SmartBridge

Genetec RSA
Guide de configuration

Table des matières

Introduction

Ce guide de configuration expliquera comment ajouter et configurer les événements d'alarme fournis par le SmartBridge dans le VMS de Genetec RSA et comment tester et afficher l'événement d'alarme dans Genetec Security Center.

Prérequis

Genetec Security Center

La première étape consiste à installer correctement Genetec Security Center. Une version 5.10.4.1 ou supérieure est nécessaire.

Licence RSA

Activer une licence RSA PRO de Genetec avec le nombre de « Fence » requis. Il faut se procurer cette licence auprès de Genetec.

Plugin RSA

Installer le Plugin RSA sur la même machine que Security Center. La version actuellement validée et recommandée est 4.2.74.0.

Inter-System Gateway Service

Installer Inter-System Gateway Service sur la même machine que Security Center. La version actuellement validée et recommandée est 1.0.75.0

Lors de l'installation, s'assurer que RabbitMQ sera aussi installé par la même occasion. La version de RabbitMQ validée est 3.9.13.4.

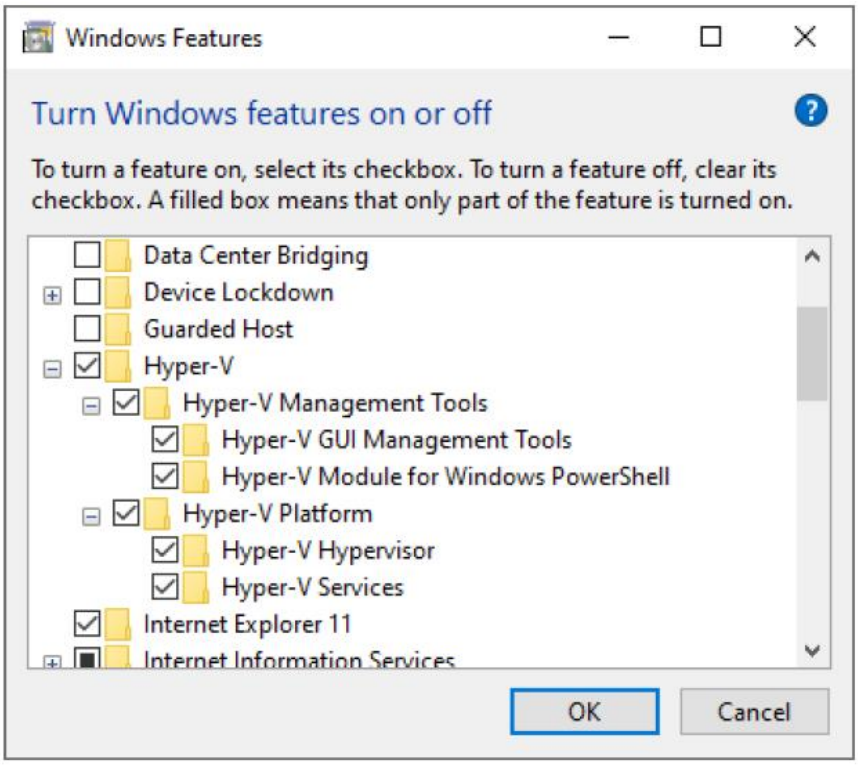
SmartBridge

Installer le SmartBridge sur la même machine que Security Center. La version actuellement validée et recommandée est 4.6.0. Se référer au manuel du SmartBridge pour plus d'information.

Docker

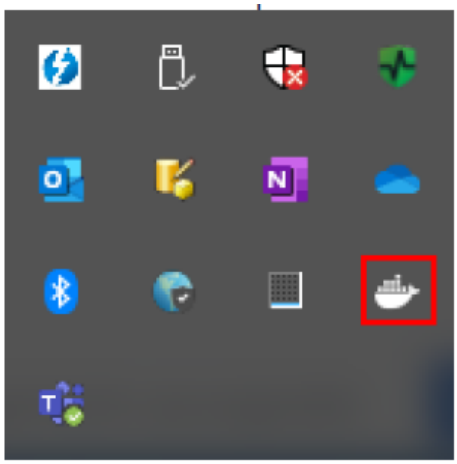
Docker est nécessaire pour exécuter le driver du SmartBridge. Il est recommandé d'installer Docker sur la même machine que Security Center. Si toutefois Docker est installé sur une autre machine, il faut s'assurer que la date/heure des deux machines soient parfaitement synchroniser. La version de Docker validée et recommandée est 4.4.4. À l'heure actuelle, les versions supérieures ne sont pas compatibles.

- S'assurer que la virtualisation est activée dans le BIOS.
- Installer Hyper-V dans Windows:



- Activer Hyper-V:
  Ouvrir Powershell en tant qu'administrateur et exécuter cette commande :
  `Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All`
- Installer Docker Desktop 4.4.4
- Installer WSL2 update :
  `https://wslstorestorage.blob.core.windows.net/wslblob/wsl_update_x64.msi`
  Redémarrer la machine.

- L'icône de Docker desktop doit s'afficher dans la barre de tâches :



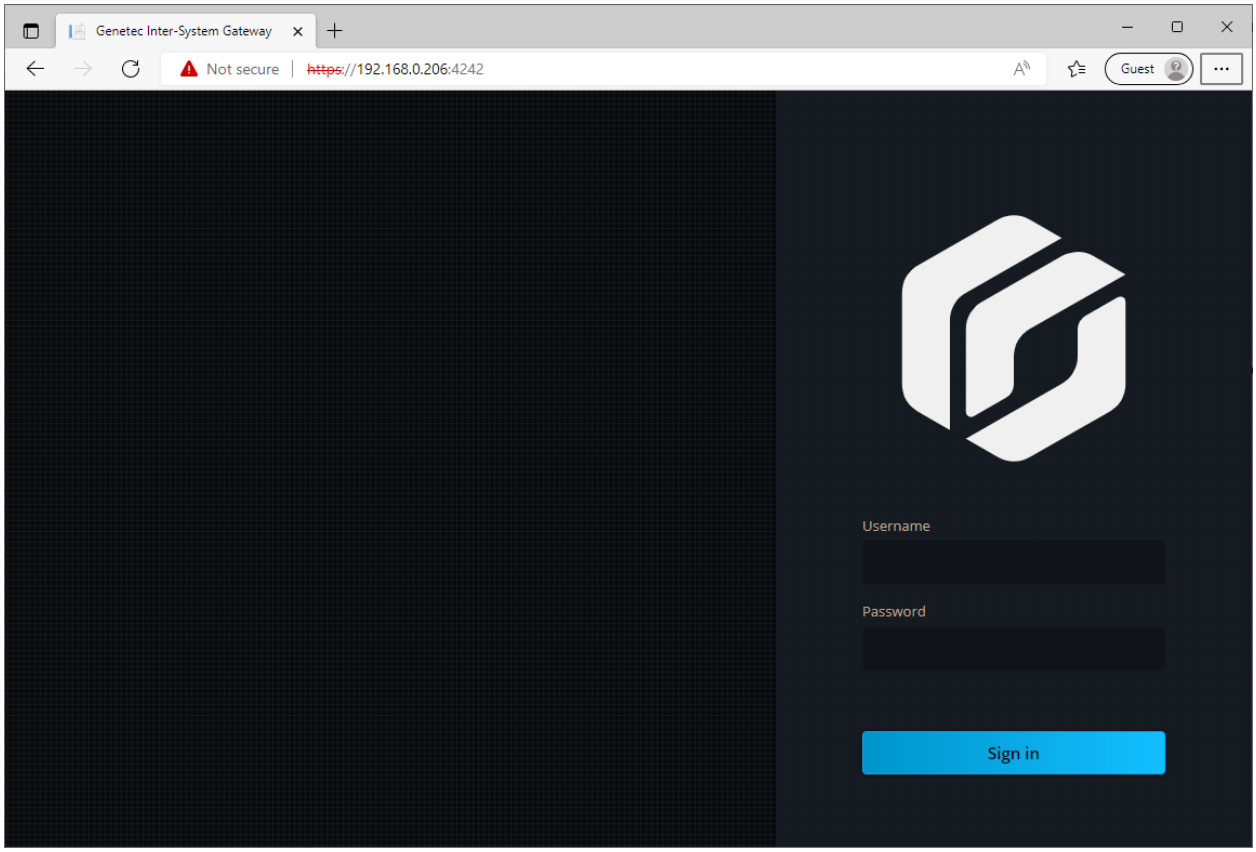
- Avec le bouton de droit, cliquer sur cette icône et choisir « switch to Windows containers… ». Attendre que docker redémarre.
- Double-cliquez sur l'icône docker dans la barre de tâches, accéder à « settings » puis « docker engine ». Modifier le contenu et le remplacer par ceci :

```
{
  "hosts": [ "tcp://0.0.0.0:2375" ]
}
```

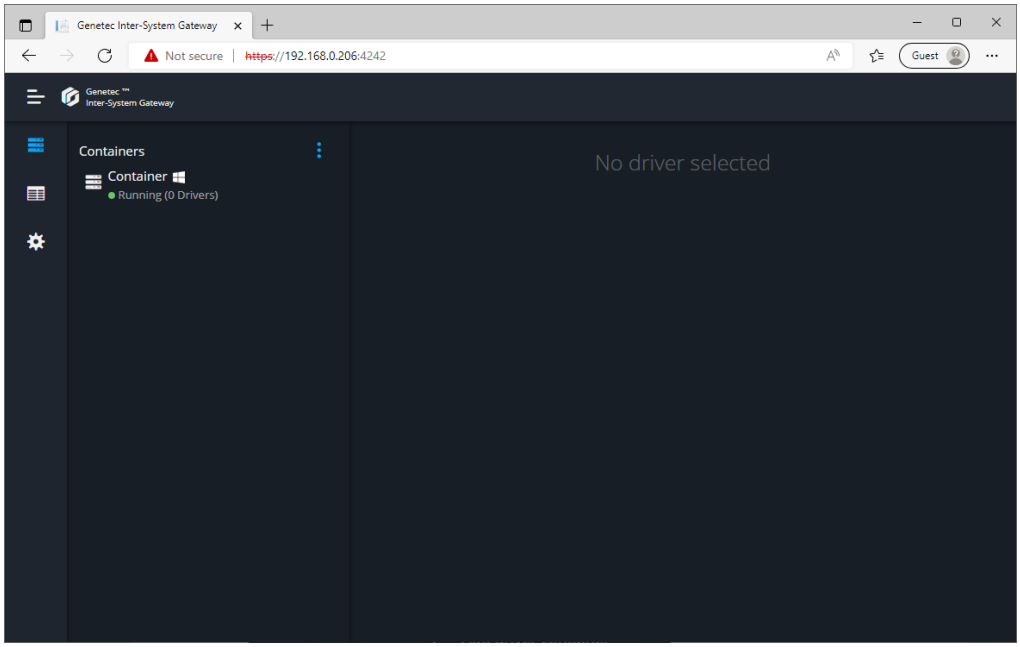
  Appliquer puis attendre que Docker redémarre.
- La configuration de Docker est maintenant terminée.

Inter-System Gateway Service

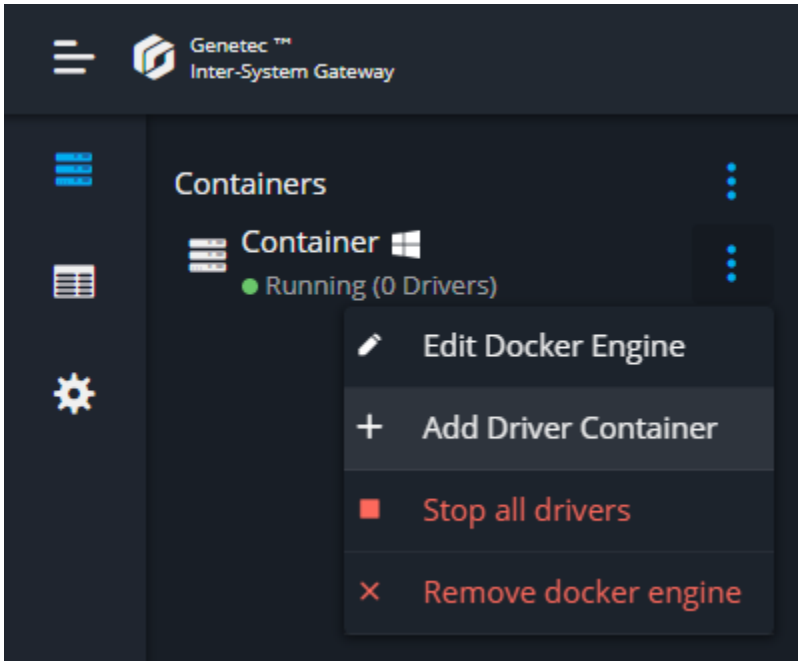
Accéder au Inter-System Gateway Service via un navigateur web. Utiliser l'adresse ip de la machine Genetec ainsi que le port du serveur (4242 par défault) :



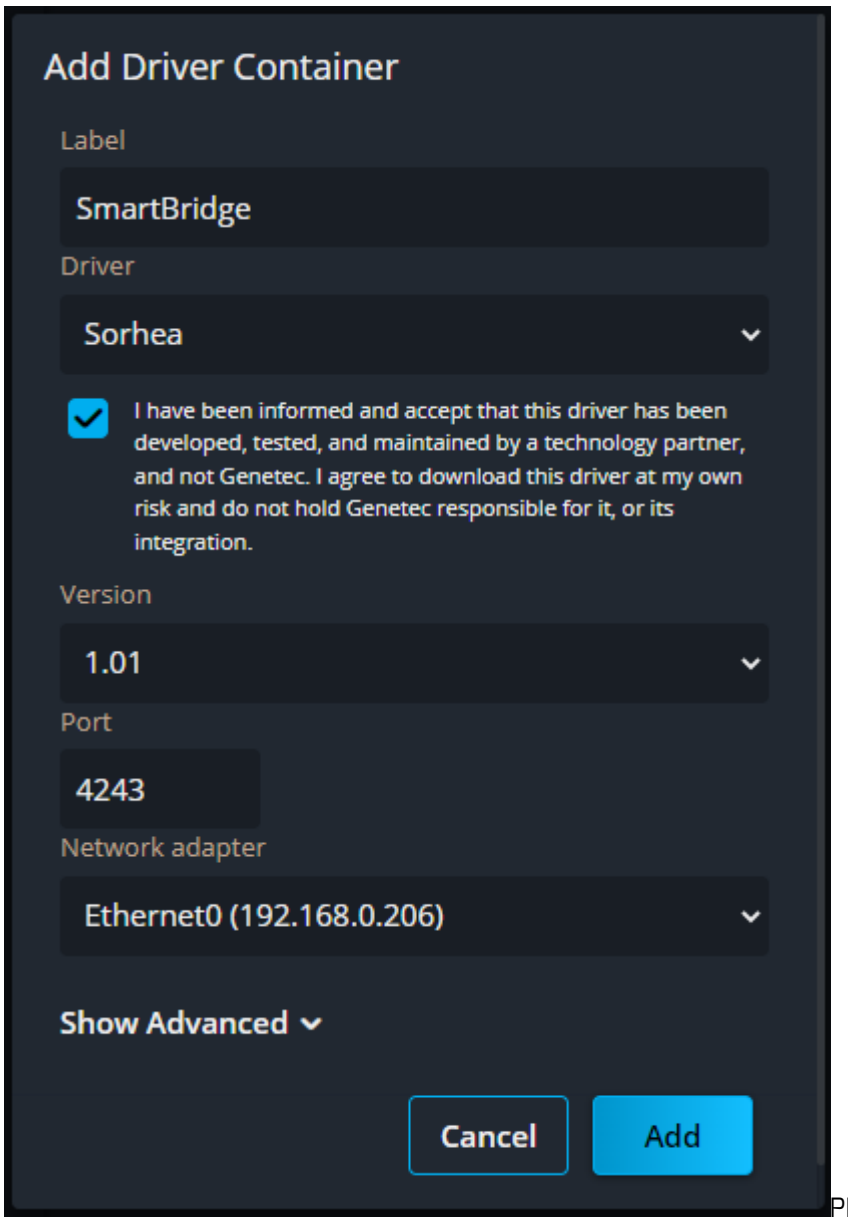
Connectez-vous au service avec votre nom d'usager et mot de passe. Une fois connecté, cette page s'affichera :



Pour ajouter le driver, ouvrir le menu et choisir « Add driver container » :



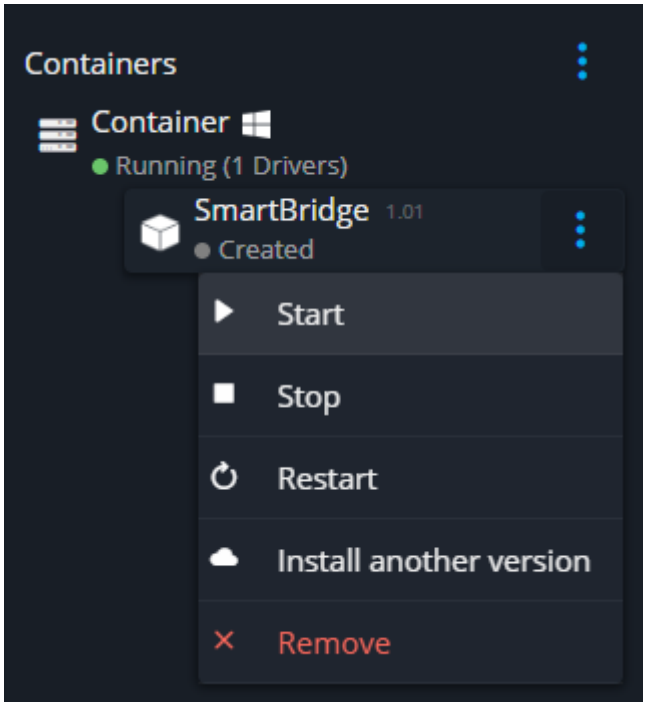
L'écran suivant s'affichera :



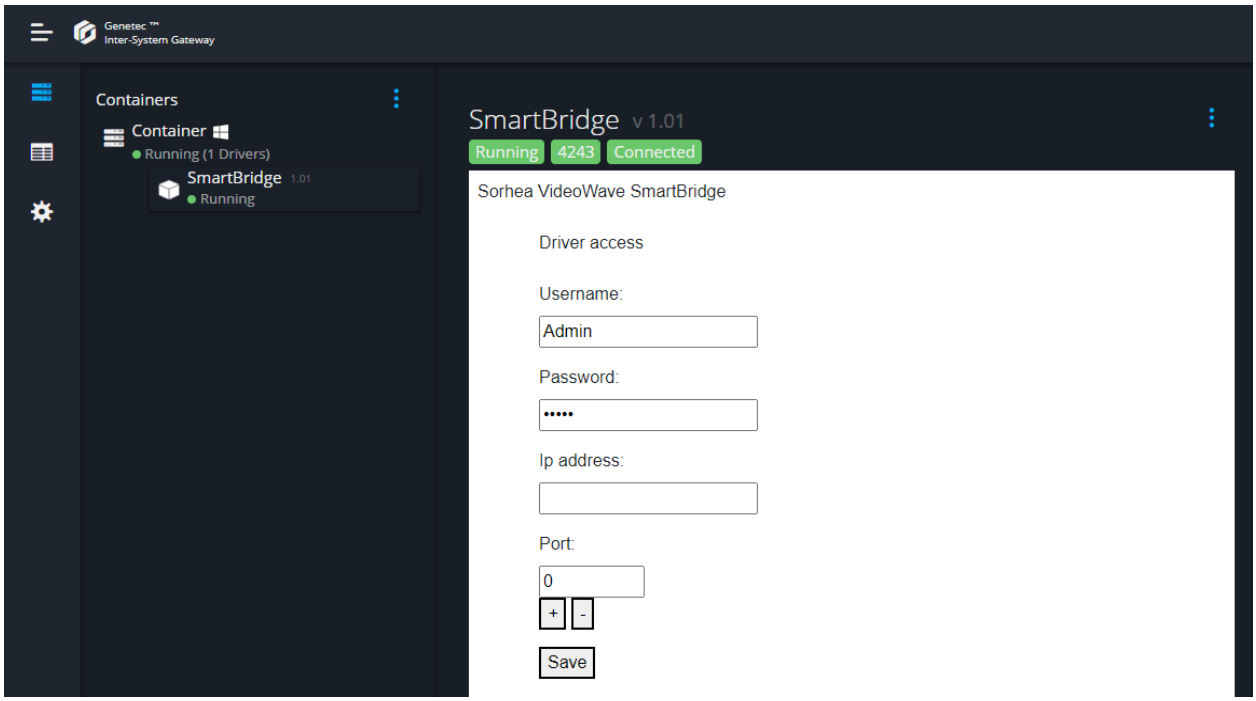
PIC!

Sous label, entrer un nom, par exemple « SmartBridge ». Sous driver, choisir « Sorhea ». Cocher la case pour accepter les conditions. Sous version, sélectionner la plus récente. Laisser le port 4243 par défaut et choisir la carte réseau du serveur Genetec. Enfin, cliquer sur « Add ».

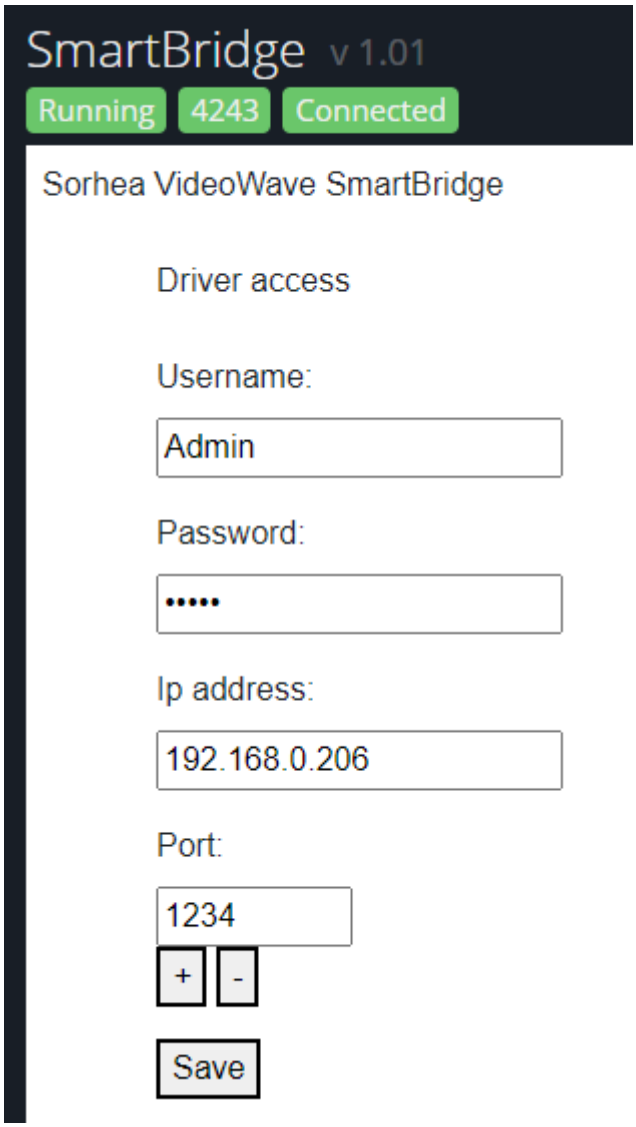
Une fois le driver créé, afficher le menu et choisir « Start » :



Une fois démarré, une page de configuration doit s'afficher :

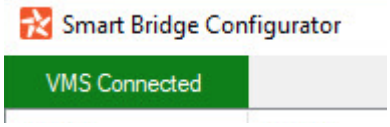


Dans cette page, entrer le Username (Admin par défaut). Entrer le mot de passe (Admin par défaut). Entrer l'adresse ip de la machine Genetec et du SmartBridge. Entrer le port du SmartBridge (1234 par défaut) :



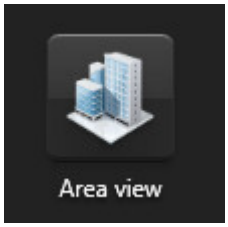
Enfin, cliquer sur Save.

Valider ensuite que le SmartBridge se connecte bien au Inter-System Gateway Server. Pour ce faire, ouvrir le configurateur du SmartBridge et vérifier que le VMS est bien connecté :

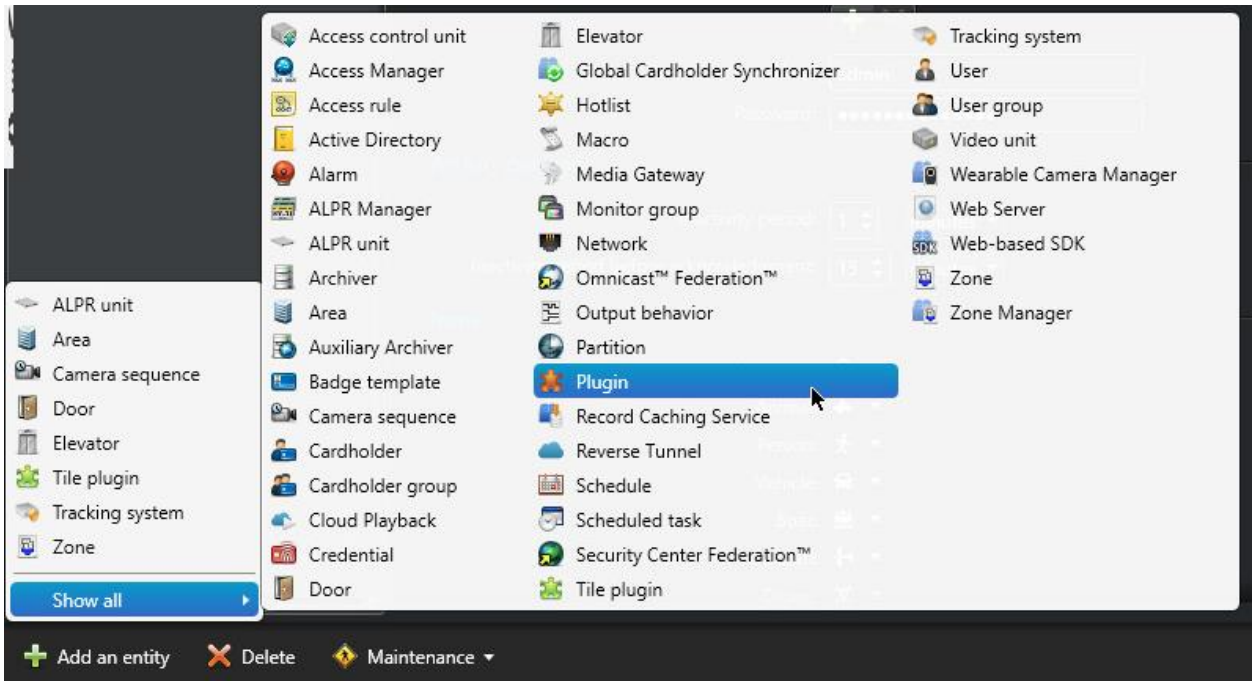


Configuration du plugin RSA

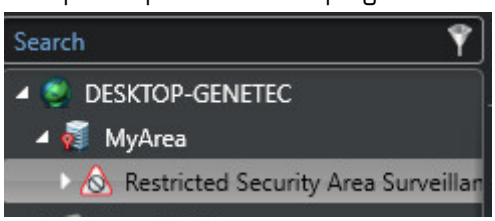
Pour configurer le plugin RSA, vous devez ouvrir l'outil Genetec Config Tool et accéder au module de configuration « Area View » :



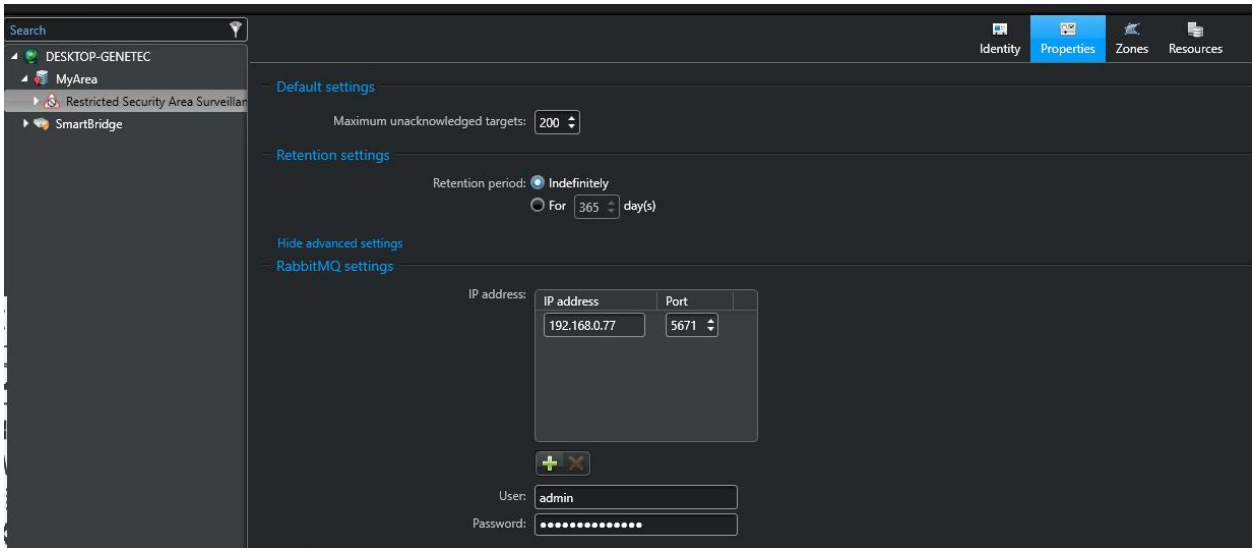
Clique sur le bouton « Add an entity » et choisir « Plugin » :



Sélectionner le plugin RSA (Restricted Security Area Surveillance) et pour compléter l'installation avec les options par défaut. Le plugin RSA devrait alors s'afficher :



Maintenant, sélectionne le plugin et accéder aux propriétés :

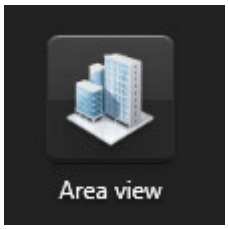


Dans cet écran, il est important de configurer la section RabbitMQ. Inscrire l'adresse ip, le port, le nom d'usager et le mot de passe du serveur RabbitMQ.

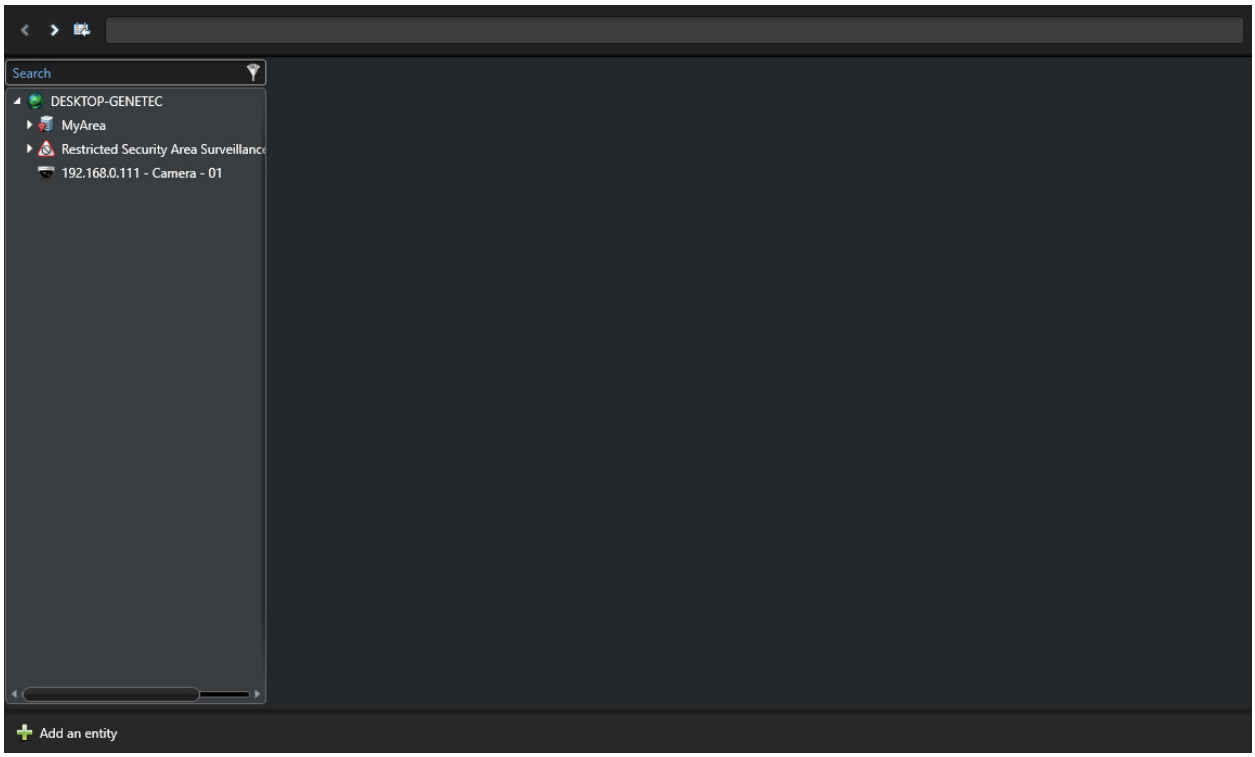
Si tout fonctionne correctement, l'élément « Restricted Security Area Surveillance » ne devrait plus s'afficher en rouge.

Configuration des appareils

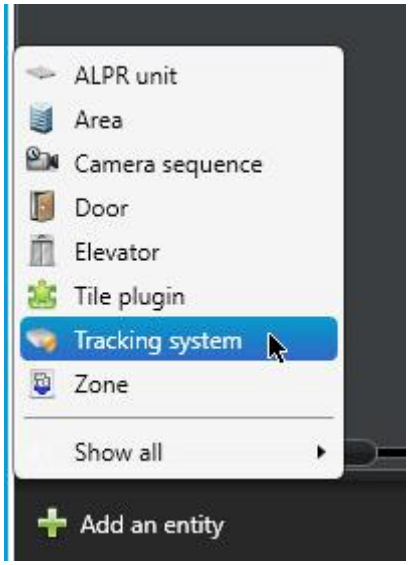
Pour configurer la passerelle des événements, vous devez ouvrir l'outil Genetec Config Tool et accéder au module de configuration « Area View » :



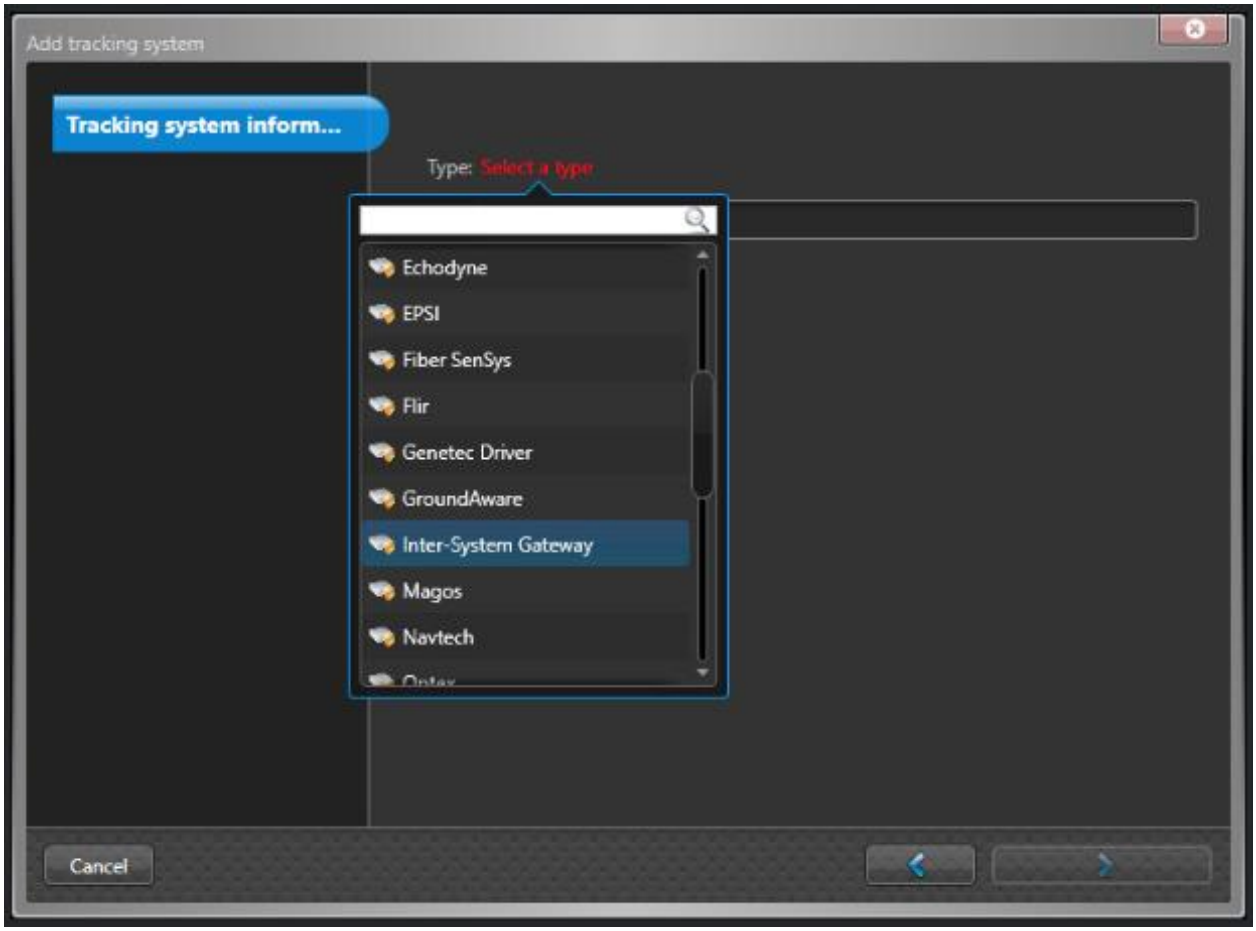
Vous aurez alors accès à cet écran :



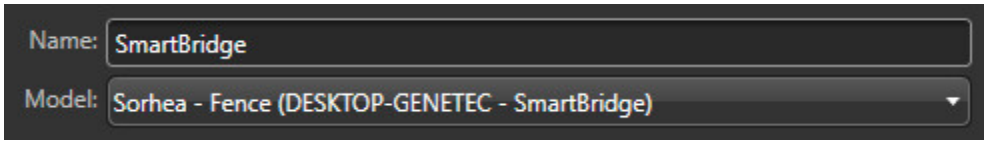
Cliquer sur le bouton Add an entity et choisir Tracking system :



Cliquer sur « Select a type » et choisir « Inter-System Gateway » :

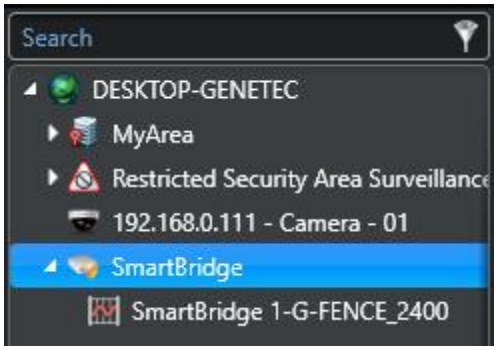


Entrer le nom « SmartBridge » et sélectionner Sorhea – Fence dans le Modèle :



Compléter la configuration avec le bouton Next.

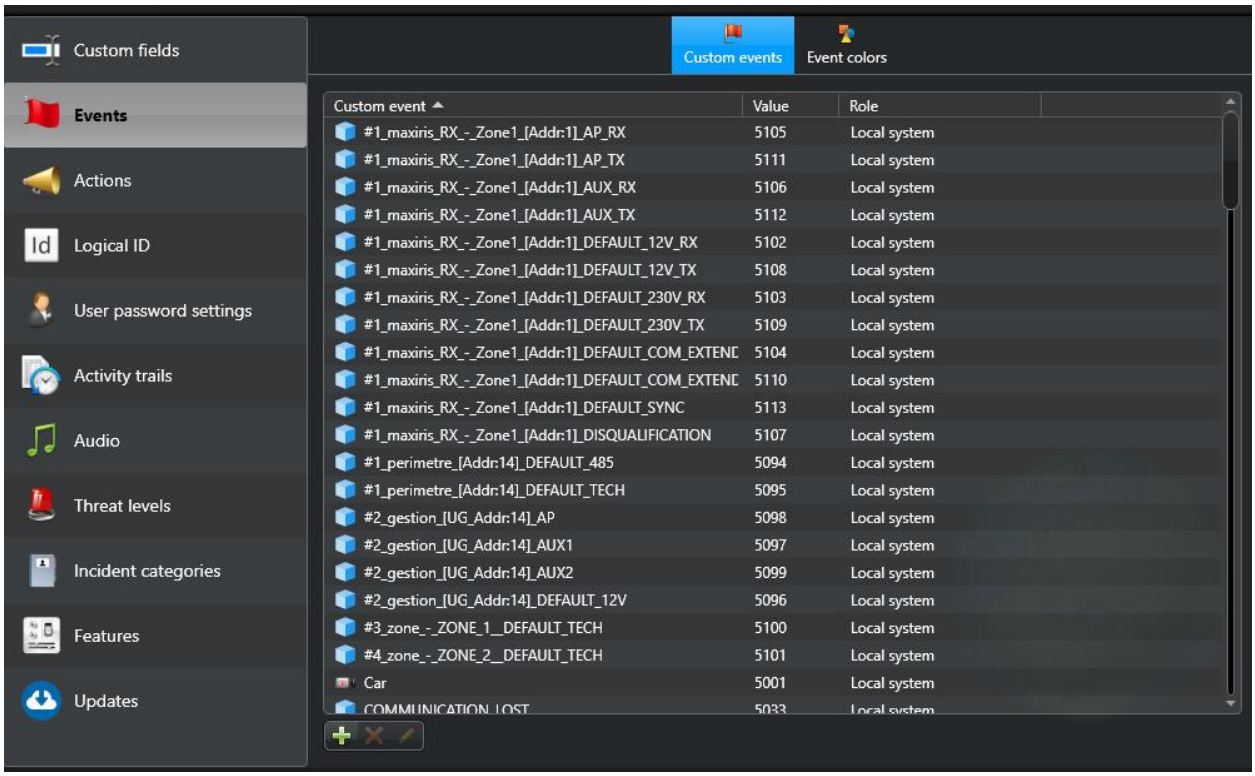
Le SmartBridge devrait alors apparaitre dans la liste. Après quelques instants, les éléments d'intrusion devraient s'afficher sous SmartBridge :



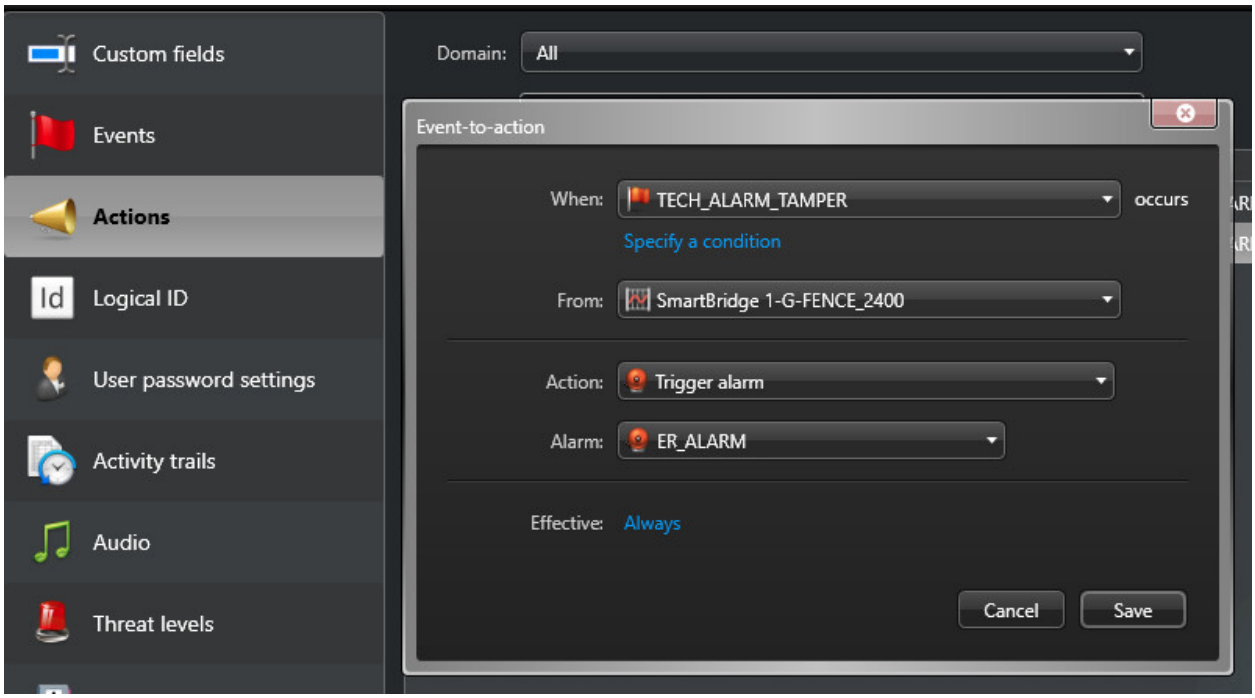
Configuration des événements

Bien que l'utilisation de RSA concerne principalement la détection d'intrusion, les autres événements sont aussi disponibles dans Genetec Security Center. Par exemple, une action peut être exécutée lors d'un événement de type défaut technique.

Lors de l'ajout de l'appareil à l'étape précédente, divers événements ont été ajoutés automatiquement dans Genetec. Il est possible de visualiser ces événements dans la section « Events » :

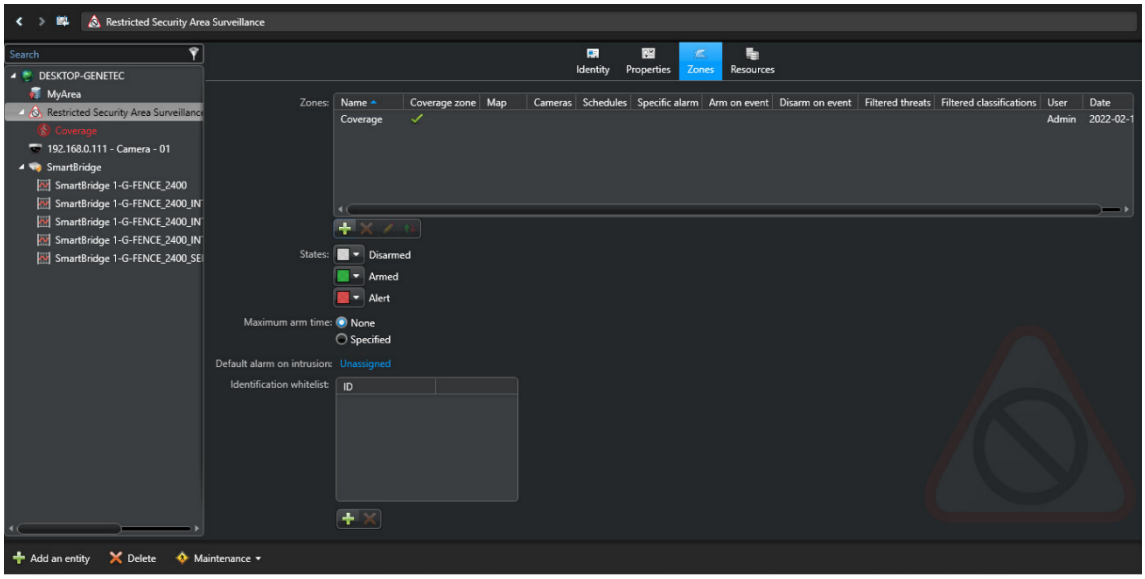


Il est alors possible de traiter ces événements comme tout autre événement de Genetec. Par exemple, pour générer une alarme lors d'un événement « Tamper », il est possible de créer un « Event-to-action » comme suit :

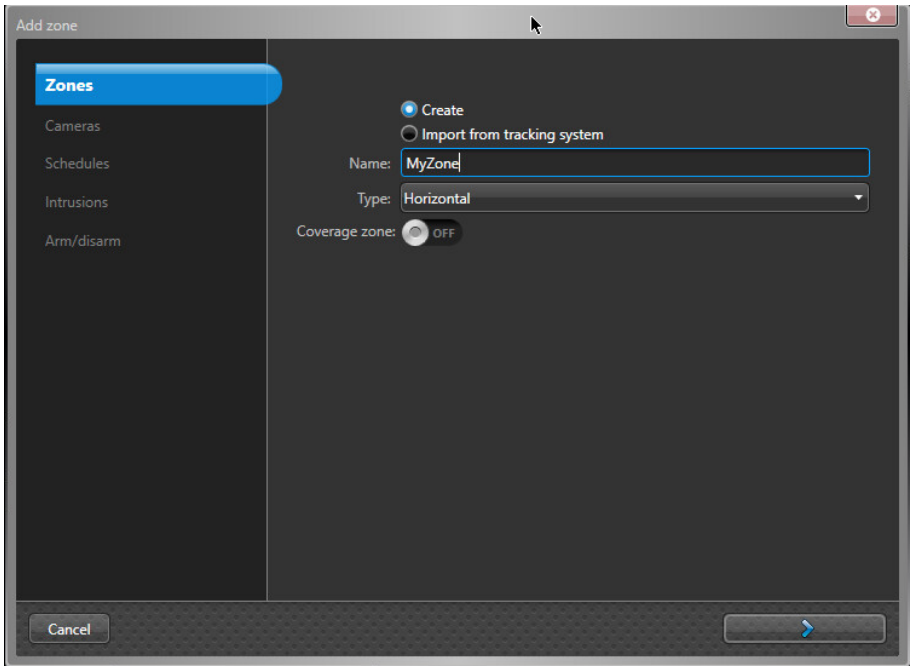


Configuration d'une zone

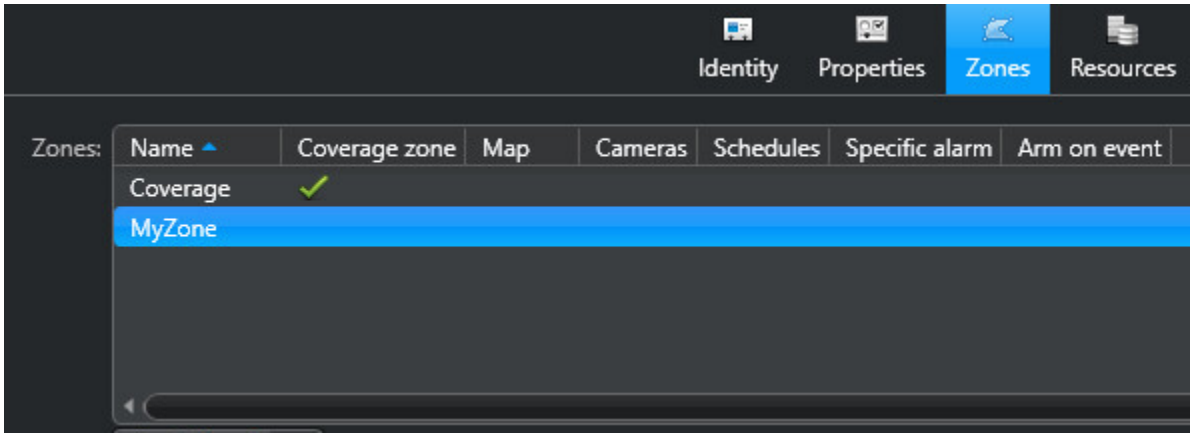
Pour pouvoir utiliser les intrusions sur une carte RSA, il faut d'abord spécifier la zone à surveiller. Dans la section « Restricted Security Area Surveillance », sous l'onglet « Zones », cliquer sur le bouton + afin ajouter une zone :



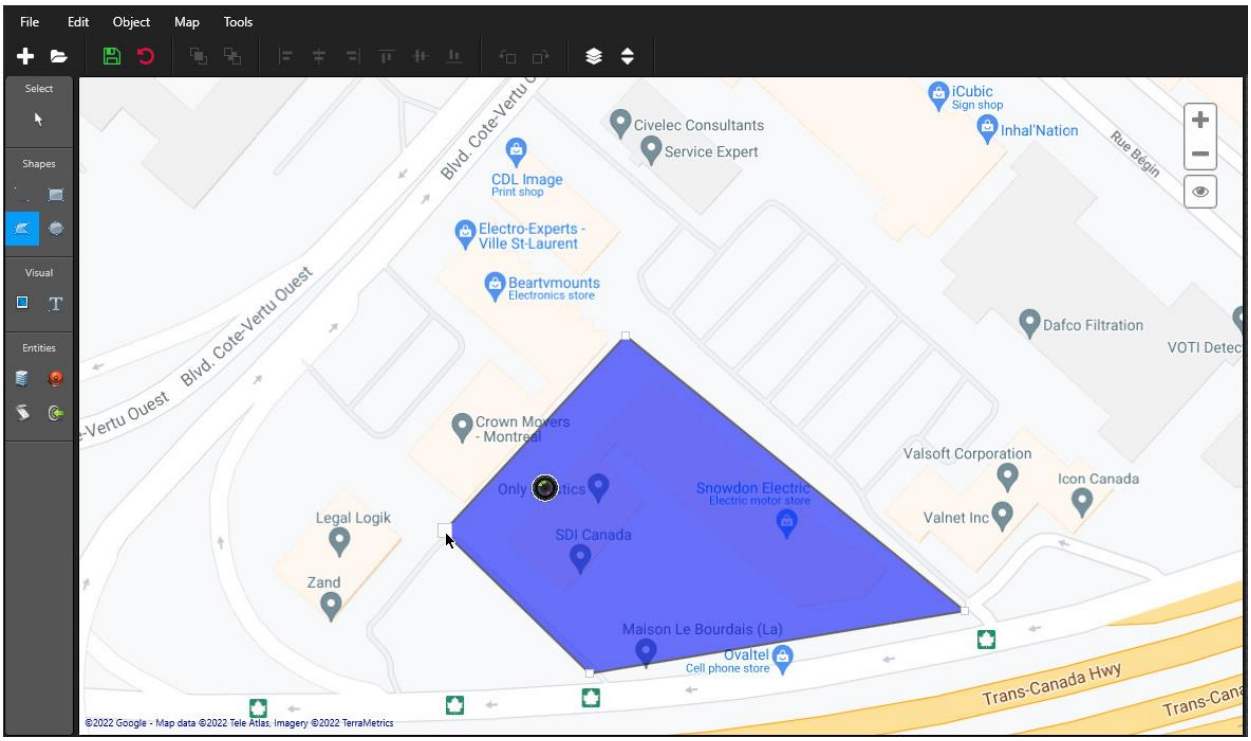
Indiquer le nom de la zone puis cliquer sur le bouton suivant Suivant jusqu'à la fermeture de l'écran :



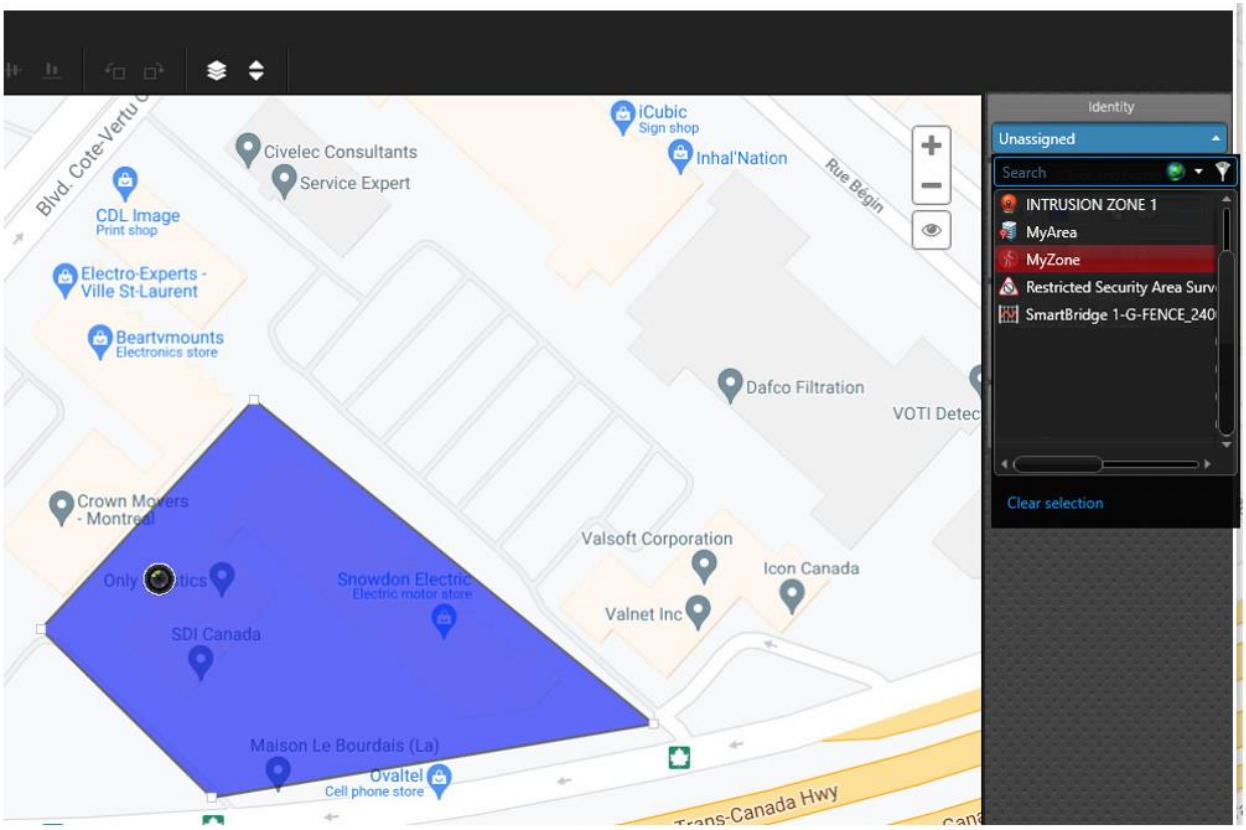
La zone créée sera alors ajoutée :



La prochaine étape consiste à désigner la zone sur la carte. Dans la carte, utiliser le bouton polygone afin de dessiner la zone sur la carte :

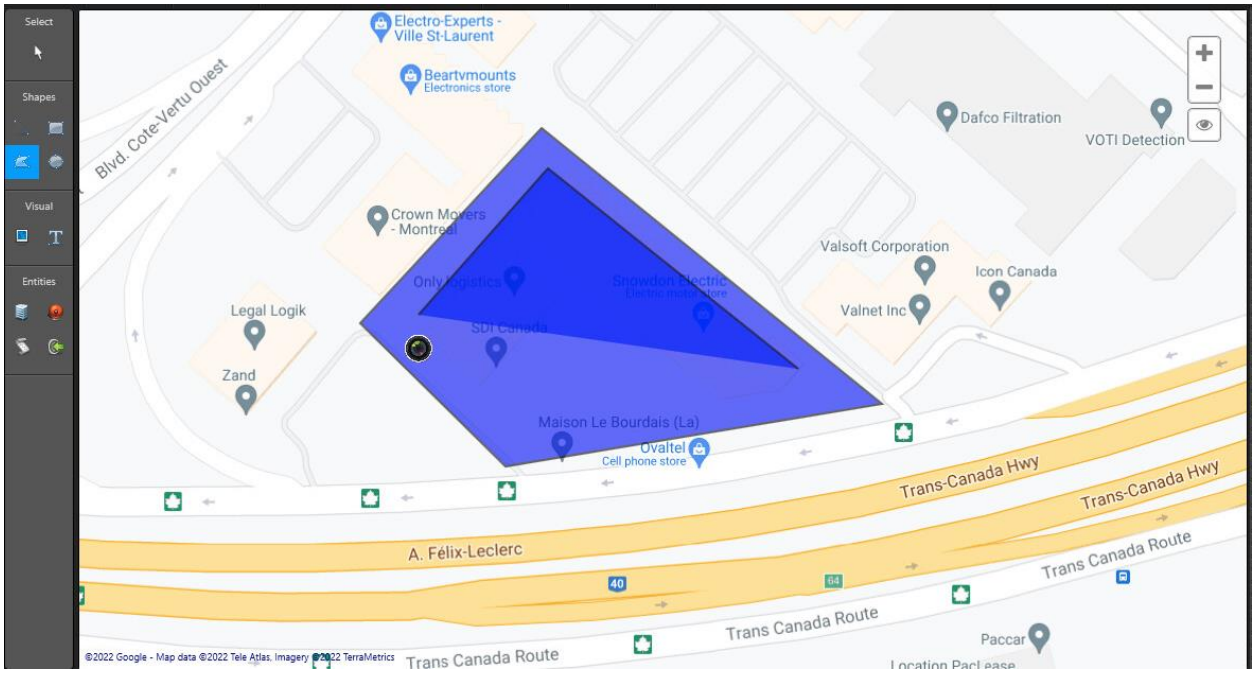


Une fois la zone dessinée, il faut l'assigner à la zone créée précédemment :



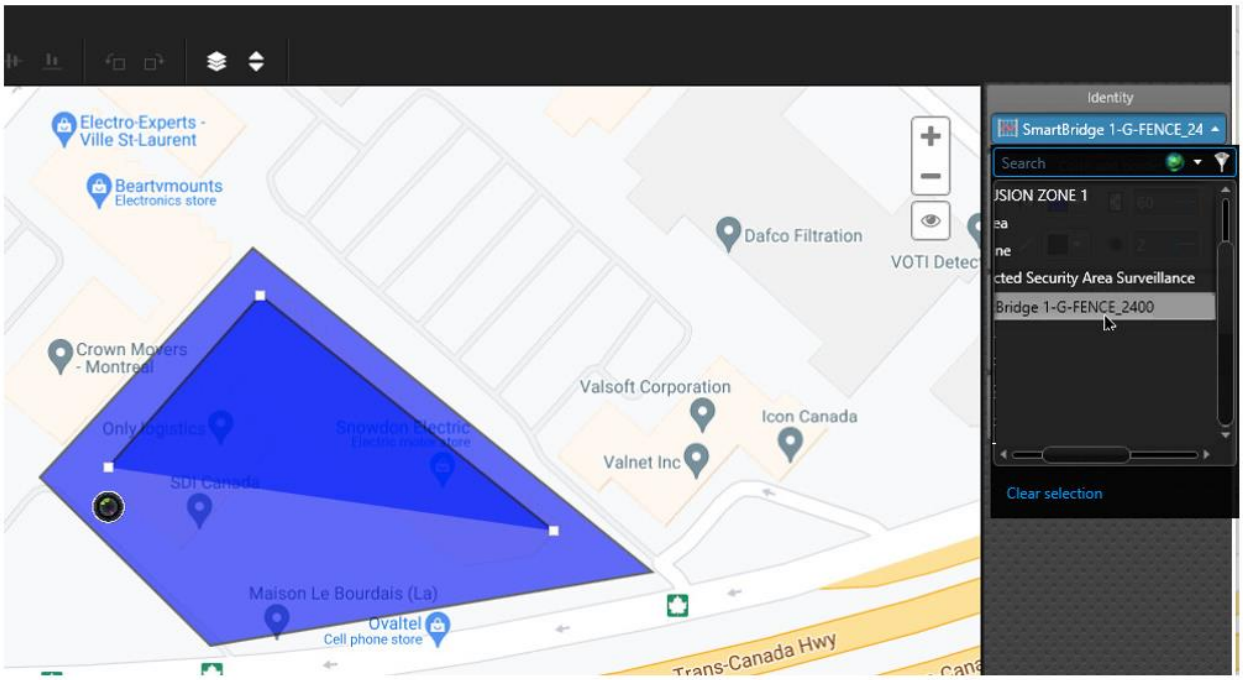
Configuration des intrusions

La configuration des clôtures d'intrusion doit se faire à l'intérieur de la zone à surveillée (zone crée à l'étape précédente). Dans la carte, utiliser le bouton polygone pour dessiner la clôture sur la carte. Dans le cas d'un GFence, l'ordre dans laquelle la zone est dessinée a un impact sur la position des détection. Il faut donc dessiner la zone dans le même ordre des capteurs :



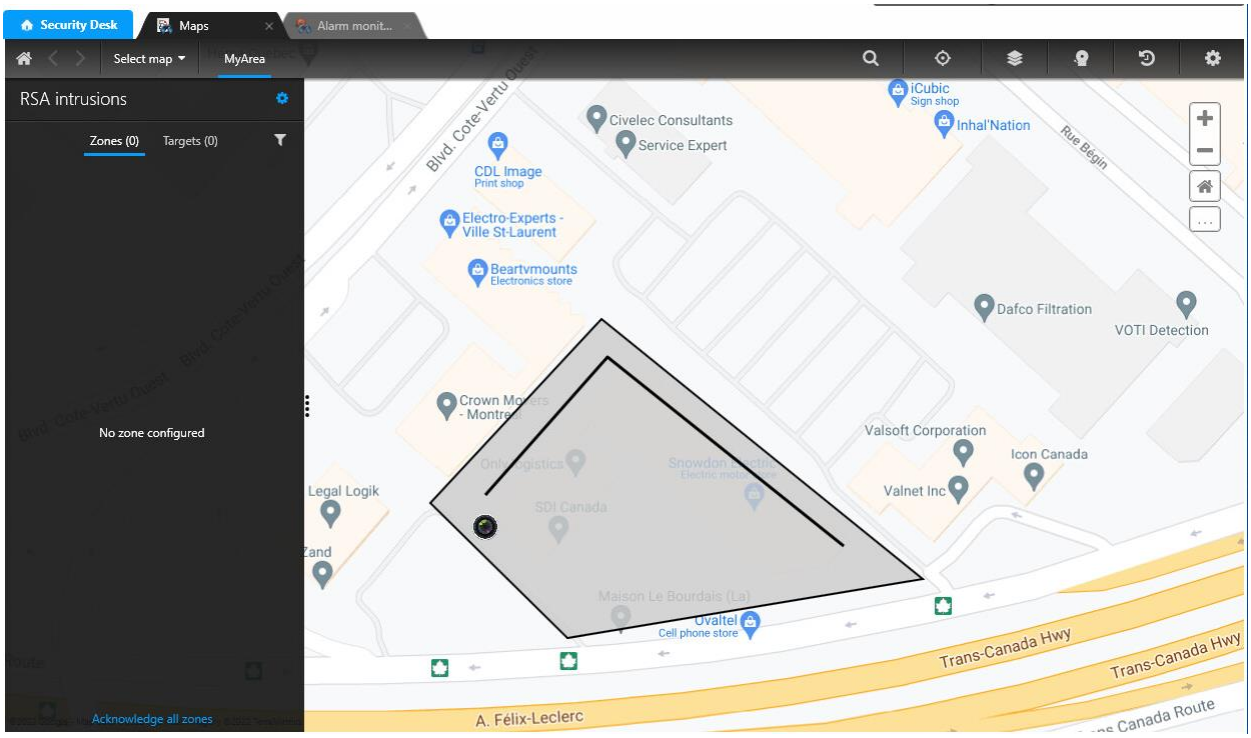
Attention : Tout système doit être dessiné sur la carte sous forme de polygone et non une autre forme.

Une fois le polygone de la clôture dessiné, il faut l'associer à l'appareil :



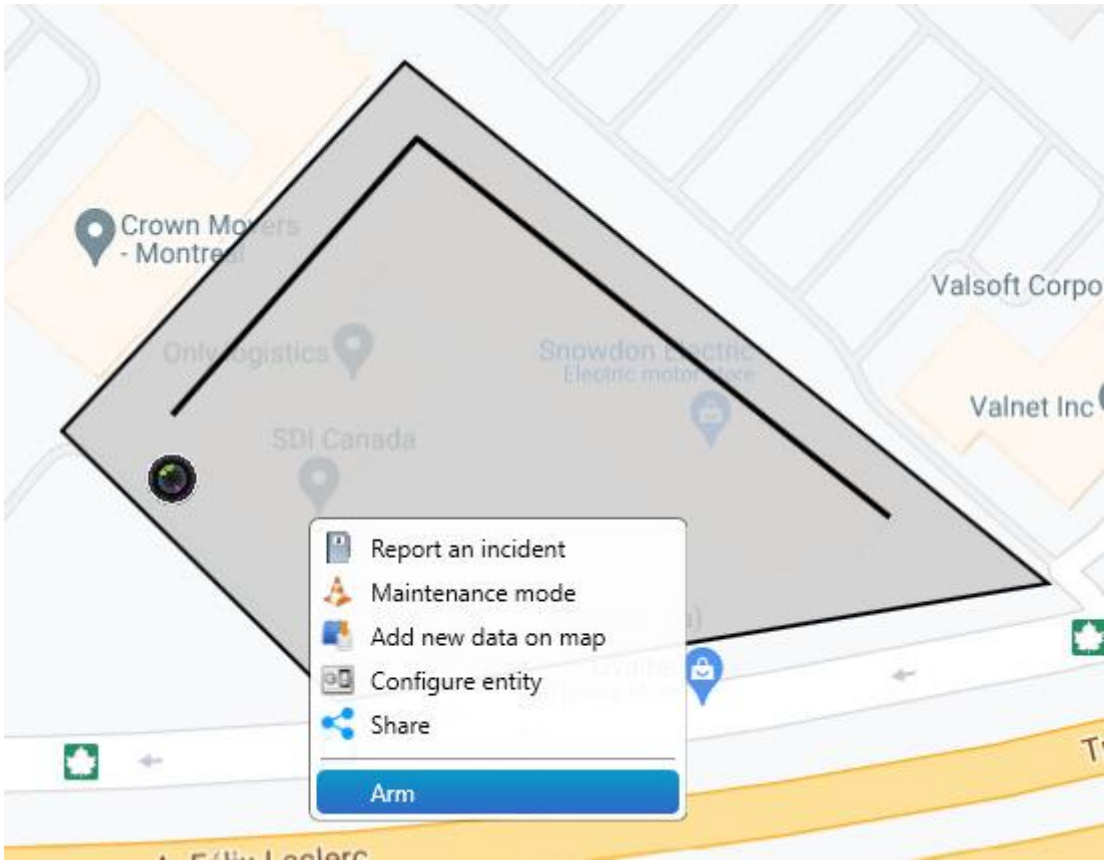
Visualisation des intrusions

Pour valider le fonctionnement en opération, ouvrir Genetec Security Desk puis accéder à la section « Maps » :

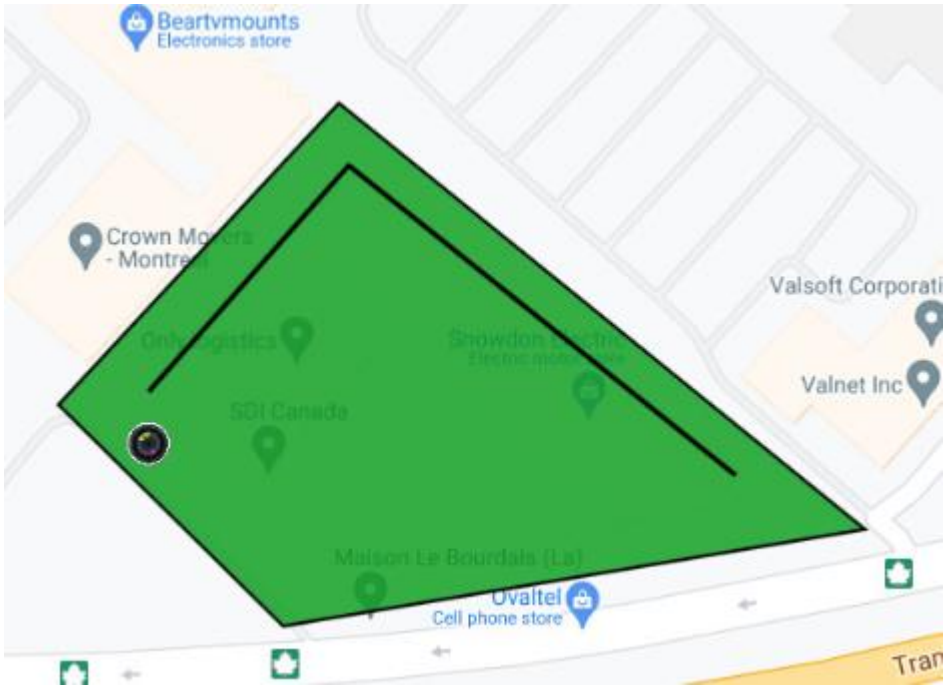


S'assurer que la zone et clôture dessinées précédemment soient visibles dans l'écran.

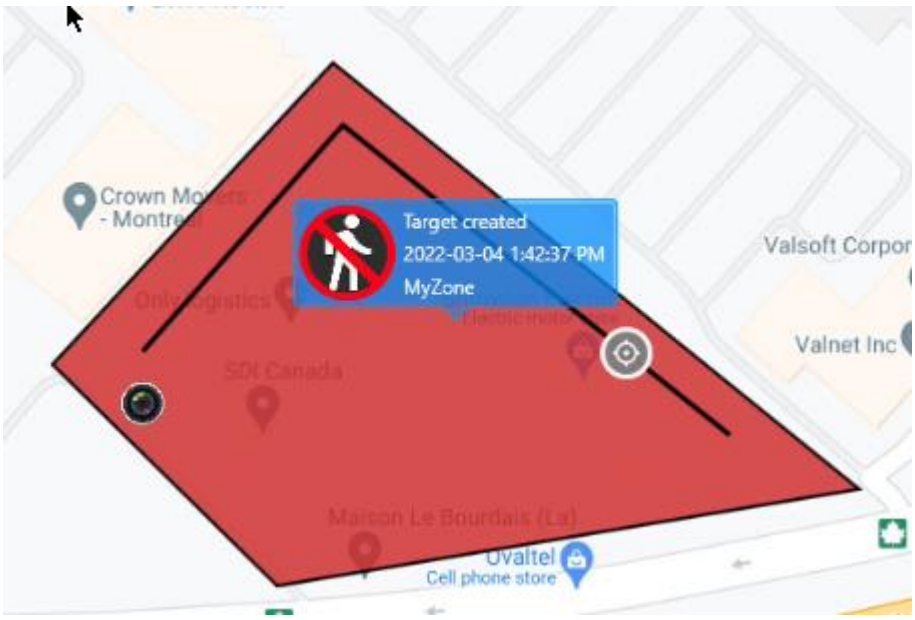
Afin de recevoir les intrusions, il faut armer la zone. Avec le bouton droit de la souris, cliquer sur la zone. Choisir « Arm » dans le menu afin d'armer la zone :



Une fois armée, la zone doit passer au vert :



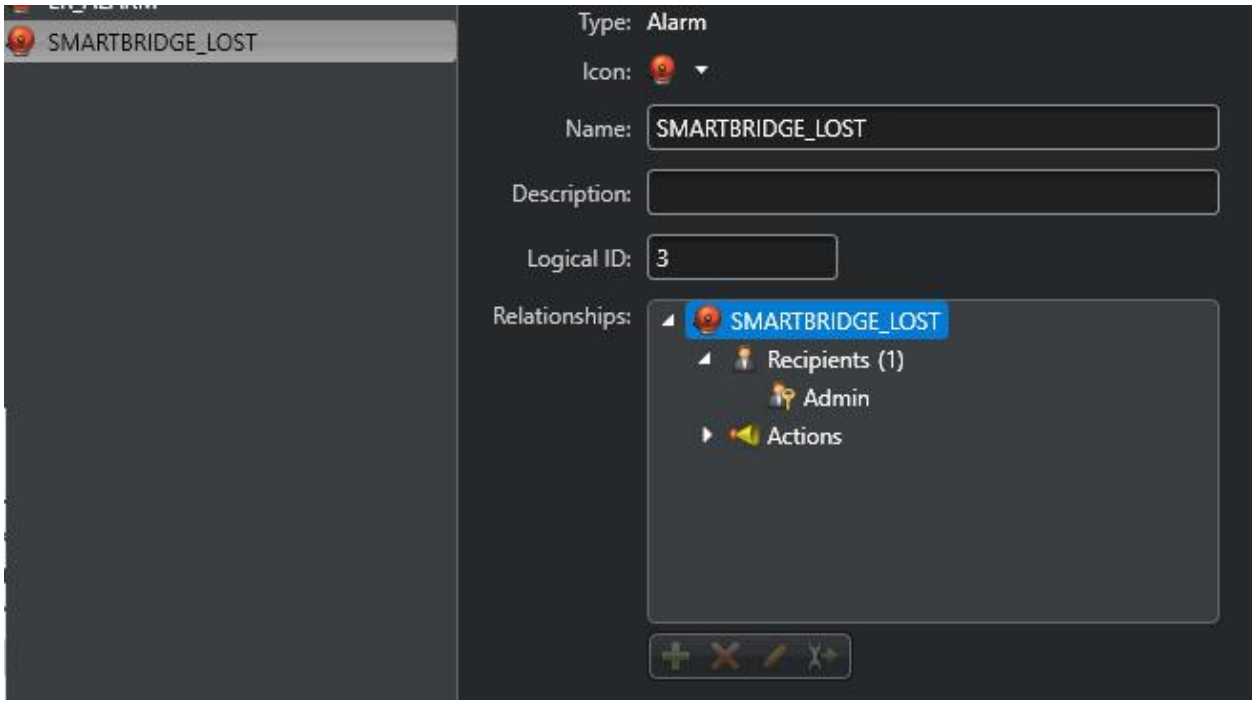
Lors d'une intrusion, la zone passera au rouge et un icone indiquera la position de l'intrusion sur la clôture :



Surveillance du SmartBridge (optionnel)

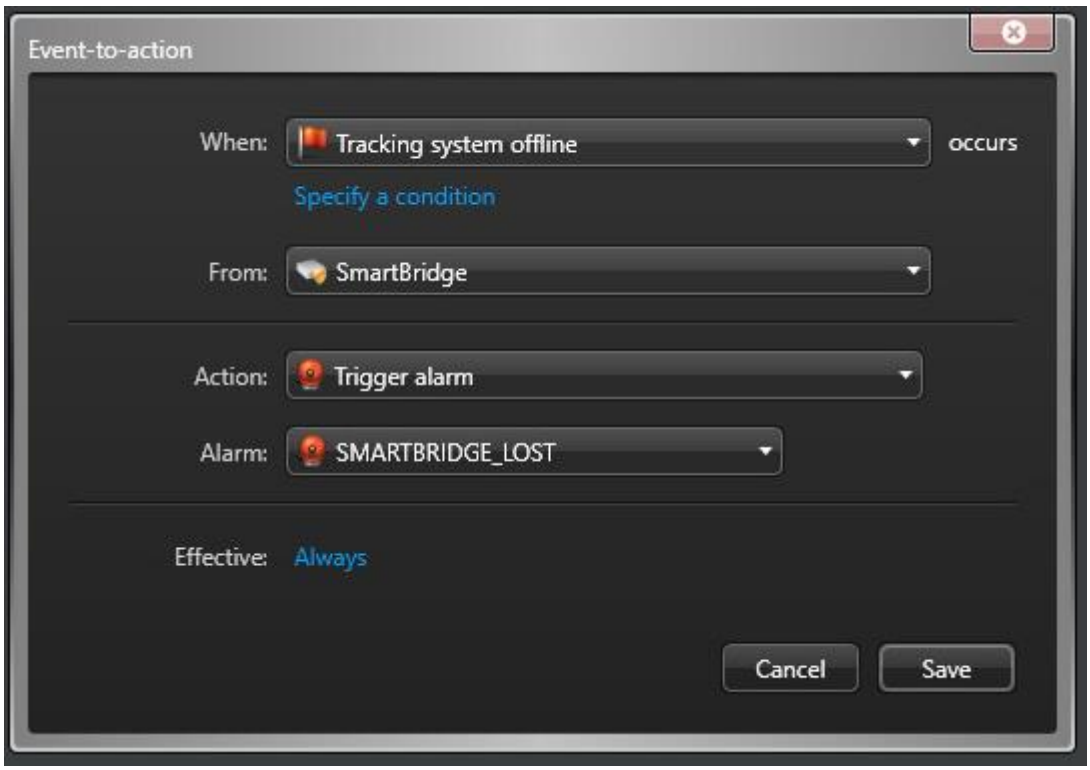
Il est possible d'ajouter un élément de sécurité supplémentaire afin de recevoir une alarme dans Genetec si le processus du SmartBridge ne communique plus. Pour ce faire, il faut créer des événements additionnels.

Tout d'abord, dans l'écran des alarmes, créer une nouvelle alarm et la nommer SMARTBRIDGE_LOST :



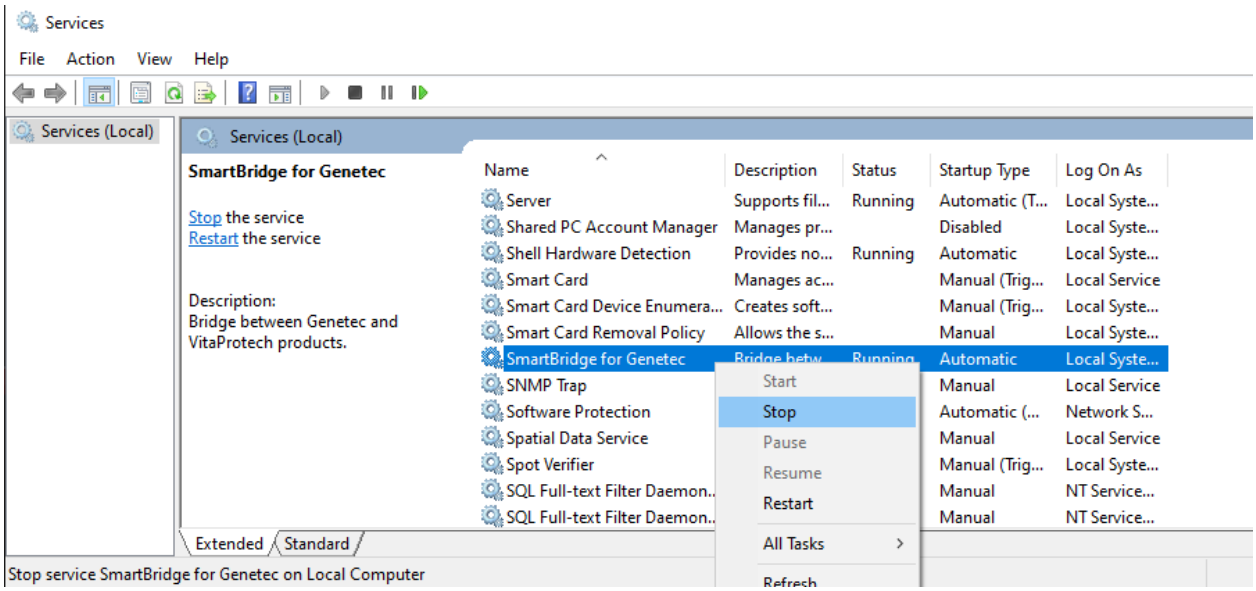
Ajouter Admin comme récipient.

Ensuite, dans l'écran des Actions, créer une nouvelle action comme suit :



Tester le fonctionnement

Afin de valider cette configuration, il faut simuler la perte d'un SmartBridge. Pour ce faire, il suffit d'arrêter le service SmartBridge dans Windows :



Après quelques secondes, l'événement SMARTBRIDGE_LOST devrait s'afficher dans Genetec :