

## *Utilisation du logiciel*

---

# *Elixir*



**Version 1.01**



<b>1. CONTENU DE CETTE DOCUMENTATION</b>	<b>3</b>
<b>2. PRÉREQUIS</b>	<b>3</b>
2.1. Matériel	3
2.2. Système	3
<b>3. INSTALLATION</b>	<b>4</b>
3.1. Dossier d'installation	4
A. Choix du dossier	4
B. Logo personnalisé	4
3.2. Configuration test accès internet	4
3.3. Désinstallation	4
<b>4. PRISE EN MAIN DU LOGICIEL</b>	<b>5</b>
4.1. Menu principal	5
4.2. Envoi d'infos	5
A. Enregistrement des paramètres	5
B. Limites de sécurité	5
C. Protocoles disponibles	6
4.3. Réception de données	6
4.4. Configuration	7
4.5. Informations	7
<b>5. VÉRIFICATION DE L'ACCÈS INTERNET</b>	<b>8</b>
<b>6. RACCORDEMENT D'UNE CENTRALE IP</b>	<b>9</b>
6.1. Accès internet fixe	9
6.2. Accès internet mobile	9
6.3. Envoi de trames	10
6.4. Traces des envois	10
A. Connexion TCP	10
B. Envoi de l'alarme au frontal	10
C. Attente de l'acquittement du frontal	10
<b>7. TEST DE RÉCEPTION D'UN FRONTAL</b>	<b>11</b>
7.1. Poste émetteur	11
A. Poste interne	11
B. Accès extérieur	11
7.2. Saisie des frontaux et protocoles	11
7.3. Saisie des transmetteurs de test	11
<b>8. SIMULATION DE RÉCEPTION D'ALARME</b>	<b>12</b>
8.1. Depuis le réseau local	12
8.2. Depuis l'accès internet public	12
8.3. Exemple de traces de réception	12



## 1. CONTENU DE CETTE DOCUMENTATION

Ce document décrit l'installation et l'utilisation du logiciel Elixir qui a été conçu pour les installateurs de centrales d'alarmes ainsi que les télésurveilleurs.

Pour les installateurs :

- tester les paramètres IP de connexion au réseau local
- envoyer des infos de test vers le télésurveilleur
- en filaire (ADSL, fibre...) ou mobile (3G, 4G, 5G...)

Pour les télésurveilleurs :

- tester les paramètres IP de connexion aux frontaux depuis l'intérieur et l'extérieur
- tester la réception et le traitement des infos reçues (frontaux, logiciel d'alarme)

## 2. PRÉREQUIS

### 2.1. Matériel

Les ressources nécessaires au fonctionnement d'Elixir sont :

- peu de ressources processeur (moins de 5% d'un cœur)
- environ 100Mo de RAM
- quelques centaines de méga-octets d'espace disque.

La configuration minimale recommandée est donc pour un PC ou une machine virtuelle :

- 2 cœurs CPU
- 4 Go de RAM
- 600 Mo d'espace disque libre

### 2.2. Système

Elixir tourne sous Windows : 10, 11 ou Server 2016, 2019 ou 2022.

D'autre part, Elixir tourne sans problème dans une machine virtuelle.

## 3. INSTALLATION

### 3.1. Dossier d'installation

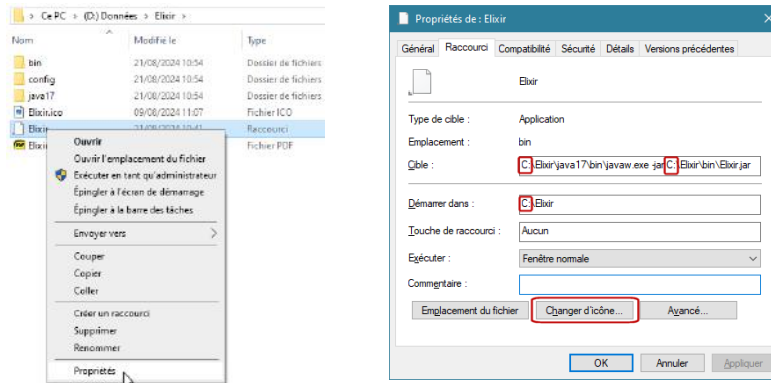
L'installation d'Elixir consiste à copier l'ensemble des fichiers nécessaires dans un dossier. La taille totale initiale des fichiers d'une installation est d'environ **270 Mo**. Les fichiers sont contenus dans un fichier .zip à extraire dans le dossier d'installation choisi.

*Java, en version 17 (ou supérieure), est nécessaire pour lancer Elixir et est inclus dans les fichiers d'installation, sous-dossier "java17".*

#### A. Choix du dossier

L'emplacement du dossier d'installation n'a pas d'importance : C:\Elixir, D:\Outils\ELIXIR...

**Nous recommandons d'installer dans le dossier C:\Elixir** pour éviter d'avoir à modifier le raccourci de lancement. Si vous installez dans un autre dossier, cliquer avec le bouton droit de la souris sur le raccourci :



Modifier les références au dossier d'installation : 2 fois dans "Cible" et une fois dans "Démarrer dans". Cliquer également sur "Changer d'icône..." et sélectionner le fichier "Elixir.ico" dans le dossier d'installation.

Dans l'exemple, le dossier d'installation est D:\Elixir ► remplacer "C:" par "D:" et sélectionner l'icône de D:\Elixir.

#### B. Logo personnalisé

Un logo peut être copié dans le dossier d'installation d'Elixir. Le fichier doit être au format PNG et nommé : **Logo.png**. Il sera affiché dans le coin supérieur gauche de la fenêtre.

### 3.2. Configuration test accès internet

Afin de tester l'accès à internet à partir du poste qui lance Elixir, le fichier texte "internet.txt" du dossier "config" contient les paramètres :

- domaine : nom de domaine existant pour tester la résolution DNS
- adresse : adresse IP et port d'un serveur externe pour tester les connexions TCP. Ce serveur (web, frontal IP) doit accepter les connexions sur le port indiqué.

Par défaut, ce sont les noms de domaine et l'adresse du serveur web de Logetel.

```
domaine = www.logetel.fr //Domaine à tester pour résolution DNS - ce nom de domaine DOIT exister
adresse = 213.186.33.19:80 //Adresse:port à tester pour connexion TCP (serveur web de Logetel)
```

Si vous souhaitez changer le nom de domaine testé ou spécifier une autre adresse IP : modifiez ce fichier texte.

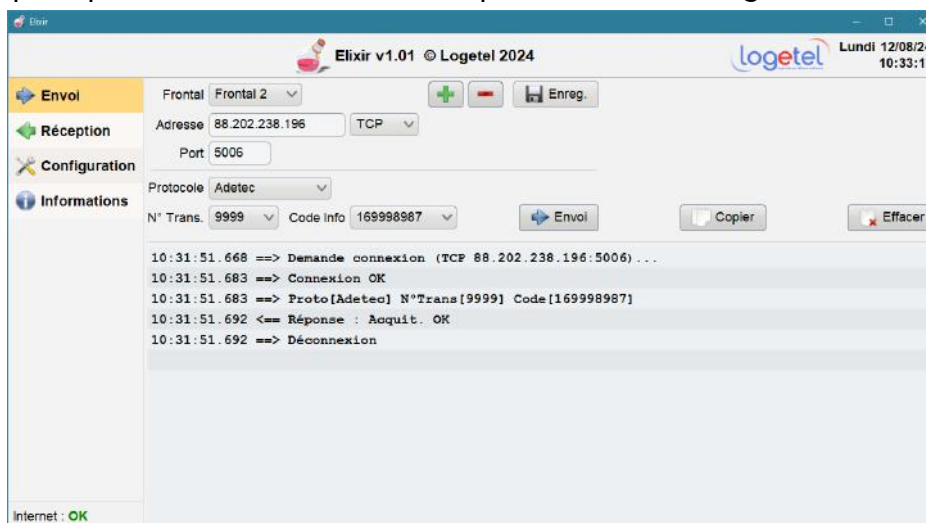
### 3.3. Désinstallation

Supprimer le dossier d'installation d'Elixir et le raccourci ajouté sur le bureau ou ailleurs.

## 4. PRISE EN MAIN DU LOGICIEL

### 4.1. Menu principal

Les fonctions principales d'Elixir sont accessibles par le menu situé à gauche de la fenêtre :



Remarque : le coin inférieur gauche donne l'état détecté de l'accès internet. Un test est lancé toutes les 10 secondes. En cas de problème d'accès le cadre est affiché avec un fond coloré et une bulle d'aide donne des indications :



Voir page 8 : **55. Vérification de l'accès internet**

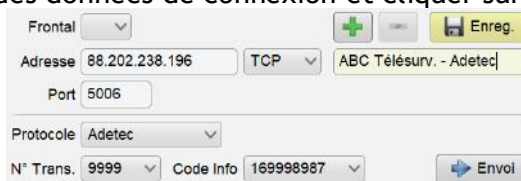
### 4.2. Envoi d'infos

C'est la fonction principale d'Elixir pour tester la connexion IP entre un site et le frontal d'un télésurveilleur. L'envoi d'infos est montré dans la copie d'écran ci-dessus.

Elixir enregistre automatiquement les derniers paramètres d'envoi et les recharge à la relance, mais il est préférable de les enregistrer.

#### A. Enregistrement des paramètres

Les paramètres d'envoi vers différents frontaux sont enregistrables. Cliquer sur le bouton "+", entrer le nom du frontal et des données de connexion et cliquer sur "Enreg." :



Remarque : L'adresse peut être une adresse IP ou un nom de domaine (ex : alarmes.securite.fr).

Par la suite, vous pouvez modifier les paramètres et les réenregistrer. Après une modification, le bouton "Enreg." est affiché en jaune pour vous rappeler d'enregistrer.

N.B. : Vous pouvez modifier les frontaux dans le module **Configuration**.

#### B. Limites de sécurité

De nombreuses limites sont présentes pour ne pas surcharger un frontal avec des infos envoyées par Elixir, et restreindre la possibilité de simuler une vraie centrale d'alarme :

- Numéros de transmetteurs limités (de 9995 à 9999)
- Codes information non-standards en Contact-ID, SIA ou Surtec
- Numéros de capteur limités (de 991 à 999 ou 987)
- Un envoi au maximum toutes les 10 secondes.



## C. Protocoles disponibles

Presque tous les protocoles connus de Logetel sont disponibles dans Elixir :

- Adetec (Vocalys)
- Aritech
- Belledonne
- BirdyBox
- Doro
- FlexC (Vanderbilt)
- Honeywell - Galaxy
- SIA-DC09
- Siemens (Syntony)
- Siemens-EDP (Intrunet SPC)
- SMB
- Solem
- Surtec - Intervox
- Synchronic
- Texecom
- TIL
- Twig
- Viewcom (Hager - Daitem)
- Visonic

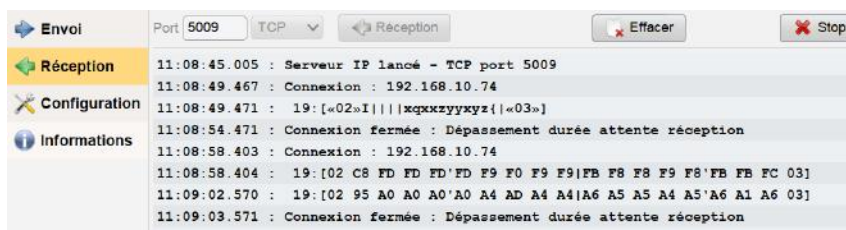
Un "protocole" spécial est présent : "Texte". Il permet d'envoyer un texte vers un frontal. Cette action sera visible dans les traces de réception du frontal sans déclencher une "fausse" réception d'alarme chez le télésurveilleur.

Certains protocoles sont absents car obsolètes (Bosch, Climax, Risco, Septam : migrés en SIA-DC09), très peu répandus (Dycon, Logetel-HTTP) ou dont les spécifications ne sont pas publiques (RSI, Paradox).

Voir page 9 : §6. Raccordement d'une centrale IP pour une description détaillée de la fonction d'envoi d'alarme.

## 4.3. Réception de données

Cette fonction affiche les trames reçues sur un port TCP ou UDP. Cela permet de vérifier la bonne réception des trames sur un PC.



Entrer le numéro de port à écouter en TCP ou UDP et cliquer sur "Réception". Les traces en-dessous montrent les trames IP reçues : l'adresse de l'expéditeur et les données reçues.

Voir page 12 : §8. Simulation de réception d'alarme pour une description détaillée et des usages de cette fonction.



## 4.4. Configuration

Cette page configure la taille par défaut des éléments graphiques et permet de réorganiser les paramètres de connexion aux frontaux :

Nom	Adresse IP	Tcp	Port	Protocole	N° Tra	Code Info	Texte	Clé Chiffr.	N° frontal
ABC Telesurv - Adetec	88.202.238.196	T	5006	Adetec	9999	169999999			
ProtectPlus - Viewcom	alarmes.protect...	T	10000	Viewcom	9997	169999999			

Buttons: Enreg., Monter, Dupliquer, Supprimer. Status: Internet : OK

Taille des éléments graphiques :

- Police : taille de la police d'affichage (de 8 à 32 points).
- Ajustement : ajuste les dimensions des éléments graphiques (recalculé automatiquement sur changement de la taille de la police).

La partie inférieure affiche la liste des frontaux enregistrés avec leur paramètres. Les noms des frontaux peuvent être modifiés en double-cliquant sur une ligne de la première colonne.

Les boutons de fonctions en bas sont :

- Monter : déplacer la ligne courante vers le haut.
- Dupliquer : duplique la ligne courante. Les paramètres du nouveau frontal sont modifiables dans le module "Envoi".
- Supprimer : Supprime le frontal courant.

## 4.5. Informations

Cette page affiche de multiples renseignements sur l'environnement d'Elixir :

Version Elixir: 1.01.01 (13/08/24 16:10)

Dernière version: 1.01.01 [Mise à jour]

Dossier Elixir: G:\Elixir\ [Ouvrir]

Version Java: 17.0.1 (Oracle Corporation)

Dossier Java: C:\Program Files\Java\jdk-17.0.1

Adresse publique: 88.202.238.196

Passerelle: 192.168.10.254 [Page Web]

Adresse(s) poste: 192.168.10.74 - Realtek PCIe GbE Family Controller #3  
172.25.192.1 - Hyper-V Virtual Ethernet Adapter [Config. réseau]

- Version Elixir : version actuelle d'Elixir et date de production
- Dernière version : dernière version disponible en mise à jour
- Dossier Elixir : dossier d'installation d'Elixir
- Version Java : version de Java lancée
- Dossier Java : dossier d'installation de Java
- Adresse publique : adresse internet publique de cette installation (déterminée par le service <http://checkip.amazonaws.com>).
- Passerelle : adresse de la passerelle locale pour l'accès à internet.
- Adresse(s) poste : adresse(s) IP locale(s) des cartes réseaux du poste.

Les boutons d'action sont :

- Mise à jour : téléchargement de la dernière version d'Elixir et mise à jour.
- Ouvrir : ouvre le dossier d'installation d'Elixir dans l'explorateur de fichiers.
- Page Web : ouvre la page web d'administration de la passerelle (la box internet).  
*Attention : ne marche pas avec toutes les box (notamment chez Free).*
- Config. réseau : ouvre la configuration système des cartes réseau : pour consulter et modifier les paramètres de connexion à internet du poste.



## 5. VÉRIFICATION DE L'ACCÈS INTERNET

Elixir teste en permanence - toutes les 10 secondes - si l'accès internet est OK. L'enchaînement des tests est le suivant :

1. Résolution DNS d'un nom de domaine
2. Connexion TCP sur un serveur
3. Test de l'accès à la passerelle
  - 3A. Passerelle OK
  - 3B. Passerelle injoignable
  - 3C. Passerelle non trouvée

Le nom de domaine testé en (1) est celui paramétré dans le fichier de configuration des tests internet. Voir page 4 : **§3.2 Configuration test accès internet**. Si la résolution DNS est OK, alors l'accès internet est considéré comme OK :

Internet : **OK**  
Accès internet OK !

Si le test (1) échoue, Elixir essaye de se connecter en TCP sur l'adresse paramétrée dans le fichier de configuration des tests. Si la connexion réussie, alors Elixir peut sans doute se connecter sur des adresses IP directes mais pas sur des noms de domaine.

Vérifier le paramétrage des serveurs DNS.

Internet : **Err. DNS**  
Accès internet sur adresses IP directes OK, mais sans noms de domaines (erreur DNS)

Si le test (2) échoue, Elixir tente de vérifier s'il peut obtenir une réponse de la passerelle :

Internet : **H.S.**  
Mais passerelle IP (192.168.10.254 - box internet, routeur...) OK

Dans ce cas, vérifier sur la passerelle l'état de la connexion à internet.

Si ce test (3) échoue :

Internet : **H.S.**  
Passerelle IP (192.168.10.254 - box internet, routeur...) non joignable

Vérifier en premier l'état de la passerelle (box internet, routeur/firewall), ainsi que les paramètres de connexion au réseau local (adresse, masque de sous-réseau, adresse de la passerelle).

Si l'adresse de la passerelle ne peut être trouvée, c'est qu'elle n'est pas activée dans la configuration de l'ordinateur :

Internet : **H.S.**  
Adresse de passerelle IP non trouvée !

Causes possibles :

- Paramètres réseau en automatique mais serveur DHCP inexistant, HS ou non joignable
- Câble réseau non branché ou Wifi non disponible
- Carte réseau ou Wifi désactivée





## 6. RACCORDEMENT D'UNE CENTRALE IP

La difficulté pour le raccordement d'une centrale en IP est qu'un ensemble de conditions doivent être réunies :

- Une connexion correcte au réseau local (adresse IP locale, masque de sous-réseau, adresse de la passerelle, serveur(s) DNS), entrés manuellement ou automatiquement (par un serveur DHCP).
- En accès fixe : le bon état du câble Ethernet et du switch ou de la box.
- En accès mobile : le bon état de la carte SIM, de son activation chez l'opérateur et de la qualité de la réception locale.
- La programmation de la centrale :
  - l'adresse IP et le port de destination chez le télésurveilleur
  - d'autres paramètres additionnels (TCP ou UDP, protocole, clé de chiffrement...)
- Chez le télésurveilleur :
  - l'état de l'accès à internet
  - la programmation du pare-feu
  - la programmation du frontal de réception

Elixir permet de vérifier une partie importante de ces différents points : les paramètres du réseau local, l'accès à internet, l'envoi en IP et l'acquittement d'un message d'alarme. Si les essais avec Elixir sont OK, il ne restera à voir "que" la programmation de la centrale.

### 6.1. Accès internet fixe

Pour vérifier la connectivité de la centrale, il faut :

- 1) débrancher le câble utilisé par la centrale et le connecter sur l'ordinateur avec Elixir.
- 2) si les paramètres de l'accès au réseau local ne sont pas automatiques (par DHCP), reprendre sur l'ordinateur les paramètres de la centrale (adresse IP, masque de sous-réseau, passerelle, serveur DNS).
- 3) lancer Elixir
- 4) vérifier si l'accès internet est OK (affichage sur écran principal et menu "Informations")

Si le point (4) est incorrect, c'est que l'accès internet n'est pas fonctionnel. Vérifier alors le câblage Ethernet, la box internet et les paramètres de connexion au réseau local.

Si le point (4) est OK, passer à : **Envoi de trames**.

### 6.2. Accès internet mobile

Il faut disposer d'un téléphone et d'un PC portable :

- 1) prendre la carte SIM de la centrale, l'insérer dans le smartphone, l'allumer et valider le code PIN de la carte SIM.
- 2) vérifier si l'accès internet est OK à partir du smartphone (avec un navigateur internet).
- 3) connecter le PC portable sur l'accès internet du smartphone (par relais Wifi ou comme modem USB)
- 4) lancer Elixir
- 5) vérifier si l'accès internet est OK dans le menu "Informations"

Si le point (2) est incorrect, c'est que l'accès internet mobile n'est pas fonctionnel. Vérifier alors si la carte SIM est bien activée chez l'opérateur. A défaut, essayer avec une autre carte.

Si le point (5) est incorrect, vérifier la connexion (3) entre le PC et le smartphone en Wifi ou USB.

Si le point (5) est OK, passer à : **Envoi de trames**.



### 6.3. Envoi de trames

- 1) Paramétrer l'accès au frontal (adresse IP, port, TCP ou UDP, protocole...)
- 2) Envoyer le message d'alarme choisi et vérifier si :
  - 2A) la connexion est établie.
  - 2B) l'acquittement est bien reçu en retour.

Si c'est le point (2A) qui bloque, vérifier avec le télésurveilleur les paramètres d'accès au frontal (adresse IP de destination, n° du port, TCP/UDP). *A noter que la quasi-totalité des protocoles communiquent en TCP.*

Si c'est le point (2B) qui bloque, vérifier avec le télésurveilleur les paramètres du protocole (protocole, numéro de port IP. Éventuellement : clé de chiffrement, numéro de frontal...). Si le télésurveilleur peut consulter les traces de réception, il peut confirmer avoir reçu ou non une trame de données depuis l'adresse IP de l'installation.

Si le point (2B) est OK, la connectivité réseau ainsi que les paramètres d'envoi des alarmes sont donc corrects. Après reconnexion de la centrale (rebranchement du câble Ethernet ou de la carte SIM), si elle ne parvient toujours pas à envoyer ses alarmes, c'est sans doute sa programmation qu'il faut revoir (paramètres IP locaux et paramètres d'envoi vers le frontal).

### 6.4. Traces des envois

Lors de l'envoi et de l'attente de la réponse du frontal, Elixir affiche les résultats des différentes étapes.

#### A. Connexion TCP

Elixir rappelle l'adresse IP et le N° de port demandé en connexion :

```

N° Trans. 9999 Code Info 169999999 [Envoi] [Copier] [Eff]
16:38:49.378 ==> Demande connexion (TCP 192.168.1.79:5004) ...
16:38:54.380 <== Erreur connexion : java.net.SocketTimeoutException: Connect timed out
16:39:03.457 ==> Demande connexion (TCP 192.168.10.79:5004) ...
16:39:05.503 <== Erreur connexion : java.net.ConnectException: Connection refused: no further information
  
```

Le premier essai montre une absence de réponse (timed out) à la demande de connexion (jusqu'à 5 secondes d'attente). Le second essai montre que le destinataire a refusé (refused) la connexion. *Remarque : en UDP, les trames sont envoyées et reçues directement, sans connexion.*

#### B. Envoi de l'alarme au frontal

Si la connexion est OK, Elixir envoie l'alarme demandée et attend l'acquittement du frontal :

```

16:45:25.274 ==> Demande connexion (TCP 192.168.10.74:5006) ...
16:45:25.291 ==> Connexion OK
16:45:25.291 ==> Proto[Doro] N°Trans[9999] Code[169999999]
16:45:28.292      Aucune réponse
16:45:28.292 ==> Déconnexion
  
```

La réponse est attendue durant 3 secondes. Cet essai montre une connexion correcte mais une absence de réponse du frontal, vérifier le numéro de port de connexion et le protocole.

#### C. Attente de l'acquittement du frontal

Et voici un exemple d'envoi réussi :

```

16:46:39.779 ==> Demande connexion (TCP 192.168.10.74:5006) ...
16:46:39.783 ==> Connexion OK
16:46:39.783 ==> Proto[Adetec] N°Trans[9999] Code[169999999]
16:46:39.794 <== Réponse : Acquit. OK
16:46:39.794 ==> Déconnexion
  
```

**Note :** certains protocoles (FlexC, Honeywell, Siemens, Synchronic, Viewcom) nécessitent un échange de plusieurs trames avant de recevoir l'acquittement final.

Si Elixir indique que l'acquittement est OK, c'est que l'info a bien été envoyée au frontal du télésurveilleur. Mais comme Elixir envoie (par sécurité) des codes non-standards, il est possible que le télésurveilleur doivent chercher pour retrouver la réception de l'info.

## 7. TEST DE RÉCEPTION D'UN FRONTAL

Cette utilisation d'Elixir concerne essentiellement les télésurveilleurs, pour vérifier la bonne réception des alarmes sur un frontal suite à :

- un changement de l'accès IP publique
- un changement du pare-feu ou de sa programmation
- une évolution du plan local des adresses IP
- un remplacement du poste hébergeant le frontal
- l'ouverture d'un nouveau protocole

### 7.1. Poste émetteur

#### **A. Poste interne**

Elixir peut être lancé sur un poste du réseau local pour tester les réceptions en local. Attention : cette action ne valide pas les réceptions depuis l'extérieur. Mais elle peut être nécessaire pour valider l'accès local, notamment si l'accès extérieur ne répond pas.

Si la réception locale ne passe pas, vérifier :

- la connexion du poste Elixir et du frontal sur le réseau local : même segment réseau IP, même réseau physique... Une commande PING <adresse\_IP> peut tester la connexion.
- la programmation du frontal : notamment le n° de port affecté au protocole testé
- l'adresse locale du frontal et le port entrés dans Elixir
- la présence et la programmation des pare-feux, éventuellement sur le réseau local, mais surtout le pare-feu logiciel sur le frontal (comme le pare-feu Windows defender). Essayer en désactivant temporairement le pare-feu logiciel du frontal.

#### **B. Accès extérieur**

Ce type de test valide l'ensemble de la chaîne de réception des frontaux IP. L'idéal est de disposer d'un second accès internet indépendant de celui des frontaux. A défaut, il est possible de tester à partir d'un accès internet mobile ou encore depuis le même accès en spécifiant l'adresse publique et non locale.

Attention : certains équipements d'accès internet (les box internet) ne permettent pas à un équipement local de se connecter sur un autre équipement local en passant par l'accès extérieur (fonction de bouclage, "loopback" en anglais). Exemple : c'est OK chez Free mais impossible avec les LiveBox d'Orange (même en version "Pro").

Si la réception extérieure ne passe pas, alors que la locale est OK, vérifier la programmation du routeur/firewall (la plupart du temps : la box internet). Le numéro du port testé est-il bien ouvert et redirigé vers l'adresse locale du poste hébergeant le frontal ?

### 7.2. Saisie des frontaux et protocoles

Il est particulièrement pratique, pour le télésurveilleur, de rentrer dans Elixir les paramètres d'accès aux frontaux et à leurs numéros de port pour chaque protocole.

Cette saisie gagne du temps pour les tests, évite les erreurs et garde une copie de la configuration des ports des frontaux.

### 7.3. Saisie des transmetteurs de test

Il est conseillé de saisir également, dans le logiciel de traitement d'alarme, le(s) numéro(s) de transmetteur et les codes infos qui vont être utilisés pour les essais. Cela simplifie la vérification des réceptions sur les différents ports/protocoles et permet de décider de l'affichage ou non aux opérateurs.

## 8. SIMULATION DE RÉCEPTION D'ALARME

Comme indiqué précédemment (page 6 : [§4.3 Réception de données](#)), cette fonction affiche les trames de données reçues en TCP ou UDP. Cette action permet de vérifier la bonne réception sur un ordinateur en validant la configuration du système (pare-feu logiciel) et des équipements réseau : box internet et/ou routeur-firewall, switch, câblage...

### 8.1. Depuis le réseau local

Dans Elixir, demander l'écoute sur un numéro de port. Démarrer l'autre équipement (centrale d'alarme en local, autre logiciel - comme [Elixir depuis un autre poste](#)) et demander l'envoi de données. Elixir affiche tout ce qu'il reçoit sur le port demandé.

**Note : Elixir n'est pas un frontal, les centrales ne sont pas acquittées des envois d'alarme.**

Si Elixir ne reçoit pas de trames en local, vérifier :

- les paramètres d'accès au réseau local de l'autre équipement. A-t-il bien accès au réseau local ?
- si l'accès au réseau local est ok, vérifier sur l'équipement les paramètres d'envoi vers Elixir : l'adresse IP locale et le numéro de port.
- si les paramètres sont OK, vérifier alors si un pare-feu système ne bloquerait pas la réception d'Elixir (comme le pare-feu Windows Defender).

Si Elixir reçoit bien les trames alors la réception locale est OK, la réception depuis l'extérieur peut être testée.

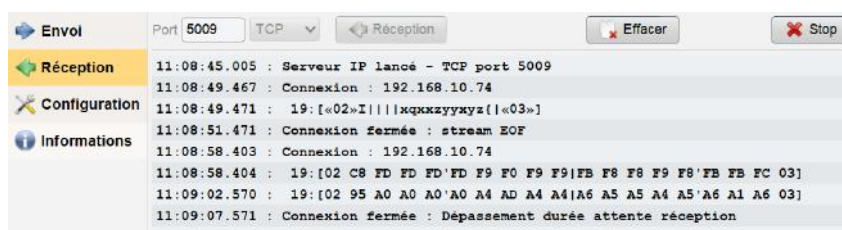
### 8.2. Depuis l'accès internet public

Idem que le test local, lancer Elixir et l'équipement distant.

Si Elixir ne reçoit pas de trames (*alors que l'accès internet est OK*), vérifier :

- si l'équipement distant a bien accès à internet.
- si l'accès à internet est ok, vérifier sur l'équipement les paramètres d'envoi vers Elixir : l'adresse IP publique et le numéro de port.
- la programmation du routeur/firewall (la plupart du temps : la box internet). Le numéro du port testé est-il bien ouvert et redirigé vers l'adresse locale du poste avec Elixir ?

### 8.3. Exemple de traces de réception



Informations affichées - date-heure des actions :

- lancement / arrêt de l'écoute sur le port demandé
- connexion IP : adresse de l'équipement distant
- trames de données reçues : nombre d'octets et contenu des trames entre [ ].
- déconnexion IP : soit par l'équipement distant (première connexion en exemple), soit d'Elixir (second exemple) qui coupe la connexion après 5 secondes sans réception de données.