NETSILON 7

User Manual

This document refers to the following products:

907 900	NETSILON 7 AC
907 901	NETSILON 7 DC
907 902	NETSILON 7 AC+DC
907 903	NETSILON 7 AC+AC

Bodet
www.bodet-time.com

BODET TIME & SPORT
1 rue du Général de Gaulle
49340 Trementines, France
Tel.: + 33 241 71 72 33

afaq ISO 9001 Qualité AFNOR CERTIFICATION
afaq ISO 14001 Environnement AFNOR CERTIFICATION
Trémentines plant

Ref.: 608065N

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

TABLE OF CONTENTS

SAFETY INFORMATION AND PROTECTIVE MEASURES

The following symbols and pictograms are used to illustrate risks or sources of danger during installation, use, and maintenance of this device.

Symbol	Description
	*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
	*IEC60417 - 5036* Dangerous voltage
	*IEC60417 - 5172* Class II equipment
	*IEC60417 - 6040* Caution, ultraviolet radiation
	*IEC60417 - 6041* Caution, visible radiation
	*IEC60417 - 6042* Caution, risk of electric shock
	*IEC60417 - 6092* Class II equipment with functional earthing
	*IEC60417 - 6151* Caution, infrared radiation
	*IEC60417 - 6172* Disconnection, all power plugs
	*IEC60417 - 6414* Waste Electrical and Electronic Equipment (WEEE)
	*IEC60417 - 0434b* Caution
	*IEC60417 - 5032-1* Three-phase alternating current
	*IEC60417 - 5032-2* Three-phase alternating current with neutral conductor
	*IEC60417 - 5009* Power, Stand-by
	*IEC60417 - 6069* Caution, very bright light

1. GENERAL POINTS

Thank you for choosing the BODET Netsilon 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. BODET shall not be responsible for any damage arising due to non-observance of these instructions. The product is guaranteed for 3 years, excluding damage caused by power surges (lightning, etc.) in the absence of a Bodet GPS surge protector on the installation.

Non-contractual data. BODET reserves the right to make changes to equipment, including functional, technical and aesthetic changes, without prior notice.

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

Please note: depending on your configuration (e.g. option cards, NTP and/or GPS or GLONASS synchronisation, etc.), some functions presented in this notice may not be available on your Netsilon time server.

1.1 Using the guide

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 to proceed as follows:

- Basic user:
  Read the whole manual 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 through 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:

: 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 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 with a secure approach to computer networks:

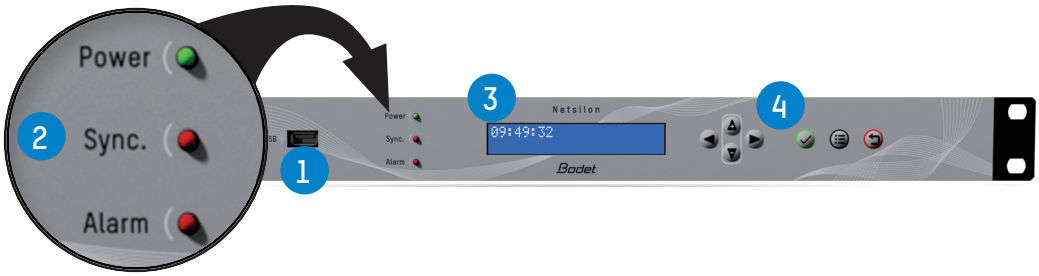
- High-precision internal clock regulated by its own TCXO quartz.
- Order of priority for the different synchronisation references.
- Modular design allowing a wide variety of input/output signals (up to four option cards).
- Network security management: enable/disable encryption, authentication, and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

4 versions are available, depending on the power supply:

- Netsilon 7 AC
- Netsilon 7 DC
- Netsilon 7 AC+DC
- Netsilon 7 AC+AC

1.3 Netsilon presentation

1.3.1. *Front panel*



The Netsilon front panel contains:

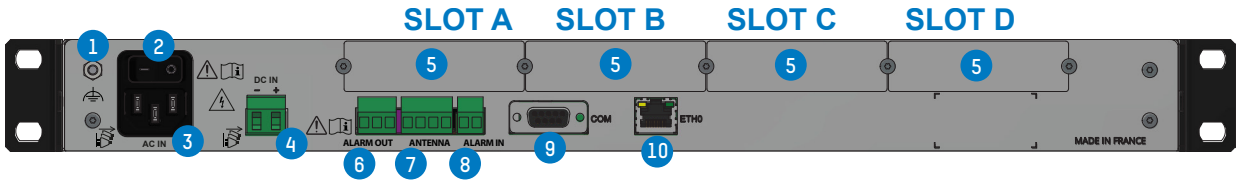
- a USB[1] 1 port
- three status LEDs for power supply, synchronisation and alarms (Power, Sync. and Alarm) 2.

See Chapter **8.1 Status of LEDs on 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 7 (AC+DC)

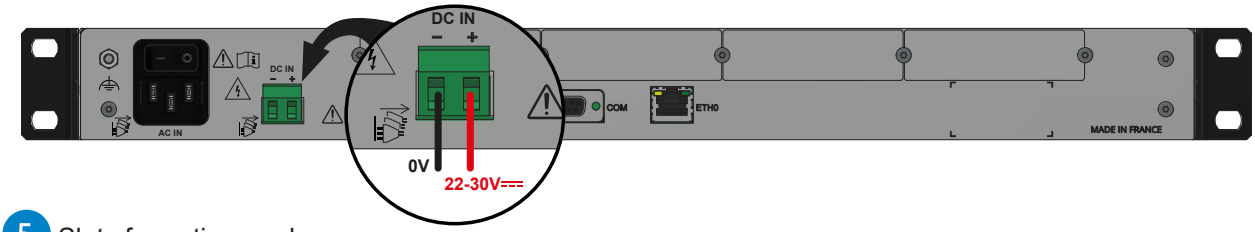


1 Functional earthing terminal ⏚: can be attached to the cabinet frame (optional).
The protective earth is provided by the IEC male connector 3.

2 On/Off switch.

3 AC IN Mains connector. IEC 320 power inlets.

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



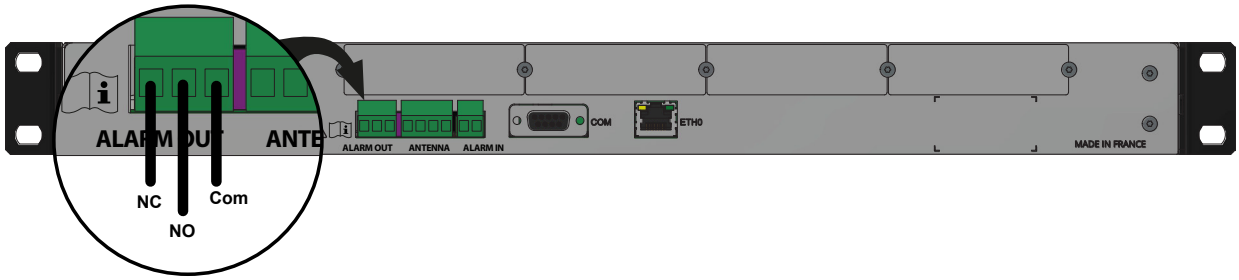
5 Slots for option cards:

- NETWORK option card (RJ45), ref. 907920.
- AFNOR option card, ref. 907940.
- IMPULSE option card, ref. 907942.
- CURRENT LOOP option card, ref. 907944.
- NETWORK FIBER option card (SFP port), ref. 907921.
- ASCII option card, ref. 907926.

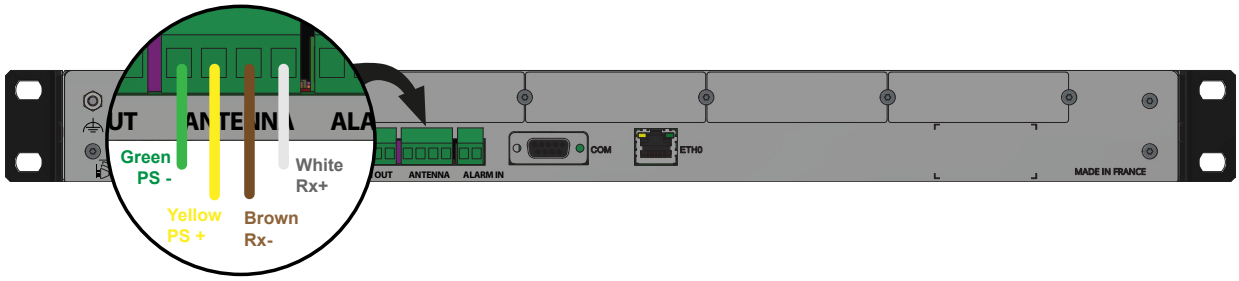
The option cards are installed in our production factory. For subsequent installation, refer to the option card installation guide.

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

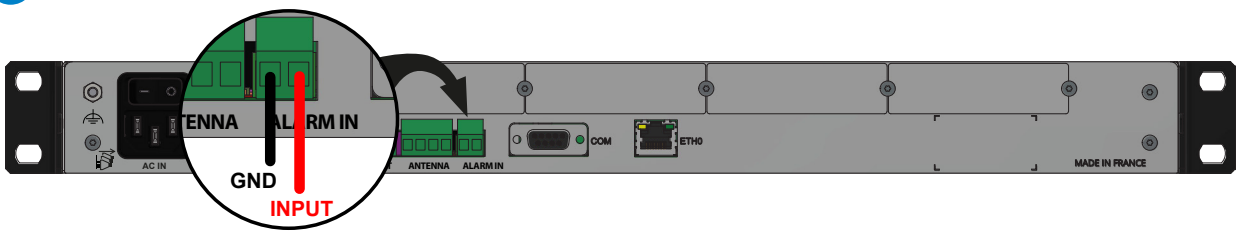
6 Common/Normally-Closed/Normally-Open relay contact output.
If contact Normally-Open: no alarms / If contact Normally-Closed: alarms.



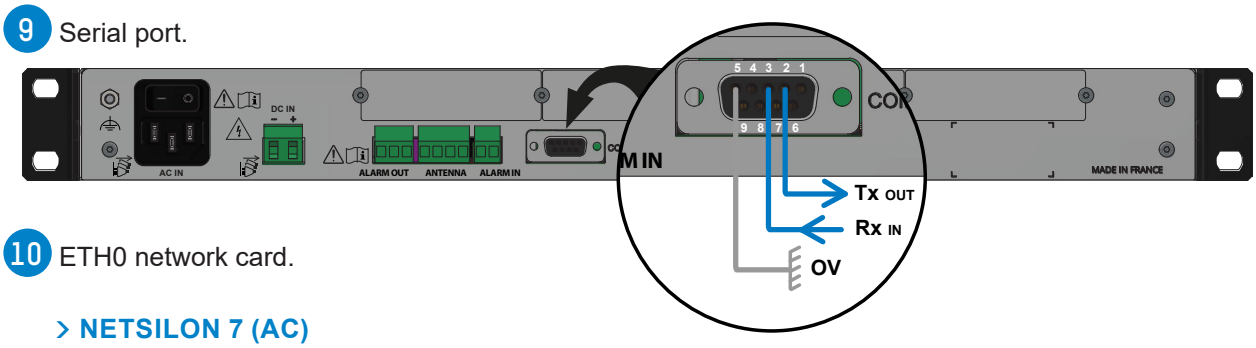
7 Terminal for monoconstellation antenna : GPS or GLONASS.



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



9 Serial port.

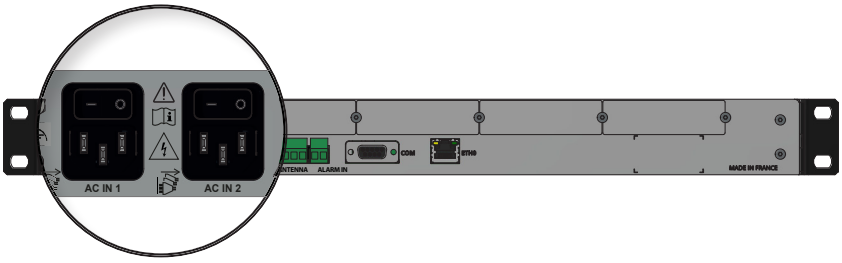


10 ETH0 network card.

> NETSILON 7 (AC)

> NETSILON 7 (DC)

> NETSILON 7 (AC+AC)



1.4 Specifications

1.4.1. Precision

	Typical values for TCXO quartz
Precision[1]	$1x10^{-9}$
Stability[2]	$1x10^{-7}$/day
Holdover[3]	5 ms (after 24 hours)

[1] *average after 24 hours with GPS or GLONASS signal,*
[2] *average after 2 weeks with GPS or GLONASS signal,*
[3] *typical value, after 2-week GPS or GLONASS synchronisation at constant temperature.*

1.4.2. Connections for time synchronization and broadcasting

Input	1x GPS or GLONASS
Outputs	1x Ethernet, 4 slots for option cards

1.4.3. Mechanical characteristics

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

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 | AC+AC : Redundant power supplies, characteristics, above.
Consumption	20W (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 port (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

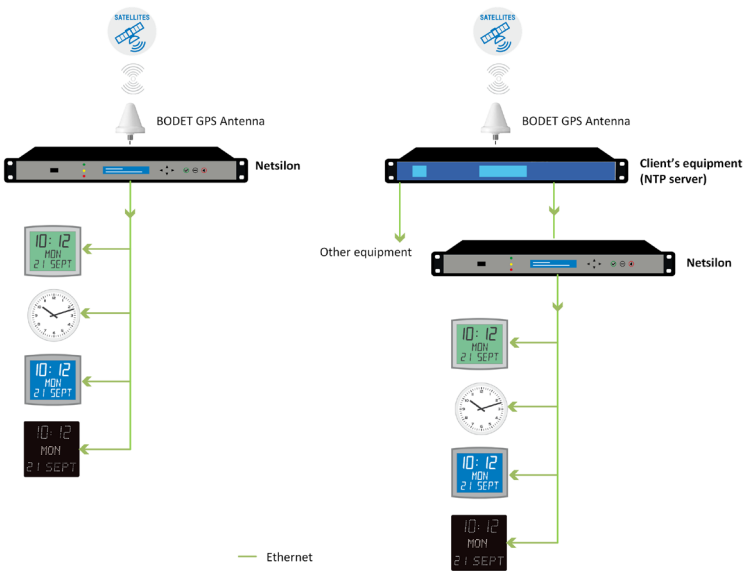
PROTOCOLS	
NTP V2, V3, V4	Compliant with RFC 1305 and 5905. Supports Unicast, Broadcast, Multicast, Anycast, MD5 authentication + integrity, peering and Autokey.
Maximum number of NTP requests per second (All Ethernet ports combined)	7 000
Maximum number of NTP clients (typical)	32 000
SNTP V3, V4	Compliant 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 (signed certificates management)
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 service
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,
- SHA-1, MD5 authentication,
- SSL/TLS: securing exchanges via computer network,
- SCP: secured copy of Netsilon files from a SSH session,
- SFTP: secured transfer of Netsilon files from a SSH session.

1.4.8. Synchronisation sources

Several synchronisation sources are available for Netsilon 7: BODET GPS or GLONASS antennas or an NTP server present on the computer network. Examples :



2. INSTALLATION

This chapter provides an overview of the steps to be followed to install Netsilon.

Several factors must be taken into account when installing Netsilon:

1) The type of power supply: AC, DC, AC+DC, AC+AC
2) The type of installation: Netsilon integration 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 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. These should include:

- The Netsilon unit, with its option cards,
- The two brackets for mounting in a 19'' rack,
- A quick start guide.
- Safety instructions.

2.2 Safety

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 be in accordance with the IEC 364 norm.

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 the equipment must comply 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-repairable 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 while 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

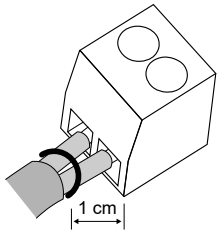
The Netsilon time server should be installed in a 19" rack or cabinet, using the two brackets supplied.

We recommend that you install Netsilon in a secure location.

[1] *It is recommended that you use the latest version of your internet browser.*

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. 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 the version:

- Netsilon 7 (100-240V~): mains power supply only.
  - Connect the power cord to the AC IN connector at the rear of the device.
- Netsilon 7 (22-30V⎓): direct current only.
  - Connect a DC cable and observe the polarity indicated at the rear of the device.
- Netsilon 7 (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 7 (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).

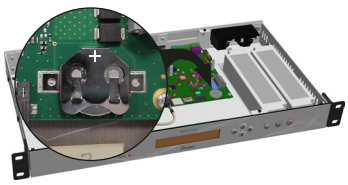
⚠ **The DC IN power supply must be protected upstream by a 6.3 AT fuse.**

When several Netsilon units are powered from 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

If 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 non-compliant battery. 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 the reach of children.
› This product contains a button battery or accumulator. If swallowed, the button battery or accumulator can cause severe internal burns which may be fatal.
› If you suspect that an accumulator cell may have been ingested or inserted anywhere in the body, you must seek immediate 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 CAT.5E or CAT.6 shielded RJ45 Ethernet cable.
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 relay circuits, provide protection with a fuse-disconnector or 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 a DHCP server: automatic assignment of an IP address.
- Without a 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 parameters have been selected to facilitate initial configuration. A single account is activated on shipment from the factory.

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

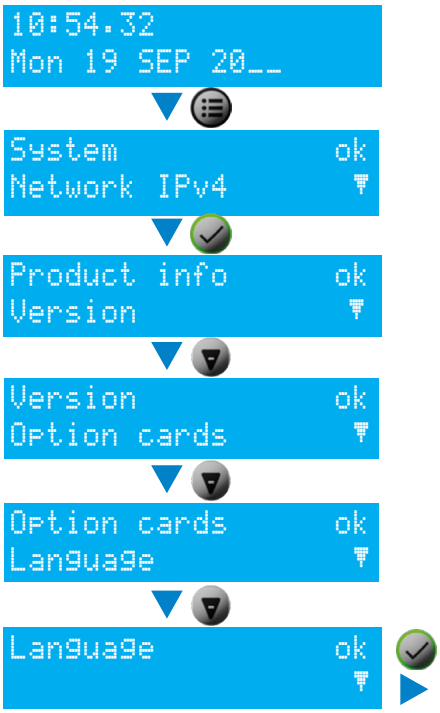
  This account cannot be deleted. However, it is strongly recommended to change the password (see Chapter 4.2.1.1 Changing the password)

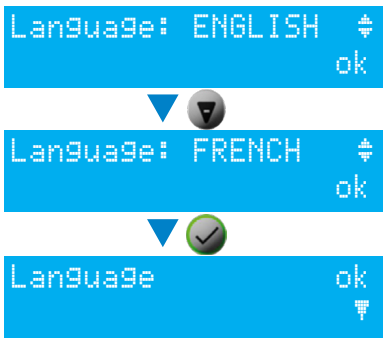
When first running Netsilon, the default parameters are as follows:

Functions	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 first necessary to select the product's display language:



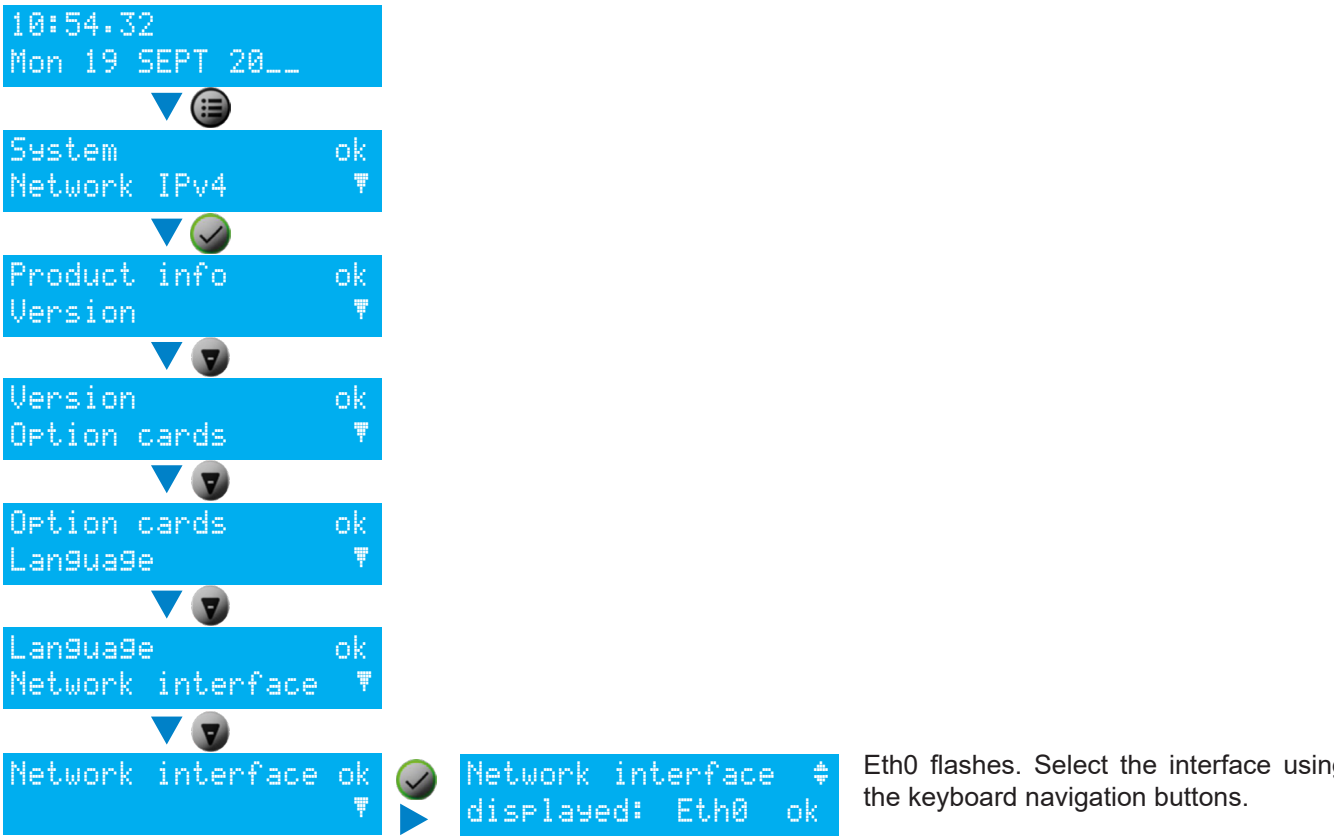


Selection of languages available: English, French, Italian, Dutch, German and Spanish

Exit the menu by pressing the button.

3.3 Choice of network interface

The product being connected to the network, select on the LCD screen the network interface concerned:



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

3.4 Configuration with a DHCP server

1) At start-up, the Netsilon 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 parameters. To read the IP address on the LCD screen, consult the network menu using the Netsilon control panel and LCD screen:

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

4) See Chapter **4. Web server menus.**

192.168.1.0/24 is the IP address with CIDR notation.

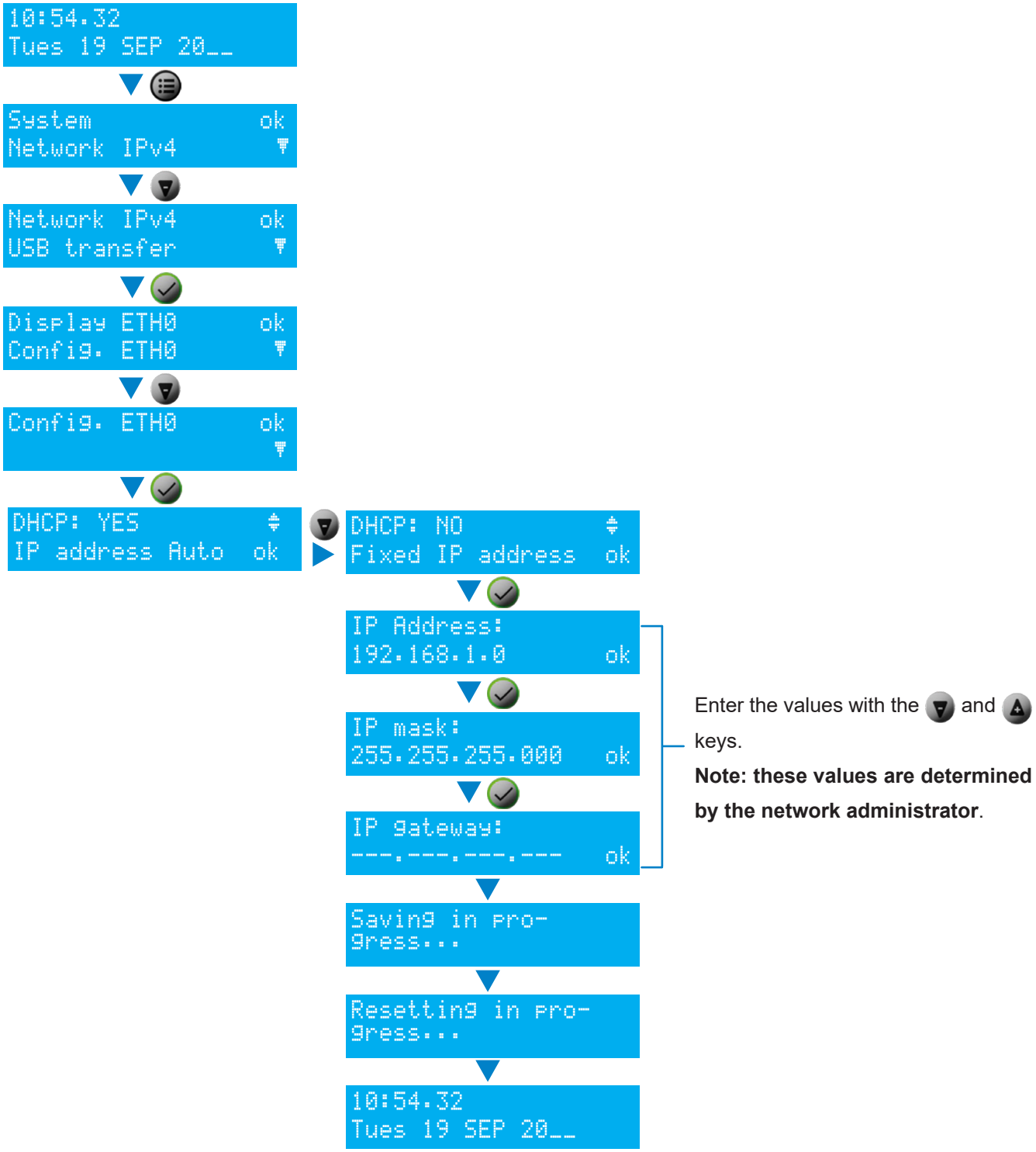
3.5 Configuration without a DHCP server

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.
- Subnet mask
  - The subnet mask defines the number of bits taken by the IP address. The number of bits used in the netmask may range from 8 to 30 bits.
- Gateway
  - The gateway address is required if the 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:



4. WEB SERVER MENUS

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, 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 in 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

: 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 threshold, 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 (setting, sources status and priority), outputs and time base.

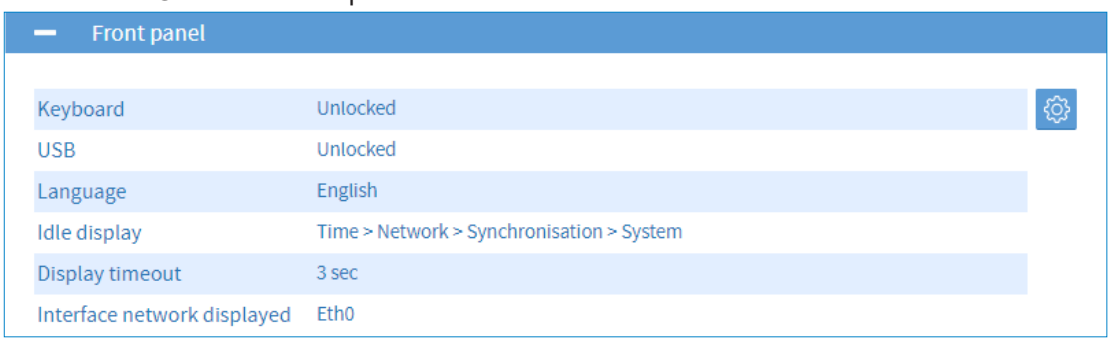
HISTORY : consultation of GNSS, NTP and ALS162 statistics, NTP logs, Sylogs logs and acknowledgement of alarms.

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

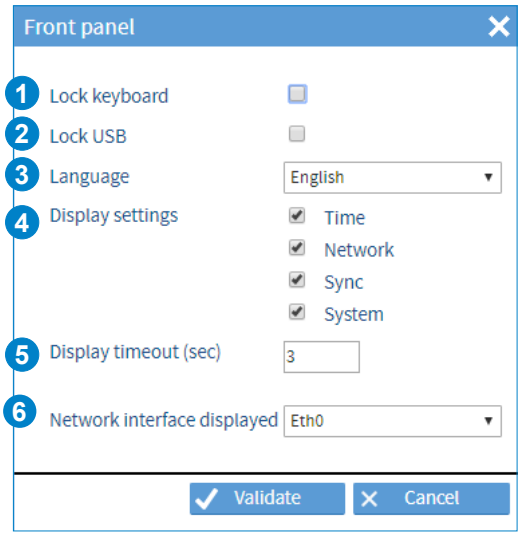
4.1.2. Configuring the Netsilon front panel

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

1) SYSTEM menu > General > Front panel:



2) Click , and the following window will appear:



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 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, not 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 from three to ten seconds.

6 Choice of the network interface for displaying on the face of its network configuration.

4) Click Validate to apply the changes.

---

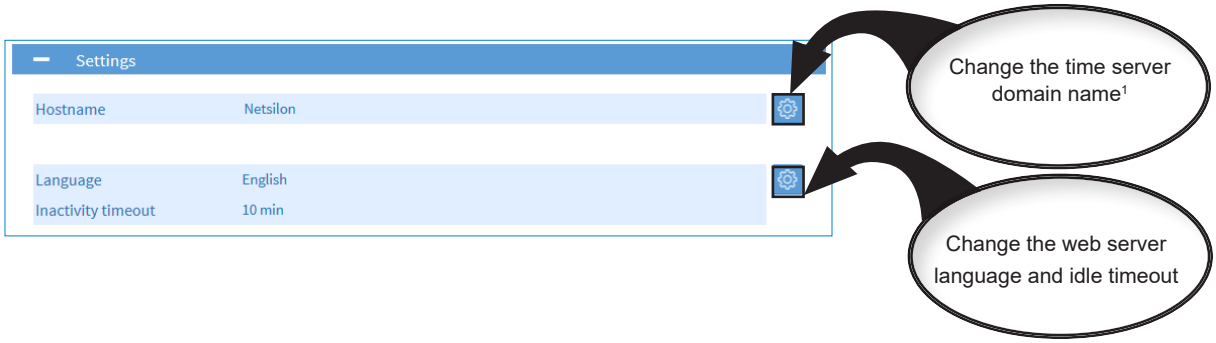
[1] *The domain name must be unique. Once changed, this will lead to regeneration of the Autokey certificate.*

4.1.3. *Changing the language*

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

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

1) SYSTEM menu > General > Settings:



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** 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 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 from 5 to 30 minutes).

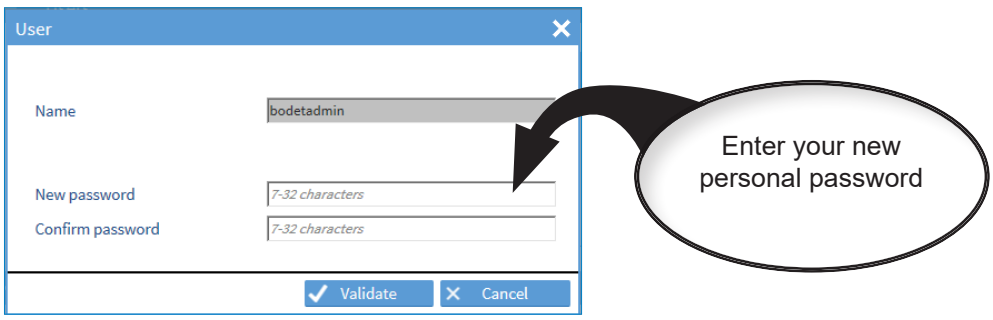
4.2.1.1 *Changing the password*

By way of 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 , and the following window will appear:



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 characters µ and §).

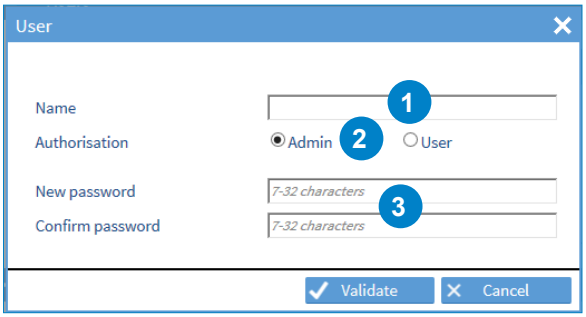
Netsilon offers SHA-512 password encryption. It is also recommended that you enable HTTPS for extra security.

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:



1. Enter a username containing between 5 and 32 characters
2. Select a profile type
3. Enter a password containing 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 permitted.
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 (to select it).

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

3) Click on Yes to apply the deletion.

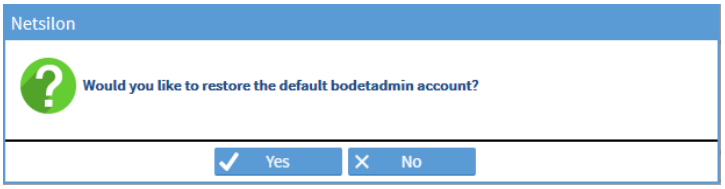
It is impossible to delete the default administrator account.

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:



3) Click on Yes to apply the changes.

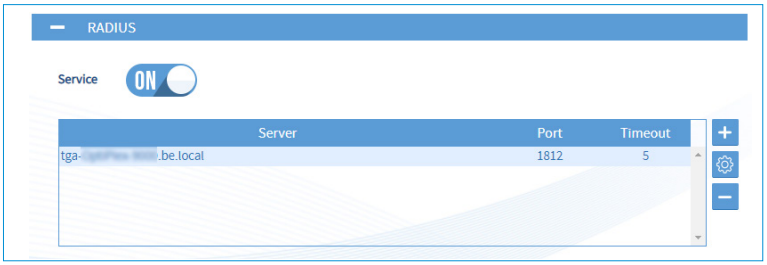
4.2.2. Centralised management

4.2.2.1 RADIUS Service

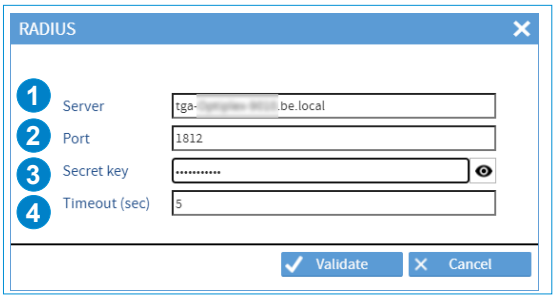
RADIUS Authentication (Remote Authentication Dial-In User Service) implies the use of an external server allowing a centralised management of users to login in to Netsilon. The login password entered by the user is stored in a RADIUS server on the network. Client/server exchanges are secured via a shared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

To enable and configure a RADIUS server :

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



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



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

1. Enter the IP address or the hostname,
2. Enter the RADIUS port number (default port: 1812),
3. Enter the shared security key (MD5 encryption) with Netsilon, (6 to 64 characters)
4. Enter the timeout (delay in communication with Netsilon), (programmable from 3 to 60 seconds)

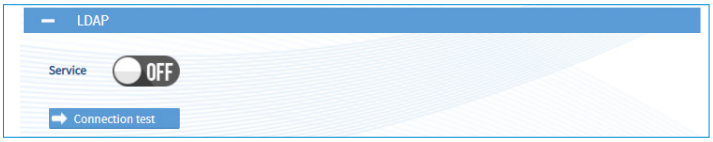
It is strongly recommended to use different user names between those used via the RADIUS server and those used locally. Do not duplicate users (declaration of local accounts in RADIUS and vice versa).
In local and RADIUS, the following users are not allowed: «radius_user», «radius_users».

4.2.2.2 LDAP Service

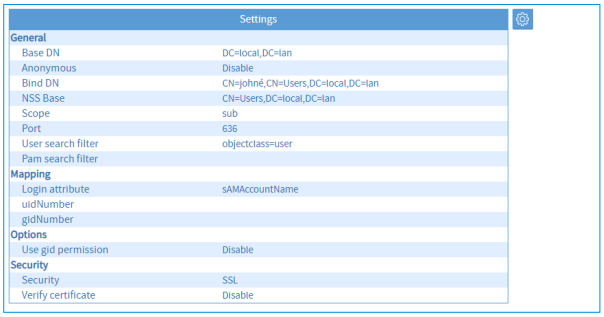
LDAP Authentication (Lightweight Directory Access Protocol) implies the use of an external server allowing a centralised management of users to login in to Netsilon. The login password entered by the user is stored in an LDAP server on the network. This protocol gives access to databases of information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

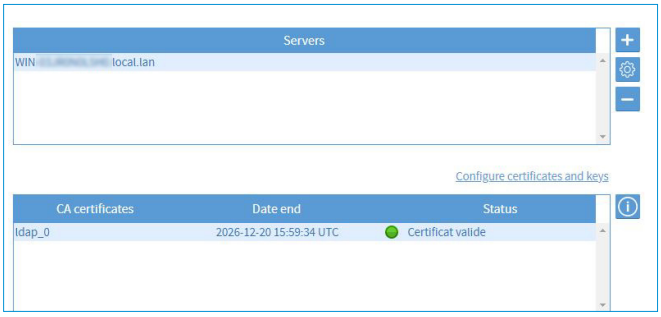
To enable and configure the LDAP service:

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

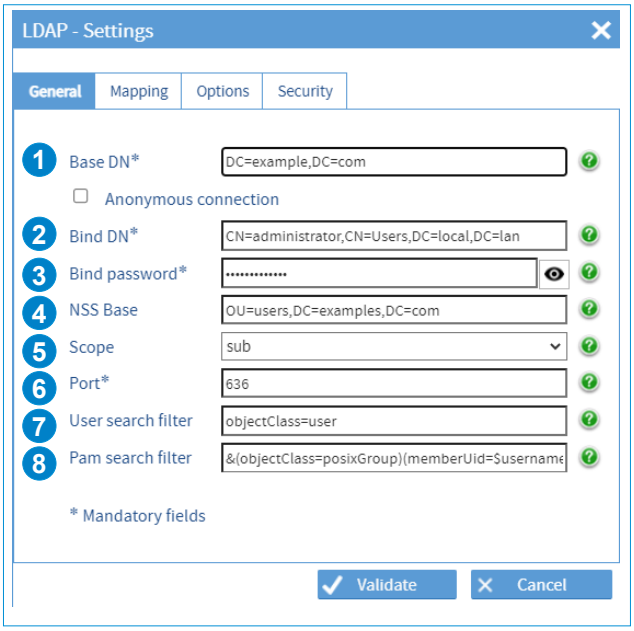


At the end of the configuration (before enabling the service), click on Connection test to ensure that the configuration is consistent (valid connection to the server). This test button is only functional if the service is disabled.





2) Click , and the following window will appear :



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.
The 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 who is 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» 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 parameters (DN) to indicate the entry point of the users search.

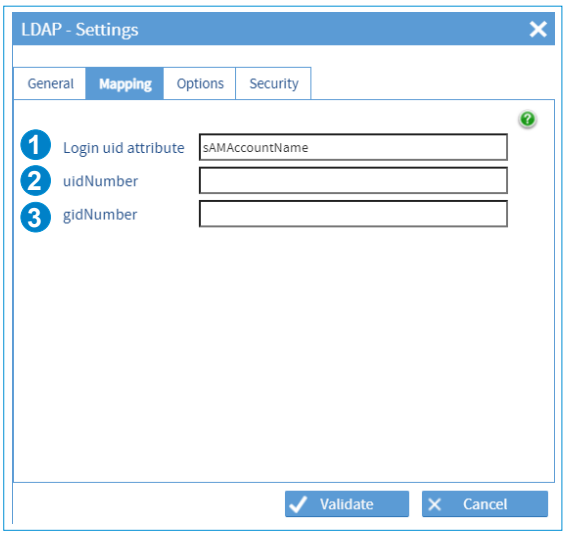
5 Choose an LDAP search scope, from «Sub», «One» and «Base».
- Sub: the entire search base (all entries) is concerned,
- One: only the entries immediately subordinated to the entry specified as the search base are concerned,
- Base: only the entry specified as the search base is concerned.

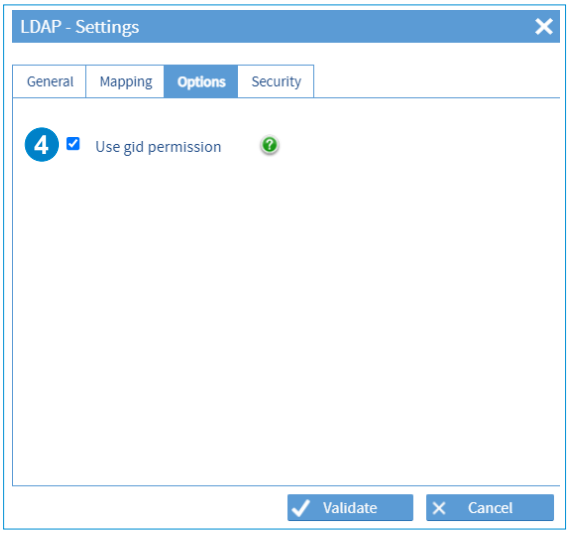
6 Choose the LDAP service port number according to the security settings:
Default standard ports: Disabled: 389, StartTLS: 389, SSL: 636.

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).

Tabs - Mapping / Options





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.

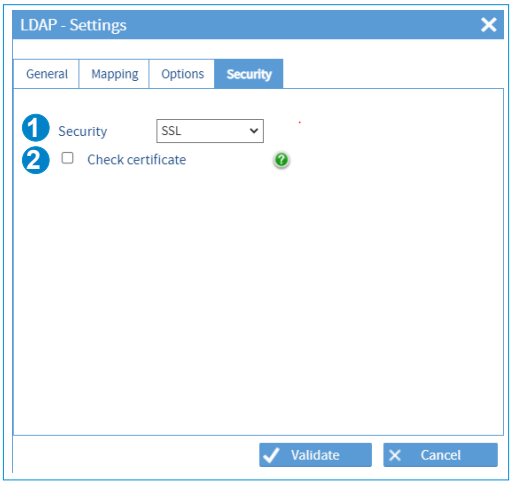
1. Variable corresponding to the login attribute used during the connection. For example, this variable can be mapped to sAMAccountName in the case of an Active Directory server (Microsoft).

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 exceed or equal 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

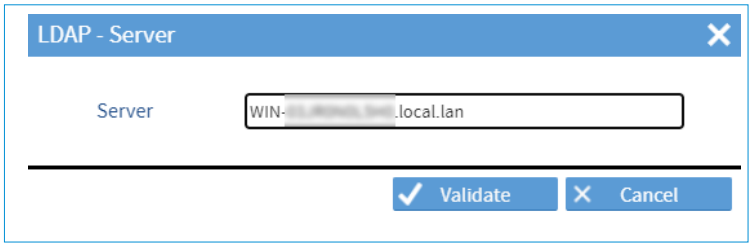


1. Choose the security option: disabled, SSL (encryption of exchanges/passwords), StartTLS.
This involves a TCP port number switch.

2. Check the box 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 **4.9 Certificate and key management.**

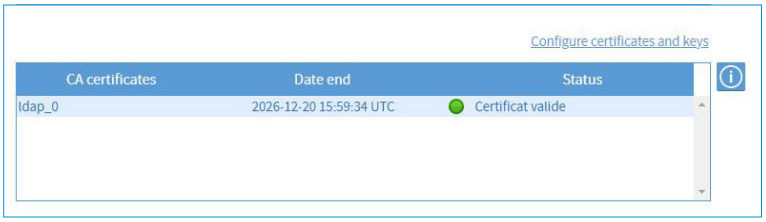
4) Add an LDAP server by clicking on +, and the following window will appear:
(possibility to add up to five servers maximum)

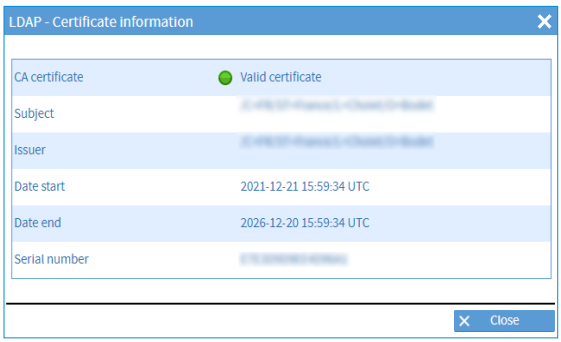


Enter the IP address or the hostname of the LDAP server.

For certificate validation, it is mandatory to indicate the full hostname 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.





The following are examples of typical LDAP service configurations :

Windows Active directory server in secure mode

OpenLdap linux server

4.3 Configuring the time zone

The time zone section enables centralised time zone creation and the programming of a manual Leap Second. Each output can be defined on a time zone, defined earlier in this chapter.

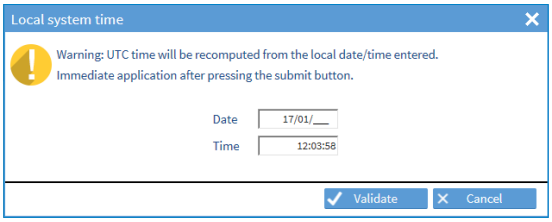
4.3.1. Defining the local time and date of the system

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

For the local time system and date, follow these steps:

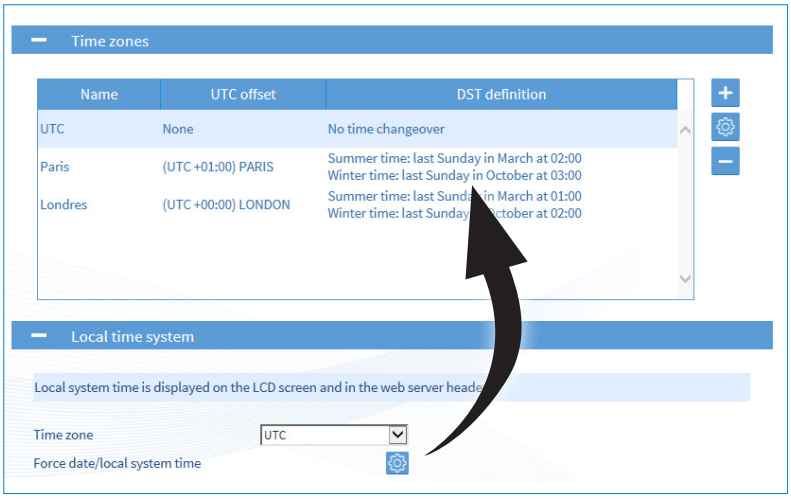
1) TIME menu > Time zones > Local time system.

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



3) Manually change the time and the date.

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



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

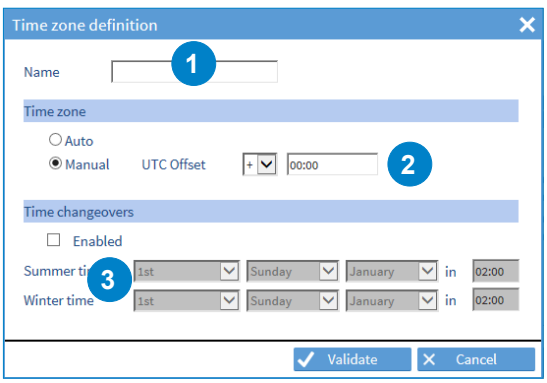
4.3.2. Creating a time zone manually

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 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 time zone differential 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 periodical day in a month or to define a date.

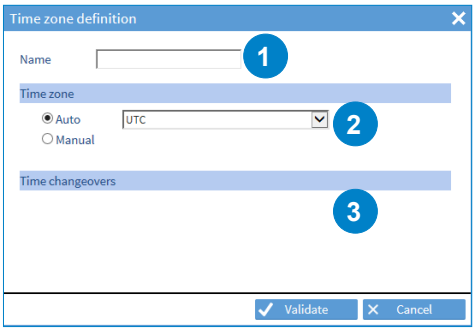
4.3.3. *Creating a time zone automatically*

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	HAWAII
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.

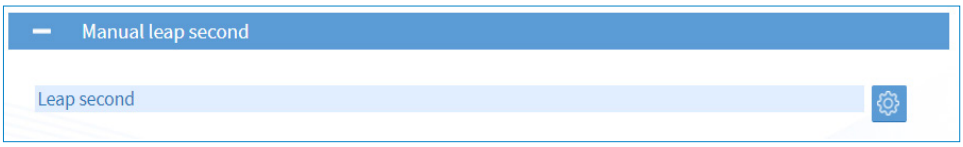
It is possible to create up to 20 time zones (including UTC). The UTC time zone cannot be deleted.

4.3.4. *Programming a manual Leap Second*

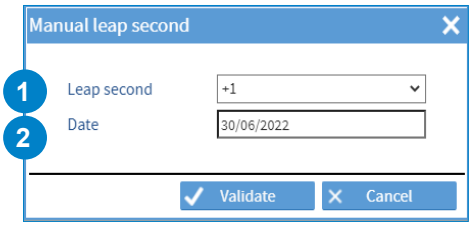
If Leap Second information is managed by the synchronisation source used, it is always possible to program a manual Leap Second. This one takes over and ensures that Leap Second is applied.

To program a manual Leap Second, follow these steps:

1) TIME menu > Time zone > Manual Leap Second



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



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

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

The manual Leap Second is erased as soon as it is passed.

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:

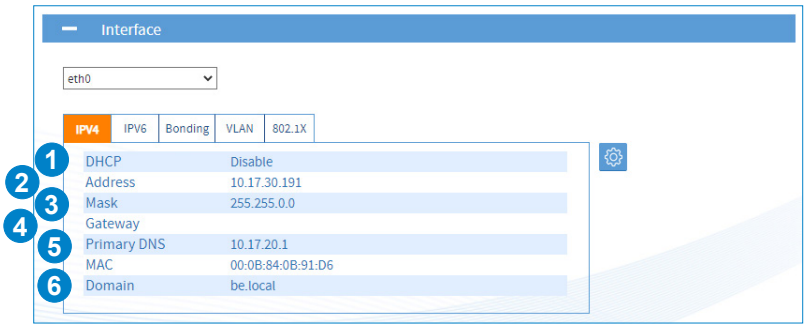
Interface eth0

4.4.1. Network interface configuration

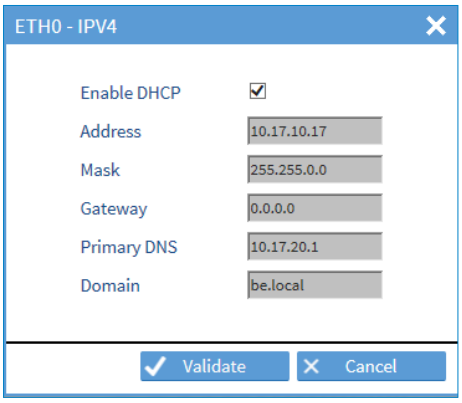
To configure a network interface, follow these steps:

1) NETWORK menu > Interfaces > ETHx interface:

IPv4 settings :



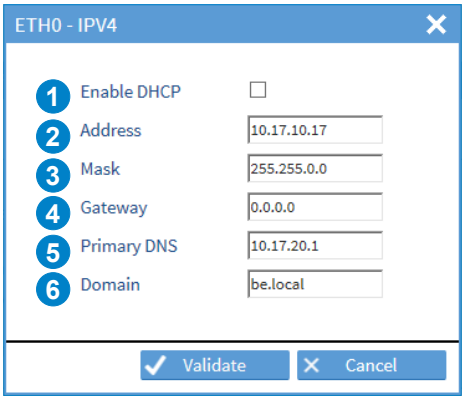
2) Click , and the following window will appear:



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.



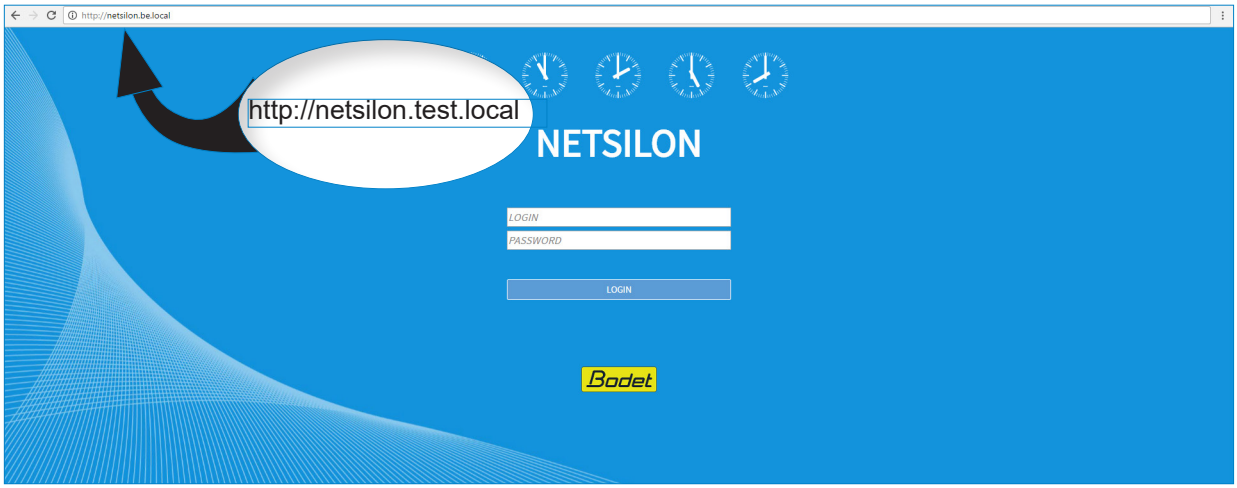
3 Enter the subnet mask in order to define the IP addresses of the products which will be able to communicate with Netsilon.

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

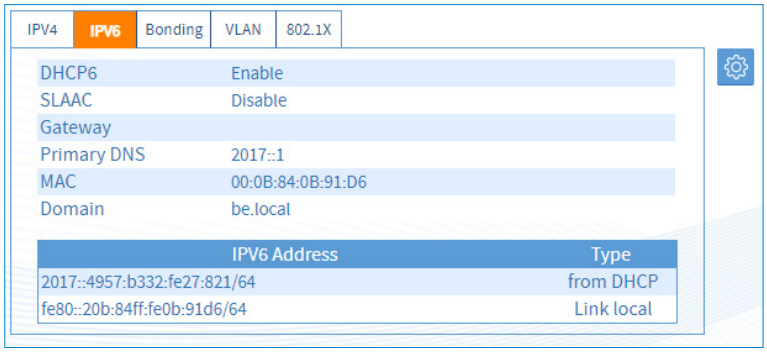
5 Enter the address of the primary DNS in order to assign a domain name.

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**)

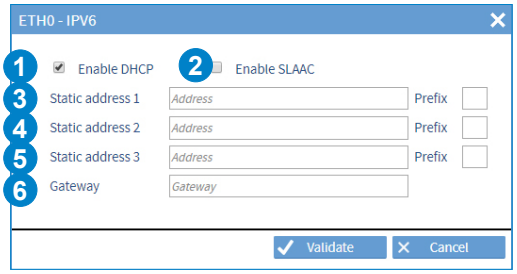
Example of access to the web server using the domain name:



IPv6 settings:



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



1 Enable DHCP (statefull):
With a DHCP server: check the box. The IP address and network settings will be assigned automatically.
Without a DHCP server: manually enter the fixed IP address for this network port.

2 Enable SLAAC (stateless with DHCP) to automatically asign a fixed IP address to Netsilon. Also allows to retrive the gateway.

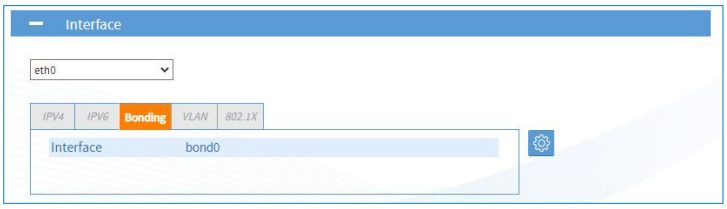
Activating the DHCP (in addition to the SLAAC) allows to obtain the DHCP options (ex .: DNS, gateway) in addition to the IP address fixed by the SLAAC process (no IP assignment by DHCP in this mode). The DHCP is enabled by default. It is possible to combine the «static» / «DHCP» / «SLAAC» modes.

3 4 5 IP fixed addresses for 3 devices. Indicate the prefix defined by the network administrator.

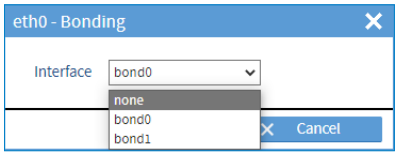
6 Network gateway defined by the network administrator. (Caution: at least one static address is required for the gateway to be taken into account).

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:



2) Click on ⚙, the following window opens:

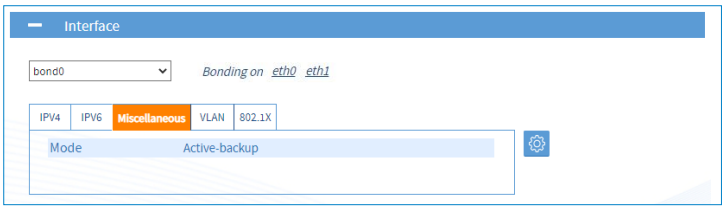


3) Select the assignment of the interface to the desired group (bond) using the drop-down list.

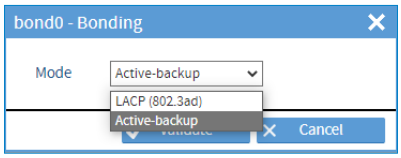
When an interface is assigned to a bond, its configuration will be that of the bond to which it belongs. The configuration of a bond is similar to that of an Ethernet port.
When an interface is assigned to a bond, the 802.1x settings of the interface that is becoming a bond are reset. When the bond is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



6) Click on ⚙, the following window opens:



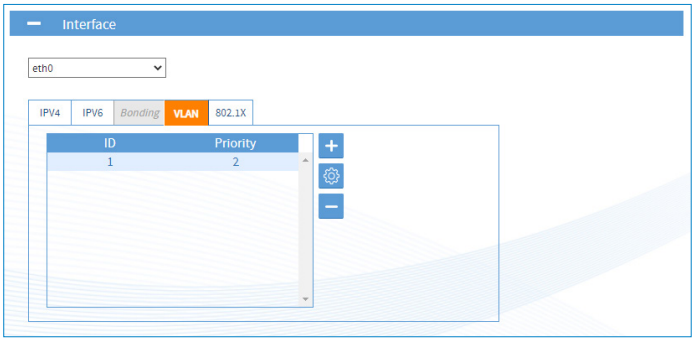
7) Choose the operating mode of this bond using the drop-down list:
Active-backup: one physical interface from the group carries all network traffic of the group. The other physical interfaces are then passive. If the active interface loses the connection, one of the passive interfaces of the group takes it over.
LACP: all interfaces of the group are aggregated 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.

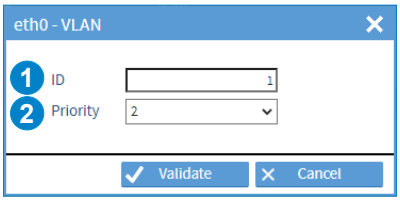
VLAN (virtual local area network):
VLANs reinforce computer security of networks by providing logical segmentation inside an extensive physical network. Each VLAN has its own broadcast domain.
Netsilon uses “VLAN tagged” with an assignment to virtual local networks via the use of a tag in the message 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 allows 4094 different VLANs to be supported.
In Netsilon, VLAN support allows a network port (or bond) to be assigned through which data will flow to one or more 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:



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



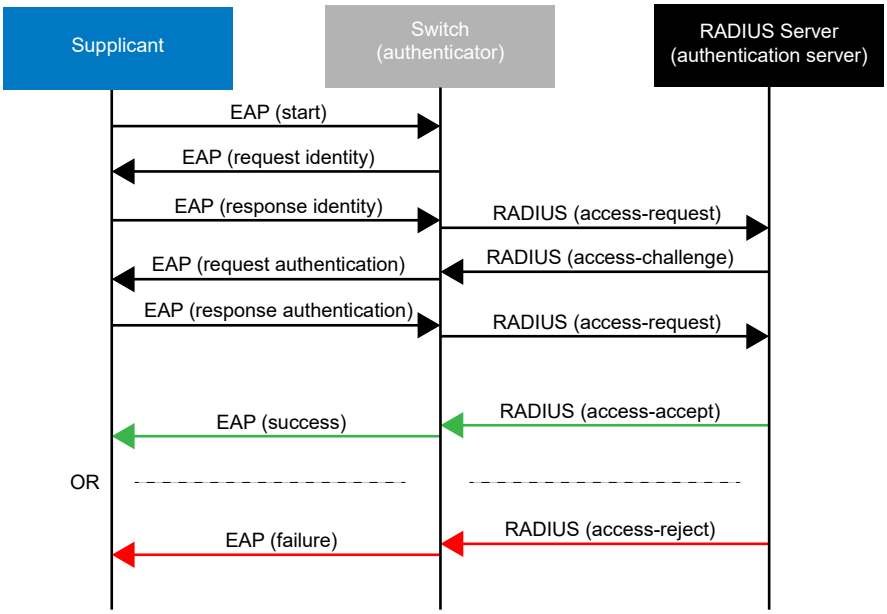
1. Enter the VLAN ID (from 1 to 4094).
2. Select a priority index (from 0 to 7) to optimise message traffic (quality of service).

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 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:

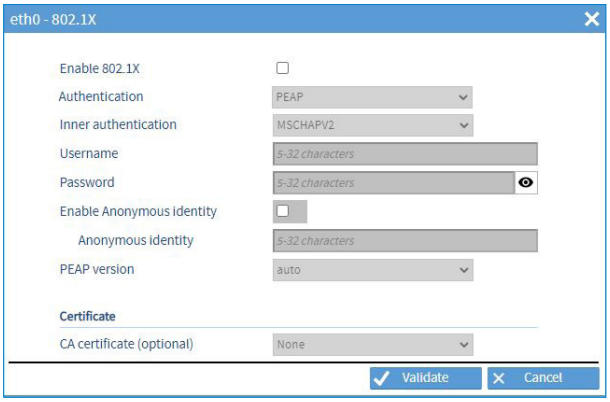
Authentication protocols	Associated internal authentication
EAP-PWD	
EAP-MD5	
EAP-TLS	
EAP-TTLS	PAP MSCHAP MSCHAPv2 MSCHAPv2 no EAP CHAP MD5 GTC
EAP-PEAP	MSCHAPv2 MD5 GTC
EAP-FAST	MASCHAPv2

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

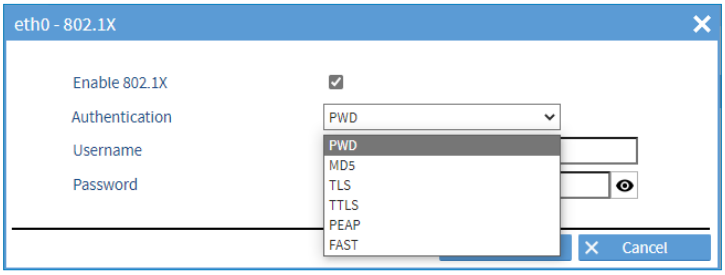
VLAN inherits the configuration of the Ethernet interface or the associated bond.

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

2) Click on , the following window opens:



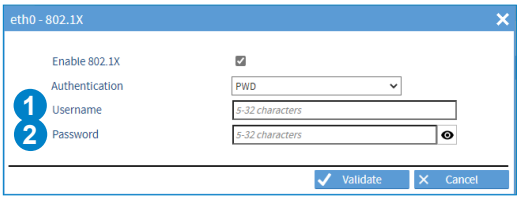
3) Activate the 802.1x protocol by checking the activation box, then choose the authentication protocol type:



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.

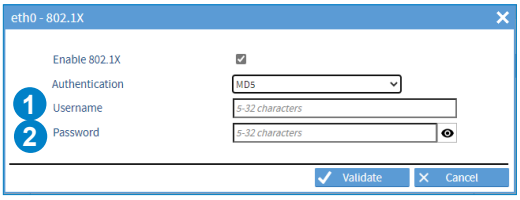
4) Set the parameters according to the chosen authentication protocol:

- PWD: authentication by using a password.



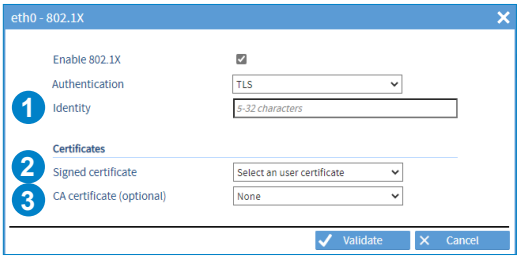
1. Enter the user name of the supplicant (Netsilon).
2. Enter the password.
   This will be verified by the authentication server.

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



1. Enter the user name of the supplicant (Netsilon).
2. Enter the password. This will be hash-protected and verified by the authentication server.

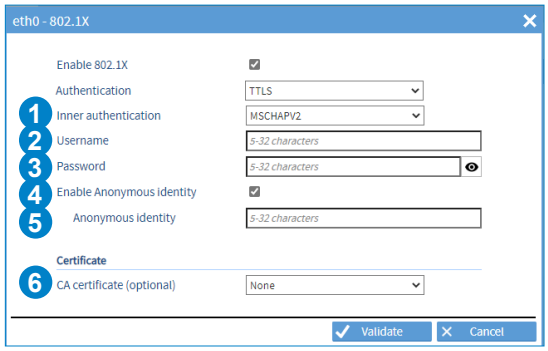
- TLS: mutual authentication of the device (supplicant) and the server through the use of certificates.



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 **4.9 Certificate and key management.**
3. Select a CA certificate (optional).
   This certificate must be previously added in the section "Certificates and keys" in the "CA certificates" tab,
   see chapter **4.9 Certificate and key management.**

- TTLS: authentication by encapsulating a TLS session in 2 phases: authentication of the server to the device

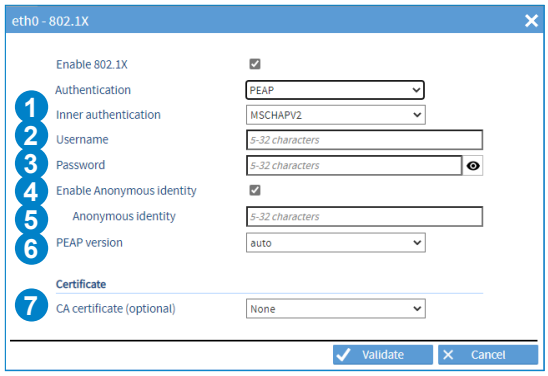
(supplicant) through the use of a certificate to create a secure TLS tunnel for data exchange between the 2 parties during the second phase. During the second phase, the client is authenticated to the server by using an internal authentication mechanism (PAP, MSCHAPv2...), through the secure tunnel.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



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 section "Certificates and keys" in the "CA certificates" tab, see chapter **4.9 Certificate and key management.**

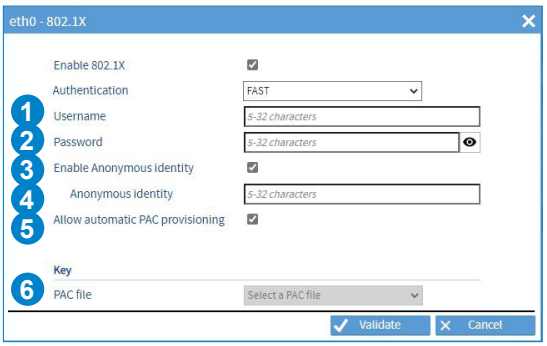
- PEAP: two-phase operation, similar to TTLS. The server first authenticates to the device (supplicant) using a certificate to create a secure TLS tunnel between the two parties. Then, the server authenticates the device within the secure tunnel using an internal authentication method (MSCHAPv2, MD5...).



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 section "Certificates and keys" in the "CA certificates" tab, see chapter **4.9 Certificate and key management.**

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



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 file 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 section “Certificates and keys” in the “public keys” tab,
   see chapter **4.9 Certificate and key management.**

4.4.2. ETHERNET option card (ref. 907920)

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 on our website www.bodet-time.com.

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

4.4.3. IPv4 / IPv6 static routes configuration

To configure static routes:

1) NETWORK menu > Routes

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

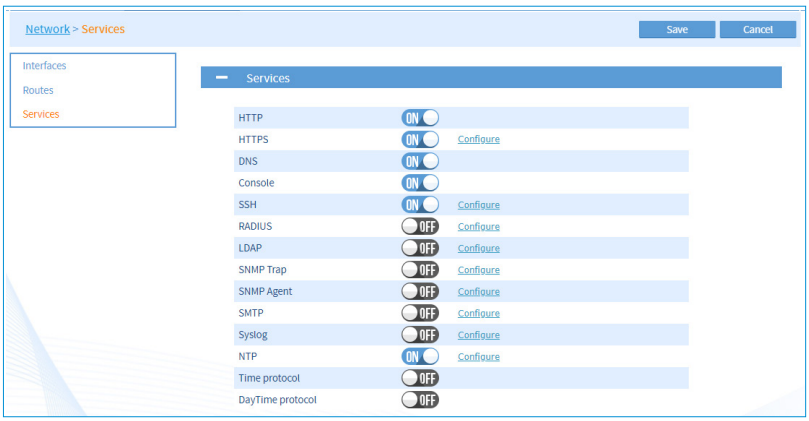
3) Choose the Ethernet interface, the bond or the VLAN.

It is possible to add up to 20 routes in IPv4 and 20 routes in IPv6.
The gateways (default routes) must be declared in the interfaces.

4.4.4. Managing network services

To manage network services, follow these steps:

1) NETWORK menu > Services



It is possible to enable or disable network services individually.

For some services, it is necessary to carry out a prior configuration. Hyperlinks (Configure) can be used to access the setting pages of services requiring configuration.

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

› HTTP - HTTPS

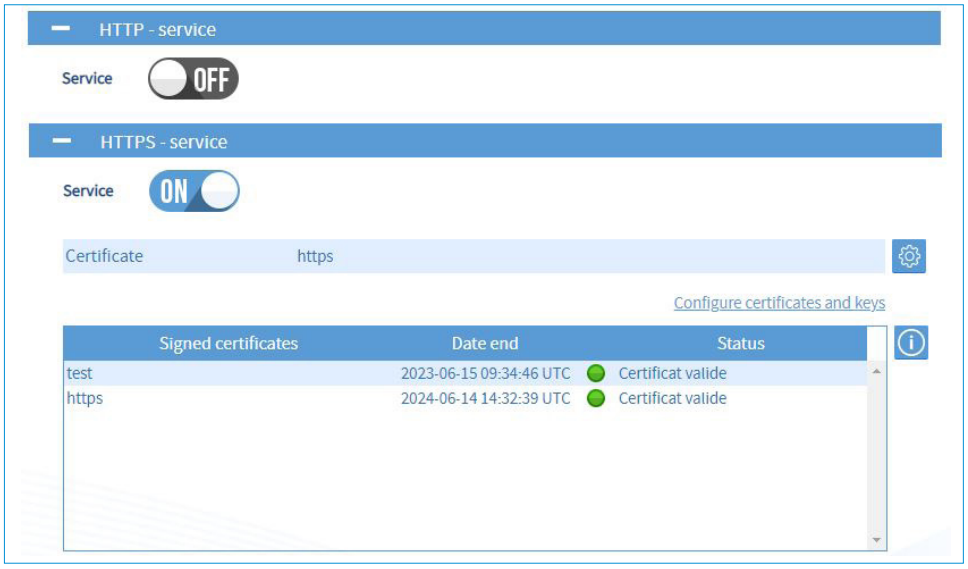
HTTPS (Hypertext Transfer Protocol Secure) is a communication protocol used to access a secure web server. If HTTPS is included in the URL instead of the usual HTTP, the message will be sent to a secure port on the server.

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:



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.

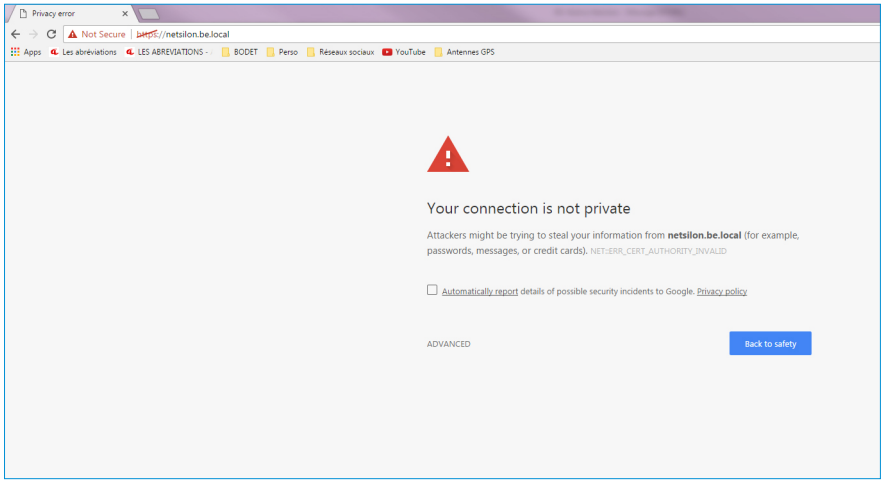
Certificates are added from the Certificates and Keys menu.
See chapter 4.9 Certificate and key management.

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

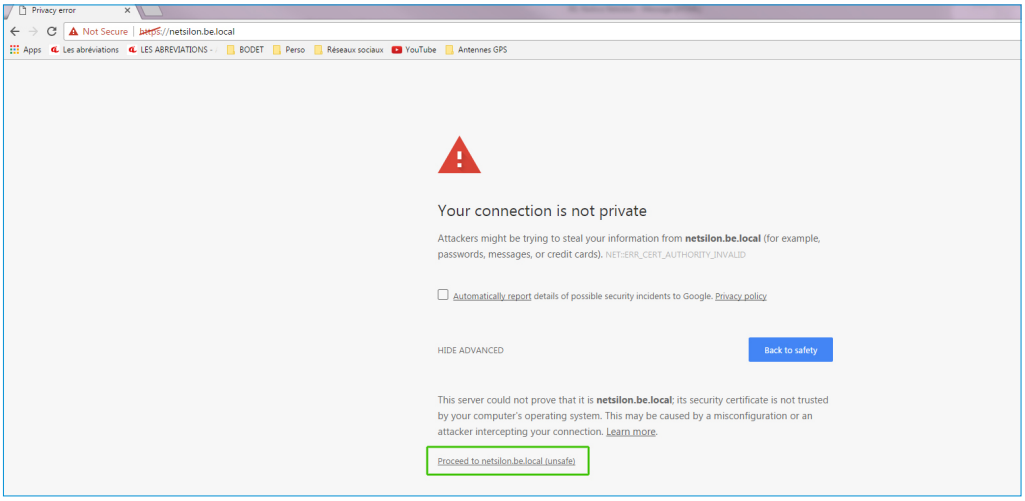
To use the secure connection, HTTP to HTTPS redirection is performed automatically:

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

2) For example: https://netsilon.be.local:



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



The connection is secure, even if "https" is crossed out 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 for optimising security when accessing the Netsilon web server.

› DNS

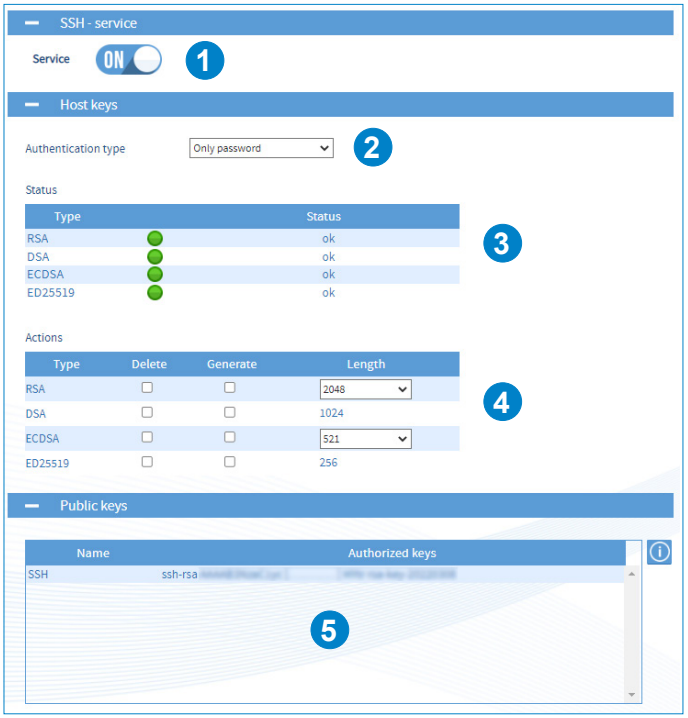
The DNS (Domain Name System) is a protocol which can be used to associate a domain name, known as the hostname, (e.g. www.netsilon.com) with an IP address.
However, if queried by a host on the destination server, only its IP address will be sent in order to determine precisely the identity of the synchronisation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

› SSH

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



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 Generates or deletes 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 supervising network devices. There are two entities: an SNMP manager and agents (e.g. Netsilon). The manager queries the agent, which will send messages to it, known as ‘traps’.

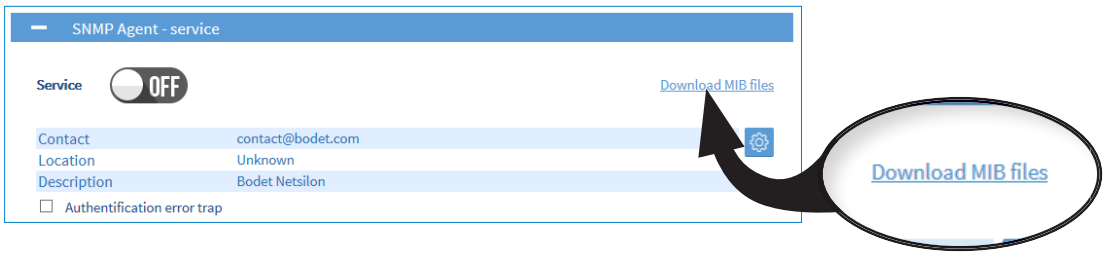
Traps
SNMP traps are messages sent using the SNMP protocol from a monitored device to a monitoring server.

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

Click on Configure then refer to chapter **4.8.2 SNMP trap Configuration.**

Downloading the MIB file

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



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 **4.10 System supervision.**

› SMTP

SMTP (Simple Mail Transfer Protocol) is used to transfer electronic messages (alarms) within a computer network. An SMTP server is a service which listens on port 25. Its main purpose is to route emails to a recipient.
Click on Configure then refer to chapter **4.8.1 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 a future analysis. It is also possible to use this service to archive events locally.
Click on Configure then refer to Chapter **4.8.4 Syslog Configuration.**

› NTP

Network Time Protocol (NTP) is a client/server protocol for synchronising time 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.**

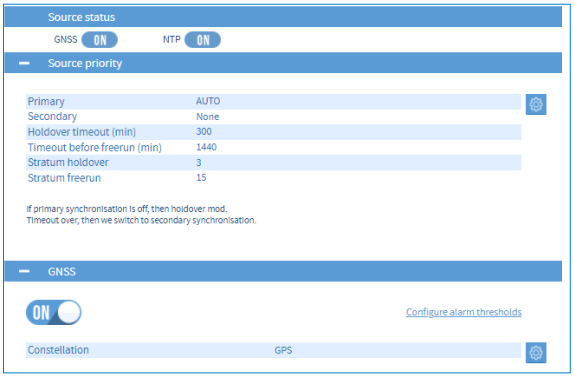
› TIME PROTOCOL and DAYTIME PROTOCOL

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



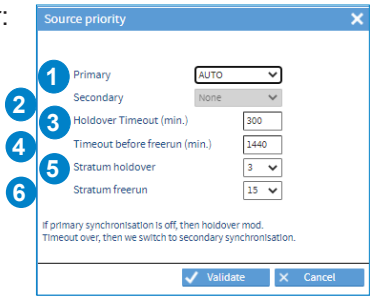
4.5.1. *Status of sources*

An overview is provided. This area shows whether or not 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, precise time signal.

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



1 4 possible choices: AUTO - GNSS - NTP - ALS162
In this mode, Netsilon automatically selects the most reliable source (with the highest quality) and automatically switches between the 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 of the source - GNSS: 5 minutes, NTP: 15 minutes, ALS: 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 4 possible choices: None - GNSS - NTP - ALS162

3 Holdover is a status in which the time 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 time-out» can be set from 1 to 14400 minutes (10 days).

4 Once the Holdover time-out has expired, and without a return of the primary synchronisation source or a secondary source to take over, a new delay is activated before switching to the «freerun» state, where the accuracy of the time base is no longer guaranteed: this is the «Time-out 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 value 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.
e.g:
Stratum holdover = 3
Local source = 2
Netsilon NTP server (for client synchronisation) = 3

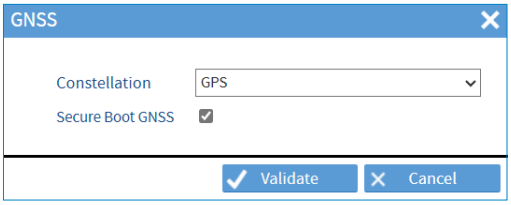
See Chapter **9.1 Annex 1: Synchronisation** for an overview of the different synchronisation scenarios.

4.5.3. Satellite receivers

Enable GNSS synchronisation using the ON button.

In the case of GNSS synchronisation, the constellation on which the time server should perform its synchronisation must be chosen, in accordance with the antenna connected to the product (GPS or GLONASS). Netsilon 7 uses only one constellation to synchronise. There is a dedicated antenna for each constellation. If the configuration is not correct (gap between settings and the installed antenna) the time server will not synchronise.

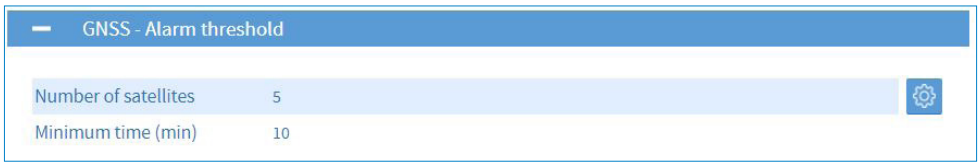
1) To select the constellation according to the antenna connected to the product, click on , the following window will appear:



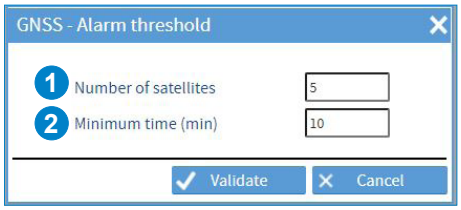
The «Secure Boot GNSS» function is active by default and enables all GNSS frames to be received before the time server is synchronised.

Activating this function extends the Netsilon's synchronisation time (approximately 12.5 minutes). If the function is inactive, the synchronisation search is faster but an offset may appear.

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



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



Set the number of satellites to define the alarm threshold:

1 Set the number of satellites, between 3 and 8.

2 Set the duration after which the alarm is notified.

For example:
- Number of satellites set to 5,
- Duration set to 10 minutes.

If less than 5 satellites are counted for 10 minutes, an alarm will be raised.

By default, the alarm threshold is activated for 5 satellites and a duration of 10 minutes.

4.5.4. ALS162

Activate the ALS synchronisation with the button ON.

⚠ **This synchronisation is only available if Netsilon is equipped with the current loop option card.**

1) Click on ⚙ to modify the distance from the Allouis transmitter. The following window opens:

GPS coordinates of the Allouis transmitter:

Latitude: 47°10’10.7’’N
Longitude: 2°12’16.7’’E

* This distance is the shortest path between two points. The default value is 228 km. Check various internet pages to determine the distance between your Netsilon and the Allouis transmitter.

The distance from the Allouis transmitter is used to compensate the propagation time (approx. 1 ms for 300 km).

It switches to holdover only after five consecutive bad frames (the status of the ALS162 source will also change to not available.)

📖 **During ALS maintenance (every Tuesday morning between 8:00 and 12:00 maximum), one or more Holdover alarms may occur (as well as possible source changes).**

4.6 NTP

4.6.1. NTP service

To enable the NTP service, proceed as follows:

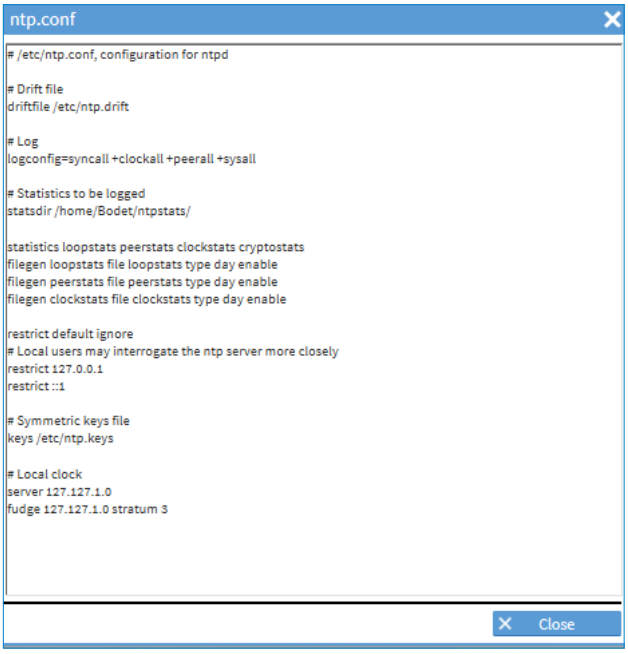
1) TIME menu > NTP > NTP service

1 Service ON/OFF button.

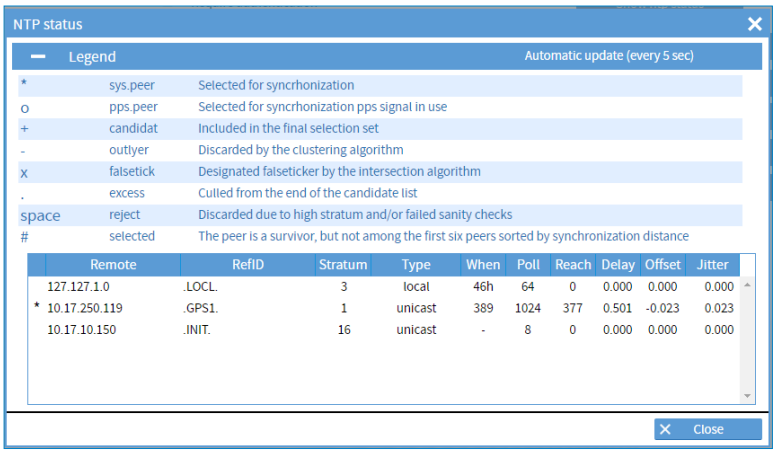
2 Tick this box to query the NTP server remotely. Authorisation of mode 6 and 7 NTP packets (remote information queries).

3 Tick 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):



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



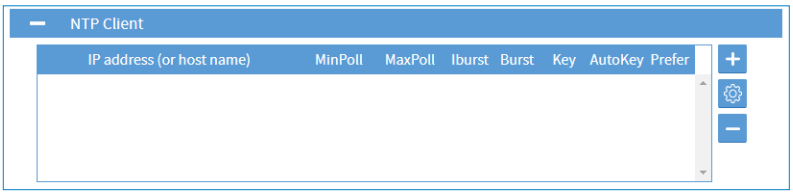
To obtain the details of a parameter, hover over the text with the PC mouse.

4.6.2. NTP client

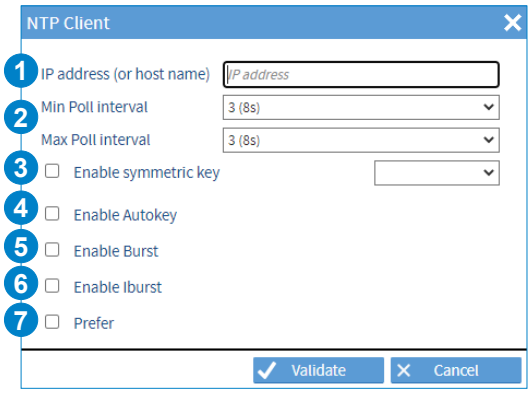
In client mode: NTP synchronises in unicast.

To add an NTP synchronisation source, follow these steps:

1) TIME menu > NTP > NTP client:



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



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.
  - 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.

This option is recommended, as it enables the rapid provision of an active NTP service.

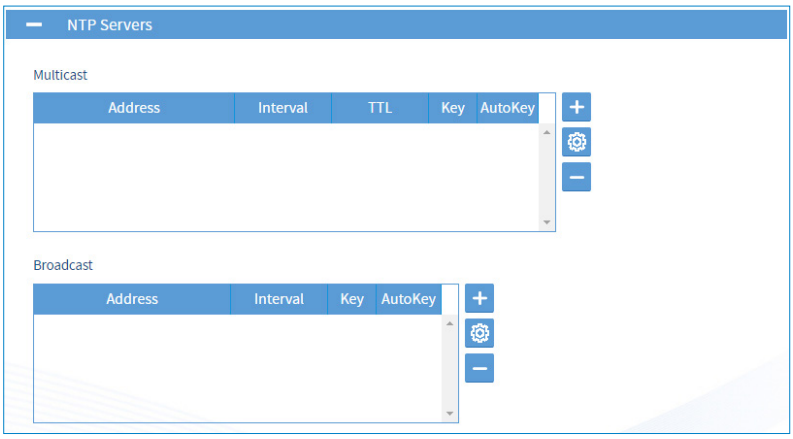
7 This parameter takes stratum N-1 servers as a reference base. This value can apply to a reference source such as GPS. If this option is ticked for Netsilon, the user assumes that this server is stable and nearby, and that it serves as a priority reference.

4.6.3. NTP servers

In server mode: NTP transmits the time in multicast or broadcast.

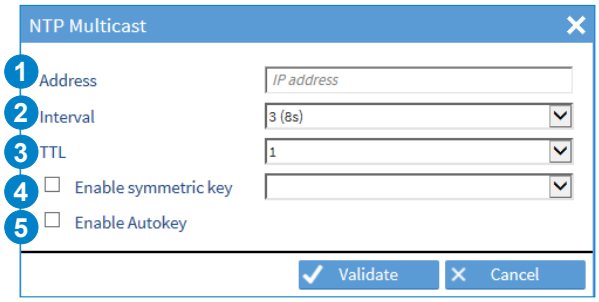
To enable NTP Servers mode, follow these steps:

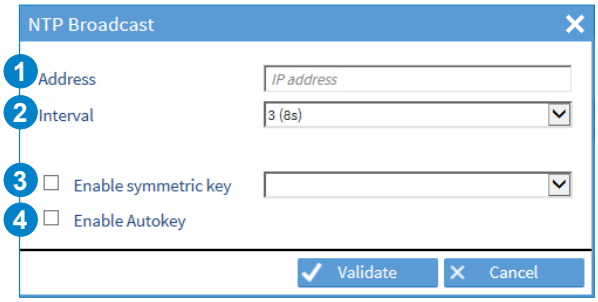
1) TIME menu > NTP > NTP servers:



2) Select the communication mode: multicast or broadcast.

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





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.
  - 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 should be retained, or the time during which a data item should be cached.
The initial value of 1 is used for some protocols to ensure that the packets are not routed beyond a segment.

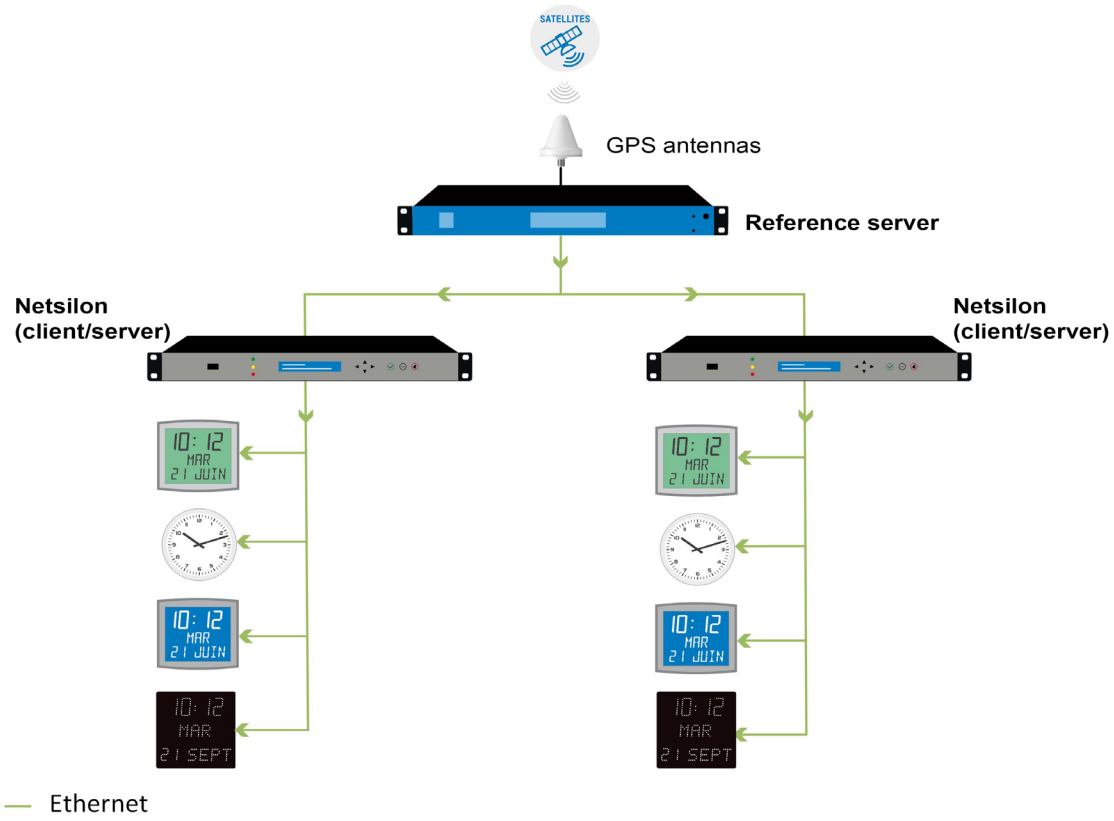
4 Before enabling this parameter, enter the autokey.

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.

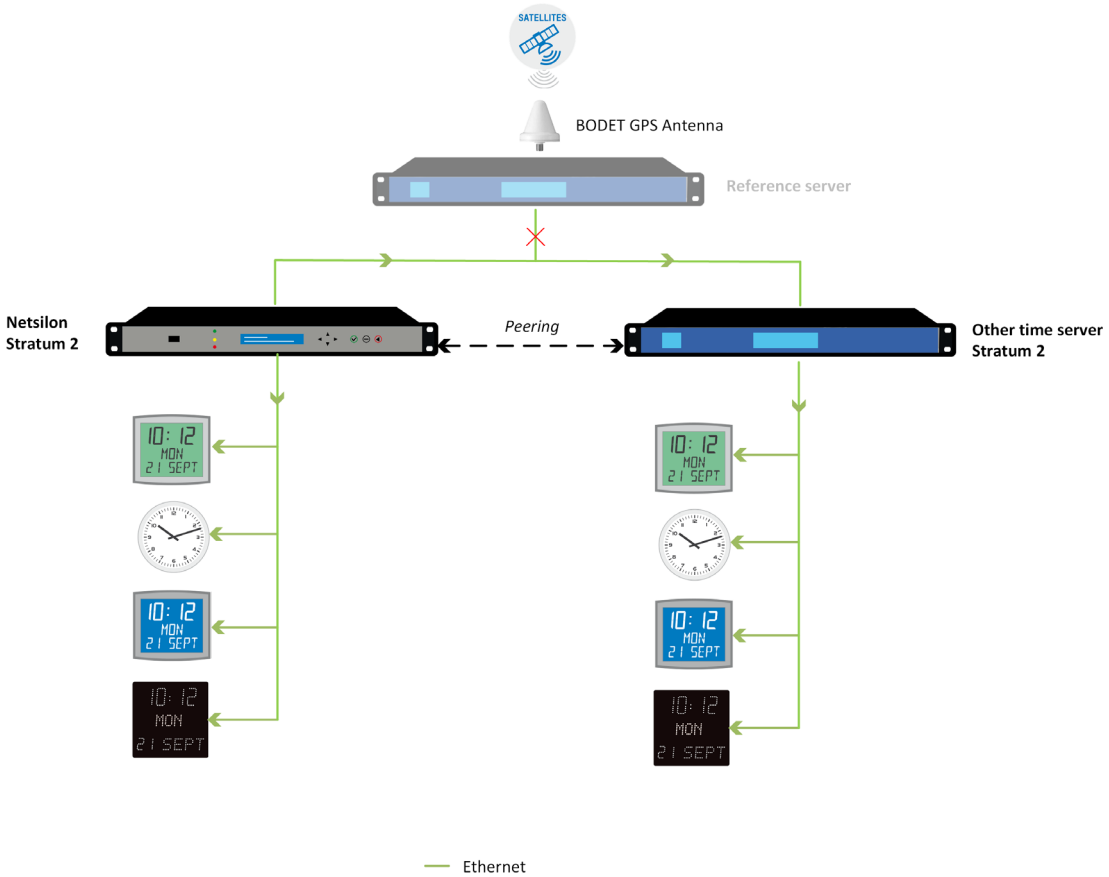
4.6.4. NTP peers

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 achieve identical synchronisation.

Scenario 1: the reference server transmits the time signal

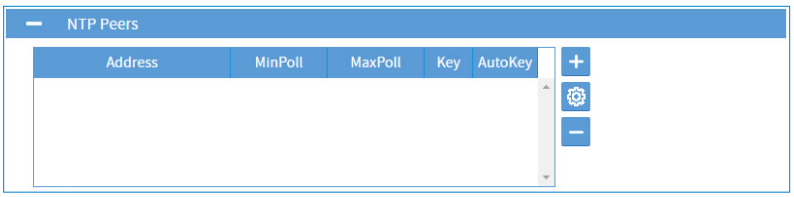


Scenario 2: the reference server no longer transmits the time signal, the third-party device synchronises on Netsilon or vice versa:

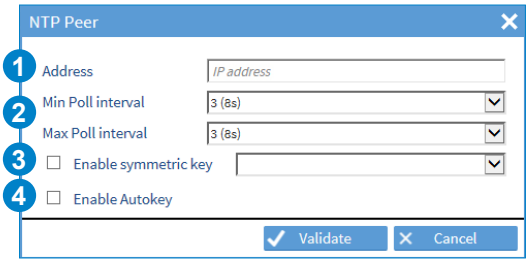


To enable NTP peers mode, follow these steps:

1) TIME menu > NTP > NTP peers:



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



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.

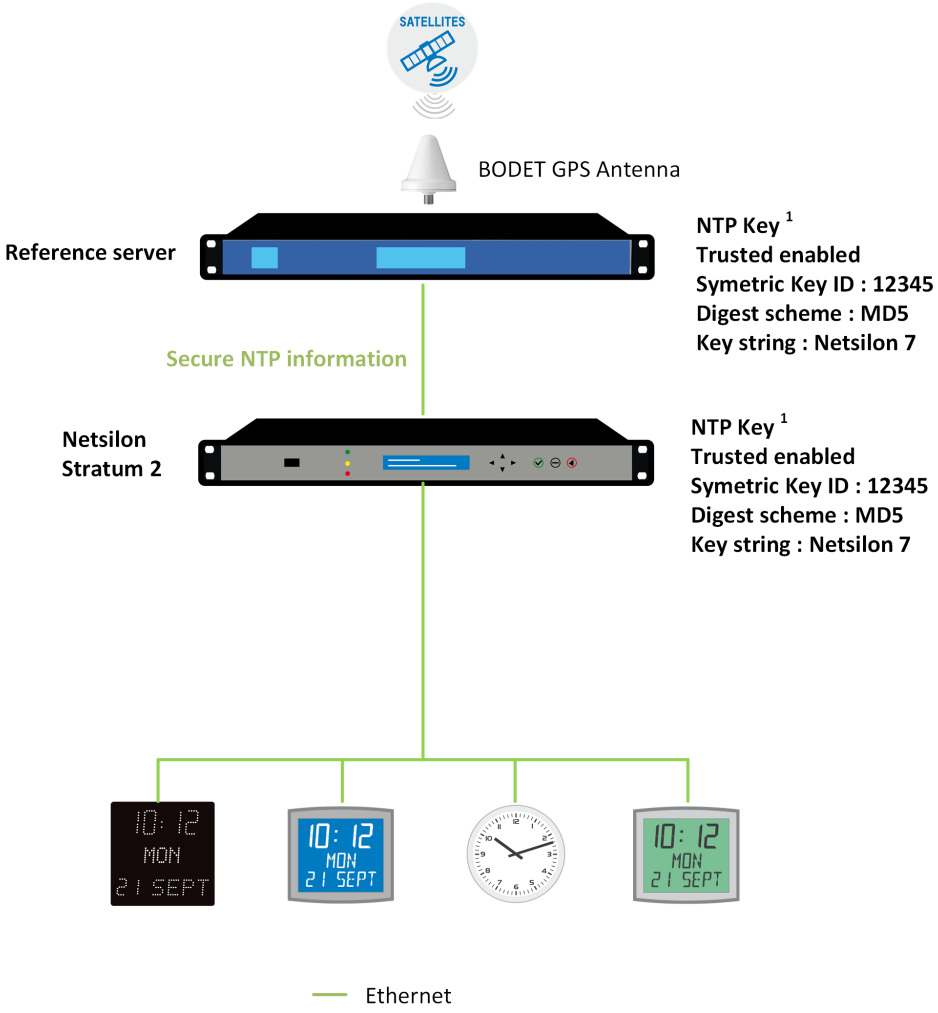
- Chosen range:
  - Automatic.
  - 3 (8 seconds) to 17 (36 hours 24 minutes and 32 seconds).

3 Values: 1, 32, 64, 96, 128, 160,192 and 224. TTL indicates the time during which a data item should be retained, or the time during which a data item should be cached.
The initial value of 1 is used for 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

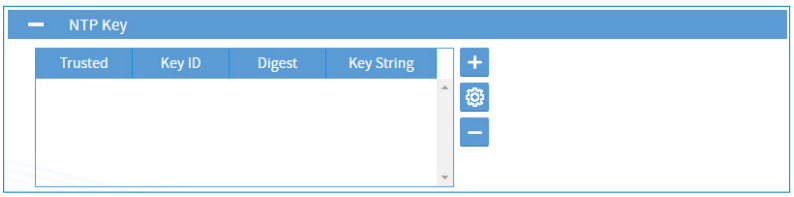
The NTP key enables secure communication between a server and an NTP client, in order to prevent intrusion by a third-party server.



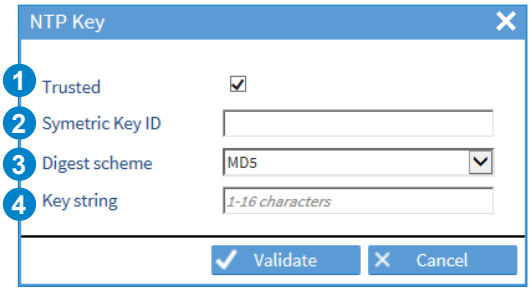
[1] **Refer to the following page for details of the parameters**

To enable NTP key mode, follow these steps:

1) TIME menu > NTP > NTP key:



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



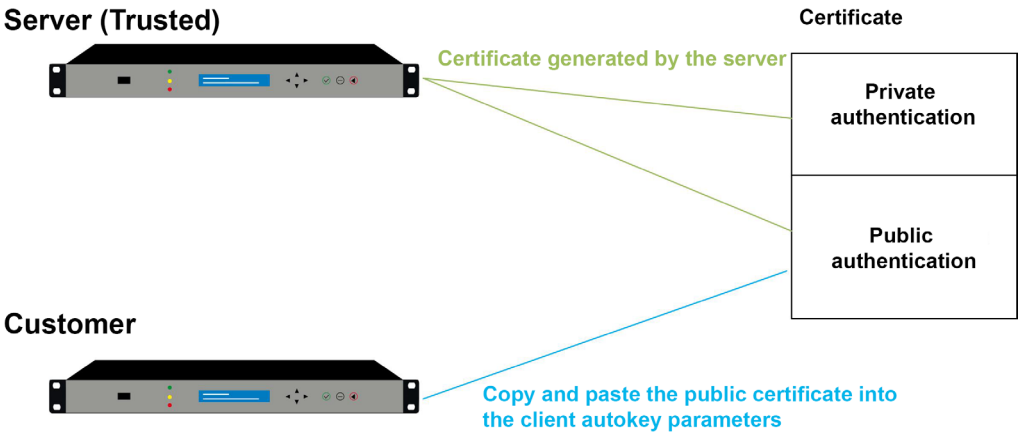
1 Tick this box to use authentication with a trusted key (by default, the NTP service only acknowledges trusted keys). The principle involves assigning and checking if the key for each network device intended to communicate with Netsilon is correct.

2 Enter a number between 1 and 65534. Netsilon supports MD5 authentication by default. This function assigns an authenticator, composed 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 (special and non-alphabetic characters not permitted). E.g: !, $, #, %)

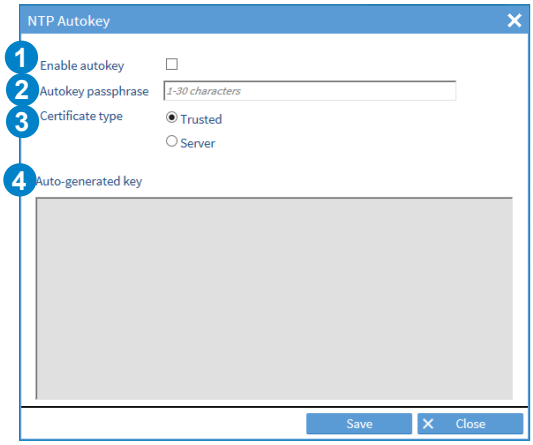


Remember that the devices must have different hostnames.

To enable NTP autokey mode, follow these steps:

1) TIME menu > NTP > NTP Autokey:

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



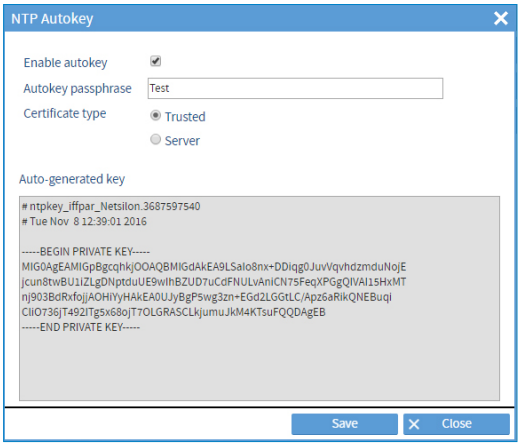
1 Tick the box to enable and define the autokey.

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

3 Before a server can be designated as a client or 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 into the NTP Autokey parameters of the client servers.

Example:



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

4.6.7. NTP-Anycast

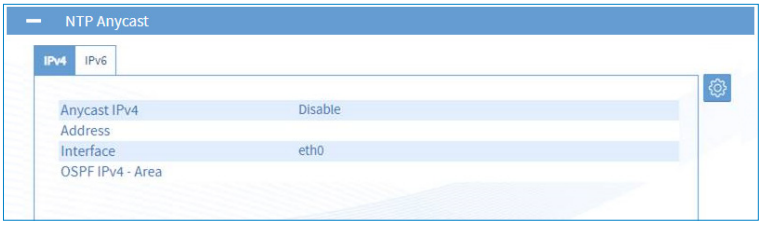
Anycast is applied to the NTP protocol to establish reliable communication between client and server (server redundancy).

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

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

To activate the NTP-Anycast mode, follow these steps:

1) TIME menu > NTP > NTP-Anycast:



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

2) Click on , the following window opens:

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 that handles the Anycast. (The IPv4 address is used as router-ID).

4.7 Time distribution

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.

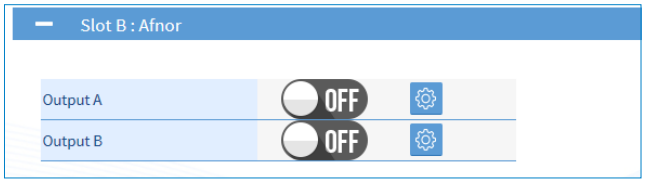
4.7.1. AFNOR option card (ref. 907940)

The AFNOR option card enables wired time distribution (AFNOR / IRIB B 127 standard) or by DHF using the DHF transmitter.

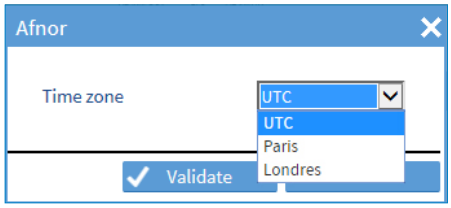
The 2 outputs can transmit a different time (different time zone).

To configure the AFNOR output, follow these steps:

1) TIME menu > Outputs > Slot B: Afnor:



2) Configure an output by clicking on ⚙, and the following window will appear:



3) Select the time zone which will be transmitted via output A and/or B of the AFNOR option card.

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

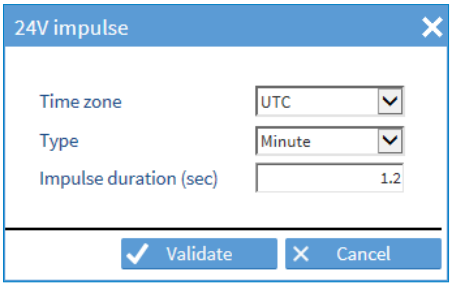
4.7.2. *IMPULSE option card (ref. 907942)*

The IMPULSE option card enables wired time distribution by sending impulses every minute or ½ minute at 24VDC parallel.

To configure the IMPULSE output, follow these steps:

1) TIME menu > Outputs > Slot D: 24V impulse:

2) Configure the output by clicking on , and the following window will appear:



3) Select the time zone which will be transmitted on the IMPULSE option card output.

4) Select the impulse type: Minute or ½ minute.

5) Set the impulse duration in seconds.

6) Enable the output using the ON button, then save.

The button can be used to configure the dial time[1] and its polarity (negative or positive).

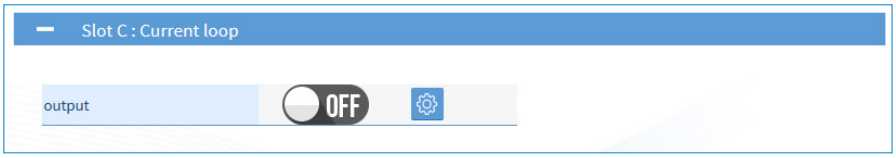
[1] *The dial time is the reference time on which the network clocks are positioned before commissioning or during a time reset.*

4.7.3. CURRENT LOOP option card (ref. 907944)

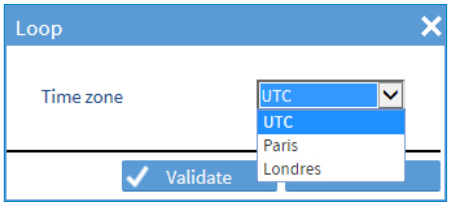
The Current Loop option card can be used to distribute time by radio (DCF) via current loop.

To configure the Current Loop output, follow these steps:

1) TIME menu > Outputs > Slot C: Current Loop:



2) Configure the output by clicking on , and the following window will appear:

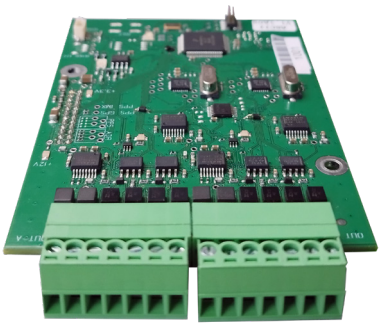


3) Select the time zone which will be transmitted on the Current Loop option card output.

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

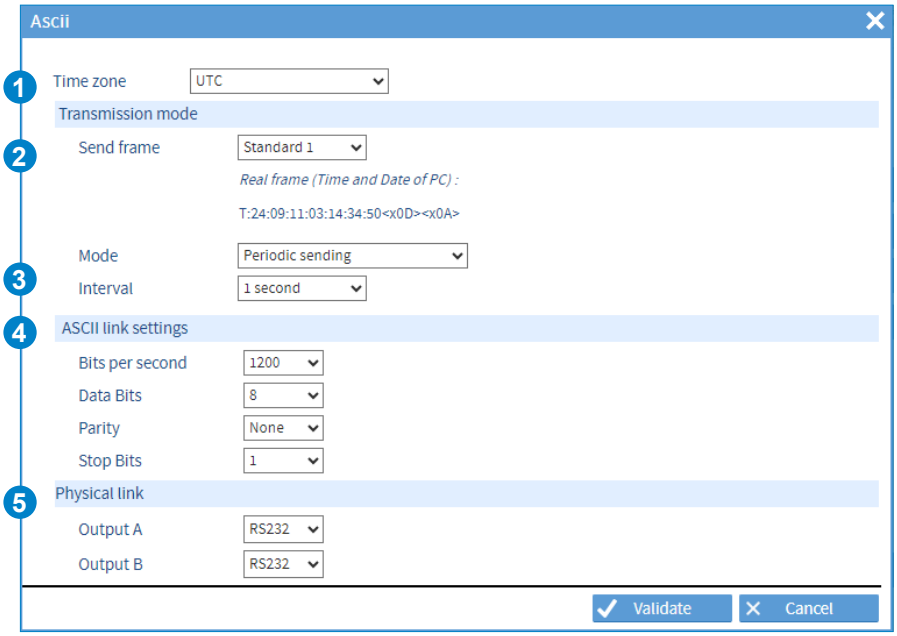
4.7.4. ASCII option card (ref: 907926)

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:


Output A Output B

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

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



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.

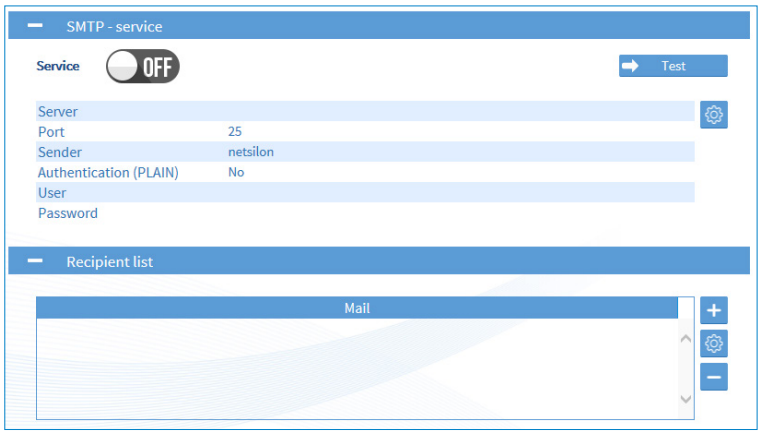
	Content of the message	Example
Standard 1	T:YY:MM:DD:ND:HH:MM:SS “x0D””x0A”	T:08:10:09:04:15:12:30<CR><LF>
Standard 2	“x02” 00 DoW DD/MM/YY HH:MM:SS “0D”	02 00 Thu 09/10/08 15:12:30<CR>
ZDA GGA GPS simulation	$GPZDA,HHMMSS.00,DD,MM,YYYY,00,00*”checksum””x0D””x0A” $GPGGA,HHMMSS.000,0000.0000,N,00000.0000,W,1,12,0.00,000.0,M,00.0,M,,*”checksum””x0D””x0A”	$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 Management of notifications

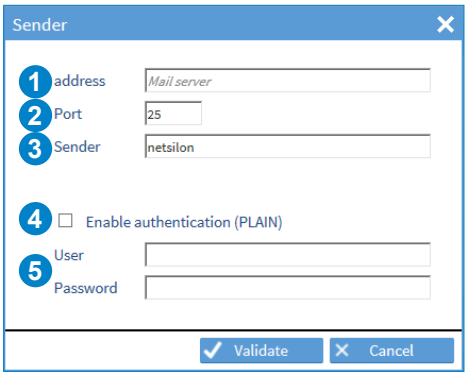
4.8.1. SMTP configuration

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



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:



1 Enter the IP address (or DNS name) of the receiving server (50 characters maximum).

2 Enter the communication port. Port: 5 digits (65535 maximum on validation).

3 Enter the name of the sender of the e-mails. i.e. the name given to the Netsilon device.

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

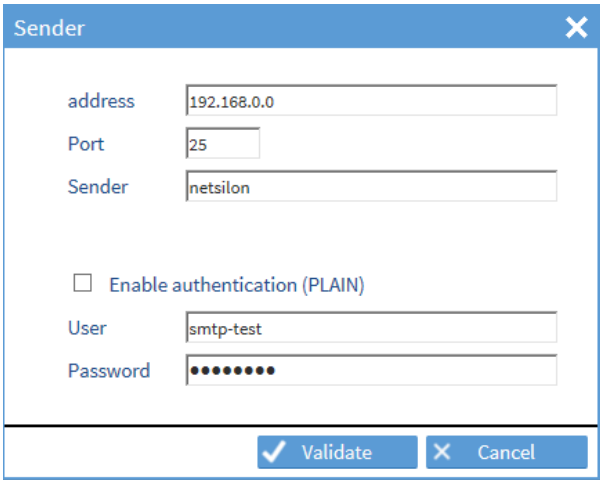
5 Enter user parameters. (Username/password: 50 characters maximum).

Refer to the next page to see a configuration example.

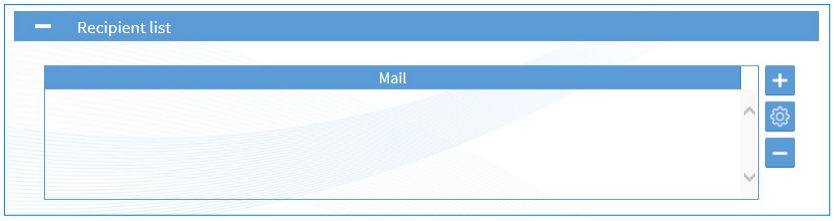
Configuration example:

1) Enter the sender's parameters:

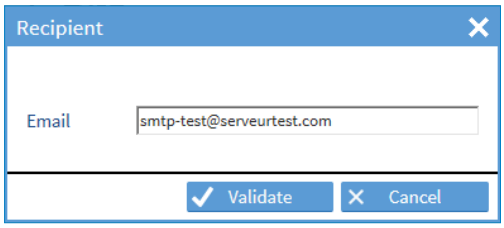
SMTP SERVER		
IP address of the SMTP server	192.168.1.254	
Port	**25**	
Users	**e-mail**	**Password**
Admin	admin@serveurtest.com	testservice
smtp-test	**smtp-test@serveurtest.com**	**testservice**
netsilon1	netsilon1@serveurtest.com	testservice



2) Enter the list of recipients:
(Maximum number of recipients: 5)



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

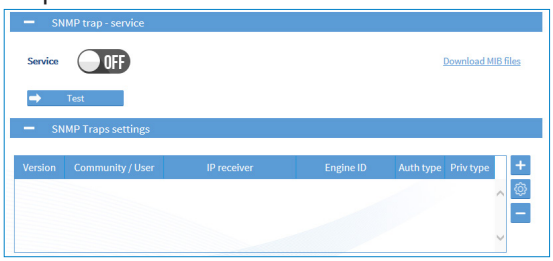


4) Enable the service using the ON button, then save.

4.8.2. SNMP trap Configuration

To configure trap receipt, follow these steps:

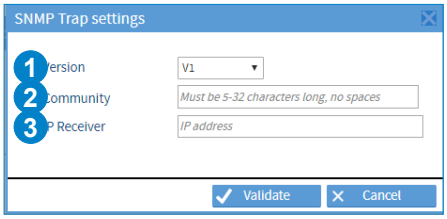
1) NOTIFICATION menu > SNMP trap:



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

v1 or v2c version:
(5 accounts maximum)

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



1 Select the supported SNMP version: v1, v2C or v3.

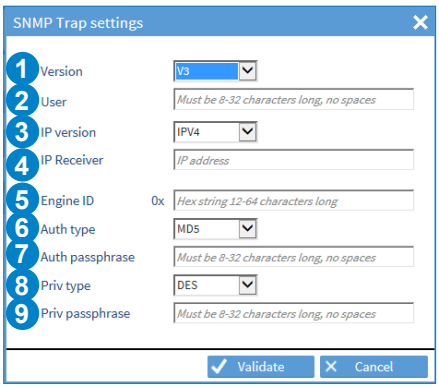
2 Enter a community name between 5 and 32 characters, without spaces.

3 Enter the IP address of the trap destination server.

3) Click on Validate .

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

v3 version:
(5 accounts maximum)



1 3 4 See above.

2 Enter the name of the user (between 8 and 32 characters without 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.

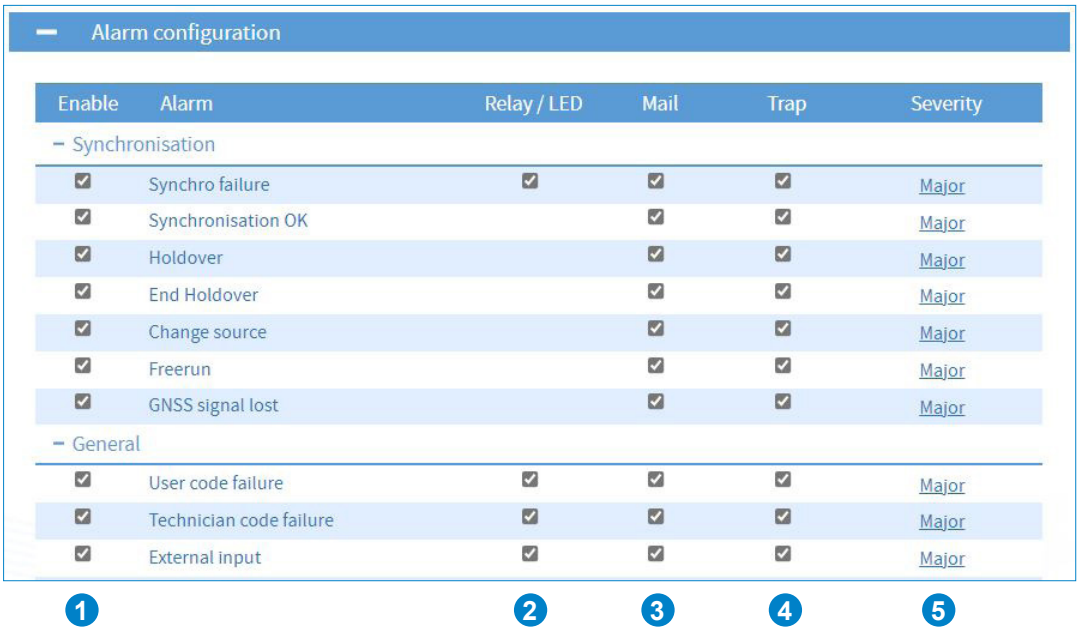
8 Select the encryption type (DES or AES128) or no encryption (NoPriv).

9 Enter the encryption passphrase.

4.8.3. *Configuration of alarms*

To define the notification mode and criticality of alarms, follow these steps:

1) NOTIFICATION menu > Alarms:



1 Tick the box to enable alarm selection.

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

3 Tick the box for the alarm to be sent by e-mail (see chapter **4.8.1 SMTP configuration**).

4 Tick the box for the alarm to be sent in trap format (see chapter **4.8.2 SNMP trap configuration**).

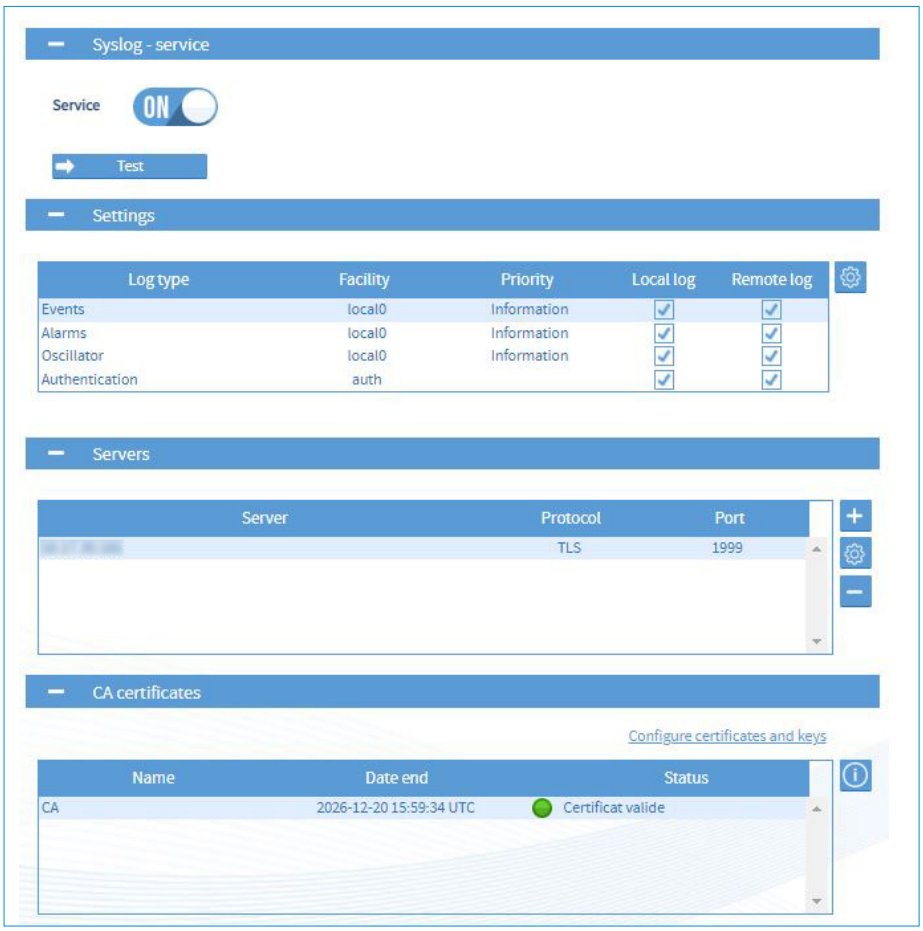
5 Choosing the alarm criticality level: minor, major or critical.

Alarms are monitored and acknowledged in the history section, see chapter 4.11.7 Alarm history.

4.8.4. *Syslog Configuration*

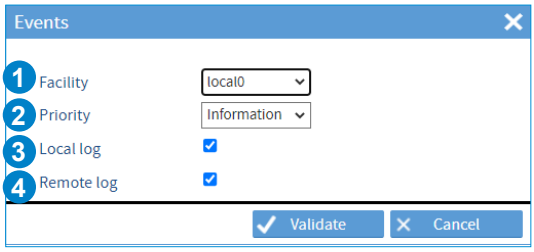
To configure the Syslog service, follow these steps:

1) NOTIFICATION Menu > Syslog:
2) Enable the service using the ON button.



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 (Event, Alarms, Oscillator, Authentication),
select it then click on ⚙, the following window will appear:



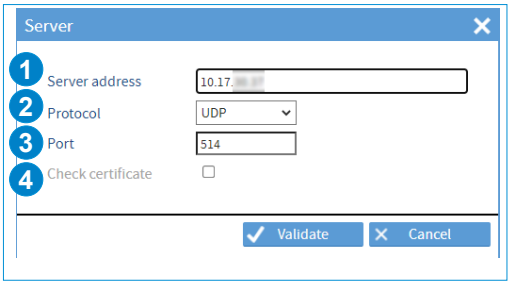
1. Choose a category for the type of message / system that caused the event (Free local use).
   For «Auth» the facility option is not adjustable because it is standardised by the Syslog protocol.

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 need to be added.

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



1 Enter the address or the hostname of the Syslog server.

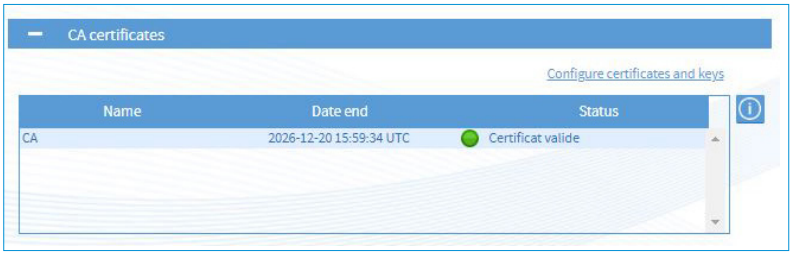
2 Choose the client / server communication protocol (UDP / TCP / TLS).

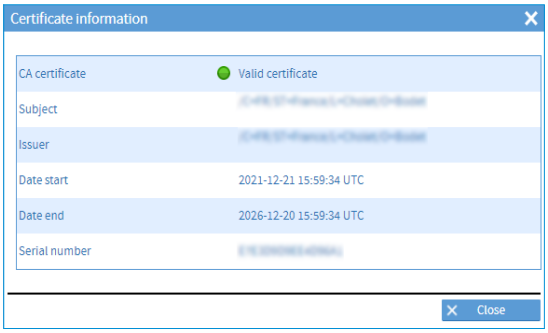
3 Enter the network port.

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 4.9 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.



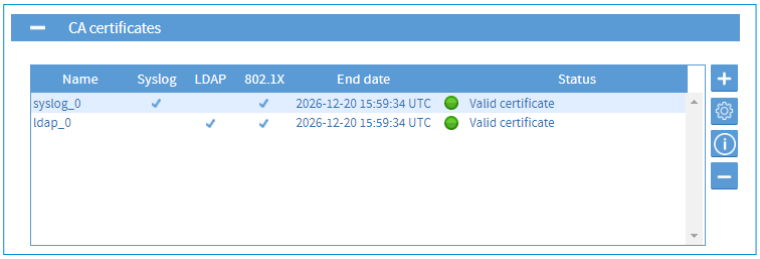


4.9 Certificate and key management

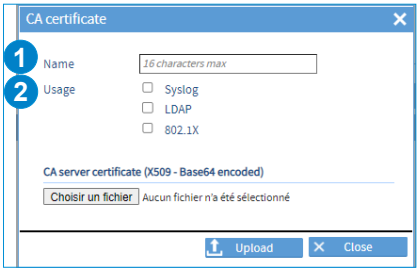
This menu allows certificates and public keys importation in Netsilon.

4.9.1. Importing CA certificates

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



2) Click on +, a window opens:

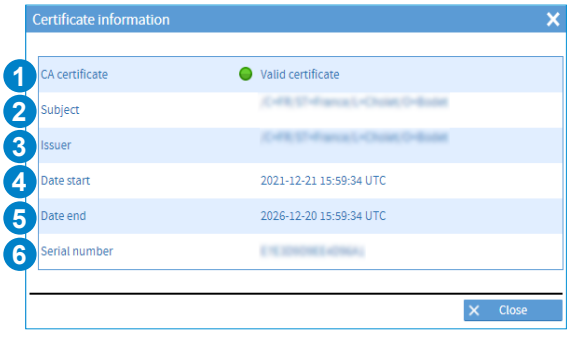


1. Enter a certificate name (16 characters maximum).
2. Select the use cases of the certificate: Syslog, LDAP, 802.1x (TLS, TTLS, PEAP).

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

The certificates must be in X.509 Base64 format. As a reminder, a 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.

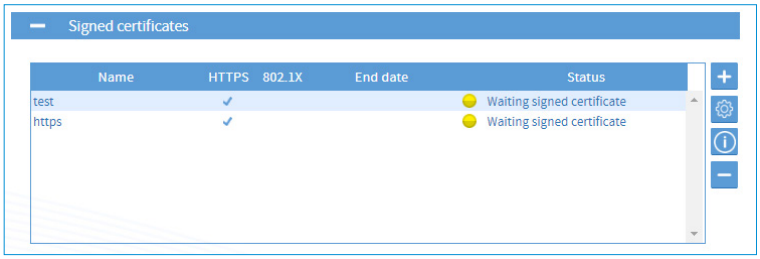
4) Click on ⓘ to see the information of the imported certificate:



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.

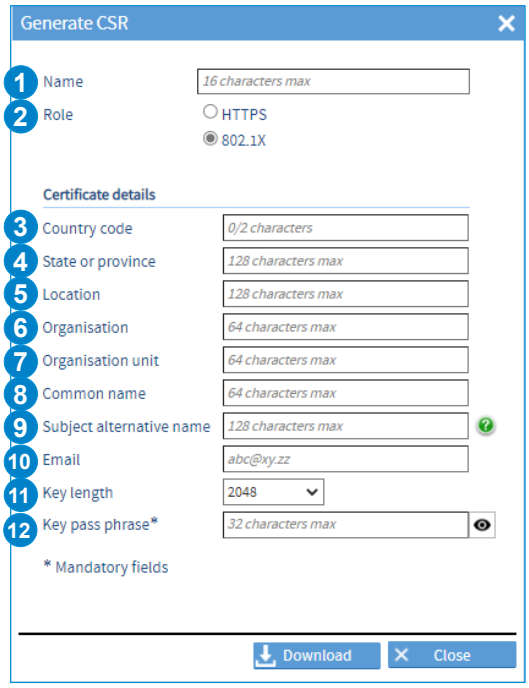
4.9.2. *Importing signed certificates*

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



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 in Netsilon. It is not possible to import a private key directly.

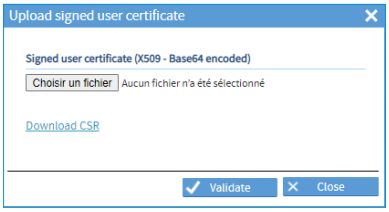
2) Click on + to generate a CSR, a window opens:



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.

4) Import in Netsilon the signed certificate corresponding to the CSR issued by clicking on ⚙, A window opens:

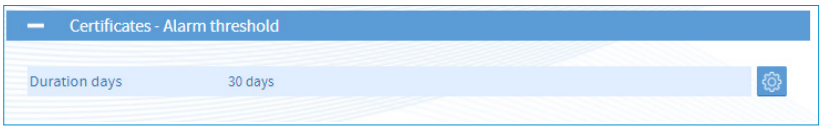


The certificates must be in X.509 Base64 format. As a reminder, a X.509 format certificate begins with «---BEGIN CERTIFICATE---» and ends with «---END CERTIFICATE---».
The number of signed certificates is limited to 20.

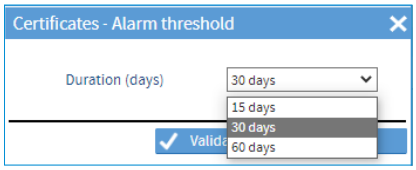
5) Click on ⓘ to see the information of the imported certificate.

4.9.3. 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



2) Click on ⚙, a window opens:

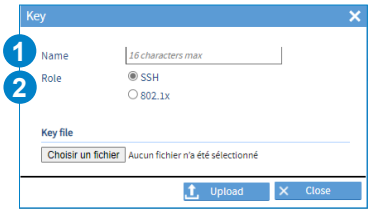


3) Select the time before the certificate expires for an alarm to be displayed.

4.9.4. Importing public keys

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

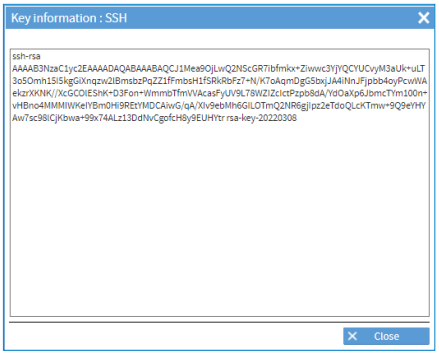
2) Click on + to add a public key, a window opens:



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:



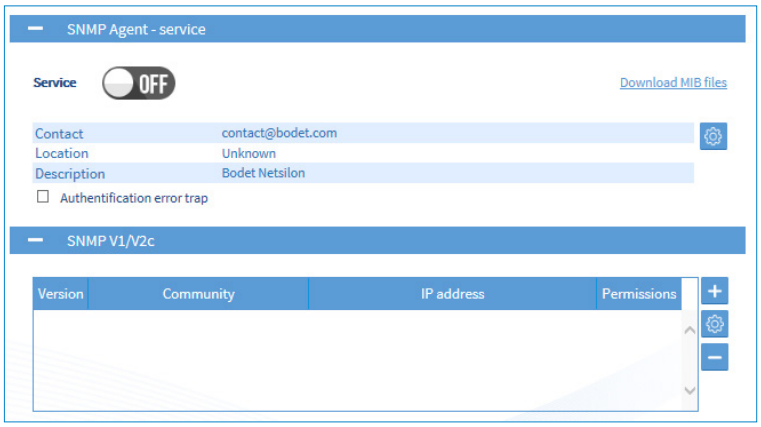
The number of keys is limited to 20.

4.10 System supervision

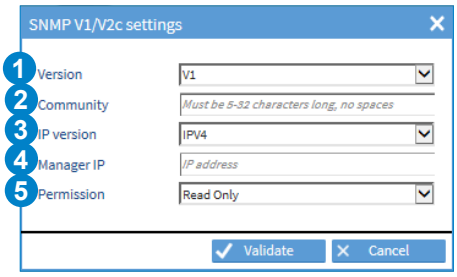
4.10.1. SNMP agent

› ENABLING THE SNMP AGENT (E.G. V1)

1) SECURITY menu > SNMP agent:



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



1 Select the SNMP version.

2 Enter a community name between 5 and 32 characters, without spaces.

3 Select the IP communication version: IPV4.

4 Enter the IP address of the server.

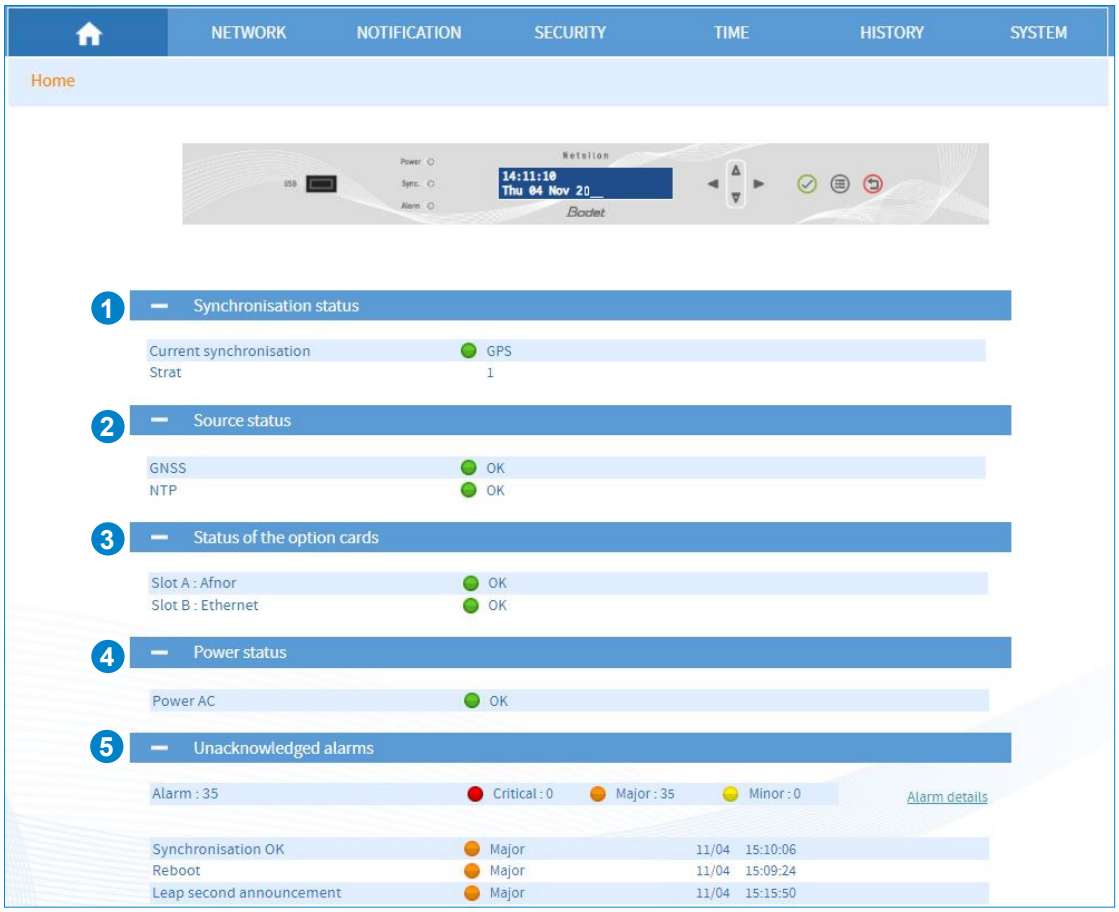
5 Choose the permission level: read only or read/write.

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

4.11 System monitoring

4.11.1. Home page

The home page is a consultation page:



1 This menu shows the status of the synchronisation in progress:

› Status of the synchronisation in progress:

› Green = synchronisation OK

› Red = no synchronisation

› The synchronisation source used: GPS, GLONASS, NTP, ALS162.

› The stratum level: level in relation to the synchronisation source (satellite).

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 inputs on the product.

3 This menu shows 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 shows the power supply status:

› The name of the power supply (AC power supply, DC power supply, AC+DC power supply, AC+AC power supply) as well as a colour for the status:

- Green = power supply OK.
- Red (in the case of double 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 shows the list of alarms requiring acknowledgement by the user.

› The link provides details of the alarms (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.

4.11.2. GNSS statistics

To view Netsilon GNSS (GPS or GLONASS) synchronisation statistics, follow these steps:

1) HISTORY menu > GNSS statistics.

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

1 The GNSS reception (GPS or GLONASS according to the connected antenna) status is symbolised by two status levels:

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

2 Graph showing the number of satellites detected according to the time. Signal reception quality is indicated by three different colours:

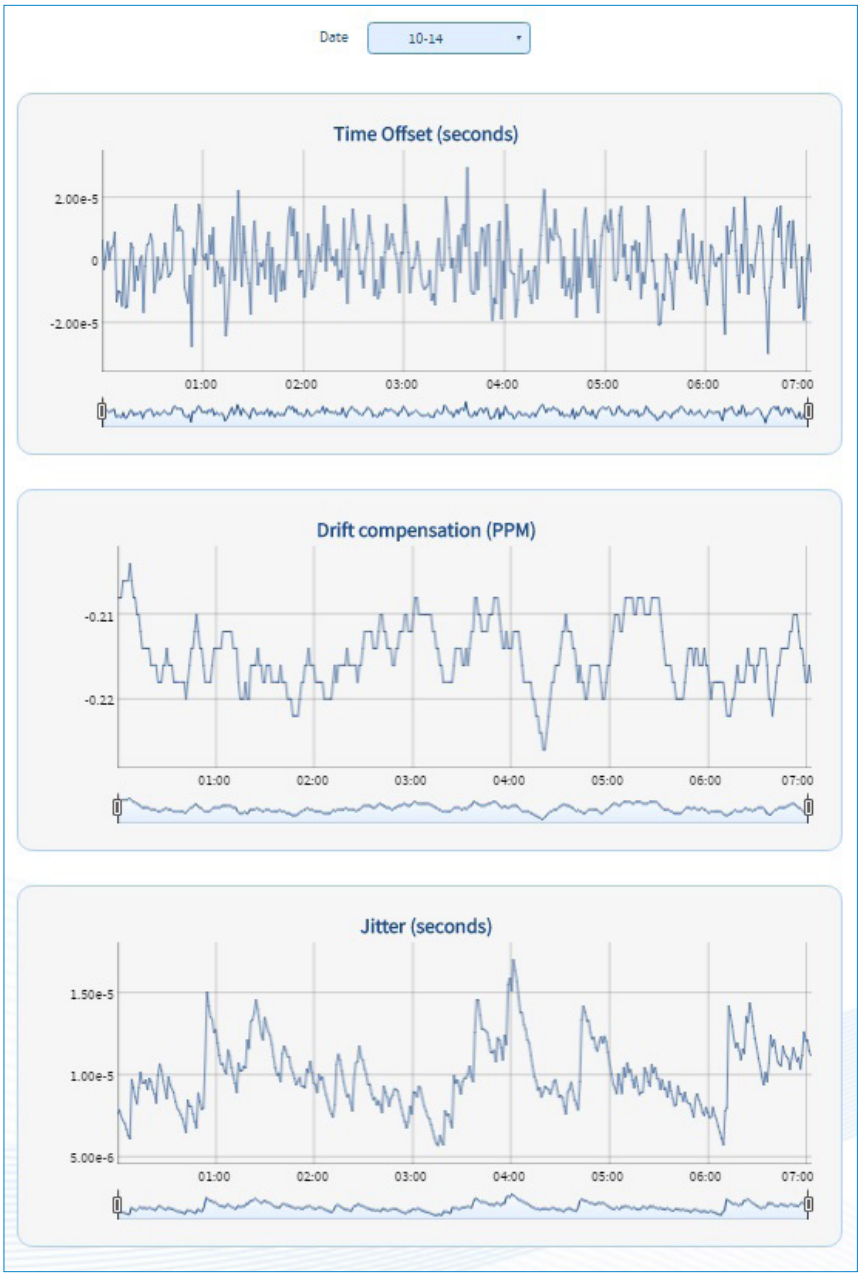
- Red: 0 to 2 satellites – no reception or poor reception quality.
- Orange: 2 to 4 satellites – moderate reception quality.
- Green: 4 to 12 or more satellites – good reception quality.

4.11.3. NTP statistics

To view Netsilon NTP synchronisation statistics, follow these steps:

1) HISTORY menu > NTP statistics.

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



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

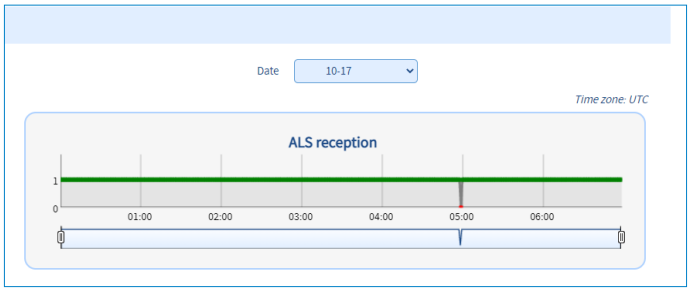
2 Drift compensation: gradual correction of the Netsilon oscillator in relation to the source. The idea is to move closer to the synchronisation source in a gradual manner (without any time jump).

3 Jitter: offset of the source around the reference.

4.11.4. ALS162 Statistics

To view the Netsilon ALS162 statistics, follow the step below:

1) HISTORY menu > ALS162 Statistics:



The status of the ALS162 reception is symbolised by two states:

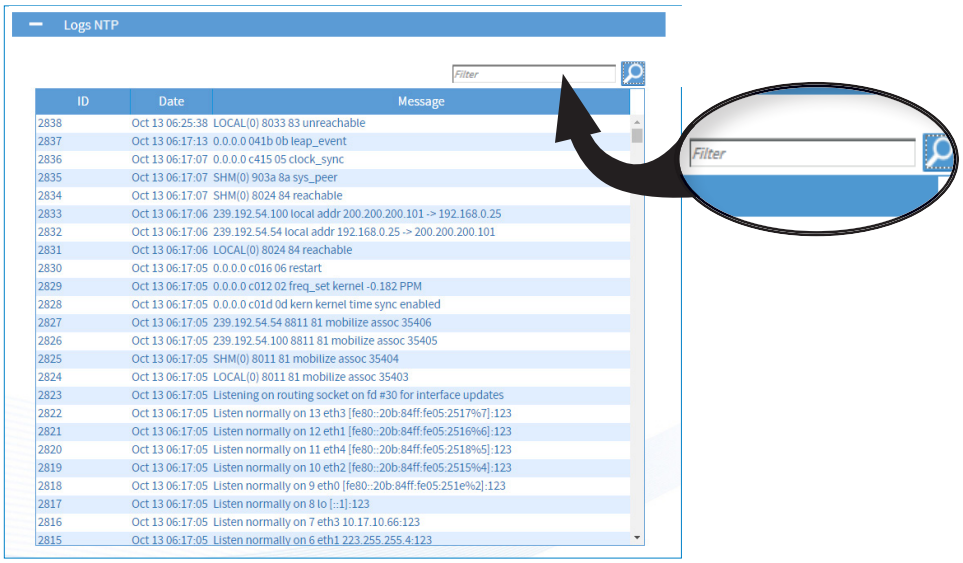
> 0: reception of a signal but no synchronisation.

> 1: reception of the signal ok.

4.11.5. NTP log

To view Netsilon NTP logs, proceed as follows:

1) HISTORY menu > NTP logs:

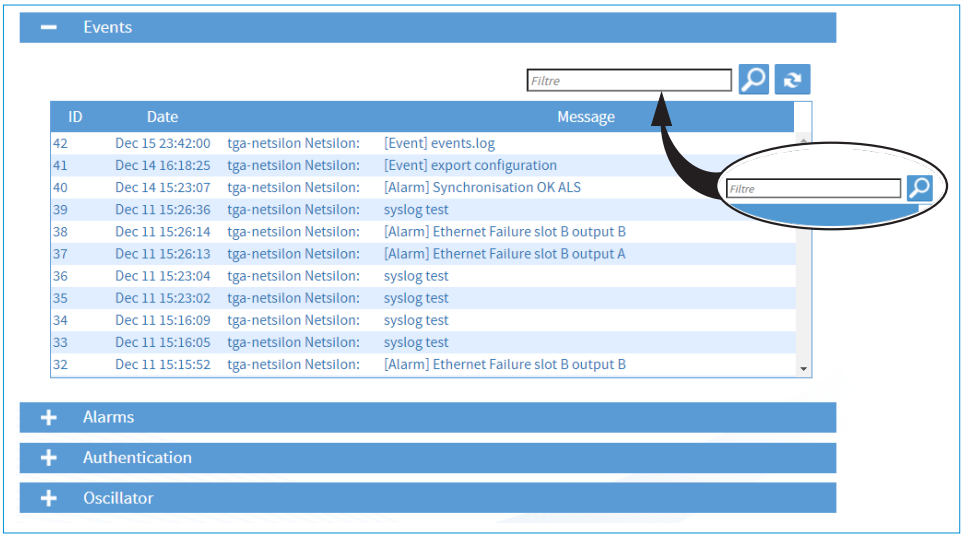


This log contains saved information. It is a standard log generated by the NTP protocol.

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

4.11.6. Syslog Log

To view the Syslog log, follow these steps:
1) HISTORY Menu > Syslog logs

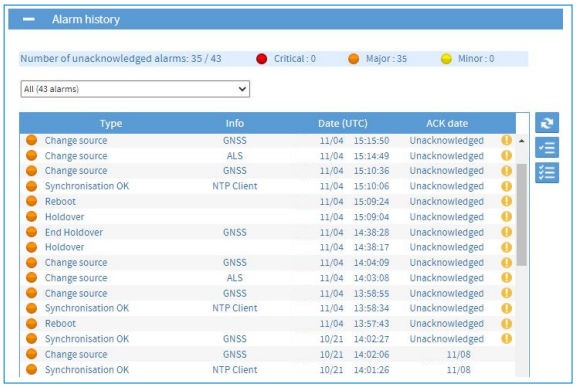


This log is a feedback for each type of log. It is a standard log generated by the Syslog protocol.

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

4.11.7. Alarm history

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

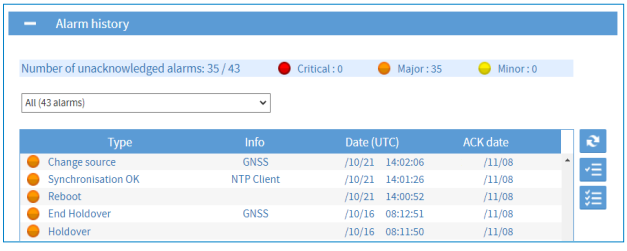


› To refresh this list, click on .

› There are two ways to acknowledge the alarms:
- individually by selecting one alarm and clicking on :
- all alarms at once by clicking on .

› Confirm by clicking on «Yes»

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



The Reboot alarm is sent approx. 10 seconds after the reboot to allow time to establish the network.

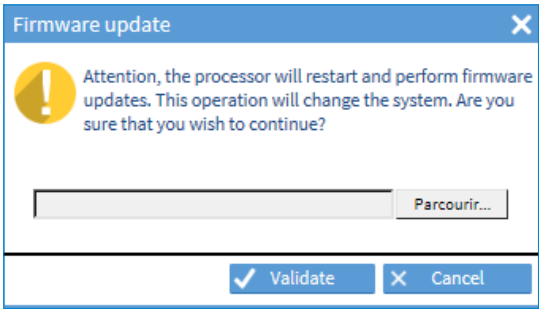
4.12 System tools

4.12.1. Firmware updates

To update the Netsilon firmware, follow these steps:

1) SYSTEM menu > Tools > Upgrade and backup.

2) Click on Update firmware , and the following window will appear for selection of the file to be imported:



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

4.12.2. Loading and saving a configuration

To save a configuration, follow these steps:

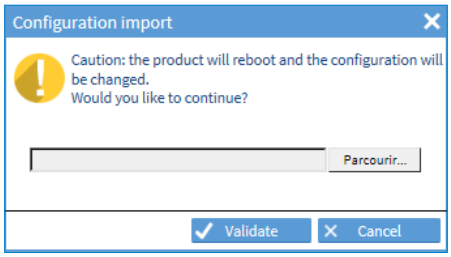
1) SYSTEM menu > Tools > Upgrade and backup.

2) Click on Save configuration , and a file named “export.nets” will download to your PC.

To load a configuration, follow these steps:

1) SYSTEM menu > Tools > Upgrade and backup.

2) Click on Upload configuration , and the following window will appear for selection of the file to be imported:



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.

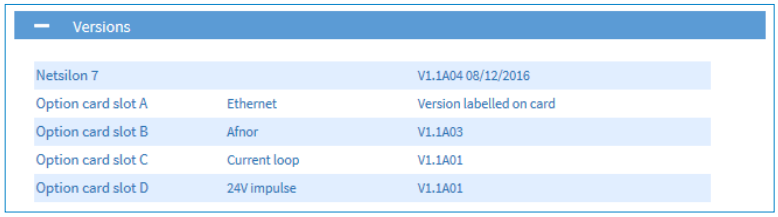
Having previously saved your Netsilon configuration means it is no longer necessary to configure it manually and follow the steps to obtain the same configuration.

To view the saved settings, see Annex 4: saved settings.

4.12.3. Firmware version and online help

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

1) SYSTEM menu > General > Versions:



To access the product manual, proceed as follows:

1) SYSTEM menu > General > Online help:

4.12.4. Firewall

Netsilon has an onboard Firewall with a configuration that changes automatically in line with the services confirmed by the client. Therefore, there is no setup at client level.

Only the corresponding ports for activated services are open.

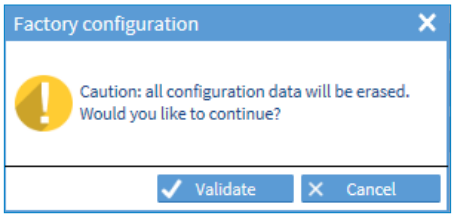
Pings are authorised but are limited to protect against ICMP flood DDoS attacks (request saturation). SSH connections are authorised (if enabled) but are limited to protect against brute force attacks (testing all possible password combinations).

4.12.5. Factory configuration

To reset Netsilon to factory configuration, follow these steps:

1) SYSTEM menu > Tools > Upgrade 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.

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).

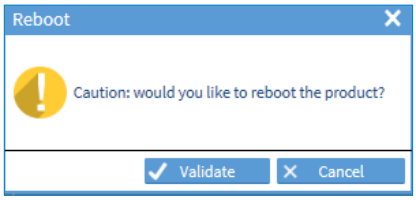
The default configurations are re-established (see chapter **3.1 Factory configuration**)

4.12.6. Restarting or switching off Netsilon

To restart Netsilon, follow these steps:

1) SYSTEM menu > Tools > Reboot > Restart.

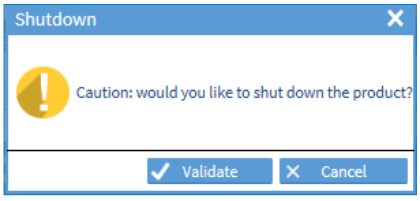
2) Click on Restart, and the window opposite will appear:



To switch off Netsilon, follow these steps:

1) SYSTEM menu > Tools > Reboot > Shut down.

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

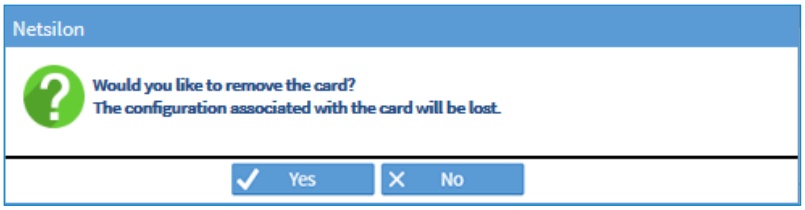


The product is switched off, but the power supply is still on: the green LED POWER light is on and the LCD screen remains in standby mode.

4.12.7. 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:



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

4.12.8. Exporting logs and statistics

To export the Netsilon logs and statistics, follow these steps:
1) SYSTEM menu > Tools > Export logs.
2) Click on the log or the type of desired statistics, a ZIP file containing the log file is uploaded 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):

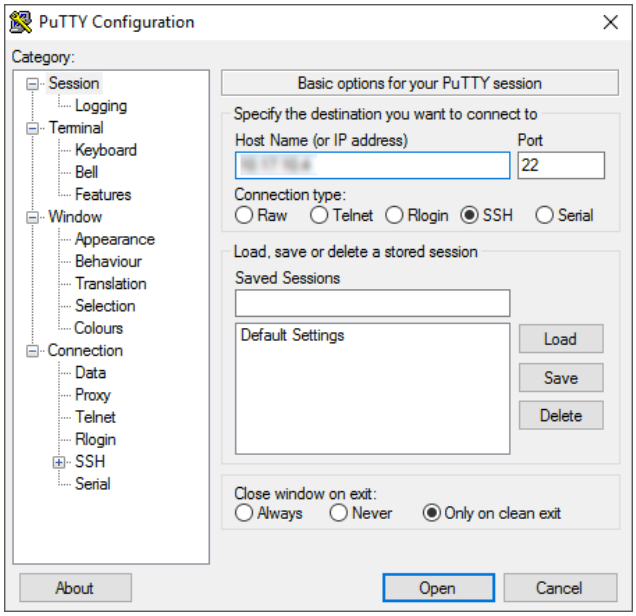
5.1 Authentication by password

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

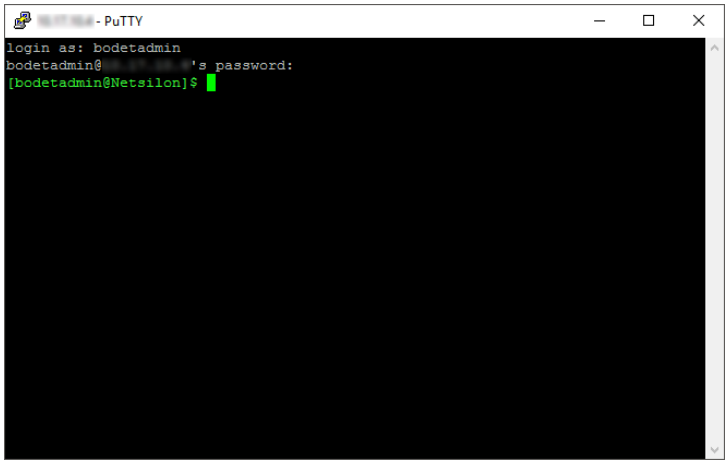
2) Note the IP address of Netsilon 7.

3) Open the program (PuTTY).

4) Enter the IP address.



5) Enter the default ID and password to access the command set. As a reminder:
- › ID: bodetadmin
- › Password: admin49



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

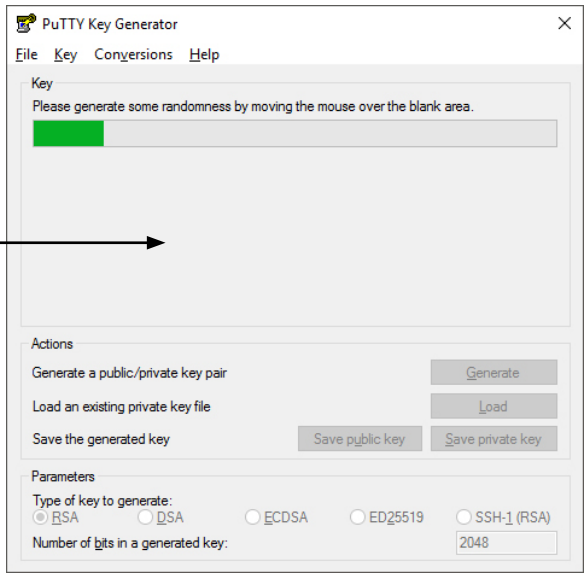
To access the list of command sets, see Annex 5: list of command sets

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 :

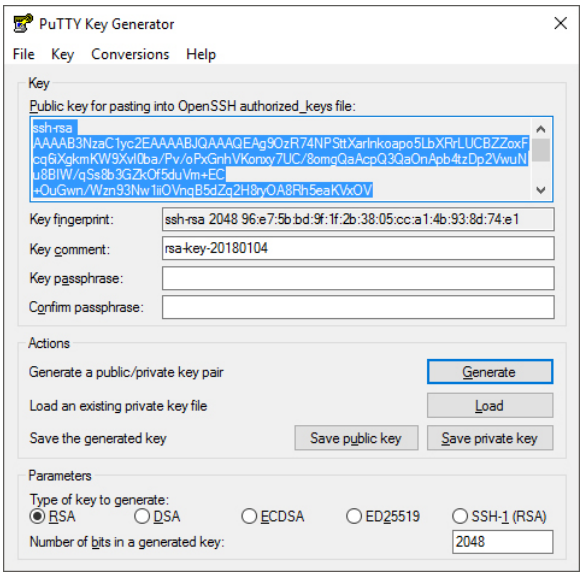
Hover your PC mouse over this space to generate the key



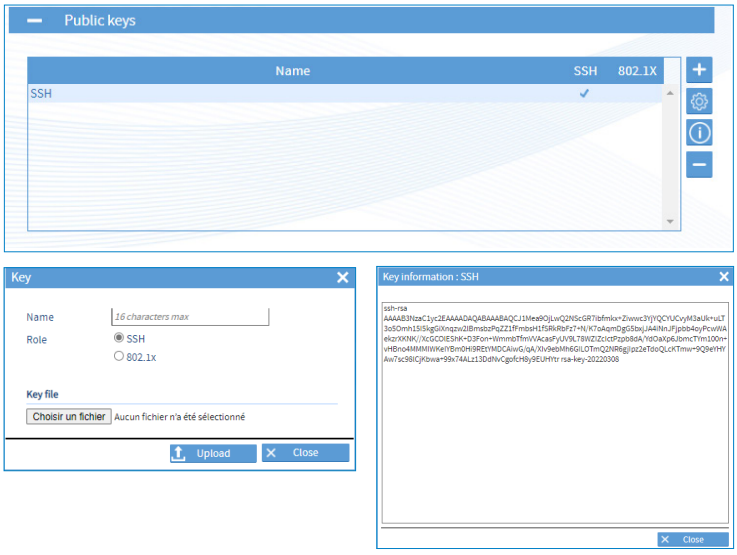
3) Save the public key in a file (.txt type) to be imported in the Certificates and keys menu of Netsilon in the «public keys» tab:

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



Import the public key in Netsilon

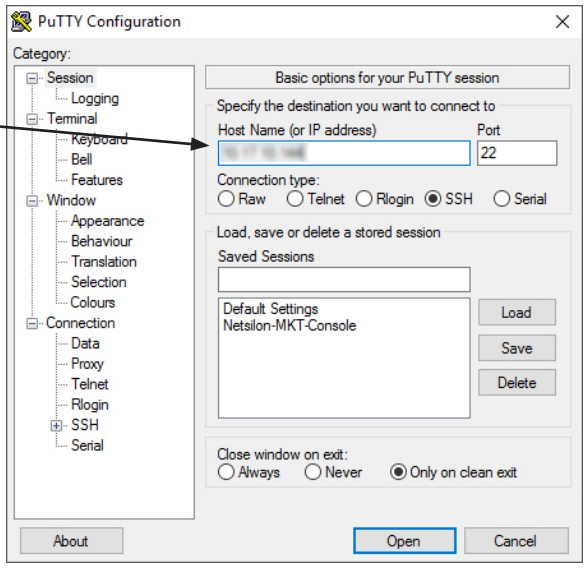


4) Save the private key to your PC.

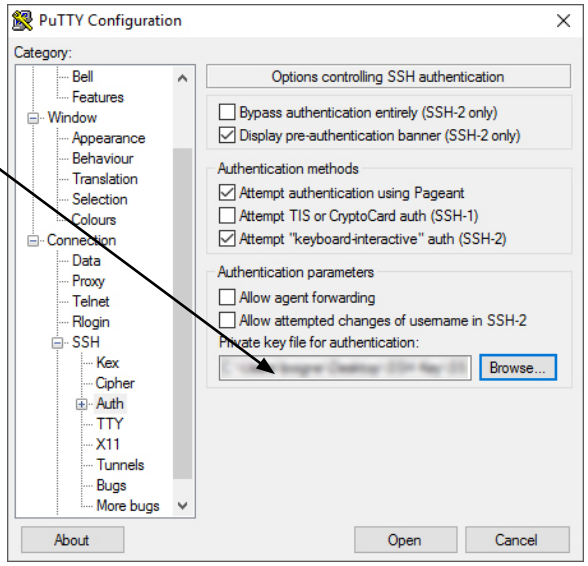
5) Download a program enabling the connection (e.g.: PuTTY).

6) Open the program (PuTTY).

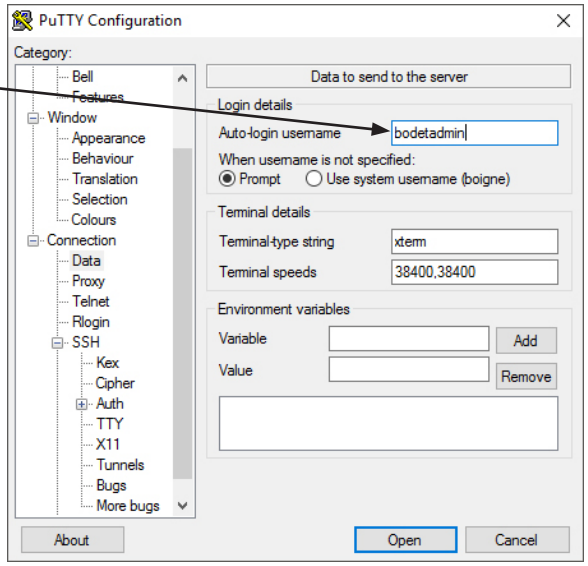
7) Enter the IP address of Netsilon:



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



9) Enter the user:



10) Click on Open, the following window opens:

6. CONFIGURATION BY CONSOLE

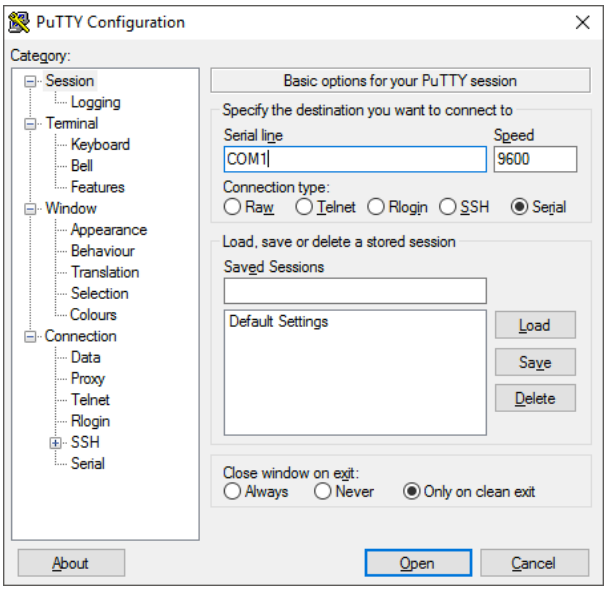
› To access the Netsilon web server, follow these steps (Netsilon must be connected to the PC via its COM serial port).

The physical connection between the PC and Netsilon must be a direct link via an RS232 (DB9) male/female serial cable.

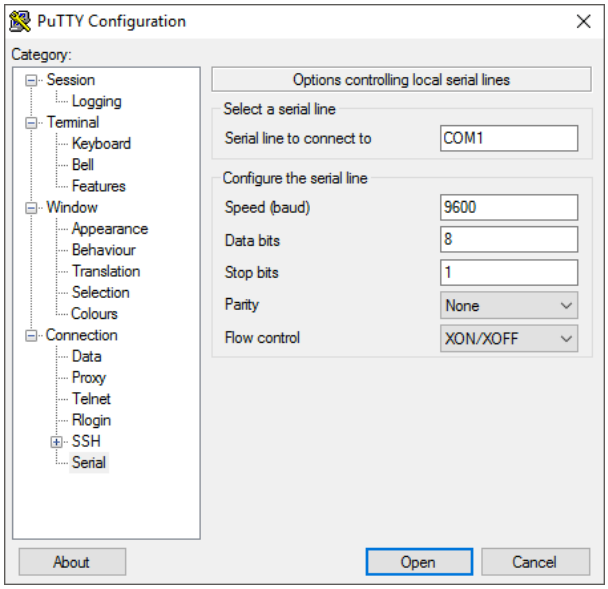
1) Download a program enabling to log in to Netsilon (e.g.: PuTTY).

2) Open the program (PuTTY).

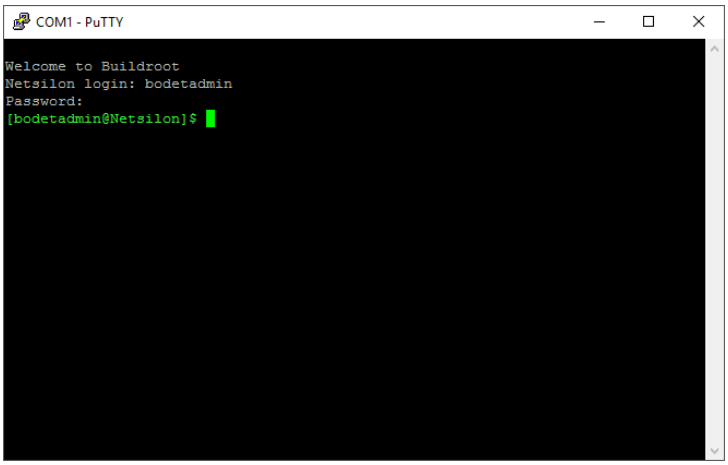
3) Enter the communication port.



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.



5) Enter the default ID and password to access the command set. As a reminder:
- › ID: bodetadmin
- › Password: admin49



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

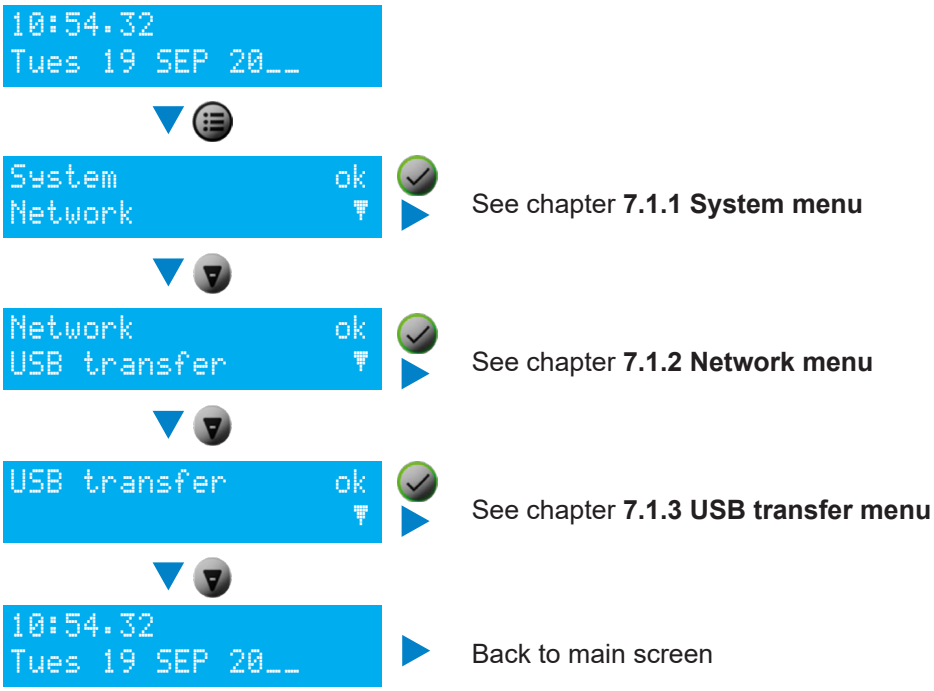
To access the list of command sets, see Annex 5: list of command sets.

7. CONTROL PANEL MENUS

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**

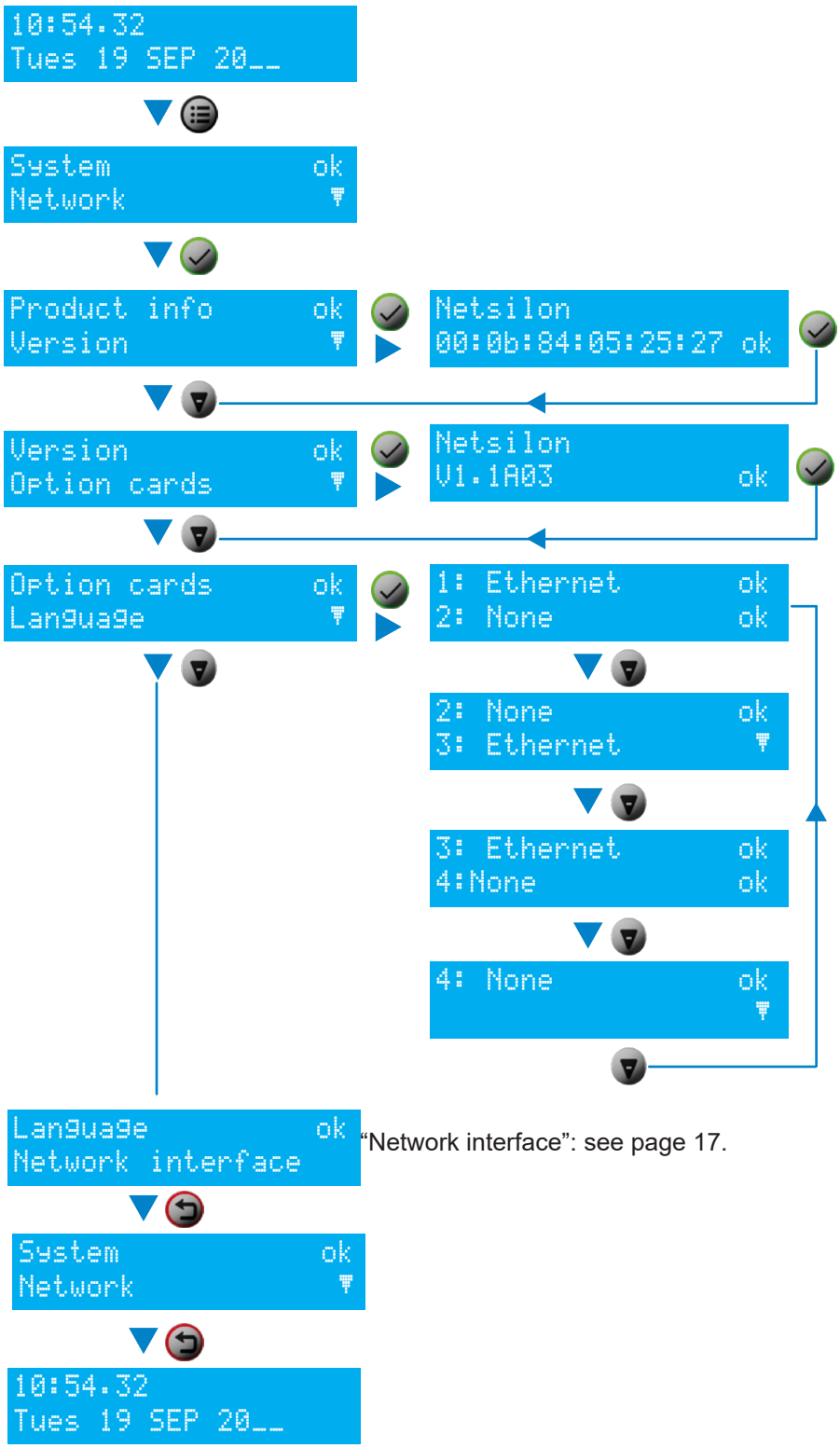
See chapter **7.1.3 USB transfer menu**

Back to main screen

7.1.1. System menu

This menu can be used to view 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

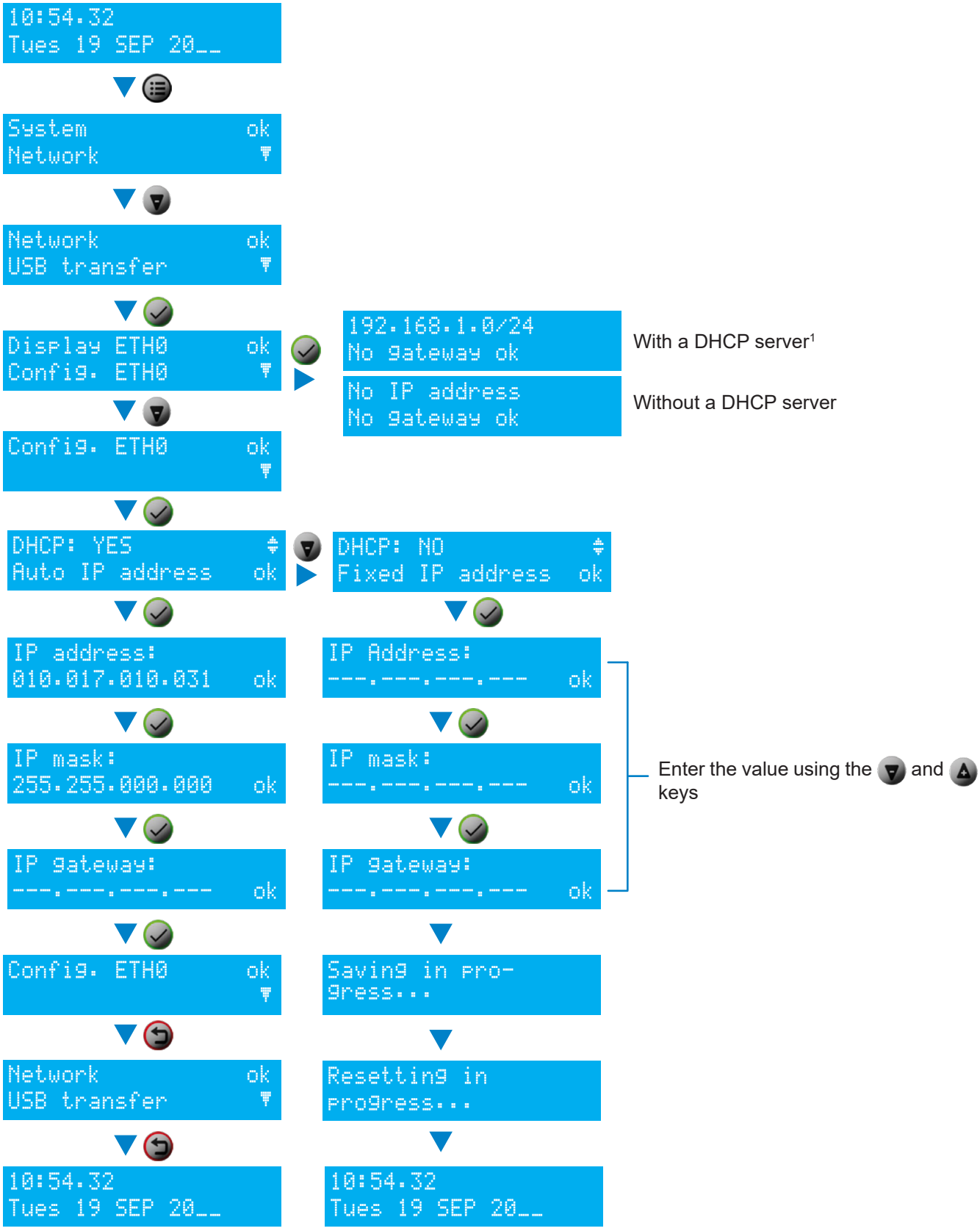
Display of option cards installed.

Reminder: Netsilon can hold up to 4 option cards.

"Network interface": see page 17.

7.1.2. Network menu

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

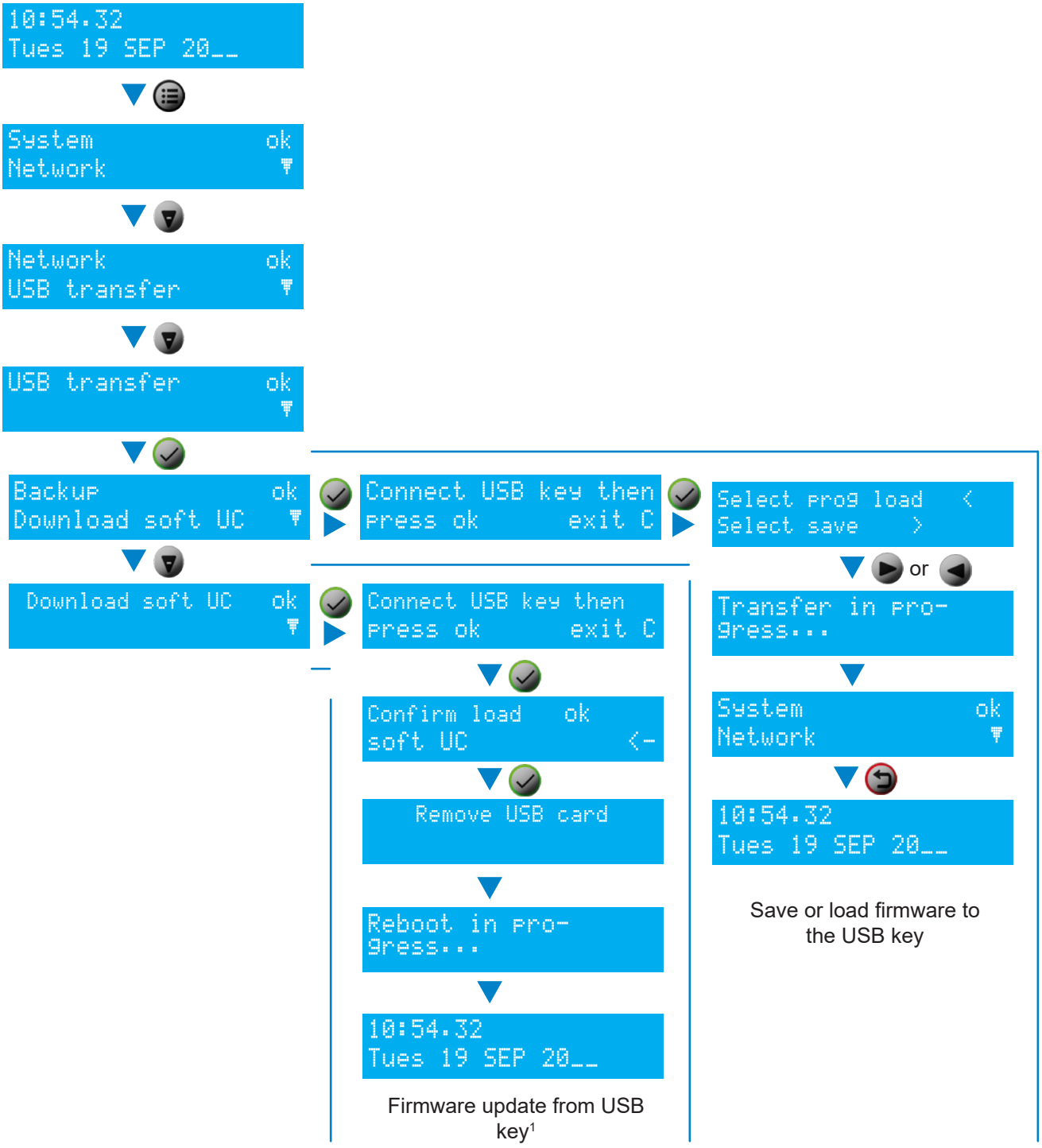


[1] *The IP address 192.168.1.0/24 and absence of gateway are given by way of example. Reminder: /24 is the CIDR addressing.*

7.1.3. USB transfer menu

The Netsilon time server can load or save its programming by means of a USB key.

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



[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] for the ETH0 network output.

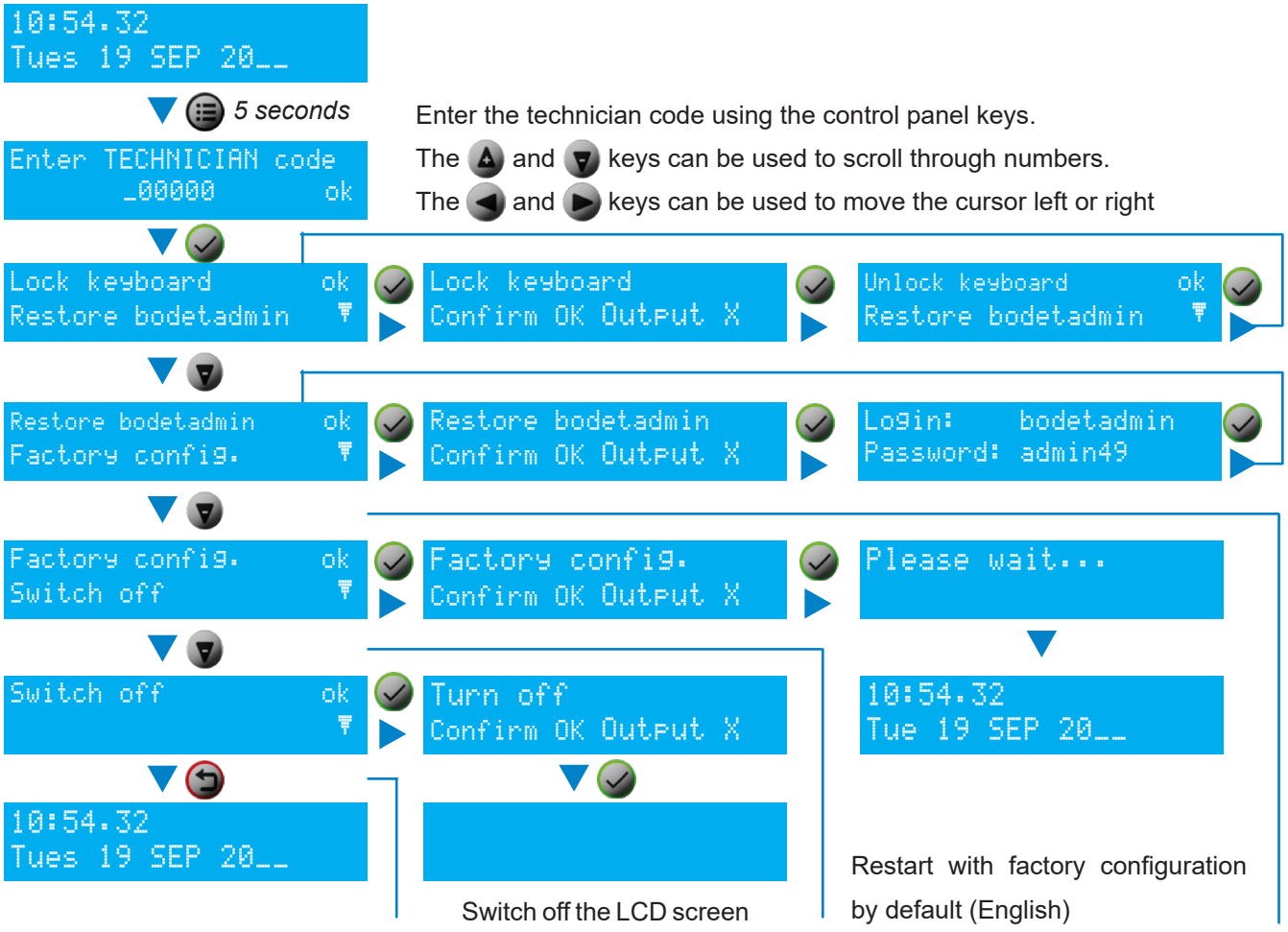
In this menu, it is possible to:

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

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.



[1] *The MAC address of the ETH0 port is shown on a label on the rear of the Netsilon device.*

8.1 Status of LEDs on 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 supply 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 double supply version (AC+DC or 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 GLONASS 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 GLONASS synchronisation source, check that Netsilon is connected to this antenna). 2) The GLONASS antenna installation is operational (where applicable).
	Flashing red	Synchronisation lost Holdover exceeded / freerun	**Please note:** If Netsilon has just restarted, no troubleshooting is necessary. Wait several minutes until the synchronisation is detected. 1) The priority synchronisation input is available (e.g. for a GPS synchronisation source, check that Netsilon is connected to this antenna). 2) The GPS antenna installation is operational (where applicable).
Alarm	Off	No alarm	-
	Flashing red	Critical alarm	**Please note:** If Netsilon has just restarted, no troubleshooting is necessary. Wait several 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 GLONASS synchronisation source, check that Netsilon is connected to this antenna).

8.2 Web browser not opening

› With a DHCP server

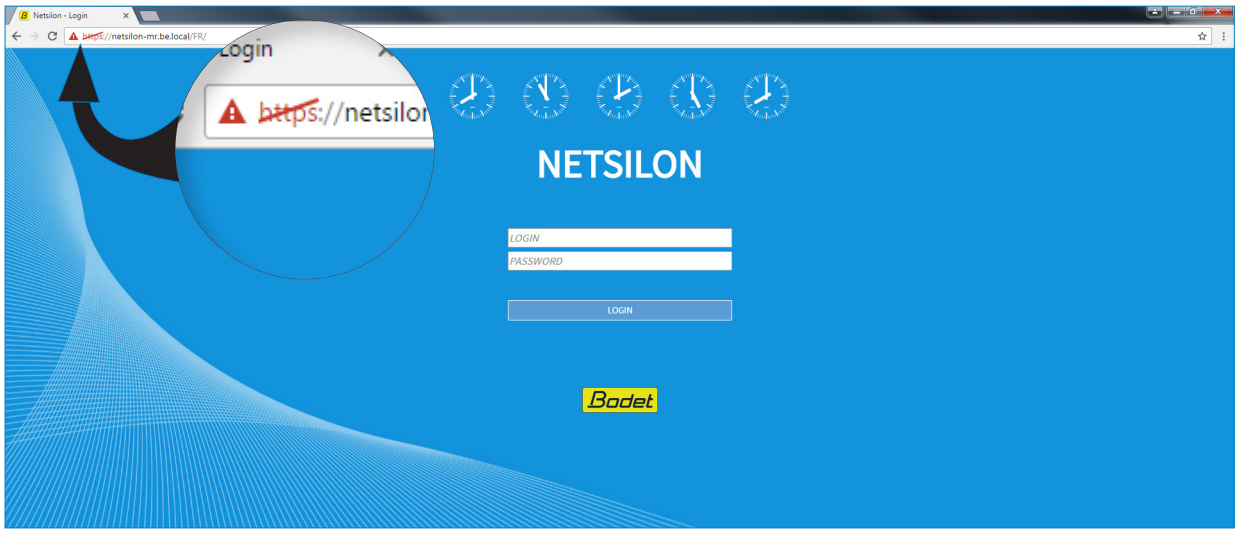
Check that the DHCP server delivers the IP address: IP address displayed on Netsilon LCD screen (see chapter **3.4 Configuration with a DHCP server**)

› Without a DHCP server: fixed IP address

Check that the network settings are correct: IP address available, subnet mask, gateway, etc. (see chapter **3.5 Configuration without a DHCP server**)

› HTTP/HTTPS

If using the DNS:
HTTP: enter the domain name, and the home page will open.
HTTPS: enter the domain name, and the home page will open. However, the connection is not secure and is indicated as follows:



It is possible to force the connection: see chapter › **HTTPS**

› Enable cookies

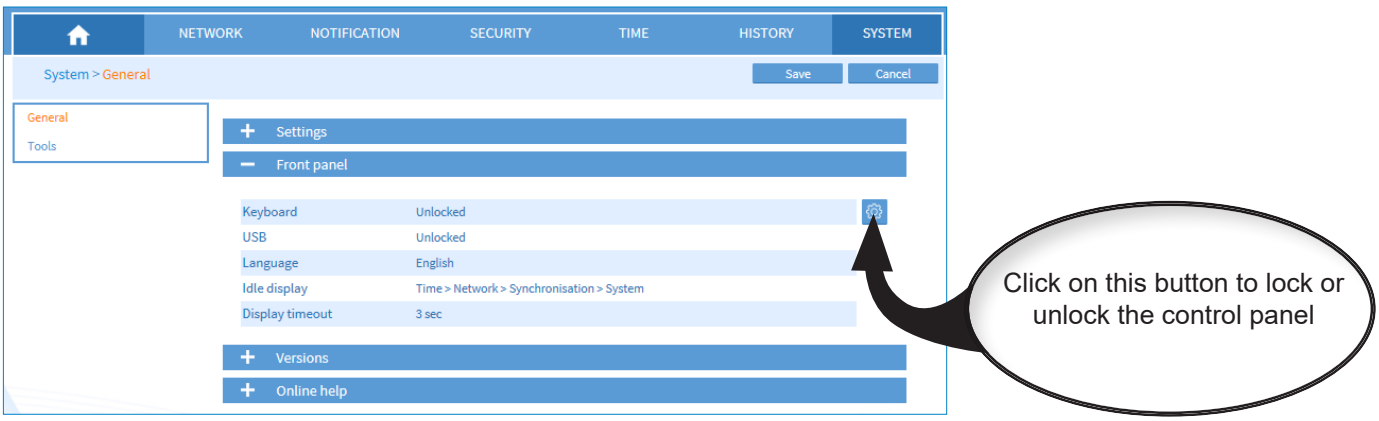
Cookies must be enabled in order to access the Netsilon web server.

8.3 Control panel inactive

The control panel on the front of the Netsilon device can be locked in order to prevent any misuse by a third party. Once locked, the functioning of the control panel is disabled until it is unlocked by using one of the following two methods:

› From the technician menu: see chapter **7.2 Technician menu.**

› Via the web server: System menu > General > Front panel:



8.4 Data synchronisation

To configure Netsilon via the web server, several parameters must be met:

- The PC must be on the same network as Netsilon. Ensure 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 less than Stratum 15. If this is not the case, Netsilon must be synchronised to a more precise reference source or operate in holdover mode. Check the NTP synchronisation level.

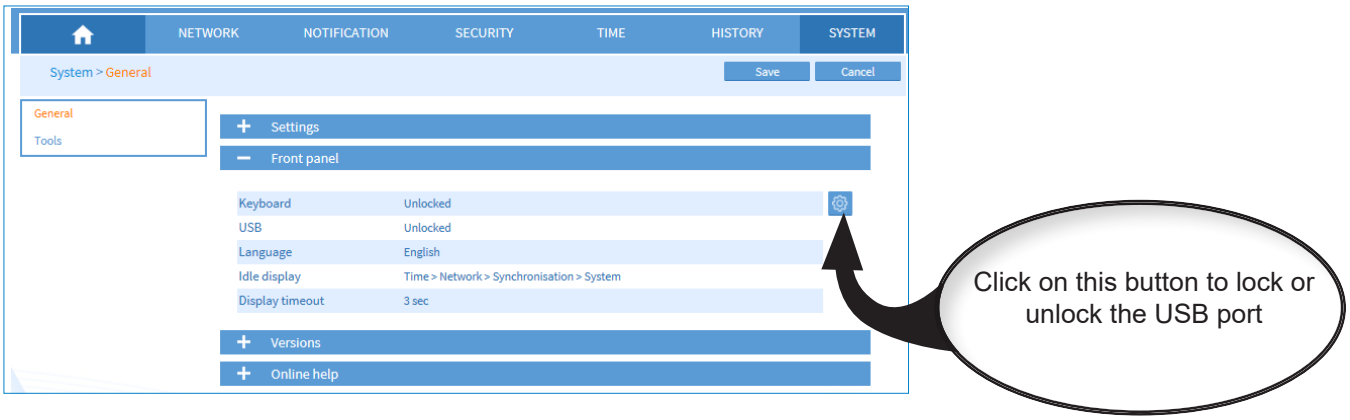
If the problem persists, contact BODET technical support.

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:



- 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: http://www.bodet-time.com/en/customer-support.html

2) Fill in the contact form.

Telephone support is available from Monday to Friday from 8.00 to 12.00 am and 1.30 to 5.00 pm.

To speed up your Netsilon diagnosis, carry out a backup of the system and note the Netsilon MAC address.

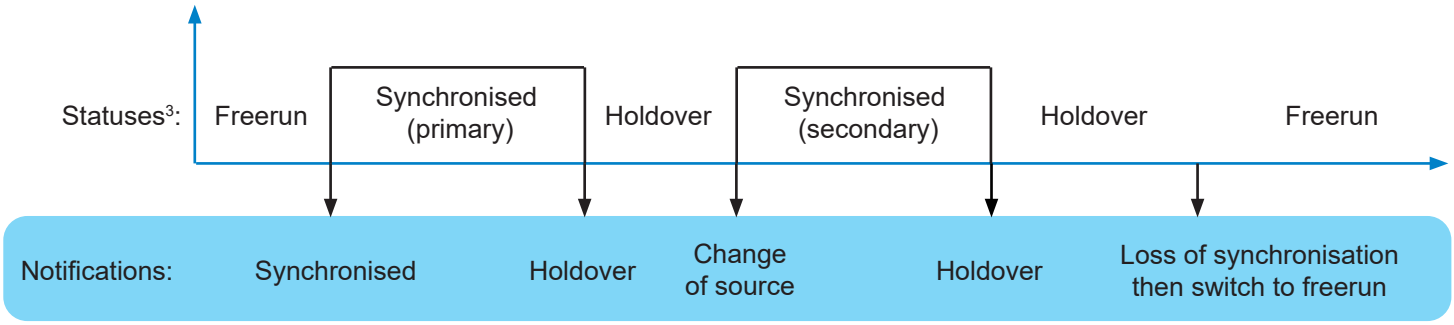
9. ANNEXES

9.1 Annex 1: synchronisation

9.1.1. Primary source / secondary source

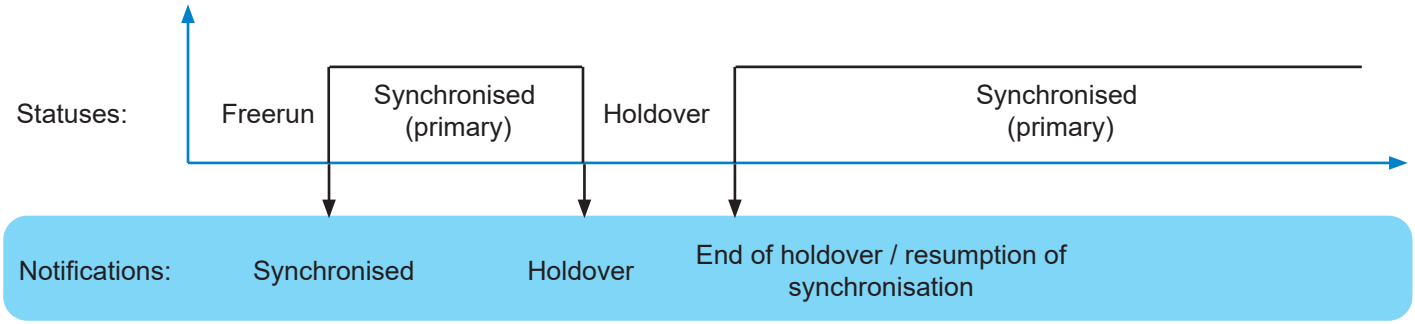
Scenario 1: loss of synchronisation from the primary then secondary sources

- Freerun[1] on product start-up
- Synchronisation with the primary source (e.g. GLONASS)
- Loss of synchronisation from the primary source
- Holdover[2]
- Synchronisation with the secondary source (e.g. NTP)
- Loss of synchronisation from the secondary source
- Holdover
- No synchronisation detected
- Freerun



Scenario 2: resynchronisation with primary source after momentary loss of primary source

- Freerun on product start-up
- Synchronisation with the primary source (e.g. GLONASS)
- Loss of synchronisation from the primary source
- Holdover
- Re-synchronisation with the primary source



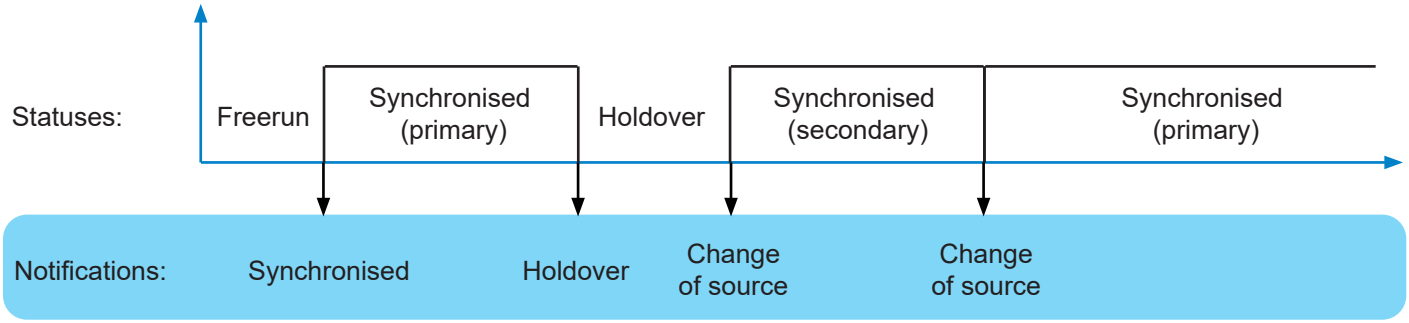
[1] this is a status in which Netsilon can transmit a time signal without any guarantee of its precision. The precision of the time zone is no longer guaranteed.

[2] reminder: the holdover mode duration can be set via the web server.

[3] these statuses are shown on the Netsilon LCD screen.

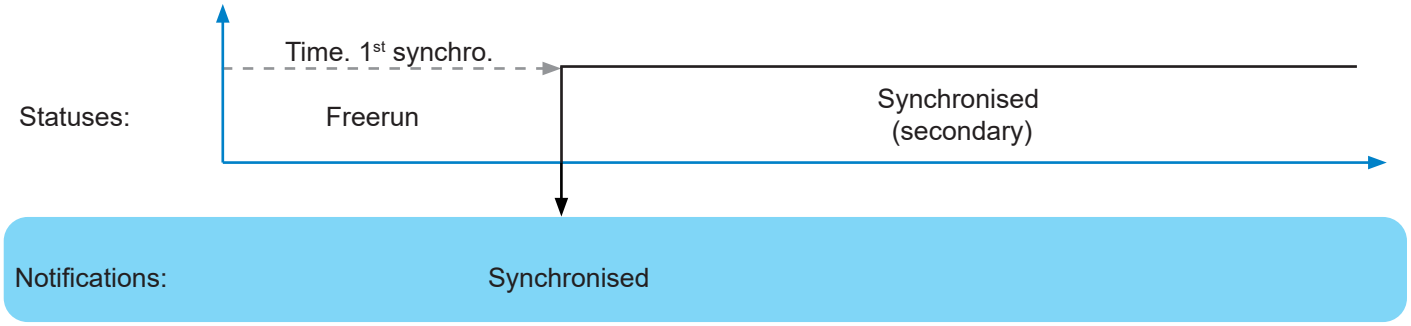
Scenario 3: re-establishment of the primary source

- Freerun on product start-up
- Synchronisation with the primary source (e.g. GPS)
- Loss of synchronisation from the primary source
- Holdover
- Synchronisation with the secondary source (e.g. NTP)
- Switch to the primary synchronisation source.



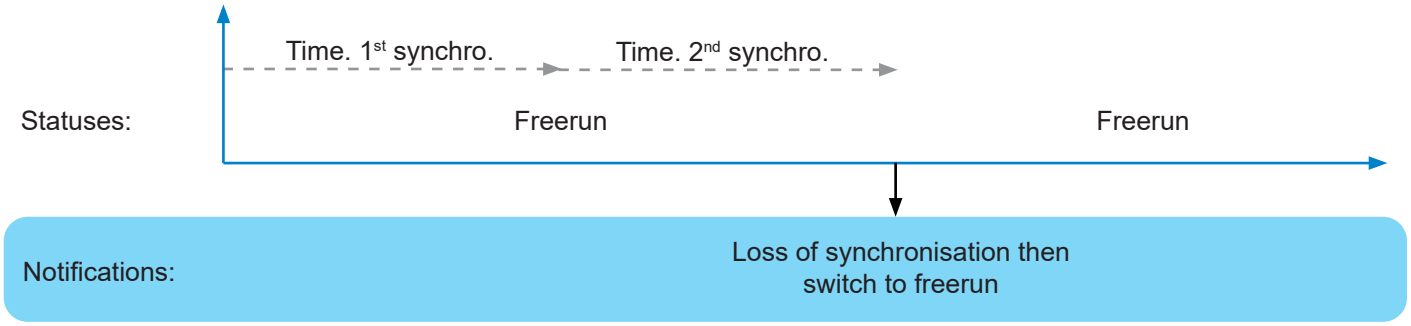
Scenario 4: synchronisation with the secondary source where no primary source is present

- Freerun on product start-up
- Timeout[1] for synchronisation with the primary source (e.g. GLONASS)
- Synchronisation with the secondary source (e.g. NTP)



Scenario 5: no synchronisation source

- Freerun on product start-up
- Timeout for synchronisation with the primary source (e.g. GPS)
- Timeout for synchronisation with the secondary source (e.g. NTP)
- No synchronisation: switch to freerun



[1] *The timeout duration depends on the synchronisation source:*

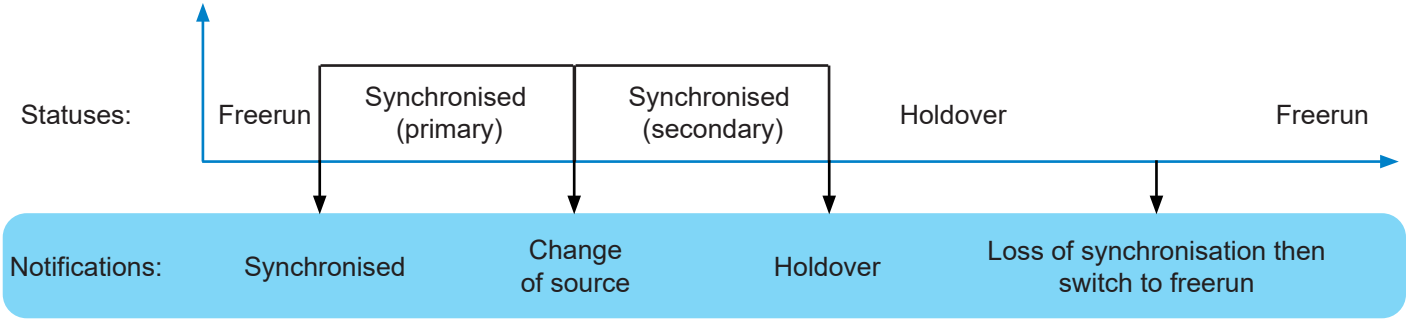
- *Bodet GPS / GLONASS: 5 minutes*
- *NTP: 15 minutes*
- *ALS: 10 minutes (switching in holdover mode after 5 consecutive bad frames – the status of the ALS162 source becomes unavailable)*

9.1.2. *Automatic selection*

The synchronisation source is automatically selected based on reception quality.
No holdover between changing synchronisation sources.

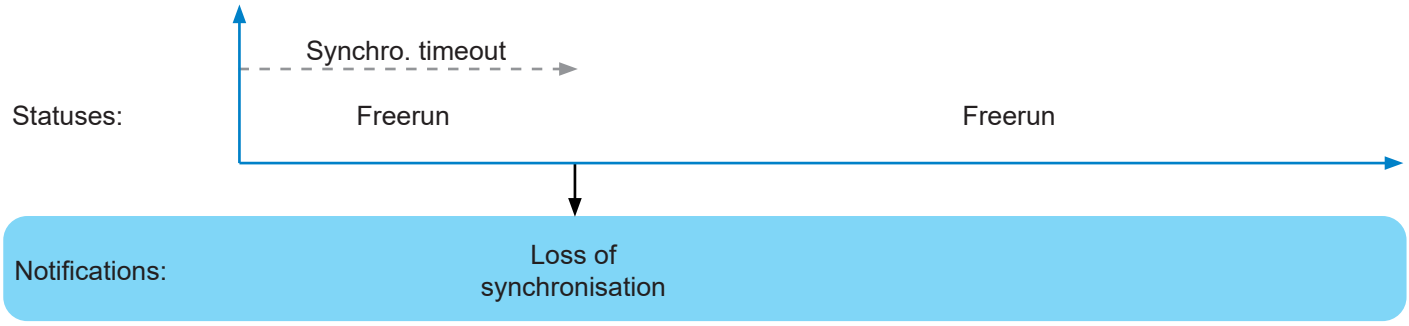
Scenario 1: loss of synchronisation from the primary then secondary sources

- Freerun on product start-up
- Synchronisation with the primary source (e.g. GPS)
- Synchronisation with the secondary source (e.g. NTP)
- Loss of synchronisation from the secondary source
- Holdover
- No synchronisation: switch to freerun



Scenario 2: no synchronisation source

- Freerun on product start-up
- Timeout for both synchronisation sources (e.g. GLONASS + NTP)
- No synchronisation: switch to 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 static IPv4 / IPv6 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 the 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 set up 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	√	-	-	-
	Outputs: configure outputs (option cards)	√	-	-	-
	Time zone: configure local time system	√	-	-	-
	Time zone: define time zones	√	-	-	-
	Time zone : programming a manual Leap Second	√	-	-	-
History					
	GNSS statistics	√	-	-	-
	NTP statistics	√	-	-	-
	ALS 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 settings.	√	-	-	√ (except LCD screen settings)
	General>Versions: consult the Netsilon firmware version and the option cards installed	√	√	√	√
	General>Consult this notice	√	-	-	-
	Tools>Upgrade and backup: save or load the configuration, set to factory configuration and update the firmware	√	-	√ (only factory configuration)	√
	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:

Function mode	Description	Admin.	User
Network			
	Interfaces: configure the ETH0 interface	R/W[1]	R
	Interfaces: configure the other network interfaces	R/W	R
	Routes: configure static IPv4 / IPv6 routes	R/W	R
	Services: activate services	R/W	R/W
Notification			
	Alarms: configure alarms and alarm thresholds (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 set up 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
	Outputs: configure outputs (option cards)	R/W	R/W
	Time zone: configure local time system	R/W	R/W
	Time zone: define time zones	R/W	R/W
	Time zone: programming a manual Leap Second	R/W	R/W
History			
	GNSS statistics	R	R
	NTP statistics	R	R
	ALS 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 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 notice	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

Function mode	Description	Saved
Network		
	Interfaces: configure the ETH0 interface	-
	Interfaces: configure the other network interfaces	-
	Routes: configure static IPv4 / IPv6 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 the 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 set up 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	√
	Outputs: configure outputs (option cards)	√
	Time zone: configure local time system	-
	Time zone: define time zones	√
	Time zone: programming a manual Leap Second	√
History		
	GNSS statistics	-
	NTP statistics	-
	ALS 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 settings.	√
	General>Versions: consult the Netsilon firmware version and the option cards installed	-
	General: consult this guide	-
	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 installed option cards.
	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 power 1.
	systempowerac2status	Indicates the status of the AC power 2. (only useful for AC+AC version)
	systempowerdcstatus	Indicates the status of the DC power.
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 settings and restarts Netsilon.
	toolreboot	Restarts Netsilon.
	toolshutdown	Shuts Netsilon down.
	toolcancel	Cancels a command in progress. Valid only for toolrestore, toolreboot and toolshutdown.
Network IPv4		
	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
Network IPv6		
	net6getinfo	Display IPv6 parameters of all ports or the requested port: IP address and gateway.
	net6getdhcp [interface]	Display the state of DHCP of all ports or the requested port. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6setdhcp [interface] [ON/OFF]	Enable or disable 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]	Set the state of slaac (enable/disable) for the 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]	Define the gateway. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6getstaticip [interface]	Define the static IP address and mask. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6addstaticip [interface] [addr6]/[prefix]	Indicate 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. Authentication is carried out by using 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
```

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:

```
sftp scp 10.10.200.5
scp 10.10.200.135 password: admin49
(always use the same password as bodetadmin)
sftp>
```

The user receives the SFTP invitation enabling the file transfer.

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
sftp>
```

The user receives the SFTP invitation enabling the file transfer.