



SGSE

Soluciones Globales de Seguridad Electrónica



NEDAP INTRUSION INTÉGRÉ DANS MILESTONE



milestone

L'intégration existant entre le système de contrôle d'accès AEOS et Milestone XProtect® est un excellent plugin qui permet de profiter, dans un environnement unique, des avantages de deux solutions logicielles leaders dans leur segment. Le système de contrôle d'accès AEOS complet intégré dans la plateforme ouverte du VMS de Milestone, XProtect®.

Disposer du contrôle d'accès et de la gestion vidéo sur une plateforme unique vous donne le contrôle de vos installations et de votre sécurité. Si vous pouviez ajouter l'intrusion à cette plateforme, vous auriez toute la gestion de la sécurité dans un seul environnement, avec une interface unique et une relation étroite entre les systèmes... Qui dit que vous ne le pouvez pas ?

Le nouveau plugin développé par SGSE, AEOS Intrusion Monitor, vous permet aussi d'intégrer AEOS dans Milestone comme un système anti-intrusion de sorte que vous disposez d'un VMS qui vous permet également de surveiller et gérer votre système de contrôle d'accès en même temps que votre système anti-intrusion. Ça sonne bien, n'est-ce pas?

Configuration extrêmement simple






La façon d'intégrer AEOS Intrusion dans Milestone est extrêmement simple. Activez et configurez simplement l'interface socket sur votre serveur AEOS, configurez les paramètres de communication dans le plugin pour vous connecter à AEOS à travers cette interface et... le tour est joué!

Le plugin importera automatiquement toutes les zones et détecteurs définis dans AEOS Intrusion et créera tous les items correspondants dans Milestone. Le plugin est maintenant prêt!

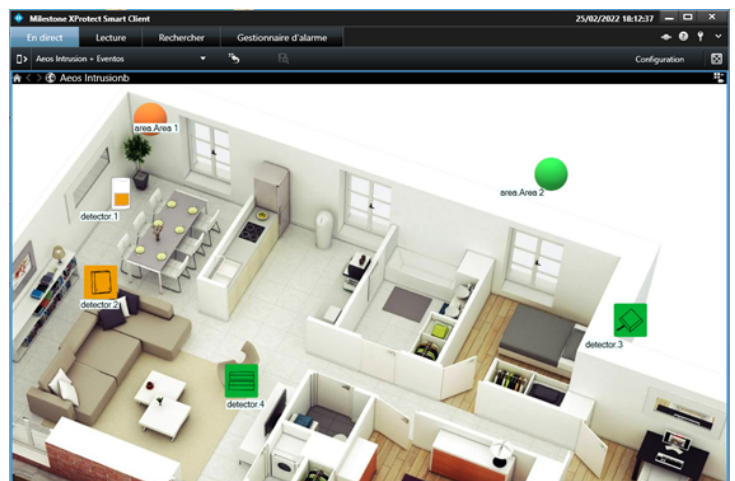
Aucune configuration supplémentaire n'est nécessaire pour que le plugin fonctionne même si certains réglages complémentaires

peuvent donner à l'opérateur une meilleure idée du système anti-intrusion et rendre l'intégration plus utile et opérationnelle comme par exemple spécifier le type de détecteurs installés, inclure les éléments anti-intrusion dans les plans ou définir des alarmes qui se déclencheront lors de la réception d'évènements déterminés liés à AEOS Intrusion.

Le plugin permet à l'utilisateur de définir le type de détecteur en sélectionnant l'un des types disponibles. Cela entraînera le changement de l'icône du détecteur dans les plans du Smart Client et dans l'arborescence latérale. Les types de détecteurs disponibles sont:

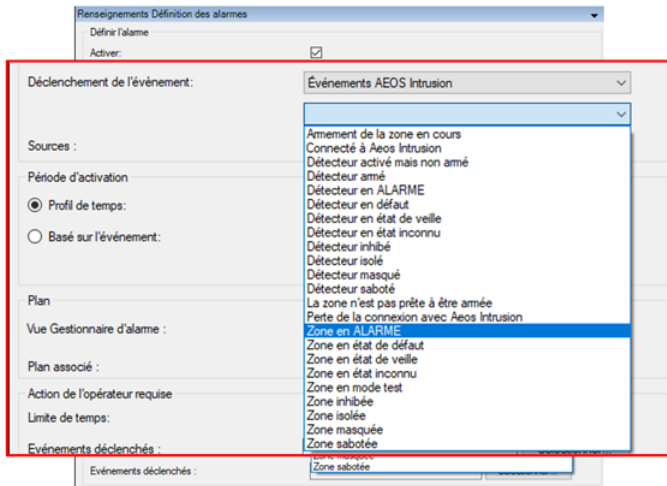
-  Volumétrique
-  Détecteur sismique
-  Bris de verre
-  Contact magnétique
-  Bouton anti-panique

On peut faire glisser les éléments anti-intrusion (comme les caméras, entrées, sorties...) dans les plans pour pouvoir les localiser facilement, voir leur état et exécuter des commandes sur ceux-ci.

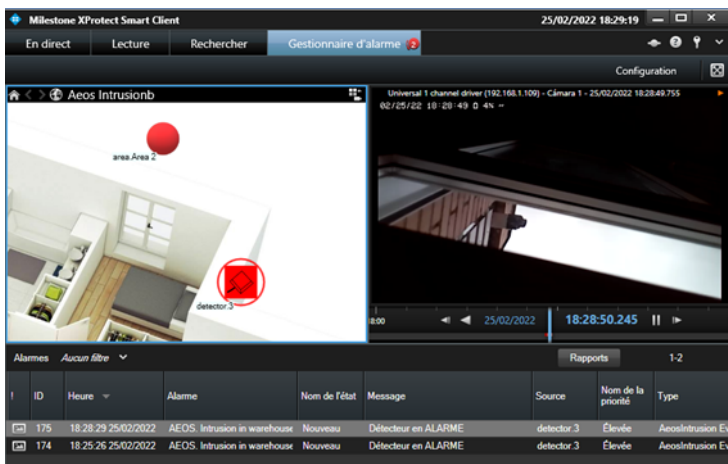


AlarmEs

Le plugin définit une série d'évènements qui peuvent être générés par l'intégration à AEOS Intrusion. Ces évènements peuvent être utilisés pour définir des alarmes, en sélectionnant ceux d'entre eux, lorsqu'ils proviendront d'un élément déterminé, qui doivent être considérés comme des alarmes.



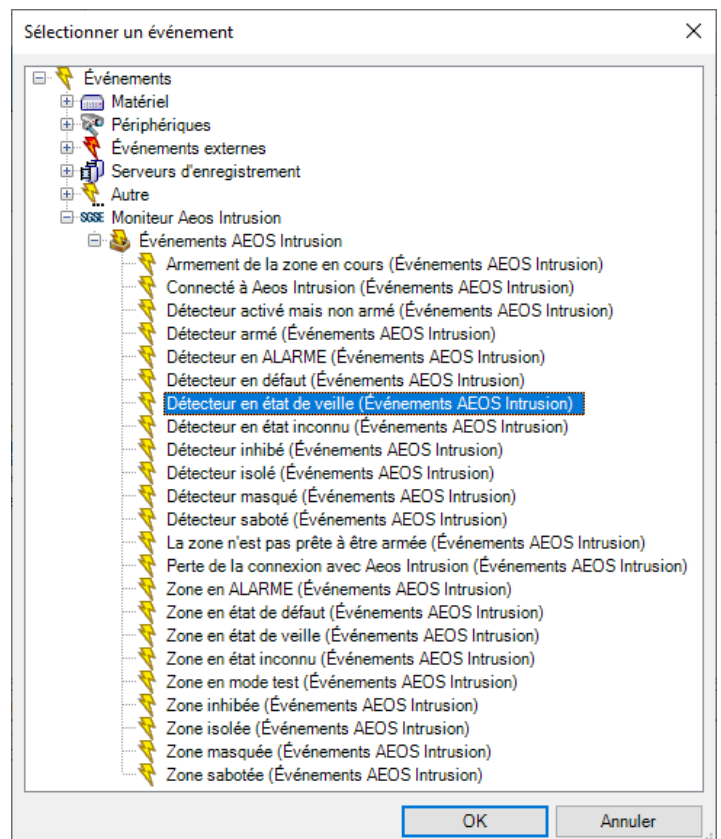
On peut par exemple définir une alarme dans Milestone lorsque l'évènement "Détecteur en alarme" se déclenche sur n'importe quel détecteur. Ainsi, lorsque l'un des détecteurs passera en état d'alarme dans AEOS Intrusion, une alarme se déclenchera dans Milestone. On pourra associer des caméras aux alarmes d'un détecteur déterminé de sorte que les alarmes d'un détecteur d'AEOS seront associées dans Milestone aux images d'une ou plusieurs caméras de Milestone.



Règles : évènements et actions

Les mêmes évènements qui peuvent être définis comme des alarmes peuvent également être utilisés pour déclencher des règles dans Milestone. Vous pouvez ainsi utiliser n'importe quel évènement d'AEOS Intrusion pour réaliser n'importe quelle action disponible dans Milestone : déplacer une caméra PTZ, démarrer des enregistrements, afficher une caméra à l'écran, activer une sortie, envoyer un e-mail...

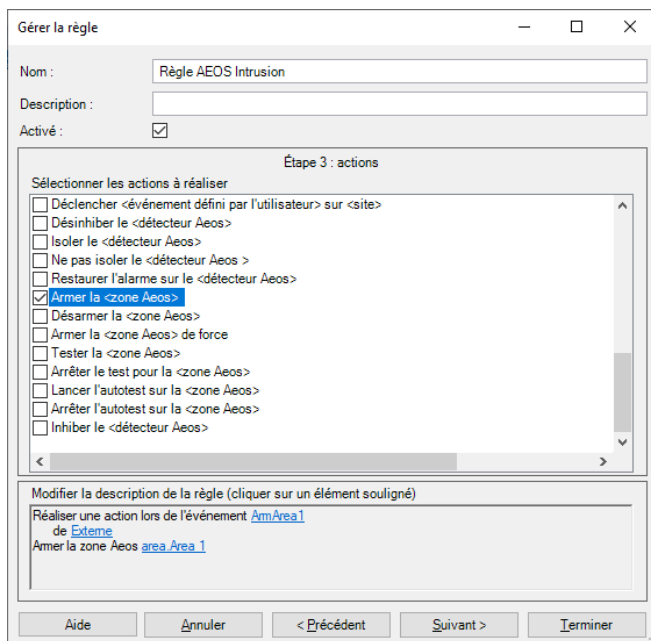
Il pourra ainsi être intéressant de déplacer une caméra PTZ vers un préréglage déterminé lorsque l'un des détecteurs, par exemple celui de la ruelle arrière, sera actif (il détecte quelque chose) mais que la zone correspondante ne sera pas armée, ce ne sera donc pas une alarme d'intrusion. On pourra alors créer une règle de manière à ce que lors du déclenchement de l'évènement "Détecteur actif mais non armé" depuis le détecteur situé dans la ruelle arrière, la caméra PTZ associée au préréglage orientée sur la ruelle arrière se déplace.



Les évènements disponibles à la fois pour définir des alarmes et déclencher des règles sont:

- Zone armée
- Zone en alarme
- Zone en panne
- Zone au repos
- Zone en test
- Zone en état inconnu
- Zone inhibée
- Zone isolée
- Zone masquée
- Zone ne peut être armée
- Zone en tamper
- Connexion établie avec AEOS Intrusion
- Connexion perdue avec AEOS Intrusion
- Détecteur actif mais non armé
- Détecteur armé
- Détecteur en panne
- Détecteur en alarme
- Détecteur au repos
- Détecteur en état inconnu
- Détecteur inhibé
- Détecteur isolé
- Détecteur masqué
- Détecteur en tamper

Mais le plugin permet également d'exécuter automatiquement des actions dans AEOS Intrusion lorsque surviendra un évènement qui pourra se produire dans Milestone.



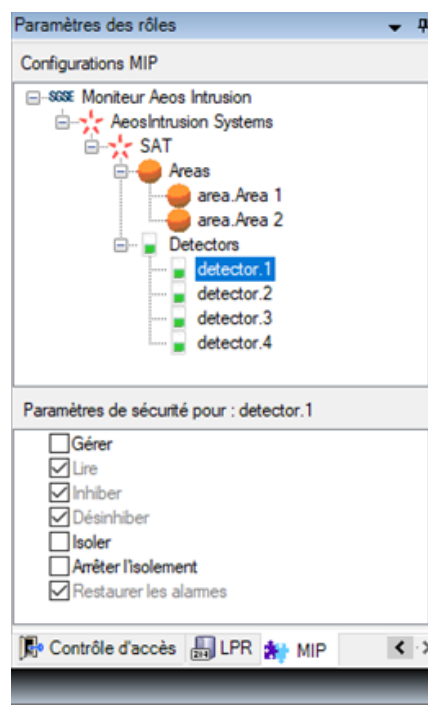
Par exemple, lorsqu'on accordera un accès à une personne précise par une porte déterminée, vous pourrez désarmer une zone d'intrusion. On pourra également inhiber automatiquement un détecteur durant un laps de temps déterminé (tous les lundi à 7:00 du matin), en le désinhibant ensuite (à 8:00) parce que la personne chargée de la maintenance vient tous les lundis dans cet intervalle pour effectuer ses tâches. On pourra même armer une zone d'intrusion lorsqu'une caméra aura cessé de transmettre des images...

Les actions qui peuvent être automatisées sont les suivantes:

- Armer une zone
- Désarmer une zone
- Armement forcé d'une zone
- Mode test dans une zone
- Terminer test
- Démarrer autotest dans une zone
- Finir autotest dans une zone
- Inhiber un détecteur
- Désinhiber un détecteur
- Isoler un détecteur
- Désisoler un détecteur
- Restaurer alarmes sur un détecteur

Autorisations

Le plugin vous permet d'assigner aux utilisateurs des autorisations spécifiques sur chaque élément anti-intrusion. On pourra par exemple assigner à un rôle d'utilisateurs l'autorisation d'armer des zones mais non de les désarmer. On peut également spécifier des autorisations différentes pour différents éléments de même type, par exemple, un rôle peut avoir toutes les autorisations sur un ensemble de zones et détecteurs (ceux appartenant à un étage ou un bâtiment) mais ne pas avoir d'autorisations pour voir les autres zones et détecteurs du système (qui peuvent appartenir à d'autres étages ou à d'autres bâtiments).



Bien évidemment, lorsqu'une gestion des autorisations aussi approfondie n'est pas nécessaire, on peut également donner des autorisations en général sur tous les éléments d'un même type.

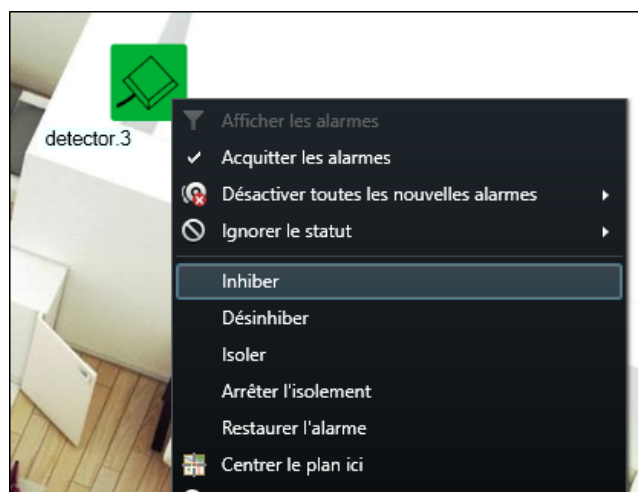
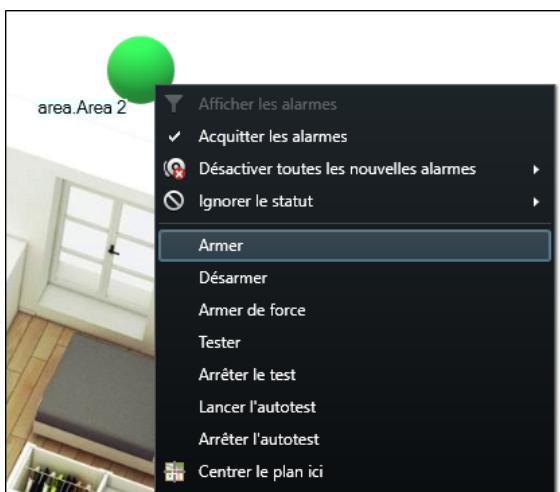
Comment fonctionne-t-il ?

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

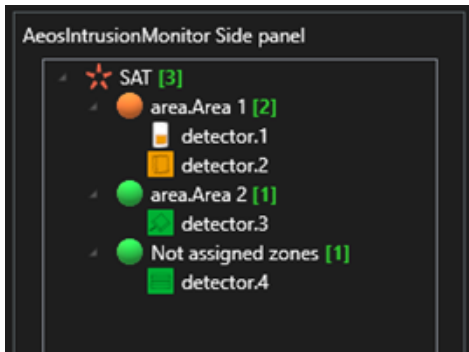
La surveillance et l'interaction manuelle s'opèrent à travers le Smart Client qui est l'interface utilisateur standard dans Milestone XProtect®.

Le principal outil pour surveiller et interagir avec le système sont les plans du Smart Client sur lesquels on peut facilement voir au moyen d'icônes les endroits où sont situés les dispositifs anti-intrusion, le type de détecteur et son état. En outre, les icônes permettent également d'interagir avec l'élément correspondant à travers son menu contextuel (bouton droit de la souris).

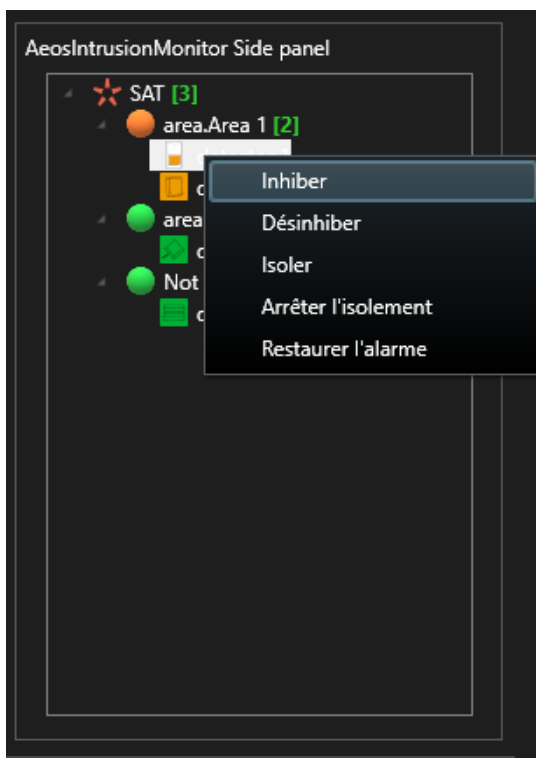
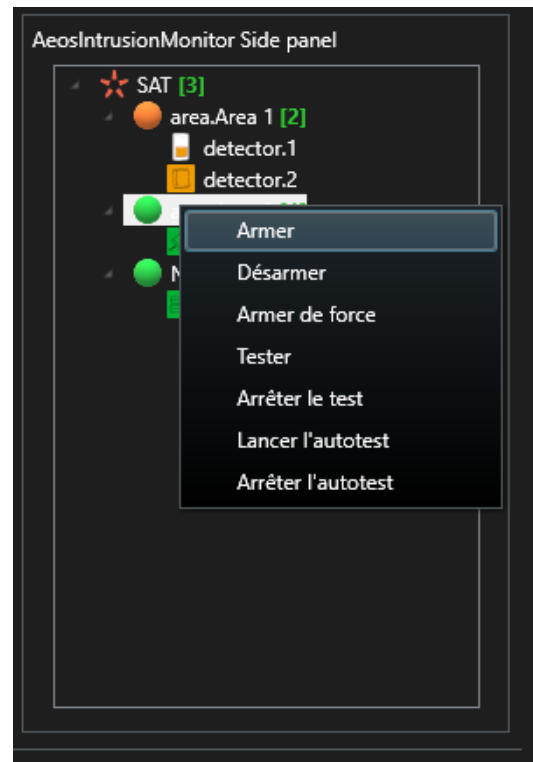
De cette manière, le plugin permet d'interagir avec les zones pour les armer, les désarmer, faire un armement forcé, démarrer ou arrêter le test et démarrer ou arrêter l'autotest et avec les détecteurs pour les inhiber, les désinhiber, les isoler, les désisoler ou restaurer les alarmes:



Pour avoir un aperçu général rapide du système à tout moment, on peut également voir les zones avec leurs détecteurs associés dans l'arborescence du panneau latéral.



Les icônes représentent l'état des éléments, tout comme sur les plans, et permettent d'interagir directement avec eux, en exécutant les mêmes commandes que celles exécutées sur les plans via le menu contextuel de chaque élément.



Déployez vos solutions d'intrusion Nedap intégrées dans Milestone via SGSE

SGSE – Soluciones Globales de Seguridad Eletrónica

www.sgse.eu

Calle Anabel Segura, 7 Esc.A 1ºB
28108 Alcobendas (Madrid) – España
+34 91 056 43 96 – info@sgse.eu

