NETSILON 9 / 11

Manuel utilisateur

Le document est relatif aux produits suivants :

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

Le document est relatif aux produits suivants :

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

Bodet
www.bodet-time.com

BODET TIME & SPORT
1 rue du Général de Gaulle
49340 TREMENTINES - France
Tél. support France: 02 41 71 72 99
Tél. support Export: +33 241 71 72 33

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

Réf : 6084033J

S'assurer à réception que le produit n'a pas été endommagé durant le transport pour réserve au transporteur.

SOMMAIRE

INFORMATIONS RELATIVES À LA SÉCURITÉ

Les pictogrammes ci-dessous permettent d'illustrer des risques ou des sources de danger lors de l'installation, de l'utilisation et de la maintenance de ce produit.

Symbole	Description
	*IEC60417 - 1641* Manuel d'utilisation
	*IEC60417 - 5002* Positionnement de la pile
	*IEC60417 - 5017* Classe I
	*IEC60417 - 5018* Connexion de terre fonctionnelle
	*IEC60417 - 5019* Connexion de terre de protection
	*IEC60417 - 5031* Courant continu
	*IEC60417 - 5032* Courant alternatif
	*IEC60417 - 5033* Courant AC+DC
	*IEC60417 - 5036* Tension dangereuse
	*IEC60417 - 5172* Classe II
	*IEC60417 - 6040* Danger, rayonnement UV
	*IEC60417 - 6041* Danger, rayonnement lumière visible
	*IEC60417 - 6042* Danger, risque de choc électrique
	*IEC60417 - 6092* Classe II avec connexion de mise à la terre fonctionnelle
	*IEC60417 - 6151* Danger, rayonnement IR
	*IEC60417 - 6172* Déconnecter toutes les sources d'énergie
	*IEC60417 - 6414* Collecte séparée des déchets d'équipements électriques et électroniques (DEEE)
	*IEC60417 - 0434b* Attention
	*IEC60417 - 5032-1* Alimentation triphasée
	*IEC60417 - 5032-2* Alimentation triphasée + Neutre
	*IEC60417 - 5009* Power, Stand-by
	*IEC60417 - 6069* Danger, faisceaux lumineux

1. GÉNÉRALITÉS

Nous vous remercions d'avoir choisi un serveur de temps Netsilon 9 / Netsilon 11 BODET. Ce produit a été conçu avec soin pour votre satisfaction selon les règles de notre système qualité ISO9001 et ISO14001.

Nous vous recommandons de lire attentivement ce manuel avant de commencer à manipuler le produit.

Conserver ce manuel pendant toute la durée de vie de votre produit afin de pouvoir vous y reporter à chaque fois que cela sera nécessaire.

Tout usage non conforme à la présente notice peut causer des dommages irréversibles, et entraîner l'annulation de la garantie. La responsabilité de la société BODET ne pourra donc pas être engagée. Le produit est garanti 3 ans hors dégâts liés à des surtensions (foudre,...) en l'absence d'un parafoudre GNSS Bodet sur l'installation.

Données non contractuelles. La société BODET se réserve le droit d'apporter aux appareils certaines modifications fonctionnelles, techniques ou esthétiques, sans préavis.

Ce manuel est sujet à des changements sans préavis. Pour obtenir la version la plus récente de cette documentation, consulter notre site internet : www.bodet-time.com.

Remarque : en fonction de votre configuration (ex.: cartes options, synchronisation NTP et/ou GNSS...), certaines fonctionnalités présentées dans cette notice ne seront pas disponibles sur votre serveur de temps Netsilon.

1.1 Utilisation de la notice

Différents profils d'utilisateurs peuvent être amenés à installer ou utiliser ce produit.

En fonction de l'intervention à réaliser et du niveau de compétence de l'utilisateur, voici nos recommandations :

- Utilisateur simple (personne ordinaire sans expérience):
  Parcourir ce manuel dans son intégralité avant d'installer et configurer Netsilon.
- Utilisateur formé et qualifié (personne avertie et expérimentée):
  Parcourir ce manuel à partir du chapitre **2. Installation.**
- Dans le cas où Netsilon est en fonctionnement :
  Afin de modifier un réglage spécifique ou mieux connaître les caractéristiques et fonctions, parcourir ce manuel à partir du chapitre **3. Mise en service**. Utiliser la fonction de recherche ou cliquer sur un signet du PDF ou utiliser la table des matières.
- Dans le cas de problèmes techniques : se référer au chapitre **8. Assistance.**

Identification des pictogrammes :

: indique un conseil, une recommandation ou toute autre information notable pour l'usage de Netsilon.

: indique qu'une attention particulière doit être apportée.

: indique qu'un danger électrique est présent en cas de mauvaise utilisation ou de non respect des indications. Cette information doit obligatoirement être prise en compte lors de l'installation ou de l'utilisation de Netsilon.

1.2 Introduction

Netsilon est un serveur de temps conçu pour distribuer un signal horaire de haute précision.
Compact et modulaire, le serveur de temps Netsilon allie précision d'une horloge mère et approche sécurisée des réseaux informatiques :

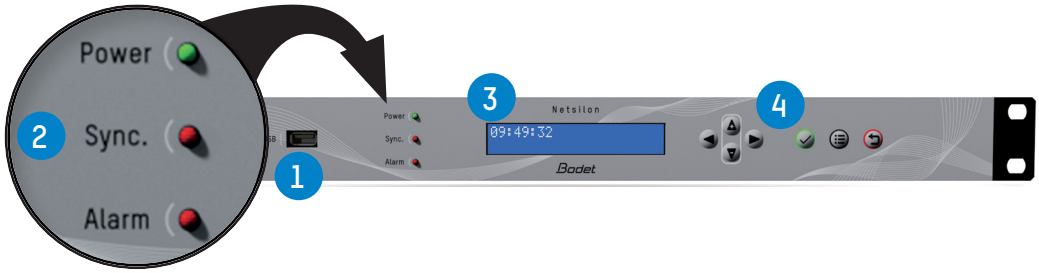
- Horloge interne de haute précision cadencée à partir de son quartz OCXO.
- Ordre de priorité pour les différentes références de synchronisation.
- Conception modulaire permettant d'offrir une grande variété de signaux d'entrée/sortie (jusqu'à 4 cartes options).
- Gestion de la sécurité réseau : activer ou désactiver les protocoles d'encryption, d'authentification, d'accès.
- Information des alarmes sous forme de traps SNMP et d'e-mails.

4 versions sont disponibles en fonction de l'alimentation:

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

1.3 Présentation de Netsilon

1.3.1. Face avant

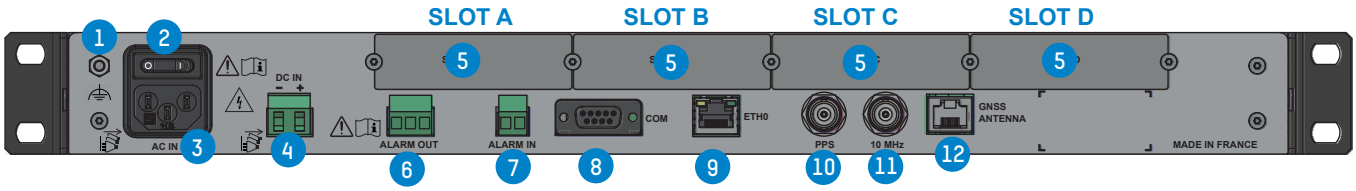


La face avant de Netsilon est composée de :

- un port USB[1] 1,
- trois LEDs d'états pour l'alimentation, la synchronisation et les alarmes (Power, Sync. et Alarm) 2.
  Se reporter au chapitre **8.1 Etat des LEDs sur la façade**
- un afficheur LCD sur deux lignes 3,
- un clavier de commande 4 pour le paramétrage initial (paramétrage complet depuis le serveur web).

1.3.2. Face arrière

› NETSILON 9 / 11 (AC+DC)

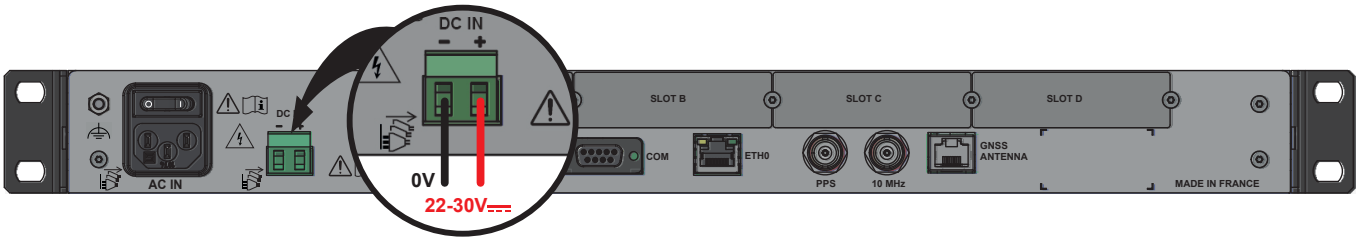


1 Terre fonctionnelle ⏚: possibilité de raccorder au châssis de la baie, en option.
La terre de protection est assurée par le connecteur mâle IEC 3.

2 Interrupteur marche/arrêt.

3 Connecteur secteur AC IN power inlets IEC 320.

4 Bornier d'alimentation en courant continu DC IN (bornier 3,81 mm).



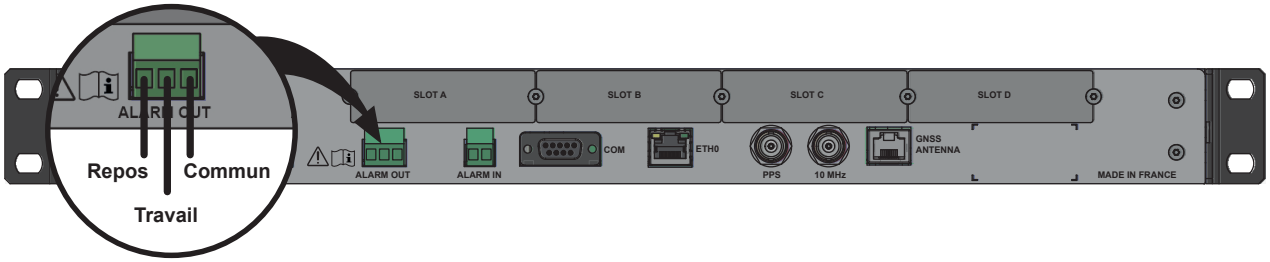
5 Emplacements pour cartes options :

- Carte option NETWORK (RJ45), réf.: 907 920. 2 cartes Option maximum [Slot A ou B ou C].
- Carte option NETWORK (SFP), réf.: 907 921. 2 cartes Option maximum [Slot A ou B ou C].
- Carte option PTP (RJ45+SFP), réf.: 907 922. 1 carte Option maximum [Slot A ou B ou C ou D].
- Carte option IRIG OUTPUT, réf.: 907 930. 4 cartes Option maximum [Slot A ou B ou C ou D].
- Carte option IRIG INPUT, réf.: 907 947. 1 carte Option maximum [Slot A ou B ou C ou D].
- Carte option ASCII, réf.: 907 926. 4 cartes Option maximum [Slot A ou B ou C ou D].

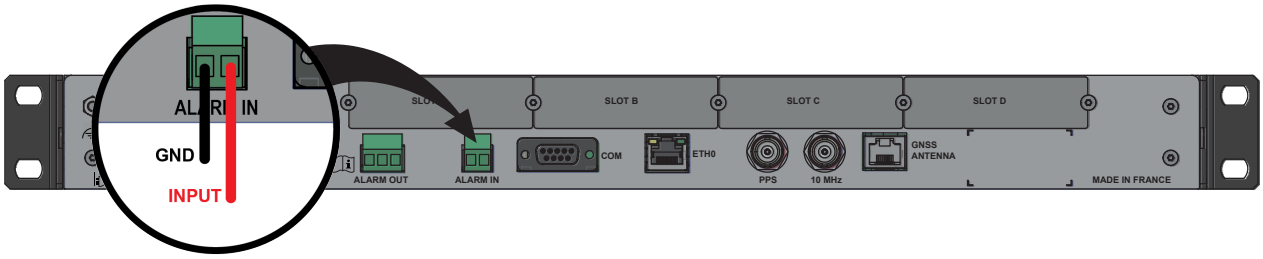
Les cartes options sont installées dans notre usine de production. Dans le cas d'une installation ultérieure, se reporter à la notice d'installation des cartes options (réf.: 608511).

[1] *Netsilon supporte les clés USB formatées en FAT16/FAT32 et NTFS*

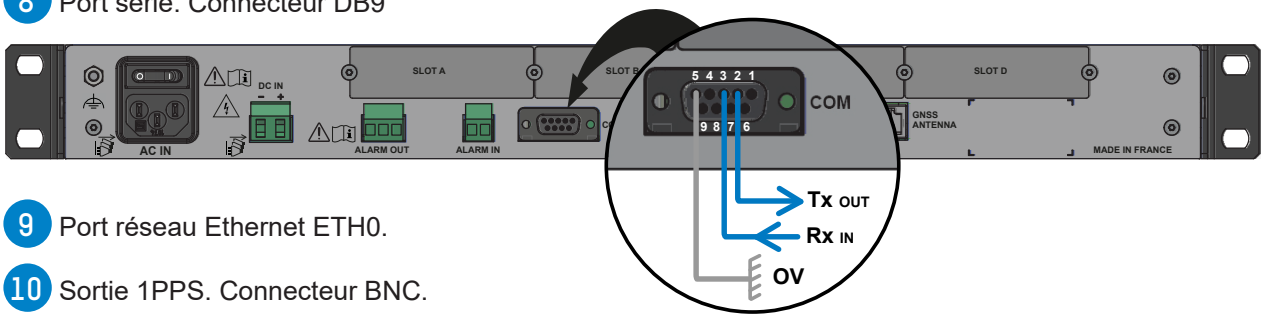
6 Sortie contact relais Commun Repos/Travail.
Si contact sur Travail : pas d'alarmes / Si contact sur Repos : alarmes.



7 Entrée d'alarmes : s'interface avec le contact sec de l'équipement client.



8 Port série. Connecteur DB9



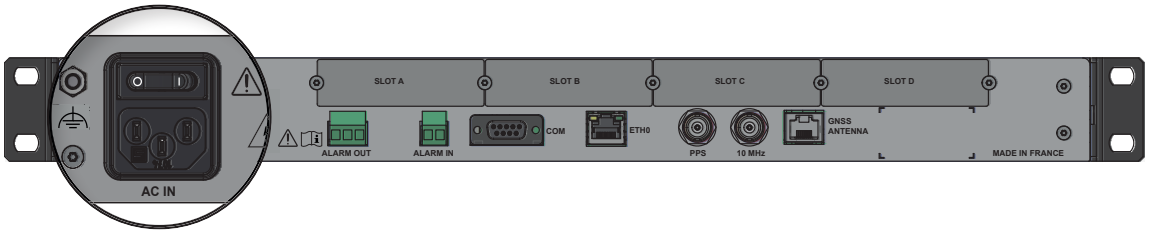
9 Port réseau Ethernet ETH0.

10 Sortie 1PPS. Connecteur BNC.

11 Sortie 10MHz. Connecteur BNC

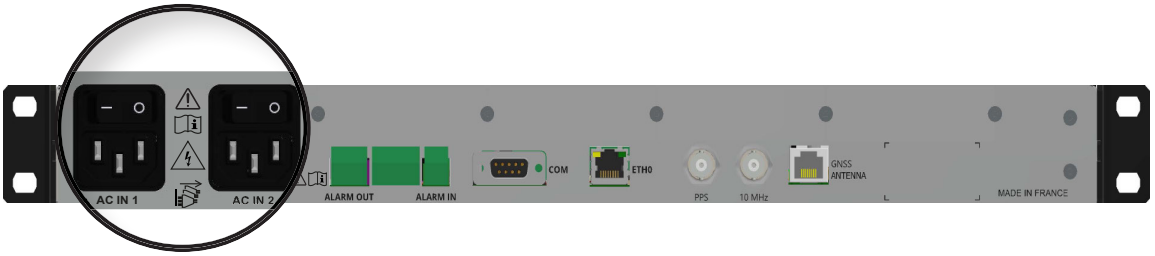
12 Antenne GNSS. Prise RJ45

> NETSILON 9 / NETSILON 11 (AC)



> NETSILON 9 / NETSILON 11 (DC)

> NETSILON 9 / NETSILON 11 (AC+AC)



1.4 Spécifications

1.4.1. Précision

	Valeurs typiques - Netsilon 9	Valeurs typiques - Netsilon 11
Précision[1]	$1x10^{-11}$	$1x10^{-11}$
Stabilité[2]	$1x10^{-9}$/jour	$1x10^{-9}$/jour
Holdover[3]	**15** µs (après 24 heures)	**2,5** µs (après 24 heures)

[1] *moyenne après 24 heures avec signal GPS*
[2] *moyenne après 2 semaines avec signal GPS*
[3] *valeur typique, après une synchronisation GPS de 2 semaines à température constante*

1.4.2. Connexions de synchronisation et de diffusion du temps

	Standard	Option
Entrées	GNSS NTP	NTP PTP IRIG
Sorties	NTP 10 MHz 1PPS	NTP PTP Temps codé : NMEA 0183,... IRIG

1.4.3. Caractéristiques mécaniques

Construction	Boîtier métallique - rack 1 U - 19''
Température de fonctionnement	0°C à +50°C
Taux d'humidité relative à 40°C	0 à 90% HR sans condensation
Indice de protection	IP20
Poids	2,5 kg
Dimensions	442 x 264 x 44,2 mm

1.4.4. Caractéristiques électriques

Alimentation	AC : 100-240V~ / 50-60Hz / 1.9-0.8A DC : 22-30V⎓ / 3.2-1.9 A AC+DC | Alimentations redondantes, AC+AC | caractéristiques ci-dessus.
Consommation	20W (sans carte option)
Entrée alarme	Alarm IN Entrée par contact sec, libre de potentiel. $I_{IN} \leq 10$ mA
Sortie alarme	Alarm OUT Relais NC-NO-C. Courant maximum : 1A/50V⎓, 1A/30V~
MTBF	100 000 heures

1.4.5. Communications

Port réseau	RJ45, 10/100/1000-BaseT (Gigabit)
Façade	USB - Prise USB (désactivable) pour sauvegarde et mise à jour du firmware. Clavier (verrouillable) et écran LCD pour la configuration réseau.
Interface série	COM - RS232 - connecteur DB9

1.4.6. Caractéristiques réseau

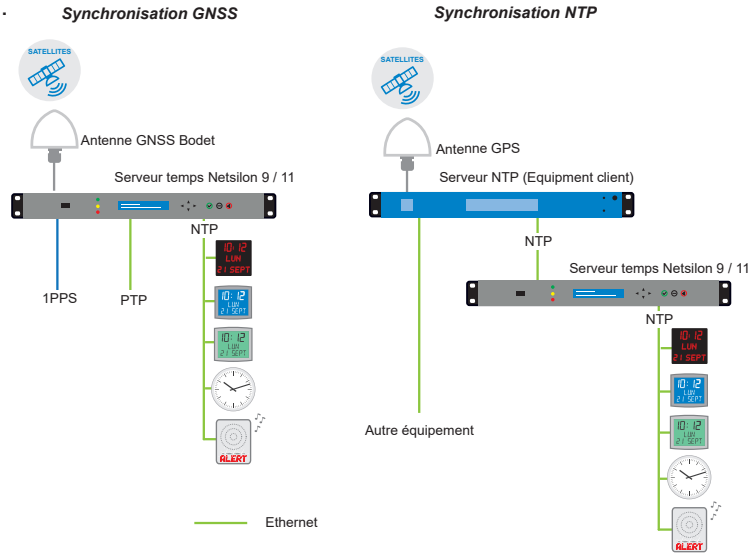
PROTOCOLES	
NTP V2, V3, V4	Conformes avec RFC 1305 et 5905. Support Unicast, Broadcast, Multicast, Anycast, authentification + intégrité MD5, peering et Autokey.
Nombre maximum de requêtes NTP par seconde. Tous ports Ethernet confondus	7 000
Nombre maximum de clients NTP (typique)	32 000
SNTP V3, V4	Conformes avec RFC 1769, 2030, 4330 et 5905
TIME protocolE	Conforme avec RFC 868
DAYTIME protocolE	Conforme avec RFC 867
COMMUNICATION	
HTTP/HTTPS	Conforme RFC 2616 (gestion des certificats signés)
SSH	SSH v1.3, SSH v1.5, SSH v2 (OpenSSH)
MANAGEMENT	
IP	IPv4, IPv6 : Dual stack
VLAN	Standard 802.1Q (unique / multi)
SERVICES	
DHCP	DHCPv4, DHCPv6, Autoconf & Slaac
SMTP	Envoi d'e-mails
SUPERVISION	
Alarme	Traps SNMP, e-mail et contact relais
SNMP	v1 (RFC 1157), v2c (RFC 1901-1908) et v3 (RFC 3411-3418) (traps + agents)
Syslog	Services de journaux d'évènements
Contact relais / Entrée externe	Envoi et réception des alarmes (Alarm OUT / Alarm IN)

1.4.7. Fonctions de sécurité

- Activation / désactivation des protocoles,
- Authentification via protocole 802.1x,
- Redondance via protocole LACP,
- Protection par authentification unique (identification + mot de passe) ou authentification LDAP / Radius,
- Chiffrement DES et AES,
- Authentification SHA1, MD5,
- SSL/TLS : sécurisation des échanges par réseau informatique,
- SCP : copie sécurisée des fichiers de Netsilon à partir d'une session SSH,
- SFTP : transfert sécurisé des fichiers de Netsilon à partir d'une session SSH.

1.4.8. Sources de synchronisation

Deux sources de synchronisation sont disponibles pour Netsilon 9 / 11 : l'antenne GNSS BODET ou un serveur NTP présent sur le réseau informatique.



2. INSTALLATION

Ce chapitre donne un aperçu des étapes à suivre pour l'installation d'un Netsilon 9 ou Netsilon 11.

Plusieurs facteurs sont à prendre en compte pour l'installation de Netsilon 9 / 11 :

1) Le type d'alimentation : AC, DC, AC+DC, AC+AC
2) Le type d'installation : intégration de Netsilon 9 / 11 dans un réseau Ethernet existant ou mise en place d'une nouvelle installation (prévoir l'accessibilité des câbles).
3) Disposer d'un PC connecté au réseau Ethernet avec un navigateur internet[1] tel que Google Chrome®, Mozilla Firefox, Microsoft Edge ou Internet Explorer®.

Si Netsilon 9 / 11 est équipé de cartes options, ces dernières doivent être configurées depuis le serveur web, une fois la configuration du réseau terminée (du port ETH0).

2.1 Vérification de l'emballage

Déballer soigneusement le serveur de temps et vérifier le contenu de l'emballage. Celui-ci doit comprendre :

- L'unité Netsilon 9 ou Netsilon 11 avec ses cartes options,
- Les deux équerres pour la fixation en rack dans une baie 19'',
- Un guide de démarrage rapide.
- Une notice sur les consignes de sécurité.

2.2 Sécurité

Ce produit a été conçu avec soin pour votre satisfaction selon les règles de notre système qualité ISO9001 et ISO14001.
Avant de commencer l'installation et la configuration de Netsilon, lire attentivement les différentes consignes de sécurité.
S'assurer de toujours respecter les avertissements de sécurité, les précautions lors de l'installation, l'exploitation et l'entretien de votre produit.

L'installation et l'entretien de ce matériel doivent être réalisés par une personne qualifiée et formée au matériel BODET.

Le « produit » est raccordé à l'alimentation secteur. L'installation doit être conforme à la norme IEC 364 (NFC 15-100 pour la France).

2.2.1. Installation de l'équipement

L'installation et l'entretien de ce matériel doivent être réalisés par du personnel habilité. Ce produit ne doit pas être installé par les utilisateurs / opérateurs sans autorisation et sans formation.
L'installation électrique de l'équipement doit être conforme aux normes électriques en vigueur dans le pays d'utilisation de l'équipement.
Cet équipement ne convient pas à une utilisation dans des lieux susceptibles d'accueillir des enfants.

2.2.2. Ouverture de l'équipement

L'intérieur de cet équipement ne possède pas de pièces réparables par l'utilisateur : contacter l'assistance clientèle BODET si cet équipement doit être réparé.
Ne pas ouvrir l'équipement, à l'exception d'ajout ou de changement de cartes options et de changement de pile :

- **Attention, risque de choc électrique. Déconnecter toutes les sources d'énergie.**
- **Ne jamais ouvrir le produit tant que les alimentations repérées par le symbole sont connectées.**
- **Veiller à ce que toutes les sources d'alimentation soient retirées de l'appareil avant d'installer les cartes options.**

L'interrupteur est de type fonctionnel. Il ne s'agit pas d'un sectionneur d'alimentation. Débrancher l'alimentation et les circuits relais avant intervention afin de sectionner l'(es) alimentation(s).

2.3 Installation mécanique en rack

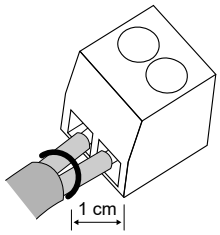
Le serveur de temps Netsilon doit être installé dans une armoire ou une baie 19" à l'aide des deux équerres livrées.

Nous recommandons l'installation de Netsilon 9 / 11 dans un lieu sécurisé.

[1] *Il est recommandé de posséder la dernière version du navigateur utilisé.*

2.4 Installation électrique

Les différents câbles doivent être fixés dans « l' armoire ou le coffret » de façon à ne pas exercer de contraintes sur les bornes de raccordement. De plus, les conducteurs d'un même circuit doivent être attachés entre eux près du bornier pour éviter une réduction de l'isolation dans le cas ou une des bornes viendrait à se desserrer.



⚠ **Le matériel doit être mis sous tension seulement après sa fixation dans le rack 19" de destination**.

2.4.1. Alimentation

Gestion des alimentations en fonction de la version :

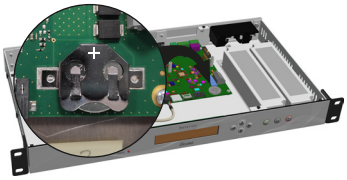
- Netsilon 9 / 11 (100-240V⁓) : alimentation secteur uniquement.
  - Brancher le cordon d'alimentation fourni sur le connecteur AC IN à l'arrière de l'équipement.
- Netsilon 9 / 11 (22-30V⎓) : alimentation continue uniquement.
  - Brancher un câble DC et respecter la polarité indiquée à l'arrière de l'équipement.
- Netsilon 9 / 11 (100-240V⁓ + 22-30V⎓) : alimentation secteur et/ou alimentation continue.
  - Brancher le cordon d'alimentation fourni sur le connecteur AC IN et/ou un câble DC en respectant la polarité indiquée à l'arrière de l'équipement.
- Netsilon 9 / 11 (100-240V⁓ + 100-240V⁓) : double alimentation secteur.
  - Brancher le(s) cordon(s) d'alimentation fourni(s) sur le(s) connecteur(s) AC IN à l'arrière de l'équipement.

En option, possibilité de raccorder la borne de terre fonctionnelle au châssis de la baie.

⚠ **L'alimentation DC IN doit être protégée en amont par un fusible de 6,3 AT.**
Quand plusieurs Netsilon sont alimentés par la même alimentation, protéger chaque entrée DC IN par un fusible distinct de 6,3 AT.
Bien vérifier la polarité de l'alimentation DC IN avant de brancher.

2.4.2. Pile de sauvegarde - CR2032

En cas de remplacement de la pile CR2032, il est impératif de respecter la polarité suivant les indications inscrites sur le slot de la pile.



⚠ **Danger :**

› Il y a risque d'explosion si la pile est remplacée par une pile de type incorrect. Utiliser uniquement les piles recommandées par le fabricant.
› Mettre au rebut les piles usagées conformément aux instructions présentes sur notre site internet.
› Ne pas ingérer l'accumulateur, risque de brûlures.
› Conserver les accumulateurs neufs et usagés hors de portée des enfants.
› Ce produit contient une pile ou accumulateur bouton. En cas d'ingestion, la pile ou l'accumulateur bouton, peut causer des brûlures internes sévères ou mortelles.
› En cas de soupçon d'ingestion d'un accumulateur ou d'introduction dans une partie quelconque du corps, demander immédiatement un avis médical.

2.4.3. Ethernet

Le port Ethernet ETH0, accessible sur le face arrière de l'équipement, permet une connexion facile aux routeurs, commutateurs ou hubs.
1) Utiliser un câble Ethernet RJ45 blindé CAT. 5E ou CAT. 6.
2) Brancher le câble réseau Ethernet sur le connecteur RJ45 en face arrière de Netsilon.

La mise en service du produit s'effectue en activant l'interrupteur en face arrière de l'équipement.
La société Bodet recommande fortement de raccorder et utiliser Netsilon exclusivement sur un réseau de type privé (VLAN).

2.4.4. Circuits relais alarmes

Pour les circuits relais, prévoir une protection par sectionneur-fusible ou disjoncteur 1A maximum.
La maintenance doit être réalisée hors tension. Sectionner l'alimentation et les circuits relais sous tension dangereuse.

3. MISE EN SERVICE

La configuration de Netsilon 9 / 11 s'effectue exclusivement sur le serveur web. Lors de la mise en service, il est nécessaire de paramétrer le port ETH0, depuis l'écran LCD et le clavier de commande, pour accéder au serveur web.

⚠ **Afin de ne pas rompre la synchronisation de Netsilon avec les autres produits présents sur le réseau, il est important de maintenir une identification du serveur de temps.**

Afin d'accéder au serveur web, il existe deux solutions :

- Avec serveur DHCP : attribution automatique d'une adresse IP.
- Sans serveur DHCP : attribution d'une adresse IP fixe manuellement depuis le clavier de commande dans le menu réseau de Netsilon.

3.1 Configuration usine

Les paramètres de configuration par défaut ont été choisis pour faciliter la configuration initiale. Un seul compte est activé en sortie d'usine.

- Compte utilisateur par défaut du serveur web :
  - Identifiant : bodetadmin
  - Mot de passe : admin49

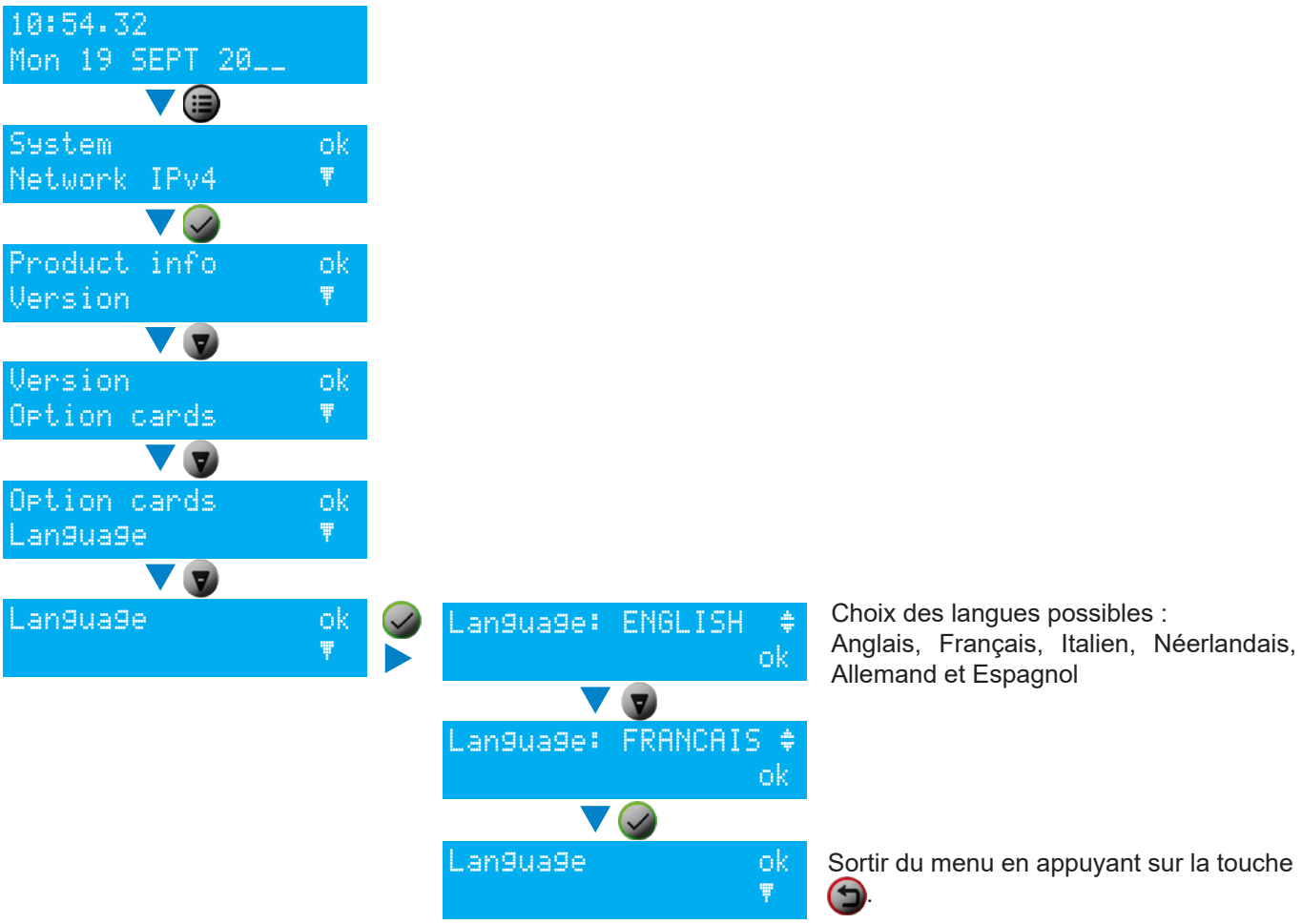
Ce compte ne peut pas être supprimé. En revanche, il est fortement recommandé de modifier le mot de passe (se reporter au chapitre 4.2.1.1 Changer le mot de passe du compte par défaut).

Lors du premier démarrage de Netsilon, les paramètres par défaut sont les suivants :

Fonctionnalités	État par défaut	Où configurer ?
Clavier de commande & écran LCD	Déverrouillé	Clavier de commande (menu technicien) + serveur web
	Langue : anglais	Serveur web
	Alternance des informations : heure, réseau, synchronisation et état système	Serveur web
Port USB	Activé	Serveur web
Port Ethernet ETH0	Services : HTTP : ON HTTPS : ON DNS : ON Console: ON SSH : ON	Serveur web
	Adresse IP non renseignée	Clavier de commande + serveur web

3.2 Choix de la langue d'affichage de l'écran LCD

Les paramètres réseaux pour la configuration du port ETH0 (attribution d'une adresse IP) peuvent être lus ou configurés à partir du clavier de commande de Netsilon. Au préalable, il est nécessaire de choisir la langue d'affichage du produit:

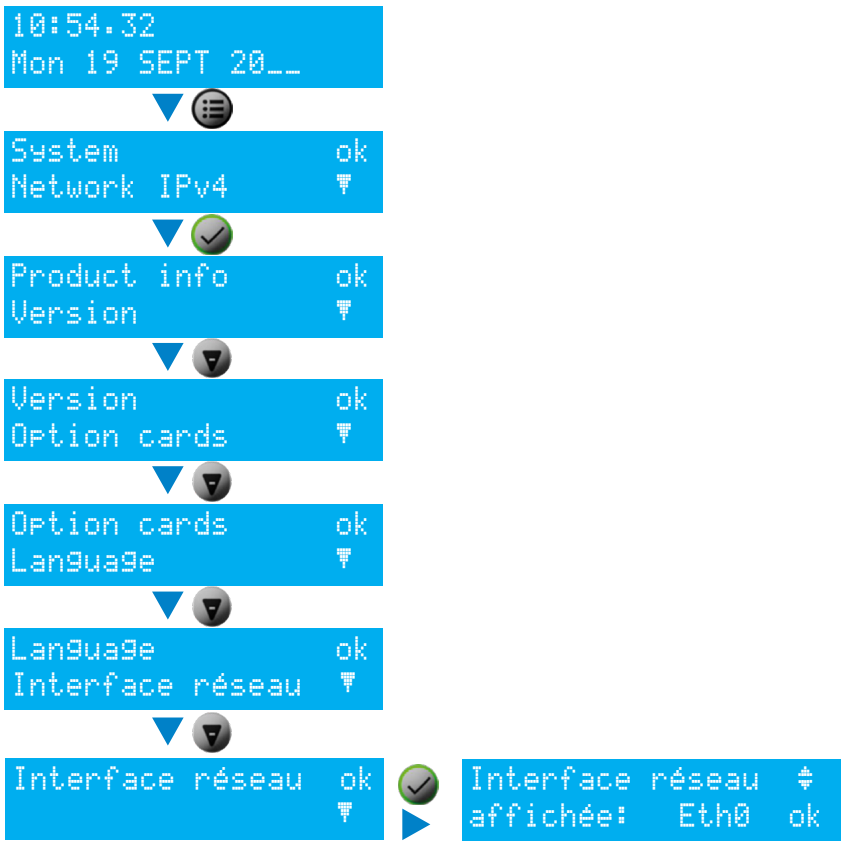


Choix des langues possibles : Anglais, Français, Italien, Néerlandais, Allemand et Espagnol

Sortir du menu en appuyant sur la touche .

3.3 Choix de l'interface réseau

Le produit étant relié au réseau, sélectionné sur l'écran LCD l'interface réseau concernée :



Eth0 clignote. Sélectionner l'interface à l'aide des bouton de navigation du clavier.

3.4 Configuration avec serveur DHCP

1) Au démarrage, le serveur de temps Netsilon 9 / 11 attend l'attribution automatique d'une adresse IP par le serveur DHCP. Cela peut prendre quelques minutes.

2) Une fois attribuée, cette adresse IP s'affiche à l'écran LCD. Par défaut, l'affichage de l'écran LCD alterne l'affichage de plusieurs paramètres. Pour lire l'adresse IP sur l'écran LCD, consulter le menu réseau en utilisant le clavier de commande et l'écran LCD de Netsilon :

3) Saisir l'adresse IP, lue sur l'écran LCD, dans le navigateur Internet (Google Chrome®, Mozilla Firefox, Microsoft Edge ou Internet Explorer®).

4) Se reporter au chapitre **4. Configuration par serveur web.**

192.168.1.0/24 est l'adresse IP avec CIDR (Classless Inter-Domain Routing).

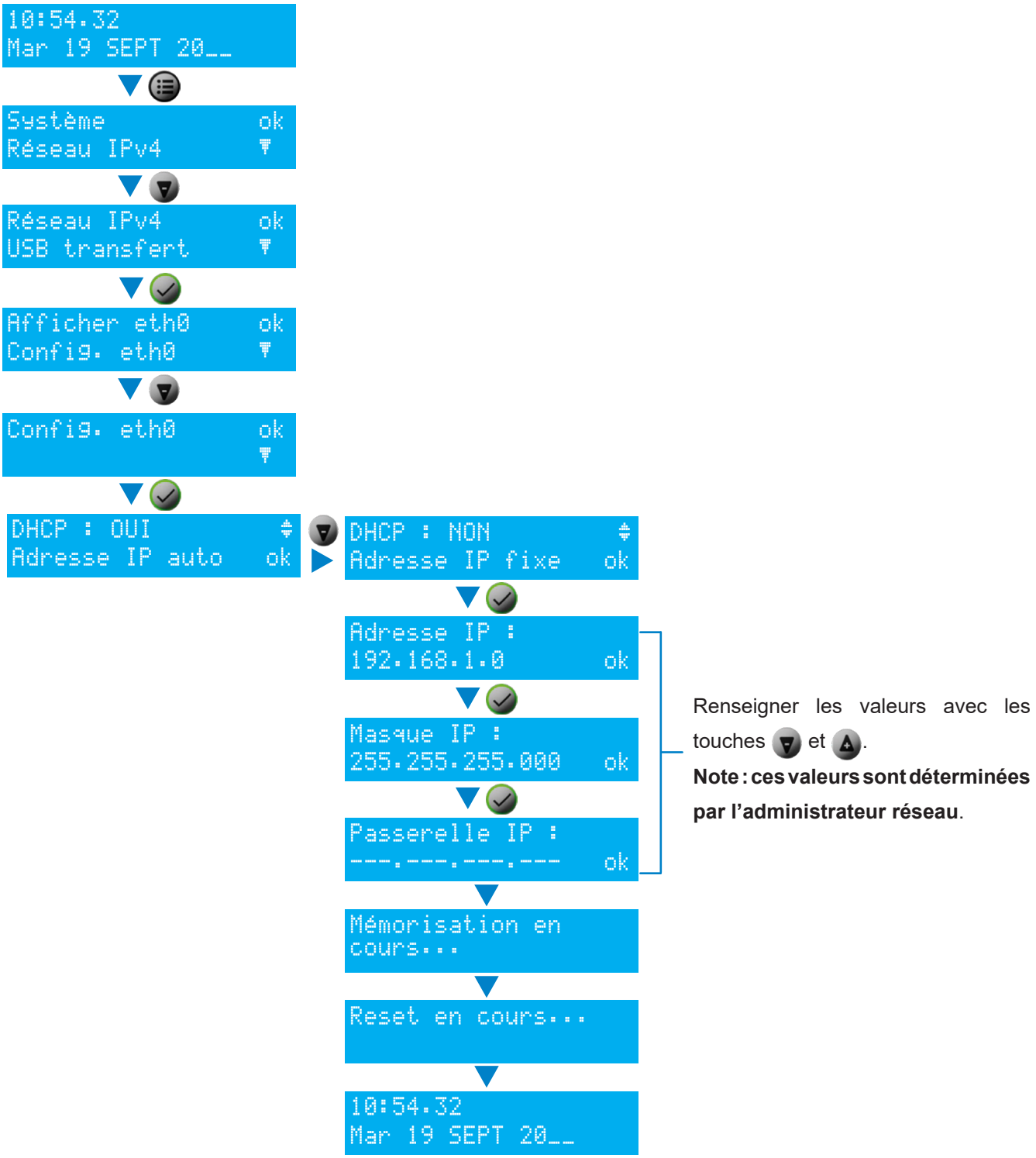
3.5 Configuration sans serveur DHCP

Sans l'attribution automatique d'une adresse IP par un serveur DHCP, il est nécessaire d'attribuer manuellement une adresse IP fixe.

Pour configurer manuellement les paramètres réseau de Netsilon, renseigner les trois paramètres suivants :

- Attribution de l'adresse IP
  - Il s'agit d'une adresse unique attribuée à Netsilon par l'administrateur du réseau. S'assurer que l'adresse choisie est disponible.
- Masque de sous-réseau
  - Le masque de sous-réseau définit le nombre de bits pris par l'adresse IP. Le nombre de bits utilisés dans le masque de réseau peut varier de 8 à 30 bits.
- Passerelle
  - L'adresse de la passerelle est nécessaire si la communication avec Netsilon est en dehors du réseau local. Par défaut, la passerelle est désactivée.

Pour configurer ces trois paramètres, utiliser le menu réseau de Netsilon à l'aide de son clavier de commande :



Renseigner les valeurs avec les touches et .

Note : ces valeurs sont déterminées par l'administrateur réseau.

4. CONFIGURATION PAR SERVEUR WEB

L'ordre des chapitres correspond aux étapes à réaliser dans le cadre d'une première mise en service. Il est important de respecter cet ordre pour le bon déploiement du système.

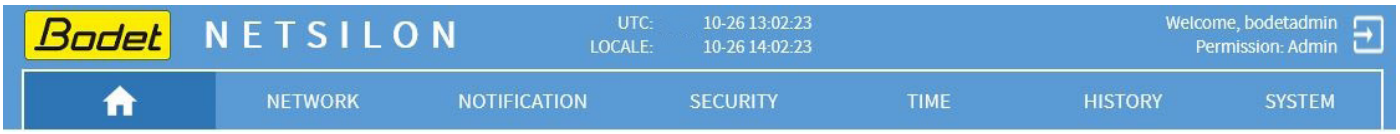
Les paramètres du serveur web présentés dans ce chapitre sont modifiables exclusivement avec le profil administrateur. Pour visualiser les droits en fonction du profil utilisé, se reporter à l'**annexe 3 : droits en fonction du profil**.

Pour accéder au serveur web de Netsilon, respecter les étapes suivantes :

1) Se munir de l'adresse IP de Netsilon.
2) Ouvrir une page du navigateur internet.
3) Renseigner l'adresse IP dans la barre d'adresse du navigateur web.
4) Renseigner l'identifiant et le mot de passe par défaut pour accéder au serveur web. Pour rappel :
   - Identifiant : bodetadmin
   - Mot de passe : admin49

4.1 Démarrage

4.1.1. Présentation du menu général



: tableau de bord permettant de visualiser l'état des synchronisation, des sources, des alarmes, des alimentations, le statut des sorties et les alarmes non acquittées.

RESEAU : configuration des interfaces, des routes statiques et des services réseaux.

NOTIFICATION : configuration des alarmes, du seuil des alarmes, des traps SNMP, du SMTP, de Syslog.

SECURITE : gestion des utilisateurs en local ou centralisée (LDAP, RADIUS), des agents SNMP, du SSH, des services HTTP/HTTPS, des certificats et des clés.

TIME : configuration des synchronisations (paramétrage, état et priorité des sources), des sorties, de la base temps et des échelles de temps (offset TAI/UTC, Leap Second manuel).

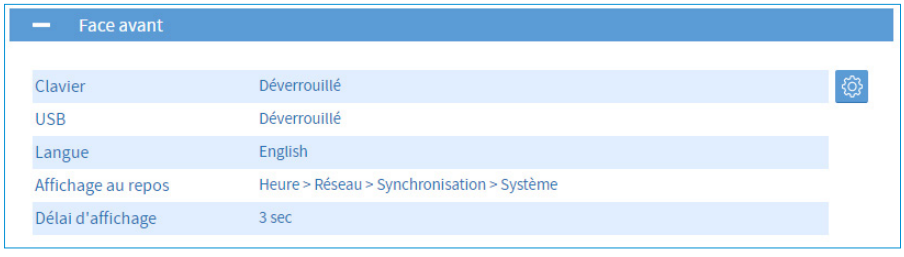
HISTORIQUE : consultation des statistiques GNSS, NTP, PTP, IRIG (en fonction des options sélectionnées) et oscillateur, des logs NTP, des Syslog logs et acquittement des alarmes.

SYSTEME : configuration du système, de l'affichage sur l'écran LCD, consultation des versions de firmware, aide en ligne et outils du système (mise à jour et sauvegarde, rédémarrage, versions des cartes options et exportation des logs).

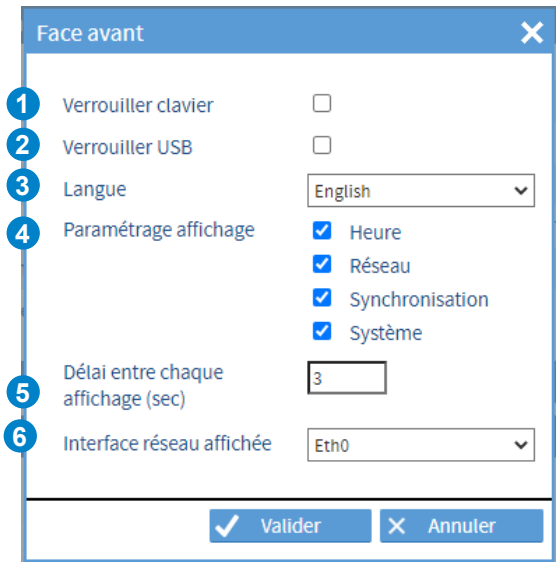
4.1.2. Paramétrer la face avant de Netsilon

Pour configurer l'interface (affichage LCD, port USB et clavier de commande), suivre les étapes ci-dessous :

1) Menu SYSTEME > Général > Face avant :



2) Cliquer sur , la fenêtre suivante apparaît :



3) Effectuer la configuration désirée :

1 Permet de verrouiller le clavier de commande de Netsilon lorsque la case est cochée.
› Cette fonction permet d'éviter toute mauvaise manipulation d'une tierce personne.

2 Permet de désactiver le fonctionnement du port USB présent en façade lorsque la case est cochée.
› Cette fonction permet d'éviter d'insérer une clé USB contenant des fichiers malveillants d'une tierce personne.

3 Permet de sélectionner la langue affichée sur l'écran LCD de Netsilon.
› Par défaut : anglais
› Langues disponibles : anglais, français, espagnol, allemand, néerlandais et italien.

4 Permet de sélectionner les paramètres défilants affichés sur l'écran LCD au repos de Netsilon :
› **Heure**
› Heure et date locale.
› **Réseau**
› Adresse IP
› Masque de sous-réseau
› Passerelle.
› **Synchronisation**
› Affichage de la ou les source(s) de synchronisation (primaire et/ou secondaire).
› **Système**
› Affichage de l'état du système (synchronisé, holdover, changement de référence entre synchronisation primaire et secondaire, non synchronisé et autonome). Afin d'interpréter ces états, se reporter à l'**annexe 1 : synchronisation**.

5 Permet de configurer le délai d'affichage de défilement entre chaque caractéristique (Heure, réseau, Synchronisation et Système) en seconde. Par défaut, ce temps est de 3s mais peut être programmé de 3 à 10 secondes.

6 Choix de l'interface réseau pour l'affichage et la configuration des paramètres sur la visu.

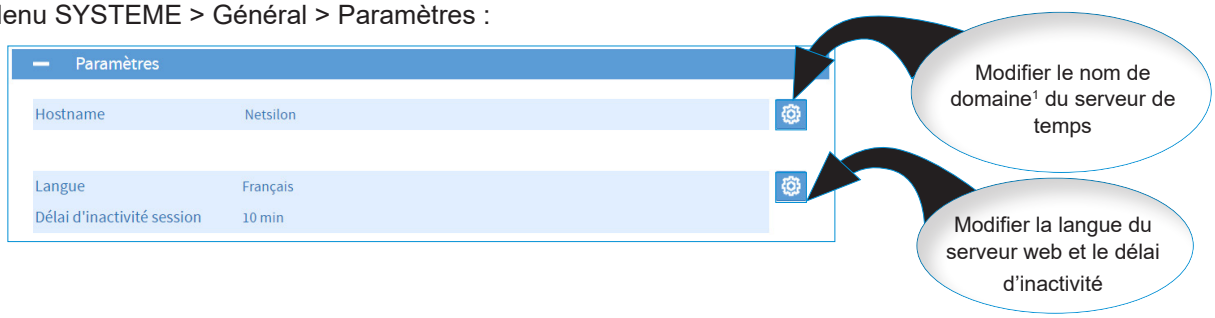
4) Cliquer sur Valider pour appliquer les modifications.

4.1.3. Changer la langue

Il est recommandé de changer la langue avant de commencer la configuration pour plus de confort de navigation.

Afin de choisir la langue d'affichage du serveur web, suivre les étapes ci-dessous :

1) Menu SYSTEME > Général > Paramètres :



2) **L'anglais est la langue par défaut.** Il est aussi possible de paramétrer le délai à partir duquel le serveur web se déconnecte pour revenir à la page d'identification.

Après la configuration de chaque paramètre, cliquer sur Enregistrer **pour appliquer les modifications.**

4.2 Gérer les utilisateurs

4.2.1. Gestion en local

La saisie d'un mauvais utilisateur/mot de passe génère une alarme (si activée).

Il existe un time-out de déconnexion automatique au bout duquel il y a déconnexion de l'utilisateur et perte éventuelle des modifications non validées. Par défaut, le time-out d'inactivité est de 10 minutes. (modifiable de 5 à 30 minutes)

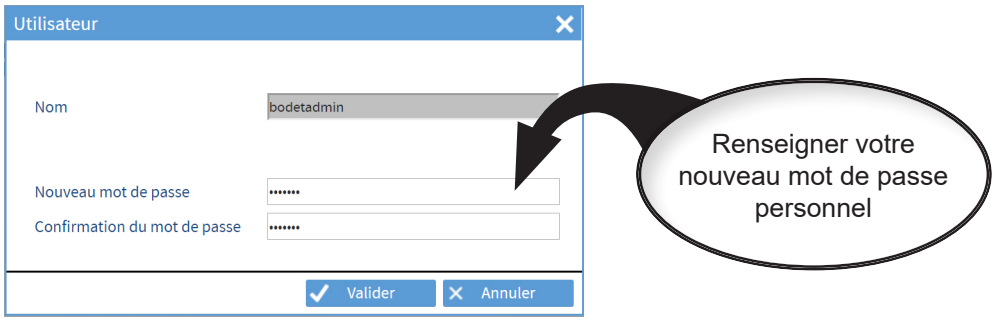
4.2.1.1 Changer le mot de passe

Pour rappel , il est fortement recommandé de modifier le mot de passe par défaut avant de commencer la configuration de Netsilon.

Pour changer le mot de passe du compte administrateur par défaut, suivre les étapes ci-dessous :

1) Menu SECURITE > Gestion utilisateurs > Utilisateur locaux

2) Cliquer sur Changer mon mot de passe , la fenêtre suivante apparaît :



3) Cliquer sur Valider pour appliquer les modifications.

Le mot de passe peut être saisi avec les paramètres suivants :

Alphabet autorisé: A-Z + a-z + 0-9 + caractères spéciaux : !#$%&()*+,-./ :; «<=>?@[]^_{|}~µ§ avec un total 94 symboles (dont 32 caractères spéciaux). A noter que le client SSH ou RS232 doit être configuré en UTF8 (pour le support des caractères µ et §).

Netsilon propose un chiffrement des mots de passe SHA-512. Il est également recommandé d'activer le « https » pour une sécurité renforcée.

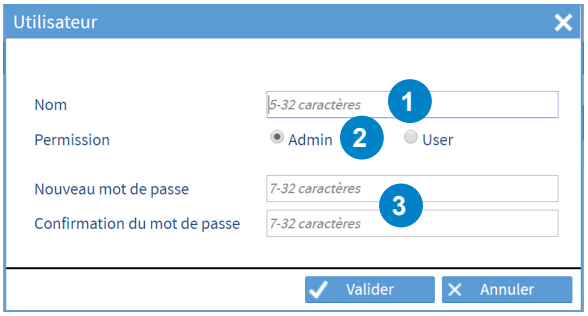
[1] *Le nom de domaine doit être individuel. Une fois modifier, celui-ci engendre la regénération du certificat autokey.*

4.2.1.2 Créer ou modifier un compte

Afin de créer un nouveau compte, suivre les étapes ci-dessous :

1) Menu SECURITE > Gestion utilisateurs > Utilisateurs locaux

2) Cliquer sur + pour ajouter un compte. la fenêtre suivante apparaît :



1. Saisir un nom d'utilisateur compris entre 5 et 32 caractères
2. Sélectionner un type de profil
3. Saisir un mot de passe compris entre 7 et 32 caractères

3) Cliquer sur Valider pour appliquer les modifications.

Netsilon peut gérer jusqu'à 20 utilisateurs. L'usage de doublons utilisateur n'est pas autorisé.
Le nom d'utilisateur peut être saisi avec les paramètres suivants :
Alphabet autorisé: a-z, A-Z, 0-9, -_.@

Se reporter à l'annexe 3 pour visualiser les différences des profils administrateur et utilisateur.

4.2.1.3 Supprimer un compte

Afin de supprimer un compte, suivre les étapes ci-dessous :

1) Menu SECURITE > Gestion utilisateurs > Utilisateurs locaux

2) Cliquer sur le compte à supprimer (afin de le sélectionner).

3) Cliquer sur − pour supprimer le compte. la fenêtre suivante apparaît :

3) Cliquer sur Oui pour appliquer la suppression.

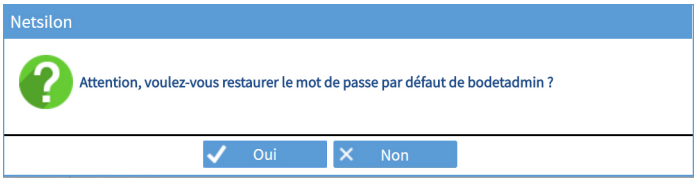
Il est impossible de supprimer le compte administrateur par défaut.

4.2.1.4 Restaurer le mot de passe par défaut

Afin de restaurer le mot de passe du compte administrateur par défaut, suivre les étapes ci-dessous :

1) Menu SECURITE > Gestion utilisateurs > Utilisateurs locaux

2) Cliquer sur Restaurer le compte admin par défaut, la fenêtre suivante apparaît :



3) Cliquer sur Oui pour appliquer les modifications.

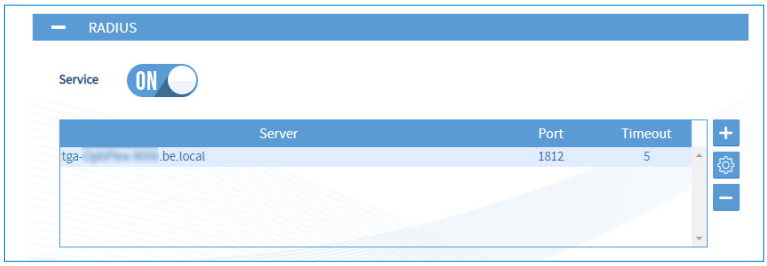
4.2.2. Gestion centralisée

4.2.2.1 Service RADIUS

L'authentification via RADIUS (Remote Authentification Dial-In User Service) implique l'utilisation d'un serveur externe permettant une gestion centralisée des utilisateurs pour se connecter à Netsilon. Le mot passe de connexion saisi par l'utilisateur est ainsi stocké dans un serveur RADIUS présent sur le réseau. Les échanges client/serveur sont sécurisés via une clé secrète partagée.

Pour activer et configurer un serveur RADIUS :

1) Menu SECURITE > Gestion utilisateurs > RADIUS
Activer le service à l'aide du bouton ON.



2) Ajouter un serveur RADIUS en cliquant sur +, la fenêtre suivante apparaît :

3) Saisir les informations liées au serveur RADIUS :
(Possibilité d'ajouter jusqu'à 5 serveurs maximum)

1. Saisir l'adresse IP ou le hostname,
2. Saisir le numéro de port RADIUS (port réseau par défaut : 1812),
3. Saisir la clé de sécurité partagée (hachage cryptographique MD5) avec Netsilon, (de 6 à 64 caractères)
4. Saisir le timeout (délai d'attente dans la communication avec Netsilon), (programmable de 3 à 60 secondes)

Il fortement recommandé d'utiliser des noms d'utilisateurs différents entre ceux utilisés via le serveur RADIUS et ceux utilisés en local. Ne pas dupliquer les utilisateurs (déclaration des comptes locaux en RADIUS et inversement). En local et en RADIUS , les users suivants ne sont pas autorisés : «radius_user», « radius_users».

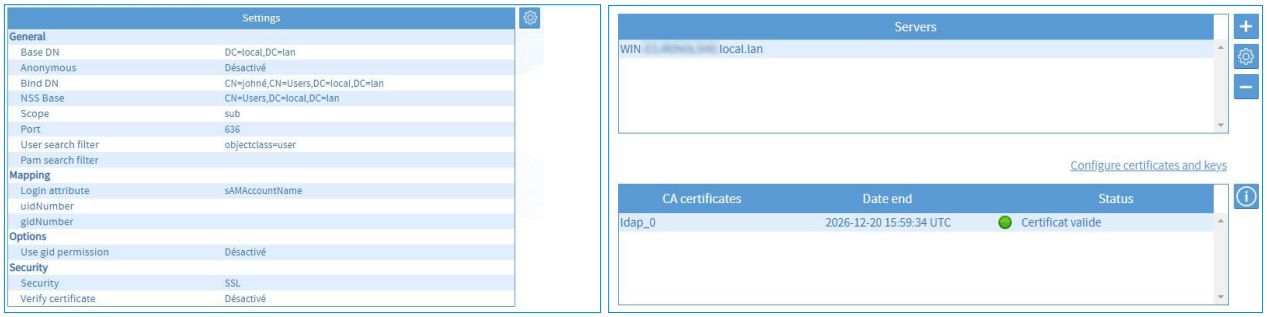
4.2.2.2 Service LDAP

L'authentification via LDAP (Lightweight Directory Access Protocol) implique l'utilisation d'un serveur externe permettant une gestion centralisée des utilisateurs pour se connecter à Netsilon. Le mot passe de connexion saisi par l'utilisateur est ainsi stocké dans un serveur LDAP présent sur le réseau. Ce protocole permet d'obtenir un accès à des bases d'informations sur les utilisateurs d'un réseau au moyen de l'interrogation d'annuaires. L'accès aux données stockées dans la base est sécurisé via des mécanismes de chiffrement et d'authentification.

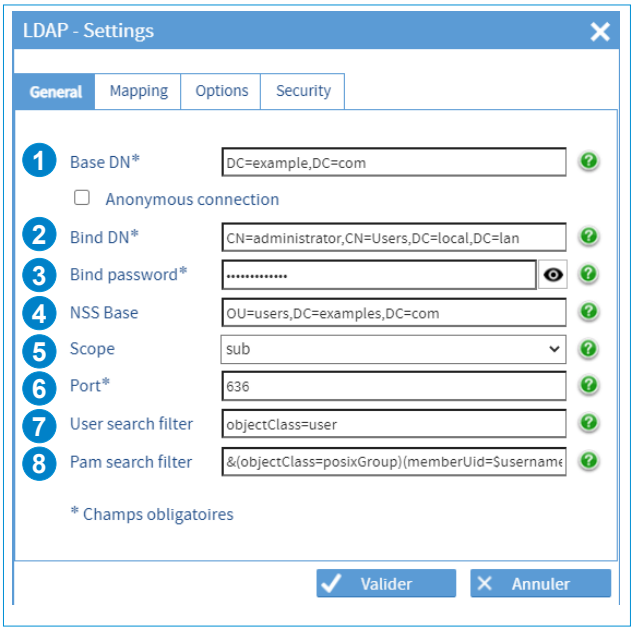
Pour activer et configurer le service LDAP:

1) Menu SECURITE > Gestion utilisateurs > LDAP
Activer le service à l'aide du bouton ON. L'activation / désactivation du service provoque un redémarrage du produit.

En fin de paramétrage (avant d'activer le service), cliquer sur Test connexion permet de s'assurer que la configuration est cohérente (connexion au serveur valide). Ce bouton de test est fonctionnel uniquement si le service est désactivé.



2) Pour effectuer le paramétrage, cliquer sur , la fenêtre suivante apparaît :



3) Compléter les différents champs permettant le paramétrage :

Onglet - General

1 Base DN (Distinguished Name) : saisir le nom de la base de recherche contenant les répertoires du serveur à être interrogés pour trouver une correspondance d'authentification. Généralement, c'est le niveau supérieur de l'arborescence de l'annuaire LDAP. Le DN est l'identifiant d'une entrée LDAP (chemin dans l'arborescence).

2 Bind DN (Distinguished Name to bind server with) : saisir un utilisateur sur le serveur LDAP autorisé à effectuer des recheches au sein de l'annuaire LDAP (dans son intégralité ou partiellement). La fonction du Bind DN est d'interroger l'annuaire à l'aide de requêtes filtrantes afin d'autoriser ou non l'authentification des utilisateurs. Ce champ est masqué si la fonction d'authentification anonyme (Anonymous connection) est activée.

3 Saisir le mot de passe qui correspond à l'utilisateur du Bind DN autorisé à effectuer des recherches au sein de l'annuaire. Ce champ est masqué dans le cas d'une authentification anonyme (Anonymous connection).
Le bouton permet de visualiser le mot de passe en clair uniquement lors de sa saisie.

4 Saisir les paramètres de la base de recherche (DN) pour indiquer le point d'entrée de la recherche des utilisateurs.

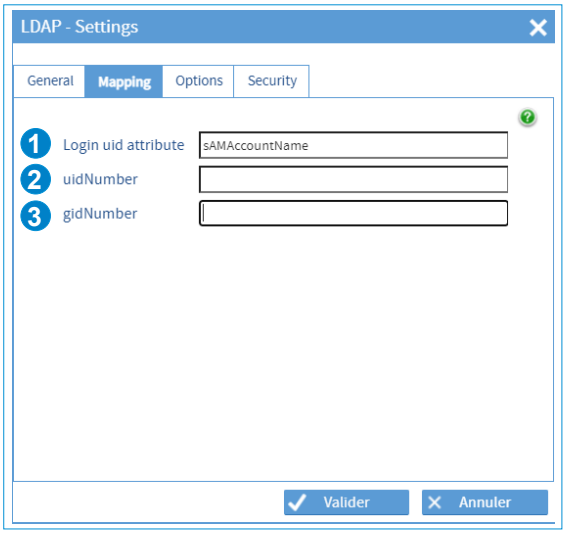
5 Choisir un périmètre de recherches LDAP, parmi «Sub», «One» et «Base» :
- Sub : l'intégralité de la base de recherche (toutes les entrées) est concernée,
- One : seules les entrées immédiatement subordonnées à l'entrée spécifiée comme base de recherche sont concernées,
- Base : seule l'entrée spécifiée comme base de recherche est concernée.

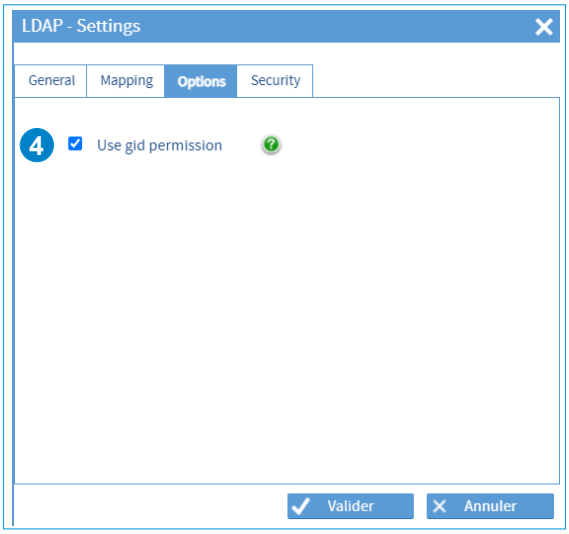
6 Choisir le numéro de port du service LDAP en fonction du paramétrage de la sécurité.
Ports standards par défaut : Désactivé : 389, StartTLS : 389, SSL : 636.

7 Saisir un filtre de recherche permettant de choisir les entrées à renvoyer lors d'une opération de recherche.

8 Saisir un filtre additionnel, si l'utilisateur correspond aux règles du filtre, l'accès est autorisé, sinon l'accès est refusé. Exemple : &(objectClass=posixGroup)(memberUid=$username)(cn=group01).

Onglets - Mapping / Options





Si une ou plusieurs de ces variables n'existent pas dans la base de votre serveur LDAP au niveau des comptes utilisateurs, les connexions seront impossibles. Il est cependant possible de mapper les variables suivantes «Login uid attribute », « uidNumber » et « gidNumber » vers d'autres variables.

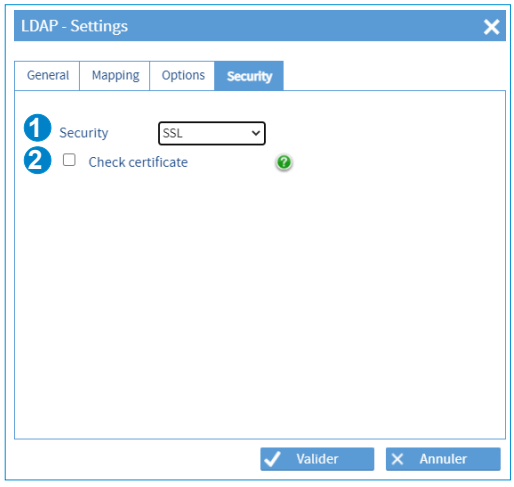
1. Variable correspondant à l'attribut du login utilisé lors de la connexion. Cette variable peut être mappée par exemple vers sAMAccountName dans le cas d'un serveur Active Directory (Microsoft).

2. uidNumber est un identifiant numérique d'utilisateur. Les utilisateurs doivent disposer d'un uidNumber dont la valeur doit être supérieure ou égale à 1050. En cas de mappage vers un autre attribut, vérifier que la valeur est bien supérieure ou égale à 1050 par utilisateur.
uidNumber peut être déclaré manuellement par utilisateur dans le cas d'un serveur Active Directory (Microsoft).

3. gidNumber est un identifiant de groupe et doit être supérieur ou égale à 1 pour une authentification sur Netsilon. En cas de mappage vers un autre attribut, vérifier que la valeur est bien supérieure ou égale à 1 par utilisateur.

4. Si l'option n'est pas activée, les utilisateurs doivent disposer d'un gidNumber supérieur ou égale à 1 et auront un accès au Netsilon avec les droits administrateur.
Si l'option est activée, Netsilon vérifie le gidNumber de l'utilisateur pour lui attribuer les droits :
- gidNumber = "111" : les utilisateurs disposeront des droits administrateur.
- gidNumber = "112" ou une valeur supérieur ou égale à 1 : les utilisateurs auront les droits utilisateur.

Onglet - Sécurité

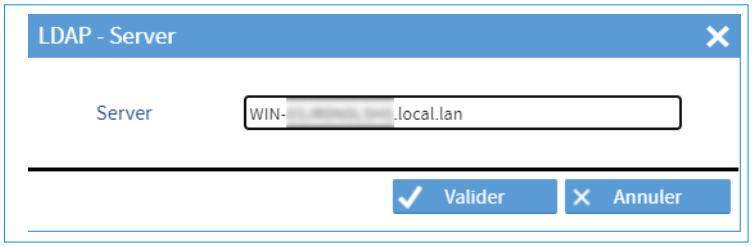


1. Choisir le type de sécurité : désactivé, SSL (chiffrement des échanges / des mots de passe), StartTLS.
Cela implique un basculement du numéro de port TCP.

2. Cocher pour activer la vérification des certificats.
Si activé, le certificat du serveur est requis.
Par défaut, si aucun certificat n'est fourni (ou un certificat défectueux), la session est interrompue automatiquement.

L'ajout d'un certificat permet de générer un chiffrage et d'éviter une liaison en clair.
La vérification du certificat permet de contrôler l'authenticité du serveur.
Pour ajouter un certificat, reportez-vous au chapitre 4.10 Gestion des certificats et des clés.

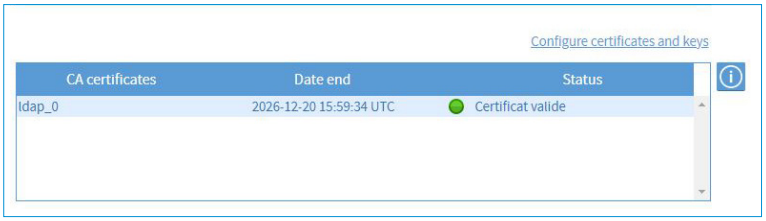
4) Ajouter un serveur LDAP en cliquant sur +, la fenêtre suivante apparaît :
(Possibilité d'ajouter jusqu'à 5 serveurs maximum)

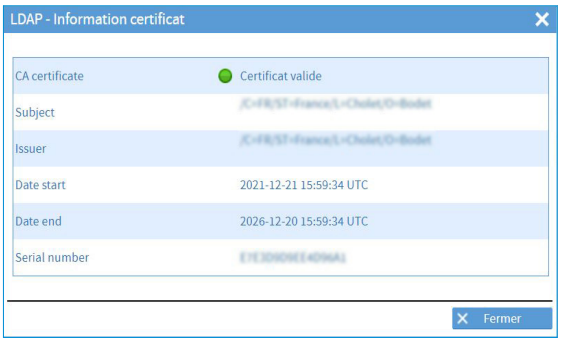


Saisir l'adresse IP ou le hostname du serveur LDAP.

Pour la validation du certificat, il faut indiquer obligatoirement le « full hostname » (FQDN) du serveur LDAP.
Il fortement recommandé d'utiliser des noms d'utilisateurs différents entre ceux utilisés via le serveur LDAP et ceux utilisés en local.
Ne pas dupliquer les utilisateurs (déclaration des comptes locaux en LDAP et inversement).

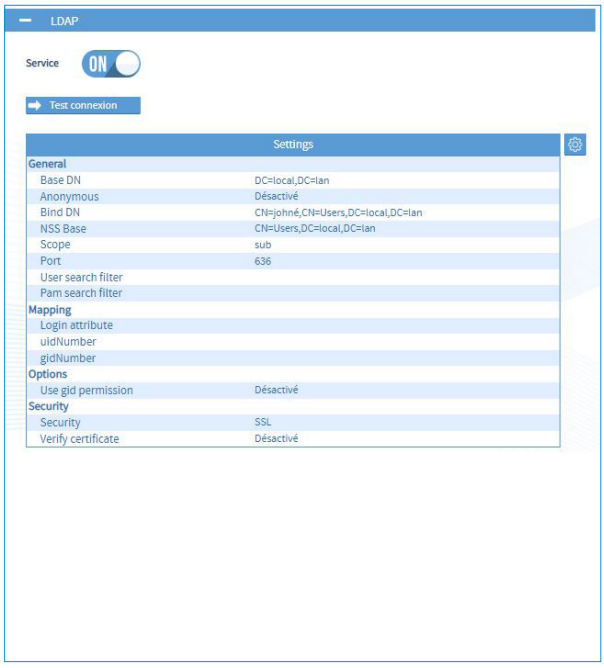
5) Cliquer sur ⓘ pour visualiser les informations du certificat éventuellement importé depuis le pool des certificats et sur configure certificates and keys pour accéder à ce pool.





Ci-dessous, pour exemple, des configurations typiques du service LDAP :

Serveur Windows Active directory en mode sécurisé



Serveur linux OpenLdap

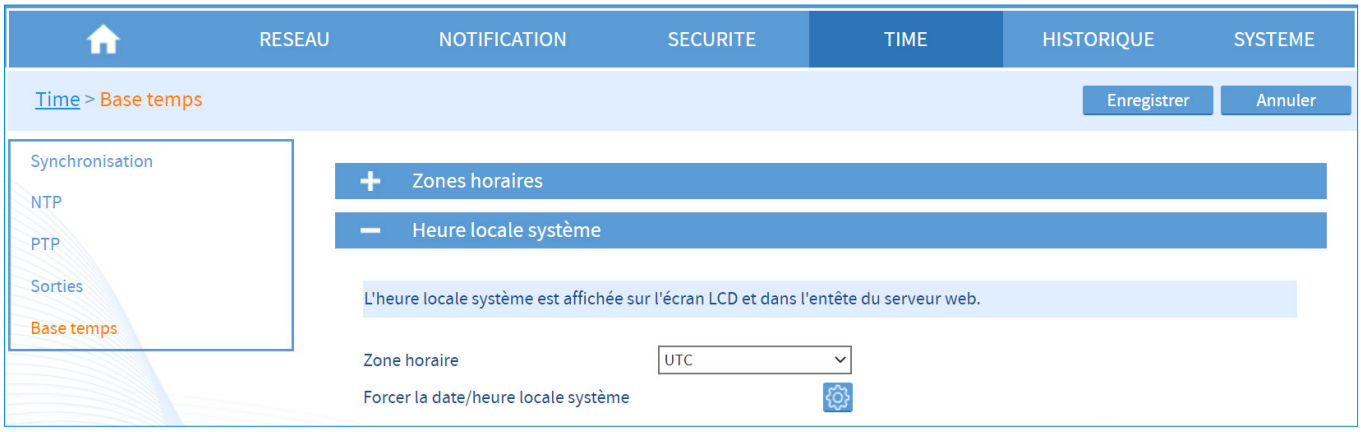
4.3 Configurer les bases de temps

La section base de temps permet de centraliser la création des zones horaires et la gestion des échelles de temps. Chaque sortie pourra être définie sur une zone horaire, préalablement défini dans ce chapitre.

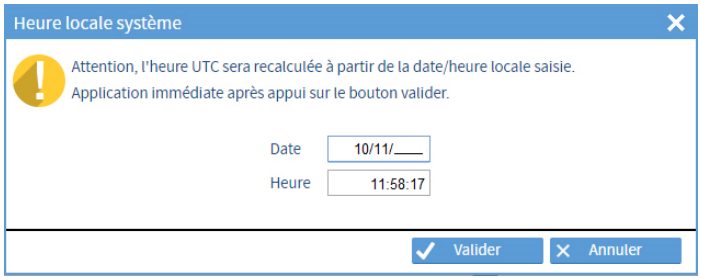
4.3.1. Définir l'heure et la date du système

La modification de l'heure locale doit être effectuée uniquement en cas de changement de la pile CR2032.

Pour l'heure et la date du système, suivre les étapes ci-dessous :
1) Menu TIME > Base temps > Heure locale système.

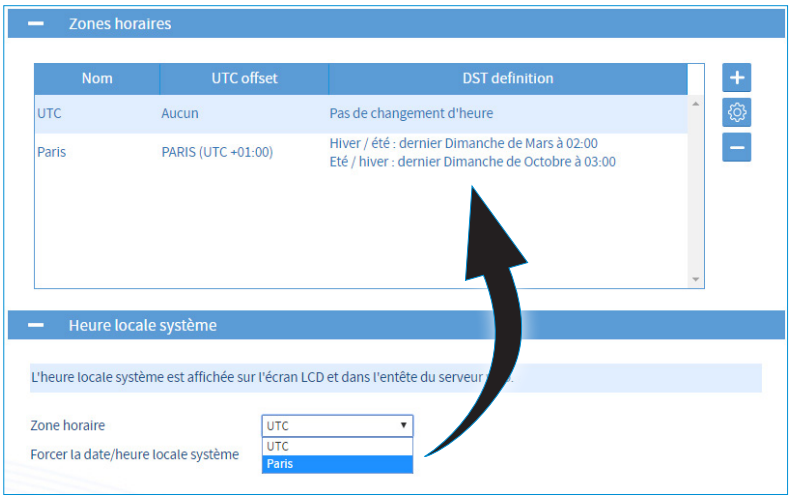


2) Cliquer sur , la fenêtre suivante apparaît :



3) Modifier manuellement l'heure et la date.

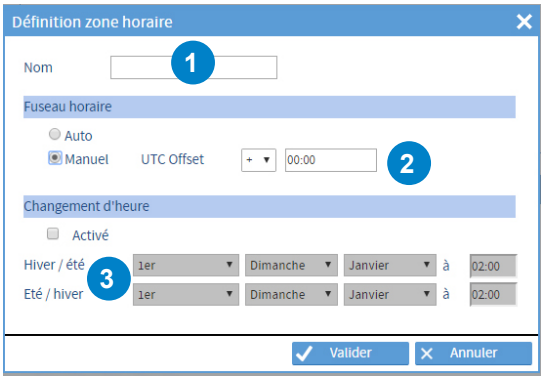
4) Choisir la zone horaire depuis le menu déroulant. Les zones horaires précédemment ajoutées sont présentes :



L'heure locale est l'heure affichée sur l'écran LCD.

4.3.2. *Créer une zone horaire manuellement*

Pour créer une zone horaire, suivre les étapes ci-dessous :
1) Menu TIME > Base temps > Zones horaires.
La référence UTC est présente par défaut.
2) Cliquer sur + pour créer une zone puis cocher **Manuel**, la fenêtre suivante apparaît :

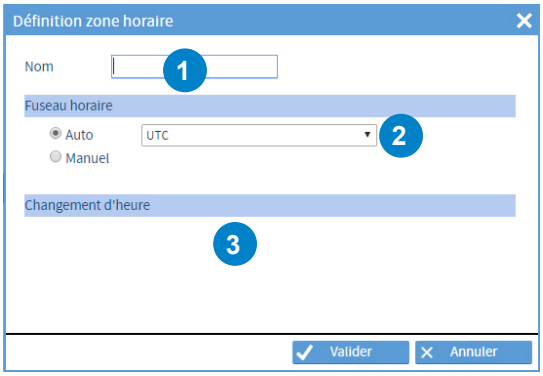


1 Renseigner le nom de la zone horaire.
2 Définir le décalage horaire par rapport à la référence UTC. Le menu déroulant permet d'attribuer un décalage positif ou négatif. Saisir les heures et minutes souhaitées pour ce décalage. Le décalage manuel maximum est limité à -12h/+14h.
3 Si la zone est conditionnée par un changement d'heure : activer puis renseigner les changements d'heures désirés.

Il est possible de choisir un jour périodique dans un mois ou de définir une date.

4.3.3. *Créer une zone horaire automatiquement*

Pour ajouter une zone horaire, suivre les étapes ci-dessous :
1) Menu TIME > Base temps > Zones horaires.
La référence UTC est présente par défaut.
2) Cliquer sur + pour ajouter une zone, la fenêtre suivante apparaît :



1 Renseigner le nom de la nouvelle zone horaire.

2 Choisir la zone horaire dans le menu déroulant :

DÉCALAGE UTC	VILLES
UTC-10:00	HAWAI
UTC-08:00	LOS ANGELES
UTC-07:00	DENVER
UTC-06:00	CHICAGO
UTC-05:00	NEW YORK
UTC-04:00	FORT-DE-FRANCE
UTC-03:00	CAYENNE
UTC-01:00	ACORES
UTC+00:00	LONDRES
UTC+01:00	PARIS
UTC+01:00	TUNIS
UTC+02:00	HELSINKI
UTC+03:00	MOSCOU
UTC+03:00	SAINT-DENIS

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

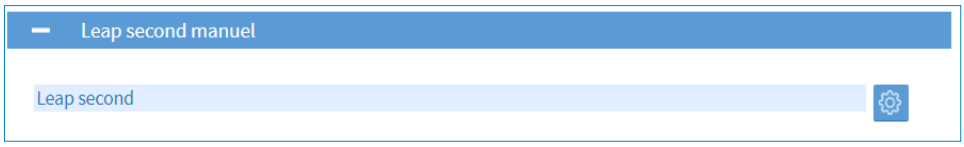
3 Les changements d'heures sont indiqués en fonction du fuseau horaire choisi.

Il est possible de créer jusqu'à 20 zones maximum (y compris l'UTC).
La zone UTC n'est pas supprimable.

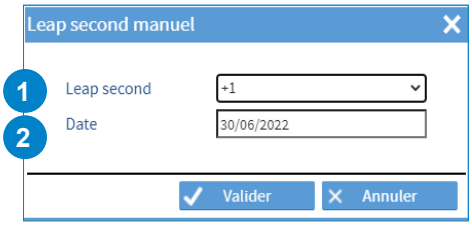
4.3.4. Programmer un Leap Second manuel

Si la programmation d'un Leap Second est prévue et dans le cas où Netsilon est synchronisé depuis une source ne gérant pas cette information (exemple : synchronisation IRIG), alors elle doit être saisie manuellement dans Netsilon.
En l'absence de cette information, celle-ci ne sera pas transmise aux clients NTP et un saut de temps d'une seconde sera effectif après le passage du Leap Second.
Dans le cas où Netsilon est Master PTP, l'offset TAI / UTC ne sera pas à jour.

Pour ajouter un Leap Second manuel, suivre les étapes ci-dessous :
1) Menu TIME > Base de temps > Leap second manuel



2) Cliquer sur pour définir le Leap Second, la fenêtre suivante apparaît :



1 Définir la valeur du Leap Second : + / - 1 seconde.

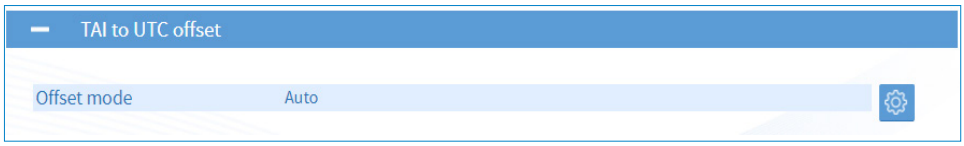
2 Définir la date du Leap Second : **programmation pour un 30/06 ou un 31/12 obligatoirement.**

En cas de gestion du Leap Second par la source de synchronisation utilisée, il est toujours possible de programmer un Leap Second manuel. Celui-ci prend alors l'ascendant et permet de s'assurer que le Leap Second sera bien appliqué.
Le Leap Second programmé manuellement s'efface dès que celui-ci est passé.

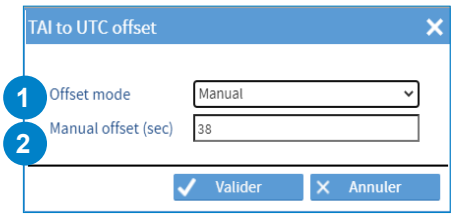
4.3.5. Définir l'offset TAI / UTC

Si la source de synchronisation utilisée ne fournit pas le nombre de Leap Second (exemple : IRIG) et si Netsilon diffuse en TAI, il faut impérativement renseigner cette valeur manuellement dans Netsilon. L'offset TAI/UTC est notamment dédié au cas particulier d'une synchronisation IRIG si Netsilon est master PTP (reportez vous au chapitre 4.5.5 Carte option IRIG INPUT).

Pour saisir manuellement l'offset TAI/UTC, suivre les étapes ci-dessous :
1) Menu TIME > Base de temps > TAI to UTC offset



2) Cliquer sur ⚙ pour paramétrer la gestion de l'offset, la fenêtre suivante apparaît :



1 Définir le mode d'offset : automatique / manuel.
Si la source de synchronisation fournit l'information du nombre de Leap Second, le choix du mode automatique est recommandé. Dans le cas contraire, choisir le mode manuel.

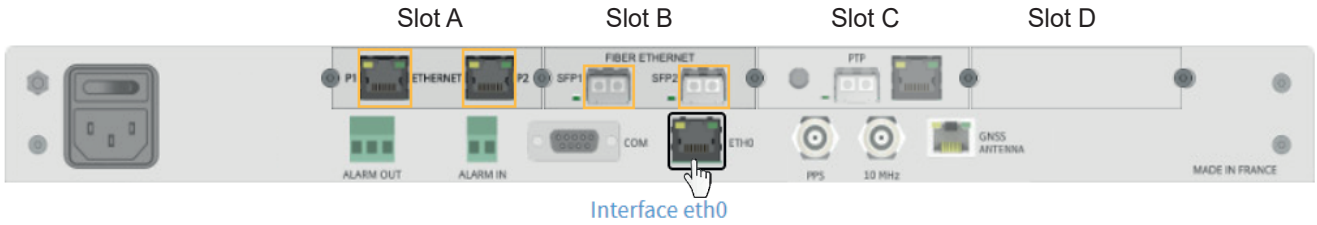
2 Saisir la valeur de l'offset (disponible en mode manuel uniquement).

Au passage d'un Leap Second programmé manuellement, l'offset manuel TAI/UTC évoluera en conséquence (+/- 1).

4.4 Paramétrage du réseau informatique

1) Cliquer sur le RESEAU afin de configurer les interfaces réseaux.

Concernant la configuration des interfaces réseaux, la navigation est interactive : passer la souris sur le connecteur de l'interface à configurer puis cliquer dessus :



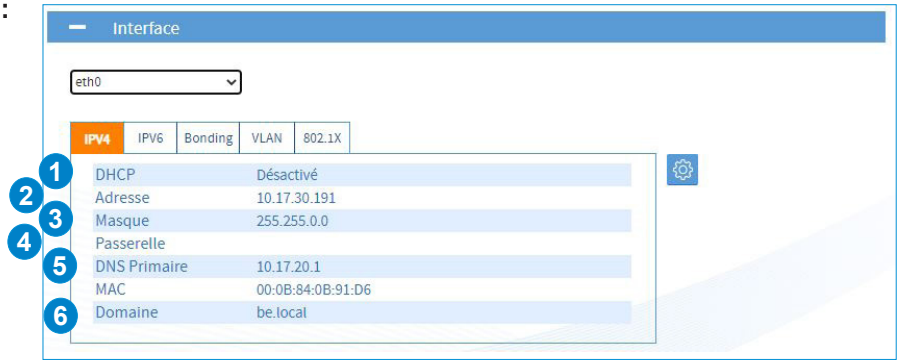
Interface eth0

4.4.1. *Configuration des interfaces réseaux*

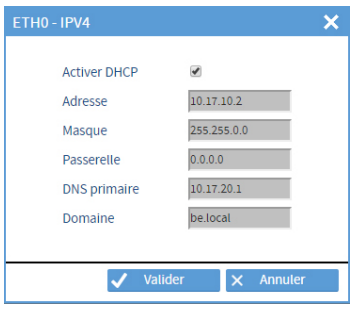
Pour configurer une interface réseau, suivre les étapes ci-dessous :

1) Menu RESEAU > Interfaces > interface ethx :

Configuration IPv4 :



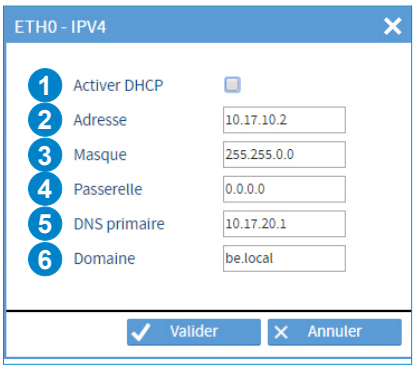
2) Cliquer sur ⚙, la fenêtre suivante apparaît :



3) Configurer les différents paramètres :

1 Avec serveur DHCP : cocher la case. L'attribution de l'adresse IP et des paramètres réseaux seront automatiques.

2 Sans serveur DHCP : indiquer manuellement l'adresse IP fixe pour ce port réseau.

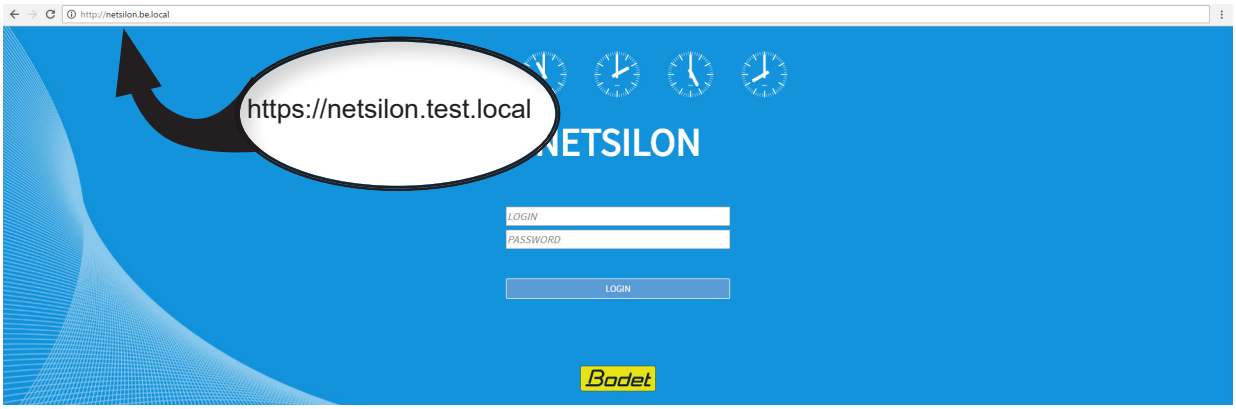


3 Indiquer le masque de sous-réseau afin de définir les adresses IP des produits qui pourront communiquer avec Netsilon.

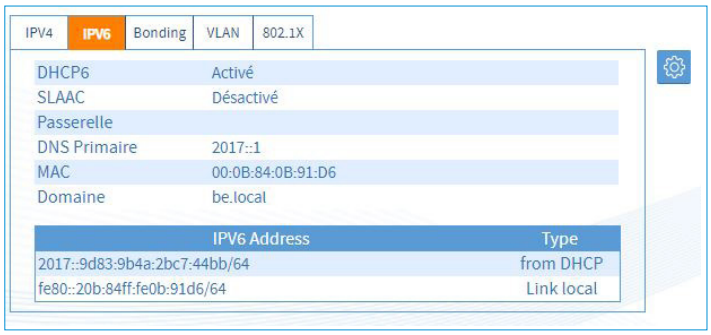
4 Définir la passerelle si un produit se trouve en dehors du réseau local (LAN).

5 Définir l'adresse du DNS primaire afin d'attribuer un nom de domaine.

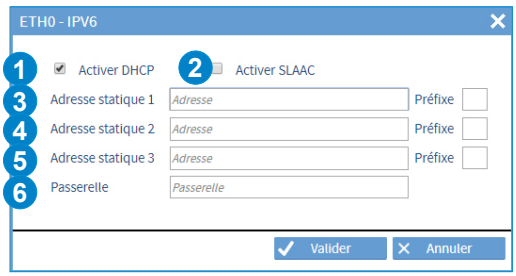
6 Définir l'extension du nom de domaine afin d'accéder au serveur web du produit à partir du DNS.
Ex.: si le nom du produit est «Netsilon» (se reporter au chapitre **4.1 Démarrage**)
Exemple d'accès au serveur web à partir du nom de domaine :



Configuration IPv6 :



1) Cliquer sur , la fenêtre suivante apparaît :



1 Activer DHCP (statefull) pour l''attribution de l'adresse IP et des paramètres réseaux (automatiques).

2 Activer SLAAC (stateless avec DHCP) pour attribuer automatiquement une adresse IP à Netsilon, permet aussi de récupérer la passerelle.

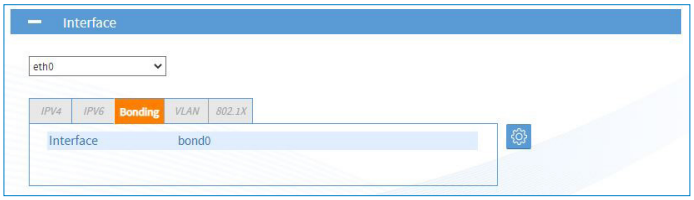
L'activation du DHCP (en supplément du SLAAC) permet d'obtenir les options DHCP (ex.: DNS, Domine) en plus de l'adresse IP fixée par le processus SLAAC (pas d'attribution IP par DHCP dans ce mode). Le DHCP est activé par défaut. Il est possible de cumuler les modes «statique»/»DHCP»/ «SLAAC».

3 4 5 Adresses IP fixes. Indiquer le préfixe défini par l'administrateur du réseau.

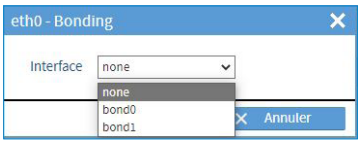
6 Passerelle réseau définie par l'administrateur du réseau. (Attention, il faut au moins une adresse statique pour la prise en compte de la passerelle).

Bonding (redondance Ethernet) :
Le bonding permet de lier des interfaces réseaux (cela implique la présence d'au moins une carte option Network dans Netsilon) dans un groupe appelé "bond". Cette redondance au niveau des ports offre une sécurité en cas de défaillance d'une interface réseau, le serveur de temps restant toujours accessible et disponible via une ou plusieurs autres interfaces du groupe (bond). Il existe deux modes de fonctionnement possible pour chaque bond.
Pour affecter une interface à un bond puis choisir son mode de fonctionnement :

1) Sélectionner une interface puis choisir l'onglet "Bonding",



2) Cliquer sur ⚙, la fenêtre suivante apparaît :



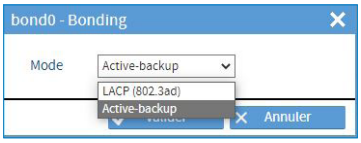
3) Sélectionner l'affectation de l'interface au groupe (bond) souhaité avec la liste déroulante.

Lorsqu'une interface est rattachée à un bond, sa configuration sera celle du bond auquel elle appartient. La configuration d'un bond est similaire à celle d'un port Ethernet.
Lors du rattachement d'une interface à un bond, les paramètres 802.1x de l'interface qui passe en bond sont réinitialisés. Lorsque le bond est supprimé (aucune interface reliée au bond), les paramètres 802.1x du bond sont réinitialisés.

4) Renouveler ces étapes pour les interfaces à rattacher dans un bond,

5) Paramétrer le mode de fonctionnement du bond en le sélectionnant puis choisir l'onglet "Divers" :

6) Cliquer sur ⚙, la fenêtre suivante apparaît :



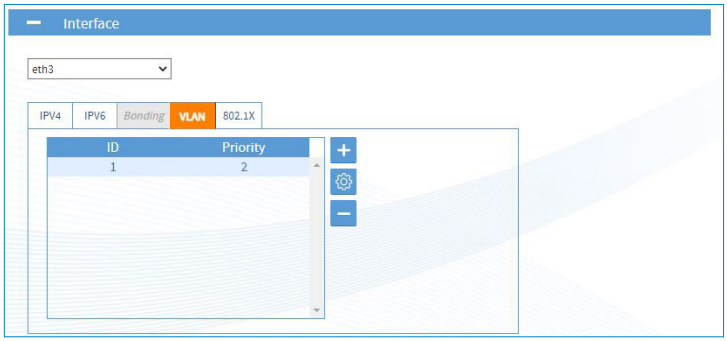
7) Choisir le mode de fonctionnement de ce bond avec la liste déroulante :
Active-backup : une interface physique du groupe fait transiter tout le trafic réseau du groupe. Les autres interfaces physiques sont alors passives. Si l'interface active perd la connexion, une des interfaces passives du groupe prend le relais de manière transparente.
LACP : toutes les interfaces du groupe sont agrégées ensemble et travaillent de manière dynamique, ce qui augmente le niveau de sécurité en cas de panne. Ce mode de fonctionnement implique une prise en charge du LACP par les autres équipements du réseau.

Sur un bond Ethernet, l'élément limitant étant le CPU, le doublement du bond n'apportera pas d'augmentation de la bande passante. Un maximum de 2 bonds est possible au total.

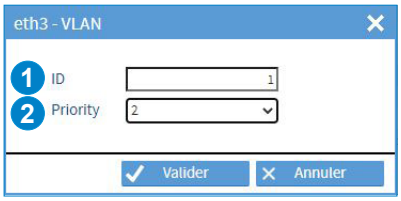
VLAN (réseau local virtuel) :
Les VLAN renforcent la sécurité informatique des réseaux en permettant la constitution de segments logiques de faible ampleur à l'intérieur d'un vaste réseau physique. Chaque VLAN dispose d'un domaine de diffusion broadcast propre.
Netsilon utilise le "VLAN tagged" avec une attribution aux réseaux locaux virtuels par l'intermédiaire d'une balise (tag) dans la trame du paquet de messages. La balise contient l'identifiant au réseau local virtuel (VID) et permet au switch de déterminer dans quel VLAN la communication s'effectue. Les propriétés de la balise autorise 4094 VLAN différents.
Dans Netsilon, le support VLAN permet de rattacher un port réseau (ou un bond) par lequel va transiter les données vers un ou plusieurs VLAN désignés (VLAN ID).

Pour lier un port réseau (ou un bond) vers un ou plusieurs VLAN :

1) Sélectionner le port Ethernet (ou bond) parent puis choisir l'onglet "VLAN" :



2) Cliquer sur + ou ⚙ pour ajouter ou configurer une interface VLAN, la fenêtre suivante apparaît :



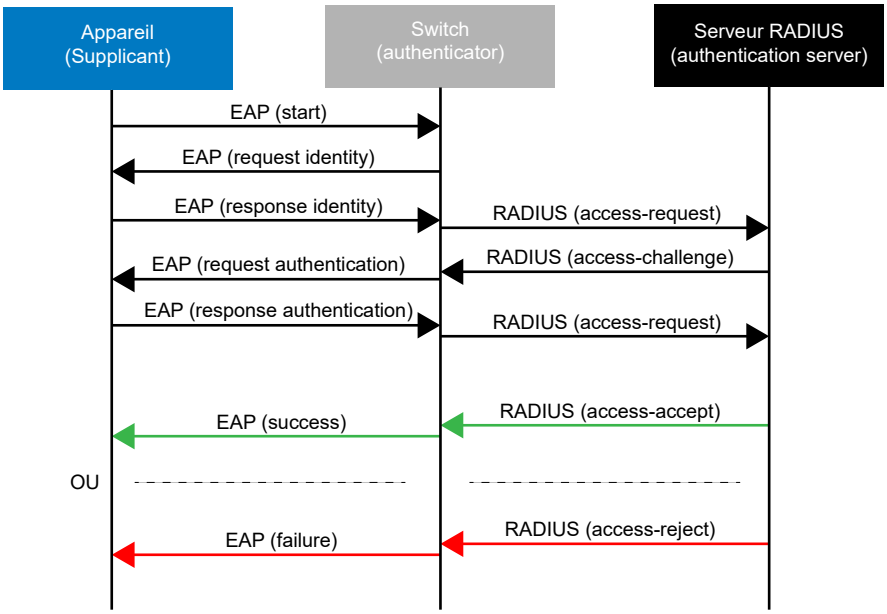
1. Saisir l'identifiant du VLAN (de 1 à 4094).
2. Sélectionner un indice de priorité (de 0 à 7) pour optimiser le trafic des messages (qualité de service).

Il est possible d'effectuer jusqu'à 20 rattachements répartis sur les différentes interfaces sans limitation.
Le libéllé sera affiché sous le format : [eth/bond].[VLAN ID] dans la liste des interfaces.
Il est possible de configurer les interfaces VLAN (IPV4 / IPV6).

Protocole d'authentification 802.1x :
Le protocole 802.1x permet de contrôler l'accès des équipements aux infrastructures réseau par un processus d'authentification des appareils souhaitant se connecter au réseau.

Le processus d'authentification se déroule de la manière suivante :
1. L'appareil (appelé supplicant) cherchant à rejoindre le réseau se connecte au point d'entrée de celui-ci par un switch (appelé authenticator).
2. Le switch active un port ne laissant transiter que les trames 802.1x et demande à l'appareil de s'identifier.
3. En réponse, l'appareil transmet son identifiant au switch qui fait parvenir cette information jusqu'à un serveur d'authentification de type RADIUS (appelé authentication server).
4. Le serveur RADIUS reçoit l'identifiant de l'appareil et lui demande de prouver son identité en fournissant un mot de passe ou un certificat.
5. L'appareil fournit les données d'authentification demandées au serveur RADIUS qui contrôle alors la validité des informations transmises.
6. Si les informations fournies par l'appareil sont valides, le serveur RADIUS ordonne au switch d'autoriser l'accès au réseau à l'appareil. Dans le cas contraire, l'accès est refusé et l'appareil reste sur un réseau de quarantaine.

Le schéma ci-après synthétise les trames échangées pendant le processus d'authentification :



Le procotole EAP (Extensible Authentication Protocol) gère le transport des informations d'identification suivant le mode client/serveur. Il gère le transport des protocoles d'authentification pour sécuriser les communications.

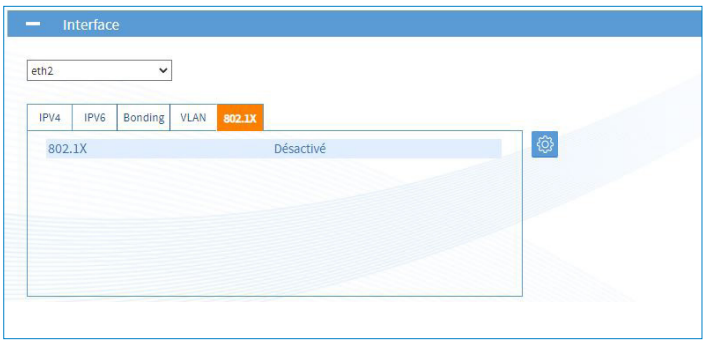
Netsilon supporte les protocoles d'authentification suivants :

Protocoles d'authentification	Authentification interne associée
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

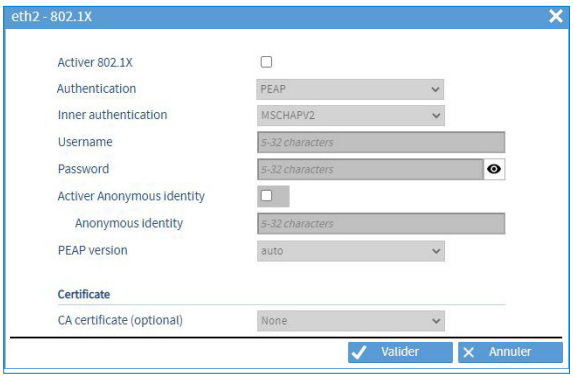
Pour effectuer la configuration du protocole 802.1x sur les interfaces Ethernet ou sur les bonds :

Le VLAN hérite de la configuration de l'interface Ethernet ou du bond associé.

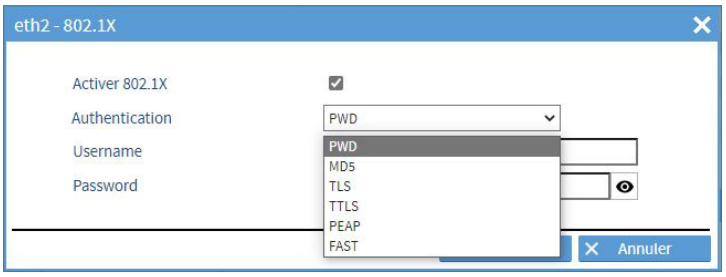
1) Sélectionner une interface Ethernet ou un bond, puis choisir l'onglet "802.1x" :



2) Cliquer sur , la fenêtre suivante apparaît :



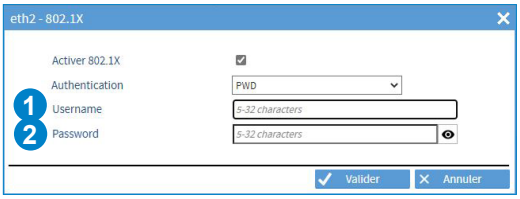
3) Activer le protocole 802.1x en cochant la case d'activation puis choisir le type de protocole d'authentification :



Le champs "Authentication" désigne le protocole utilisé pour sécuriser la connexion 802.1x entre le supplicant et l'authenticator et identifier le supplicant à l'aide de son identité ou username.

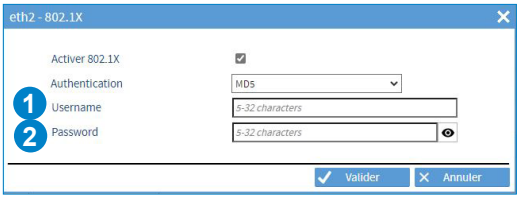
4) Effectuer le paramétrage suivant le protocole d'authentification choisi :

- PWD : authentification par mot de passe.



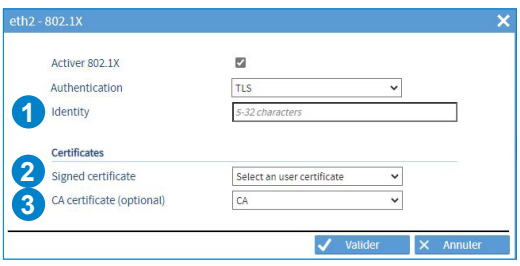
1. Saisir l'username du supplicant (Netsilon).
2. Saisir le mot de passe.
   Celui-ci sera vérifié par le serveur d'authentification.

- MD5 : authentification de l'appareil (supplicant) par un protocole de défi-réponse (avec le serveur d'authentification) avec la fonction de hachage MD5.



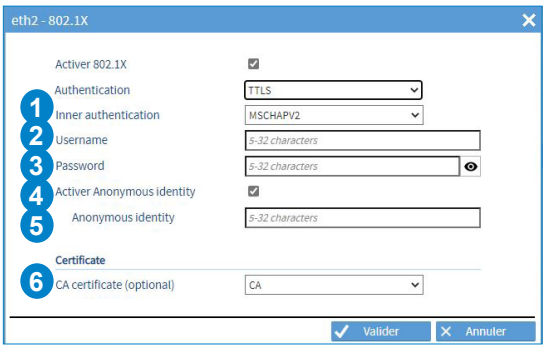
1. Saisir l'username du supplicant (Netsilon).
2. Saisir le mot de passe. Celui-ci est protégé par hachage et sera vérifié par le serveur d'authentification.

- TLS : authentification mutuelle de l'appareil (supplicant) et du serveur par l'utilisation de certificats.



1. Saisir l'identifiant du supplicant (Netsilon).
2. Sélectionner un certificat signé (obligatoire).
   Ce certificat doit être préalablement ajouté dans le pool certificats et clés dans l'onglet "Certificats signés", voir chapitre **4.10 Gestion des certificats et des clés.**
3. Sélectionner un certificat CA (optionnelle).
   Ce certificat doit être préalablement ajouté dans le pool certificats et clés dans l'onglet "Certificats CA", voir chapitre **4.10 Gestion des certificats et des clés.**

- TTLS : authentification par encapsulation d'une session TLS en 2 phases : authentification du serveur auprès du de l'appareil (supplicant) par un certificat pour créer un tunnel sécurisé TLS pour l'échange de données entre les 2 parties durant la deuxième phase. Dans la deuxième phase, le client est authentifié auprès du serveur par l'utilisation d'un mécanisme d'authentification interne (PAP, MSCHAPv2,...) en passant par le tunnel sécurisé. Grâce à cela, l'identité du supplicant est protégée pendant la phase d'authentification.

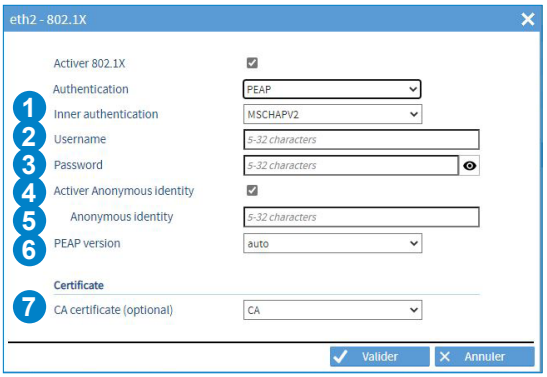


Note : 5

Si le caractère "@" est utilisé alors l'"Anonymous identity" doit être de la forme d'un nom de domaine contenant un point
(exemple : @exemple.com).

1. Choisir le mécanisme d'authentification interne.
Ce mécanisme permet d'authentifier Netsilon grâce à son mot de passe. Le mot de passe sera transmis selon la forme du mécanisme de chiffrement sélectionné (MD5, MSCHAP…).
2. Saisir l'username du supplicant (Netsilon).
3. Saisir le mot de passe.
Celui-ci sera vérifié par le serveur d'authentification.
4. Pour protéger l'username du supplicant (Netsilon) lors de de la première phase d'identification lorsque la connexion entre Netsilon et le switch (authenticator) n'est pas encore sécurisée par le tunnel TLS, un "Anonymous identity" est utilisable à la place.
Si le paramètre « Anonymous identity » n'est pas sélectionné, c'est l'username qui est utilisé lors de la première phase.
5. Saisir l'"Anonymous identity" (n'est pas relié à l'username et au mot de passe pour l'authentification).
6. Sélectionner un certificat CA (optionnelle).
Ce certificat doit être préalablement ajouté dans le pool certificats et clés dans l'onglet "Certificats CA",
voir chapitre **4.10 Gestion des certificats et des clés.**

- PEAP : fonctionnement en deux phases, proche du TTLS. Le serveur s'authentifie d'abord auprès de l'appareil (supplicant) avec un certificat afin de créer un tunnel sécurisé TLS entre les deux parties. Puis, le serveur authentifie l'appareil au sein du tunnel sécurisé avec une méthode d'authentification interne (MSCHAPv2, MD5,...).

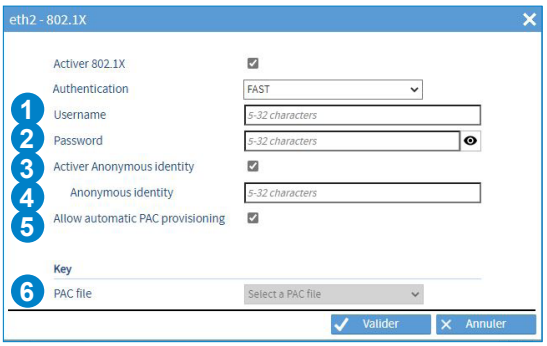


Note : 5

Si le caractère "@" est utilisé alors l'"Anonymous identity" doit être de la forme d'un nom de domaine contenant un point
(exemple : @exemple.com).

1. Choisir le mécanisme d'authentification interne.
Ce mécanisme permet d'authentifier Netsilon grâce à son mot de passe. Le mot de passe sera transmis selon la forme du mécanisme de chiffrement sélectionné (MSCHAPv2, MD5,...).
2. Saisir l'username du supplicant (Netsilon).
3. Saisir le mot de passe.
Celui-ci sera vérifié par le serveur d'authentification.
4. Pour protéger l'username du supplicant (Netsilon) lors de la première phase d'identification lorsque la connexion entre Netsilon et le switch (authenticator) n'est pas encore sécurisée par le tunnel TLS, un "Anonymous identity" est utilisable à la place.
Si le paramètre « Anonymous identity » n'est pas sélectionné, c'est l'username qui est utilisé lors de la première phase.
5. Saisir l'"Anonymous identity" (n'est pas relié à l'username et au mot de passe pour l'authentification).
6. Choisir la version de PEAP selon la compatibilité.
Possibilité de mettre le paramètre en automatique.
7. Sélectionner un certificat CA (optionnelle).
Ce certificat doit être préalablement ajouté dans le pool certificats et clés dans l'onglet "Certificats CA",
voir chapitre **4.10 Gestion des certificats et des clés.**

- FAST : authentification via un tunnel sécurisé TLS au moyen d'un PAC (Protected Access Credential) généré dynamiquement par le serveur d'authentification.



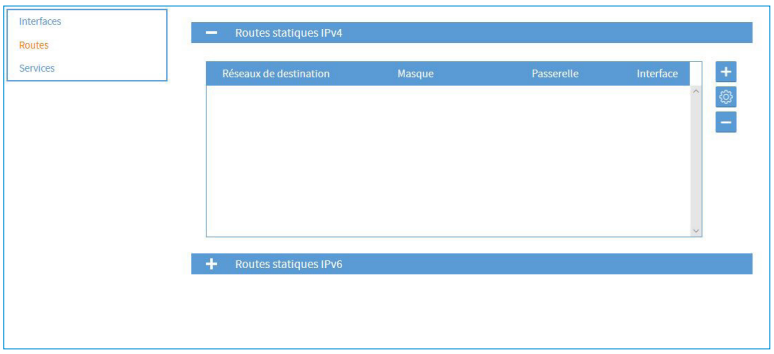
Note : 4

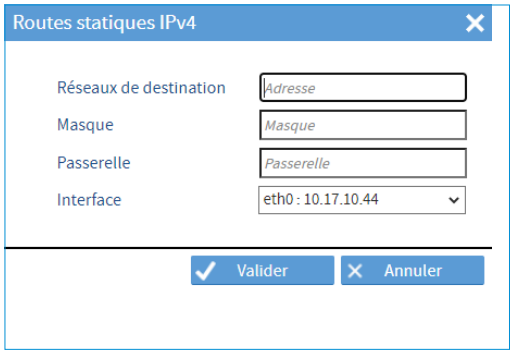
Si le caractère "@" est utilisé alors l'"Anonymous identity" doit être de la forme d'un nom de domaine contenant un point
(exemple : @exemple.com).

1. Saisir l'username du supplicant (Netsilon).
2. Saisir le mot de passe.
   Celui-ci sera vérifié par le serveur d'authentification.
3. Pour protéger l'username du supplicant (Netsilon) lors de la première phase d'identification lorsque la connexion entre Netsilon et le switch (authenticator) n'est pas encore sécurisée par le tunnel TLS, un "Anonymous identity" est utilisable à la place.
   Si le paramètre « Anonymous identity » n'est pas sélectionné, c'est l'username qui est utilisé lors de la première phase.
4. Saisir l'"Anonymous identity" (n'est pas relié à l'username et au mot de passe pour l'authentification).
5. Activer la récupération automatique du PAC (protected access credential) file lors des échanges.
   L'utilisateur n'a pas besoin d'en fournir un.
6. Sélectionner un PAC file si l'option "Allow automatic PAC provisionning" n'est pas activée.
   Ce PAC file doit être préalablement ajouté dans le pool certificats et clés dans l'onglet "clés publiques",
   voir chapitre **4.10 Gestion des certificats et des clés.**

4.4.2. *Configurer des routes statiques IPv4 / IPv6*

Il est possible de configurer des routes statiques :
1) MENU RESEAU > Routes





2) Cliquer sur + et une fenêtre s'ouvre, renseigner ensuite les différents paramètres demandés pour configurer le routage :
- Réseaux de destination,
- Masque (ou préfixe pour l'IPv6),
- Passerelle.

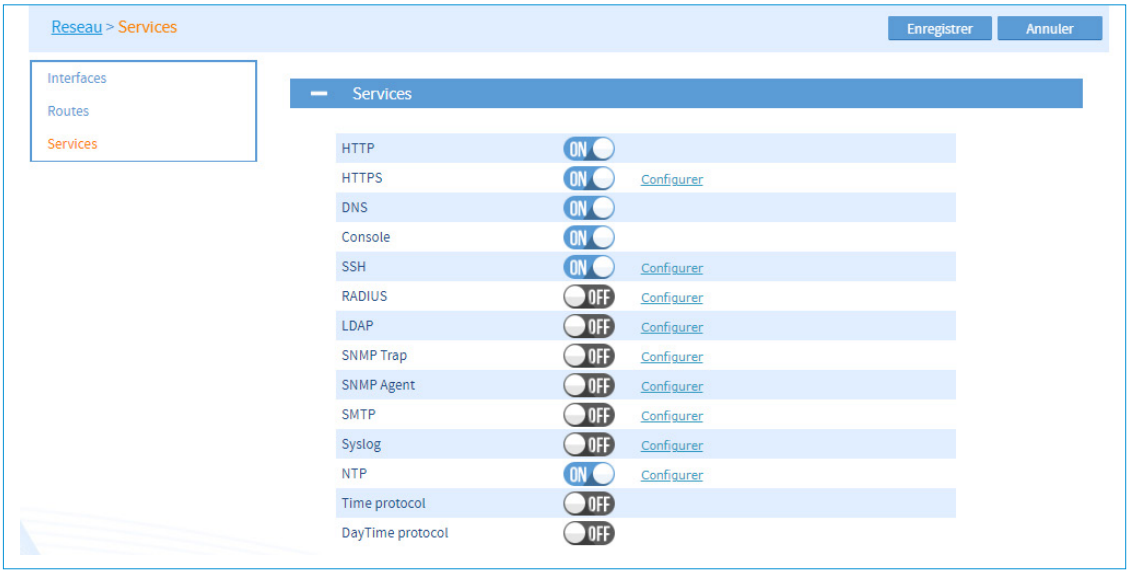
3) Choisissez l'interface Ethernet, le bond ou le VLAN.

Il est possible d'ajouter jusqu'à 50 routes en IPv4 et 50 routes en IPv6.
Les passerelles (routes par défaut) doivent être déclarées dans les interfaces.
Dans le cas de réseaux complètement isolés, il est nécessaire de déclarer une seule route par défaut dans une interface et de déclarer les autres réseaux distants en routes statiques.

4.4.3. *Gérer les services réseaux*

Pour gérer les services réseaux, suivre les étapes ci-dessous :

1) Menu RESEAU > Services



Il est possible d'activer ou désactiver les services réseaux individuellement.

Pour certains services, un paramétrage est nécessaire au préalable. Des hyperliens (Configurer) permettent d'accéder aux pages de configuration des services nécessitant un paramétrage.

Dans la suite de ce chapitre, les généralités des services réseaux sont présentées. Pour chaque service réseau, afin d'obtenir plus d'information sur la configuration, se reporter au chapitre détaillé.

› HTTP - HTTPS

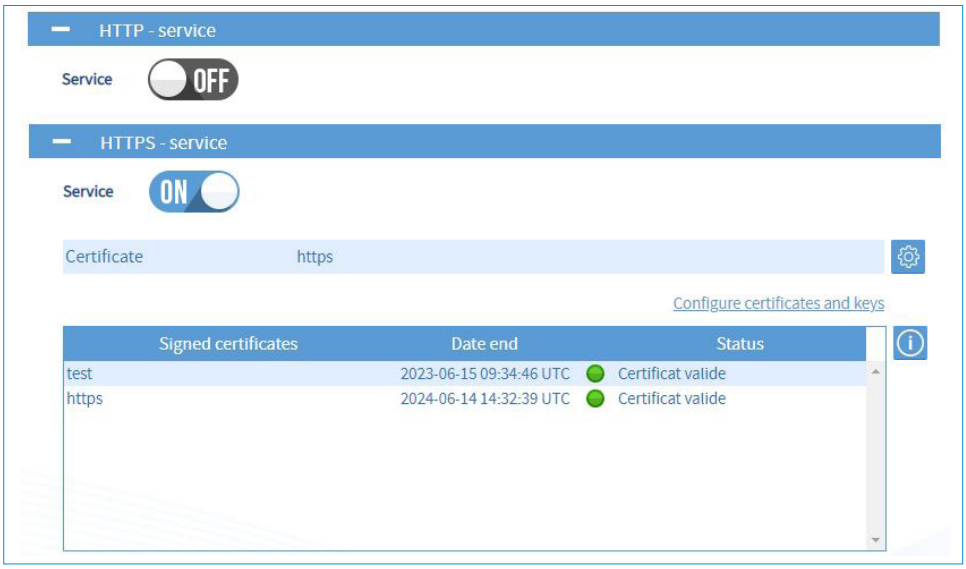
HTTPS (HyperText Transfer Protocol Secure) est un protocole de communication utilisé pour l'accès à un serveur Web sécurisé. Si l'on indique HTTPS dans l'URL au lieu de la mention HTTP normale, le message sera adressé vers un port d'entrée sécurisé du serveur.

Le protocole HTTPS permet une gestion sécurisée de l'accès au serveur web pour la configuration de Netsilon.

Le certificat SSL est requis pour que la connexion soit sécurisée avec Netsilon (HTTPS).

Il est possible de choisir entre un certificat signé par une Autorité de Certification (CA) externe et un certificat auto-signé.
Chaque Netsilon génère un certificat SSL auto-certifié. Le certificat est renouvelé automatiquement au bout de 10 ans. Le certificat renouvelé 4 jours avant son expiration.

Afin de configurer ce paramètre, cliquer sur Configurer :



Ce menu permet de choisir le certificat à utiliser (auto-signé ou signé d'une Autorité de Certification externe) et de consulter les informations des certificats externes.

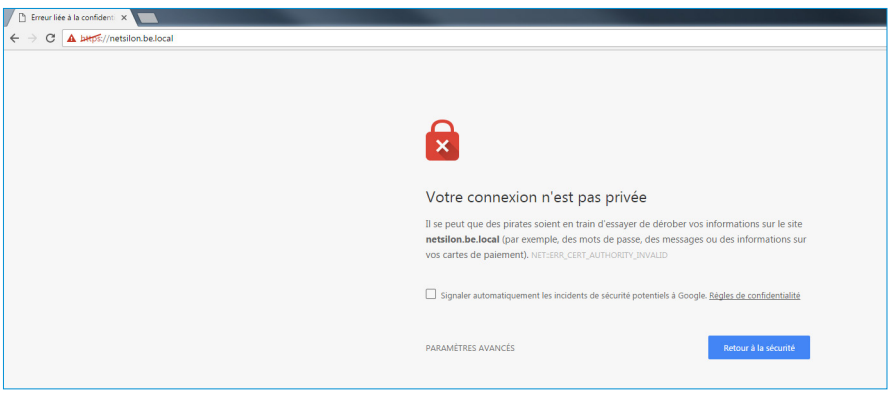
L'ajout des certificats s'effectue depuis le pool Certificats et clés.
Voir chapitre 4.10 Gestion des certificats et des clés.

Lors d'une modification d'un service (HTTP ou HTTPS) ou lors de la modification du certificat, le produit retourne sur la page d'accès au serveur web.

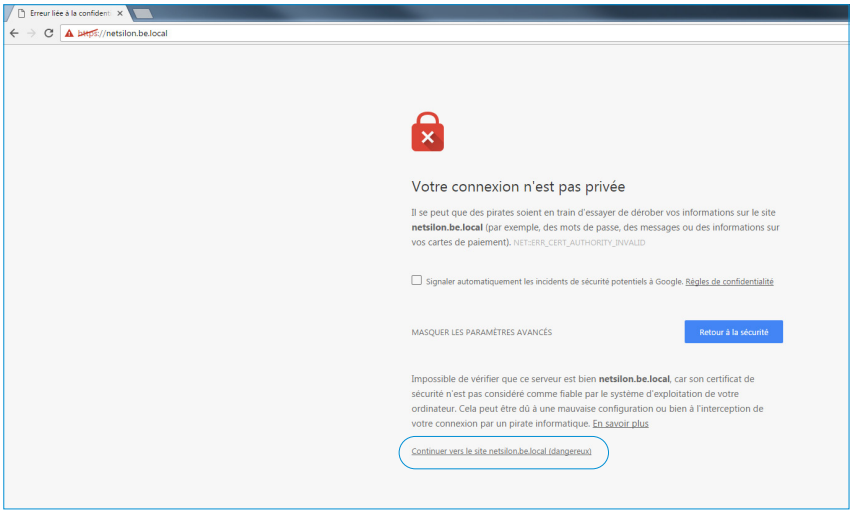
Pour utiliser la connexion sécurisée, une redirection HTTP vers HTTPS est réalisée automatiquement :

1) Saisir dans la barre d'adresse du navigateur : https://NomDuProduit.Domaine.

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



3) Déployer les paramètres avancés du navigateur puis cliquer sur «continuer vers le site netsilon.be.local» :



La connexion est sécurisée même si «https» est barré et en rouge. Cet avertissement indique uniquement que le certificat n'est pas validé par un organisme certifié.

Bodet recommande l'utilisation du mode «https» pour optimiser la sécurité lors de l'accès au serveur web de Netsilon.

› DNS

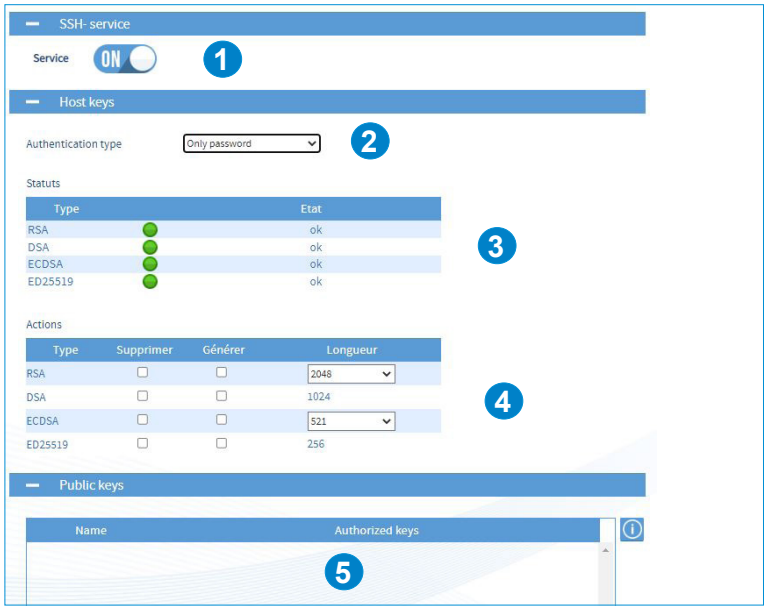
Le DNS (Domaine Name System) est un protocole permettant d'associer un nom de domaine, appelé Hostname, (ex : www.netsilon.com) à une adresse IP. Cependant, en cas d'interrogation par un hôte du serveur de destination, seule son adresse IP sera transmise afin de connaître avec exactitude l'identité du serveur de synchronisation.
Le Hostname est défini dans SYSTEME>Général>Paramètres.

› CONSOLE

Sur le port série, à l'aide de jeux de commandes, il est possible de modifier la configuration de Netsilon (paramètres basiques).
Pour la configuration du port série, **se reporter au chapitre 6. Configuration Console** - paramétrage basique.

› SSH

Sur le port ethernet, à l'aide de jeux de commandes, il est possible de modifier la configuration de Netsilon.
Afin de configurer ce paramètre, cliquer sur Configurer :



1 Activation du service SSH

2 Authentification par :
- Only password : authentification uniquement par mot de passe
- Only public key : authentification uniquement par clé publique.
- Public key or password : authentification par mot de passe ou clé publique.

3 Types de clés supportées :
- RSA : 1024/2048/4096 bits
- DSA : 1024 bits (fixe)
- ECDSA : 256/384/521 bits
- ED25519 : 256 bits (fixe)

4 Permet de générer ou supprimer les certificats de chaque type de clé. Pour générer un nouveau certificat il est nécessaire de supprimer le précédent. **Si l'utilisateur supprime les certificats RSA et DSA, sans en générer de nouveaux, alors la fonction SSH ne fonctionnera plus.**

5 Visualiser une clé public. Pour ajouter une clé, vous devez enregistrer dans un fichier la clé publique générée par l'utilitaire (ex.: PuTTY key Generator) puis l'importer dans Netsilon. Se reporter au chapitre **5.2 Authentification par clé publique**

› RADIUS

Le protocole RADIUS (Remote Authentification Dial-In User Service) est un protocole d'authentification standard reposant sur un système client / serveur définissant les accès pour les utilisateurs distants à un réseau.

Cliquer sur Configurer puis se reporter au chapitre **4.2.2.1 Service RADIUS**

› LDAP

Le protocole LDAP (Lightweight Directory Access Protocol) est utilisé pour accéder à des informations sur les utilisateurs d'un réseau par le biais de l'interrogation des services d'annuaire.

Cliquer sur Configurer puis se reporter au chapitre **4.2.2.2 Service LDAP**

› SNMP

SNMP (Simple Network Management Protocol) est un protocole de supervision d'équipements réseaux. Il y a deux entités : un superviseur (SNMP Manager) et des agents (Ex.: Netsilon).

Traps

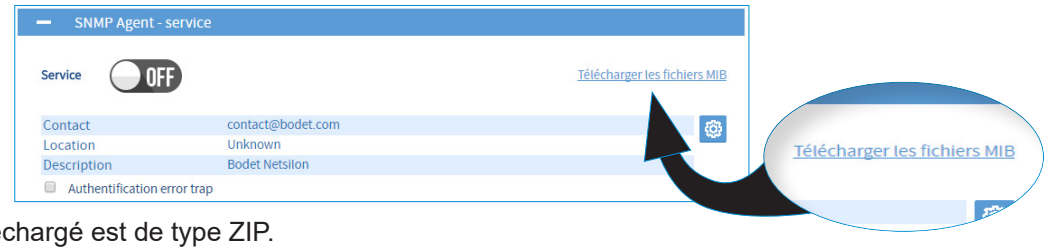
Les traps SNMP sont des informations envoyées en utilisant le protocole SNMP depuis un équipement supervisé vers un serveur de supervision.

Afin de pouvoir interpréter l'évènement reçu, le serveur de supervision doit posséder dans sa configuration le nécessaire pour traduire l'évènement. Pour cela, il doit disposer d'une base de données contenant les fichiers MIB.

Cliquer sur Configurer puis se reporter au chapitre **4.9.2 Configuration SNMP trap.**

Téléchargement du fichier MIB

Le fichier MIB est à récupérer dans SECURITE > Agent SNMP > SNMP Agent-service :



Le fichier téléchargé est de type ZIP.

Agents

Les agents sont chargés de transmettre les informations liées à la gestion de l'équipement au format SNMP.
Cliquer sur Configurer puis se reporter au chapitre **4.11 Supervision du système.**

› SMTP

SMTP (Simple Message Transfert Protocole) est utilisé pour transférer les messages électroniques (alarmes) sur un réseau informatique.
Un serveur SMTP est un service qui écoute sur le port 25. Son principal objectif est de router les mails vers un destinataire.
Cliquer sur Configurer puis se reporter au chapitre **4.9.1 Configuration SMTP.**

› SYSLOG

Syslog est un protocole standard permettant d'envoyer des évènements du journal système des équipements présents sur un réseau vers un serveur dédié qui va centraliser ces informations en vue de leur analyse.
Il est également possible d'utiliser ce service pour un archivage des évènements en local.

Cliquer sur Configurer puis se reporter au chapitre **4.9.4 Configuration Syslog**

› NTP

Network Time Protocol (NTP) est un protocole client/serveur pour la synchronisation du temps sur les réseaux IP.
Il est possible d'activer ou désactiver le service NTP. Lorsque NTP est désactivé, aucune information NTP ne sera envoyée au réseau. Lorsqu'il est activé le service NTP fonctionne en mode Unicast par défaut.
L'intégralité des paramètres peuvent être modifiés afin de configurer les applications NTP spécifiques : NTP client, NTP servers, NTP peers, NTP Key et NTP autokey.

Cliquer sur Configurer puis se reporter au chapitre **4.6 Synchronisation NTP.**

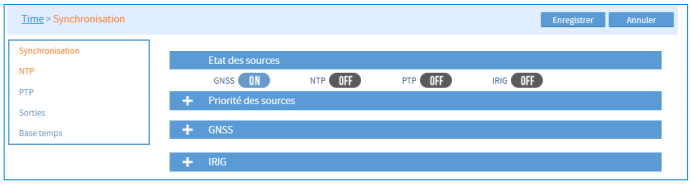
› TIME PROTOCOLE et DAYTIME PROTOCOLE

L'activation de ces paramètres permet à Netsilon d'envoyer l'heure et la date UTC (non paramétrable) sur plusieurs équipements du réseau informatique.

4.5 Choix des sources de synchronisation

Pour choisir la ou les source(s) de synchronisation, suivre les étapes ci-dessous :

1) Menu TIME > Synchronisation



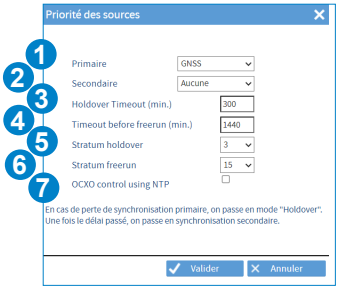
4.5.1. Etat des sources

Il s'agit d'une visualisation. Cet espace indique si les sources de synchronisation disponibles sont activées.

4.5.2. Priorité des sources

La priorité des sources de synchronisation permet de définir les priorités entre chaque source disponible afin de permettre à Netsilon de délivrer un signal horaire précis en continu.

Afin d'établir une priorité dans les sources de synchronisation et effectuer des paramétrages : cliquer sur  , la fenêtre suivante apparaît :



1 5 choix possibles : AUTO - GNSS - NTP - PTP- IRIG (PTP et IRIG : seulement si la carte correspondante est installée).
En mode auto, Netsilon choisit automatiquement la source la plus fiable (de meilleure qualité) et réalise un basculement automatiquement entre les sources (en cas de perte d'une source).
En mode Primaire / Secondaire, il y a tentative de synchronisation sur la source primaire. S'il n'y a pas de synchronisation après plusieurs minutes (timeout en fonction de la source - GNSS : 5 minutes, PTP : 10 minutes, NTP : 15 minutes, IRIG : 10 minutes), il y a basculement sur la source secondaire. En cas de retour de la synchronisation primaire, il y a basculement automatique vers la source primaire. S'il y a perte de synchronisation sur la source primaire, après le « Holdover time-out », il y a basculement vers la source secondaire.

2 5 choix possibles : Aucune - GNSS - NTP - PTP- IRIG.

3 Le holdover est un état dans lequel le serveur de temps continue de délivrer un signal horaire sans présence de source de synchronisation. Par défaut, la valeur du holdover est fixée à 300 minutes (5 heures). Celle-ci dépend de l'environnement d'utilisation de Netsilon et des attentes de l'utilisateur sur la précision du signal horaire. Cette valeur est suffisamment grande pour masquer les éventuelles micro-coupures de source synchronisation, mais suffisamment faible pour garantir un signal horaire de qualité. La valeur du «Holdover time-out» est paramétrable de 1 à 14400 minutes, soit 10 jours.

4 Après passage en Holdover time-out et une fois ce délai écoulé, en l'absence d'un retour de la synchronisation primaire et d'une source secondaire pour prendre le relai, un nouveau délai s'active avant passage à l'état «freerun» où la précison de la base de temps n'est alors plus garantie : c'est le «Time-out before freerun». La valeur est paramétrable jusqu'à 43200 minutes, soit 30 jours.

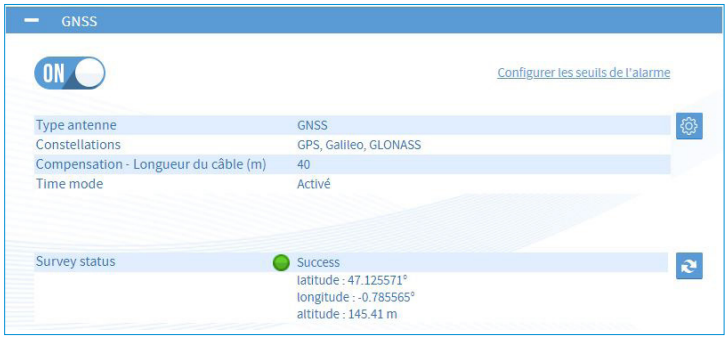
5 **6** Les options « Stratum holdover» et «Stratum freerun» paramètrent le stratum du serveur NTP du Netsilon (et non de la source locale). La strate du serveur si non synchronisé (suivant l'état «holdover» ou «freerun») peut être programmée de 1 à 15. Par défaut : Stratum holdover = 3 / Stratum freerun = 15.
Le stratum de la source locale est donc d'un rang inférieur.
Exemple :
Stratum holdover = 3
Source Locale = 2
Serveur NTP Netsilon (pour la synchronisation de client) = 3

7 Asservissement de l'oscillateur OCXO depuis une source NTP. Si la synchronisation primaire est GNSS et la source secondaire NTP, l'oscillateur est asservi par la source GNSS en priorité (meilleure précision).

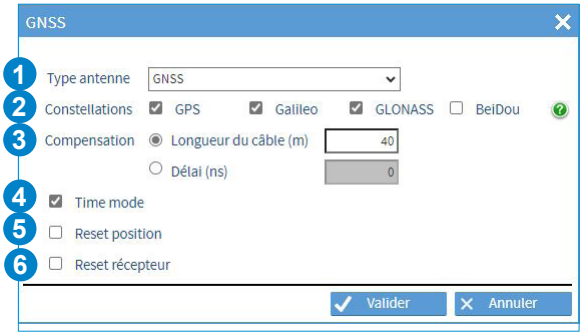
Se reporter au chapitre **9 Annexe 1 : synchronisation** pour visualiser les différents scénarios de synchronisation

4.5.3. *Récepteurs satellites*

Activer la synchronisation GNSS à l'aide du bouton ON.

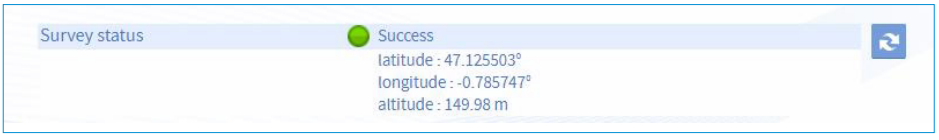


1) Cliquer sur pour sélectionner le type d'antenne puis la ou les constellations (le bouton liste les combinaisons GNSS autorisées).



1. Choix du type d'antenne : GNSS ou Secure GNSS (résistant aux tentatives de brouillage et de leurrage).
   Si l'antenne Secure GNSS est choisie, une option permettant d'exclure la synchronisation GNSS en cas de détection de leurrage est proposée. Dans ce cas, le serveur utilisera automatiquement une autre source de synchronisation.
   Tout changement d'antenne (exemple : remplacement d'une antenne GNSS par une Secure GNSS) doit s'effectuer à froid et demande un redémarrage de l'appareil.
2. Choix des constellations suivant les combinaisons possibles.
   Pour l'antenne Secure GNSS, il est possible de sélectionner l'ensemble des constellations en simultané.
   La détection d'une attaque de leurrage demande un minimum de 2 constellations sélectionnées.
3. Pour effectuer la compensation, il y a 2 possibilités :
   - › Sélectionner la longueur de câble de l'antenne GNSS,
   - › Indiquer directement la valeur à compenser (utile dans le cas d'utilisation de l'interface antenne GNSS RF standard).

   Dans le cas de l'interface GNSS RF standard, on peut calculer le délai suivant cette méthode :
   D : délai total en ns
   L1 : longueur câble ethernet (serveur temps / boitier interface antenne)
   L2 : longueur du câble coaxial (boitier interface antenne / antenne RF)
   D = L1 . C1 + L2 . C2
   C1 = 5.8 ns/m
   C2 dépend du câble coaxial. Pour un câble de type LMR-400, C2 = 4 ns/m
   C2 peut également être calculé à partir des données constructeur du câble avec cette formule :
   C2 = 1/ (0.3 . v) avec v la vélocité du câble (exemple 0.66 pour 66%)
4. « Time mode » est sélectionnée par défaut. Cela permet d'améliorer la précision du PPS en travaillant à position fixe. Ce mode n'est utile que dans le cas d'une utilisation du PPS généré par le serveur temps.
   La position de l'antenne est déterminée automatiquement par l'antenne avec la procédure « survey ».
   L'état « survey » peut prendre les valeurs suivantes :
   - Unknown / In progress (avec le temps écoulé depuis le lancement) / Success / Aborted
   Si l'état « success » est présent, la position de l'antenne est indiquée. (altitude MSL = Mean Sea Level)

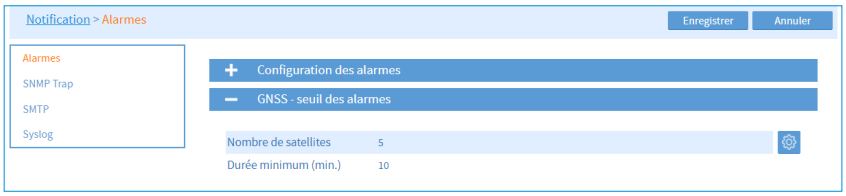


   Si « time mode » est décoché : time et position.

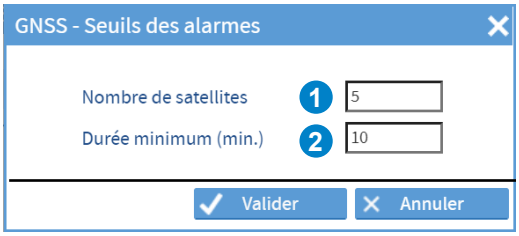
5 « Reset position » n'est accessible qu'en « Time mode » et permet de relancer la procédure « survey » permettant de déterminer automatiquement la position de l'antenne (par exemple, suite à un changement de position de cette dernière).

6 « Reset récepteur » permet de redémarrer le récepteur GNSS en cas de besoin.

1) Pour configurer le seuil des alarmes, cliquer sur le lien Configurer les seuils de l'alarme, la fenêtre suivante apparaît :



2) Cliquer sur ⚙, la fenêtre suivante apparaît :



1 Configurer le nombre de satellites pour définir le seuil d'alarme (entre 3 et 8).

2 Definir la durée à partir de laquelle l'alarme est remontée.

Exemple :
- Constellation GPS
- Durée fixée à 10 minutes

Si moins de 5 satellites sont recensés pendant 10 minutes, alors une alarme sera remontée.

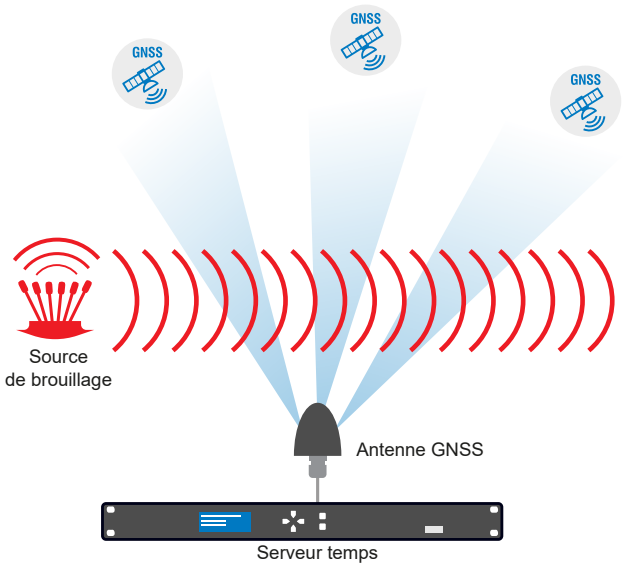
Par défaut, le seuil d'alarme est activé pour 5 satellites et une durée de 10 minutes.

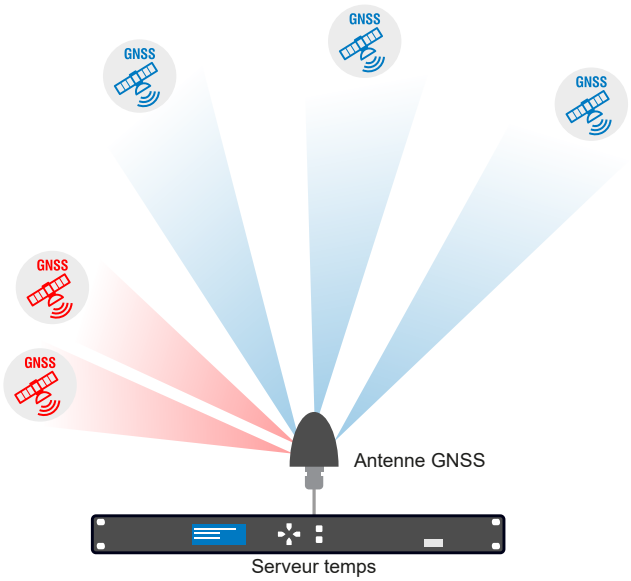
4.5.4. *Leurrage et brouillage des signaux GNSS*

Les satellites GNSS fonctionnent à partir de l'orbite terrestre. Le signal transmis est extrêmement faible à l'arrivée à la surface de la terre. Cette faible puissance du signal au niveau des récepteurs rend l'utilisation des signaux GNSS sensibles aux interférences intentionnelles (malveillant) ou non intentionnelles.
On distingue majoritairement 2 types d'interférences, le leurrage (spoofing) et le brouillage (jamming).

Le brouillage est la présence d'un signal parasite qui empêche le récepteur GNSS de décoder le vrai signal satellite.

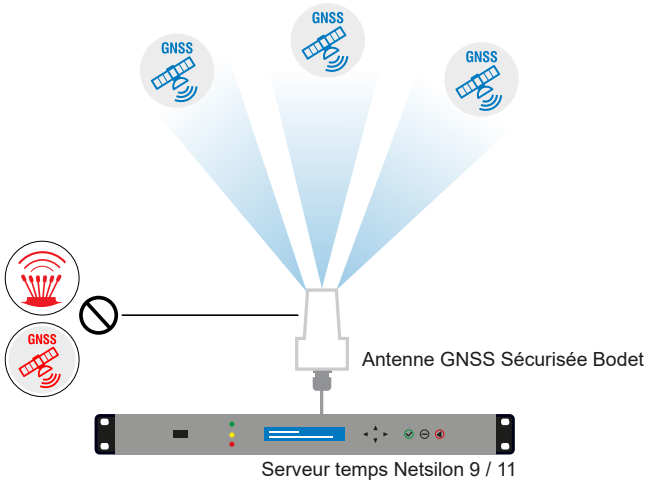
Le leurrage est la transmission intentionnelle de faux signaux GNSS pour détourner les utilisateurs de la véritable source. Il nécessite un équipement sophistiqué pour recréer les signaux satellites.
Le leurrage est plus difficile à détecter qu'un brouillage.



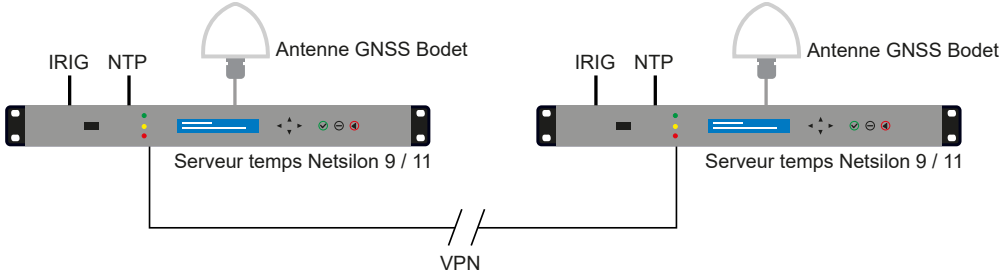


Afin de se prémunir de ces risques, plusieurs options existent :

Option 1 : l'antenne GNSS sécurisée (Secure GNSS).
Cette antenne BODET offre une couche de sécurité supplémentaire contre les tentatives de brouillage et de leurrage par sa conception et l'utilisation d'algorithmes avancés de détection.

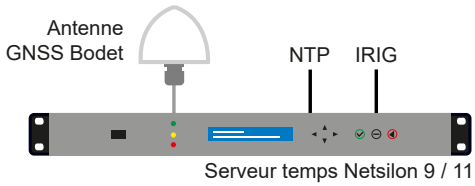


Option 2 : l'installation distante
Les tentatives de brouillage et de leurrage sont rendues complexes avec 2 sites géographiquement distants à attaquer.



2 serveurs de temps sur 2 sites différents se synchronisent ensemble (via NTP, PTP ou IRIG) en passant par un réseau privé (VPN). Cette option suppose que les 2 serveurs de temps Bodet soient en mode automatique (choix de la source) et disposent chacun de 3 sources de synchronisation indépendantes.

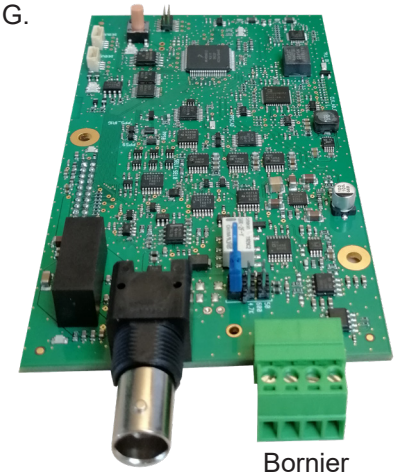
Option 3 : une installation multisources
Le serveur de temps utilise plusieurs sources de synchronisation et effectue des comparaisons pour choisir la plus fiable. En cas de brouillage et de perte des signaux GNSS, le serveur de temps peut basculer automatiquement sur une autre source.



Cette option suppose que le serveur de temps Bodet soit en mode automatique (choix de la source) et dispose de 3 sources de synchronisation indépendantes.

4.5.5. Carte option IRIG INPUT (réf.: 907 947)

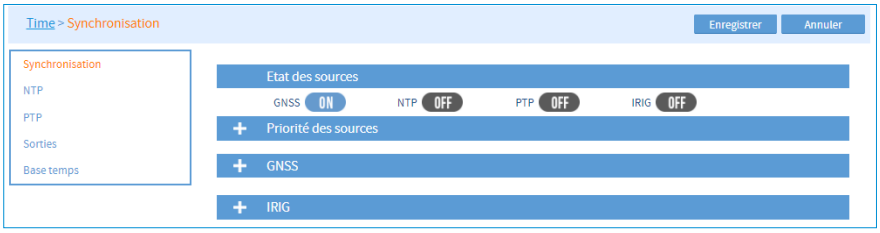
La carte option IRIG INPUT permet de synchroniser Netsilon depuis un signal IRIG.



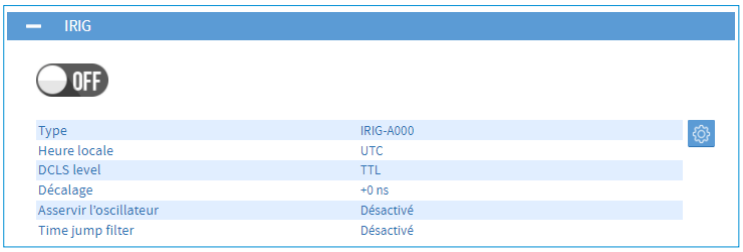
Connecteur BNC — Bornier débrochable

Pour paramétrer l'entrée IRIG, suivre les étapes ci-dessous :

1) Menu TIME > Synchronisation > IRIG



2) Activer la synchronisation à l'aide du bouton ON.



3) Effectuer la configuration, cliquer sur bouton , la fenêtre suivante apparaît :

1 Choix du format d'entrée suivant la source du signal : IRIG A/B/E/G, AFNOR 87500.
Les formats IRIG se caractérisent par des fréquences d'impulsion différentes.

Format	Fréquence d'impulsion	Intervalle
IRIG A	1000 PPS	1 ms
IRIG B	100 PPS	10 ms
IRIG E	10 PPS	100 ms
IRIG G	10000 PPS	0.1 ms

2 Choix du type de modulation du signal d'entrée :
- (0) DCLS (DC Level Shift) : codage en largeur d'impulsion,
- (1) AM (Amplitude Modulated) : onde sinusoïdale porteuse modulée en amplitude.

3 Choix de la fréquence de modulation.
Elle dépend directement du format et du type de modulation préalablement choisi.

Fréquence de modulation
(0) Pas de porteuse (DCLS)

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

4 Choix de l'expression codée. Elle dépend directement du format et du type de modulation préalablement choisi. Cela définit la nature des données incluses dans le signal IRIG.

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

5 Choix du mode de transmission (TTL ou RS422) en fonction de l'interface avec la source IRIG et du type de câble utilisé dans la connexion avec Netsilon (formats DCLS).

6 Fuseau horaire utilisé par la source IRIG. Déclarer préalablement la zone horaire correspondante dans Netsilon si besoin : Menu TIME > Base de temps > Zones horaires.

7 Offset servant à compenser le délai de transmission du signal IRIG entre la source et Netsilon (longueur du câble). Suivant la qualité du signal, un décalage peut aussi être constaté entre le top générateur du signal et la synchronisation.
La gestion de la compensation n'est pas disponible avec l'IRIG E.

8 Option permettant l'asservissement de l'oscillateur OCXO du Netsilon sur le signal IRIG.
L'asservissement demande une qualité de signal supérieure. En cas de baisse de la qualité du signal, l'oscillateur peut passer à l'état «Tracking» ou «Holdover». En cas d'asservissement de l'oscillateur, le temps de synchronisation peut être plus important.
Le format IRIG E ne permet pas l'asservissement de l'oscillateur.

9 Le «Time jump filter» est un filtrage permettant de pallier à un décalage horaire momentané du générateur de signal IRIG avec la base de temps, en effectuant un basculement vers une autre source de synchronisation au-delà d'un certain seuil paramétré par l'utilisateur (valeur programmable de 0.7 à 900 s).
Exemple : un générateur de signal IRIG diffuse momentanément un signal horaire décalé de 10 secondes par rapport à la base de temps. Si le seuil autorisé par l'utilisateur est de 8 secondes, Netsilon détecte l'anomalie et rejette cette source. Suivant le paramétrage, il y aura ensuite basculement vers une autre source de synchronisation disponible ou passage à l'état "holdover", puis "freerun".
En cas de seuil de faible valeur, la synchronisation initiale peut être rendue difficile. Dans ce cas, activez l'option « Accepter la première synchronisation». Cela désactive le filtrage uniquement pour la première synchronisation. Par défaut, si le filtrage est désactivé, le décalage maximum autorisé est de 15 minutes.

› **Cas particulier d'une synchronisation IRIG si Netsilon est Master PTP :**

Si Netsilon est master PTP, la synchronisation IRIG doit obligatoirement asservir l'oscillateur OCXO. Cela nécessite un signal de qualité. Voir le 8 pour activer l'option d'asservissement.

Le signal IRIG délivre un signal horaire UTC sans indication du nombre de Leap Second tandis que le protocole PTP diffuse le temps TAI (Temps Atomique International). Il est donc nécessaire de connaître l'offset TAI/UTC.

En conséquence, il est obligatoire de renseigner manuellement dans Netsilon :
- le décalage actuel entre TAI et UTC (TAI to UTC offset),
- l'information du prochain Leapsecond afin qu'il soit automatiquement pris en compte.

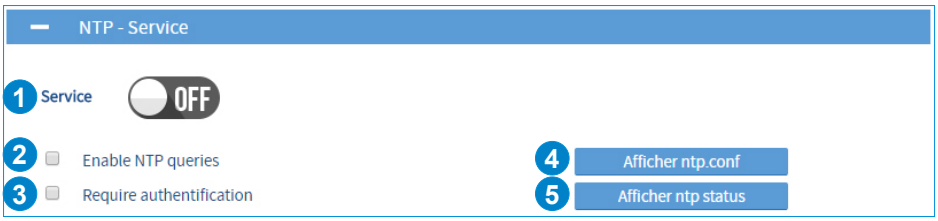
Reportez-vous aux chapitres **4.3.5 Définir l'offset TAI/UTC** et **4.3.4 Programmer un Leap Second manuel** pour effectuer ces saisies.

4.6 NTP

4.6.1. NTP-Service

Pour activer le service NTP, suivre l'étape ci-dessous :

1) Menu TIME > NTP > NTP-Service

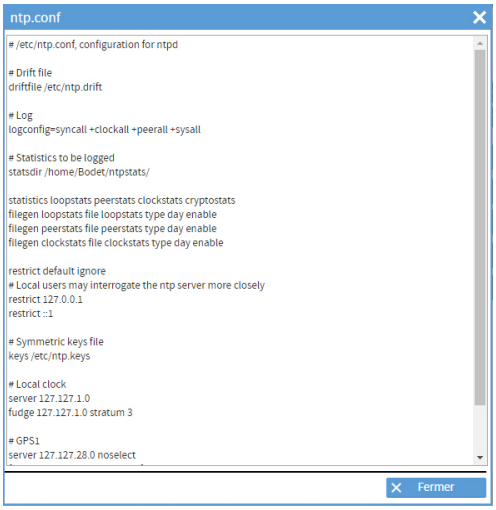


1 Bouton d'activation du service.

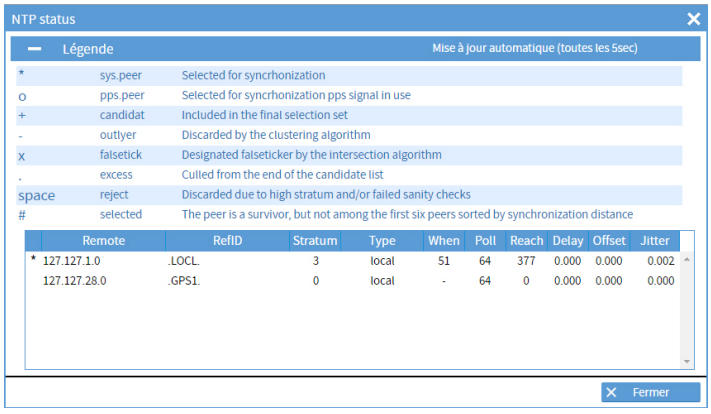
2 Cocher cette case pour interroger le serveur NTP à distance. Autorisation des paquets NTP mode 6 et 7 (information queries à distance).

3 Cocher cette case pour forcer l'authentification avec une clé symétrique ou autokey. Sans cette authentification, la synchronisation est impossible.

4 ntp.conf permet d'afficher le fichier de configuration (à titre d'information en lecture) :



5 Permet d'afficher le statut NTP, exemple :



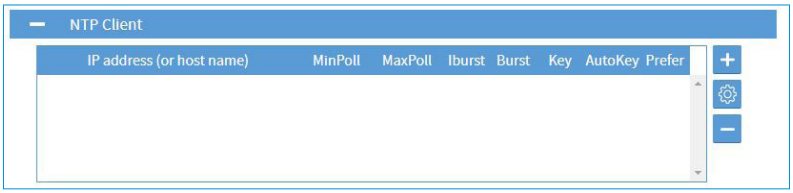
Pour obtenir la signification d'un paramètre, survoler le texte à l'aide de la souris du PC.

4.6.2. NTP client

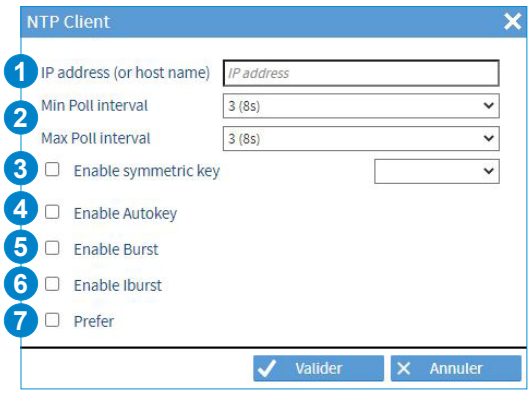
En mode client : le Netsilon se synchronise sur un serveur NTP en unicast.

Pour ajouter une source de synchronisation NTP, suivre les étapes ci-dessous :

1) Menu TIME > NTP > NTP Client :



2) Ajouter un serveur NTP en cliquant sur +, la fenêtre suivante apparaît :
(possibilité d'ajouter jusqu'à 10 serveurs maximum.)



1 Renseigner l'adresse IP (ou le host name) du serveur NTP.

2 Poll interval : il s'agit de l'intervalle, en secondes, entre deux interrogations. La valeur relevée dans le tableau du statut de la configuration NTP (se reporter page précédente) sera inférieure à la valeur minimum pour permettre une synchronisation rapide.

Une fois la synchronisation effectuée, cette valeur va augmenter afin de réduire le trafic réseau et la charge sur les serveurs de temps.

- Plage de choix :
  - Automatique.
  - de 3 (8 secondes) à 17 (36 heures 24 minutes et 32 secondes).

3 Activer et sélectionner une clé symétrique préalablement définie.

4 Avant d'activer ce paramètre, renseigner l'autokey.

5 L'option Burst est à activer lorsque le serveur est joignable. Elle active l'envoi de 8 paquets espacés de 16 secondes entre le premier et le second, puis deux secondes pour le reste. Cette option améliore la stabilité des échanges.

6 L'option iBurst permet de synchroniser plus rapidement le serveur dès son lancement.

⚠ **La société Bodet recommande l'utilisation de iBurst permettant de donner un service NTP actif rapidement.**

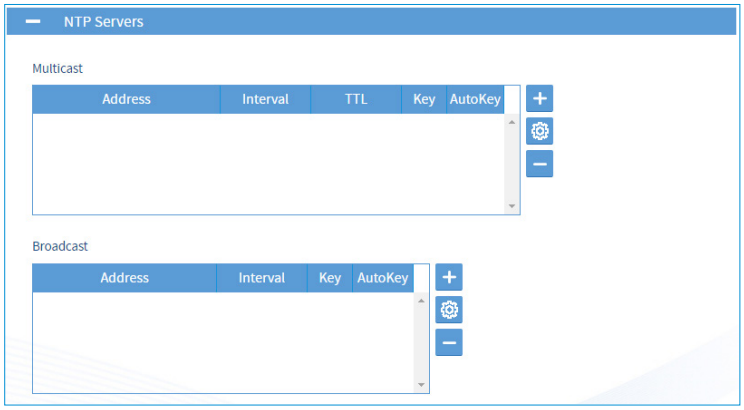
7 Ce paramètre prend comme base de référence des serveurs de strate N-1. Cette valeur peut s'appliquer à une source de référence telle que le GPS. Si cette option est cochée pour Netsilon, l'utilisateur estime que ce serveur est stable et proche et qu'il sert de référence en priorité.

4.6.3. NTP servers

En mode serveur : Netsilon diffuse l'heure en multicast ou broadcast ou unicast.

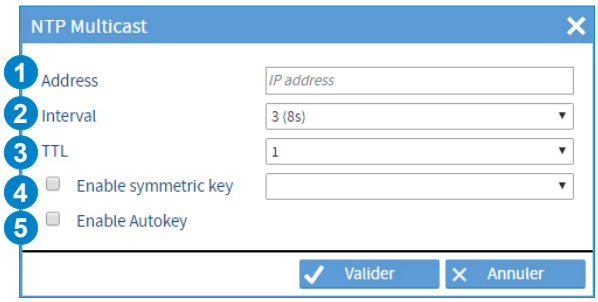
Pour activer le mode NTP Servers, suivre les étapes ci-dessous :

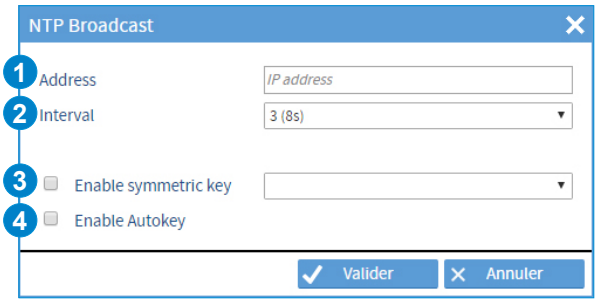
1) Menu TIME > NTP > NTP Servers :



2) Choisir le mode de communication : multicast ou broadcast.

3) Ajouter un serveur NTP en cliquant sur +, la fenêtre suivante apparaît :
(possibilité d'ajouter jusqu'à 5 serveurs en multicast et en broadcast)





1 Renseigner l'adresse IP du client NTP.

2 Poll interval : il s'agit de l'intervalle, en secondes, entre deux interrogations. La valeur relevée dans le tableau du statut de la configuration NTP (se reporter page précédente) sera inférieure à la valeur minimum pour permettre une synchronisation rapide.

Une fois la synchronisation effectuée, cette valeur va augmenter afin de réduire le trafic réseau et la charge sur les serveurs de temps.

› Plage de choix :

› Automatique.

› de 3 (8 secondes) à 17 (36 heures 24 minutes et 32 secondes).

3 Valeurs : 1, 32, 64, 96, 128, 160,192 et 224. TTL indique le temps pendant lequel une information doit être conservée, ou le temps pendant lequel une information doit être gardée en cache.
La valeur initiale de 1 est utilisée par certains protocoles pour s'assurer que les paquets ne sont pas routés au-delà d'un segment.

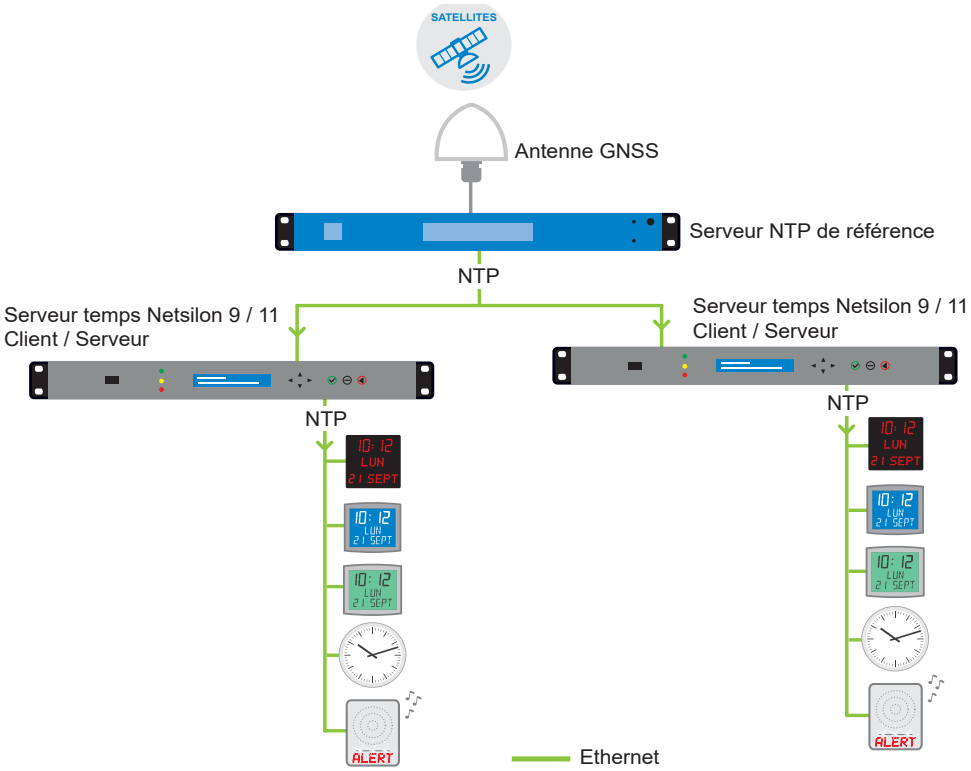
4 Avant d'activer ce paramètre, renseigner l'autokey.

5 L'option Burst est à activer lorsque le serveur est joignable. Elle active l'envoi de 8 paquets espacés de 16 secondes entre le premier et le second, puis deux secondes pour le reste. Cette option améliore la stabilité des échanges.

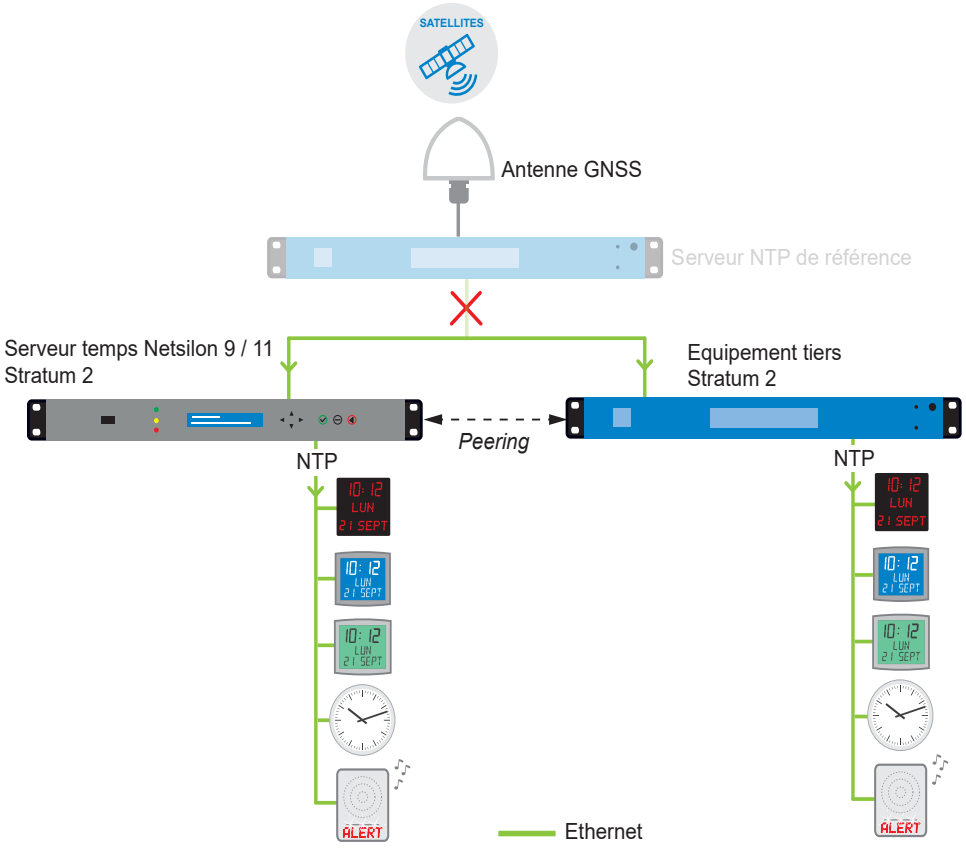
4.6.4. NTP-Peers

NTP peer est défini entre deux serveurs de temps ou plus. Si ni l'un ni l'autre n'a d'autorité (au même niveau hiérarchique) pour connaître l'heure, les deux travailleront à obtenir une synchronisation identique.

Scénario 1 : le serveur de référence délivre le signal horaire

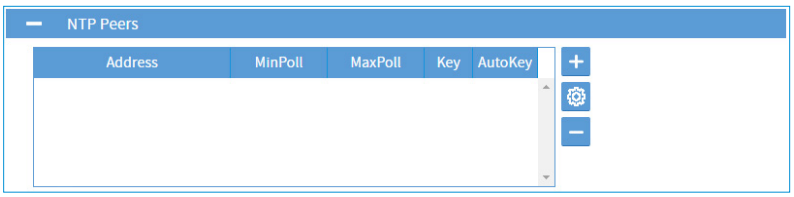


Scénario 2 : le serveur de référence ne délivre plus le signal horaire, l'équipement tiers se synchronise sur Netsilon ou vice-versa :

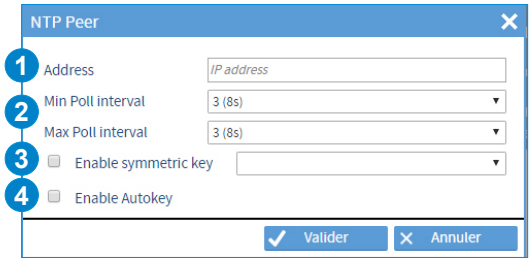


Pour activer le mode NTP Peers, suivre les étapes ci-dessous :

1) Menu TIME > NTP > NTP-Peers :



2) Ajouter un serveur NTP en cliquant sur +, la fenêtre suivante apparaît :
(possibilité d'ajouter jusqu'à 5 serveurs maximum)



1 Renseigner l'adresse IP du client NTP.

2 Poll interval : il s'agit de l'intervalle, en secondes, entre deux interrogations. La valeur relevée dans le tableau du statut de la configuration NTP (se reporter page précédente) sera inférieure à la valeur minimum pour permettre une synchronisation rapide.

Une fois la synchronisation effectuée, cette valeur va augmenter afin de réduire le trafic réseau et la charge sur les serveurs de temps.

› Plage de choix :

› Automatique.

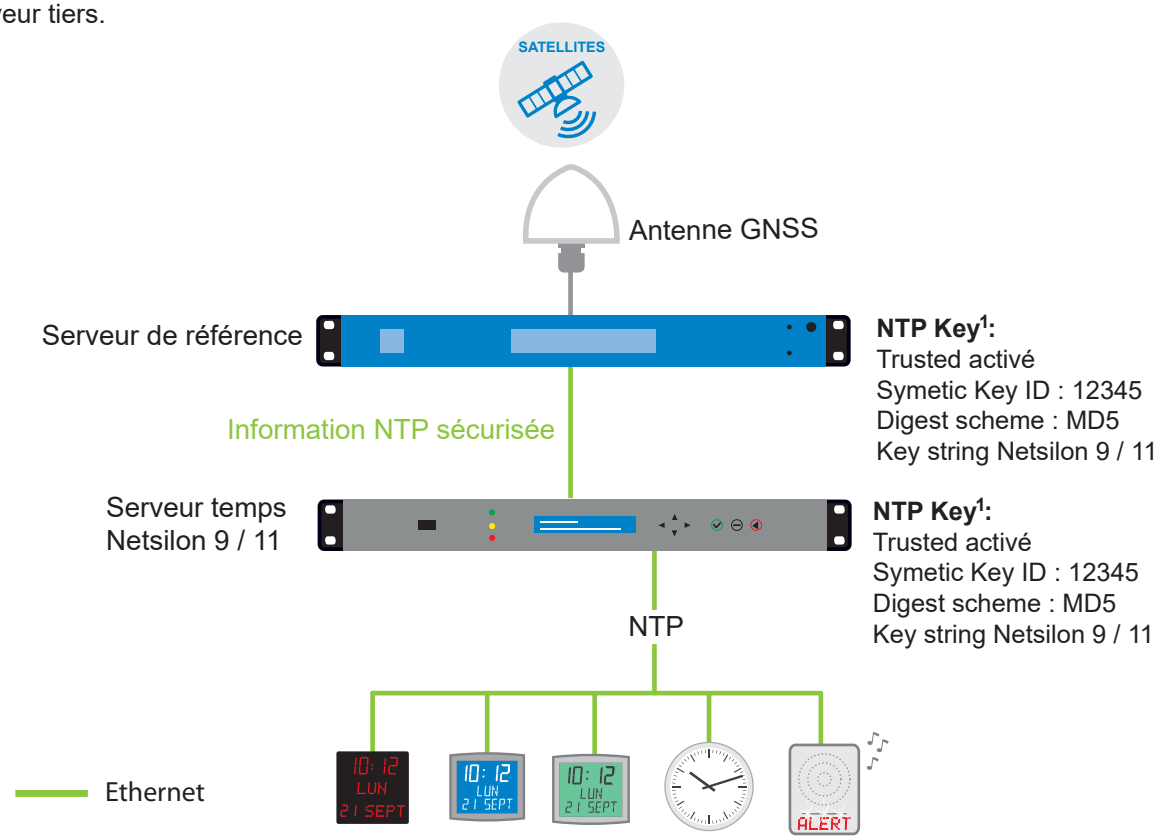
› de 3 (8 secondes) à 17 (36 heures 24 minutes et 32 secondes).

3 Valeurs : 1, 32, 64, 96, 128, 160,192 et 224. TTL indique le temps pendant lequel une information doit être conservée, ou le temps pendant lequel une information doit être gardée en cache.
La valeur initiale de 1 est utilisée par certains protocoles pour s'assurer que les paquets ne sont pas routés au-delà d'un segment.

4 Avant d'activer ce paramètre, renseigner l'autokey.

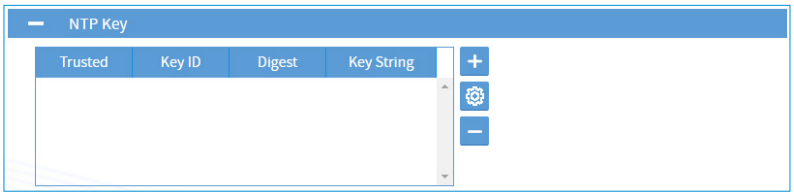
4.6.5. NTP-Key

La clé NTP permet de sécuriser la communication entre un serveur et un client NTP afin d'éviter l'intrusion d'un serveur tiers.

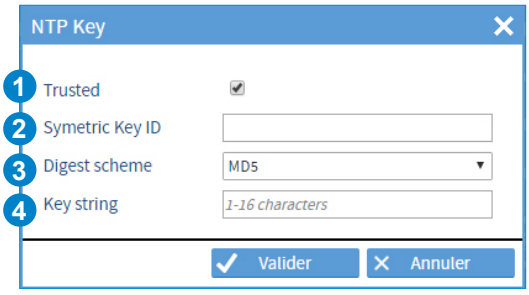


Pour activer le mode NTP key, suivre les étapes ci-dessous :

1) Menu TIME > NTP > NTP-Key :



2) Ajouter une clé NTP en cliquant sur +, la fenêtre suivante apparaît :
(possibilité d'ajouter jusqu'à 15 clés NTP maximum)



1 Cochez cette case pour utiliser l'authentification avec une clé de confiance (par défaut, le service NTP prend en compte uniquement des clés Trusted). Le principe consiste à assigner et vérifier si la clé de chaque équipement du réseau destiné à communiquer avec Netsilon, est correcte.

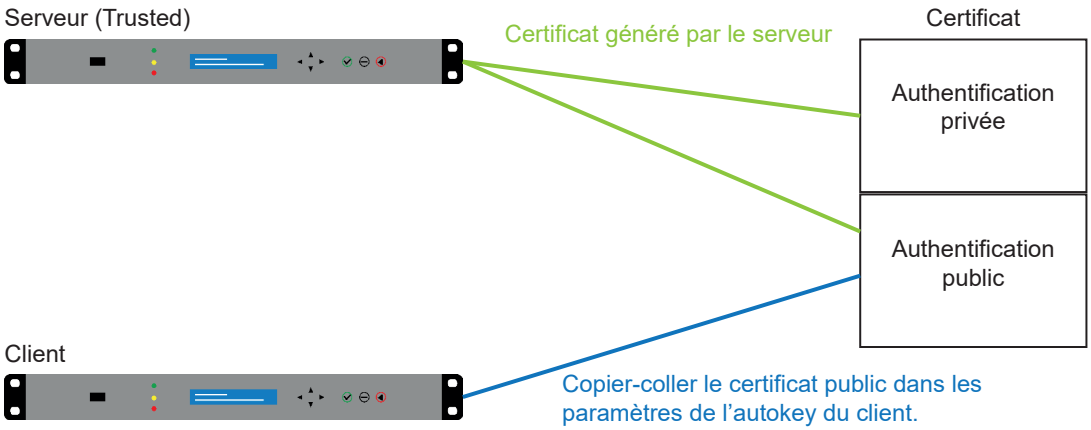
2 Définir un nombre compris entre 1 et 65534. Netsilon supporte l'authentification MD5 par défaut. Cette fonction assigne un authentificateur, qui se compose d'une clé et d'un message MD5 à la fin de chaque requête. Ceci afin de garantir que la transmission NTP provient d'un client ou serveur NTP de confiance.

3 Choisir l'authentification parmi la liste suivante :

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

4 Définir une clé comprise entre 1 et 16 caractères (caractères spéciaux et non alphabétiques impossibles. Ex.: !, $, #, %)

4.6.6. NTP-Autokey

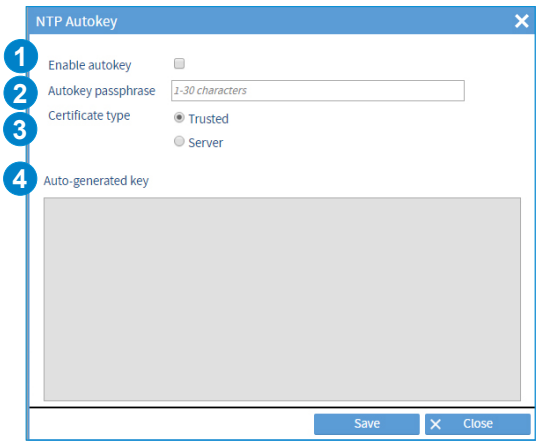


Pour rappel, il est indispensable que les appareils disposent de hostname différents.

Pour activer le mode NTP autokey, suivre les étapes ci-dessous :

1) Menu TIME > NTP > NTP-Autokey :

2) Cliquer sur Configure, la fenêtre suivante apparaît :

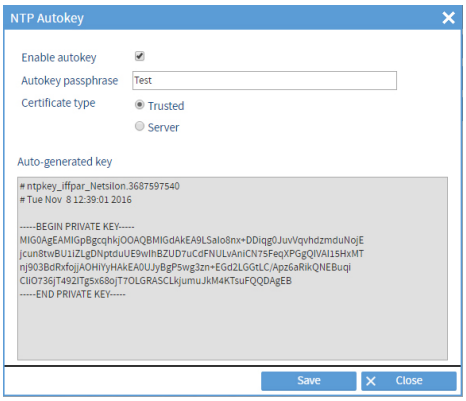


1 Cocher la case pour activer et définir l'autokey.

2 Définir la passphrase en respectant le nombre maximum de 30 caractères.

3 Avant qu'un serveur puisse être désigné client ou serveur, il doit être désigné comme Trusted. Lors de la désignation d'un serveur comme Trusted, choisir Trusted puis sauvegarder. Un certificat est ensuite généré pour le réseau.

4 Certificat. Ce certificat est à copier-coller dans les paramètres NTP Autokey des serveurs clients.
Exemple :



Le certificat est valable 1 an mais il est auto-renouvelé tous les mois.

4.6.7. NTP-Anycast

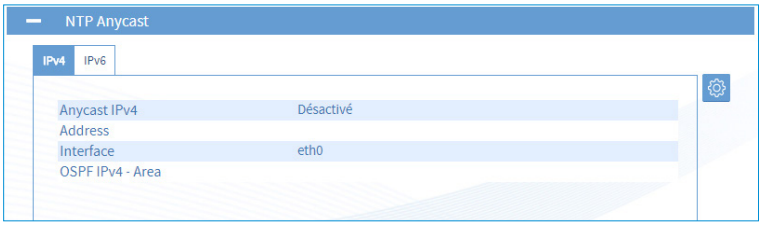
Anycast est appliqué au protocole NTP afin d'établir une communication fiable entre client et serveur (redondance de serveurs).

Le réseau (routeur / switch) doit supporter le protocole OSPF.

Les horloges (clients) envoient une requête à destinations des serveurs. Le switch Anycast OSPF sélectionnera le serveur répondant le plus rapidement afin de redescendre l'informations aux clients.

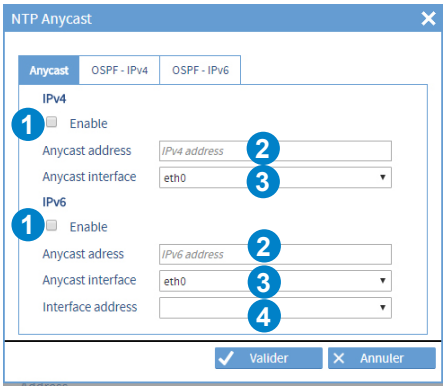
Pour activer le mode NTP anycast, suivre les étapes ci-dessous :

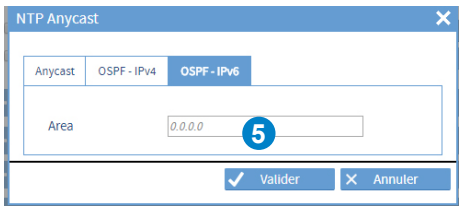
1) Menu TIME > NTP > NTP-Anycast :



L'Anycast ne se lance que si le produit est synchronisé.
Il se coupe en cas de perte de synchronisation.

2) Cliquer sur ⚙, la fenêtre suivante s'ouvre :





1 Activation/désactivation du mode NTP Anycast.

2 Renseigner l'adresse Anycast.

3 Sélectionner l'interface réseau sur laquelle est connecter le câble du réseau. Contacter l'administrateur réseau.

4 Sélectionner l'adresse de l'interface.

5 Renseigner l'adresse «Area» (doit être identique à celle paramétrée dans votre Switch Anycast OSPF). Contacter l'administrateur réseau.

L'Anycast IPv6 a besoin d'une adresse IPv4 sur l'ETH qui gère l'Anycast (l'adresse IPv4 est utilisée comme router-ID).

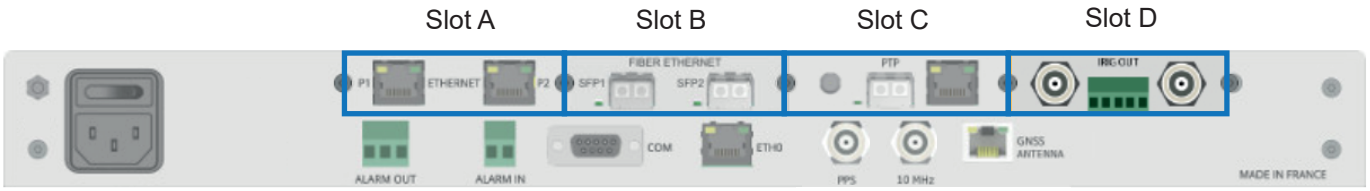
4.7 Distribuer l'heure

La distribution de l'heure peut être réalisée de plusieurs façons:

- NTP en utilisant les cartes option Ethernet RJ45 et/ou Ethernet SFP.
- PTP.
- IRIG.
- ASCII : temps codé NMEA 0183,...

La sélection des cartes options peut s'effectuer de deux façons :

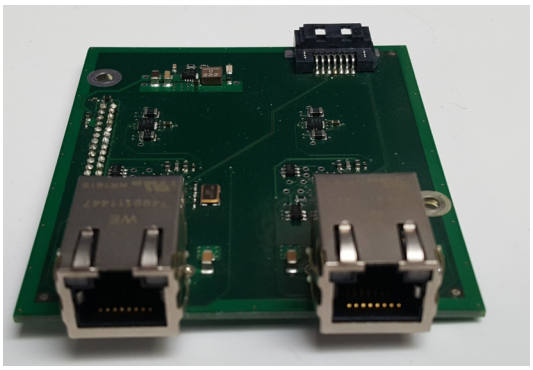
- En mode dynamique : passer la souris sur la carte option désirée puis cliquer. Le menu dédié à cette carte option se déroule à l'écran.
- Cliquer sur la touche + de la carte option désirée.



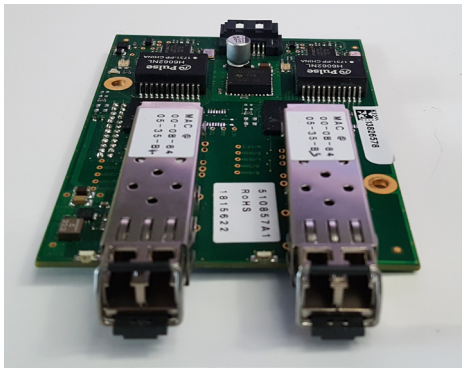
Les cartes option Ethernet (RJ45 et/ou SFP) ne peuvent être installées que dans les slots A, B, C.

Voir chapitre 4.4 pour la configuration des cartes Ethernet.

4.7.1 Carte option ETHERNET (RJ45 réf.: 907 920) (SFP réf.: 907 021)



RJ45



SFP

La carte option réseau permet de synchroniser plusieurs réseaux Ethernet indépendants.

Pour configurer une sortie réseau, se reporter au chapitre **4.4.1 Configuration des interfaces réseaux.**

L'installation mécanique est réalisée dans notre usine. Dans le cas d'une installation ultérieure, se reporter à la notice d'installation des cartes options disponibles sur www.bodet-time.com.

Les étiquettes contenant l'adresse MAC de chaque port sont placées dans la lignée du connecteur RJ45.

Lors de l'inspection d'un connecteur de fibre optique, toujours s'assurer qu'il n'y a plus de source lumineuse. Il y a risque de dommage grave pour les yeux.

4.7.2. Carte option PTP (réf.: 907 922)

Le PTP (Précision Time Protocole – IEEE1588) est un protocole Ethernet permettant d'atteindre un haut niveau de précision horaire de l'ordre de la nanoseconde. Contrairement au NTP, le PTP fait intervenir la couche physique pour atteindre un tel niveau de précision en horodatant et en transmettant l'horodatage lors de l'envoi des trames sur le réseau. Le PTP permet en outre de synchroniser 2 équipements en temps, en fréquence et en phase.

Ce protocole est régi par un fonctionnement Maître-Esclave (Master-Slave) des horloges présentes sur le réseau. Certaines, par leur paramétrage et leurs meilleures caractéristiques de synchronisation sont alternativement éligibles au statut de Master Clock et diffusent les messages de synchronisation horaire SYNC aux Slaves. L'intervalle de temps entre l'émission de 2 trames de synchronisation par la Master Clock est appelé Sync Interval. La Master Clock doit être elle-même synchronisée par la réception d'un signal horaire en provenance d'une constellation (GPS, Glonass, Galileo…).

Pour définir la Master Clock, il existe un algorithme nommé BMCA (Best Master Clock Algorithm) dont certains paramètres sont réglables par l'utilisateur.

Voici les critères du BMCA pour le choix de la Master Clock :

1. Priority 1 (réglable par l'utilisateur) : valeur sur 8 bits qui donne un indice de priorité (plus la valeur est faible, plus la priorité est haute)
2. Clock Class: classe de l'horloge (fiabilité de la source horaire, suivant son statut : synchronisée sur une constellation, holdover,…) qui lui confère un indice de priorité,
3. Clock Accuracy: la plage de précision entre l'horloge et l'UTC (en provenance de la constellation de synchronisation), en nanosecondes,
4. Clock Variance: la stabilité de l'horloge,
5. Priority 2 (réglable par l'utilisateur) : valeur sur 8 bits qui donne un indice de priorité en cas de défaillance des autres critères (plus la valeur est faible, plus la priorité est haute),
6. ClockIdentity: identifiant unique de chaque horloge (MAC de l'interface)

Le BMCA est présent dans chaque périphérique PTP afin que tous choisissent la même Master Clock. Les horloges éligibles au statut de Master Clock mais n'ayant pas ce rôle à jouer à l'instant courant (car n'ayant pas les meilleures caractéristiques de synchronisation) passent en mode « passif ».

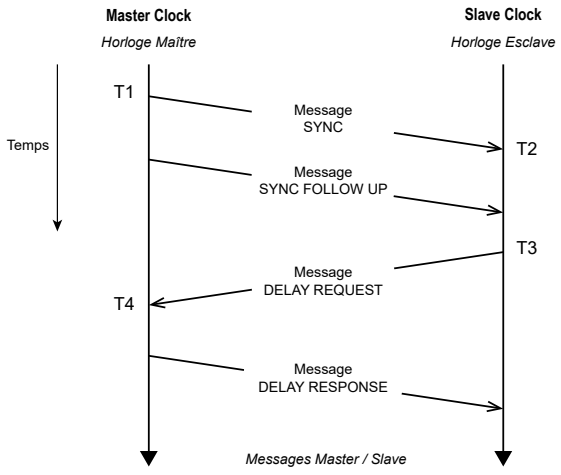
Périodiquement, les horloges éligibles au statut de Master Clock diffusent sur le réseau aux Slaves un message ANNOUNCE comportant ses paramètres et ses caractéristiques de synchronisation. L'intervalle de temps entre l'émission de 2 de ces messages est appelé Announce Interval. Suite à réception de ce message ANNOUNCE par les Slaves, le BMCA définit la Master Clock pour l'ensemble des Slaves qui vont donc se synchroniser sur elle.

La précision extrême de ce protocole tient aussi au fait que le délai de propagation d'une trame PTP à travers le réseau (et donc le retard induit généré) est constamment corrigé par un algorithme de calcul.

Au départ d'une trame de synchronisation SYNC de la Master Clock vers les Slaves, soit la trame est horodatée directement par le port de sortie du périphérique (mode One Step) de la Master Clock, soit un deuxième message FOLLOW UP suit immédiatement le message SYNC pour donner son heure d'émission (mode Two Step).

Après réception du message SYNC, les Slaves envoient un message DELAY REQUEST vers la Master Clock qui répond par un message DELAY RESPONSE.

Ces échanges de messages horodatés entre Master et Slaves permettent de mesurer le délai de transit et l'offset puis d'appliquer une correction par un algorithme de calcul afin que Master et Slave soient synchronisés.

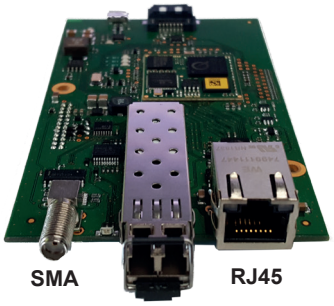


Pour garantir un haut niveau de précision sur un réseau véhiculant des trames PTP, il convient d'utiliser des switchs spécifiques. On distingue 2 types de Switchs :

› La **Boundary Clock** (BC) qui se synchronise sur la Master Clock (devenant ainsi son Slave) mais devient Master pour les Slaves à qui elle sert de relai sur le réseau,

› La **Transparent Clock** (TC) laisse passer les trames PTP en provenance de la Master Clock en ajoutant une correction horaire pour prendre en compte le temps de transit à travers son périphérique.

Le protocole PTP nécessite une architecture réseau adaptée (switch, routeurs,…) pour garantir un haut niveau de précision.



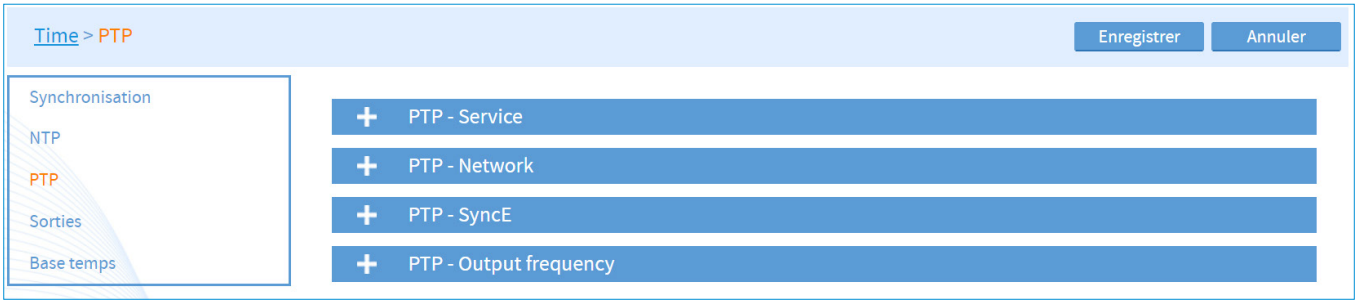
L'option PTP ne fonctionne que pour une réception GNSS.
Le mode master fonctionne avec une réception GNSS mais ne fonctionne pas si la réception GNSS est basée sur la constellation GLONASS uniquement.

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

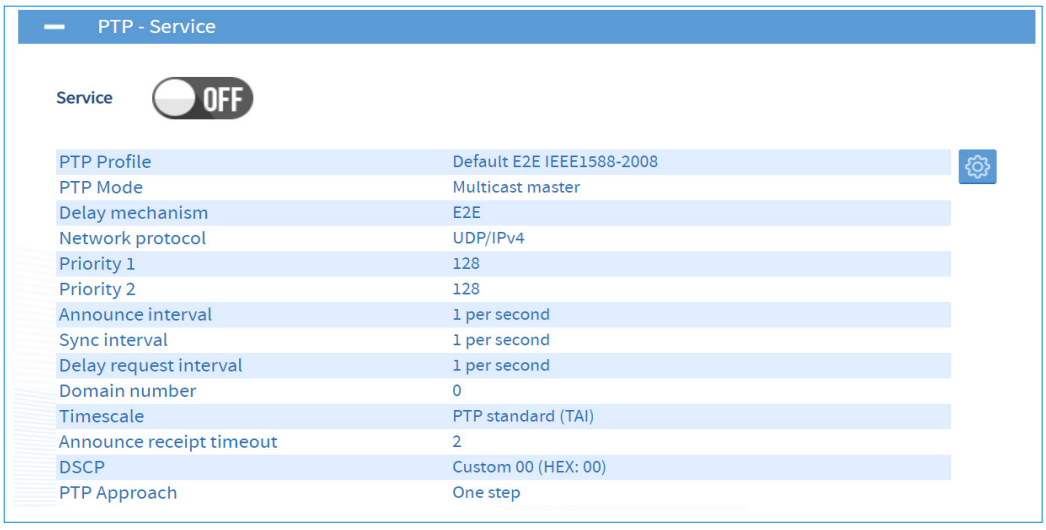
Sortie Frequence sur connecteur SMA configurable.

Pour paramétrer la sortie PTP, suivre les étapes ci-dessous :

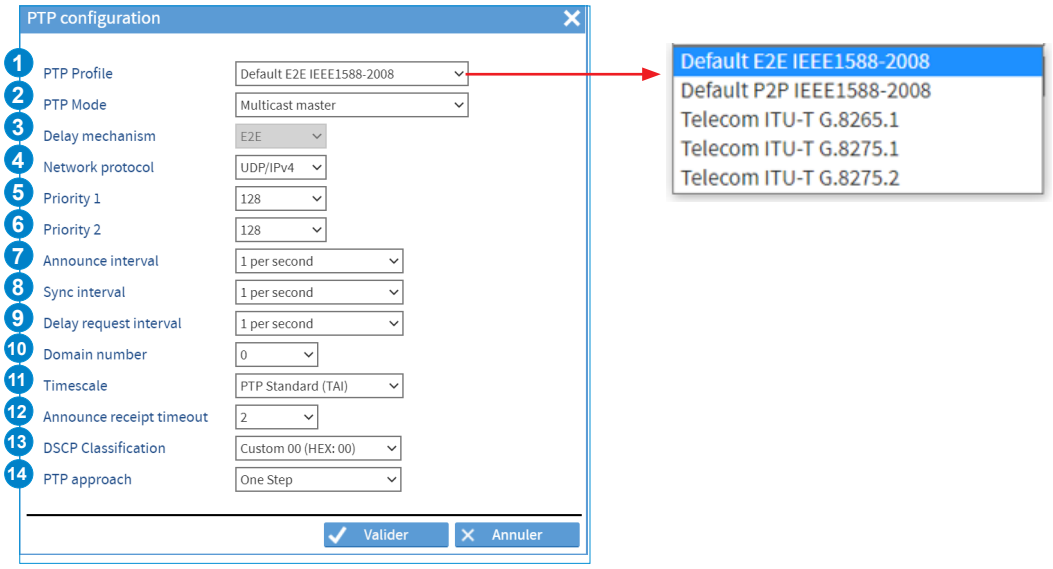
1) Menu TIME > PTP



2) Activer le service à l'aide du bouton ON ,



3) Effectuer la configuration, cliquer sur , la fenêtre suivante apparaît :



1 PTP Profile : choisir le «PTP profile» qui définit et implique notamment :

- Les paramètres de l'algorithme pour le choix de la meilleure Master Clock sur le réseau (BMCA),
- Les paramètres de configuration et d'envoi des trames de données,
- La manière de déterminer le délai de retard des trames de données (End-to-end ou Peer-to-Per).

Les «PTP profile» suivant sont supportées :

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

Les «PTP profile» Telecom répondent à des besoins spécifiques aux réseaux de télécommunication par l'utilisation d'un BMCA (Best Master Clock Algorithm) particulier. Le produit supporte les profils télécom, par contre, sa conformité aux normes télécom, qui, en plus du protocole imposent des contraintes de précision (par ex. sur le MTIE et le DTEV), n'a pas été contrôlée.

L'utilisation du profil P2P requiert la présence d'un réseau (machines, switch, routeurs…) supportant ce type de mécanisme de mesure. Le mécanisme P2P n'est pas disponible en liaison unicast (PTP mode).

2 PTP mode : choisir le rôle et le mode de synchronisation sur le réseau.
Les possibilités de synchronisation dépendent du «PTP Profile» préalablement choisi.

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

* uniquement en multicast

› **Mode Multicast** : Les trames de données sont envoyées du Master vers les Slaves par le biais d'une adresse de diffusion Multicast dédiée spécifiquement au protocole PTP. Seuls les Slaves qui écoutent sur cette adresse reçoivent les paquets de données.

› **Mode Unicast** : Liaison point à point entre le Master et les Slaves réalisée par le biais d'une adresse IP unique pour chaque horloge esclave du réseau. Le Master envoie pour chaque Slave les paquets de données. Ce mode de liaison suppose plus de ressources de la part du Master et génère plus de trafic.

Certains routeurs peuvent bloquer le mode multicast.

3 Delay mechanism : choisir le mécanisme pour la mesure du délai de retard.
Il indispensable de connaître la durée de transit du message SYNC du Master jusqu'aux Slaves pour mesurer puis corriger la latence du réseau et fournir une information horaire correcte. La manière de mesurer le retard

des paquets de données au travers du réseau dépend directement du choix du «PTP Profile». On distingue les profils Default E2E (End-to-end) de Default P2P (Peer-to-Per) car il existe deux mécanismes différents pour mesurer le délai de retard d'un message.

›E2E : le délai de retard des paquets est directement déterminé par un échange de requêtes directes qui traversent le réseau du Master jusqu'aux Slaves.

›P2P : le délai de retard des paquets est déterminé entre 2 éléments consécutifs du réseau (switch,…) puis additionnés successivement pour donner le délai de retard total du Master jusqu'aux Slaves.

4 Network protocol : choisir le protocole réseau entre l'UDP IPv4, l'IPv6 et l'IEEE 802.3. Il est recommandé d'utiliser les protocoles UDP IPv4 / IPv6 qui sont compatibles dans la plupart des environnements réseau.

5 Priority 1 : choisir une valeur. La saisie de cette valeur définissable sur 8 bits est le paramètre principal qui permet de définir la meilleure Master Clock sur le réseau entre plusieurs éligibles (algorithme BMCA). La valeur par défaut est 128 et peut osciller entre 0 et 255. Plus la valeur est faible plus la priorité est importante.

6 Priority 2 : choisir une valeur. La saisie de cette valeur définissable sur 8 bits est le cinquième paramètre (sur six) qui permet de définir la meilleure Master Clock sur le réseau entre plusieurs éligibles (algorithme BMCA). La valeur par défaut est 128 et peut osciller entre 0 et 255. Plus la valeur est faible plus la priorité est importante.

7 Announce interval : choisir l'intervalle de durée auquel les horloges éligibles au statut de Master Clock envoient le message ANNOUCE, comportant leurs paramètres de synchronisation et de précision sur le réseau. En fonction de la qualité des valeurs transmises et des priorités fixées au sein de son algorithme, le BMCA définit la Master Clock.

8 Sync interval : choisir l'intervalle de durée pour l'envoi d'une trame de synchronisation. Plus le nombre de trames est élevé, meilleure est la précision. En contrepartie, cela surcharge le réseau. Il y a donc un compromis à trouver entre la précision et la charge générée sur le trafic.

9 Delay request interval : Choisir l'intervalle de durée pour l'envoi d'une requête des Slaves vers la Master Clock afin de déterminer le délai de retard des paquets de données.

10 Domain number : choisir le numéro de domaine. Il est possible de définir plusieurs domaines au sein d'un même réseau. Chaque domaine aura sa propre Master Clock et ses Slaves.

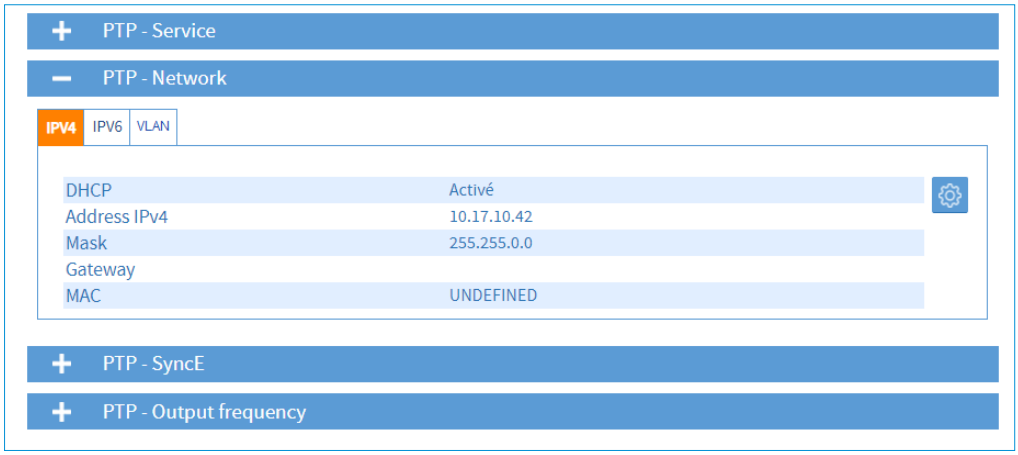
11 Timescale : choisir l'échelle de temps. Par défaut, le Temps Atomique International (TAI) est sélectionné. Celui-ci se base sur la définition de la seconde élaborée à l'aide de l'horloge atomique et n'est pas impacté par les secondes intercalaires. Néanmoins, l'offset pour calculer l'UTC est transmis dans les trames PTP.
L'échelle de temps arbitraire (UTC=0) ne peut servir que dans le cadre de tests. Avec cette échelle, les horloges esclaves ne seront pas en capacité de calculer l'heure UTC valide.

12 Announce receipt timeout : choisir une valeur qui définit le délai avant déconnexion d'un Slave au Master sans réception d'un message ANNOUNCE de sa part. Cette valeur est un multiplicateur.
Exemple : si le Announce Interval est de 2 secondes et que le Announce receipt timeout est de 3, l'intervalle de temps avant expiration est de 6 secondes.

13 DSCP classification : choisir un profil. Celui-ci permet d'effectuer un choix de priorisations des trames PTP.
DSCP (Differentiated Services Code Point) est une architecture réseau qui définit un mécanisme pour ordonner et contrôler le trafic réseau tout en fournissant de la qualité de service (faire transiter dans les meilleures conditions possibles un type de trafic, en termes de disponibilité, de débit,…), en faisant la distinction entre les services et les données avec un code.
Le DSCP permet donc d'identifier et de prioriser les trames PTP en cas de surcharge réseau pour garantir la précision des systèmes critiques.

14 PTP approach : choisir le mode de fonctionnement.
Le PTP implique l'envoie périodique de messages SYNC du Master vers les Slaves avec un horodatage précis. Pour ce faire, suivant le matériel utilisé, il y a 2 possibilités :
› En mode One Step, le message SYNC est envoyé et horodaté directement depuis le port de sortie du Master (grâce à sa couche physique) vers les Slaves.
› En mode Two Step, le message SYNC est envoyé depuis le Master vers les Slaves sans horodatage inclus dans le message. Un deuxième message dit FOLLOW UP suit immédiatement le premier message pour l'horodater.

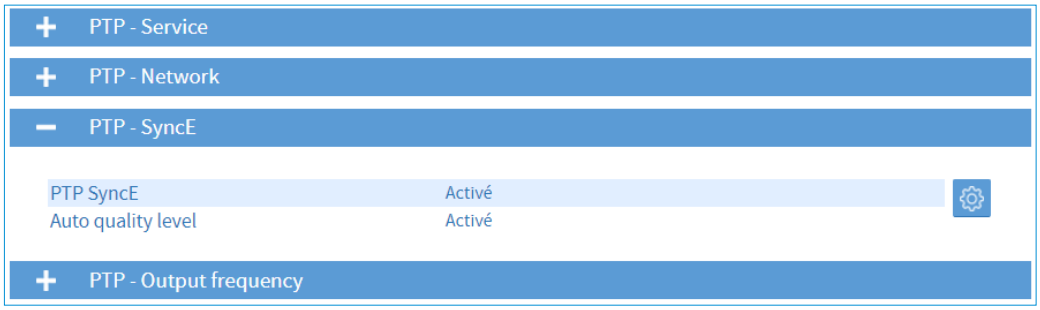
4) Configurer PTP Network :



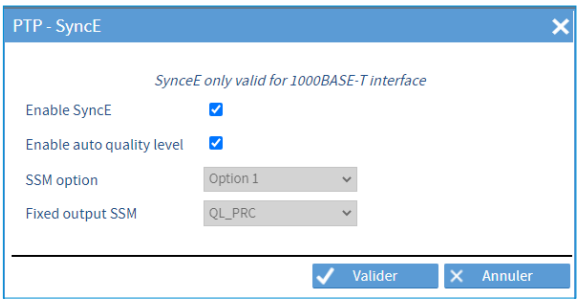
Fonctionnement en IPv4 : configuration IP fixe ou service DHCP
Fonctionnement en IPv6 : adresse locale de lien (avec adresse IPv4: IP fixe ou service DHCP activé)
Support du VLAN tagging : gestion optimisée du trafic (VLAN ID + indice de priorité).

5) Configurer PTP SyncE.

SyncE (Synchronous Ethernet) est un protocole permettant de faciliter la circulation des signaux d'horloge sur la couche physique Ethernet en assurant une propagation fiable et synchrone du signal de la Master Clock vers les horloges esclaves d'un réseau. Son activation permet donc de gagner en précision.

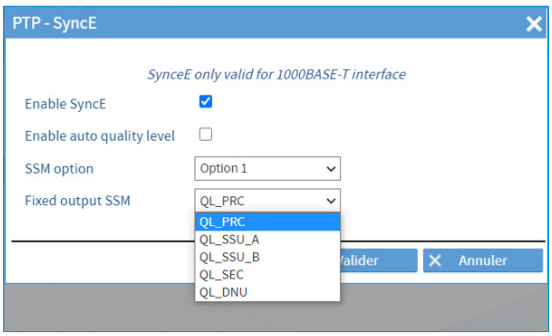


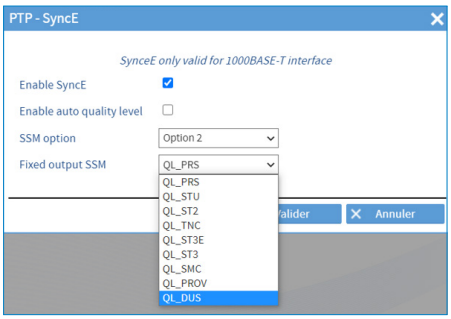
En cliquant sur , la fenêtre suivante apparaît :



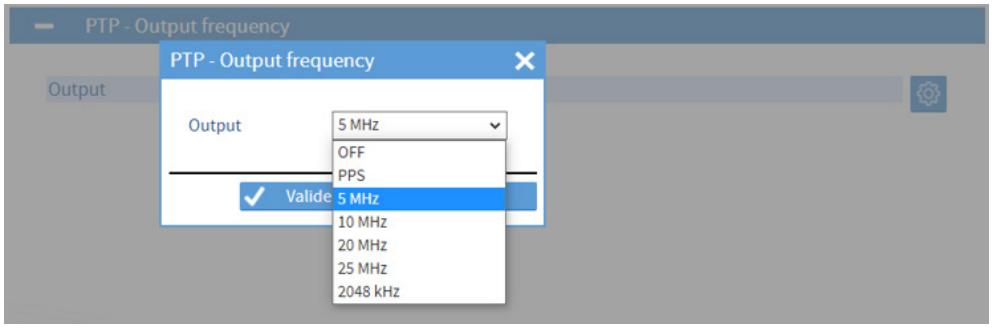
Il est recommandé de laisser cocher « Enable auto quality level ».

« Enable auto quality level » désactivé, 2 options de SSM sont proposées avec les choix suivants:





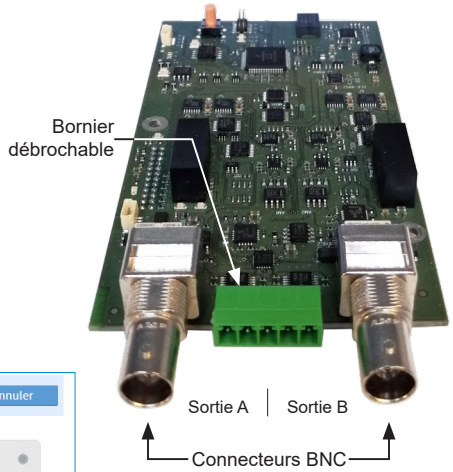
6) Configurer Sortie Fréquence.



- La sortie fréquence SMA est toujours liée au master:
  - o Mode master : la fréquence et la phase du 1pps sont l'image de la base de temps du Netsilon.
  - o Mode slave : la fréquence et la phase du 1pps sont l'image de la base de temps du master sur lequel l'option est synchronisée.

4.7.3. Carte option IRIG OUTPUT (réf.: 907 930)

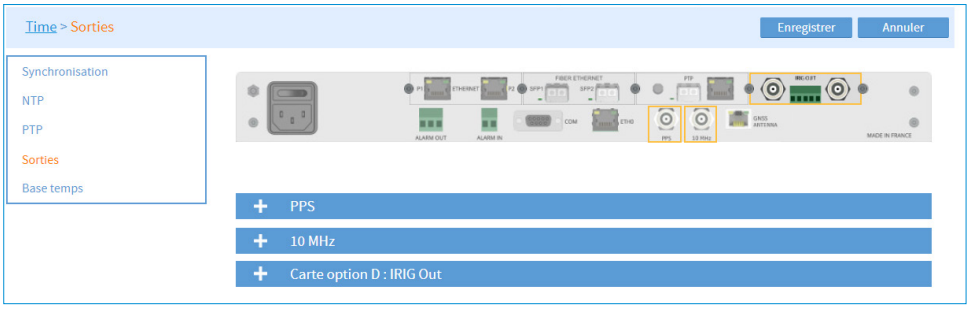
La carte option IRIG OUTPUT dispose de 2 sorties indépendantes générant des signaux IRIG pour synchroniser des équipements.



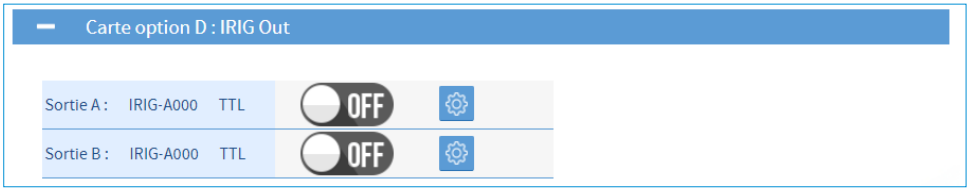
Ces 2 sorties indépendantes permettent de générer 2 formats d'IRIG différents et la gestion de 2 zones horaires.

Pour paramétrer les 2 sorties IRIG,
suivre les étapes ci-dessous :

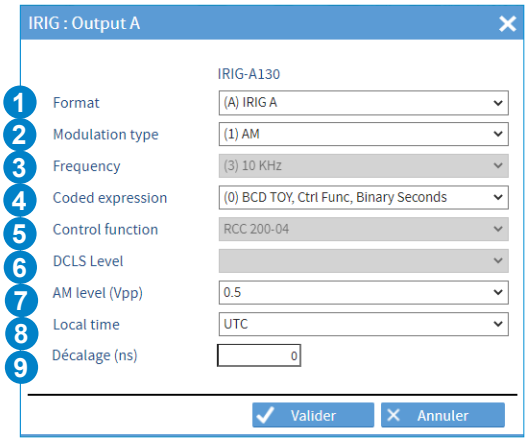
1) Menu TIME > Sorties > IRIG OUT



2) Activer les sorties de la carte option avec le bouton ON correspondant à chaque sortie.



3) Effectuer la configuration de chaque sortie, cliquer sur les boutons , la fenêtre suivante apparaît :



1 Choix du format de sortie : IRIG A/B/E/G, AFNOR 87500.
Les formats IRIG se caractérisent par des fréquences d'impulsion différentes.

Format	Fréquence d'impulsion	Intervalle
IRIG A	1000 PPS	1 ms
IRIG B	100 PPS	10 ms
IRIG E	10 PPS	100 ms
IRIG G	10000 PPS	0.1 ms

2 Choix du type de modulation du signal de sortie :
- (0) DCLS (DC Level Shift) : codage en largeur d'impulsion,
- (1) AM (Amplitude Modulated) : onde sinusoïdale porteuse modulée en amplitude.

3 Choix de la fréquence de modulation du signal de sortie.
Elle dépend directement du format et du type de modulation préalablement choisi.

Fréquence de modulation
(0) Pas de porteuse (DCLS)
(1) 100 Hz
(2) 1 kHz
(3) 10 kHz
(4) 100 kHz

4 Choix de l'expression codée. Elle dépend directement du format et du type de modulation préalablement choisi.
Cela définit la nature des données incluses dans le signal IRIG.

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

5 «Control Function» est une série de bits disponibles pour faire transiter au choix des informations complémentaires dans le signal IRIG de sortie (exemple : l'année en cours).
Netsilon est compatible avec la norme RCC 200-04.

6 Choix du mode de transmission (TTL ou RS422) pour les formats DCLS en fonction du type de câble utilisé entre Netsilon et l'appareil récepteur du signal IRIG.

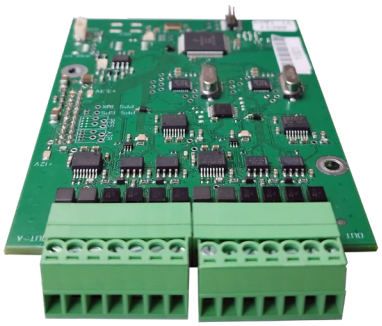
7 Choix de la tension du signal pour les formats AM afin de pallier à d'éventuelles interférences ou à une distance de transmission importante avec l'appareil récepteur du signal.

8 Fuseau horaire du signal IRIG de sortie.
La zone horaire doit être préalablement ajoutée dans Netsilon (sauf si UTC) :
Menu TIME > Base de temps > Zones horaires.

9 Offset servant à compenser le délai de transmission du signal IRIG entre Netsilon et l'appareil récepteur (suivant la longueur du câble). **La gestion de la compensation n'est pas disponible avec l'IRIG E.**

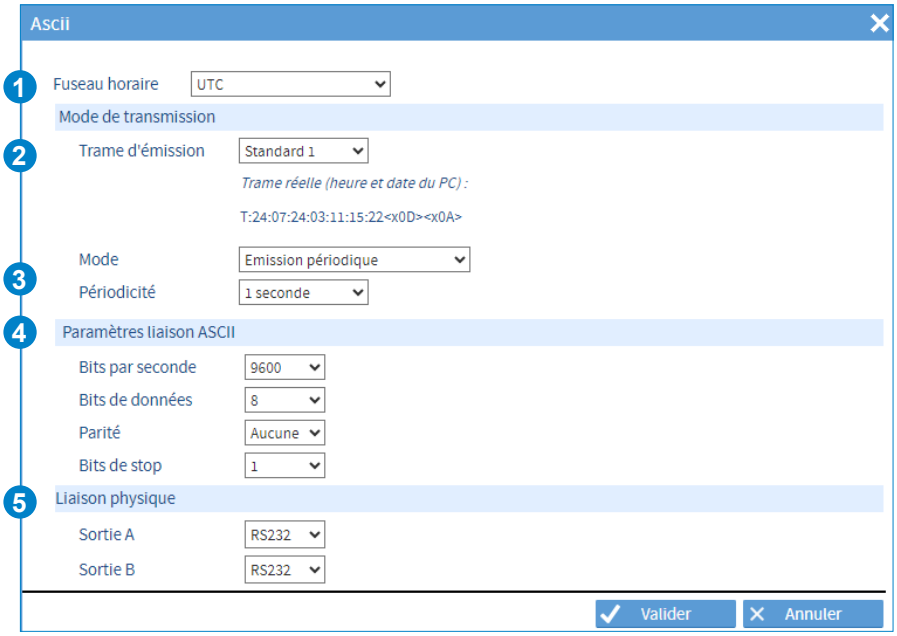
4.7.4. *Carte option ASCII (réf.: 907 924)*

La carte option ASCII permet de distribuer l'heure en temps codé sur une interface série RS232, RS422 et RS485.
Pour paramétrer les sorties ASCII, suivre les étapes ci-dessous :
1) Menu TIME > Sorties > Carte option ASCII :


Sortie A Sortie B

2) Activer les sorties à l'aide du bouton ON, puis enregistrer.

3) Cliquer sur pour la configuration, la fenêtre suivante s'ouvre :



1 Fuseau horaire du signal ASCII de sortie.
La zone horaire doit être préalablement ajoutée dans Netsilon (sauf si UTC) :
Menu TIME > Base de temps > Zones horaires.

2 Choix de l'expression codée. Cela définit la nature des données incluses dans le signal ASCII.

	Contenu du message	Exemple
Standard 1	T:AA:MM:JJ:NJ:HH:MM:SS "x0D""x0A"	T:08:10:09:04:15:12:30<CR><LF>
Standard 2	"x02" 00 JdS JJ/MM/AA HH:MM:SS "0D"	02 00 Jeu 09/10/08 15:12:30<CR>
Simulation GPS ZDA GGA	$GPZDA,HHMMSS.00,JJ,MM,AAAA,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,082613.000,0000.00,N,00000.0000,W,1,12,0.00,000.0,M,00.0,M,,*73<CR><LF>
Prog.	%01 : jour du mois %02 : mois %03 : année %04 : heure %05 : minute %06 : seconde %07 : jour de la semaine %08 : Signe décalage horaire %09 : Heure décalage horaire %10 : Minutes décalages horaire %11 : Saison %31 : ID de la trame %32 : Checksum	« TIME :%04 :% :05% :%06 » à 12h30 et 12 secondes sera « TIME :12 :30 :12 »

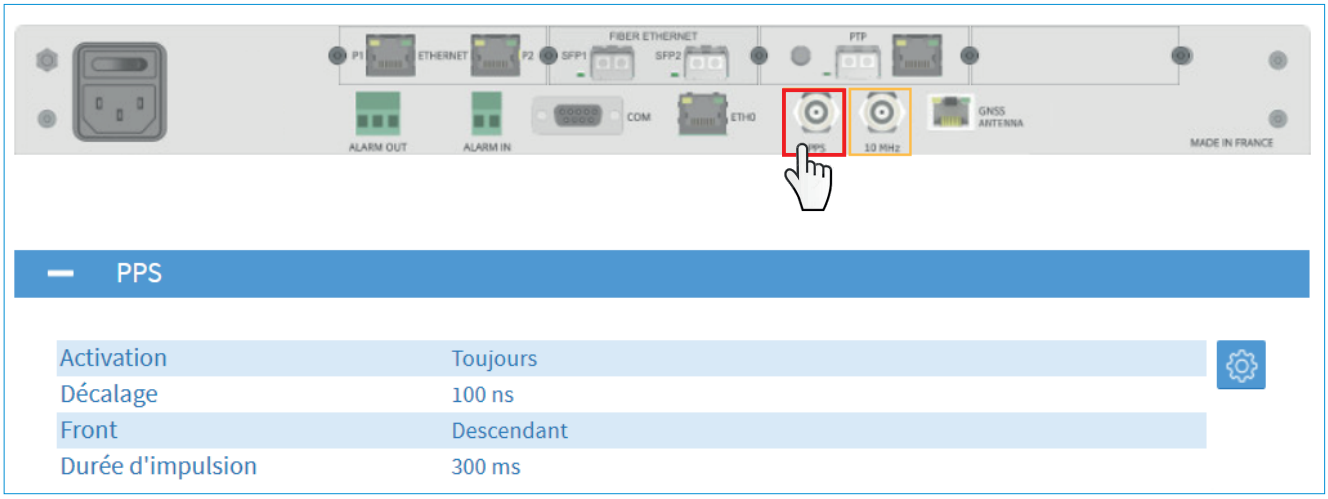
3. Choix du mode d'envoi de la trame ainsi que du réglage associé :
   - Emission sur demande à la suite d'une requête « T », « ? » ou programmable (Prog.),
   - Emission périodique avec un intervalle de 1 seconde, 30 secondes, 1 minute, 10 minutes ou 1 heure.
4. Paramètres de la liaison ASCII :
   - Bits par seconde : 1200 à 57600 bauds,
   - Bits de données : 7 ou 8 bits,
   - Parité : aucune, paire ou impaire,
   - Bits de stop : 1 ou 2 bits.
5. Choix du type de liaison physique RS232/422/485 :
   - Sortie A,
   - Sortie B.

4.8 Sorties 1PPS et 10 MHz

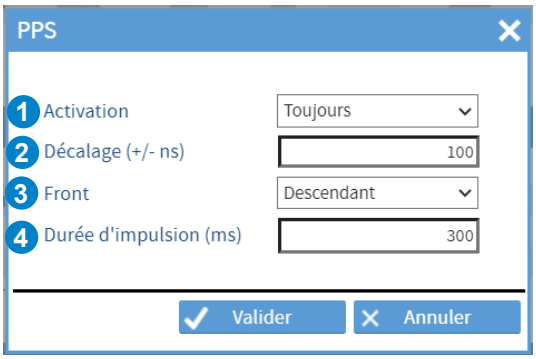
4.8.1 Sortie 1PPS

La sortie 1PPS sur connecteur BNC émet un pulse par seconde de grande précision.

1) Menu TIME > Sorties > Curseur de souris sur sortie 1PPS:



Pour paramétrer la sortie 1PPS cliquer sur . La fenêtre suivante s'ouvre :



1 Activation : -Toujours (Par défaut)
- Sync ou Holdover
- Sync
- Jamais

2 Décalage (+ /- ns) : saisir la valeur manuellement entre -500 000 000 et 500 000 000 (valeur par défaut : 100 ns)

Pour information, un décalage sur la sortie 1PPS n'a pas d'impact sur la synchronisation PTP master.

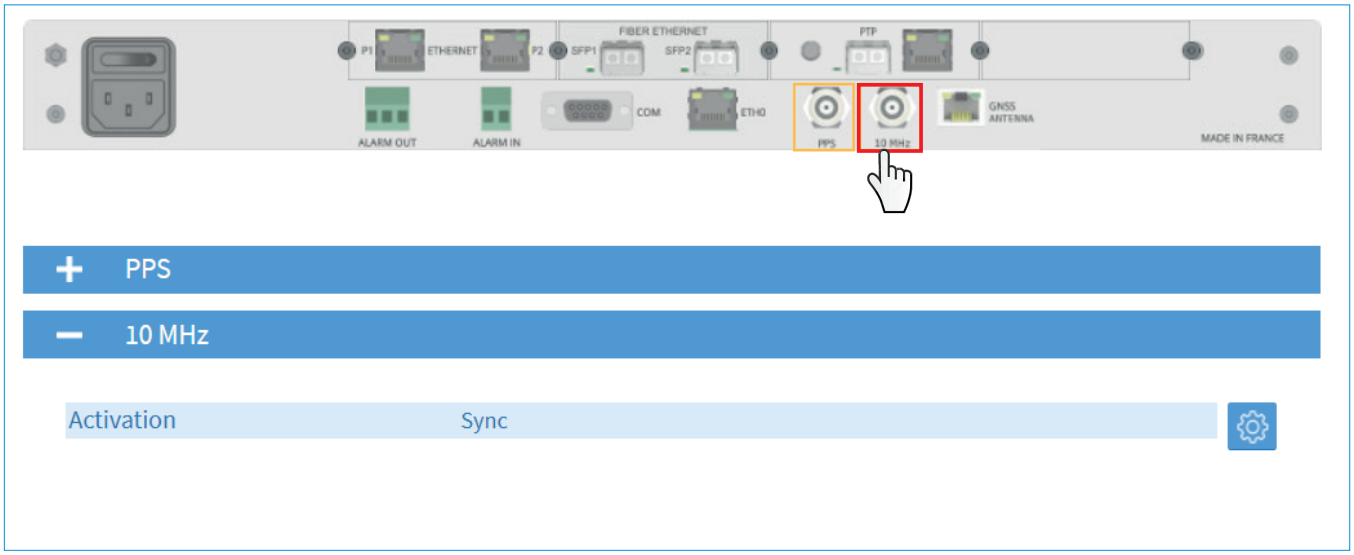
3 Front : - Descendant
- Montant

4 Durée impulsion (ms) : saisir la valeur manuellement entre 1 et 800 (valeur par défaut : 300 ms).

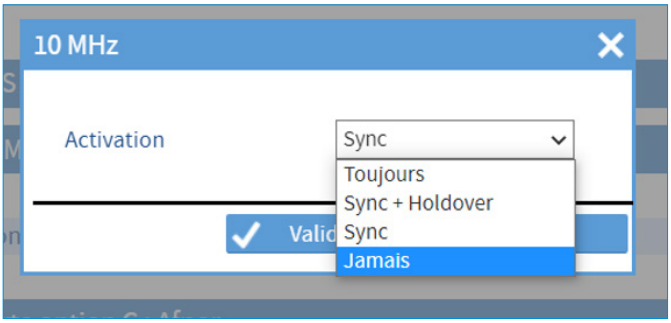
4.8.2 Sortie 10MHz

La sortie 10 MHz sur connecteur BNC émet un signal sinusoîdal de 10 MHz. Pour information, la sortie 1PPS et la sortie 10 Mhz sont liées.

1) Menu TIME > Sorties > Curseur de souris sur sortie 10 MHz:



Pour paramétrer la sortie 10 MHz cliquer sur . La fenêtre suivante s'ouvre :

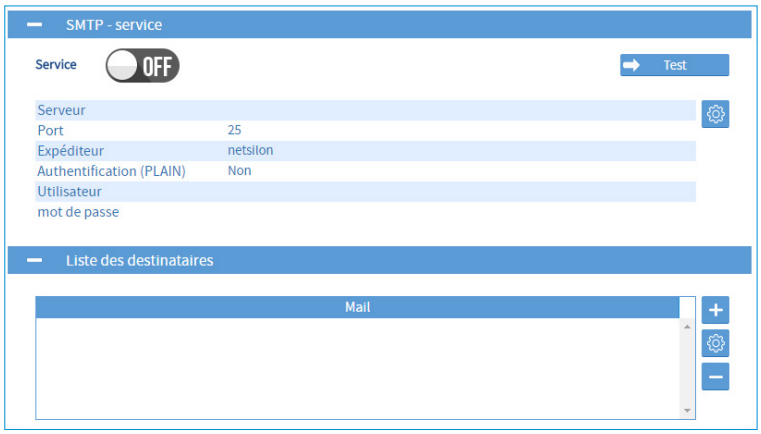


Activation : -Toujours
- Sync ou Holdover
- Sync (par défaut)
- Jamais

4.9 Gestion des notifications

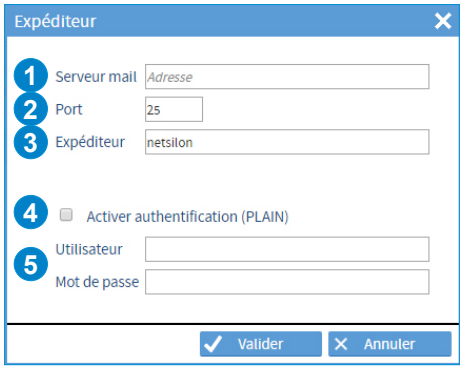
4.9.1. Configuration SMTP

Pour déclarer un serveur SMTP afin d'envoyer les e-mails, suivre les étapes ci-dessous :
1) Menu NOTIFICATION > SMTP :



Cliquer sur Test permet de tester le service directement (sans à avoir à provoquer un défaut sur la centrale).

2) Dans SMTP - service, cliquer sur ⚙, la fenêtre suivant apparaît :



1 Renseigner l'adresse IP du serveur de réception (50 caractères maximum).

2 Définir le port de communication. Port : 5 digits (65535 maximum à la validation).

3 Définir le nom de l'expéditeur des e-mails. C'est-à-dire le nom donné à Netsilon.

4 Cocher la case pour activer l'authentification (type Plain).

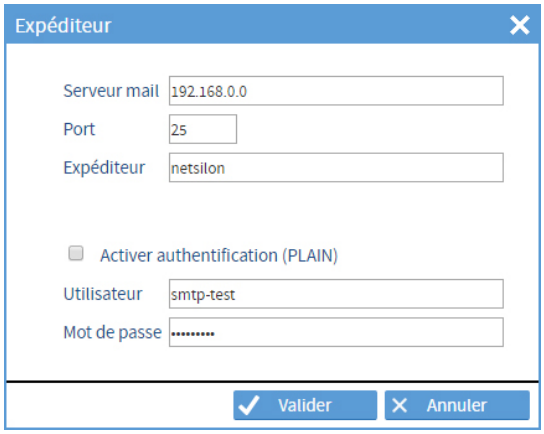
5 Définir les paramètres utilisateurs (utilisateur / mot de passe : 50 caractères maximum).

Se reporter page suivante pour visualiser un exemple de configuration.

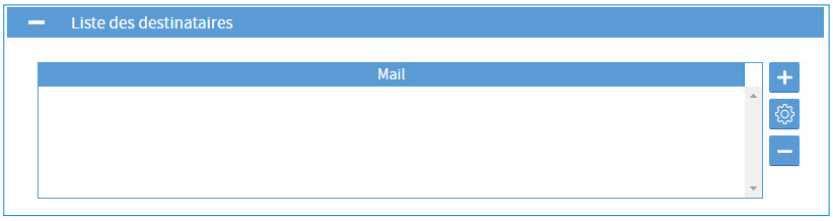
Exemple de configuration :

1) Définir les paramètres de l'expéditeur :

SERVEUR SMTP		
Adresse IP du serveur SMTP	192.168.1.254	
Port	**25**	
Utilisateurs	**e-mail**	**Mot de passe**
Admin	admin@serveurtest.com	testservice
smtp-test	**smtp-test@serveurtest.com**	**testservice**
netsilon1	netsilon1@serveurtest.com	testservice



2) Définir la liste des destinataires :
(5 destinataires maximum)



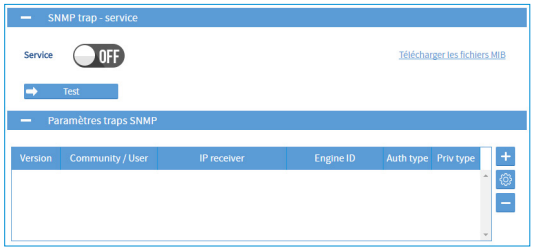
3) Cliquer sur + pour ajouter l'adresse e-mail :
(50 caractères maximum)

4) Activer le service à l'aide du bouton ON, puis enregistrer.

4.9.2. Configuration SNMP trap

Pour configurer la réception des traps, suivre les étapes ci-dessous :

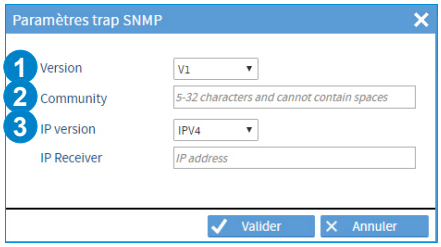
1) Menu NOTIFICATION > SNMP Trap :



Cliquer sur Test permet de tester le service directement (sans à avoir à provoquer un défaut sur la centrale).

Version v1 ou v2c :
(5 comptes maximum)

2) Cliquer sur +, la fenêtre suivante apparaît :



1 Choisir la version SNMP supportée : v1, v2c ou v3.

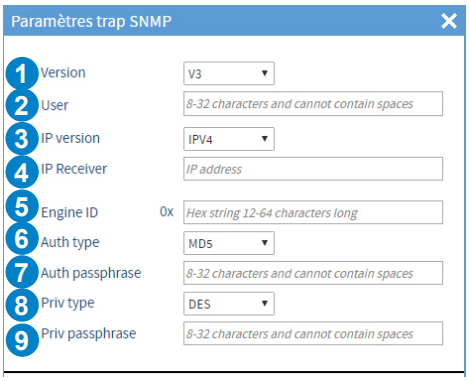
2 Définir un nom de communauté compris entre 5 et 32 caractères sans espace.

3 Renseigner l'adresse IP du serveur de destination des traps.

3) Cliquer sur Valider.

4) Activer le service à l'aide du bouton ON, puis enregistrer.

Version v3 :
(5 comptes maximum)



1 3 4 Se reporter à la capture d'écran précédent.

2 Renseigner le nom de l'utilisateur (entre 8 et 32 caractères sans espace).

5 Renseigner l'identifiant du moteur SNMP.

6 Sélectionner le type d'authentification (MD5 ou SHA) ou l'absence d'authentification (NoAuth).

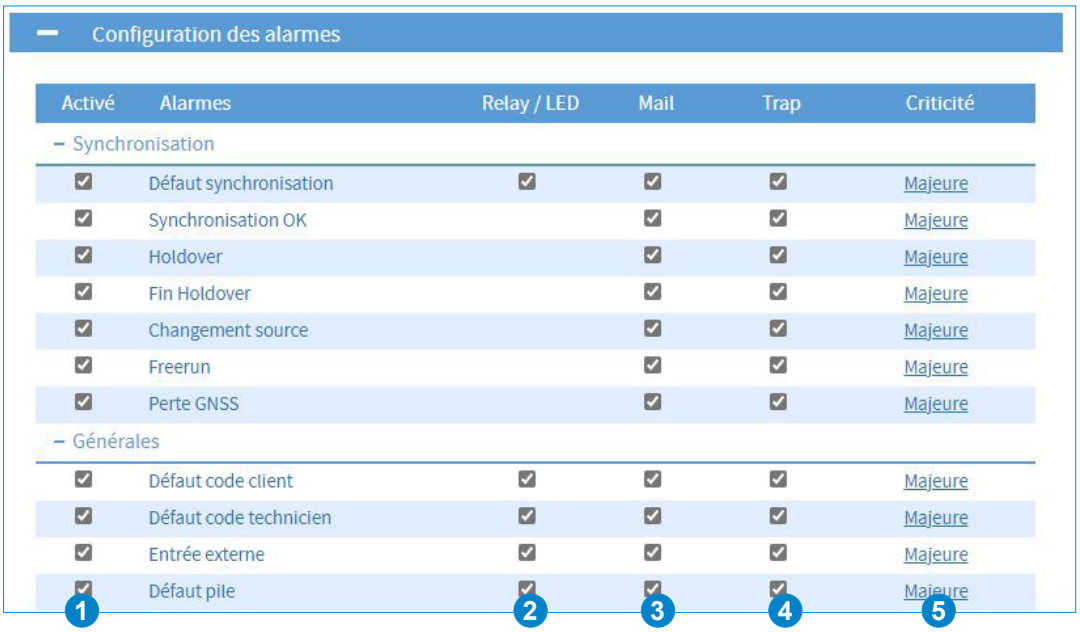
7 Renseigner la passphrase d'authentification (entre 8 et 32 caractères sans espace).

8 Sélectionner le cryptage (DES ou AES128) ou l'absence de cryptage (NoPriv).

9 Renseigner la passphrase d'encryption (entre 8 et 32 caractères sans espace).

4.9.3. Configuration des alarmes

Pour définir le mode de remontée et la criticité des alarmes, suivre les étapes ci-dessous :
1) Menu NOTIFICATION > Alarmes :



1 Cocher la case pour activer la sélection de l'alarme.

2 Cocher la case pour que l'alarme soit identifiée depuis la LED sur la façade avant de Netsilon et remontée par un contact relais.

3 Cocher la case pour que l'alarme soit envoyée par e-mail (se reporter au chapitre **4.9.1 Configuration SMTP**).

4 Cocher la case pour que l'alarme soit envoyée sous forme de trap (se reporter au chapitre **4.9.2 Configuration SNMP trap**).

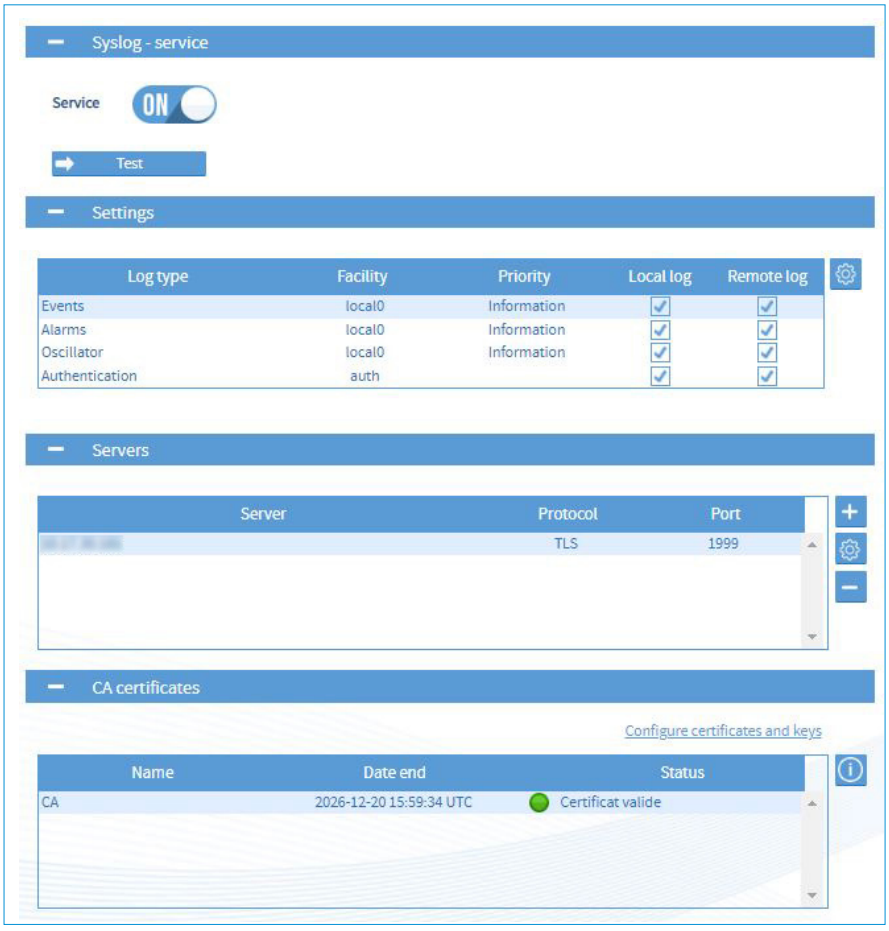
5 Choix du niveau de criticité de l'alarme : mineure, majeure ou critique.

Le suivi et l'acquittement des alarmes sont réalisés dans la section historique, se reporter au chapitre 4.12.9 Historique des alarmes.

4.9.4. Configuration Syslog

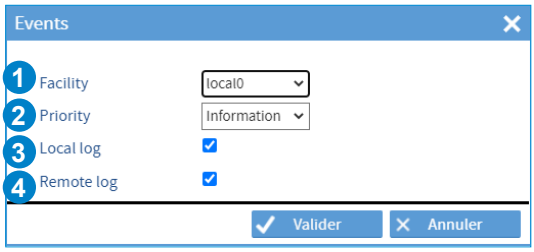
Pour configurer le service Syslog, suivre les étapes ci-dessous :

1) Menu NOTIFICATION > Syslog :
2) Activer le service à l'aide du bouton ON,



Cliquer sur Test permet de tester le service (envoi d'un message Syslog même si les «Events» ne sont pas validés).

3) Pour paramétrer chaque type de log (Events, Alarms, Oscillator, Authentification), sélectionner-le puis cliquer sur ⚙, la fenêtre suivante apparaît :



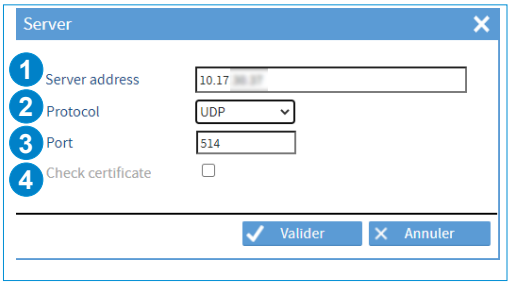
1 Choisir une catégorie au type de message / système à l'origine de l'évènement (Utilisation locale libre). Pour «Auth» l'option facility n'est pas réglable car standardisée par le protocole Syslog.

2 Choisir l'indice de gravité du message.

3 Cocher pour activer le stockage du journal en local.

4 Cocher pour activer l'envoi du journal vers un serveur Syslog. Celui-ci doit encore être ajouté.

4) Ajouter un serveur Sylog en cliquant sur +, la fenêtre suivante apparaît :
(Possibilité d'ajouter jusqu'à 5 serveurs maximum)



1 Saisir l'adresse ou le hostname du serveur Syslog.

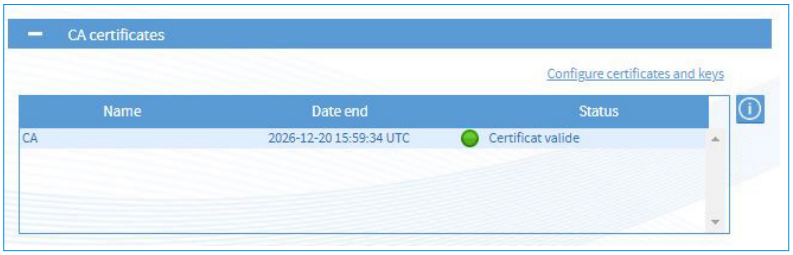
2 Choisir le protocole de communication client/serveur (UDP/TCP/TLS).

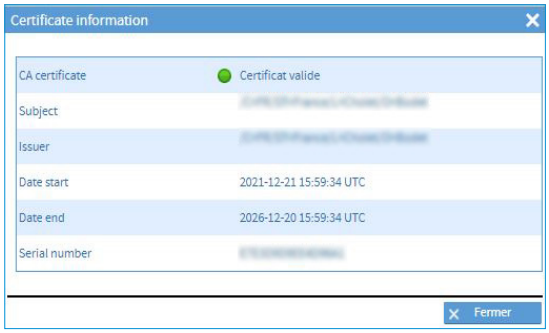
3 Saisir le port réseau.

4 Activer la vérification du certificat (TLS uniquement).

L'ajout d'un certificat permet de générer un chiffrage et d'éviter une liaison en clair.
La vérification du certificat permet de contrôler l'authenticité du serveur.
Pour ajouter un certificat, reportez-vous au chapitre 4.10 Gestion des certificats et des clés.

5) Cliquer sur ⓘ pour visualiser les informations du certificat éventuellement importé depuis le pool des certificats et sur configure certificates and keys pour accéder à ce pool.



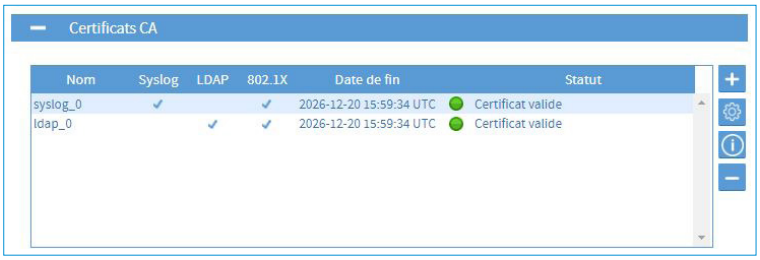


4.10 Gestion des certificats et des clés

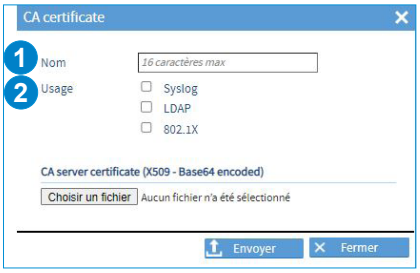
Ce menu permet l'importation des certificats et des clés publiques dans Netsilon.

4.10.1. Importer des certificats CA

Pour ajouter des certificats CA :
1) Menu SÉCURITÉ > Certificats et clés > Certificats CA



2) Cliquer sur +, une fenêtre apparaît :

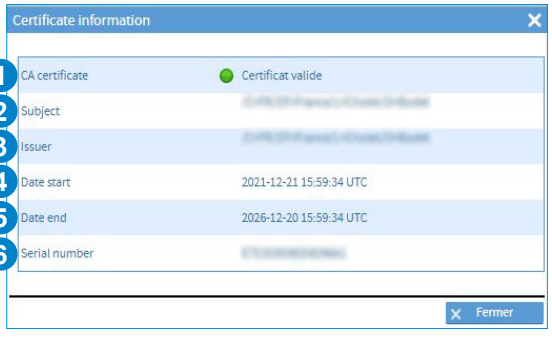


1. Saisir un nom pour le certificat (16 caractères maximum).
2. Sélectionner les cas d'usage du certifcat : Syslog, LDAP, 802.1x (TLS, TTLS, PEAP).

3) Sélectionner le certificat puis cliquer sur Envoyer pour l'importer.

Les certificats doivent être au format X.509 en Base64. Pour rappel, un certificat au format X.509 commence par «---BEGIN CERTIFICATE---» et se termine par «---END CERTIFICATE---».
Le nombre de certificats CA est limité à 40.
Possibilité d'attribuer au maximum 5 certificats CA pour le service Syslog et 5 certificats CA pour le service LDAP. Il est impossible d'ajouter deux fois le même certificat CA.

4) Cliquer sur ⓘ pour visualiser les informations du certificat importé :



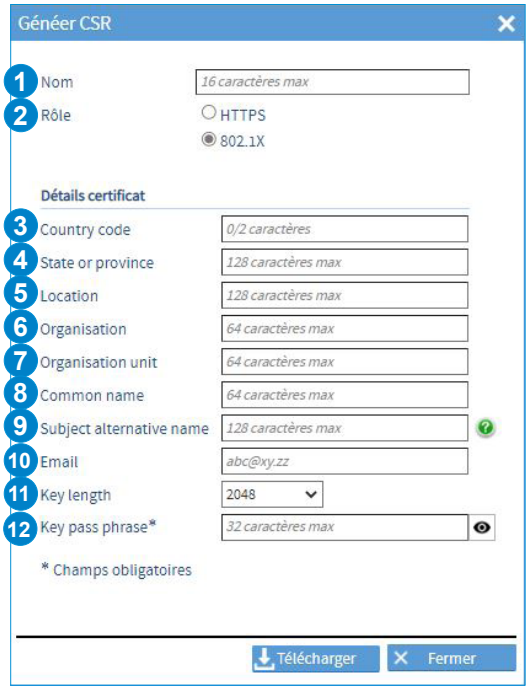
1. Validité du certificat.
2. Auteur du CSR (Certificate Signing Request).
3. Émetteur du certificat (Autorité de Certification).
4. Date de début de validité du certificat.
5. Date de fin de validité du certificat.
6. Numéro de série du certificat.

4.10.2. Importer des certificats signés

Pour ajouter des certificats signés :
1) Menu SÉCURITÉ > Certificats et clés > Certificats signés

Pour importer des certificats signés, la création d'une demande de signature de certificat (CSR: Certificate Signing Request) est nécessaire au préalable. Cette CSR doit être signée par l'Autorité de Certification puis le certificat signé peut être importé dans Netsilon. Il est impossible d'importer directement une clé privée. Il est recommandé de consulter l'Autorité de Certification pour connaître les champs requis dans la demande de certificat X509.

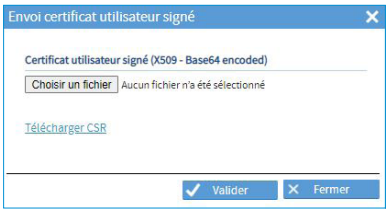
2) Cliquer sur + pour générer une CSR, une fenêtre apparaît :



1. Saisir un nom pour la CSR
(16 caractères maximum, a-z, A-Z, 0-9).
2. Sélectionner le cas d'utilisation du certificat signé demandé auprès de l'Autorité de Certification.
3. Saisir votre code pays
(2 caractères maximum, a-z, A-Z, 0-9).
Voir : https://www.ssl.com/country-codes/
4. Saisir votre région
(128 caractères maximum, a-z, A-Z, 0-9,espace).
5. Saisir votre ville
(128 caractères maximum, a-z, A-Z, 0-9,espace).
6. Saisir le nom légal de votre organisation
(64 caractères maximum, a-z, A-Z, 0-9,espace).
7. Saisir le nom de votre service / département
(64 caractères maximum, a-z, A-Z, 0-9,espace).
8. Saisir le nom complet (FQDN) du domaine à sécuriser
(64 caractères maximum, a-z, A-Z, 0-9,espace, _.+@*:,-).
9. Saisir des noms de domaine alternatifs à sécuriser
(128 caractères maximum, a-z, A-Z, 0-9,espace, _.+@*:,-).
10. Saisir une adresse mail de contact
(128 caractères maximum, a-z, A-Z, 0-9, _.+@-).
11. Sélectionner la taille de la clé privée
(1024, 2048 ou 4096 bits).
12. Saisir un mot de passe de protection de la clé privée obligatoire pour le 802.1x
(de 5 à 32 caractères maximum, a-z, A-Z, 0-9, _.:#*?@+!-/).

3) Cliquer sur Télécharger pour télécharger la demande de signature de certificat (CSR) à transmettre à l'Autorité de Certification pour signature. Il est recommandé d'inspecter le contenu de la CSR / demande de certificat X509 générée et d'appliquer si nécessaire un template lors de la signature pour répondre à des contraintes internes.

4) Importer dans Netsilon le certificat signé correspondant à la CSR émise en cliquant sur ⚙, une fenêtre apparaît :



Les certificats doivent être au format X.509 en Base64. Pour rappel, un certificat au format X.509 commence par «---BEGIN CERTIFICATE---» et se termine par «---END CERTIFICATE---».
Le nombre de certificats signés est limité à 20.

5) Cliquer sur pour visualiser les informations du certificat importé.

4.10.3. Expiration des certificats (Certificats CA et certificats signés)

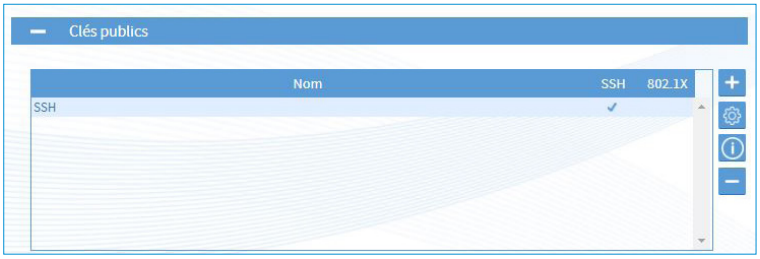
Il est possible de programmer une alarme pour avertir de l'expiration prochaine des certificats.
1) Menu NOTIFICATION > Alarmes > Certificats - Seuil des alarmes

2) Cliquer sur , une fenêtre apparaît :

3) Sélectionner la durée avant laquelle le certificat expire pour l'affichage d'une alarme.

4.10.4. Importer des clés publiques

Pour ajouter des clés publiques :
1) Menu SÉCURITÉ > Certificats et clés > Clés publiques

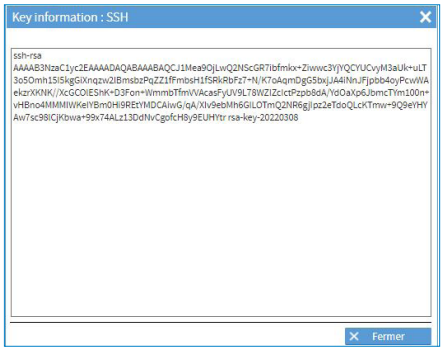


2) Cliquer sur pour ajouter une clé publique, une fenêtre apparaît:

1. Saisir un nom pour la clé publique.
2. Sélectionner le cas d'utilisation de la clé publique.

3) Sélectionner la clé puis cliquer sur Envoyer pour l'importer.

4) Cliquer sur pour visualiser la clé importé :



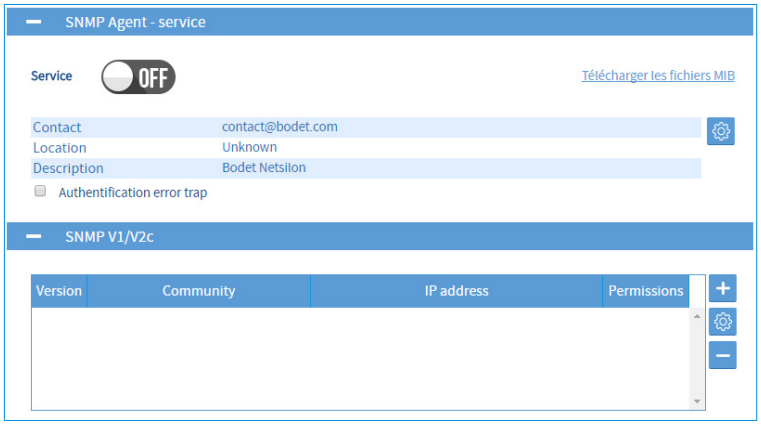
Le nombre de clés est limité à 20.

4.11 Supervision du système

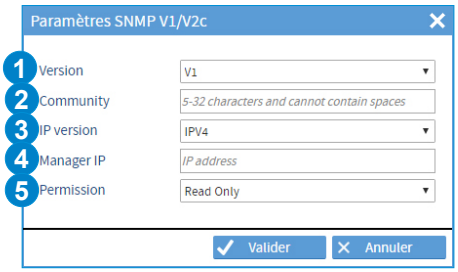
4.11.1. SNMP agent

› ACTIVER L'AGENT SNMP (EXEMPLE V1)

1) Menu SECURITE > Agent SNMP :



2) Cliquer sur +, la fenêtre suivante apparaît :



1 Sélection de la version SNMP.

2 Définir un nom de communauté compris entre 5 et 32 caractères sans espace.

3 Choisir la version de communication IP : IPV4.

4 Renseigner l'adresse IP du serveur.

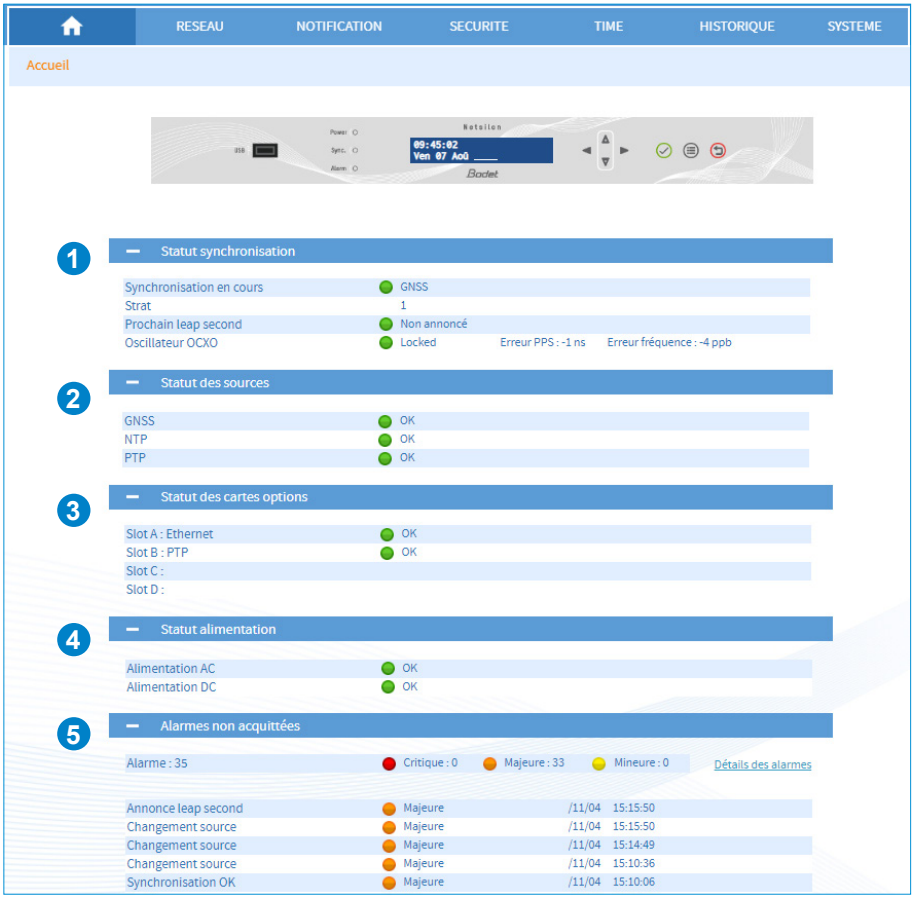
5 Choisir la permission : lecture uniquement ou lecture/écriture.

3) Activer le service à l'aide du bouton ON, puis enregistrer.

4.12 Suivi du système

4.12.1. Page d'accueil

La page d'accueil est une page de consultation :



1 Ce menu affiche l'état de la synchronisation en cours :

› L'état de la synchronisation en cours et la source de synchronisation utilisée :

› Vert = synchronisation OK,

› Rouge = pas de synchronisation.

› Le niveau de stratum : niveau par rapport à la source de synchronisation (satellite).

› Annonce du prochain leap second (seconde intercalaire / saut de seconde).

› Statut de l'oscillateur : Locked / Tracking / Holdover / Freerun.

2 Ce menu affiche l'état des sources de synchronisation :

› Le nom de la source et son état.

Cette liste est dynamique et dépend du nombre d'entrées existantes sur le produit.

3 Ce menu affiche le statut des sorties :

› Le nom de la sortie et son état.

Cette liste est dynamique et dépend du nombre de sorties existantes sur le produit.

4 Ce menu affiche l'état de l'alimentation :

› Le nom de l'alimentation (alimentation AC, alimentation DC, alimentation AC+DC, alimentation AC+AC) ainsi qu'une couleur pour l'état :

- Vert = alimentation OK.
- Rouge (cas en double alimentation) = erreur sur une des alimentations.

Cette liste est dynamique et dépend du nombre d'alimentations existantes sur le produit.

5 Ce menu affiche la liste des alarmes qui nécessitent un acquittement de l'utilisateur.

› Le lien permet de se rendre dans le détails des alarmes (Historique>Alarmes).

› Le nom de l'alarme, son état (majeure ou mineure), la date et l'heure UTC.

Cette liste est dynamique et dépend des alarmes remontées.

4.12.2. Statistiques GNSS

Pour visualiser les statistiques de synchronisation GNSS de Netsilon, suivre les étapes ci-dessous :

1) Menu HISTORIQUE > Statistiques GNSS.

2) Sélectionner la date à l'aide du menu déroulant :

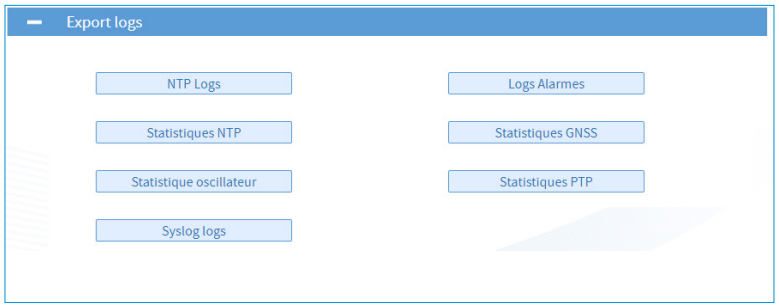
1 L'état de la réception GNSS est symbolisé par deux états :

- 0 : réception de trame GPS mais pas de synchronisation (délai d'attente pour vérification si la source est fiable).
- 1 : réception de trame GPS.

2 Graphique présentant le nombre de satellites détectés en fonction de l'heure. Trois couleurs indiquent la qualité de réception du signal :

- Rouge : 0 à 2 satellites - pas de réception ou qualité de réception faible.
- Orange : 2 à 4 satellites - qualité de réception moyenne.
- Vert : 4 à 12 et + satellites - qualité de réception bonne.

Ces statistiques peuvent être exportées, pour cela ouvrir «Export Logs» et cliquer sur Statistiques GNSS:

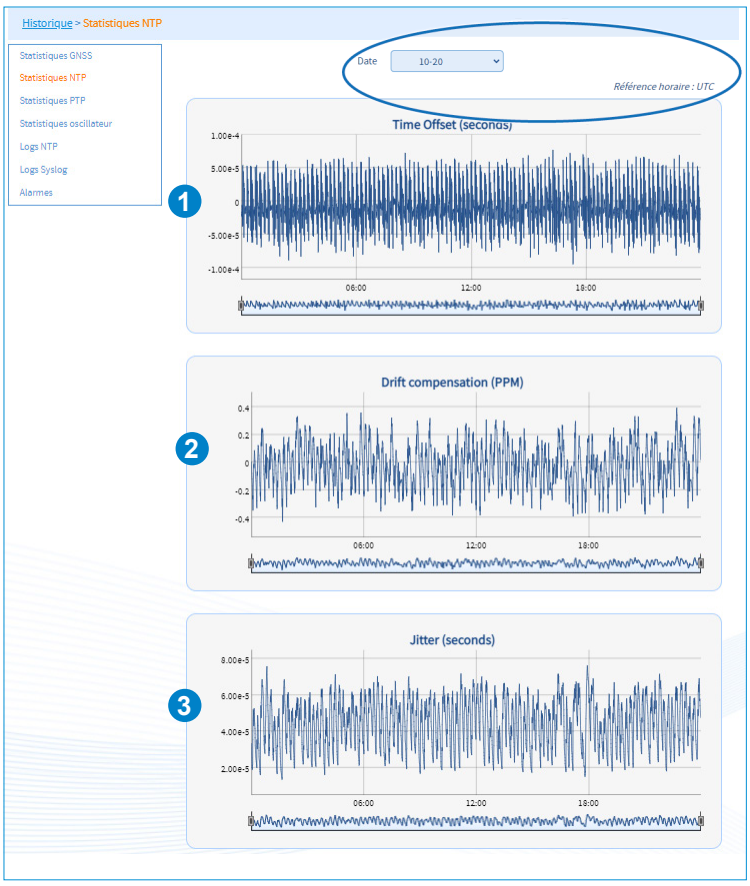


4.12.3. Statistiques NTP

Pour visualiser les statistiques de synchronisation NTP de Netsilon, suivre les étapes ci-dessous :

1) Menu HISTORIQUE > Statistiques NTP.

2) Sélectionner la date à l'aide du menu déroulant «Date»:



1 Time offset : décalage de temps par rapport à la source de synchronisation de référence.

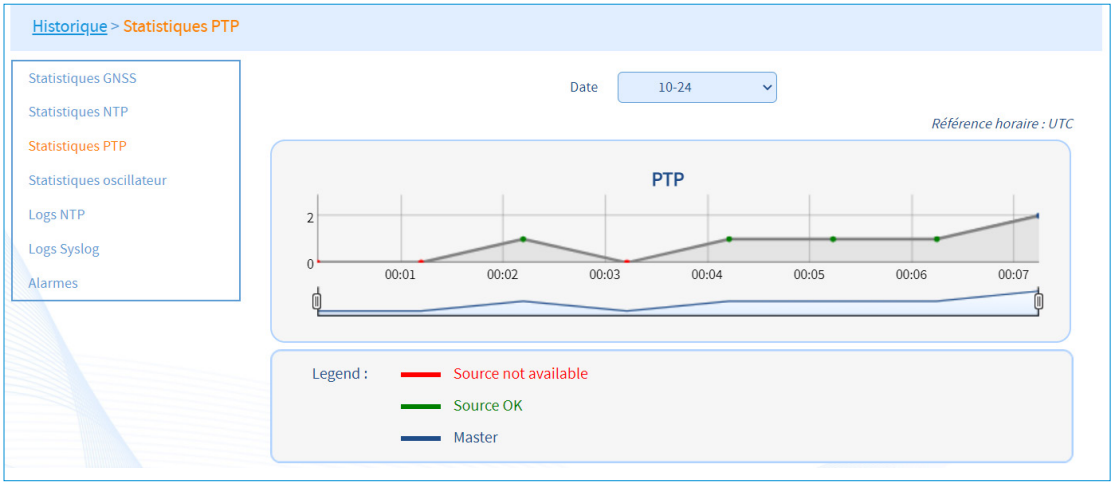
2 Drift compensation : correction progressive de l'oscillateur de Netsilon par rapport à la source. Il s'agit de se rapprocher de la source de synchronisation de manière progressive (sans effectuer de saut dans le temps).

3 Jitter : décalage de la source autour de la référence.

4.12.4. Statistiques PTP

Pour visualiser les statistiques PTP de Netsilon, suivre l'étape ci-dessous :

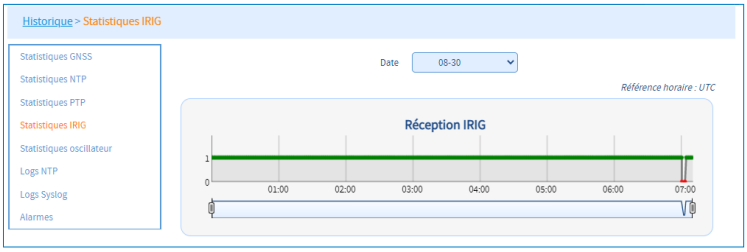
1) Menu HISTORIQUE > Statistiques PTP



4.12.5. Statistiques IRIG

Pour visualiser les statistiques de synchronisation IRIG de Netsilon, suivre l'étape ci-dessous :

1) Menu HISTORIQUE > Statistiques IRIG.



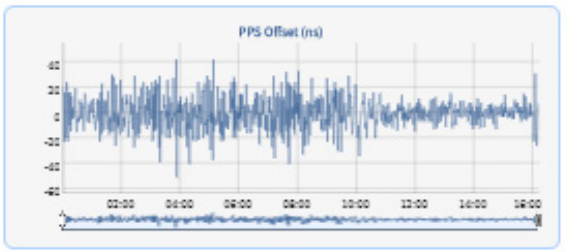
4.12.6. Statistiques Oscillateur

Pour visualiser les statistiques de l'oscillateur de Netsilon, suivre l'étape ci-dessous :

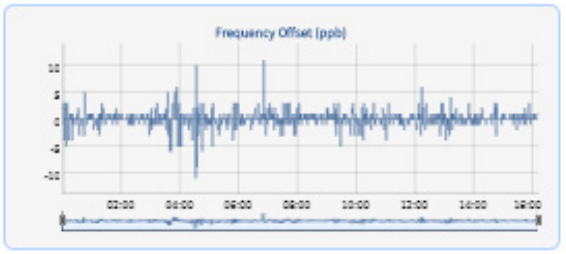
1) Menu HISTORIQUE > Statistiques Oscillateur

Au démarrage du produit, l'oscillateur est en Freerun (comme si n'ayant jamais été asservi), il recherche ensuite le signal PPS pour s'asservir et passe à l'état Tracking (poursuite du signal PPS). Ayant réussi à s'asservir sur le PPS, l'oscillateur se verrouille sur ce signal (état Locked). En cas de perte du signal PPS, il passe à l'état Holdover puis à l'état Freerun lorsque que sa base de temps n'est plus assez fiable.

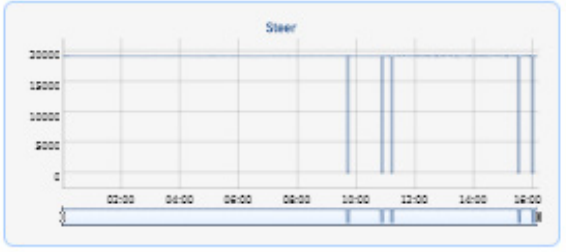
Erreur 1PPS en ns.
(PPS_Out par rapport au
1PPS de référence)



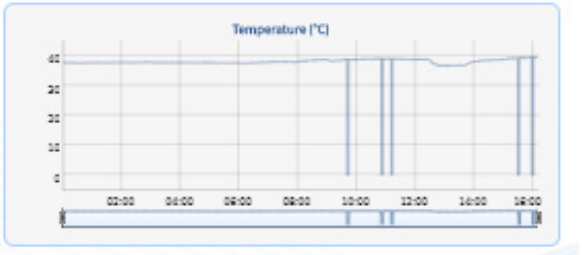
Erreur de fréquence
de l'oscillateur en ppb



Correction appliquée
à l'oscillateur

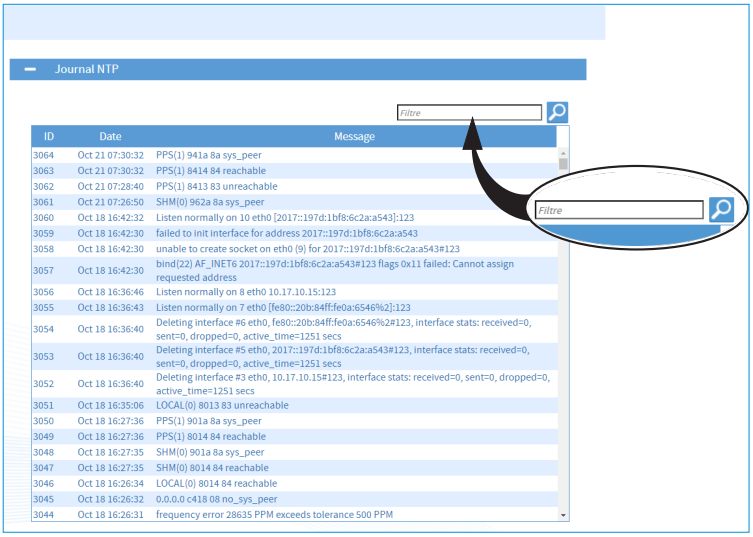


Température ambiante
de l'oscillateur



4.12.7. Journal NTP

Pour visualiser le journal des logs de Netsilon, suivre l'étape ci-dessous :
1) Menu HISTORIQUE > Logs NTP :

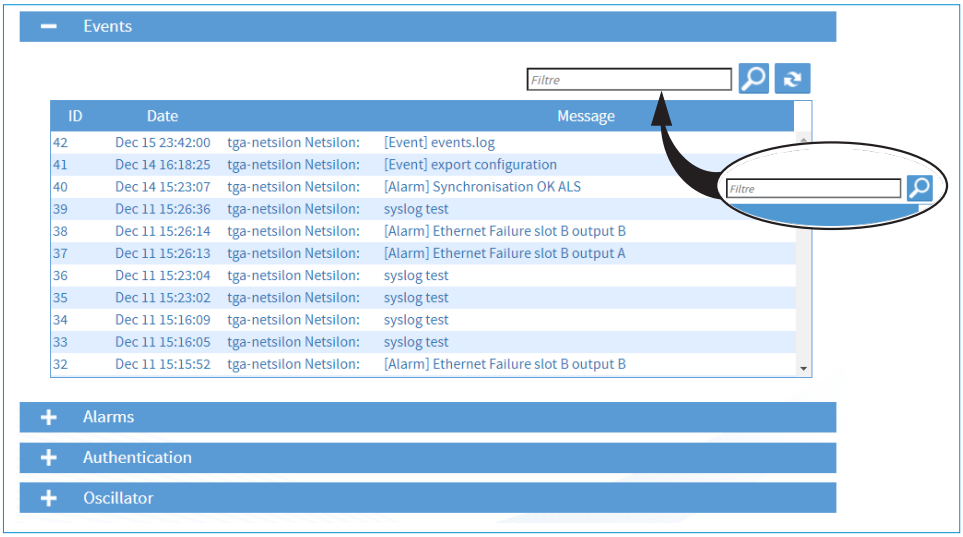


Ce journal est une remontée d'informations. C'est un journal standard généré par le protocole NTP.

Il est possible d'effectuer une recherche sur ce journal à l'aide de la barre de recherche.

4.12.8. Journal Syslog

Pour visualiser le journal Syslog, suivre l'étape ci-dessous :
1) Menu HISTORIQUE > Logs Syslog



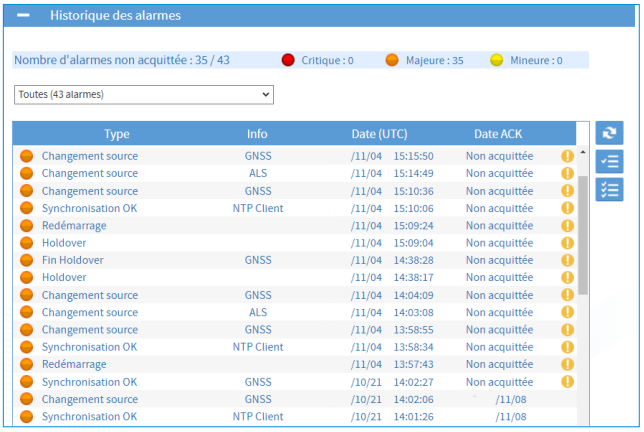
Ce journal est une remontée d'informations pour chaque type de log. C'est un journal standard généré par le protocole Syslog.

Il est possible d'effectuer une recherche sur ce journal à l'aide de la barre de recherche.

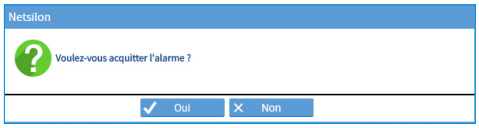
4.12.9. Historique des alarmes

Pour visualiser l'historique des alarmes et les acquitter, suivre les étapes ci-dessous :

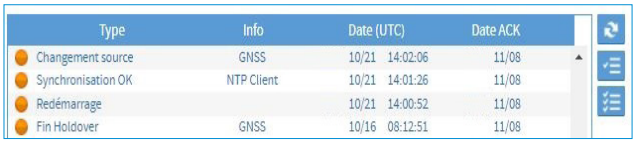
1) Menu HISTORIQUE > Alarmes :



- Pour rafraîchir cette liste, cliquer sur .
- Acquittement des alarmes : les alarme peuvent être acquittées de 2 manières
  - Individuellement en sélectionnant l'alarme à acquiter puis en cliquant sur .
  - Toutes les alarmes à la fois en cliquant sur .
- Puis confirmer en cliquant sur « Oui »



Une fois acquittée, le point d'exclamation disparait de la ligne de l'alarme concernée : :

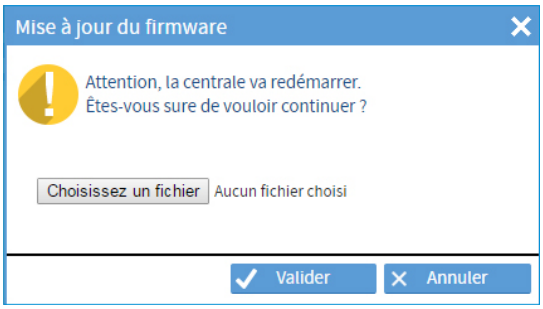


L'alarme Reboot est envoyée environ 10 secondes après le reboot pour laisser le temps à l'établissement du réseau.

4.13 Outils du système

4.13.1. Mise à jour du firmware

Pour mettre à jour le firmware de Netsilon, suivre les étapes ci-dessous :
1) Menu SYSTEME > Outils > Mise à jour et sauvegarde.
2) Cliquer sur Mise à jour du firmware, la fenêtre suivante apparaît pour choisir le fichier à importer :

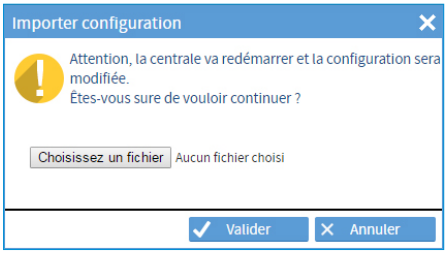


La dernière version du firmware est disponible sur www.bodet-time.com

4.13.2. Charger et sauvegarder configuration

Pour sauvegarder une configuration, suivre les étapes ci-dessous :
1) Menu SYSTEME > Outils > Mise à jour et sauvegarde.
2) Cliquer sur Sauvegarder la configuration, un fichier nommé «export.nets» se télécharge sur le PC.

Pour charger une configuration, suivre les étapes ci-dessous :
1) Menu SYSTEME > Outils > Mise à jour et sauvegarde.
2) Cliquer sur Charger une configuration, la fenêtre suivante apparaît pour choisir le fichier à importer :



Le fichier à importer doit avoir pour extension «NomFichier.nets»

Pourquoi sauvegarder une configuration ?
L'export d'une configuration permet de sauvegarder les différents paramètres définis dans Netsilon.

Lors d'une éventuelle reconfiguration de Netsilon, il suffira simplement d'importer le fichier sauvegardé pour retrouver l'ensemble des paramètres configurés précédemment.

Sauvegarder une configuration permet de gagner un temps précieux lors de la restauration du système.

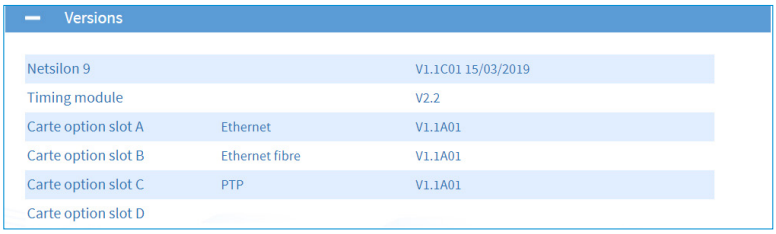
En ayant sauvegardé au préalable la configuration de Netsilon, il n'est plus nécessaire de le configurer manuellement et suivre les étapes pour obtenir la même configuration.

Afin de visualiser les paramètres sauvegardés, se reporter à l'annexe 4 : paramètres sauvegardés.

4.13.3. Version firmware et aide en ligne

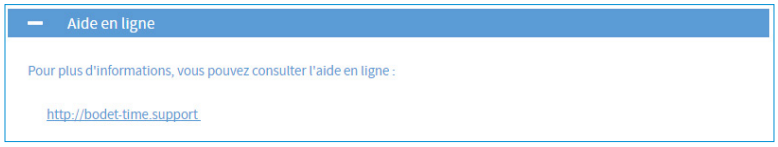
Pour visualiser la version du firmware de Netsilon et des cartes options, suivre l'étape ci-dessous :

1) Menu SYSTEME > Général > Versions :



Pour accéder à la notice du produit, suivre l'étape ci-dessous :

1) Menu SYSTEME > Général > Aide en ligne :



4.13.4. Firewall

Netsilon embarque un Firewall dont la configuration change automatiquement en fonction des services validés par le client. Il n'y a donc pas de paramétrage au niveau client.

Seuls les ports correspondants aux services activés sont ouverts.

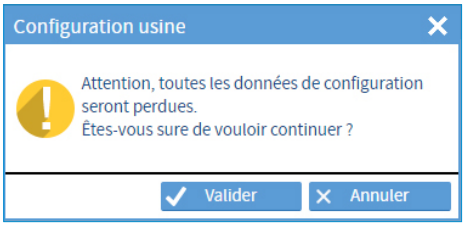
Les pings sont autorisés mais limités pour contrer les attaques de type « ICMP flood » (saturation de requêtes). Les connexions SSH sont autorisées (si activées) mais limitées pour contrer les attaques de type « brute force » (test de toutes les combinaisons possibles de mots de passe).

4.13.5. Configuration usine

Pour effectuer un retour en configuration usine de Netsilon, suivre les étapes ci-dessous :

1) Menu SYSTEME > Outils > Mise à jour et sauvegarde.

2) Cliquer sur Configuration usine, la fenêtre suivante apparaît :



Toutes les configurations seront perdues dans le cas d'un retour en configuration usine.

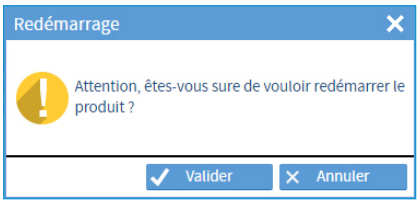
Le lien au serveur web sera rompu car l'adresse IP est perdue : il est nécessaire de re-configurer les paramètres réseaux pour accéder au serveur web (se reporter au chapitre **3. Mise en service** et effectuer les opérations indiquées).

4.13.6. Redémarrer ou éteindre Netsilon

Pour redémarrer Netsilon, suivre les étapes ci-dessous :

1) Menu SYSTEME > Outils > Redémarrer.

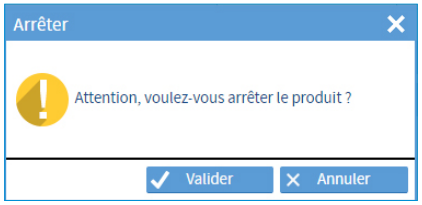
2) Cliquer sur Redémarrer, la fenêtre ci-contre apparaît :



Pour éteindre Netsilon, suivre les étapes ci-dessous :

1) Menu SYSTEME > Outils > Éteindre.

2) Cliquer sur Eteindre, la fenêtre ci-contre apparaît :

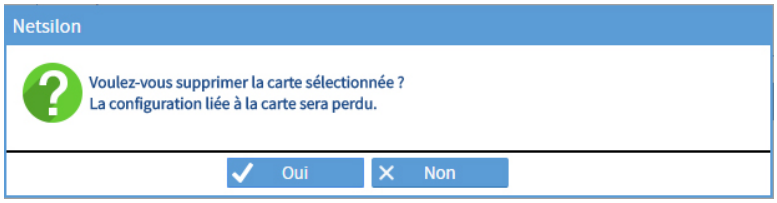


Le produit est éteint mais l'alimentation n'est pas coupée : présence de la LED verte POWER et l'écran LCD reste en mode veille.

4.13.7. Supprimer une carte option

Dans le cas où une carte option est supprimée physiquement de Netsilon, il est nécessaire de supprimer cette dernière du serveur web afin de ne pas générer d'alarmes intempestives.

Pour supprimer logiciellement une carte option de Netsilon, suivre les étapes ci-dessous :
1) Menu SYSTEME > Outils > Cartes options.
2) Sélectionner la carte option à supprimer.
3) Cliquer sur , la fenêtre suivante apparaît :



Dans le cas où cette suppression est effectuée alors que la carte option est toujours présente, celle-ci sera redétectée lorsque l'utilisateur reviendra dans ce menu.

4.13.8. Exporter les logs et statistiques

Pour exporter les logs et les statistiques de Netsilon, suivre les étapes ci-dessous :
1) Menu SYSTEME > Outils > Export logs.
2) Cliquer sur le log ou le type de statistiques désirés, un dossier ZIP contenant le fichier de logs se télécharge sur le PC.

5. CONFIGURATION PAR SSH

› Pour accéder à l'interface de jeu de commandes en ligne SSH, respecter les étapes suivantes (Netsilon, depuis son port Eth0, doit être raccordé au réseau) : :

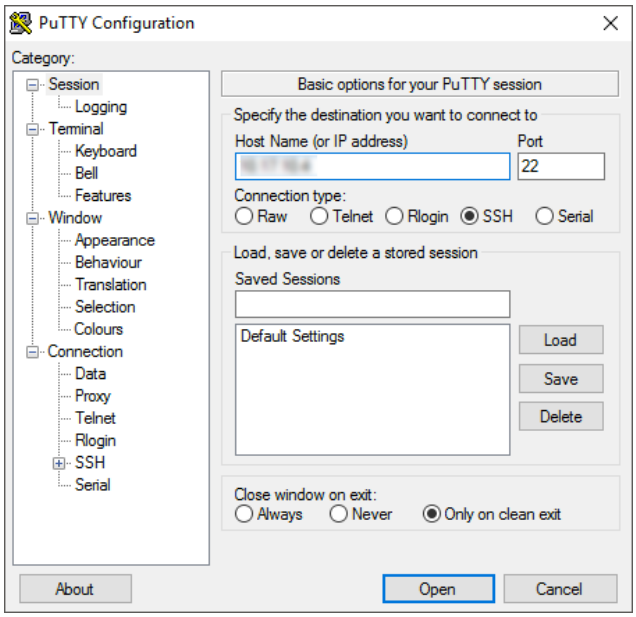
5.1 Authentification par mot de passe

1) Télécharger un programme permettant de se connecter à distance à Netsilon (ex.: PuTTY).

2) Se munir de l'adresse IP de Netsilon.

3) Ouvrir le programme (PuTTY).

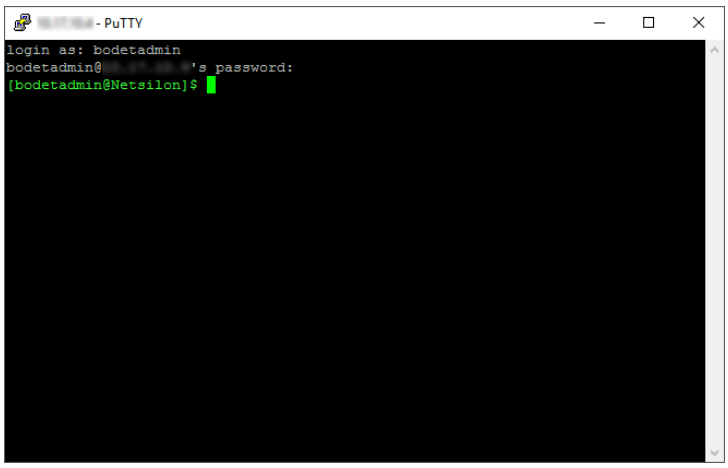
4) Renseigner l'adresse IP.



5) Renseigner l'identifiant et le mot de passe par défaut pour accéder au jeu de commandes. Pour rappel :

› Identifiant : bodetadmin

› Mot de passe : admin49



› Pour plus d'informations sur le produit et la liste des commandes en ligne (depuis le port Eth0): SYSTEME > Général > Aide en ligne

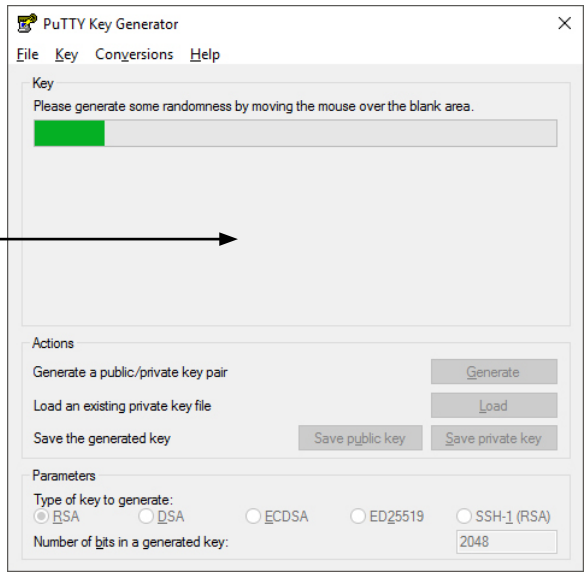
Afin d'accéder à la liste des jeux de commandes, se reporter à l'annexe 5 : liste des jeux de commandes

5.2 Authentification par clé publique

1) Télécharger un programme permettant de générer des clés privées/publiques (ex. : PuTTY Key Generator).

2) Générer une clé privée/public en cliquant sur Generate :

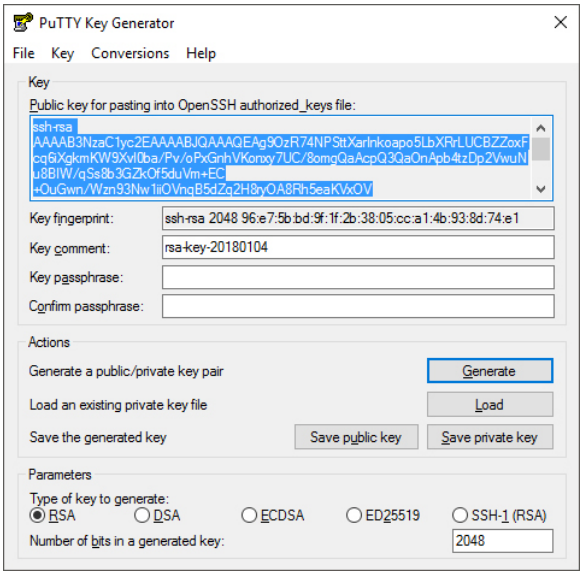
Bouger la souris de votre PC sur cet espace afin de générer la clé



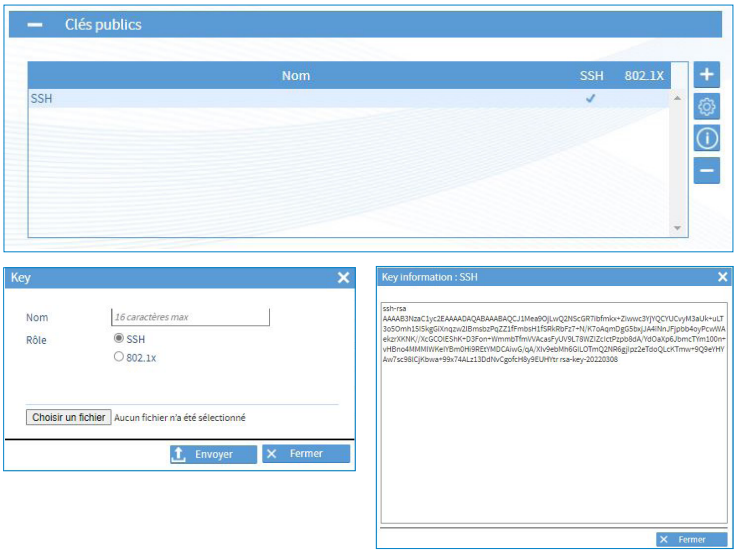
3) Enregistrer la clé publique dans un fichier (type .txt) à importer dans le pool Certificats et clés de Netsilon dans l'onglet "public keys" :

La clé publique doit démarrer par "SSH-" et commencer sur la première ligne du fichier.
Le fichier ne doit contenir que la clé publique.

Copier la clé du générateur PuTTY dans un fichier



Importer la clé publique dans Netsilon

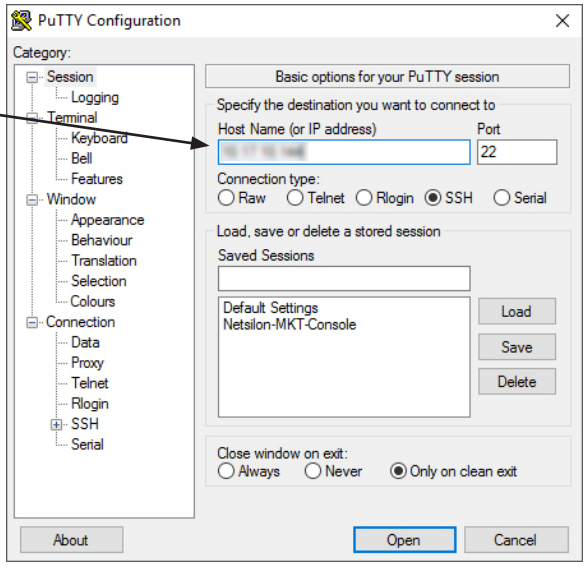


4) Sauvegarder la clé privée dans un emplacement de votre PC.

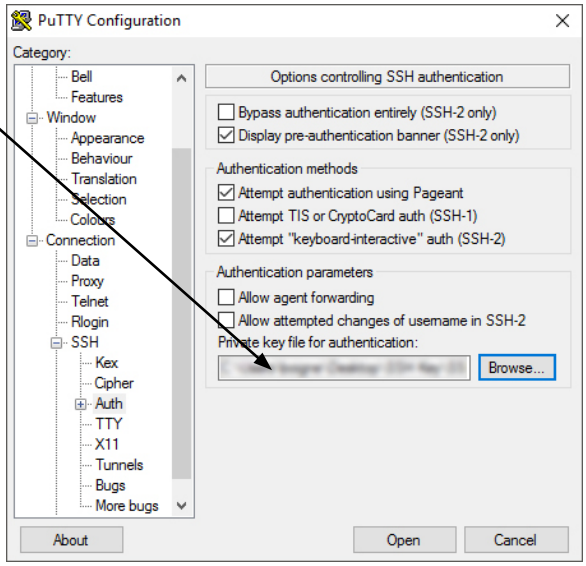
5) Télécharger un programme permettant la connexion (ex.: PuTTY).

6) Ouvrir le programme (PuTTY).

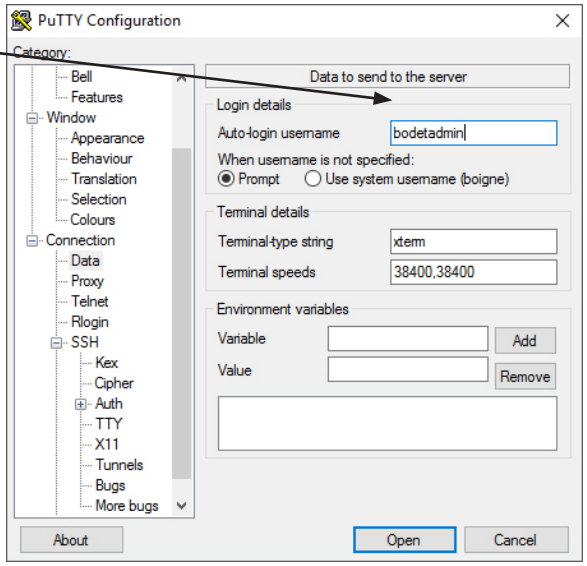
7) Renseigner l'adresse IP de Netsilon :



8) Renseigner l'emplacement PC contenant la clé privée correspondante à la clé publique importée dans Netsilon :



9) Renseigner le «user» :



10) Cliquer sur Open la fenêtre ci- dessous s'ouvre :

6. CONFIGURATION PAR CONSOLE

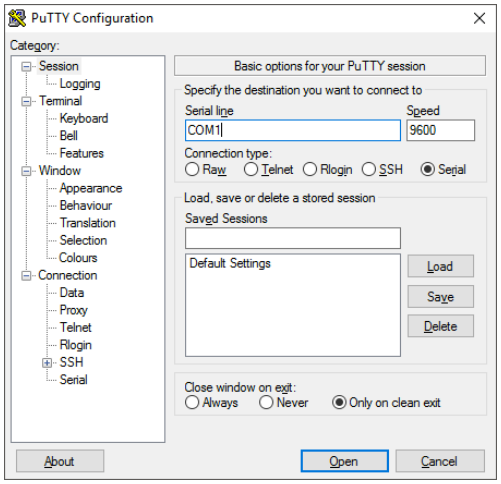
› Pour accéder au serveur web de Netsilon, respecter les étapes suivantes (Netsilon, depuis son port série COM, doit être raccordé au PC).

La liaison physique entre le PC et Netsilon doit être assurée par un câble série mâle/femelle RS232 (DB9) en liaison directe.

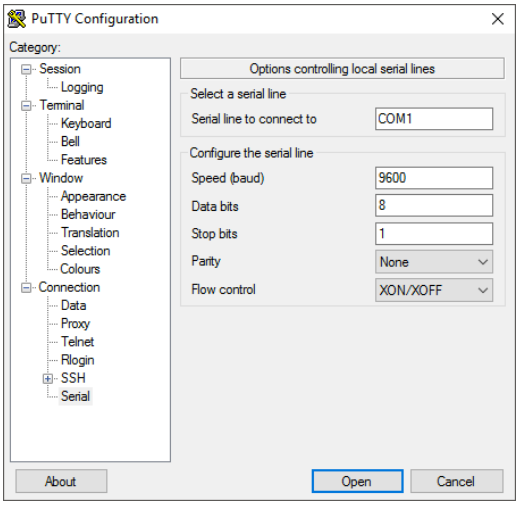
1) Télécharger un programme permettant de se connecter à Netsilon (ex.: PuTTY).

2) Ouvrir le programme (PuTTY).

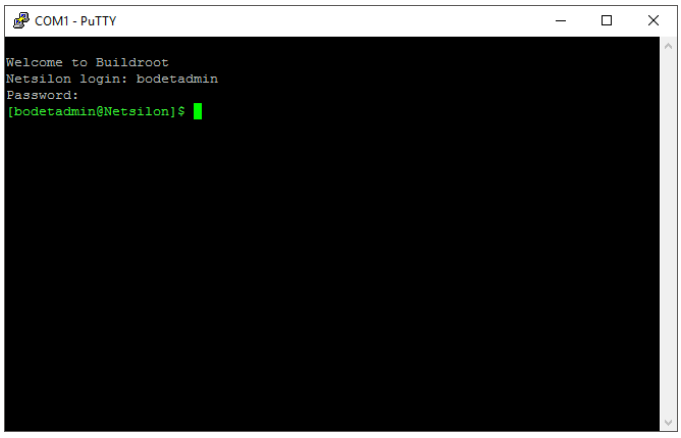
3) Renseigner le port de communication.



4) Cliquer sur «Serial» afin de contrôler les paramètres de la liaison série ASCII RS-232 :
- 9600 baud, 1 bit de start, 8 bits de donnée, 1 bit de stop, pas de parité et Loggin root interdit.



5) Renseigner l'identifiant et le mot de passe par défaut pour accéder au jeu de commandes. Pour rappel :
› Identifiant : bodetadmin
› Mot de passe : admin49



› Pour plus d'informations sur le produit et la liste des commandes en ligne (depuis le port COM): SYSTEME > Général > Aide en ligne

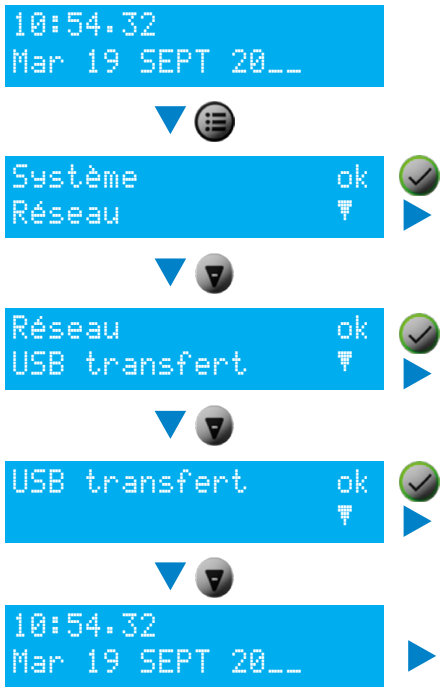
Afin d'accéder à la liste des jeux de commandes, se reporter à l'annexe 5 : liste des jeux de commandes.

7. CONFIGURATION PAR CLAVIER DE COMMANDE

7.1 Arborescence du menu général

La configuration des menus à partir du clavier de commande permet un paramétrage basique.
Le paramétrage avancé est effectué depuis le serveur web.

Sortie automatique d'un menu après 45 secondes d'inactivité sur le clavier de commande.



Se reporter au chapitre **7.1.1 Menu Système**

Se reporter au chapitre **7.1.2 Menu Réseau**

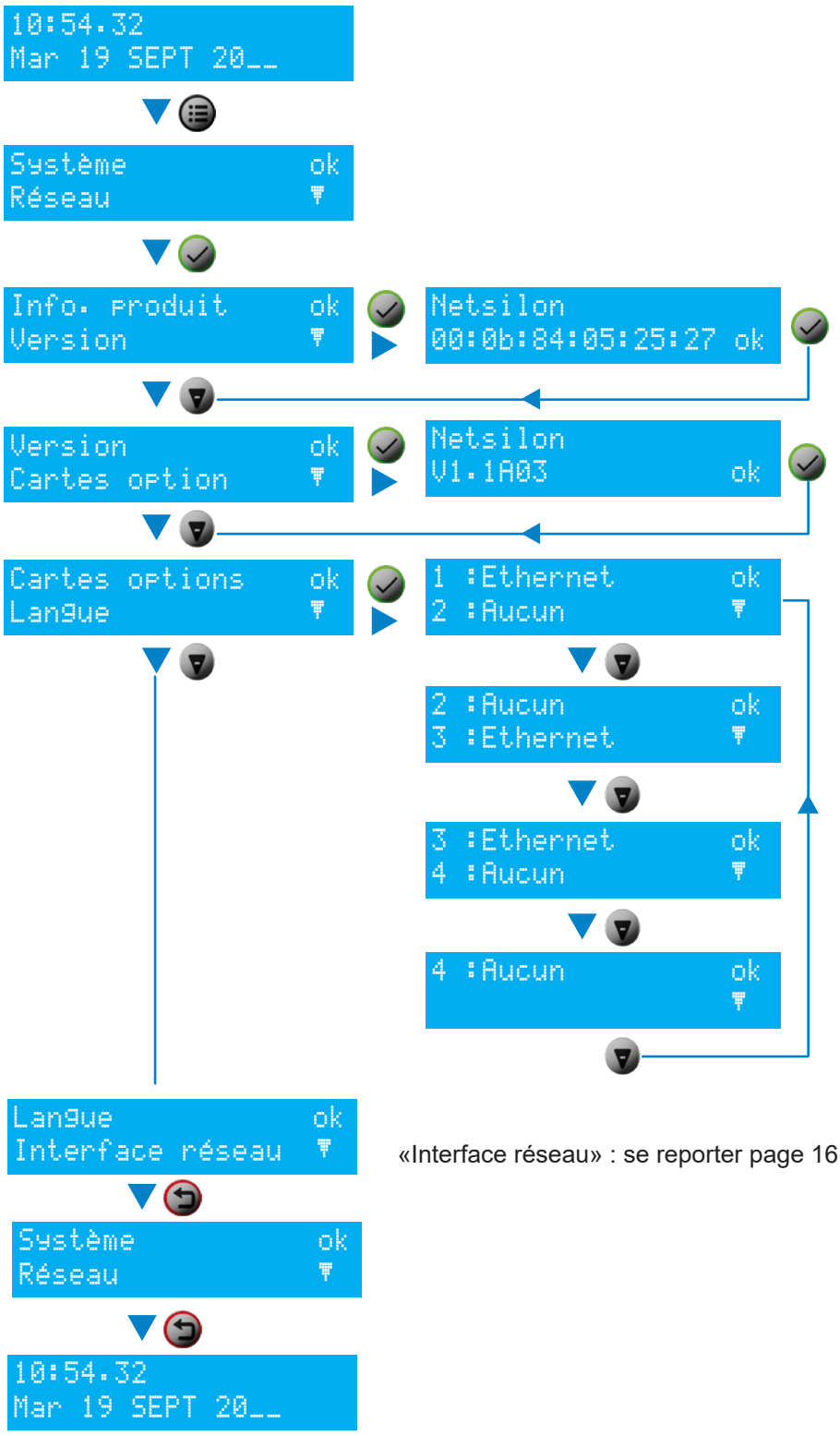
Se reporter au chapitre **7.1.3 Menu USB transfert**

Retour à l'écran principal

7.1.1. Menu Système

Ce menu permet de visualiser les paramètres suivants :

- adresse MAC du produit,
- le nom du produit et sa version firmware,
- la ou les cartes options installées,
- la langue utilisée pour les menus affichés sur l'écran LCD.



Visualisation du nom du produit ainsi que de son adresse MAC

Visualisation du nom du produit ainsi que sa version logicielle

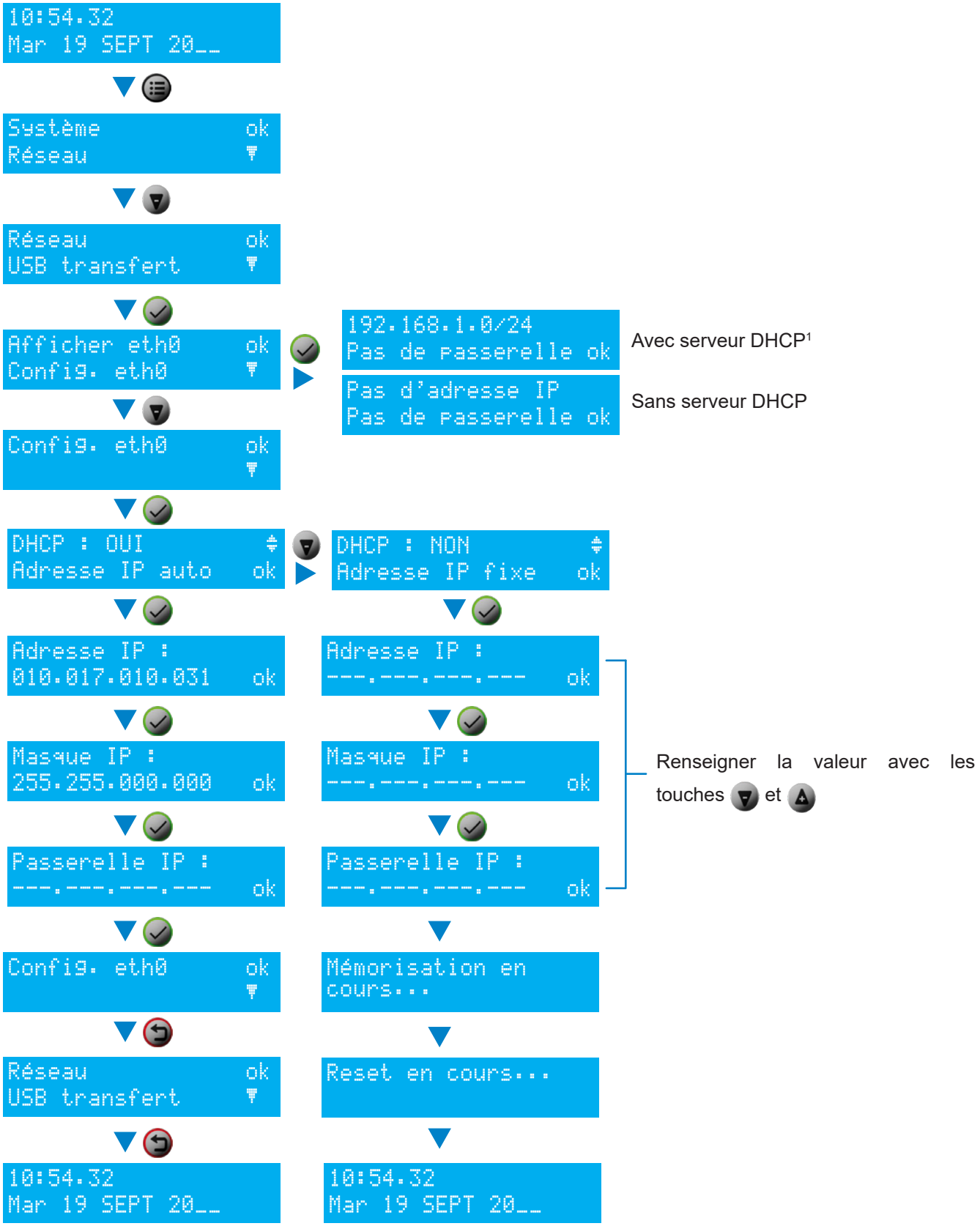
Visualisation des cartes options installées.

Netsilon peut accueillir jusqu'à 4 cartes options.

«Interface réseau» : se reporter page 16.

7.1.2. *Menu Réseau*

Ce menu permet de visualiser, définir et configurer les paramètres du port réseau ETH0 uniquement .

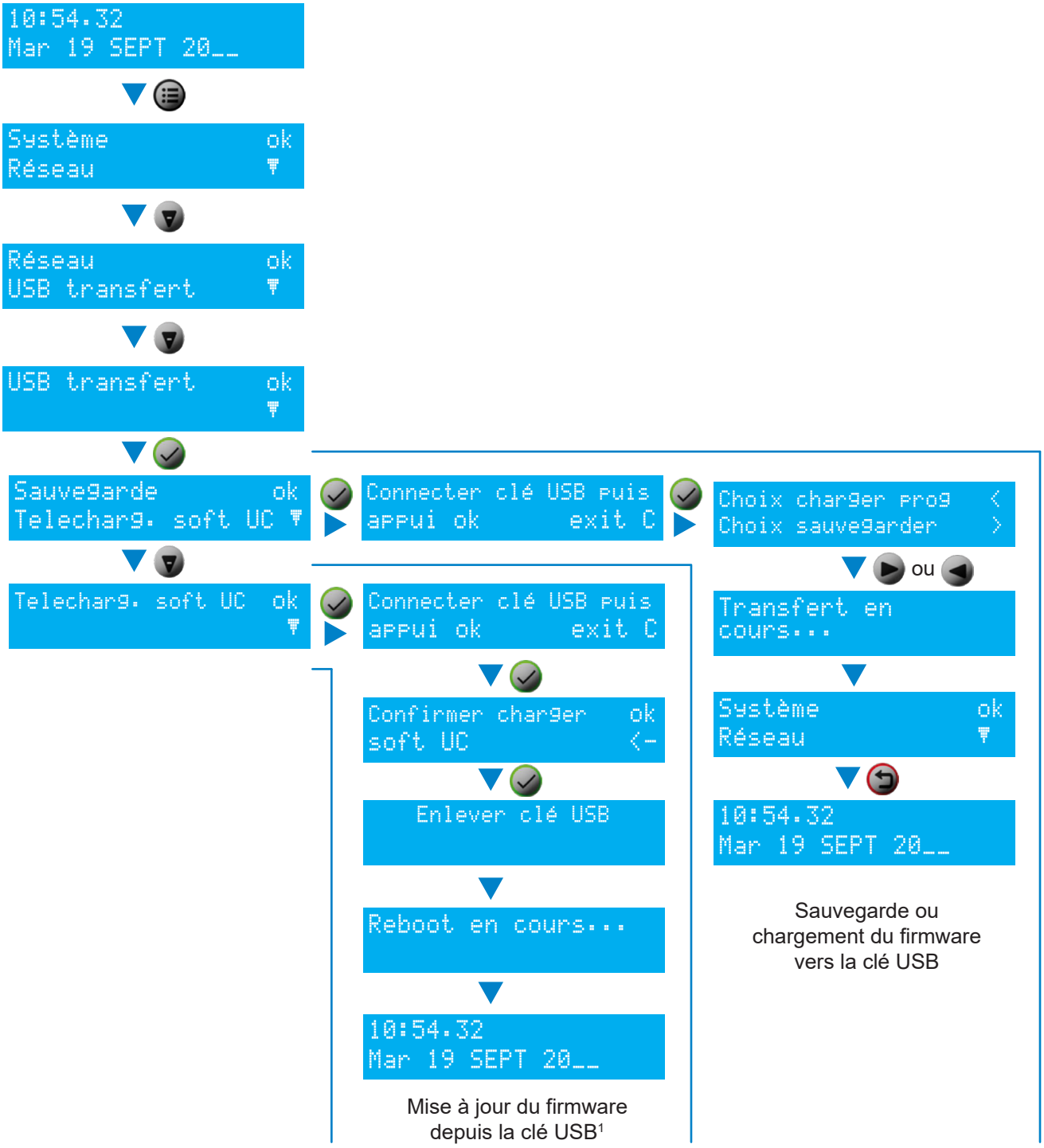


[1] *L'adresse IP 192.168.1.0/24 et l'absence de passerelle sont données à titre d'exemple. Rappel : /24 est l'adressage CIDR.*

7.1.3. *Menu USB transfert*

Le serveur de temps Netsilon peut charger ou sauvegarder sa programmation par l'intermédiaire d'une clé USB.

Avant de créer une nouvelle programmation, il est nécessaire de sauvegarder l'existante sur une clé USB.



[1] *Après le chargement du firmware vers la clé USB, Netsilon redémarre.*

7.2 Menu technicien

Ce menu est accessible uniquement avec un code technicien. Ce code journalier est détenu par la société BODET.

Pour obtenir ce code contacter l'assistance clientèle BODET et munissez-vous de l'adresse MAC[1] de la sortie réseau ETH0.

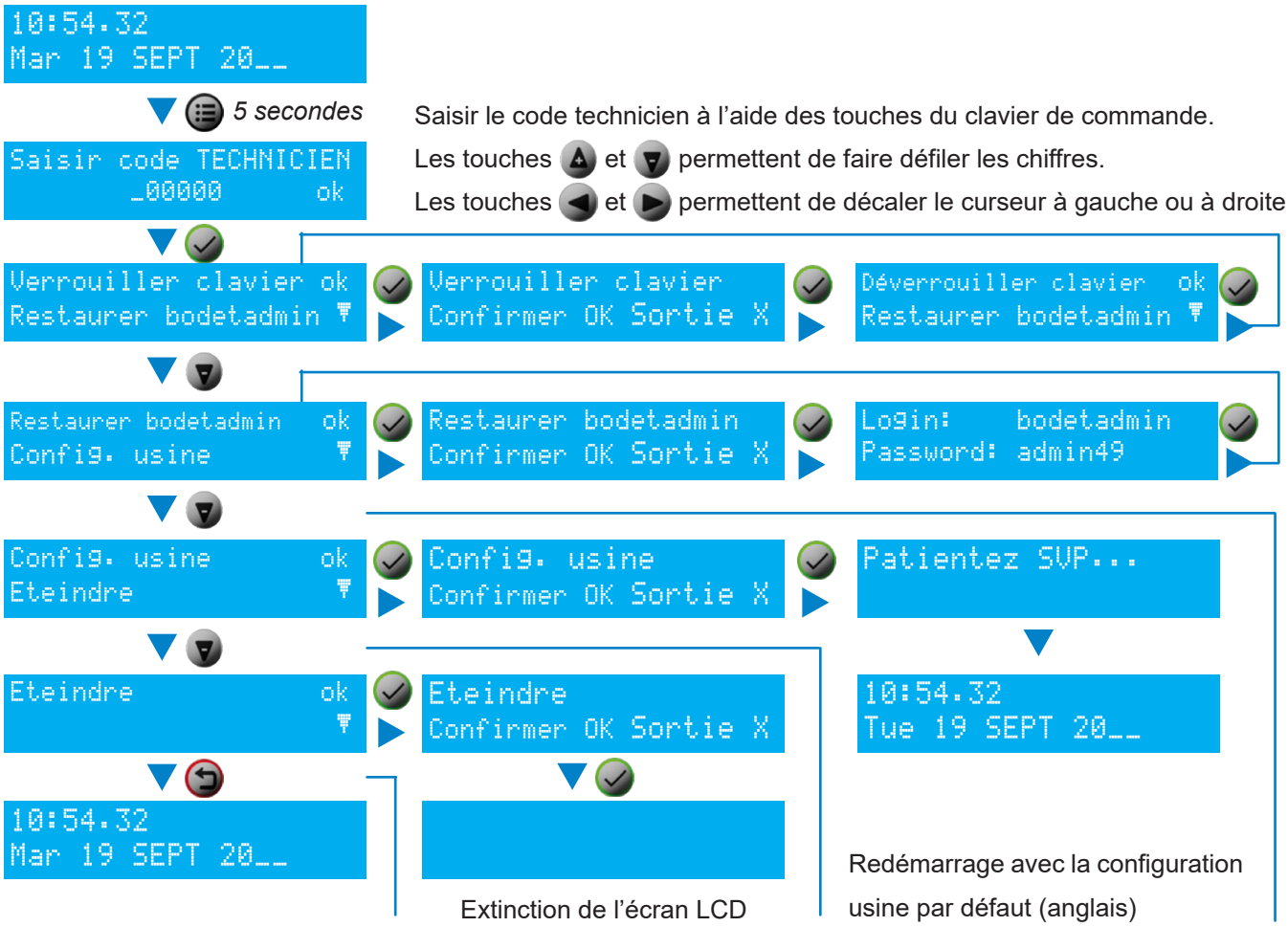
Dans ce menu, il est possible de :

- verrouiller ou déverrouiller le clavier de commande,
- restaurer le compte administrateur par défaut,
- effectuer une remise en configuration usine,

ATTENTION : cette action supprime l'intégralité du paramétrage y compris les comptes utilisateurs créés.

- éteindre Netsilon.

Pour accéder au menu technicien, appuyer sur pendant 5 secondes puis renseigner le code technicien.



[1] *L'adresse MAC de la sortie réseau ETH0 est indiquée sur une étiquette collée à l'arrière de Netsilon.*

8. ASSISTANCE

8.1 Etat des LEDs sur la façade

Les LEDs peuvent fournir des informations sur l'état Netsilon.

LED	Etat et couleur	Description	Vérifier que...
Power	Eteinte	Pas d'alimentation	1) Le câble d'alimentation secteur (AC) est connecté sur le connecteur de Netsilon et que l'interrupteur d'alimentation est à ON. 2) Les fils d'alimentation continue (DC) sont branchés sur connecteur.
	Verte fixe	Alimentation OK	-
	Rouge	Défaut sur l'alimentation	1) Dans les versions double alimentations (AC+DC, AC+AC), les deux alimentations sont correctement câblées.
Sync.	Eteinte	Pas de synchronisation en entrée	1) L'entrée de synchronisation prioritaire est disponible (ex.: si source synchronisation GNSS, vérifier que Netsilon est connectée à cette antenne).
	Verte fixe	Synchronisation OK	-
	Rouge	Synchronisation perdue Fonctionnement holdover	1) L'entrée de synchronisation prioritaire est disponible (ex.: si source synchronisation GNSS, vérifier que Netsilon est connectée à cette antenne). 2) L'installation de l'antenne GNSS est opérationnelle (le cas échéant).
	Rouge clignotante	Synchronisation perdue Holdover dépassé / freerun	**Remarque :** Si Netsilon vient d'être redémarré, aucun dépannage n'est nécessaire. Attendre quelques minutes pour que la synchronisation soit détectée. 1) L'entrée de synchronisation prioritaire est disponible (ex.: si source synchronisation GNSS, vérifier que Netsilon est connectée à cette antenne). 2) L'installation de l'antenne GNSS est opérationnelle (le cas échéant).
Alarm	Eteinte	Pas d'alarme	-
	Rouge clignotante	Alarme critique	**Remarque :** Si Netsilon vient d'être redémarré, aucun dépannage n'est nécessaire. Attendre quelques minutes pour que la synchronisation soit détectée. 1) Lorsque la synchronisation est perdue et que le Holdover est expiré, vérifier que l'entrée de synchronisation prioritaire est disponible (ex.: si source synchronisation GNSS, vérifier que Netsilon est connectée à cette antenne).

8.2 Impossibilité d'ouvrir le navigateur web

› Avec serveur DHCP

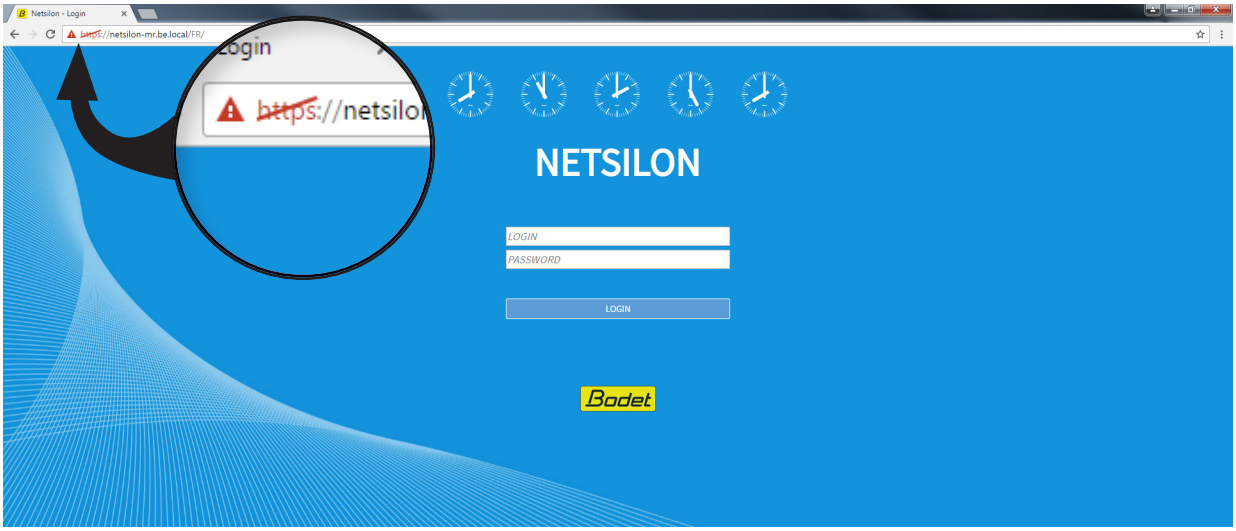
Vérifier que le serveur DHCP délivre l'adresse IP : affichage de l'adresse IP sur l'écran LCD de Netsilon (se reporter au chapitre **3.4 Configuration avec serveur DHCP**)

› Sans serveur DHCP : adresse IP fixe

Vérifier que les paramètres réseaux sont corrects : adresse IP disponible, masque de sous réseau, passerelle...(se reporter au chapitre **3.5 Configuration sans serveur DHCP**)

› HTTP/HTTPS

Dans le cas d'utilisation du DNS :
HTTP : en saisissant le nom de domaine, la page d'accueil s'ouvre.
HTTPS : en saisissant le nom de domaine, la page d'accueil s'ouvre. En revanche, la connexion n'est pas sécurisée et identifiée avec la présence ci-dessous :



Il est possible de forcer la connexion : se reporter au chapitre **HTTPS**

› Activer les cookies

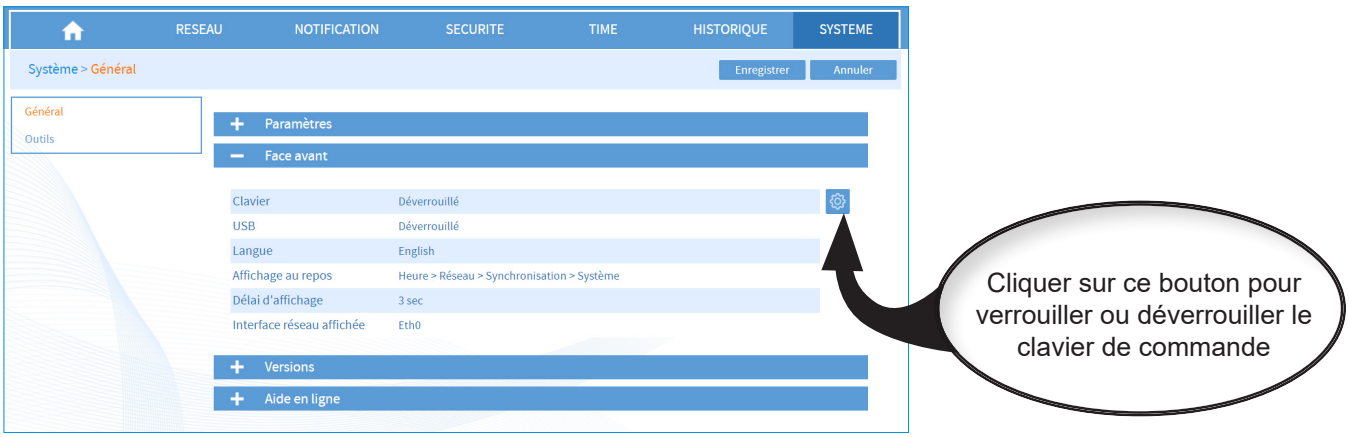
L'activation des cookies est obligatoire pour accéder au serveur web de Netsilon.

8.3 Clavier de commande inactif

Le clavier de commande sur la façade de Netsilon peut être verrouillé afin d'empêcher toute mauvaise manipulation d'une tierce personne.
Une fois verrouillé, le fonctionnement du clavier est désactivé jusqu'à ce qu'il soit déverrouillé en utilisant l'une des deux méthodes suivantes:

› Depuis le menu technicien : se reporter au chapitre **7.2. Menu technicien.**

› Depuis le serveur web : Menu Système > Général > Face avant :



8.4 Synchronisation des informations

Afin de paramétrer Netsilon depuis le serveur web, plusieurs paramètres doivent être respectés :

- Le PC doit être sur le même réseau que Netsilon. S'assurer qu'un navigateur web est installé sur le PC (Google Chrome®, Mozilla Firefox, Microsoft Edge ou Internet Explorer®). Si le PC ne peut pas accéder au serveur web, un problème réseau existe. Vérifier la configuration au réseau.
- Le niveau de synchronisation de la source NTP doit être inférieur à Stratum 15. Dans le cas contraire Netsilon doit être synchronisé à une source de référence plus précise ou fonctionner en mode holdover. Vérifier le niveau de synchronisation NTP.

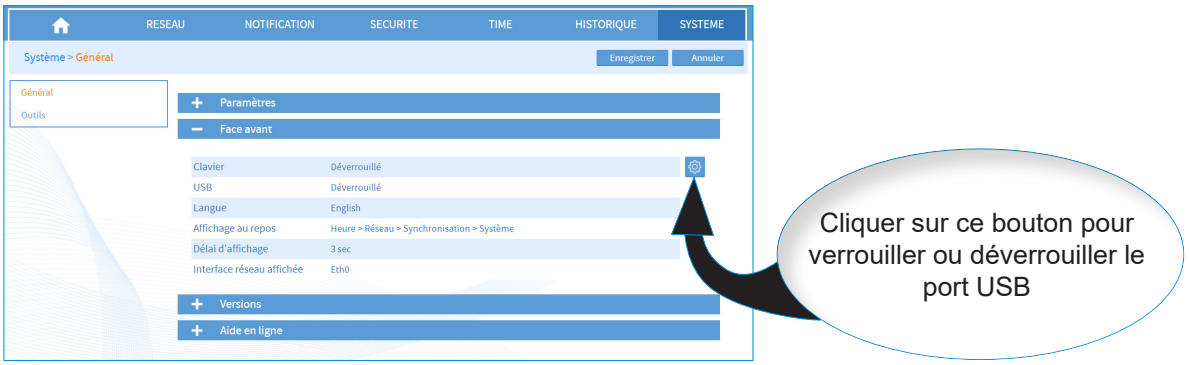
Si le problème persiste, contacter le support technique BODET.

8.5 Chargement USB

Si la clé USB n'est pas détecté sur le port USB, vérifier que :

- Le port USB n'est pas verrouillé.

Depuis le serveur web : Menu Système > Général > Face avant :



- Le format (système de fichiers) de la clé USB est FAT16/FAT32 ou NTFS.

8.6 Support technique BODET

Pour demander une assistance technique pour cet équipement :

1) Aller à la page «Support» du site internet www.bodet-time.com :
Cliquer sur le lien : http://www.bodet-time.com/assistance-clientele.html

2) Renseigner la page de contact.

L'assistance téléphonique est disponible du lundi au vendredi de 8h à 12h et de 13h30 à 17h.

Pour accélérer le diagnostic de votre Netsilon, effectuer une sauvegarde du système et noter l'adresse MAC de Netsilon.

8.7 Historique des mises à jour de la notice

Indice	Description de la mise à jour	Date
A	Création	Sep - 20
B	Notice adaptée pour Netsilon 11	Nov - 20
C	Ajout version AC+AC Conformité électrique (DBT) Ajout des limitations et d'informations diverses (firewall...).	Fev - 21
D	Ajout LDAP / RADIUS / Syslog / informations PTP	Mai - 21
E	Ajout : IRIG IN/OUT, Leap Second manuel, Offset TAI/UTC / màj paramètres de synchronisation	Jan - 22
F	Ajout : 802.1x / VLAN / Bonding / HTTPS / Pool certificats et clés	Jui - 22
G	Limites routes statiques / Antenne GNSS Sécurisée	Jui - 23
H	Intégration AuthNoPriv / NoAuthNoPriv - Protocole SNMP v3	Fev - 24
I	Intégration carte ASCII - Asservissement OCXO via NTP	Jui - 24
J	Mise à jour des trames ASCII	Avril - 25

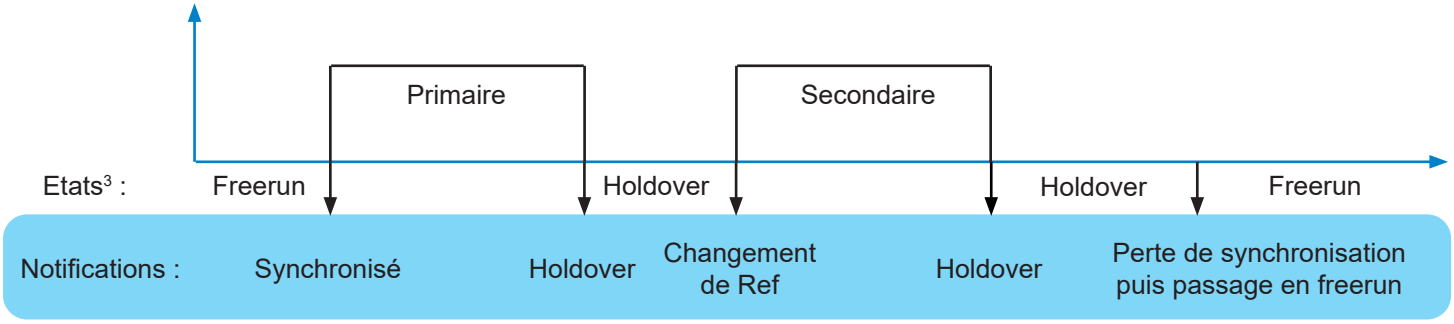
9. ANNEXES

9.1 Annexe 1 : synchronisation

9.1.1. Avec paramétrage source primaire / source secondaire

Scénario 1 : perte de la synchronisation des sources primaire puis secondaire

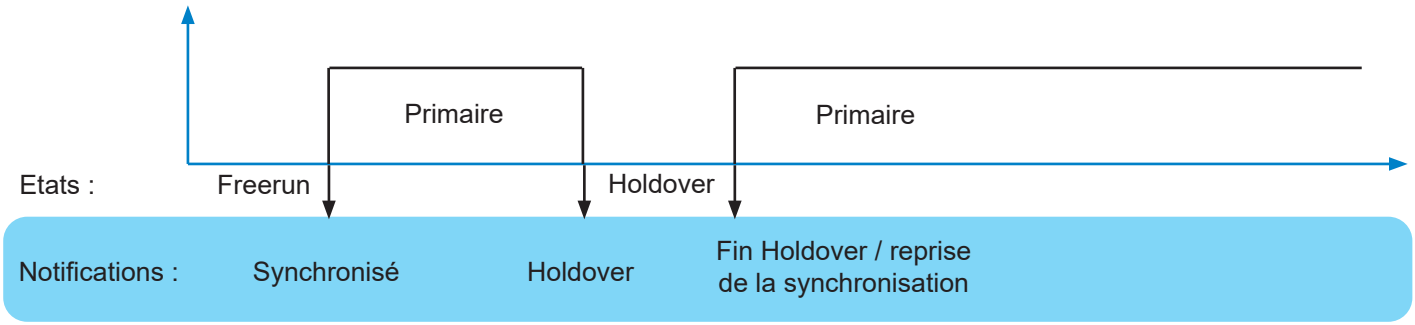
- Freerun[1] au démarrage du produit
- Synchronisation sur la source primaire (ex.: GNSS)
- Perte de la synchronisation de la source primaire
- Holdover[2]
- Synchronisation sur la source secondaire (ex. NTP)
- Perte de la synchronisation de la source secondaire
- Holdover
- Pas de synchronisation détectée
- Freerun



En **freerun** on ne garantit pas le précision de la base de temps

Scénario 2 : resynchronisation sur la source primaire après perte momentanée de la source primaire

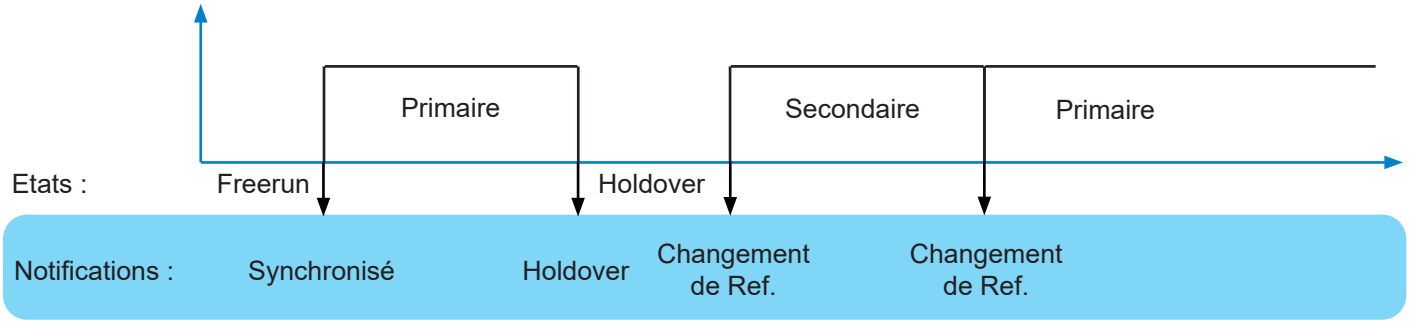
- Freerun au démarrage du produit
- Synchronisation sur la source primaire (ex.: GNSS)
- Perte de la synchronisation de la source primaire
- Holdover
- Re-synchronisation sur la source primaire



[1] Il s'agit d'un état où Netsilon peut distribuer un signal horaire sans aucune garantie concernant sa précision. La précision de la base de temps n'est plus garantie.
[2] Rappel : la durée en mode holdover est paramétrable dans le serveur web.
[3] Ces états sont affichés sur l'écran LCD de Netsilon.

Scénario 3 : rétablissement de la source primaire

- Freerun au démarrage du produit
- Synchronisation sur la source primaire (ex.: GNSS)
- Perte de la synchronisation de la source primaire
- Holdover
- Synchronisation sur la source secondaire (ex. NTP)
- Passage sur la source de synchronisation primaire.

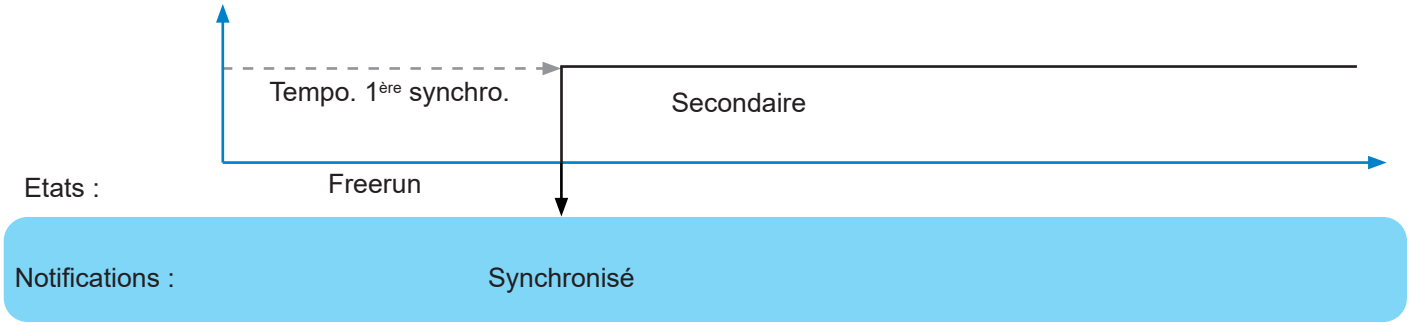


Pas de notification de changement de Ref si passage d'un serveur NTP à un autre.

Scénario 4 : synchronisation sur la source secondaire sans présence d'une source primaire

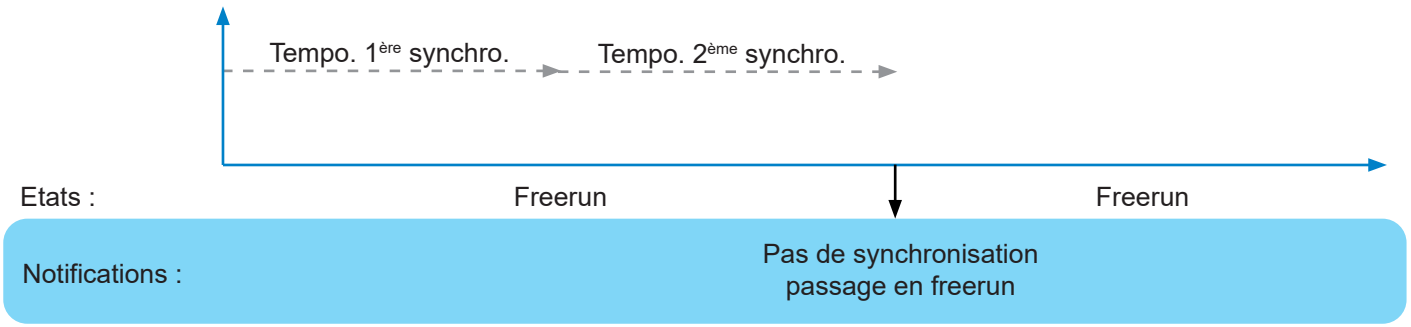
- Freerun au démarrage du produit
- Temporisation[1] pour la synchronisation sur la source secondaire (ex.: NTP)

Pour plus de réctivité, si la synchro n'ait pas trouvée, aubout de 5 minutes le système tente de se synchroniser sur la source secondaire.



Scénario 5 : aucune source de synchronisation

- Freerun au démarrage du produit
- Temporisation pour la synchronisation sur la source primaire (ex.: IRIG)
- Temporisation pour la synchronisation sur la source secondaire (ex. NTP)
- Pas de synchronisation : passage en freerun



---

[1] *La valeur du time-out de la temporisation 1ère sychro dépend de la source de synchronisation:*

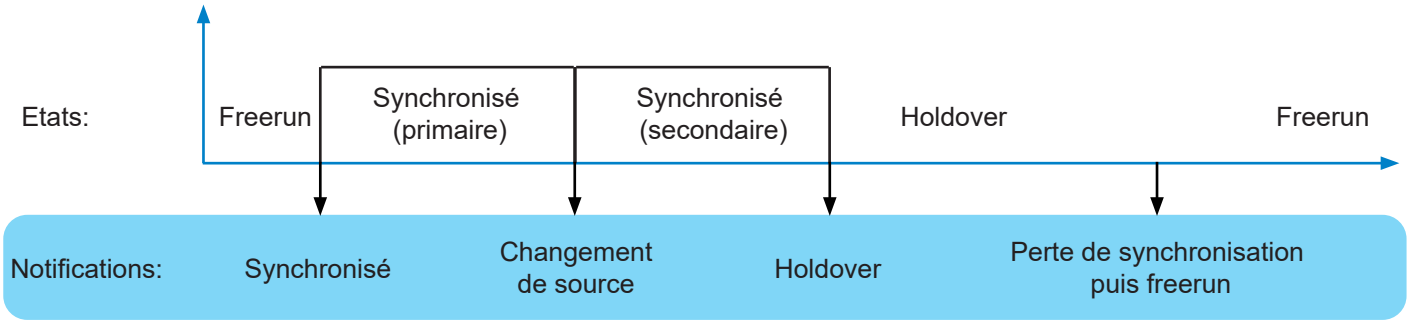
- *GNSS Bodet : 5 minutes*
- *PTP : 10 minutes*
- *NTP : 15 minutes*
- *IRIG : 10 minutes*

9.1.2. Sélection automatique

La source de synchronisation est automatiquement sélectionnée suivant la qualité de réception. Il n'y a pas de holdover déterminé entre les changements de source.

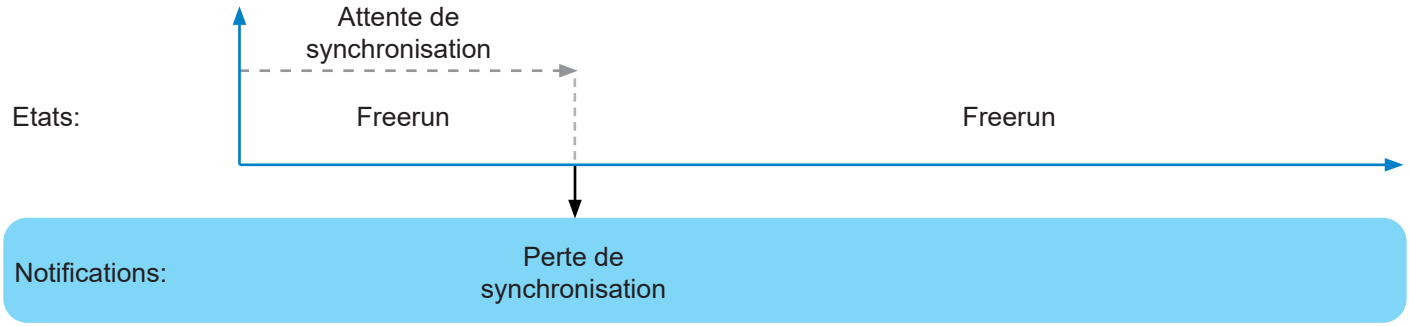
Scénario 1 : Perte de synchronisation de la source primaire puis secondaire

- Freerun au démarrage du produit
- Synchronisation sur la source primaire (ex : GNSS)
- Synchronisation sur la source secondaire (ex: NTP)
- Perte de synchronisation sur la source secondaire
- Holdover
- Pas de synchronisation: freerun



Scénario 2 : Pas de source de synchronisation

- Freerun au démarrage du produit
- Attente de synchronisation auprès des sources (ex : GNSS + NTP)
- Pas de synchronisation: freerun



9.2 Annexe 2 : fonctionnalités

Le tableau suivant résume la disponibilité des fonctions :

Fonctions	Description	Serveur web	SSH	Console	Clavier de commande
Réseau					
	Interfaces : configurer l'interface ETH0	√	√	√	√
	Interfaces : configurer les autres interfaces réseaux	√	√	√	-
	Routes : configurer des routes statiques IPv4 / IPv6	√	-	-	-
	Services : activer les services	√	√	√	-
Notification					
	Alarmes : configurer les alarmes et les seuils d'alarmes (réception des satellites et expiration des certificats)	√	-	-	-
	SNMP Trap : activer et configurer le SNMP Trap	√	-	-	-
	SMTP : activer et configurer le SMTP	√	-	-	-
	Syslog : activer et configurer le journal Syslog	√	-	-	-
Sécurité					
	Gestion utilisateurs : ajouter/modifier/supprimer un compte, changer un mot de passe et restaurer le compte administrateur par défaut	√	-	-	√ (restauration du compte admin. uniquement)
	Gestion utilisateurs : activer les services LDAP / RADIUS	√	-	-	-
	Agent SNMP : activer et configurer l'agent SNMP gestion de la supervision (SNMP V1/V2c - V3)	√	-	-	-
	SSH : activation et gestion des clés pour authentification	√	-	-	-
	HTTPS : activer les services HTTP/HTTPS	√	-	-	-
	HTTPS : choix du certificat (HTTPS)	√	-	-	-
	Certificats et clés : importer et paramétrer des certificats (CA, signés) et des clés	√	-	-	-
Time					
	Synchronisation : activer et paramétrer les sources	√	-	-	-
	Synchronisation : gérer les priorités	√	-	-	-
	Synchronisation : définir les comportements (holdover, stratum,...)	√	-	-	-
	NTP : activer et configurer le protocole NTP	√	-	-	-
	PTP : activer et configurer le protocole PTP	√	-	-	-
	Sorties : paramétrer les sorties (cartes options)	√	-	-	-
	Base temps : configurer l'heure du système	√	-	-	-
	Base temps : définir les zones horaires	√	-	-	-
	Base de temps : programmer un Leap Second manuel	√	-	-	-
	Base de temps : définir l'offset TAI/UTC	√	-	-	-
Historique					
	Statistiques GNSS	√	-	-	-
	Statistiques NTP	√	-	-	-
	Statistiques PTP	√	-	-	-
	Statistiques IRIG	√	-	-	-
	Statistiques Oscillateur	√	-	-	-
	Logs NTP	√	-	-	-
	Logs Syslog	√			
	Alarmes : acquitter et consulter l'historique des alarmes	√	-	-	-
Système					
	Général>Paramètres : modifier le nom du produit, la langue et la durée avant déconnection automatique de la session.	√	√ (langue uniquement)	√ (langue uniquement)	-
	Général>face avant : verrouiller le clavier et le port USB, modifier la langue et les paramètres d'affichage de l'écran LCD de Netsilon.	√	-	-	√ (sauf paramètres d'affichage de l'écran LCD)
	Général>Versions : consulter la version firmware de Netsilon et les cartes options installées	√	√	√	√
	Général>Consulter cette notice	√	-	-	-
	Outils>Mise à jour et sauvegarde : sauvegarder ou charger la configuration, passer en configuration usine et mettre à jour le firmware	√	-	√ (configuration usine uniquement)	√
	Outils>Redémarrer : redémarrer ou éteindre Netsilon	√	√	√	-
	Outils>Cartes options : supprimer une carte option. **ATTENTION : l'action est irréversible sans une action mécanique.**	√	-	-	-
	Outils>Export logs : exporter les logs	√	-	-	-

9.3 Annexe 3 : droits en fonction du profil : administrateur & utilisateur

Le tableau suivant résume la disponibilité des fonctions :

Fonctions	Description	Admin.	User
Réseau			
	Interfaces : configurer l'interface ETH0	L/E[1]	L
	Interfaces : configurer les autres interfaces réseaux	L/E	L
	Routes : configurer des routes statiques IPv4 / IPv6	L/E	L
	Services : activer les services	L/E	L/E
Notification			
	Alarmes : configurer les alarmes et les seuils d'alarmes (réception des satellites et expiration des certificats)	L/E	L/E
	SNMP Trap : activer et configurer le SNMP Trap	L/E	L/E
	SMTP : activer et configurer le SMTP	L/E	L/E
	Syslog : activer et configurer le journal Syslog	L/E	L/E
Sécurité			
	Gestion utilisateurs : ajouter/modifier/supprimer un compte, changer un mot de passe et restaurer le compte administrateur par défaut	L/E	L
	Gestion utilisateurs : activer les services LDAP / RADIUS	L/E	L
	Agent SNMP : activer et configurer l'agent SNMP	L/E	L/E
	SSH : activation et gestion des clés pour authentification	L/E	L
	HTTPS : activer les services HTTP/HTTPS	L/E	L
	HTTPS : choix du certificat (HTTPS)	L/E	L
	Certificats et clés : importer et paramétrer des certificats (CA, signés) et des clés	L/E	L
Time			
	Synchronisation : activer et paramétrer les sources	L/E	L/E
	Synchronisation : gérer les priorités	L/E	L/E
	Synchronisation : définir les comportements (holdover, stratum,...)	L/E	L/E
	NTP : activer et configurer le protocole NTP	L/E	L/E
	PTP : activer et configurer le protocole PTP	L/E	L/E
	Sorties : paramétrer les sorties (cartes options)	L/E	L/E
	Base temps : configurer l'heure du système	L/E	L/E
	Base temps : définir les zones horaires	L/E	L/E
	Base de temps : programmer un Leap Second manuel	L/E	L/E
	Base de temps : définir l'offset TAI/UTC	L/E	L/E
Historique			
	Statistiques GNSS	L	L
	Statistiques NTP	L	L
	Statistiques PTP	L	L
	Statistiques IRIG	L	L
	Statistiques Oscillateur	L	L
	Logs NTP	L	L
	Logs Syslog	L	L
	Alarmes : acquitter et consulter l'historique des alarmes	L/E	L/E
Système			
	Général>Paramètres : modifier le nom de Netsilon, la langue et le temps d'inactivité du serveur web.	L/E	L : nom de Netsilon E : langue et délai d'inactivité
	Général>face avant : verrouiller le clavier et le port USB, modifier la langue et les paramètres d'affichage de l'écran LCD de Netsilon.	L/E	L : verrouiller le clavier USB E
	Général>Versions : consulter la version firmware de Netsilon et les cartes options installées	L	L
	Général : consulter cette notice	L	L
	Outils>Mise à jour et sauvegarde : sauvegarder ou charger la configuration, passer en configuration usine et mettre à jour le firmware	L	L: sauvegarde ou chargement d'une configuration uniquement
	Outils>Redémarrer : redémarrer ou éteindre Netsilon	L	L
	Outils>Cartes options : supprimer une carte option. **ATTENTION : l'action est irréversible sans une action mécanique.**	L	L
	Outils>Export logs : exporter les logs	L	L

[1] *L/E = Lecture/Ecriture*

9.4 Annexe 4 : paramètres sauvegardés

Fonctions	Description	Sauvegarde
Réseau		
	Interfaces : configurer l'interface ETH0	-
	Interfaces : configurer les autres interfaces réseaux	-
	Routes : configurer des routes statiques IPv4 / IPv6	-
	Services : activer les services	-
Notification		
	Alarmes : configurer les alarmes et les seuils d'alarmes (réception des satellites et expiration des certificats)	-
	SNMP Trap : activer et configurer le SNMP Trap	√
	SMTP : activer et configurer le SMTP	√
	Syslog : activer et configurer le journal Syslog	√
Sécurité		
	Gestion utilisateurs : ajouter/modifier/supprimer un compte, changer un mot de passe et restaurer le compte administrateur par défaut	-
	Gestion utilisateurs : activer les services LDAP / RADIUS	√
	Agent SNMP : activer et configurer l'agent SNMP	√
	SSH : activation et gestion des clés pour authentification	√
	HTTPS : activer les services HTTP/HTTPS	√
	HTTPS : choix du certificat (HTTPS)	-
	Certificats et clés : importer et paramétrer des certificats (CA, signés) et des clés	√ (CA uniquement)
Time		
	Synchronisation : activer et paramétrer les sources	√
	Synchronisation : gérer les priorités	√
	Synchronisation : définir les comportements (holdover, stratum,...)	√
	NTP : activer et configurer le protocole NTP	√
	PTP : activer et configurer le protocole PTP	√
	Sorties : paramétrer les sorties (cartes options)	√
	Base temps : configurer l'heure du système	-
	Base temps : définir les zones horaires	√
	Base de temps : programmer un Leap Second manuel	√
	Base de temps : définir l'offset TAI/UTC	√
Historique		
	Statistiques GNSS	-
	Statistiques NTP	-
	Statistiques PTP	-
	Statistiques IRIG	-
	Statistiques Oscillateur	-
	Logs NTP	-
	Logs Syslog	-
	Alarmes : acquitter et consulter l'historique des alarmes	-
Système		
	Général>Paramètres : modifier le nom de Netsilon, la langue et le temps d'inactivité du serveur web.	√
	Général>face avant : verrouiller le clavier et le port USB, modifier la langue et les paramètres d'affichage de l'écran LCD de Netsilon.	√
	Général>Versions : consulter la version firmware de Netsilon et les cartes options installées	-
	Général : consulter cette notice	-
	Outils>Mise à jour et sauvegarde : sauvegarder ou charger la configuration, passer en configuration usine et mettre à jour le firmware	-
	Outils>Redémarrer : redémarrer ou éteindre Netsilon	-
	Outils>Cartes options : supprimer une carte option. **ATTENTION : l'action est irréversible sans une action mécanique.**	-
	Outils>Export logs : exporter les logs	√

9.5 Annexe 5 : listes des jeux de commandes

Liste des commandes de Netsilon :

Catégorie	Commande	Description
Général		
	helpcli	Liste de toutes les commandes.
Système		
	systemversion	Affiche les versions de Netsilon et de ses cartes options.
	systemoptioncard	Liste des cartes options installées.
	systemlistservices	Affiche l'état des services.
	systemservice [service] [ON/OFF]	Modifier l'état d'un service.
	systemlanguage [FR/UK/ES/DE/NL/IT]	Modifier la langue de Netsilon.
	systemtimeget	Permet de lire l'heure locale.
	systemstratlevel	Indique le numéro de strat de Netsilon.
	systempowerac1status	Indique le statut de l'alimentation AC 1.
	systempowerac2status	Indique le statut de l'alimentation AC 2 (utile uniquement en cas de double alimentation : version AC+AC).
	systempowerdcstatus	Indique le statut de l'alimentation DC.
Synchronisation		
	synccurentsource	Indique la source de référence.
	syncsystemstatus	Indique l'état du système.
	synccurrentnbsat	Indique le nombre de satellites détectés.
Alarme		
	alarmnbminor	Indique le nombre d'alarmes mineures actives.
	alarmnbmajor	Indique le nombre d'alarmes majeures actives.
	alarmnbcritical	Indique le nombre d'alarmes critiques actives.
Outils (tool)		
	toolpreupdate	Préparation de Netsilon pour recevoir un fichier de mise à jour.
	toolupdate	Lance la mise à jour précédemment copiée sur Netsilon.
	toolrestore	Retour à la configuration usine et redémarre Netsilon.
	toolreboot	Redémarrage de Netsilon.
	toolshutdown	Arrêt de Netsilon.
	toolcancel	Annule une commande en cours. Valable uniquement pour toolrestore, toolreboot et toolshutdown.
Réseau IPv4 (network)		
	net4getinfo	Affichage les paramètres IPv4 de tous les ports ou du port demandé: adresse IP et passerelle.
	net4getdhcp [interface]	Indique l'état du DHCP de tous les ports ou du port demandé. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net4setdhcp [interface] [ON/OFF]	Active ou désactive le mode DHCP. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net4getdns [interface]	Indique le serveur DNS de tous les ports ou du port demandé. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net4setdns [interface] [addr4]	Définir les paramètres du serveur DNS. Interface=ethX,ethX.vlan,bondX, bondX.vlan

	net4getgate [interface]	Indique la passerelle de tous les ports ou du port demandé. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net4setgate [interface] [addr4]	Définir la passerelle. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net4setstaticip [interface]	Définir l'adresse IP et le masque en statique. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net4getstaticip [interface] [addr4/cidr]	Indique l'adresse IP et le masque en statique de tous les ports ou du port demandé. Interface=ethX,ethX.vlan,bondX, bondX.vlan
Réseau IPv6 (network)		
	net6getinfo	Affichage les paramètres IPv6 de tous les ports ou du port demandé: adresse IP et passerelle.
	net6getdhcp [interface]	Indique l'état du DHCP de tous les ports ou du port demandé. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6setdhcp [interface] [ON/OFF]	Active ou désactive le mode DHCP. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6getslaac [interface]	Afficher l'état de slaac (activer / désactiver) pour chaque interface réseau. Afficher les informations uniquement pour l'interface spécifiée, le cas échéant. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6setslaac [interface] [ON/OFF]	Définit l'état de slaac (activer / désactiver) pour l'interface réseau spécifiée. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6getgate [interface]	Indique la passerelle de tous les ports ou du port demandé. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6setgate [interface] [addr6]	Définir la passerelle. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6getstaticip [interface]	Définir l'adresse IP et le masque en statique. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6addstaticip [interface] [addr6]/[prefix]	Indique l'adresse IP et le masque en statique de tous les ports ou du port demandé. Interface=ethX,ethX.vlan,bondX, bondX.vlan
	net6delstaticip [interface] [index]	Supprime une adresse/préfixe statique IPv6 pour l'interface réseau spécifiée. Interface=ethX,ethX.vlan,bondX, bondX.vlan Index= index de l'adresse statique IPv6 (1,2,3) Exemple : net6delstaticip 0 1

9.6 Annexe 6 : fichier sécurisé pour le transfert SCP et SFTP

Netsilon propose une fonctionnalité de transfert de fichiers sécurisées à l'aide d'outils clients : SCP et SFTP. L'authentification est effectuée à l'aide du mot de passe du compte par défaut ou de la clé publique.

1. Effectuer un transfert de fichier SCP vers Netsilon à l'aide de l'authentification par mot de passe du compte par défaut :

```
scp authorized_keys scp 10.10.200.5: .ssh
scp 10.10.200.135 password: admin49
```

(toujours utiliser le même mot de passe que bodetadmin)

```
publickeys 100%
  ********************************************  5 00:00
```

```
sftp scp 10.10.200.5
scp 10.10.200.135 password: admin49
```

(toujours utiliser le même mot de passe que bodetadmin)

```
sftp>
```

2. Effectuer un transfert de fichier SCP vers Netsilon à l'aide de la clé publique :

```
scp -i ./id_rsa scp 10.10.200.5: .ssh
Entrez le mot de passe pour la clé ./id_rsa: mysecretpassphrase

publickeys 100%
 *********************************************  5 00:00
```

3. Effectuer un transfert de fichier SFTP vers Netsilon à l'aide de l'authentification par mot de passe du compte par défaut :

4. Effectuer un transfert de fichier SFTP vers Netsilon à l'aide de la clé publique :

```
sftp -i ./id_rsa scp 10.10.200.5
Entrez le mot de passe pour la clé ./id_rsa: mysecretpassphrase
```

L'utilisateur reçoit l'invitation SFTP permettant le transfert des fichiers.

```
sftp>
```

L'utilisateur reçoit l'invitation SFTP permettant le transfert de fichiers.