Sound-Scanner
Manuel d'installation et de paramétrage
Firmware Version AF2.3.0.0

Table des matières

Introduction

Les détecteurs Sound-Scanner de la marque SENSIVIC™ comportent une antenne acoustique à 4 microphones disposés sur le plan de fond du détecteur. C'est ce dispositif qui assure la détection des événements sonores et la détermination de la direction de leur source.

Placement

Ce plan de prise de son doit être placé :

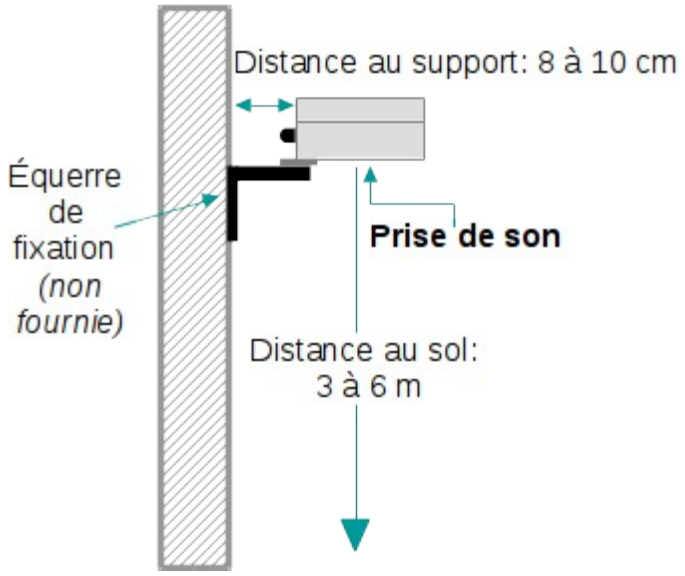
- horizontalement
- à une hauteur comprise entre 3m et 6m

Le boîtier est fourni avec 2 accroches de fixation qui permettent soit de le fixer en paroi soit de le fixer par cerclage sur un mât en utilisant des équerres non fournies (ou tout autre système de fixation équivalent).

Le boîtier est très léger, il ne requiert pas une fixation spécialement robuste.

Étant alimenté en mode PoE (par le câble-réseau IP 4 paires cat5e ou mieux), le passage d'un seul câble est à prévoir.

L'utilisation d'un câble cat5e à enterrer n'est pas nécessaire. Il suffit que son enveloppe soit résistante aux UV et à l'humidité.



Câblage

Le câblage est réalisé à partir d'un câble cat 5e en bobine.

Le boîtier est ouvert, le câble est introduit dans le boîtier à travers le presse-étoupe et un connecteur RJ45 est serti à l'extrémité du câble. Le boîtier est ensuite refermé en prenant garde au sens de placement du couvercle et au placement du joint dans sa gorge.

Les câbles cat5e destinés à un usage extérieur disposent d'une enveloppe de protection contre les UV et l'humidité, ils sont plus rigides que les câbles destinés à un usage intérieur.

Pour réaliser un sertissage de la prise RJ45 souple, après le passage du câble à travers le presse-étoupe, il est nécessaire de retirer l'enveloppe de protection sur une longueur d'environ 10cm. Attention à ne pas dé-torsader les paires sur un longueur dépassant 10 à 12mm.

L'enveloppe de protection ne joue aucun rôle électrique ; ce n'est qu'une protection physique des conducteurs électriques. Il n'y a aucun inconvénient à la retirer sur quelques centimètres.

Paramétrage

Le paramétrage du détecteur est réalisé :

- à partir de son site web embarqué,
- au niveau du logiciel de vidéoprotection en ce qui concerne le paramétrage des actions associées aux notifications d'alarme.

Le repérage de la direction de la source d'une alarme utilise le modèle de la montre où chaque

direction est associée à une heure : alarme à « 2 heures », alarme à « 7 heures », etc. La direction « 12 heures » est celle qui est à l'opposé du presse-étoupe. Le paramétrage des alarmes suppose un opérateur dos à la fixation et regardant sa montre.

Les 360° d'écoute du détecteur peuvent être partagés soit en 6 zones de détection de 60° + 1 soit en 12 zones de 30° + 1. La zone supplémentaire est située immédiatement sous le détecteur.

Les paramètres peuvent être replacés en configuration d'usine en appuyant sur le bouton poussoir placé sur la carte électronique pendant au moins 3 sec. jusqu'à ce que le redémarrage s'effectue.

Le site Web embarqué dont l'URL est l'adresse IP du détecteur (192.168.1.10 en sortie de production) comporte 6 pages :

- Paramètres de Connexion
- Notifications SNMP/TCP/UDP
- Monitoring
- Réglages
- Aide

Toutes les pages proposent un lien imprimer cette page pour constituer le dossier de paramétrage du détecteur.

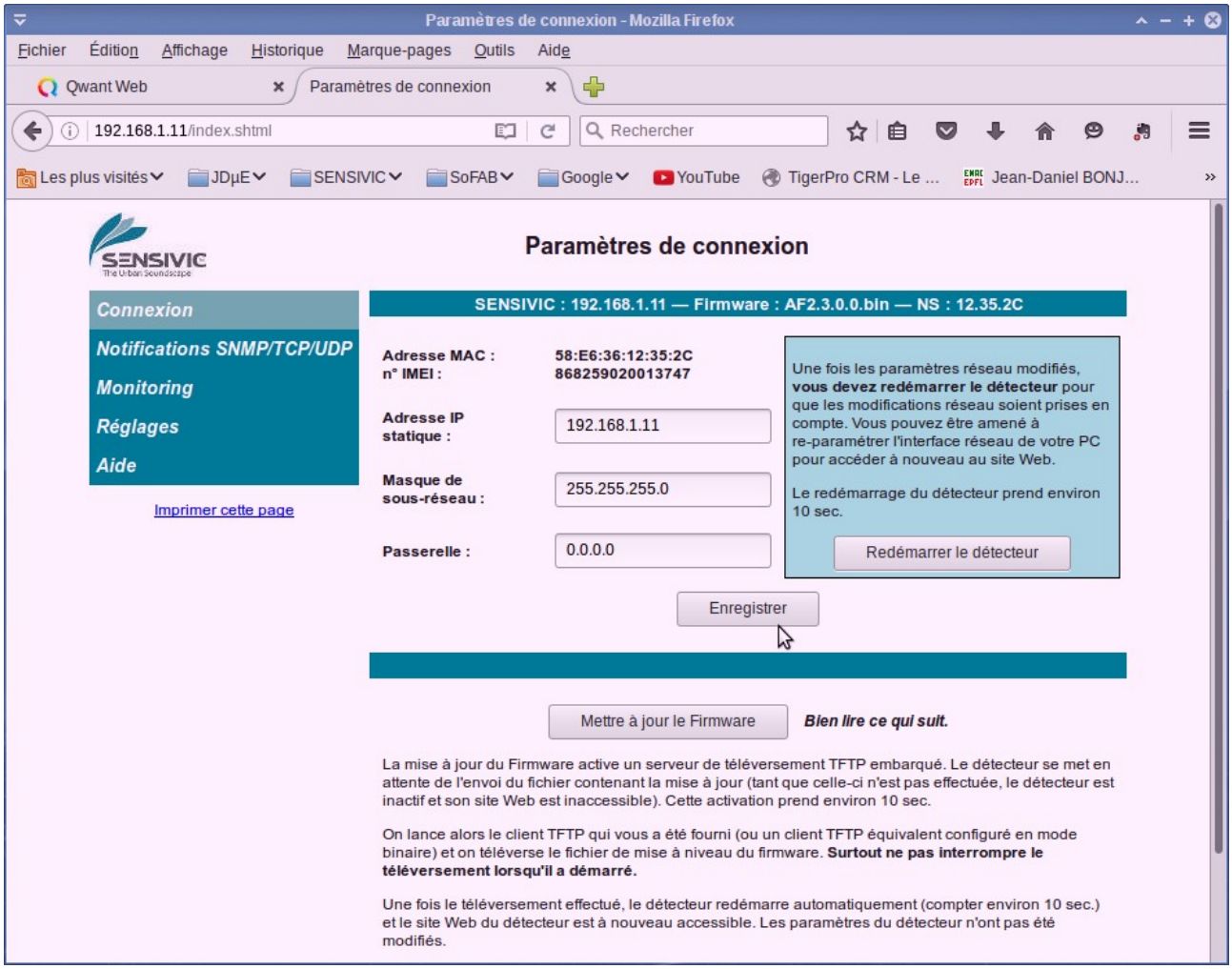
La configuration des Leds caractérise les conditions de fonctionnement du détecteur.

Power :	allumée lorsque alimenté (par le PoE)
Systick :	clignote tant que le système est vivant.
Init :	est allumée pendant tout la phase de pre-learning.
Alarm :	s'allume au moment où un événement est signalé. Elle s'éteint lorsque la détection est déverrouillée.

À la mise sous tension, toutes les leds sont allumées pendant l'auto-test de démarrage.

Puis le détecteur démarre et la led **Systick** clignote. La led **Init** s'allume pendant environ 7min.30 (phase de pre-learning). Pendant cette phase, seules les alarmes de tests sont signalées entraînant l'allumage de la led **Alarm**.

Enfin la led **Init** s'éteint et le détecteur est opérationnel.



Cette étape est **obligatoire** car tous les détecteurs ont, en sortie d'usine, la même adresse IP. Placés sans modification dans le même réseau, ils perturberaient gravement son fonctionnement.

Lorsque l'adresse IP a été modifiée, il est nécessaire de **redémarrer le détecteur** en cliquant sur le bouton Redémarrer le détecteur.

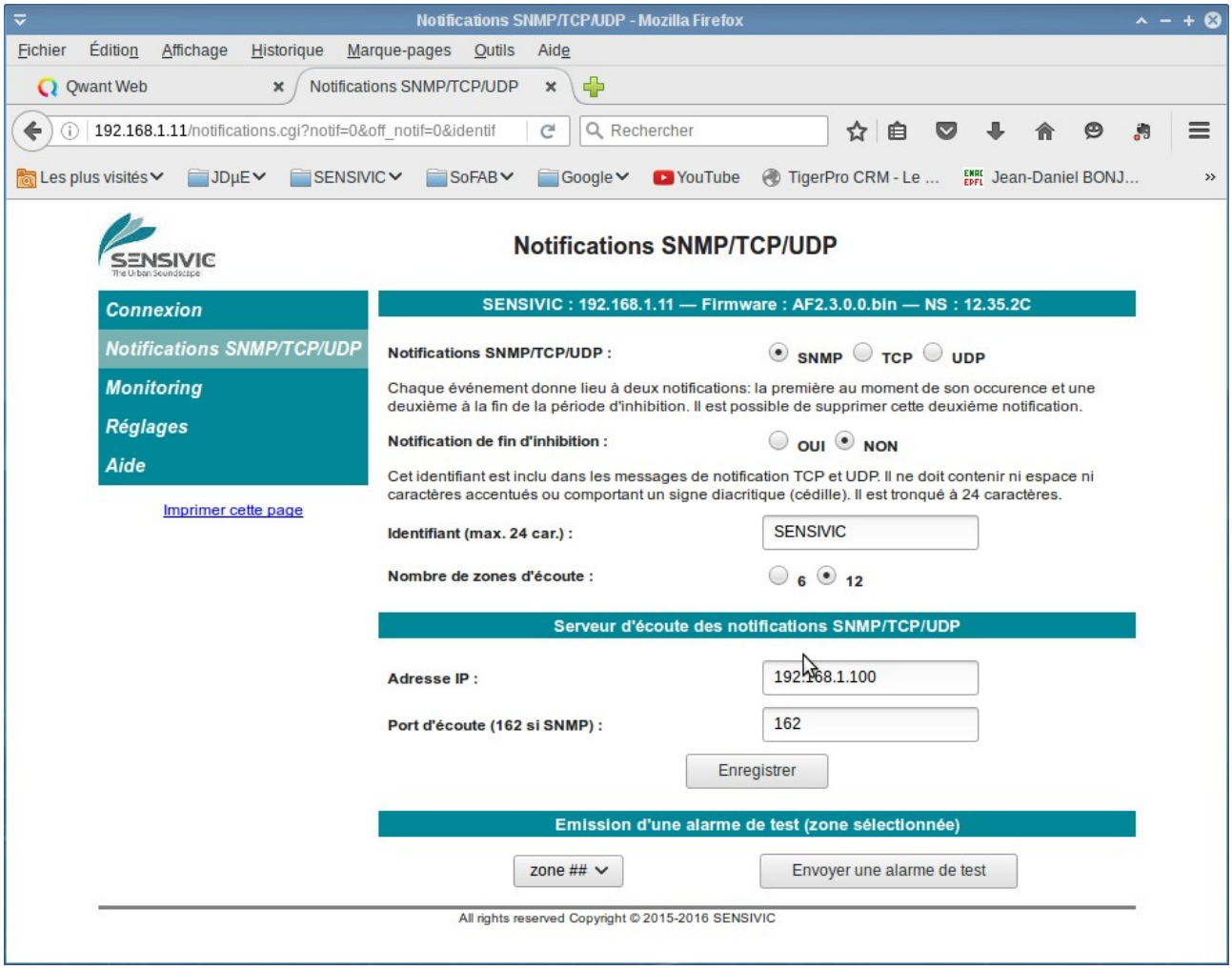
Attention : l'adresse IP du détecteur ayant changé, l'URL du site Web également et elle doit être modifiée dans le navigateur pour retrouver la connexion au site Web de paramétrage..

Si le détecteur a changé de réseau, le reparamétrage de l'interface réseau du PC de paramétrage est nécessaire.

Il est également possible de définir des sous-réseaux de détecteurs en modifiant le masque de sous-réseau et d'utiliser un réseau routé en indiquant l'adresse de la passerelle permettant l'accès au réseau routé des détecteurs.

On voit apparaître un nouveau bouton, Mettre à jour le Firmware. Cliquer sur ce bouton met en route la procédure de mise à jour (cf. paragraphe Mise à jour du Firmware).

Penser à imprimer cette page pour se souvenir du paramétrage de l'interface IP.



Les notifications SNMP sont activées par défaut. Les notifications utilisant le protocole TCP ou UDP sont désactivées par défaut.

Les trames SNMP suivent le standard associé à la norme SNMP V1. Ce sont des trames de type UDP.

Les trames TCP ou UDP sont, en général, identifiées par le serveur de supervision par un mécanisme de filtrage du contenu de la trame à paramétrer. Chaque événement produit deux notifications : (1) lorsque l'alarme est activée au moment de la détection, (2) lorsque l'alarme est désactivée à la fin du temps de verrouillage des détections. La deuxième détection peut être désactivée.

Les notifications TCP ou UDP sont de la forme :

<identifiant> <adresse IP> <n° de la zone de détection> ON

<identifiant> <adresse IP> <n° de la zone de détection> OFF

Une notification UDP se traduit par l'émission d'une seule trame. Cette notification est donc très rapide (moins de 100ms) Par contre, sur un réseau de mauvaise qualité, certaines trames peuvent être perdues sans que cela se sache.

Une notification TCP se traduit par l'ouverture d'une session TCP requise par le détecteur, puis la transmission de la trame de notification, puis la fermeture de la session TCP requise par le détecteur. Ce protocole est totalement sûr, par contre, la transmission de la notification est un peu plus lente (entre 150 et 200ms).

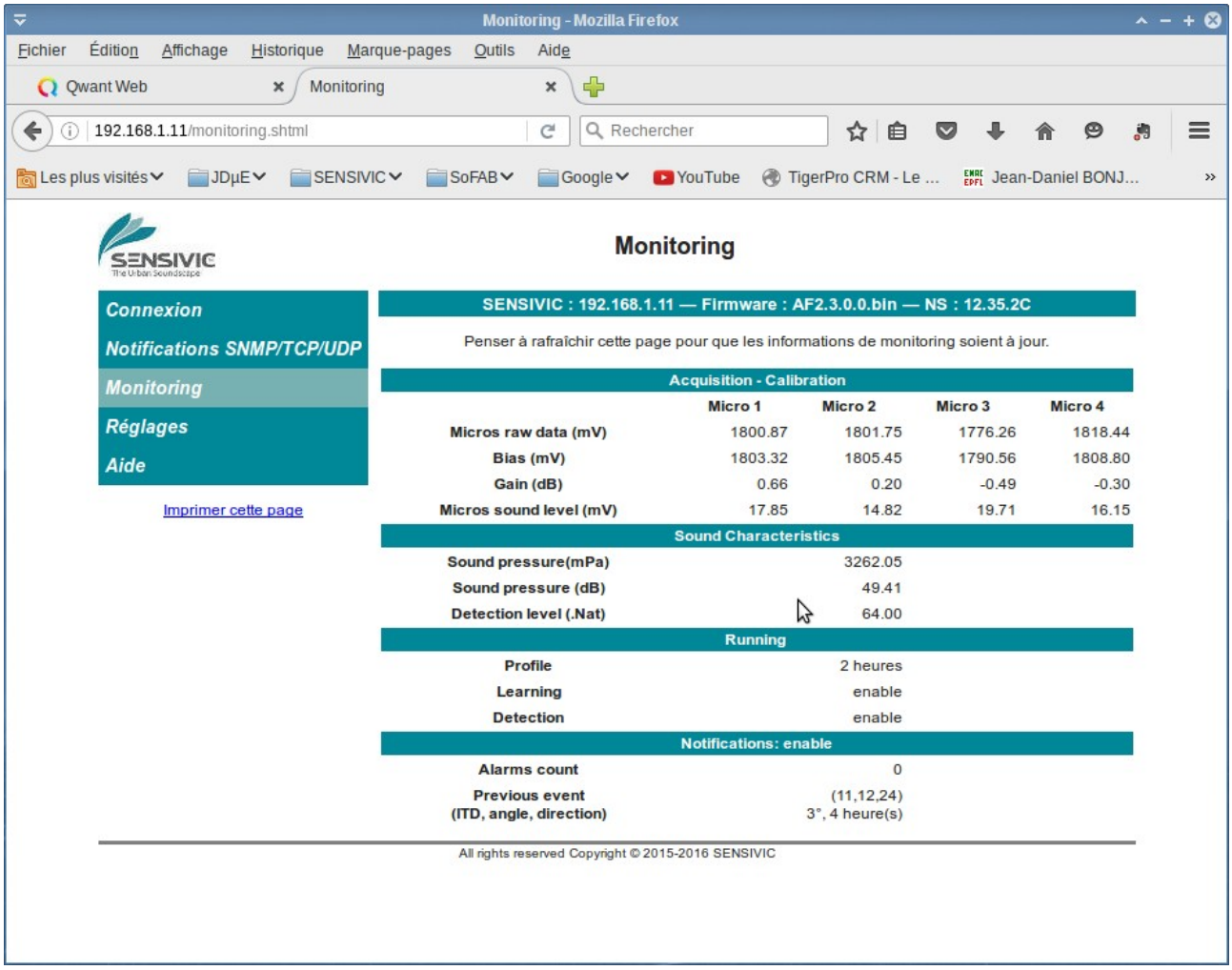
Pour choisir le protocole utilisé pour transmettre les notifications d'alarme, il faut :

- choisir le protocole de notification utilisé
- choisir le nombre des zones de détection
- indiquer si la notification de fin d'alarme est à émettre
- définir l'identifiant personnalisé (l'identifiant par défaut est SENSIVIC)
- définir les coordonnées (adresse, port) du serveur d'écoute SNMP/TCP/UDP utilisé.

Lorsque le paramétrage du logiciel de supervision a été effectué, il est possible d'envoyer des « alarmes de test » pour vérifier la réception et le traitement des notifications d'alarmes.

Ces paramétrages sont pris en compte immédiatement, il n'est pas nécessaire de redémarrer le détecteur.

Penser à imprimer cette page pour se souvenir du paramétrage des notifications SNMP/TCP/UDP.



Cette page affiche les principales données de fonctionnement du détecteur. Pensez à la rafraîchir pour mettre à jour les données affichées.

Un microphone en bon état fournit une mesure (raw data) comprise entre 500mV et 3100mV.

Les données de « Bias » et de « Gain » permettent de suivre le mécanisme d'autocalibration permanent des microphones. Le « Bias » se stabilise aux environs de 1800 mV tandis que le « Gain » se stabilise aux environs de 0dB.

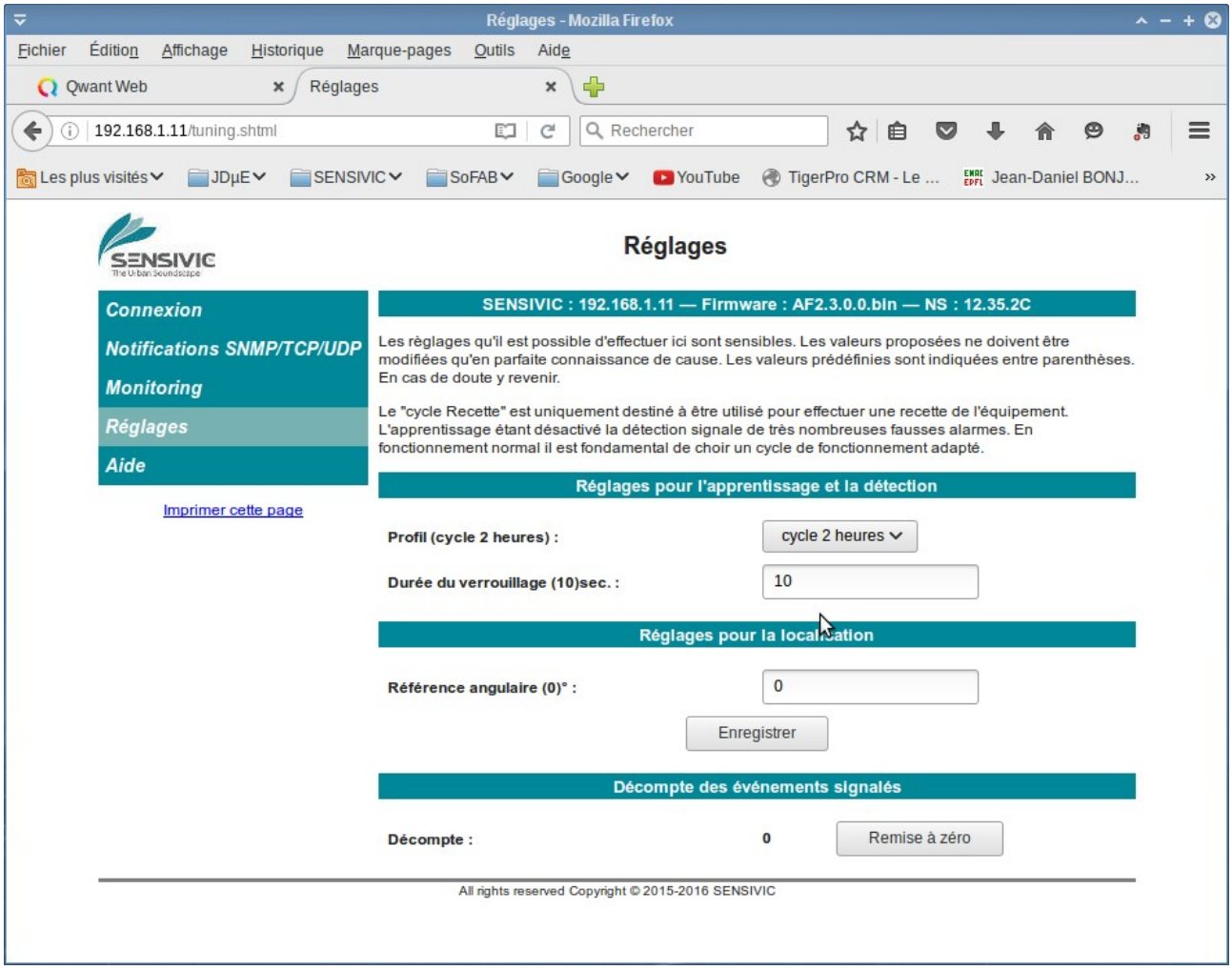
Le « Sound pressure level » (en mPa ou en dB) est une mesure du niveau sonore ambiant.

La valeur (et surtout l'évolution de cette valeur) « Detection top level » est une indication sur le fonctionnement du mécanisme d'auto-apprentissage.

La signalisation des événements sonores détectés ne s'effectue que lorsqu'elle est « enable ». Elle est inhibée pendant l'étape de « Pre learning » initiale et pendant les quelques secondes qui suivent la détection d'une alarme signalée.

Les données correspondant à « Previous event » permettent de vérifier le bon fonctionnement du mécanisme de détermination de la direction de la source de l'événement sonore signalé. Cette direction est notée en heures en suivant le modèle de la montre : « 12 heure(s) » est la direction opposée au presse-étoupe, « 0 heure(s) » dénote la zone située en-dessous du détecteur.

Penser à imprimer cette page et à nous la transmettre en cas de besoin.
Ces données permettent d'identifier une source de panne éventuelle.



Ces réglages ne sont pas à modifier en général. Ils correspondent aux situations courantes. Dans certains cas, il peut être utile de les raffiner.

Apprentissage et Détection

Profil : on dispose de 4 profils

- **Cycle Recette** : l'apprentissage est très limité. Ce profil est uniquement destiné à la recette du détecteur. Il est alors très sensible et permet de démontrer la détection et la transmission des alarmes. **Ce profil n'est pas destiné à l'exploitation**.
- **Cycle 1 heure** : la période d'oubli est courte, le détecteur retrouve rapidement sa vigilance initiale. Sa mémoire d'apprentissage se vide de la moitié de son contenu en 1 heure.
- **Cycle 2 heure** : la mémoire d'apprentissage se vide de la moitié de son contenu en 2 heures.
- **Cycle 4 heure** : la mémoire d'apprentissage se vide de la moitié de son contenu en 4 heures.

Durée du verrouillage : correspond à l'intervalle de temps qui suit immédiatement la détection et l'émission d'une alarme pendant lequel la détection est inhibée.

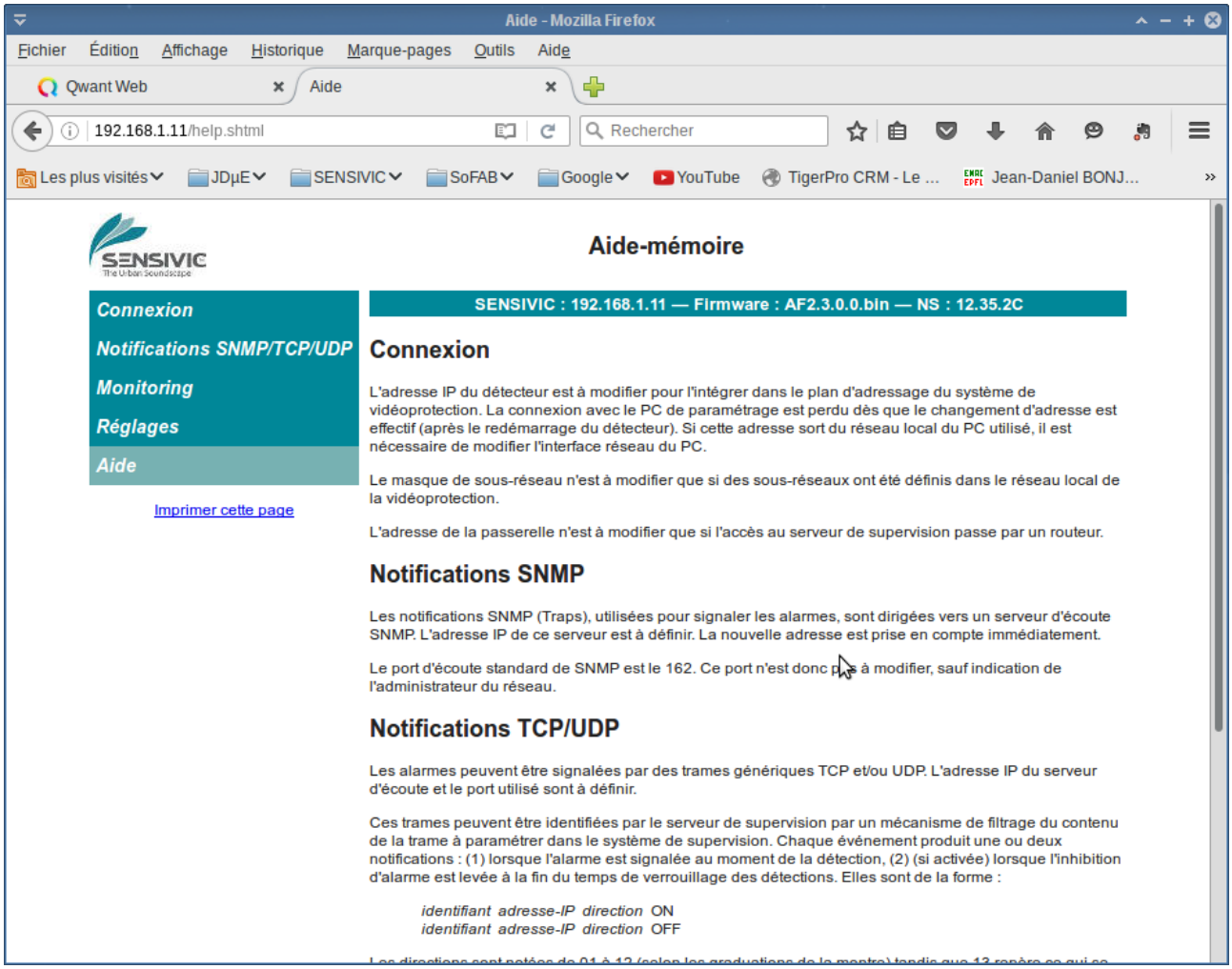
Localisation

Référence angulaire : cette valeur détermine la surface de l'espace considéré comme situé en-dessous du détecteur. Elle peut être légèrement augmentée si le détecteur a été placé moins

haut que la hauteur recommandée et légèrement diminuée si le détecteur a été placé plus haut que la hauteur recommandée.

Le décompte des événements signalés permet de rapprocher le nombre des alarmes reçues par le logiciel de supervision et le nombre de celles émises par le détecteur pendant une période de temps donnée. On peut alors remettre cette indication à 0 pour démarrer une nouvelle période.

Penser à imprimer cette page pour se souvenir des réglages appliqués.


Aide - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils Aide
Qwant Web
Aide
192.168.1.11/help.shtml
Rechercher
Les plus visités
JDµE
SENSIVIC
SoFAB
Google
YouTube
TigerPro CRM - Le ...
Jean-Daniel BONJ...
SENSIVIC
The Urban Soundscape
Aide-mémoire
Connexion
Notifications SNMP/TCP/UDP
Monitoring
Réglages
Aide
Imprimer cette page
SENSIVIC : 192.168.1.11 — Firmware : AF2.3.0.0.bin — NS : 12.35.2C
Connexion
L'adresse IP du détecteur est à modifier pour l'intégrer dans le plan d'adressage du système de vidéoprotection. La connexion avec le PC de paramétrage est perdu dès que le changement d'adresse est effectif (après le redémarrage du détecteur). Si cette adresse sort du réseau local du PC utilisé, il est nécessaire de modifier l'interface réseau du PC.
Le masque de sous-réseau n'est à modifier que si des sous-réseaux ont été définis dans le réseau local de la vidéoprotection.
L'adresse de la passerelle n'est à modifier que si l'accès au serveur de supervision passe par un routeur.
Notifications SNMP
Les notifications SNMP (Traps), utilisées pour signaler les alarmes, sont dirigées vers un serveur d'écoute SNMP. L'adresse IP de ce serveur est à définir. La nouvelle adresse est prise en compte immédiatement.
Le port d'écoute standard de SNMP est le 162. Ce port n'est donc pas à modifier, sauf indication de l'administrateur du réseau.
Notifications TCP/UDP
Les alarmes peuvent être signalées par des trames génériques TCP et/ou UDP. L'adresse IP du serveur d'écoute et le port utilisé sont à définir.
Ces trames peuvent être identifiées par le serveur de supervision par un mécanisme de filtrage du contenu de la trame à paramétrer dans le système de supervision. Chaque événement produit une ou deux notifications : (1) lorsque l'alarme est signalée au moment de la détection, (2) (si activée) lorsque l'inhibition d'alarme est levée à la fin du temps de verrouillage des détections. Elles sont de la forme :
identifiant adresse-IP direction ON
identifiant adresse-IP direction OFF

Mise à jour du Firmware

La procédure de mise à jour du firmware est en 3 étapes :

- Cliquer sur le bouton « Mettre à jour le Firmware ».
  Le fonctionnement normal du détecteur est interrompu pour activer un serveur TFTP permettant de téléverser la nouvelle version du firmware (fichier XXXX.bin). Lorsque ce serveur est activé, la connexion avec le site web est perdue. L'activation du serveur TFTP prend environ 10 sec.
- Ouvrir un logiciel client TFTP, définir les paramètres de connexion, le mode de transfert utilisé (binaire ou octet), la taille des blocs (512) puis lancer (PUT) le téléversement du fichier de mise à jour. Un message de fin de téléversement indique que tout s'est bien passé. Lorsque le téléversement est terminé, le détecteur redémarre automatiquement sur la nouvelle version. Ce redémarrage prend environ 10sec.
- Se reconnecter au site web en cliquant sur la rubrique **Connexion** du menu (si la page est toujours affichée à l'écran).

Ne pas rafraîchir la page précédente car cela aurait pour effet de relancer la procédure de mise à jour et

… bloquer le détecteur si on ne la recommence pas.

Truc : si le site web embarqué n'est pas accessible, c'est que le détecteur est en attente d'un téléversement de mise à jour.

Windows

Nous recommandons d'utiliser le programme **Tftpd32/Tftpd64**. Ce logiciel est Opensource et nous a donné toute satisfaction.C'est le plus robuste de ceux que nous avons essayé sous Windows.

Host : définir l'adresse IP adresse du détecteur à mettre à jour. Avez-vous bien pensé à sélectionner Mettre à jour le Firmware dans la page « Connexion ».

Local File : sélectionner le fichier à téléverser dans le détecteur.

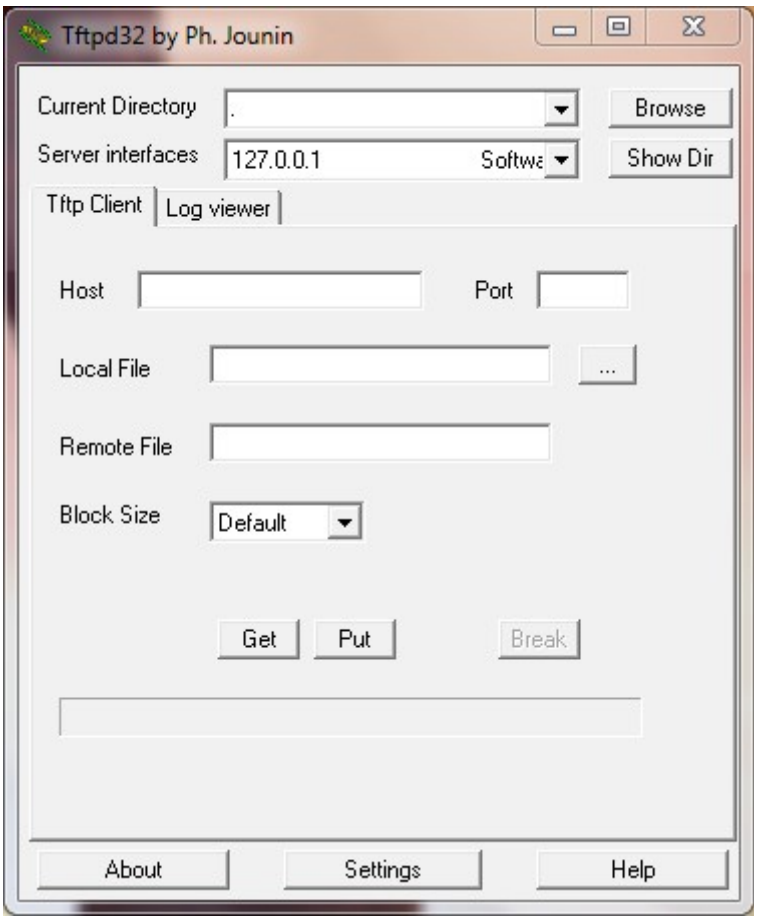
Cliquer ensuite sur Put.

Après quelques secondes le message « block #0 » apparaît, il indique que l'application à prévenu le détecteur et qu'elle attend le feu vert du détecteur pour envoyer la mise à jour.

Après quelques secondes une barre d'avancement bleue s'affiche.

Si après plusieurs secondes le téléversement ne démarre pas, cela indique que le serveur TFTP de réception n'était pas encore prêt. Dans ce cas, cliquer sur Break puis sur Put à nouveau.

Ne jamais interrompre un téléversement en cours.
Le détecteur pourrait se trouver dans l'impossibilité de redémarrer.



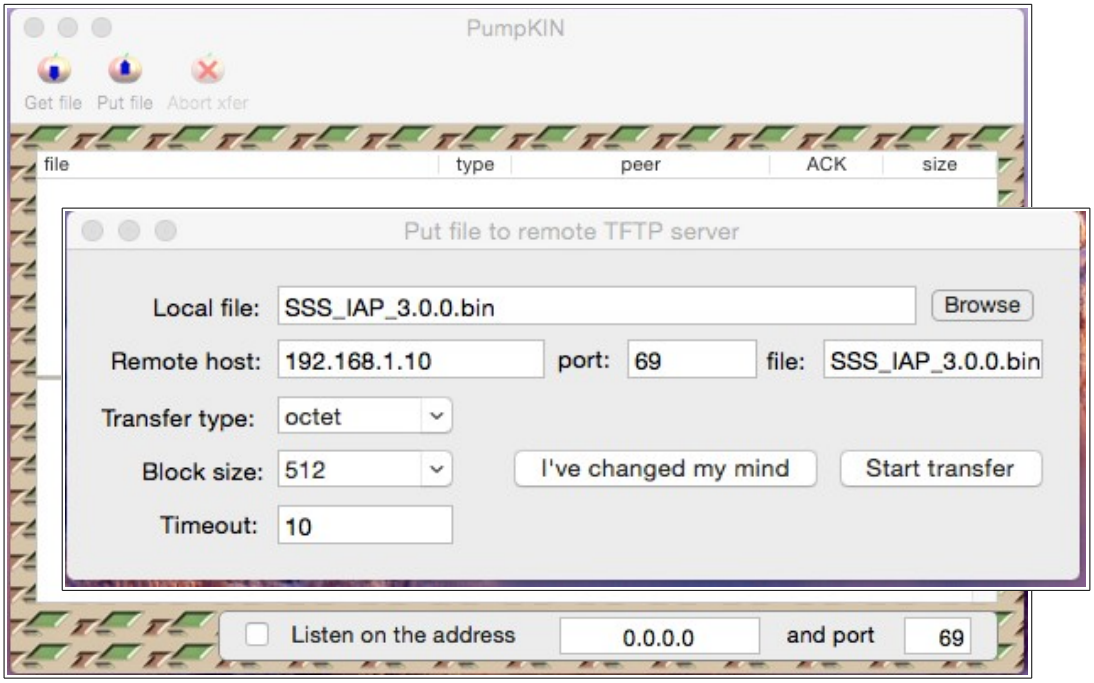
Mac OS

Nous recommandons d'utiliser le client PumpKIN. Ce logiciel est Opensource et nous a donné toute satisfaction.

Lors du premier lancement, désactiver le serveur TFTP associé en décochant la case située en bas de la fenêtre.

Cliquer ensuite sur « Put file » en haut à gauche.

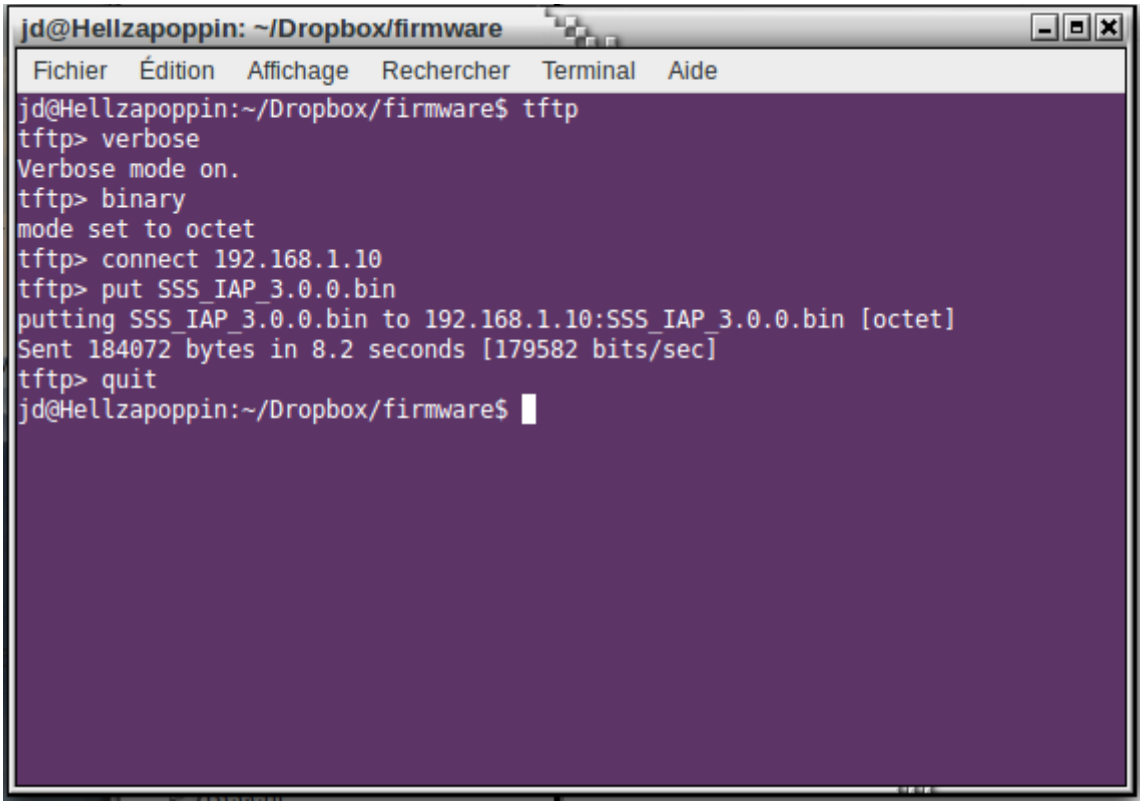
Renseigner la fenêtre « Put File to remote TFTP server » puis cliquer sur « Start transfert ».



Linux

Un client Linux TFTP est disponible pour la plupart des distributions[1]. Il fonctionne en mode « ligne de commande » et s'utilise dans un terminal.

Il suffit de recopier les lignes présentées dans l'exemple suivant en changeant l'adresse IP indiquée et le nom du fichier à téléverser.



1 Il peut être nécessaire d'installer le paquet correspondant.