM menu > Tools > Export logs.
2) Click on the log or the type of statistics, and a ZIP folder containing the log file will be downloaded to the PC.

5. CONFIGURATION BY SSH

> To access the SSH online command set interface, follow these steps (Netsilon must be connected to the network via its ETH0 port) :

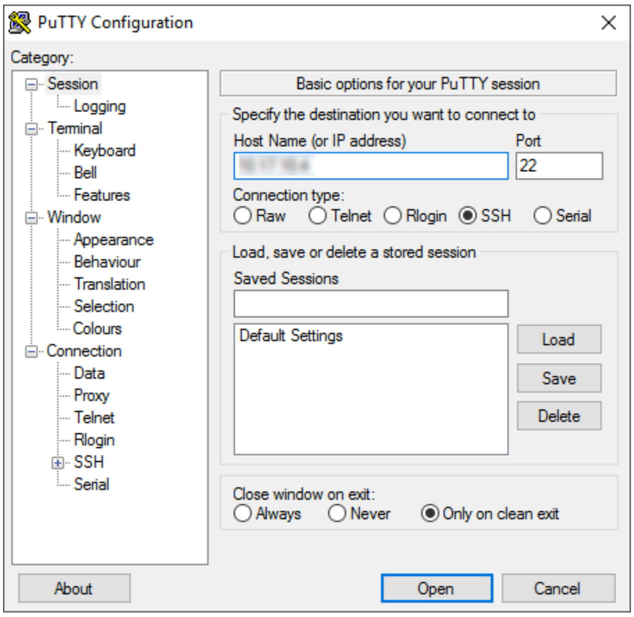
5.1 Authentication by password

1) Download a program enabling you to log into Netsilon remotely (e.g.: PuTTY).

2) Provide the Netsilon IP address.

3) Open the program (PuTTY).

4) Enter the IP address.



Specify the destination you want to connect to

Host Name (or IP address): [redacted]

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

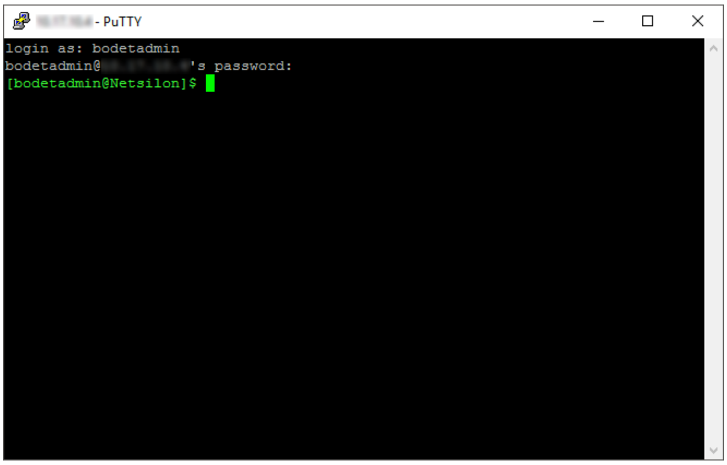
Saved Sessions:

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

5) Enter the default ID and password to access the command set. As a reminder:

- > ID: bodetadmin
- > Password: admin49



[redacted] - PuTTY

```
login as: bodetadmin
bodetadmin@[redacted]'s password:
[bodetadmin@Netsilon]$
```

> For more information on the product and the list of online commands (via the ETH0 port): SYSTEM > General > Online help

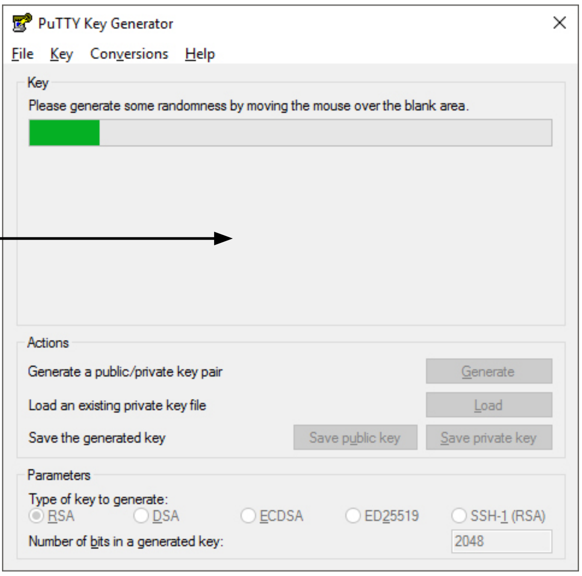
To access the list of command sets, see Annex 5: list of command sets

5.2 Authentication by public key

1) Download a program that will generate public/private keys (e.g.: PuTTY Key Generator).

2) Generate a public/private key by clicking on Generate :

Hover your PC mouse over this space to generate the key



Key

Please generate some randomness by moving the mouse over the blank area.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

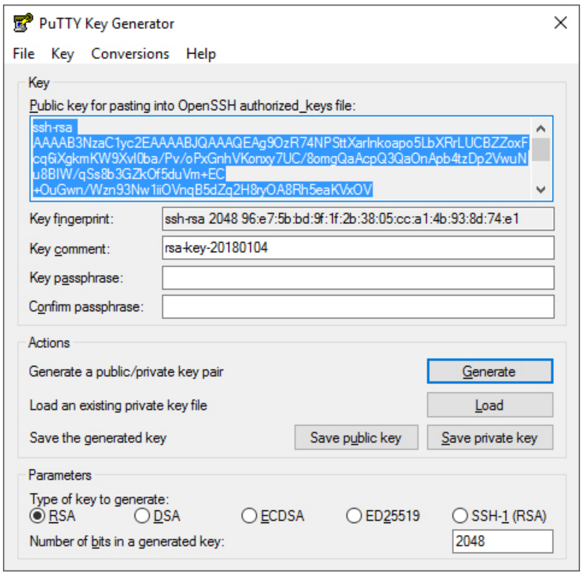
Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

3) Save the public key in a file (.txt type) to be imported in the Certificates and keys menu of Netsilon in the "public keys" tab:

The public key must start with "SSH-" and begin on the first line of the file.
The file must contain only the public key.

Copy the PuTTY generator key in a file



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAg9OzR74NPSttXarlnkoapo5LbXRrLUCBZZoxF
cq6iXgkmKW9Xvl0ba/Pv/oPxGnhVKonxy7UC/8omgQaAcpQ3QaOnApb4tzDp2VwuN
u8BIW/qSs8b3GZkOf5duVm+EC
+OuGwn/Wzn93Nw1iiOVnqB5dZq2H8ryOA8Rh5eaKVxOV
```

Key fingerprint: ssh-rsa 2048 96:e7:5b:bd:9f:1f:2b:38:05:cc:a1:4b:93:8d:74:e1

Key comment: rsa-key-20180104

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Load an existing private key file

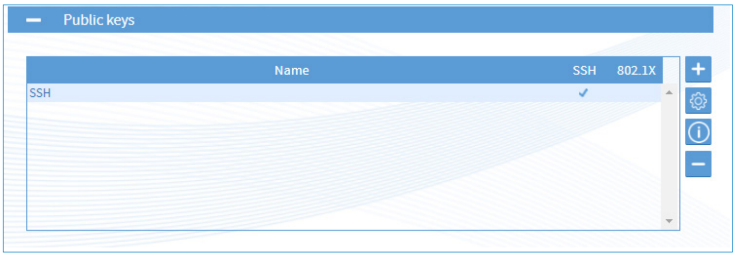
Save the generated key

Parameters

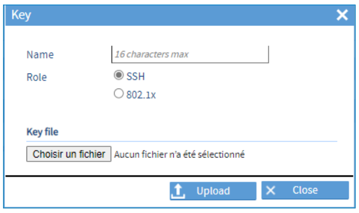
Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Import the public key in Netsilon



Name	SSH	802.1X
SSH	✓	

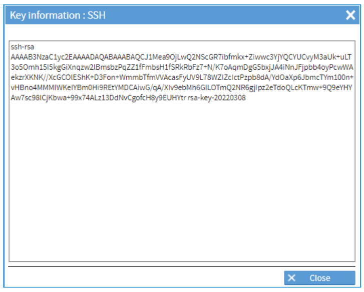


Name: 16 characters max

Role: ● SSH ○ 802.1x

Key file

Choisir un fichier Aucun fichier n'a été sélectionné



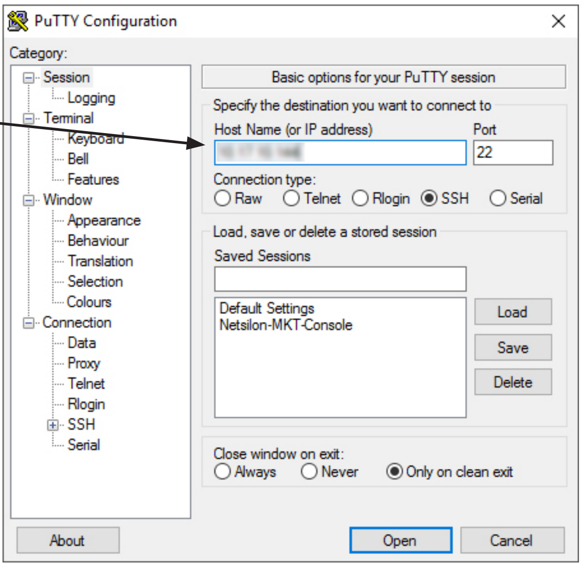
```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCJ1Mea9OjLwQ2NScGR7ibfmkx+Ziwwc3YjYQCYUCvyM3aUk+uLT
3o5Omh15I5kgGiXnqzw2lBmsbzPqZZ1fFmbsH1fSRkRbFz7+N/K7oAqmDgG5bxjJA4iNnJFjpbb4oyPcwWA
ekzrXKNK//XcGCOlEShK+D3Fon+WmmbTfmVVAcasFyUV9L78WZIZcIctPzpb8dA/YdOaXp6JbmcTYm100n+
vHBno4MMMIWKeIYBm0Hi9REtYMDCAiwG/qA/XIv9ebMh6GILOTmQ2NR6gjIpz2eTdoQLcKTmw+9Q9eYHY
Aw7sc98lCjKbwa+99x74ALz13DdNvCgofcH8y9EUHYtr rsa-key-20220308
```

4) Save the private key to your PC.

5) Download a program enabling the connection (e.g: PuTTY).

6) Open the program (PuTTY).

7) Enter the IP address of Netsilon:



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): [redacted]

Port: 22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

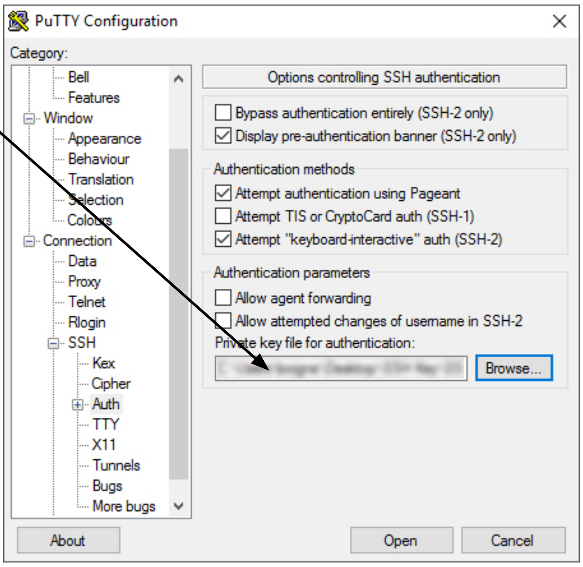
Load, save or delete a stored session

Saved Sessions

Default Settings
Netsilon-MKT-Console

Close window on exit:
○ Always ○ Never ● Only on clean exit

8) Enter the location on your PC containing the private key matching the public key imported to Netsilon:



Options controlling SSH authentication

□ Bypass authentication entirely (SSH-2 only)
☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

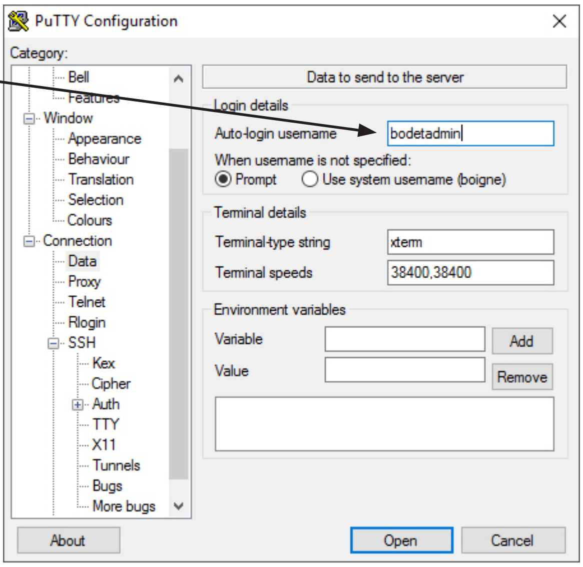
☑ Attempt authentication using Pageant
□ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

Private key file for authentication: [redacted]

9) Enter the user:



Data to send to the server

Login details

Auto-login username: bodetadmin

When username is not specified:
● Prompt ○ Use system username (boigne)

Terminal details

Terminal-type string: xterm

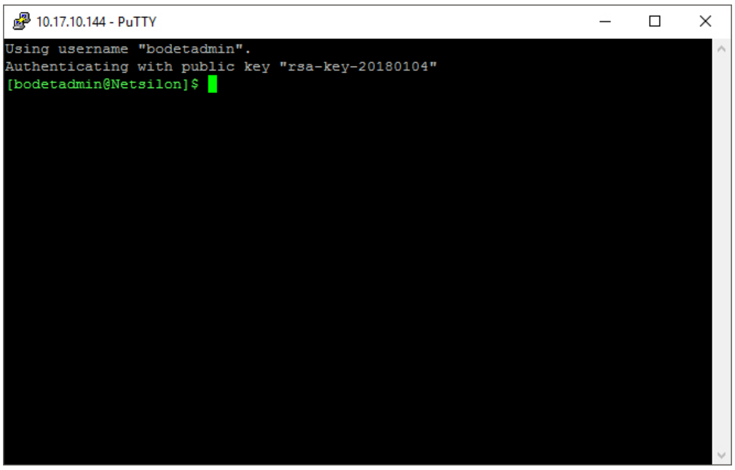
Terminal speeds: 38400,38400

Environment variables

Variable

Value

10) Click on Open the following window opens:



```
Using username "bodetadmin".
Authenticating with public key "rsa-key-20180104"
[bodetadmin@Netsilon]$
```

6. CONFIGURATION BY CONSOLE

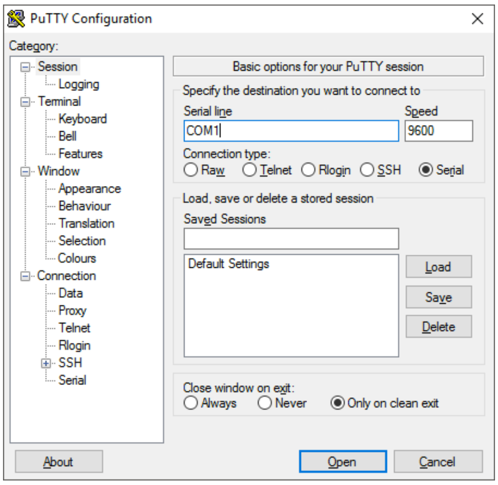
> To access the Netsilon web server, follow these steps (Netsilon must be connected to the PC via its COM serial port).

The physical connection between the PC and Netsilon must be provided by an RS232 (DB9) male/female serial cable.

1) Download a programm enabling you to log into Netsilon (e.g.: PuTTY).

2) Open the program (PuTTY).

3) Enter the communication port.



Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM1

Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

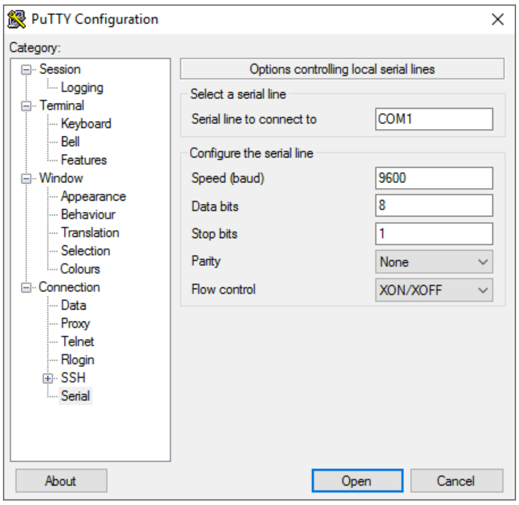
Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

4) Click on “Serial” to check the parameters of the ASCII RS-232 serial connection:
-9600 baud, 1 start bit, 8 data bits, 1 stop bit, no parity and no root login.



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud): 9600

Data bits: 8

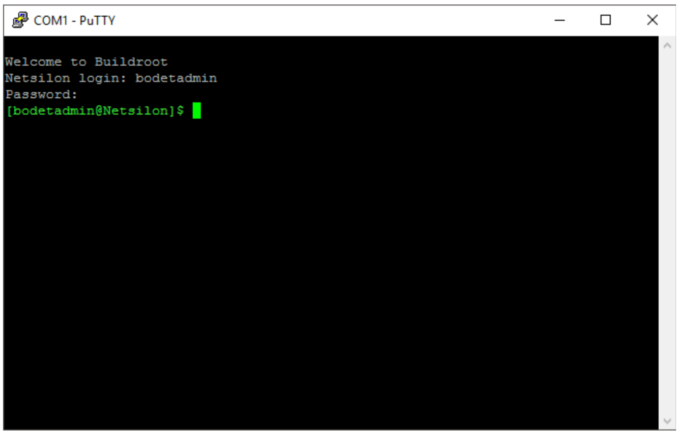
Stop bits: 1

Parity: None

Flow control: XON/XOFF

5) Enter the default ID and password to access the command set. As a reminder:

- ID: bodetadmin
- Password: admin49



```
Welcome to Buildroot
Netsilon login: bodetadmin
Password:
[bodetadmin@Netsilon]$
```

> For more information on the product and the list of online commands (via the COM port): SYSTEM > General > Online help

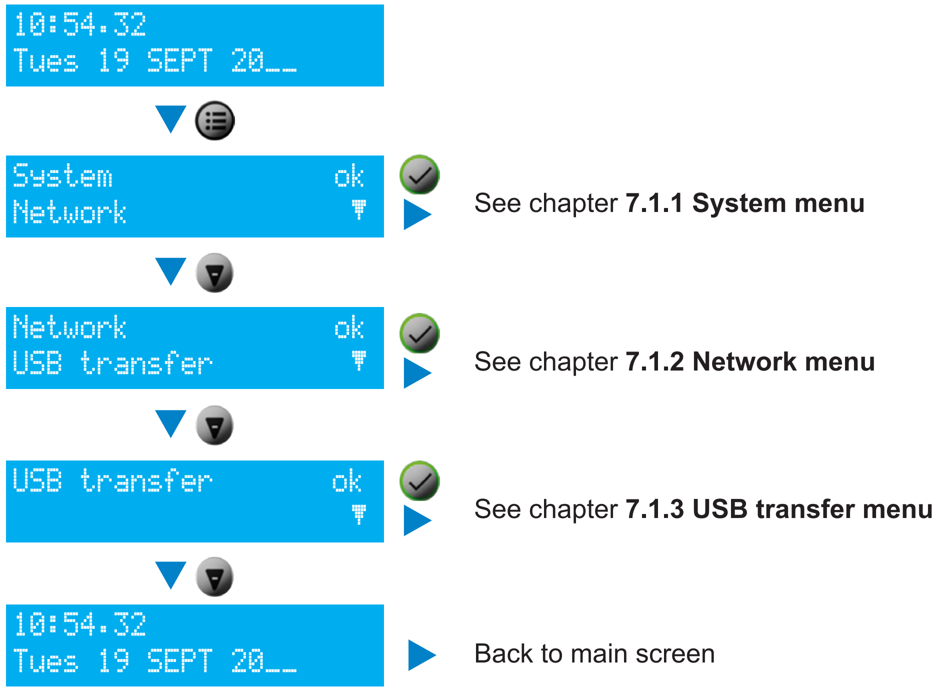
To access the list of command sets, see Annex 5: list of command sets.

7. CONFIGURATION BY CONTROL PANEL

7.1 Main menu tree

Configuration of menus via the control panel provides for basic settings.
Advanced settings are configured via the web server.

Menus are automatically closed after 45 seconds of inactivity on the control panel.



See chapter **7.1.1 System menu**

See chapter **7.1.2 Network menu**

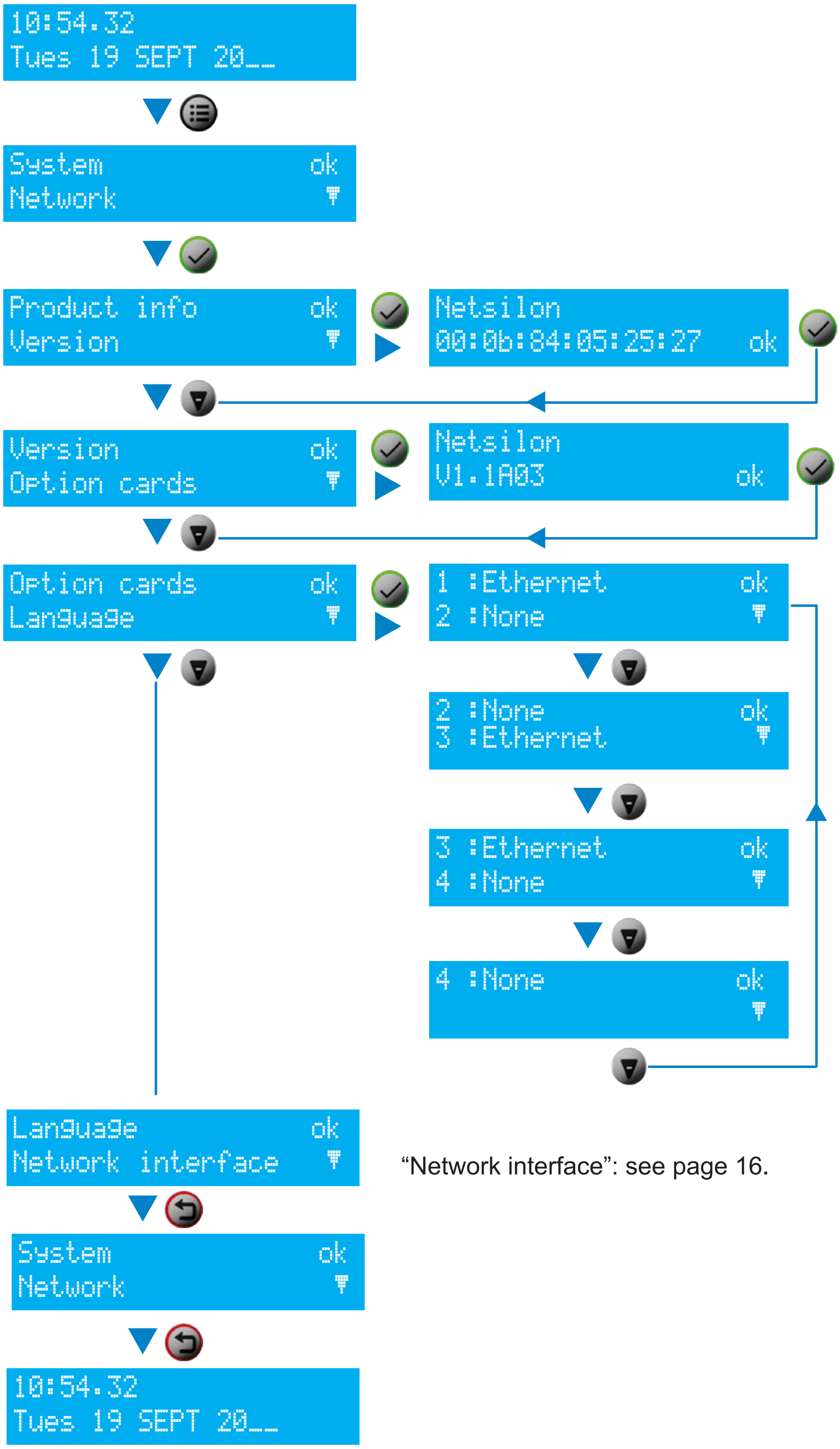
See chapter **7.1.3 USB transfer menu**

Back to main screen

7.1.1. System menu

This menu can be used to see the following parameters:

- the product's MAC address,
- the name of the product and its firmware version,
- the option card(s) installed,
- the language used for the menus displayed on the LCD screen.



Display of product name and its MAC address

Display of product name and its software version

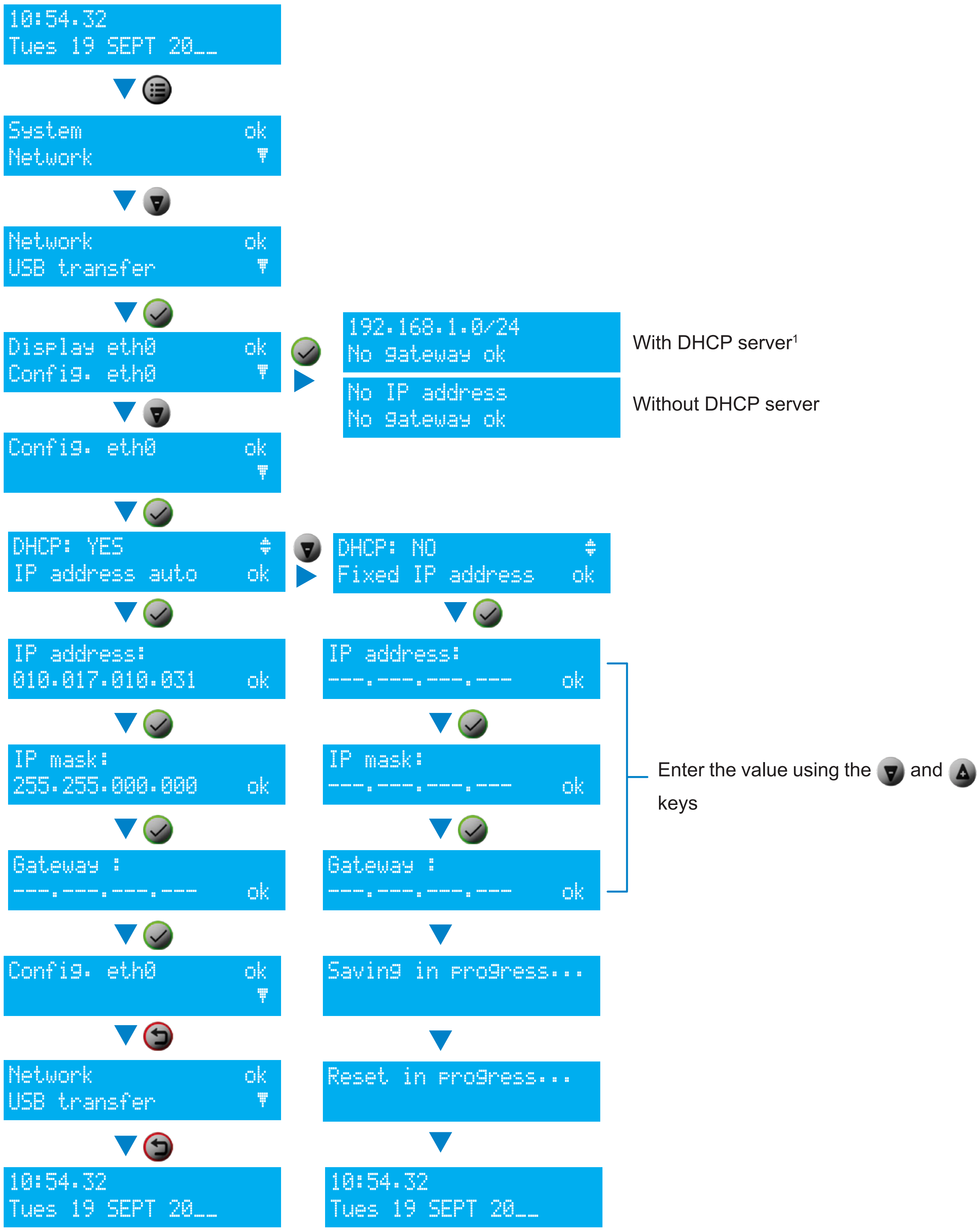
Display of option cards installed.

Netsilon can hold up to 4 option cards.

"Network interface": see page 16.

7.1.2. Network menu

This menu can be used to see, define and configure the parameters of the ETH0 network port only.



```
10:54.32
Tues 19 SEPT 20__
```

```
System          ok
Network         ▾
```

```
Network         ok
USB transfer    ▾
```

```
Display eth0    ok
Config. eth0    ▾
```

```
192.168.1.0/24
No gateway ok
```

With DHCP server[1]

```
No IP address
No gateway ok
```

Without DHCP server

```
Config. eth0    ok
                ▾
```

```
DHCP: YES            ⇕
IP address auto     ok
```

```
DHCP: NO             ⇕
Fixed IP address    ok
```

```
IP address:
010.017.010.031     ok
```

```
IP mask:
255.255.000.000     ok
```

```
Gateway :
---.---.---.---     ok
```

```
IP address:
---.---.---.---     ok
```

```
IP mask:
---.---.---.---     ok
```

```
Gateway :
---.---.---.---     ok
```

Enter the value using the ▼ and ▲ keys

```
Config. eth0    ok
                ▾
```

```
Network         ok
USB transfer    ▾
```

```
10:54.32
Tues 19 SEPT 20__
```

```
Saving in progress...
```

```
Reset in progress...
```

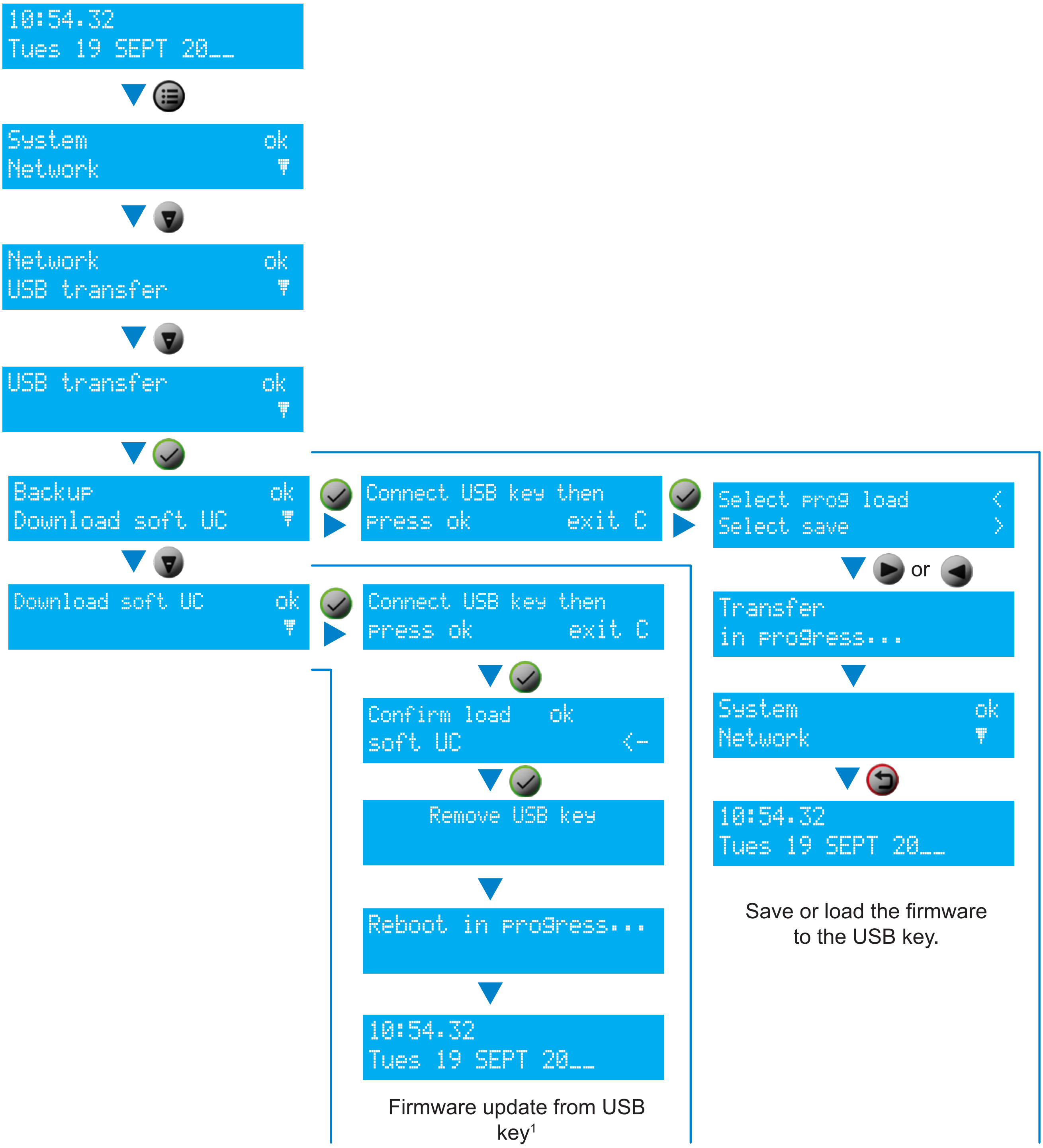
```
10:54.32
Tues 19 SEPT 20__
```

[1] *The IP address 192.168.1.0/24 and absence of gateway are given by way of example. Reminder: /24 is the CIDR addressing.*

7.1.3. USB transfer menu

The Netsilon time server can load or save its programming via a USB key.

Before creating any new programming, it is necessary to save the existing one on a USB key.



10:54.32
Tues 19 SEPT 20__

System ok
Network

Network ok
USB transfer

USB transfer ok

Backup ok
Download soft UC

Connect USB key then
press ok exit C

Select prog load <
Select save >

or

Transfer
in progress...

System ok
Network

10:54.32
Tues 19 SEPT 20__

Save or load the firmware to the USB key.

Download soft UC ok

Connect USB key then
press ok exit C

Confirm load ok
soft UC <-

Remove USB key

Reboot in progress...

10:54.32
Tues 19 SEPT 20__

Firmware update from USB key[1]

[1] *After loading the firmware to the USB key, Netsilon will restart.*

7.2 Technician menu

⚠ **This menu is only accessible with a technician code. This daily code is held by BODET.**

To obtain this code, contact BODET customer support and ensure that you have the MAC address[1] of the ETH0 network output.

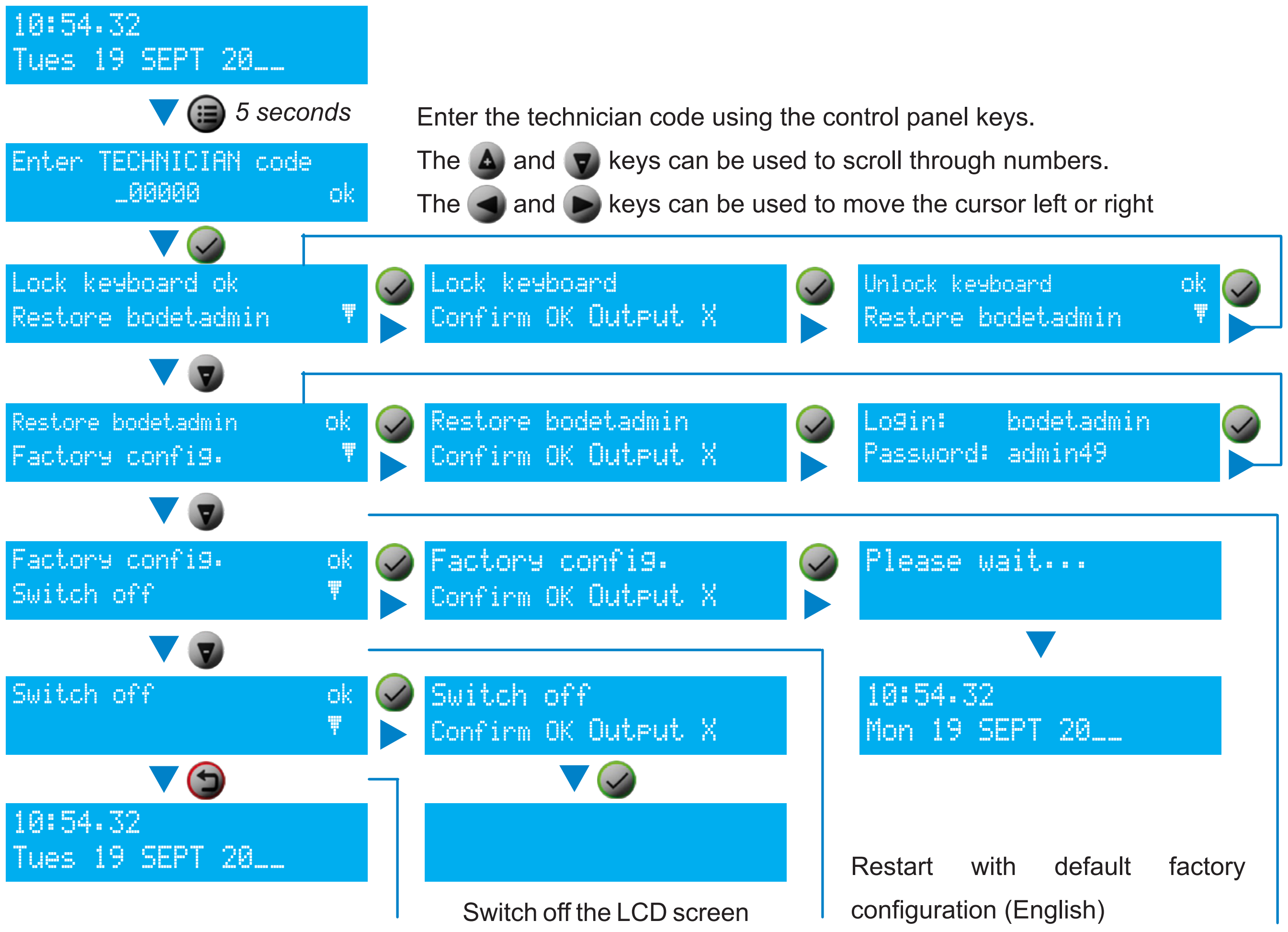
In this menu, it is possible to:

- lock or unlock the control panel,
- restore the default administrator account,
- perform a factory configuration reset.

ATTENTION: This will delete all settings, including the user accounts created.

- switch off Netsilon.

To access the technician menu, press ☰ for 5 seconds, then enter the technician code.



```
10:54.32
Tues 19 SEPT 20__
```

▼ ☰ *5 seconds*

```
Enter TECHNICIAN code
      _00000         ok
```

Enter the technician code using the control panel keys.

The ▲ and ▼ keys can be used to scroll through numbers.

The ◀ and ▶ keys can be used to move the cursor left or right

▼ ✓

```
Lock keyboard ok
Restore bodetadmin
```

✓ ▶

```
Lock keyboard
Confirm OK Output X
```

✓ ▶

```
Unlock keyboard     ok
Restore bodetadmin
```

▼ ▼

```
Restore bodetadmin  ok
Factory config.
```

✓ ▶

```
Restore bodetadmin
Confirm OK Output X
```

✓ ▶

```
Login:    bodetadmin
Password: admin49
```

▼ ▼

```
Factory config.     ok
Switch off
```

✓ ▶

```
Factory config.
Confirm OK Output X
```

✓ ▶

```
Please wait...
```

▼

```
10:54.32
Mon 19 SEPT 20__
```

Restart with default factory configuration (English)

▼ ▼

```
Switch off          ok
```

✓ ▶

```
Switch off
Confirm OK Output X
```

▼ ✓

Switch off the LCD screen

▼ ↩

```
10:54.32
Tues 19 SEPT 20__
```

[1] *The MAC address of the ETH0 network output is shown on a label on the back of the Netsilon device.*

8.1 Status of LEDs on the front panel

The LEDs can provide Netsilon status information.

LED	Status and colour	Description	Check that...
Power	Off	No power supply	1) The mains (AC) power supply cable is connected to a Netsilon connector and the power switch is ON. 2) The direct current (DC) wires are connected to the connector.
	Constant green	Power supply OK	-
	Red	Power supply fault	1) In dual power supply versions (AC+DC, AC+AC), both power supplies are wired correctly.
Sync.	Off	No synchronisation on input	1) The priority synchronisation input is available (e.g.: for a GNSS synchronisation source, check that Netsilon is connected to this antenna).
	Constant green	Synchronisation OK	-
	Red	Synchronisation lost Holdover function	1) The priority synchronisation input is available (e.g.: for a GNSS synchronisation source, check that Netsilon is connected to this antenna). 2) The GNSS antenna installation is operational (if applicable).
	Flashing red	Synchronisation lost Holdover exceeded / freerun	**Please note:** If Netsilon has just been restarted, no troubleshooting is required. Wait for a few minutes until the synchronisation is detected. 1) The priority synchronisation input is available (e.g.: for a GNSS synchronisation source, check that Netsilon is connected to this antenna). 2) The GNSS antenna installation is operational (if applicable).
Alarm	Off	No alarm	-
	Flashing red	Critical alarm	**Please note:** If Netsilon has just been restarted, no troubleshooting is required. Wait for a few minutes until the synchronisation is detected. 1) When synchronisation is lost and the holdover has expired, check that the priority synchronisation input is available (e.g.: for a GNSS synchronisation source, check that Netsilon is connected to this antenna).

8.2 Impossibility to open the web browser

- With DHCP server

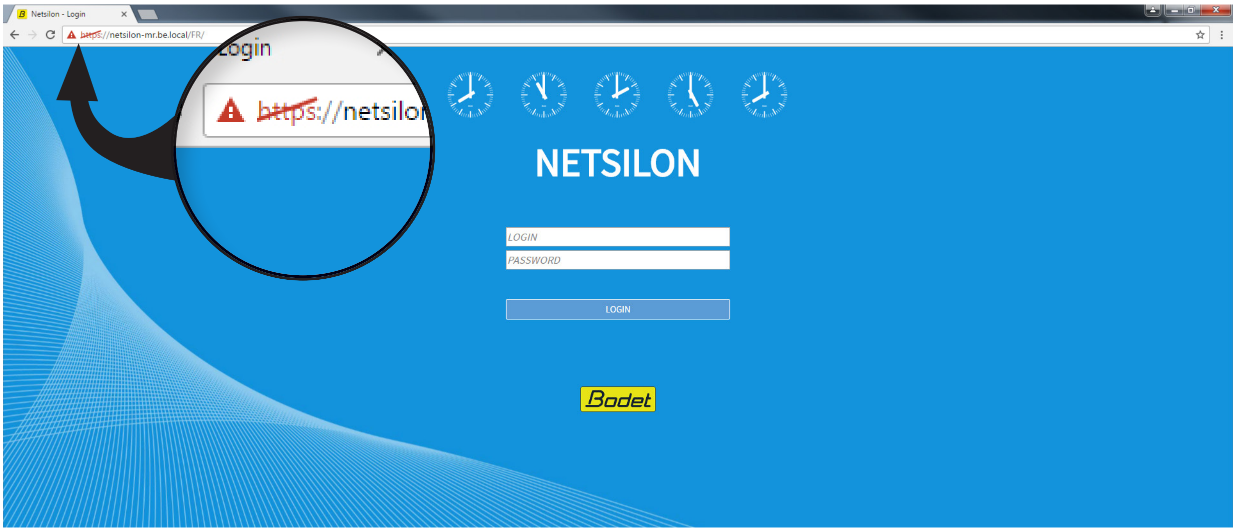
Check that the DHCP server delivers the IP address: the IP address is displayed on the Netsilon LCD screen (see chapter **3.4 Configuration with a DHCP server**)

- Without DHCP server: fixed IP address

Check that the network settings are correct: IP address available, subnet mask, gateway... (See chapter **3.5 Configuration without DHCP server**)

- HTTP/HTTPS

When using the DNS:
HTTP: enter the domain name, the homepage opens.
HTTPS: enter the domain name, the homepage opens. However, the connection is not secure and is indicated as follows:



It is possible to force the connection: please refer to chapter **HTTPS**

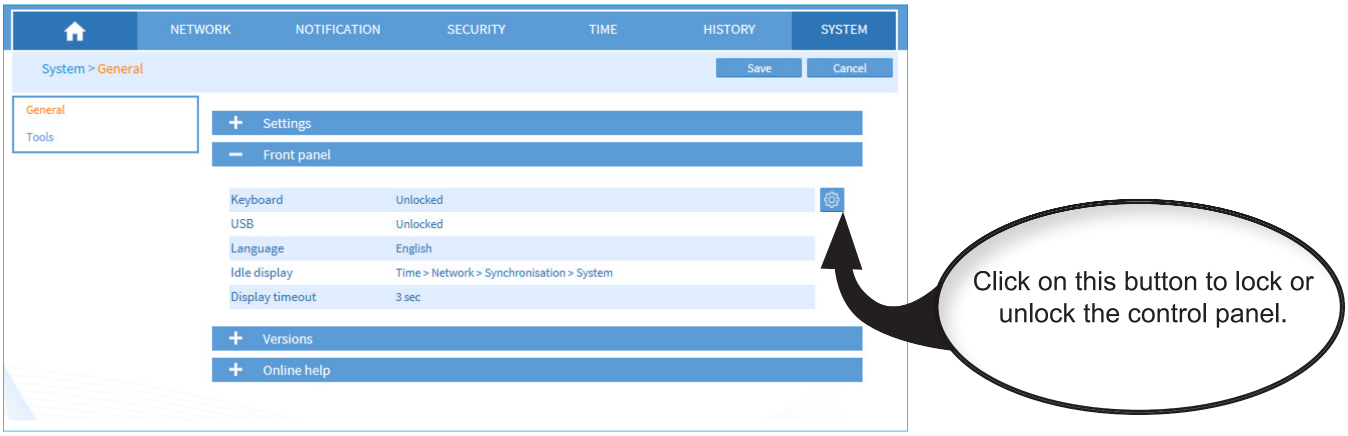
- Enable cookies

It is mandatory to enable cookies to access the Netsilon web server.

8.3 Inactive control panel

The control panel on the front of Netsilon can be locked in order to prevent any misuse by a third party.
Once locked, the control panel is disabled until it is unlocked by using one of the two following methods:

- From the technician menu: please refer to chapter **7.2. Technician menu.**
- From the web server: SYSTEM menu > General > Front panel:



Keyboard	Unlocked
USB	Unlocked
Language	English
Idle display	Time > Network > Synchronisation > System
Display timeout	3 sec

Click on this button to lock or unlock the control panel.

8.4 Data synchronisation

To configure Netsilon via the web server, several parameters must be observed:

- The PC must be on the same network as Netsilon. Make sure that a web browser is installed on the PC (Google Chrome®, Mozilla Firefox, Microsoft Edge or Internet Explorer®). If the PC cannot access the web server, there is a network problem. Check network settings.
- The synchronisation level of the NTP source must be lower than Stratum 15. If this is not the case, Netsilon must be synchronised to a more precise source or operate in holdover mode. Check the NTP synchronisation level.

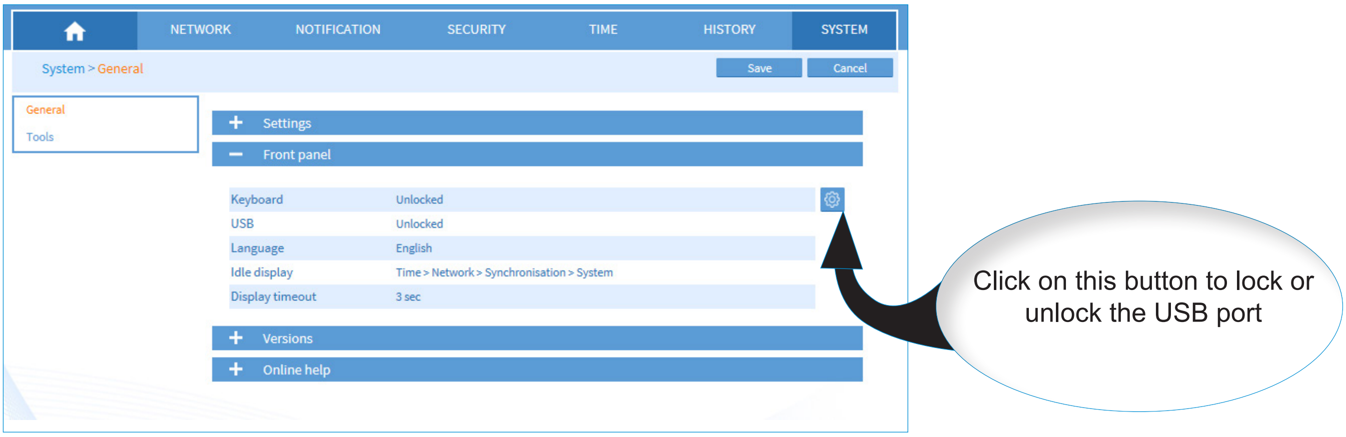
If the problem persists, please contact BODET technical support.

8.5 USB loading

If the USB key is not detected on the USB port, check that:

- The USB port is not locked.

Via the web server: SYSTEM menu > General > Front panel:



Keyboard	Unlocked
USB	Unlocked
Language	English
Idle display	Time > Network > Synchronisation > System
Display timeout	3 sec

Click on this button to lock or unlock the USB port

- The format (file system) of the USB key is FAT16/FAT32 or NTFS.

8.6 BODET technical support

To request technical support for this equipment:

1) Go to the support page of the www.bodet-time.com website:

Click on the link: https://www.bodet-time.com/support.html

2) Fill in the contact form.

The hotline support is available from Monday to Friday from 8.00 to 12.00 am and 1.30 to 5.00 pm.

To speed up the diagnosis of your Netsilon, make a system backup and note the Netsilon MAC address.

8.7 Update history of this user manual

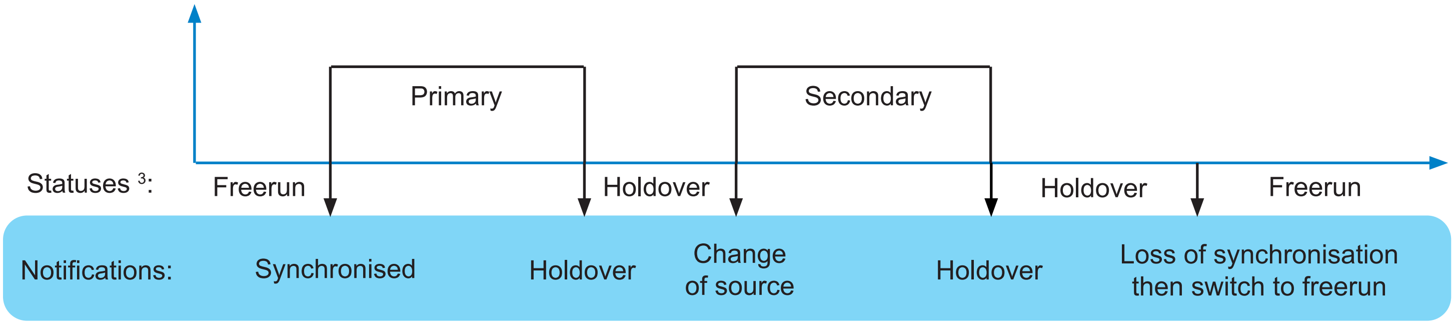
Index	Update description	Date
A	Creation	Sep - 20
B	Update for Netsilon 11	Nov - 20
C	AC+AC version Electrical compliance (DBT) Various information (firewall...).	Feb - 21
D	LDAP / RADIUS / Syslog / PTP information	May - 21
E	New: IRIG IN/OUT, manual Leap Second, TAI/UTC offet / synchronisation settings update	Jan - 22
F	New: 802.1x / VLAN / Bonding / HTTPS / Certificates and keys menu	July - 22
G	Static route limits / Secure GNSS antenna	July - 23
H	AuthNoPriv / NoAuthNoPriv - SNMP v3 protocol	Feb - 24
I	ASCII option card - Control of the OCXO via NTP	Jul - 24
J	ASCII frame update	April - 25

9.1 Annex 1: synchronisation

9.1.1. Primary source / secondary source

Scenario 1: loss of synchronisation of the primary then the secondary source

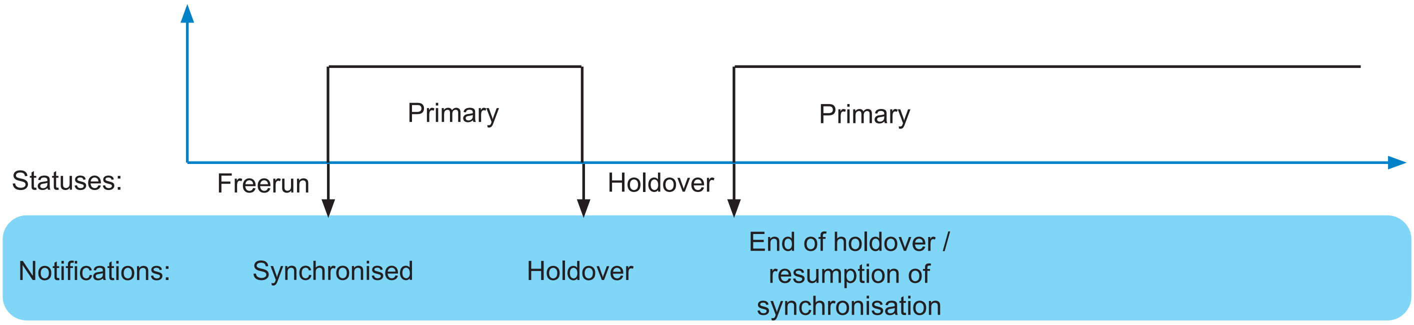
- Freerun[1] on product start-up
- Synchronisation with the primary source (e.g.: GNSS)
- Loss of synchronisation of the primary source
- Holdover[2]
- Synchronisation with the secondary source (e.g. NTP)
- Loss of synchronisation of the secondary source
- Holdover
- No synchronisation detected
- Freerun



In **freerun** mode, the accuracy of the time zone is not guaranteed.

Scenario 2: resynchronisation with primary source after momentary loss of the primary source

- Freerun on product start-up
- Synchronisation with the primary source (e.g.: GNSS)
- Loss of synchronisation of the primary source
- Holdover
- Resynchronisation with the primary source



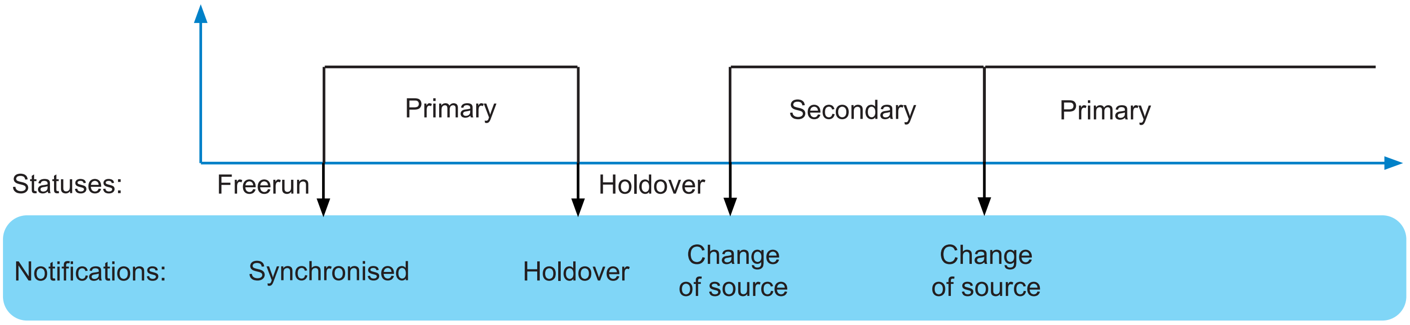
[1] *This is a status in which Netsilon can transmit a time signal without any guarantee of its precision. The precision of the time zone is no longer guaranteed.*

[2] *Reminder: the duration of the holdover mode can be set via the web server.*

[3] *These statuses are shown on the Netsilon LCD screen.*

Scenario 3: restoring the primary source

- Freerun on product start-up
- Synchronisation with the primary source (e.g.: GNSS)
- Loss of synchronisation of the primary source
- Holdover
- Synchronisation with the secondary source (e.g. NTP)
- Switch to the primary synchronisation source.

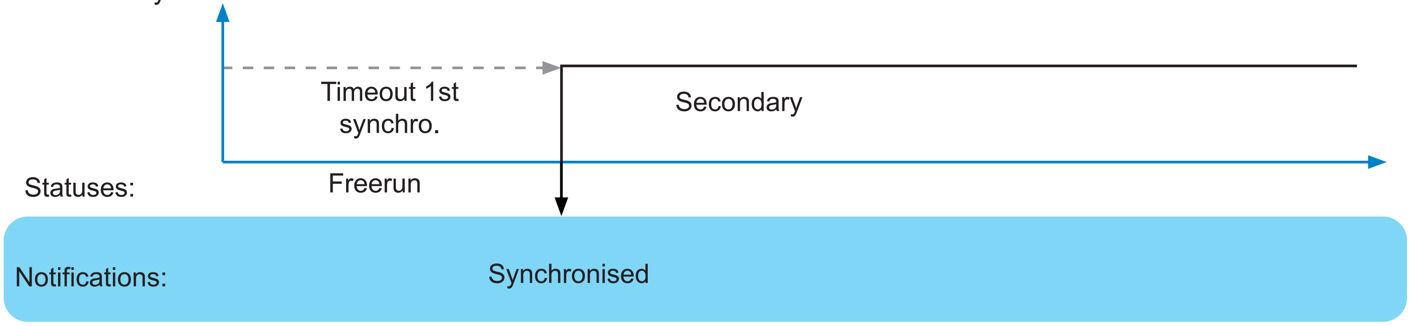


No Ref change notification if switching from one NTP server to another.

Scenario 4: synchronisation with the secondary source when no primary source is present

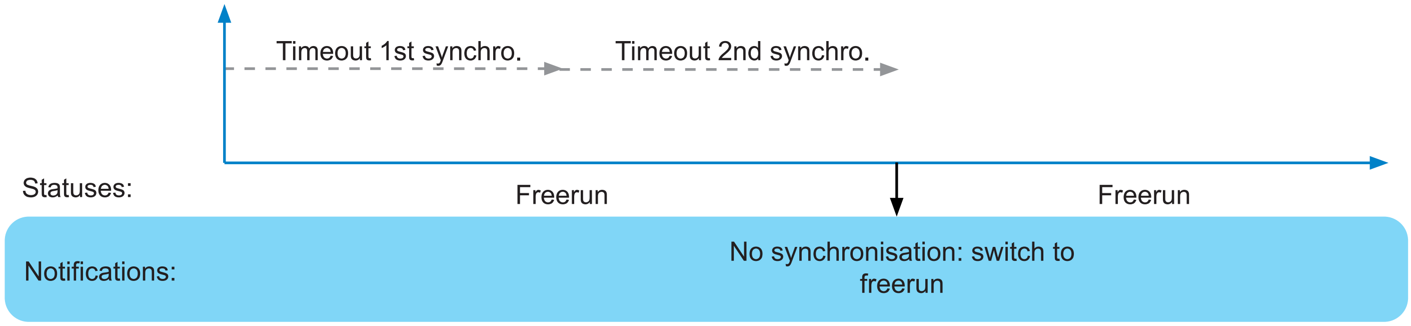
- Freerun on product start-up
- Timeout[1] for synchronisation with the secondary source (e.g.: NTP)

For more reactivity, if synchronisation is not found, after 5 minutes the system attempts to synchronise with the secondary source.



Scenario 5: no synchronisation source

- Freerun on product start-up
- Timeout for synchronisation with the primary source (e.g.: IRIG)
- Timeout for synchronisation with the secondary source (e.g. NTP)
- No synchronisation: switch to freerun



[1] *The timeout of the 1st synchronisation delay duration depends on the synchronisation source:*

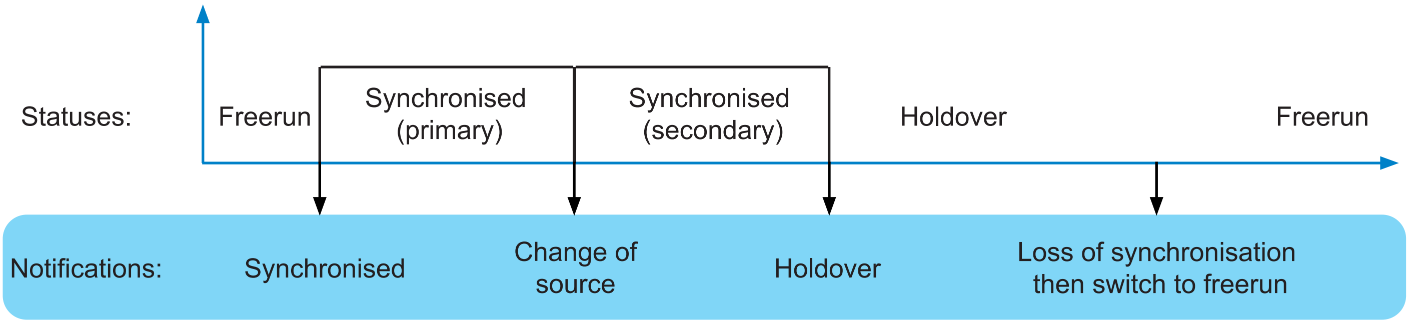
- *GNSS Bodet: 5 minutes*
- *PTP: 10 minutes*
- *NTP: 15 minutes*
- *IRIG: 10 minutes*

9.1.2. *Automatic selection*

The synchronisation source is automatically selected according to the reception quality. There is no specific holdover between source changes.

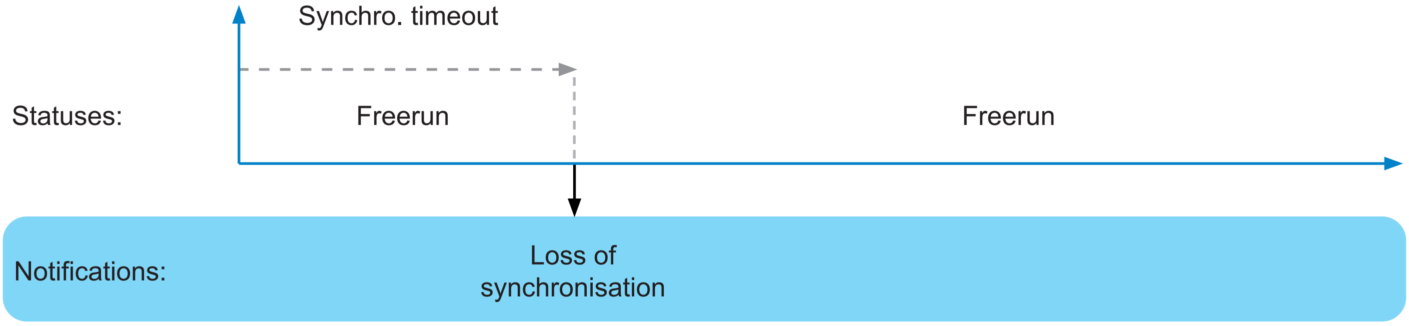
Scenario 1: Loss of synchronisation of the primary then secondary source

- Freerun on product start-up
- Synchronisation with the primary source (e.g.: GNSS)
- Synchronisation with the secondary source (e.g.: NTP)
- Loss of synchronisation with the secondary source
- Holdover
- No synchronisation: freerun



Scenario 2: No synchronisation source

- Freerun on product start-up
- Waiting for synchronisation from sources (e.g.: GNSS + NTP)
- No synchronisation: freerun



9.2 Annex 2: functions

The following table summarises the availability of functions:

Functions	Description	Web server	SSH	Console:	Control panel
Network					
	Interfaces: configure the ETH0 interface	√	√	√	√
	Interfaces: configure the other network interfaces	√	√	√	-
	Routes: configure IPv4/IPv6 static routes	√	-	-	-
	Services: activate services	√	√	√	-
Notification					
	Alarms: configure alarms and alarm thresholds (satellite reception and certificate expiration)	√	-	-	-
	SNMP trap: enable and configure the SNMP trap	√	-	-	-
	SMTP: enable and configure the SMTP	√	-	-	-
	Syslog: enable and configure Syslog log	√	-	-	-
Security					
	User management: Add/ modify/ delete an account, change a password and restore the default administrator account	√	-	-	√ (admin account restoration only)
	User management: enable LDAP/RADIUS services	√	-	-	-
	SNMP agent: enable and configure the SNMP agent Supervision management (SNMP V1/V2c - V3)	√	-	-	-
	SSH: activation and management of keys for authentication	√	-	-	-
	HTTPS: enable HTTP/HTTPS services	√	-	-	-
	HTTPS: choice of certificate (HTTPS)	√	-	-	-
	Certificates and keys: import and configure certificates (CA, signed) and keys	√	-	-	-
Time					
	Synchronisation: enable and configure sources	√	-	-	-
	Synchronisation: manage priorities	√	-	-	-
	Synchronisation: define behaviours (holdover, stratum...)	√	-	-	-
	NTP: enable and configure the NTP protocol	√	-	-	-
	PTP: enable and configure the PTP protocol	√	-	-	-
	Outputs: configure outputs (option cards)	√	-	-	-
	Time zone: configure the time of the system	√	-	-	-
	Time zone: define time zones	√	-	-	-
	Time zone: program a manual Leap Second	√	-	-	-
	Time zone: set the TAI/UTC offset	√	-	-	-
History					
	GNSS statistics	√	-	-	-
	NTP statistics	√	-	-	-
	PTP statistics	√	-	-	-
	IRIG statistics	√	-	-	-
	Oscillator statistics	√	-	-	-
	NTP logs	√	-	-	-
	Syslog logs	√			
	Alarms: acknowledge alarms and consult alarm history	√	-	-	-
System					
	General>Settings: Change product name, language and duration before automatic log out from the session.	√	√ (language only)	√ (language only)	-
	General>front panel: lock the USB port and keyboard, change the language and the Netsilon LCD screen display settings.	√	-	-	√ (except LCD screen display settings)
	General>Versions: consult the Netsilon firmware version and the option cards installed	√	√	√	√
	General>Consult this user manual	√	-	-	-
	Tools > Upgrade and backup: Save or load the configuration, set to factory configuration and update the firmware	√	-	√ (factory configuration only)	√
	Tools>Restart: restart or switch off Netsilon	√	√	√	-
	Tools>Option cards: remove an option card. **WARNING: this action is irreversible without mechanical intervention.**	√	-	-	-
	Tools>Export logs: export logs	√	-	-	-

9.3 Annex 3: rights according to profile: administrator & user

The following table summarises the availability of functions:

Functions	Description	Admin	User
Network			
	Interfaces: configure the ETH0 interface	R/W [1]	R
	Interfaces: configure the other network interfaces	R/W	R
	Routes: configure IPv4/IPv6 static routes	R/W	R
	Services: activate services	R/W	R/W
Notification			
	Alarms: configure alarms and alarm thresolds (satellite reception and certificate expiration)	R/W	R/W
	SNMP trap: enable and configure the SNMP trap	R/W	R/W
	SMTP: enable and configure the SMTP	R/W	R/W
	Syslog: enable and configure the Syslog log	R/W	R/W
Security			
	User management: add/modify/delete an account, change a password and restore the default administrator account	R/W	R
	User management: enable LDAP/RADIUS services	R/W	R
	SNMP agent: enable and configure the SNMP agent	R/W	R/W
	SSH: activation and management of keys for authentication	R/W	R
	HTTPS: enable HTTP/HTTPS services	R/W	R
	HTTPS: choice of certificate (HTTPS)	R/W	R
	Certificates and keys: import and configure certificates (CA, signed) and keys	R/W	R
Time			
	Synchronisation: enable and configure sources	R/W	R/W
	Synchronisation: manage priorities	R/W	R/W
	Synchronisation: define behaviours (holdover, stratum...)	R/W	R/W
	NTP: enable and configure the NTP protocol	R/W	R/W
	PTP: enable and configure the PTP protocol	R/W	R/W
	Outputs: configure outputs (option cards)	R/W	R/W
	Time zone: configure the time of the system	R/W	R/W
	Time zone: define time zones	R/W	R/W
	Time zone: program a manual Leap Second	R/W	R/W
	Time zone: set the TAI/UTC offset	R/W	R/W
History			
	GNSS statistics	R	R
	NTP statistics	R	R
	PTP statistics	R	R
	IRIG statistics	R	R
	Oscillator statistics	R	R
	NTP logs	R	R
	Syslog logs	R	R
	Alarms: acknowledge alarms and consult alarm history	R/W	R/W
System			
	General/Settings: change the Netsilon name, language and web server idle timeout.	R/W	R: Netsilon name W: language and idle timeout
	General>front panel: Lock the USB port and keyboard, change the language and the Netsilon LCD screen display settings.	R/W	R: lock the USB keyboard W
	General>Versions: consult the Netsilon firmware version and the option cards installed	R	R
	General: Consult this user manual	R	R
	Tools>Upgrade and backup: save or load the configuration, set to factory configuration, and update the firmware	R	R: saving or loading a configuration only
	Tools>Restart: restart or switch off Netsilon	R	R
	Tools>Option cards: remove an option card. **WARNING: this action is irreversible without mechanical intervention.**	R	R
	Tools>Export logs: export logs	R	R

[1] *R/W = Read/Write*

9.4 Annex 4: saved settings

Functions	Description	Backup
Network		
	Interfaces: configure the ETH0 interface	-
	Interfaces: configure the other network interfaces	-
	Routes: configure IPv4/IPv6 static routes	-
	Services: activate services	-
Notification		
	Alarms: configure alarms and alarm thresholds (satellite reception and certificate expiration)	-
	SNMP trap: enable and configure the SNMP trap	√
	SMTP: enable and configure the SMTP	√
	Syslog: enable and configure Syslog log	√
Security		
	User management: add/modify/delete an account, change a password and restore the default administrator account	-
	User management: enable LDAP/RADIUS services	√
	SNMP agent: enable and configure the SNMP agent	√
	SSH: activation and management of keys for authentication	√
	HTTPS: enable HTTP/HTTPS services	√
	HTTPS: choice of certificate (HTTPS)	-
	Certificates and keys: import and configure certificates (CA, signed) and keys	√ (CA only)
Time		
	Synchronisation: enable and configure sources	√
	Synchronisation: manage priorities	√
	Synchronisation: define behaviours (holdover, stratum...)	√
	NTP: enable and configure the NTP protocol	√
	PTP: enable and configure the PTP protocol	√
	Outputs: configure outputs (option cards)	√
	Time zone: configure the time of the system	-
	Time zone: define time zones	√
	Time zone: program a manual Leap Second	√
	Time zone: set the TAI/UTC offset	√
History		
	GNSS statistics	-
	NTP statistics	-
	PTP statistics	-
	IRIG statistics	-
	Oscillator statistics	-
	NTP logs	-
	Syslog logs	-
	Alarms: acknowledge alarms and consult alarm history	-
System		
	General/Settings: change the Netsilon name, language and web server idle timeout.	√
	General>front panel: Lock the USB port and keyboard, change the language and the Netsilon LCD screen display settings.	√
	General>Versions: consult the Netsilon firmware version and the option cards installed	-
	General: consult this user manual	-
	Tools>Upgrade and backup: save or load the configuration, set to factory configuration, and update the firmware	-
	Tools>Restart: restart or switch off Netsilon	-
	Tools>Option cards: remove an option card. **WARNING: this action is irreversible without mechanical intervention.**	-
	Tools>Export logs: export logs	√

9.5 Annex 5: list of command sets

List of Netsilon commands:

Category	Command	Description
General		
	helpcli	List of all commands.
System		
	systemversion	Displays the versions of Netsilon and its option cards.
	systemoptioncard	List of option cards installed.
	systemlistservices	Displays the status of services.
	systemservice [service] [ON/OFF]	Change the status of a service.
	systemlanguage [FR/UK/ES/DE/NL/IT]	Change the language of Netsilon.
	systemtimeget	Displays the local time.
	systemstratlevel	Indicates the strat number of Netsilon.
	systempowerac1status	Indicates the status of the AC 1 power supply.
	systempowerac2status	Indicates the status of the AC 2 power supply (only useful in case of dual power supply: AC + AC version).
	systempowerdcstatus	Indicates the status of the DC power supply.
Synchronisation		
	synccurentsource	Indicates the reference source.
	syncsystemstatus	Indicates the status of the system.
	synccurrentnbsat	Indicates the number of satellites detected.
Alarm		
	alarmnbminor	Indicates the number of active minor alarms.
	alarmnbmajor	Indicates the number of active major alarms.
	alarmnbcritical	Indicates the number of active critical alarms.
Tools		
	toolpreupdate	Prepares Netsilon to receive an update file.
	toolupdate	Runs the update previously copied to Netsilon.
	toolrestore	Restores to factory configuration and restarts Netsilon.
	toolreboot	Restarts Netsilon.
	toolshutdown	Switches off Netsilon.
	toolcancel	Cancels a command in progress. Valid only for toolrestore, toolreboot and toolshutdown.
IPv4 network		
	net4getinfo	Displays the IPv4 parameters of all ports or the requested port: IP address and gateway.
	net4getdhcp [interface]	Indicates the DHCP status of all ports or the requested port. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net4setdhcp [interface] [ON/OFF]	Enables or disables the DHCP mode. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net4getdns [interface]	Indicates the DNS server of all ports or the requested port. Interface=ethX,ethX.vlan,bondX, bondX.vlan

	net4setdns [interface][addr4]	Set the parameters of the DNS server. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net4getgate [interface]	Indicates the gateway of all ports or the requested port. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net4setgate [interface][addr4]	Set the gateway. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net4setstaticip [interface]	Set the static IP address and mask. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net4getstaticip [interface] [addr4/cidr]	Indicates the static IP address and mask of all ports or the requested port. Interface=ethX,ethX.vlan,bondX, bondX.vlan
IPv6 network		
	net6getinfo	Displays the IPv6 parameters of all ports or the requested port: IP address and gateway.
	net6getdhcp [interface]	Indicates the DHCP status of all ports or the requested port. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6setdhcp [interface] [ON/OFF]	Enables or disables the DHCP mode. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6getslaac [interface]	Display the state of slaac (enable/disable) for each network interface. Display the information only for the specified interface, if any. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6setslaac [interface] [ON/OFF]	Define the state of slaac (enable/disable) for each specified network interface.
	net6getgate [interface]	Indicates the gateway of all ports or the requested port. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6setgate [interface] [addr6]	Set the gateway. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6getstaticip [interface]	Set the static IP address and mask. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6addstaticip [interface] [addr6]/[prefix]	Indicates the static IP address and mask of all ports or the requested port. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6delstaticip [interface] [index]	Delete an IPv6 static address/prefix for the specified network interface. Interface=ethX,ethX.vlan,bondX, bondX.vlan Index: index of the IPv6 static address (1,2,3) Example: net6delstaticip 0 1

9.6 Annex 6: secure file for SCP and SFTP transfer

Netsilon has a secure file transfer functionality that uses client tools: SCP and SFTP. The authentication is made with the default account password or the public key.

1. Make an SCP file transfer to Netsilon using authentication by default account password:

```
scp authorized_keys scp 10.10.200.5: .ssh
scp 10.10.200.135 password: admin49
```

(Always use the same password as bodetadmin)

```
publickeys 100%
  *********************************************  5 00:00

sftp scp 10.10.200.5
scp 10.10.200.135 password: admin49
```

(Always use the same password as bodetadmin)

```
sftp>
```

2. Make an SCP file transfer to Netsilon using the public key:

```
scp -i ./id_rsa scp 10.10.200.5: .ssh
Enter the password for the key ./id_rsa: mysecretpassphrase

publickeys 100%
 *********************************************  5 00:00
```

3. Make an SFTP file transfer to Netsilon using authentication by default account password:

4. Make an SFTP file transfer to Netsilon using the public key:

```
sftp -i ./id_rsa scp 10.10.200.5
Enter the password for the key ./id_rsa: mysecretpassphrase
```

The user receives the SFTP invitation enabling the file transfer.

```
sftp>
```

The user receives the SFTP invitation enabling the file transfer.