

# SGSE

Soluciones Globales de Seguridad Electrónica

## AEOS INTRUSION MONITOR

Manuel d'installation et d'utilisation

## Table des matières

1.	Version du document.....	2
2.	Introduction.....	3
3.	Architecture.....	4
4.	Installation.....	5
5.	Licenses .....	9
5.1	Obtenir un UID .....	9
5.2	Appliquer la licence .....	9
5.3	Stations de travail (uniquement SmartClient).....	10
6.	Configuration.....	11
6.1	AEOS configuration.....	11
6.1.1	Activer l'interface Socket.....	11
6.1.2	Créer un utilisateur avec les permissions requises.....	11
6.1.3	Définir les détecteurs (AEmon) .....	12
6.1.4	Créer des zones d'intrusion (interface web AEOS Administration).....	13
6.2	Configuration du plugin .....	14
6.2.1	Configurer la connexion .....	14
6.2.2	Type de détecteur .....	15
6.2.3	Définition des alarmes.....	15
6.2.4	Règles – événements .....	16
6.2.5	Règles – Actions .....	18
6.2.6	RPermissions de rôles .....	20
7.	Utilisation .....	21
7.1	Visionneuse d'événements/alarmes et Gestionnaire d'alarmes .....	21
7.2	Cartes.....	22
7.3	Vue en arborescence du panneau latéral .....	25
7.4	Web client et Milestone Mobile.....	25
8.	Dépannage .....	27

## 1. Version du document

<b>Version</b>	<b>Date</b>	<b>Auteur</b>	<b>Description</b>
<b>1.0</b>	01/2022	SDA	Première version du document

## 2. Introduction

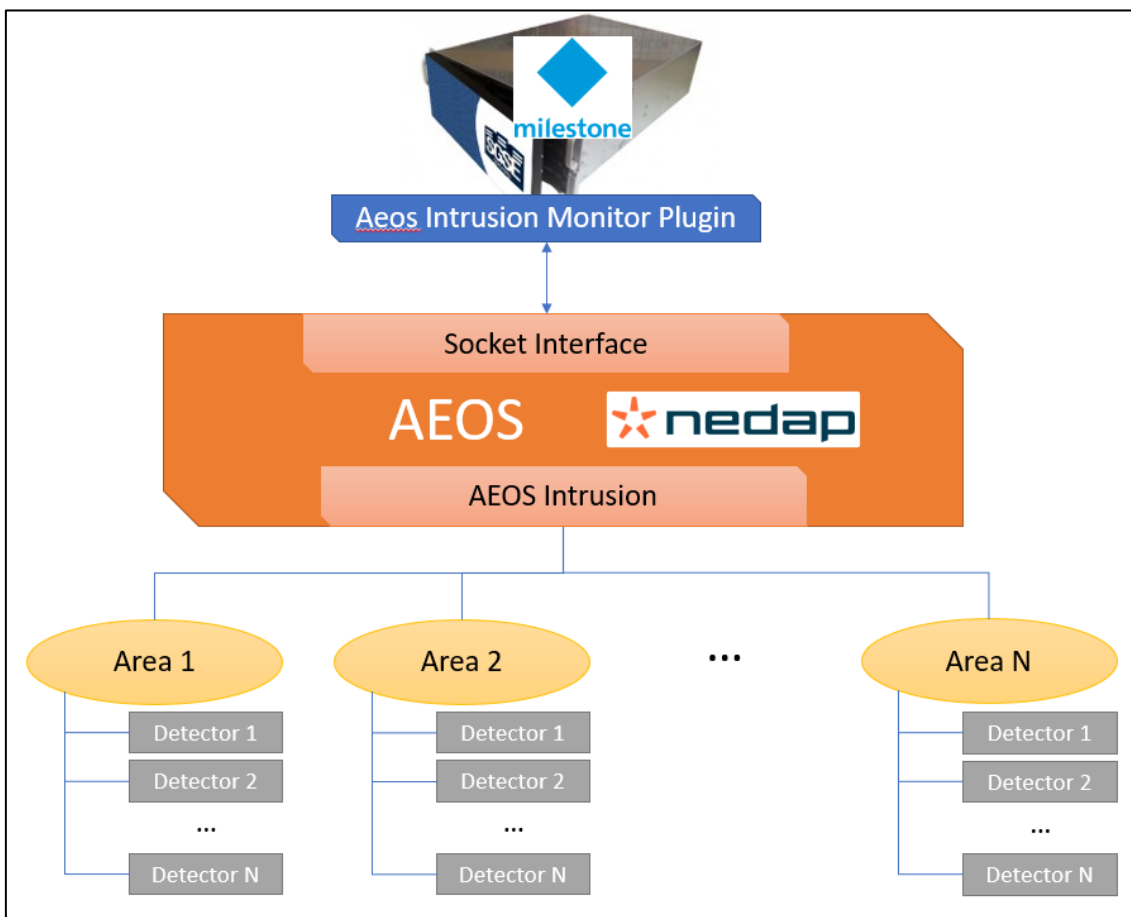
L'objectif de ce document est d'expliquer le fonctionnement, l'installation et l'utilisation de la solution logicielle appelée "AEOS Intrusion Monitor".

Cette solution consiste en un plugin qui permet de surveiller et d'interagir avec la solution AEOS Intrusion (de Nedap), depuis l'interface utilisateur et l'environnement de travail de la plateforme XProtect® de Milestone.

De cette manière, la surveillance du système d'intrusion est disponible avec les avantages du VMS XProtect® pour la gestion vidéo et d'alarme. CCTV et intrusion dans une interface unique.

### 3. Architecture

L'architecture de la solution est décrite dans le schéma ci-dessous:



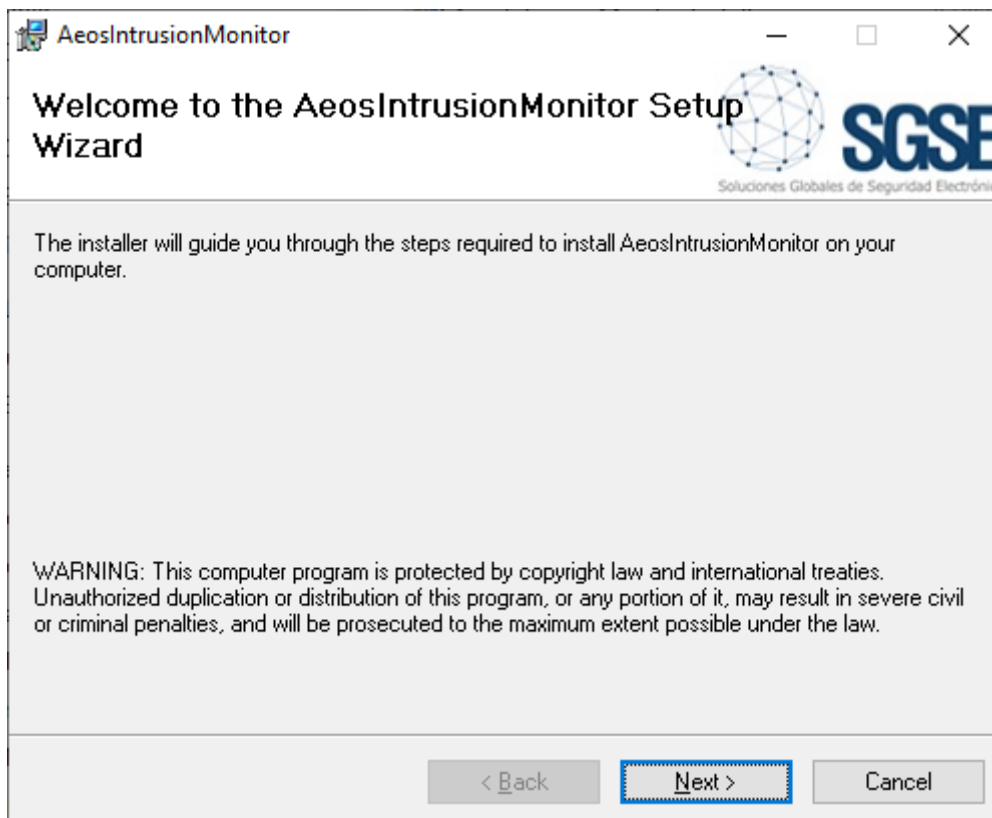
À travers le réseau Ethernet, le plugin se connecte au système AEOS via son API Socket Interface. AEOS doit être correctement configuré pour accepter les connexions et les requêtes du plugin.

Une fois la communication établie, le plugin importera la configuration AEOS Intrusion (zones et détecteurs) et créera les éléments correspondants dans Milestone. La connexion reste ouverte pour:

- ✓ Envoyer des commandes au système AEOS Intrusion.
- ✓ Mettre à jour les icônes des éléments de Milestone pour montrer l'état actuel du système d'intrusion.
- ✓ Déclencher des événements liés à l'intrusion dans Milestone au fur et à mesure qu'ils se produisent dans le système AEOS Intrusion.

## 4. Installation

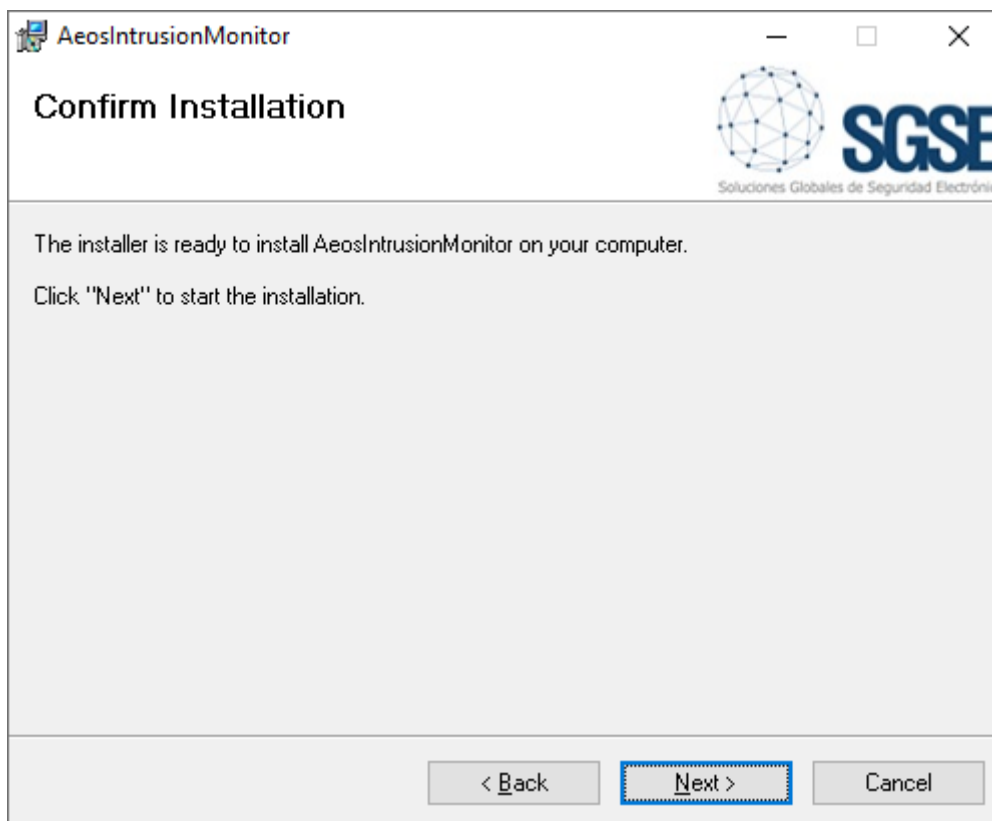
Pour installer le plugin, il suffit d'exécuter avec des droits d'administrateur l'installateur "AEOS Intrusion Monitor Installer.msi" fourni par SGSE ou téléchargé depuis le Milestone Marketplace. Le processus est automatique. Tout au long des différentes étapes de l'installateur, nous n'aurons qu'à accepter le contrat de licence de l'utilisateur final, une condition obligatoire pour pouvoir utiliser le plugin.



Cliquez sur "Next >" pour démarrer le processus d'installation.

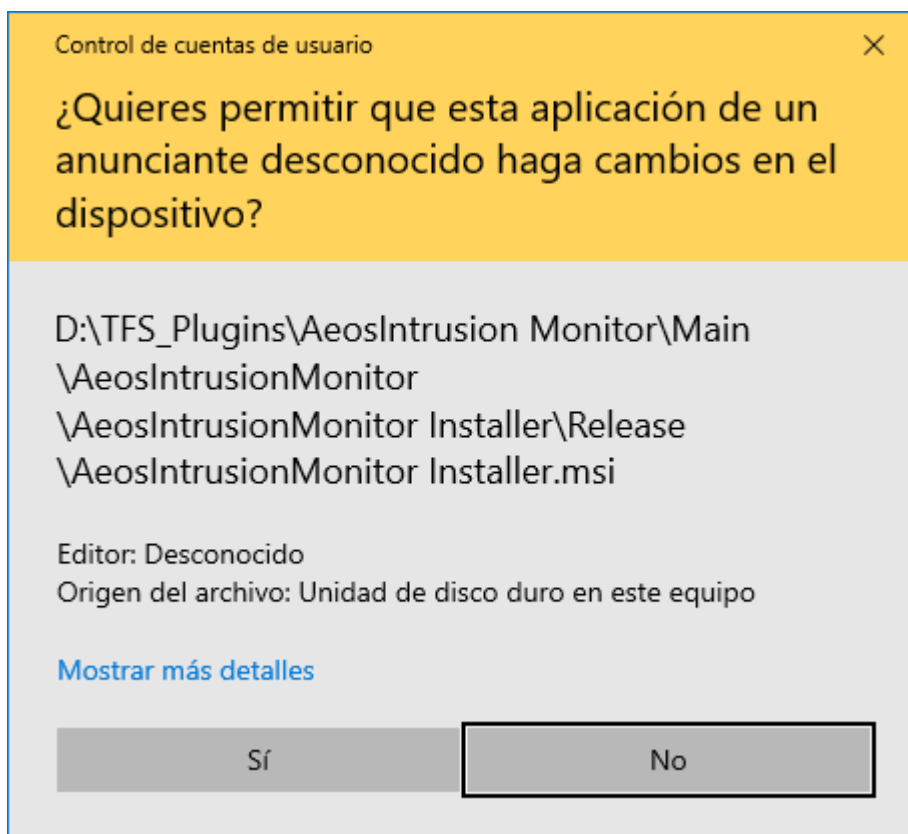


Vous devez lire et accepter le contrat de licence de l'utilisateur final pour poursuivre l'installation.

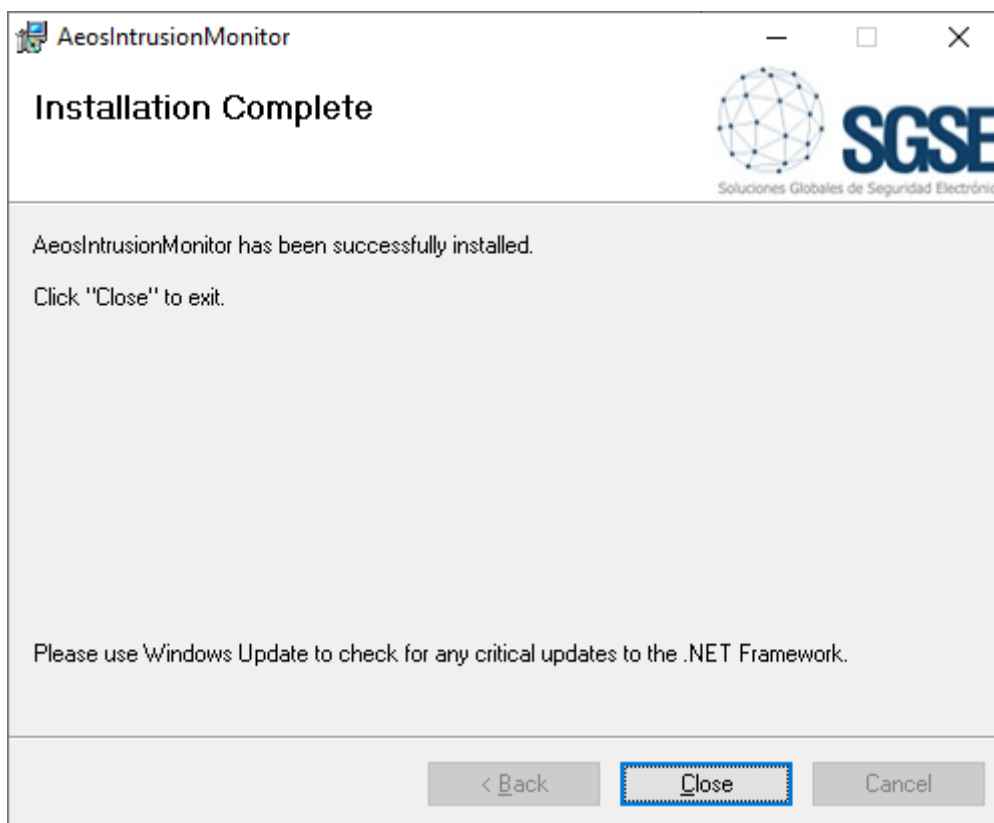


Cliquez sur "Next >" pour continuer et installer les fichiers du plugin.

Si le contrôle de compte d'utilisateur Windows est activé, vous devrez peut-être autoriser l'installateur à poursuivre l'installation.







Une fois le processus terminé, vous pouvez cliquer sur “Close”. Le plugin est déjà installé!

**NOTE:** si vous avez installé le plugin alors que Milestone XProtect était en fonctionnement, un redémarrage du serveur d'événements et de toute application cliente (Management Client, Smart Client) sera nécessaire.

## 5. Licenses

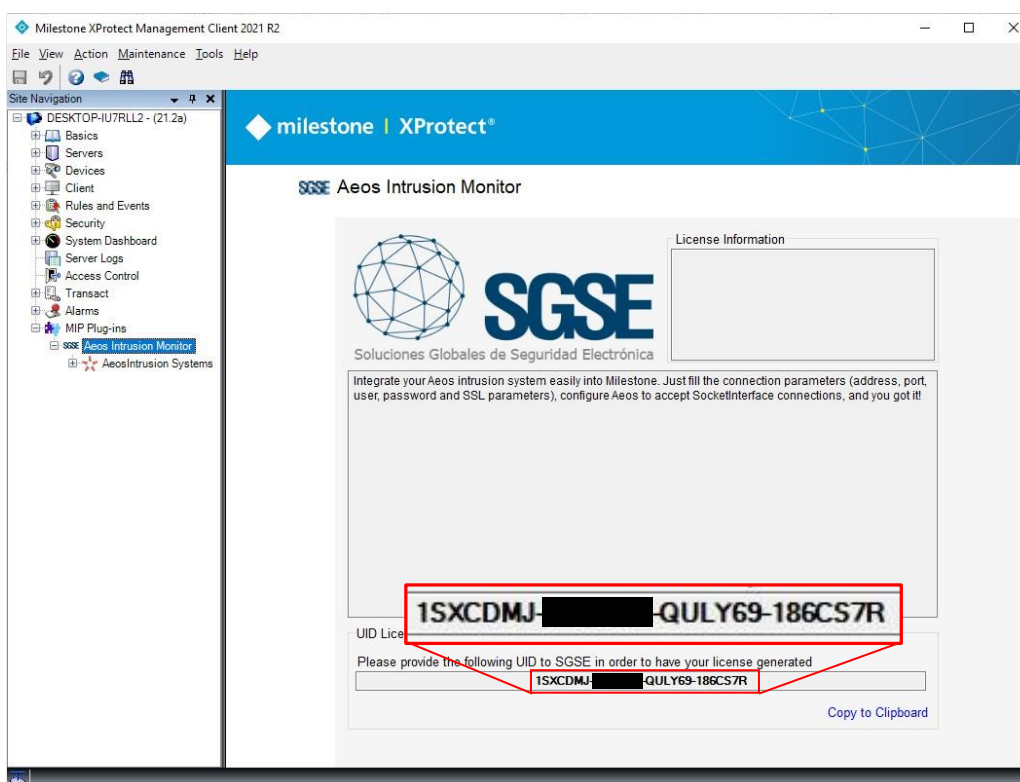
Le plugin nécessite une licence pour fonctionner. Chaque système AEOS doit être licencié. Ces licences sont générées par SGSE. La procédure pour obtenir le fichier de licence correspondant à la licence acquise est décrite ci-dessous. La licence est également liée au nombre de détecteurs existant dans les systèmes AEOS Intrusion.

### 5.1 Obtenir un UID

Pour générer la licence, vous devez fournir l'UID correspondant. Cet UID est un identifiant unique auquel la licence est liée.

Pour obtenir ce code, vous devez exécuter XProtect® Management Client après avoir installé le plugin et aller à l'élément de menu correspondant (MIP Plugins > AeosIntrusion Monitor).

Sur cet écran, lorsque le plugin n'est pas licencié, vous verrez l'UID correspondant.



Veuillez fournir cet UID à SGSE, et vous recevrez votre fichier de licence généré.

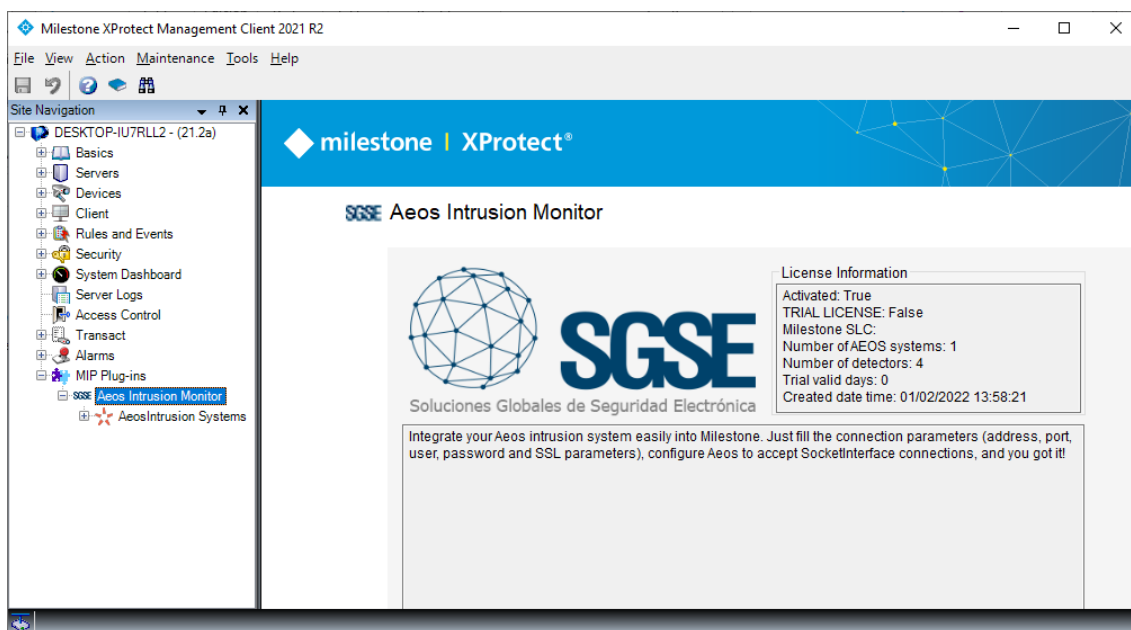
### 5.2 Appliquer la licence

Veuillez copier le fichier de licence "Licencia.lic" dans le dossier du plugin. Par défaut:

C:\Program Files\Milestone\MIPPlugins\AeosIntrusionMonitor\

Après avoir appliqué la licence, le serveur d'événements doit être redémarré pour que les changements prennent effet et que nous puissions utiliser le plugin.

Une fois la licence appliquée, l'interface Management Client affichera les informations de la licence:



### 5.3 Stations de travail (uniquement SmartClient)

Pour générer l'UID sur une station de travail où vous n'avez pas XProtect® Management Client, mais où vous utiliserez uniquement SmartClient, vous devrez utiliser l'outil SGSE, "UID Generator" pour obtenir l'UID.

Veuillez contacter le support SGSE pour obtenir cet outil.

## 6. Configuration

### 6.1 Configuration AEOS

Le plugin AEOS Intrusion Monitor utilise l'API "Socket Interface" d'AEOS. Pour que le plugin fonctionne correctement, une configuration doit être effectuée dans le système AEOS.

#### 6.1.1 Activer l'interface Socket

Pour activer l'API AEOS Socket Interface, vous devez configurer le fichier `aeos.properties`.

1. Ouvrez le fichier `aeos.properties` (...\\AEOS\\AEserver\\standalone\\configuration).
2. Recherchez la section suivante:

```
#####  
# aeos.service.InterfaceService  
#####  
aeos.service.InterfaceService.Port=8035  
aeos.service.InterfaceService.UseSSL=false  
aeos.service.InterfaceService.SSLClientAuth=false  
aeos.service.InterfaceService.SocketTimeoutSeconds=0  
aeos.service.InterfaceService.DelegateSubscriptions=true  
aeos.service.InterfaceService.RMITimeoutMinutes=480
```

3. Vérifiez les paramètres suivants:

a. Numéro de port: Le service d'interface AEOS écoute sur un port pour les connexions socket. Le numéro de port est 8035 par défaut. Si nécessaire, vous pouvez changer ce numéro. Ce port sera nécessaire dans la configuration du plugin. \_

b. UseSSL (connexion SSL/TLS): Définissez cette valeur sur `true` si vous souhaitez utiliser une connexion sécurisée SSL/TLS avec l'interface Socket AEOS. Assurez-vous que le certificat SSL/TLS correct est installé du côté du système externe de la connexion. Sans le certificat correct, la connexion sécurisée SSL/TLS ne fonctionnera pas.

c. RMITimeout: Il s'agit du paramètre de timeout pour les connexions RMIAdapter. Après ce délai, la session d'un utilisateur connecté devient invalide. À l'accès, une exception est lancée. Ce délai est défini en minutes. La valeur par défaut est de 480 minutes (8 heures). Vous pouvez changer cette valeur selon votre préférence. Lorsque la valeur est définie à 0, les sessions n'expirent pas du tout.

Lorsque vous avez modifié ces paramètres:

1. Enregistrez le fichier `aeos.properties`.
2. Redémarrez le serveur d'applications AEOS.

#### 6.1.2 Créer un utilisateur avec les permissions requises

Un rôle utilisateur peut être défini pour n'exécuter que des fonctions appartenant à l'interface Socket. Pour cela, connectez-vous à l'interface de maintenance AEOS et allez à Management/System users/Maintain user role. Créez un nouveau rôle ou assignez les fonctions liées à la connexion Socket (comme listé ci-dessous) à un rôle existant:

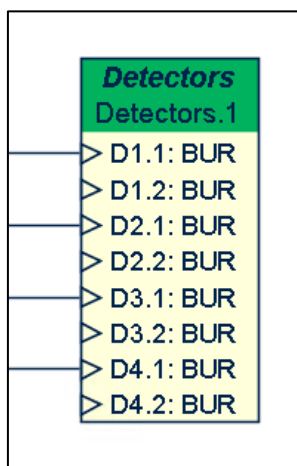
- Configuration, Socketconnection, Commands
- Configuration, Socketconnection, Events

Enfin, assignez ce rôle utilisateur à un utilisateur. Cet utilisateur avec son mot de passe sera nécessaire dans la configuration du plugin.

Pour plus d'informations sur la configuration de l'interface Socket, veuillez vous référer au manuel "AEOS Socket Interface Installation and Configuration".

### 6.1.3 Définir les détecteurs (AEmon)

En utilisant l'outil AEmon, définissez les détecteurs du système d'intrusion en utilisant les composants de comportement Intrusion > Detectors. Pour plus d'informations sur la configuration et l'installation d'AEOS Intrusion, veuillez vous référer au manuel "AEOS – Intrusion Installation and Configuration" ou à votre distributeur Nedap.

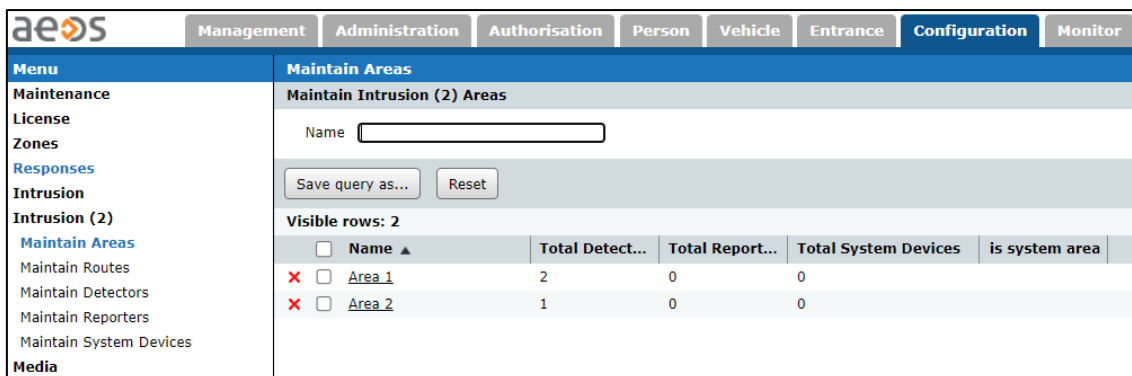


**NOTE:** en plus des détecteurs AEbc eux-mêmes, il est nécessaire d'ajouter un TaggedServiceManager pour que l'interface Socket rapporte les éléments d'intrusion au plugin.

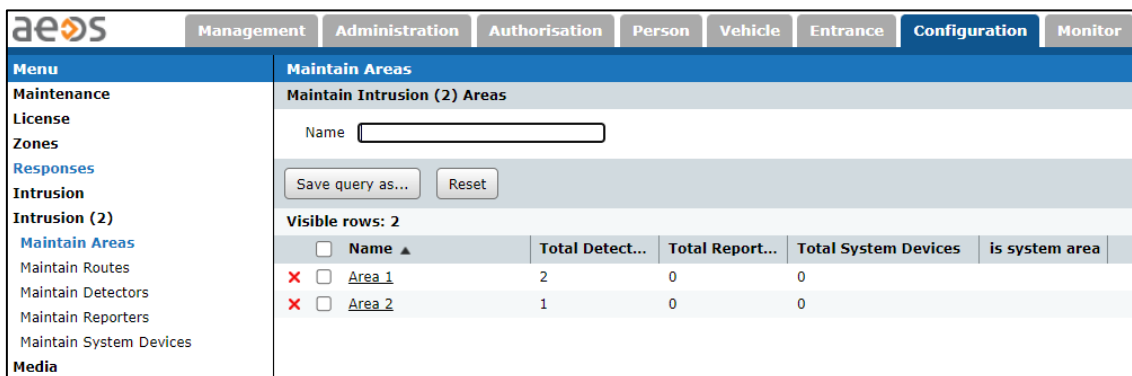


### 6.1.4 Créer des zones d'intrusion (interface web AEOS Administration)

En utilisant l'interface web d'administration AEOS, créez des zones d'intrusion et assignez-leur les détecteurs définis.



aeos						
Menu		Maintain Areas				
Maintenance		Maintain Intrusion (2) Areas				
License		Name <input type="text"/>				
Zones		Save query as... <input type="button" value="Reset"/>				
Responses		Visible rows: 2				
Intrusion		<input type="checkbox"/> Name ▲	Total Detect...	Total Report...	Total System Devices	is system area
Intrusion (2)		<input checked="" type="checkbox"/> Area 1	2	0	0	
Maintain Areas		<input checked="" type="checkbox"/> Area 2	1	0	0	
Maintain Routes						
Maintain Detectors						
Maintain Reporters						
Maintain System Devices						
Media						



aeos						
Menu		Maintain Areas				
Maintenance		Maintain Intrusion (2) Areas				
License		Name <input type="text"/>				
Zones		Save query as... <input type="button" value="Reset"/>				
Responses		Visible rows: 2				
Intrusion		<input type="checkbox"/> Name ▲	Total Detect...	Total Report...	Total System Devices	is system area
Intrusion (2)		<input checked="" type="checkbox"/> Area 1	2	0	0	
Maintain Areas		<input checked="" type="checkbox"/> Area 2	1	0	0	
Maintain Routes						
Maintain Detectors						
Maintain Reporters						
Maintain System Devices						
Media						

Pour plus d'informations sur la configuration du système d'intrusion, veuillez vous référer au manuel "AEOS – Intrusion Installation and Configuration".

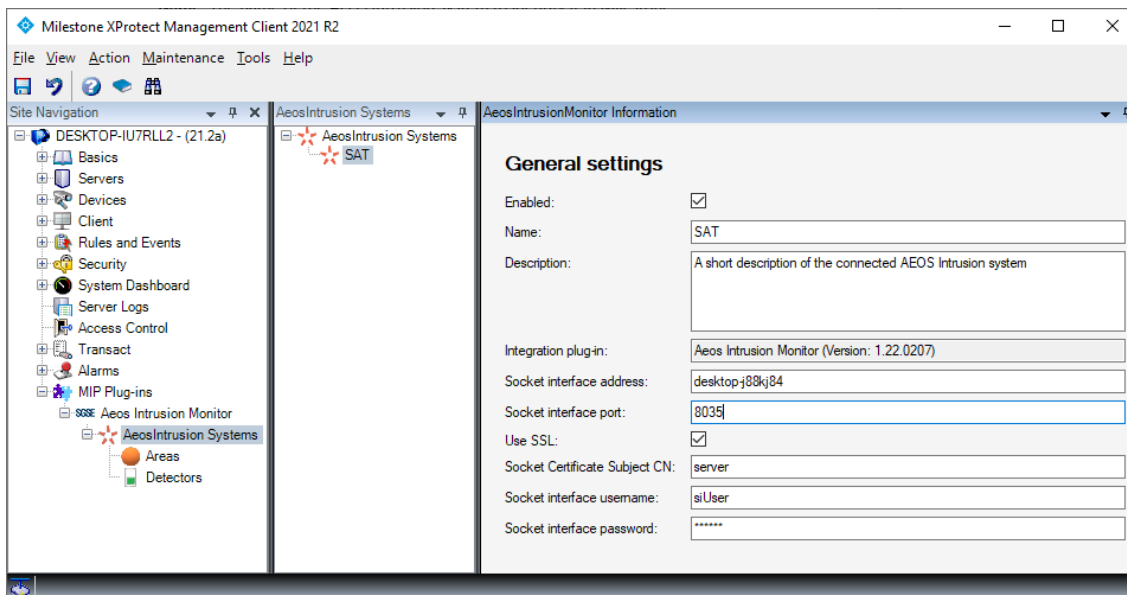
## 6.2 Configuration du plugin

### 6.2.1 Configurer la connexion

Du côté du plugin, nous devons configurer la connexion au système AEOS Intrusion. Cette configuration de connexion doit correspondre et dépendra de la configuration du serveur AEOS.

Les paramètres requis sont affichés sur l'image ci-dessous et sont les suivants :

- **Activé:** Utilisez cette case à cocher pour activer ou désactiver l'interaction avec le système AEOS Intrusion dans Milestone.
- **Nom:** Le nom du système AEOS Intrusion pour l'identifier dans Milestone.
- **Description:** Une description du système d'intrusion AEOS.
- **Adresse de l'interface Socket:** Le nom d'hôte ou l'adresse IP du serveur AEOS où l'API de l'interface socket écoute.
- **Port de l'interface Socket:** Le port sur lequel l'interface socket écoute.
- **Utiliser SSL:** Utilisez cette case à cocher pour indiquer au plugin si SSL est utilisé dans la connexion à l'interface socket.
- **Sujet du certificat Socket CN:** En cas d'utilisation de SSL, ce champ doit contenir le nom commun qui apparaît dans le certificat SSL du serveur AEOS.
- **Nom d'utilisateur de l'interface Socket:** Le nom d'utilisateur pour se connecter à AEOS via l'interface socket.
- **Mot de passe de l'interface Socket:** Le mot de passe de l'utilisateur utilisé pour se connecter à AEOS via l'interface socket.



Une fois que le plugin a été correctement configuré, il récupère automatiquement les zones et les détecteurs définis dans AEOS Intrusion et crée les éléments correspondants dans Milestone (un rafraîchissement des données en appuyant sur F5 peut être nécessaire pour voir les éléments dans le Management Client).

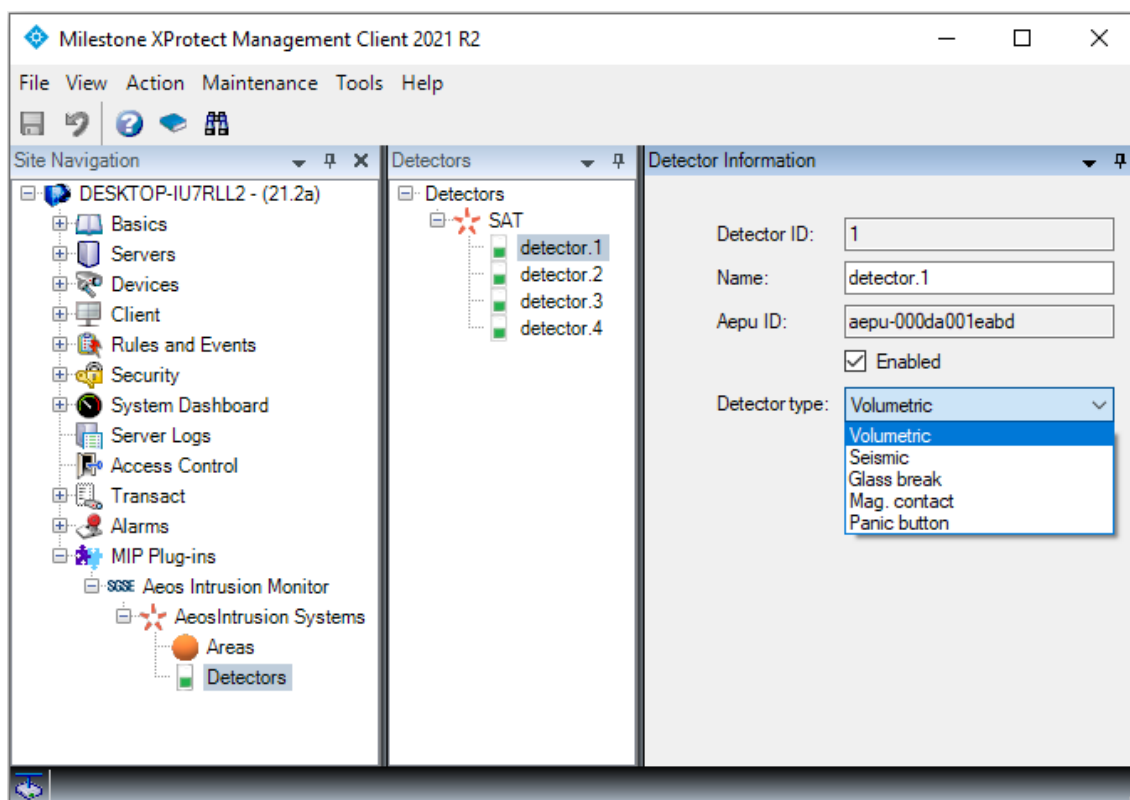
Aucune configuration supplémentaire n'est requise pour que le plugin fonctionne, bien qu'un certain réglage fin puisse être souhaité pour que les opérateurs aient une meilleure compréhension du système d'intrusion et pour obtenir une intégration complètement utile, comme spécifier le type de détecteurs ou définir les alarmes qui doivent être déclenchées lors de la réception des événements liés à l'intrusion AEOS.

### 6.2.2 Type de détecteur

L'icône par défaut pour les détecteurs est un détecteur volumétrique. Le plugin permet à l'utilisateur de définir le type de détecteur en sélectionnant parmi un ensemble de types. Cela changera les icônes des détecteurs sur les cartes Smart Client.

Pour changer le type de détecteur, allez simplement à l'élément détecteur lui-même dans le Management Client, puis sélectionnez le type de détecteur dans les options déroulantes. Les types de détecteurs disponibles sont :

- Volumétrique (PIR) – Valeur par défaut
- Sismique
- Bris de glace
- Contact magnétique
- Bouton panique

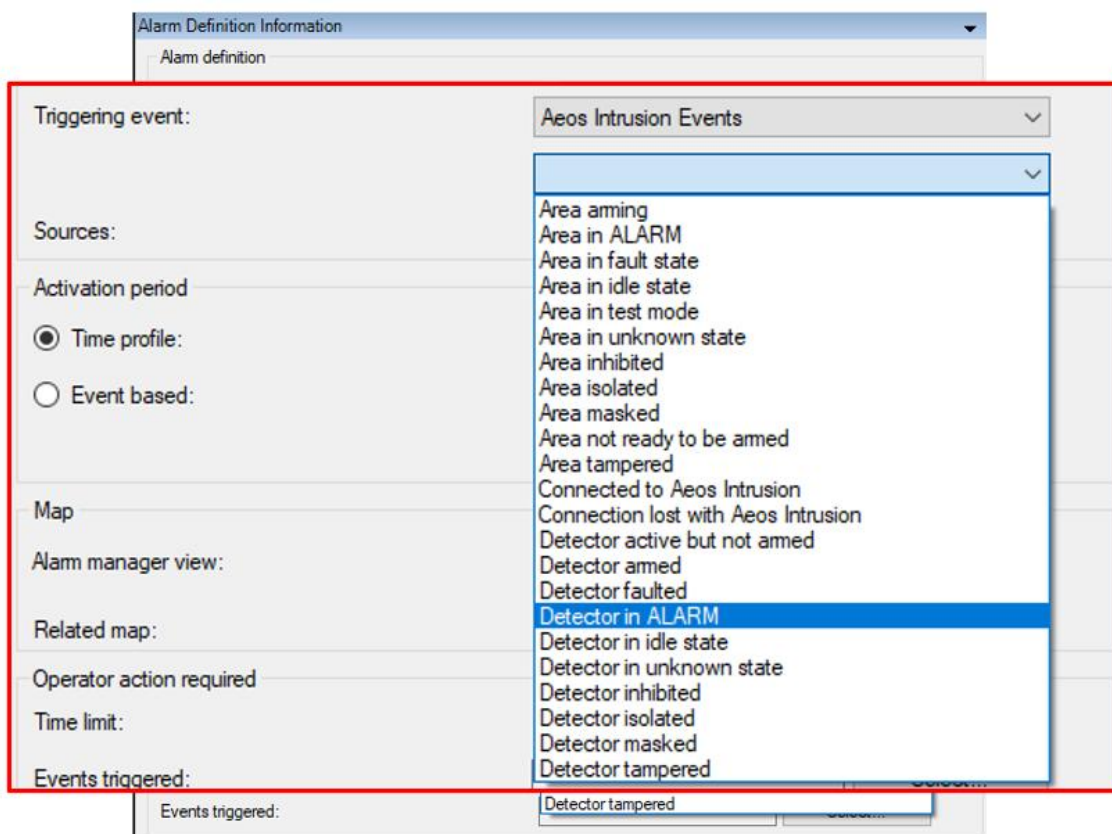


Depuis cette page, vous pouvez également voir avec quel AEpu le détecteur est associé dans AEOS, et changer le nom du détecteur dans Milestone, pour une meilleure compréhension de l'opérateur.

### 6.2.3 Définition des alarmes

Le plugin définit un ensemble d'événements déclenchés par l'intégration AEOS Intrusion. Ces événements peuvent être utilisés pour définir lesquels, lorsqu'ils sont déclenchés par des sources spécifiques, doivent être considérés comme des alarmes. Il vous suffit d'aller dans la section "Définition des alarmes", dans le Management Client, et de créer une nouvelle alarme dont l'événement déclencheur est un événement du groupe d'événements AEOS Intrusion et de spécifier l'élément ou les éléments pour lesquels vous souhaitez que cet événement soit considéré comme une alarme.





Les événements disponibles sont listés dans la section suivante.

À titre d'exemple, vous pouvez définir une alarme dans Milestone lorsque l'événement "Détecteur en ALARME" est déclenché par n'importe quel détecteur (en sélectionnant tous les détecteurs). De cette manière, chaque fois qu'un détecteur passe en état d'alarme dans les systèmes AEOS Intrusion, une alarme sera déclenchée dans Milestone.

#### 6.2.4 Règles – événements

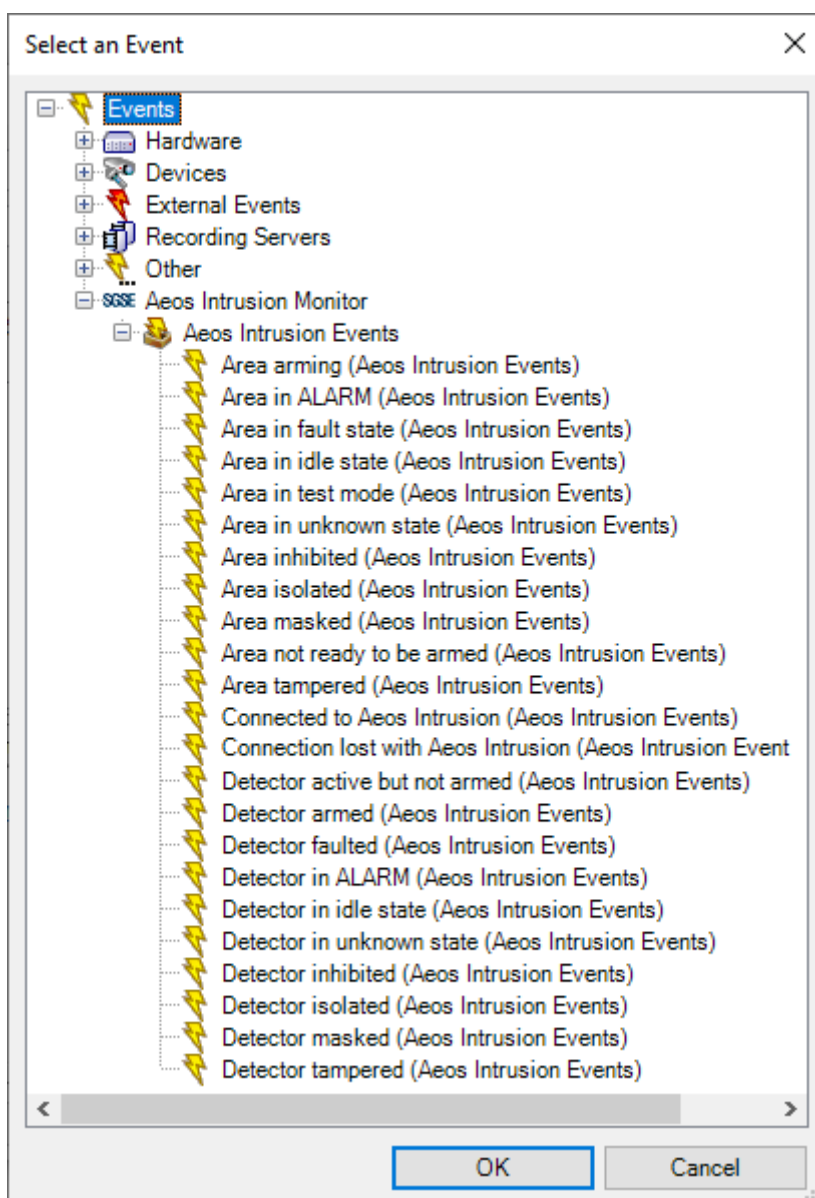
Les mêmes événements qui peuvent être définis comme des alarmes peuvent également être utilisés pour déclencher des règles dans Milestone. Créez simplement une règle et sélectionnez comme "Événement déclencheur" un événement parmi ceux ajoutés par le plugin.

Les événements actuellement pris en charge par le plugin sont :

- Armement de zone
- Zone en ALARME
- Zone en état de défaut
- Zone en état de repos
- Zone en mode test
- Zone en état inconnu
- Zone inhibée
- Zone isolée
- Zone masquée
- Zone non prête à être armée
- Zone altérée
- Connexion établie au système AEOS Intrusion

- Connexion perdue avec le système AEOS Intrusion
- Détecteur actif mais non armé
- Détecteur armé
- Détecteur en défaut
- Détecteur en ALARME
- Détecteur en état de repos
- Détecteur en état inconnu
- Détecteur inhibé
- Détecteur isolé
- Détecteur masqué
- Détecteur altéré

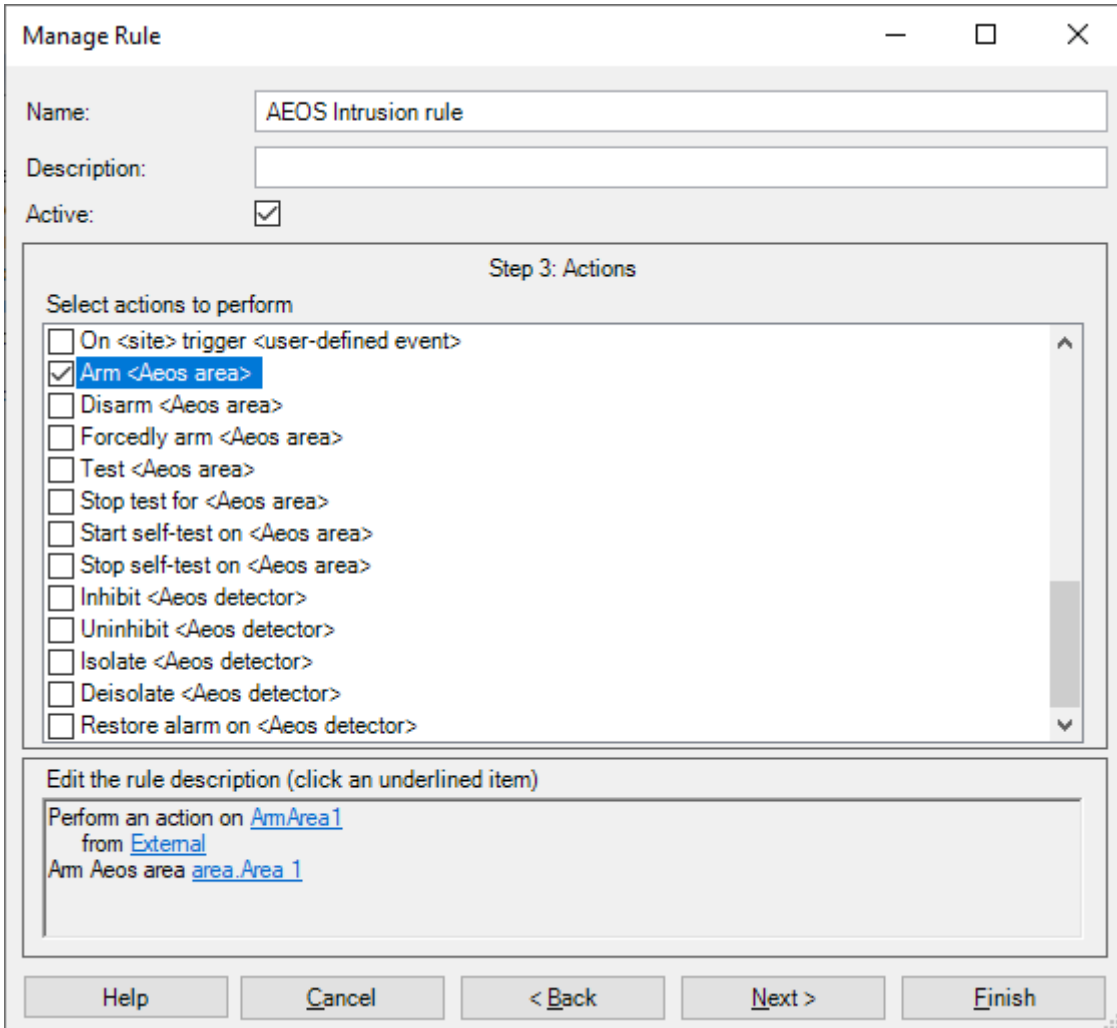
À titre d'exemple, vous pouvez vouloir déplacer une caméra PTZ vers un préréglage spécifique lorsqu'un des détecteurs, par exemple, le couloir arrière, est actif (il détecte quelque chose) mais que la zone n'est pas armée, donc ce n'est pas une alarme. Vous pouvez alors créer une règle pour que l'événement "Détecteur actif mais non armé" provenant du détecteur situé dans le couloir arrière soit l'événement déclencheur, et comme action, vous déplacez la caméra PTZ associée vers le préréglage qui surveille le couloir arrière.



### 6.2.5 Règles – Actions

Le plugin ajoute également des Actions à exécuter dans le système AEOS Intrusion lorsqu'une règle définie est déclenchée par un événement dans Milestone. Vous pouvez définir des règles pour exécuter les actions suivantes sur le système AEOS Intrusion:

- Armer une zone
- Désarmer une zone
- Armer une zone de force
- Tester une zone
- Arrêter le test sur une zone
- Démarrer l'auto-test sur une zone
- Arrêter l'auto-test sur une zone
- Inhiber un détecteur
- Désinhiber un détecteur
- Isoler un détecteur
- Désisoler un détecteur
- Restaurer les alarmes sur un détecteur



**Manage Rule** [ - ] [ □ ] [ × ]

Name:

Description:

Active:

**Step 3: Actions**

Select actions to perform

- On <site> trigger <user-defined event>
- Arm <Aeos area>**
- Disarm <Aeos area>
- Forcedly arm <Aeos area>
- Test <Aeos area>
- Stop test for <Aeos area>
- Start self-test on <Aeos area>
- Stop self-test on <Aeos area>
- Inhibit <Aeos detector>
- Uninhibit <Aeos detector>
- Isolate <Aeos detector>
- Deisolate <Aeos detector>
- Restore alarm on <Aeos detector>

Edit the rule description (click an underlined item)

Perform an action on ArmArea1  
from External  
Arm Aeos area area.Area.1

Buttons: Help | Cancel | < Back | Next > | Finish

### 6.2.6 Permissions de rôle

Milestone permet d'assigner des rôles aux utilisateurs et de leur donner des permissions spécifiques. Le plugin AEOS Intrusion ajoute la possibilité d'assigner des permissions sur les différents éléments du système d'intrusion AEOS, par groupe ou par élément spécifique. Des permissions spécifiques peuvent également être définies.

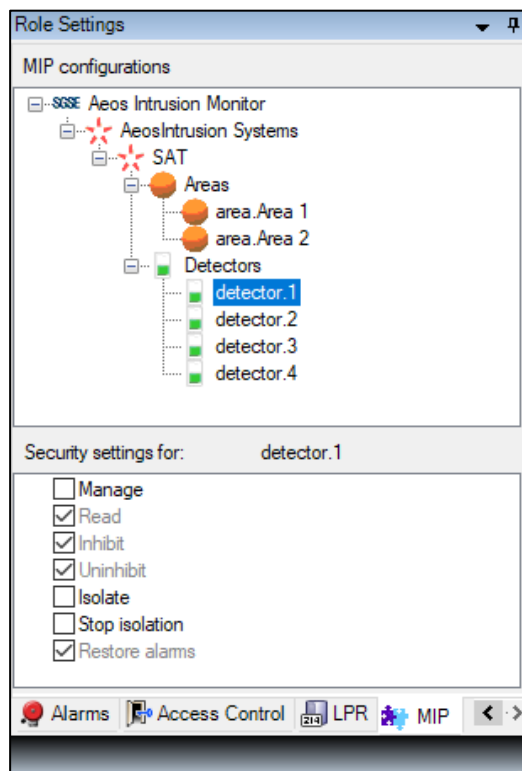
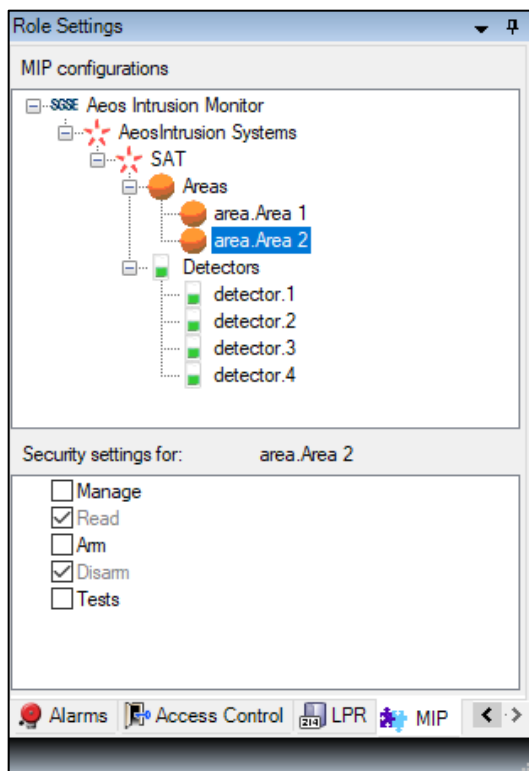
Vous pouvez définir les permissions de lecture génériques, afin que l'utilisateur puisse voir les éléments et leurs alarmes associées. Et pour définir comment les utilisateurs du rôle peuvent interagir avec les éléments d'intrusion, vous avez des permissions séparées à choisir.

Pour les zones, vous pouvez spécifier les permissions spécifiques suivantes:

- Armer
- Désarmer
- Tests

Pour les détecteurs, vous pouvez spécifier les permissions spécifiques suivantes:

- Inhiber
- Désinhiber
- Isoler
- Désisoler
- Restaurer les alarmes



## 7. Utilisation

Le plugin AEOS Intrusion Monitor vous permet de surveiller et d'interagir avec les systèmes d'intrusion AEOS. L'interaction peut être effectuée automatiquement par des règles, comme décrit précédemment, ou manuellement par l'opérateur. La surveillance et chaque interaction manuelle se font depuis le Smart Client, qui est l'interface utilisateur standard dans Milestone XProtect®.

En utilisant des événements définis par l'utilisateur avec des règles, et des alarmes, la surveillance et l'interaction peuvent également être effectuées via d'autres interfaces (Web Client, Application Mobile), bien que toutes les fonctionnalités ne soient pas disponibles via ces interfaces (comme les cartes ou la vue en arborescence du panneau latéral), comme expliqué dans la section 7.4.

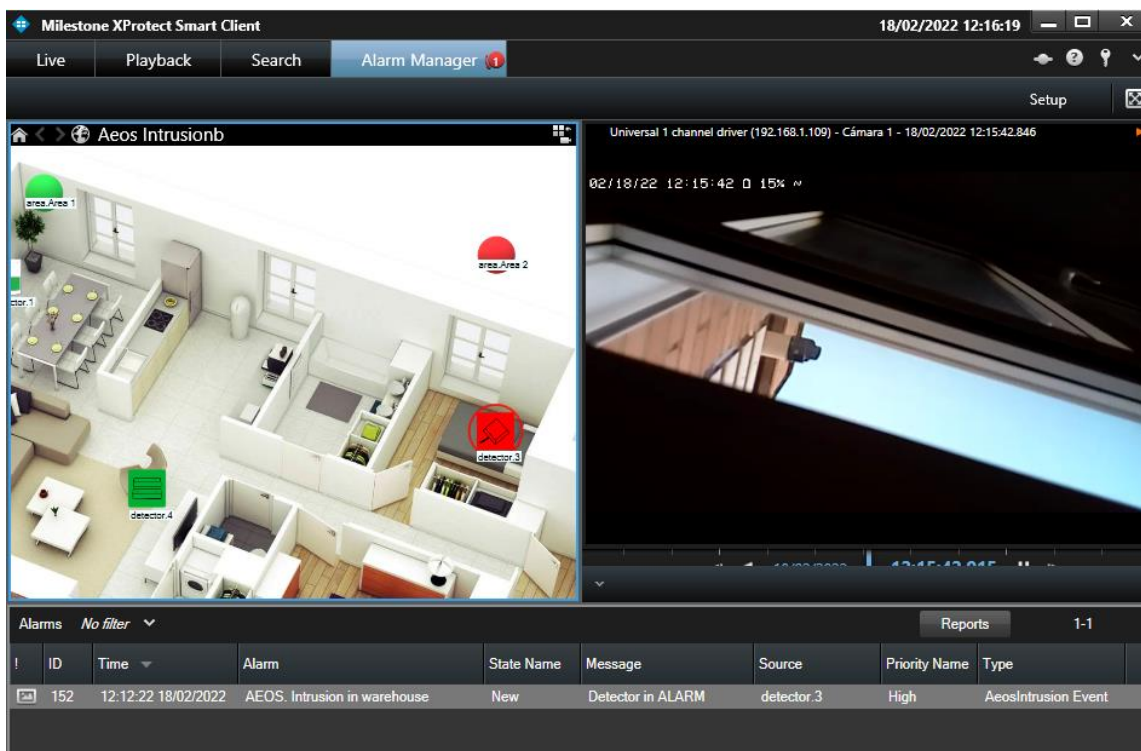
L'opérateur peut interagir avec le système AEOS Intrusion et envoyer des commandes aux zones ou aux détecteurs.

### 7.1 Visionneuse d'événements/alarmes et Gestionnaire d'alarmes

À partir de la visionneuse d'événements et d'alarmes standard, les alarmes et événements définis provenant du système AEOS Intrusion peuvent être visualisés et gérés.

Events <i>All Events (filter applied)</i> <span>Clear filter</span>					
!	ID	Time	Message	Source	Type
	61084	10:32:14 18/02/2022	Detector tampered	detector.1	AeosIntrusion Event
	61083	10:32:14 18/02/2022	Detector tampered	detector.2	AeosIntrusion Event
	61082	10:32:14 18/02/2022	Detector tampered	detector.3	AeosIntrusion Event
	61081	10:32:14 18/02/2022	Area tampered	area.Area 2	AeosIntrusion Event
	61080	10:32:14 18/02/2022	Area tampered	area.Area 1	AeosIntrusion Event
	61079	10:32:14 18/02/2022	Connected to Aeos Intrusion	SAT	AeosIntrusion Event

Les alarmes peuvent également être gérées comme n'importe quelle autre alarme Milestone en utilisant le Gestionnaire d'alarmes.



The screenshot shows the 'Alarm Manager' window in Milestone XProtect Smart Client. The interface is split into two main sections. On the left, there is a 3D floor plan of a warehouse labeled 'Aeos Intrusionb'. It features several colored zones: a green circle for 'area.Area 1', a red circle for 'area.Area 2', and four red squares for 'detector.1', 'detector.2', 'detector.3', and 'detector.4'. On the right, there is a live video feed from a camera labeled 'Universal 1 channel driver (192.168.1.109) - Cámara 1 - 18/02/2022 12:15:42.846'. The video shows a close-up of a window with a dark frame. Below the video, there is a playback control bar with a progress slider and a volume icon. At the bottom of the window, there is an 'Alarms' table with the following data:

!	ID	Time	Alarm	State Name	Message	Source	Priority Name	Type
	152	12:12:22 18/02/2022	AEOS. Intrusion in warehouse	New	Detector in ALARM	detector.3	High	AeosIntrusion Event

## 7.2 Cartes






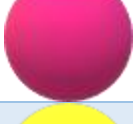



Les icônes correspondant aux zones et détecteurs peuvent être ajoutées à n'importe quelle carte XProtect® sur le Smart Client.

L'icône de chaque zone et détecteur montrera l'état de l'élément d'intrusion correspondant selon la légende de couleur référencée ci-dessous.













































Les icônes pour les zones sont les suivantes:

Couleur	Icône	Signification
<b>Vert</b>		<b>Repos:</b> La zone est OK, elle n'est pas armée et il n'y a aucun problème.
<b>Orange</b>		<b>Armée:</b> La zone est OK et armée.
<b>Rouge</b>		<b>Alarme:</b> La zone est en état d'alarme.
<b>Vert foncé</b>		<b>Non prête à être armée:</b> La zone n'est pas prête à être armée. Probablement qu'un détecteur associé est actif.
<b>Bleu</b>		<b>Inhibée ou isolée:</b> La zone est inhibée ou isolée.
<b>Magenta</b>		<b>Masquée ou sabotée:</b> La zone est masquée ou sabotée.
<b>Jaune</b>		<b>Défaillance:</b> La zone est en état de défaillance.
<b>Gris</b>		<b>Désactivée ou inconnue:</b> La zone a été désactivée dans Milestone ou l'état est inconnu.
<b>Vert/Orange</b>		<b>Test:</b> La zone est en mode test.

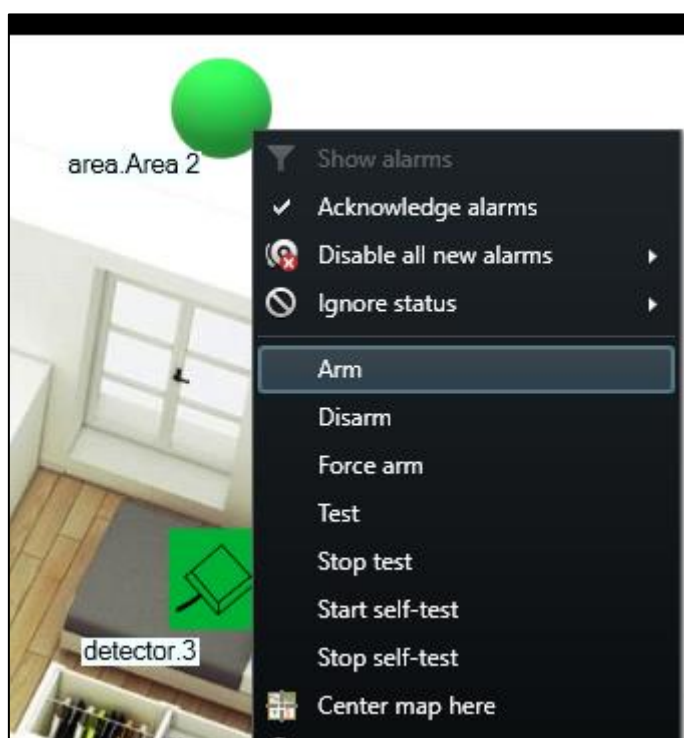


Les icônes des détecteurs représentent également le type de détecteur sélectionné lors de la configuration. Les icônes pour les détecteurs sont les suivantes:

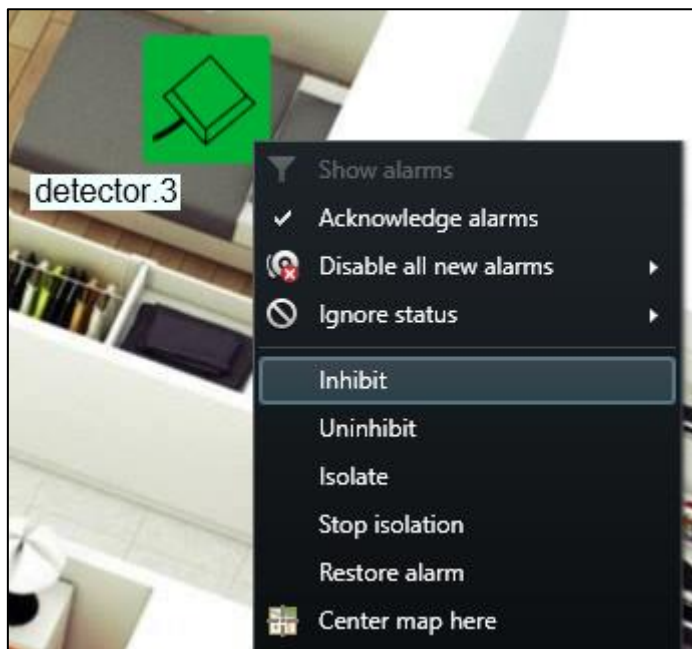
Couleur	Volumétrique	Sismique	Bris Verre	Contact magnétique	Bouton panique	Status
Vert						Repos
Orange						Armée
Rouge						Alarme
Vert foncé						Non prête à être armée
Bleu						Inhibée ou isolée
Magenta						Masquée ou sabotée
Jaune						Défaillance
Gris						Désactivée ou inconnue:

Les icônes vous permettent également d'interagir avec l'élément correspondant via leur menu contextuel (bouton secondaire de la souris).

De cette manière, vous pouvez interagir avec les zones pour armer, désarmer, armer de force, tester, arrêter le test, démarrer l'auto-test ou arrêter l'auto-test:

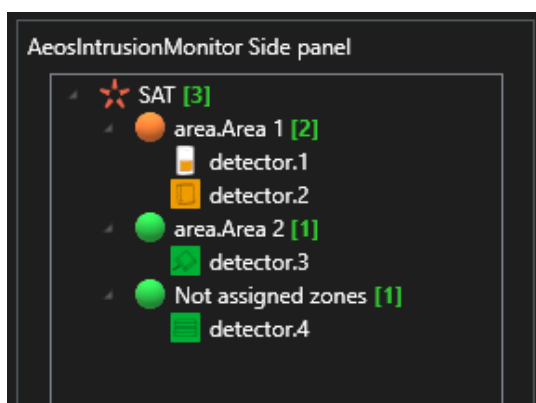


Et avec les détecteurs pour inhiber, désinhiber, isoler, désisoler ou restaurer les alarmes:



### 7.3 Vue en arborescence du panneau latéral

Pour avoir une vue d'ensemble rapide du système à tout moment, vous pouvez voir les zones et leurs détecteurs associés dans la vue en arborescence du panneau latéral.



Les icônes représentent leur état, comme sur les cartes, et vous permettent d'interagir directement avec eux, en exécutant les mêmes commandes qui peuvent être exécutées via le menu contextuel de chaque élément.

### 7.4 Web client et Milestone Mobile

Ces deux interfaces ne prennent pas en charge toutes les fonctionnalités du plugin AEOS Intrusion, comme les cartes ou la vue en arborescence du panneau latéral.

Cependant, il est toujours possible de surveiller et d'interagir avec le système AEOS Intrusion via ces interfaces. Les alarmes définies dans les systèmes peuvent être reçues dans n'importe laquelle de ces interfaces, vous permettant de surveiller le système via ses alarmes.

En utilisant des événements définis par l'utilisateur pour déclencher des règles exécutant des actions sur le système AEOS Intrusion, l'interaction peut également être effectuée via ces interfaces, car les événements définis par l'utilisateur peuvent être déclenchés à la fois depuis le Web Client et Milestone Mobile.

## 8. Dépannage

Problèmes	Raisons possibles et solutions
<b>Il n'y a pas de connexion avec AEOS</b>	<ul style="list-style-type: none"> <li>• Vérifiez la connexion réseau.</li> <li>• Vérifiez la configuration de l'interface Socket.</li> <li>• Vérifiez que la configuration du plugin correspond à la configuration de l'interface Socket.</li> <li>• Vérifiez les droits de l'utilisateur dans AEOS. Redémarrez Event Server.</li> </ul>
<b>Vous ne voyez rien en rapport avec le plugin</b>	<ul style="list-style-type: none"> <li>• Redémarrez l'application et/ou Event Server.</li> <li>• Vérifiez que le produit est licencié.</li> </ul>
<b>Les zones ont un état altéré pour une connexion perdue.</b>	<ul style="list-style-type: none"> <li>• Allez sur la page d'administration des statuts AEOS et restaurez l'état des zones.</li> <li>• Restaurez les alarmes sur les détecteurs de cette zone qui pourraient être en état altéré.</li> </ul>
<b>Vous ne pouvez pas effectuer d'actions sur les éléments</b>	<ul style="list-style-type: none"> <li>• Vérifiez les rôles et permissions de votre utilisateur Milestone.</li> <li>• Vous devriez recevoir un message de réponse</li> </ul>
<b>Le statut d'un détecteur n'est pas mis à jour.</b>	Probablement, le détecteur n'est pas assigné à une zone. Les changements d'état des détecteurs qui ne sont pas assignés à une zone d'intrusion ne sont pas signalés par AEOS.
<b>Management Client et Smart Client sur des PC séparés ne montrent rien en rapport avec le plugin.</b>	Le plugin nécessite la licence principale Event Server, mais tout PC exécutant Smart Client ou Management Client a également besoin d'un fichier de licence pour fonctionner. Demandez ces fichiers à SGSE, en précisant qu'il s'agit de licences client.

Si vous avez besoin de plus d'assistance, veuillez collecter les journaux et spécifier le problème que vous rencontrez aussi clairement que possible, en décrivant le problème lui-même, la situation dans laquelle il se produit, etc.

Les journaux pertinents peuvent être consultés dans les dossiers suivants :

- C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs\
- C:\ProgramData\Milestone\XProtect Smart Client (if logs are enabled in Smart Client)
- C:\ProgramData\SGSE\AeosIntrusionMonitor\Logs

Si vous avez besoin d'un support lié au plugin, veuillez contacter SGSE à [sat@sgse.eu](mailto:sat@sgse.eu) pour des problèmes techniques ou [info@sgse.eu](mailto:info@sgse.eu) pour des questions commerciales.

Si vous avez besoin d'un support lié à un problème général de Milestone, veuillez contacter le support Milestone (<https://www.milestonesys.com/es/support/>) ou votre fournisseur Milestone.

Si vous avez besoin d'un support lié à la configuration d'AEOS ou au système d'intrusion AEOS, veuillez contacter le support Nedap ou votre fournisseur AEOS.