Instructions de configuration

i-PRO Active Guard pour Genetec

Contenu

1. Préface

1.1. Limitation de la responsabilité

CETTE PUBLICATION EST FOURNIE « EN L'ÉTAT » SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE, Y COMPRIS, MAIS SANS S'Y LIMITER, LES GARANTIES IMPLICITES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER OU DE NON-VIOLATION DU DROIT DU TIERS.
CETTE PUBLICATION POURRAIT CONTENIR DES INEXACTITUDES TECHNIQUES OU DES ERREURS TYPOGRAPHIQUES. DES MODIFICATIONS SONT APPORTÉES AUX INFORMATIONS CONTENUES DANS LE PRÉSENT DOCUMENT, À TOUT MOMENT, POUR LES AMÉLIORATIONS DE CETTE PUBLICATION ET/OU DU (DES) PRODUIT(S) CORRESPONDANT(S).

1.2. Copyright

La distribution, la copie, le désassemblage, la compilation inverse et l'ingénierie inverse du logiciel fourni avec ce produit sont tous expressément interdits. En outre, l'exportation de tout logiciel fourni avec ce produit violant les lois sur l'exportation est interdite.

1.3. Marques commerciales et marques déposées

- Microsoft et Windows sont des marques déposées ou des marques commerciales de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

- Intel, Intel Core et Xeon sont des marques commerciales d'Intel Corporation ou de ses filiales aux États-Unis et/ou dans d'autres pays.

- Les autres noms de sociétés et de produits contenus dans ces instructions d'utilisation peuvent être des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

1.4. Abréviations

Il s'agit de descriptions des termes de base utilisés dans le présent mode d'emploi.

Microsoft® Windows est décrit comme Windows®.

1.5. Exclusion de garantie

Ce produit est conçu pour rechercher/vérifier un visage spécifié à partir d'une base de données qui stocke des informations sur les visages et des images miniatures créées à partir de visages capturés par des caméras réseau, et afficher des informations statistiques par opération à l'aide d'un terminal client ou d'un système compatible avec ce produit. Ce produit en lui-même n'est pas conçu pour la prévention du crime. Notre société décline toute responsabilité pour ce qui suit en aucune circonstance.

(1) TOUT DOMMAGE ET PERTE, Y COMPRIS, SANS LIMITATION, DIRECT OU INDIRECT, SPÉCIAL, CONSÉCUTIF OU EXEMPLAIRE, DÉCOULANT DE OU LIÉ AU PRODUIT;
(2) TOUT INCONVÉNIENT, PERTE OU DOMMAGE CAUSÉ PAR UNE UTILISATION INAPPROPRIÉE OU UNE UTILISATION NÉGLIGENTE DE L'UTILISATEUR;
(3) LE DÉMONTAGE, LA RÉPARATION OU LA MODIFICATION NON AUTORISÉS DU PRODUIT PAR L'UTILISATEUR;
(4) TOUT PROBLÈME, INCONVÉNIENT CONSÉCUTIF, PERTE OU DOMMAGE, DÉCOULANT DU SYSTÈME COMBINÉ PAR LES APPAREILS DE TIERS;
(5) TOUTE RÉCLAMATION OU ACTION EN DOMMAGES-INTÉRÊTS INTENTÉE PAR TOUTE PERSONNE OU ORGANISATION EN TANT QUE SUJET PHOTOGRAPHIÉ EN RAISON D'UNE VIOLATION DE LA VIE PRIVÉE CONCERNANT L'IMAGE OU LES DONNÉES SAUVEGARDÉES D'UNE CAMÉRA DE SURVEILLANCE, POUR UNE RAISON QUELCONQUE (Y COMPRIS L'UTILISATION LORSQUE L'AUTHENTIFICATION DE L'UTILISATEUR SUR L'ÉCRAN DES PARAMÈTRES D'AUTHENTIFICATION EST DÉSACTIVÉE), DEVENANT PUBLIQUE OU UTILISÉE À QUELQUE FIN QUE CE SOIT;
(6) PERTE DE DONNÉES ENREGISTRÉES CAUSÉE PAR UNE DÉFAILLANCE (Y COMPRIS L'INITIALISATION DU PRODUIT EN RAISON D'INFORMATIONS D'AUTHENTIFICATION OUBLIÉES TELLES QU'UN NOM D'UTILISATEUR ET UN MOT DE PASSE).
(7) TOUT PROBLÈME, DOMMAGE OU PLAINTE CAUSÉ PAR L'OPÉRATION PAR UN TIERS MALVEILLANT.

1.6. Collecte des données d'utilisation

Ce logiciel peut collecter des données sur l'utilisation de ce logiciel et les envoyer à i-PRO Co., Ltd. En particulier, nous utilisons ces données pour améliorer nos produits et services. Vous pouvez arrêter cette collecte de données en décochant la case « Envoyer des données anonymes pour améliorer le logiciel et l'expérience utilisateur ».
Voici un exemple des données collectées par ce logiciel. Nous ne recueillons pas de données sur vos informations personnelles.

- Nom de l'entreprise, pays et but de l'utilisation saisis par l'utilisateur.
- Le nombre de caméra et le logiciel d'extension de la caméra.

1.7. Sécurité du réseau

Comme vous utiliserez ce produit connecté à un réseau, votre attention est attirée sur les risques de sécurité suivants.

1. Fuite ou vol d'informations via ce produit

2. Utilisation de ce produit pour des opérations illégales par des personnes mal intentionnées

3. Interférence ou arrêt de ce produit par des personnes mal intentionnées

Il est de votre responsabilité de prendre des précautions telles que celles décrites ci-dessous pour vous protéger contre les risques de sécurité réseau ci-dessus.

- Utiliser ce produit dans un réseau sécurisé par un pare-feu, etc.

- Si ce produit est connecté à un réseau comprenant des PC, assurez-vous que le système n'est pas infecté par des virus informatiques ou d'autres entités malveillantes (à l'aide d'un programme antivirus, d'un programme anti-spyware régulièrement mis à jour, etc.).

- Protégez votre réseau contre les accès non autorisés en limitant les utilisateurs à ceux qui se connectent avec un nom d'utilisateur et un mot de passe autorisés définis à l'aide de l'authentification utilisateur.

- Une fois le produit accessible par l'administrateur, assurez-vous de fermer le navigateur Web.

- Changez régulièrement le mot de passe administrateur. Conservez les informations d'authentification (votre nom d'utilisateur et votre mot de passe) dans un endroit sûr, à l'abri des regards du public.

- Appliquez des mesures telles que l'authentification de l'utilisateur pour protéger votre réseau contre les fuites ou le vol d'informations, y compris les données d'image, les informations d'authentification (noms d'utilisateur et mots de passe), les informations de courrier d'alarme et les informations du serveur FTP.

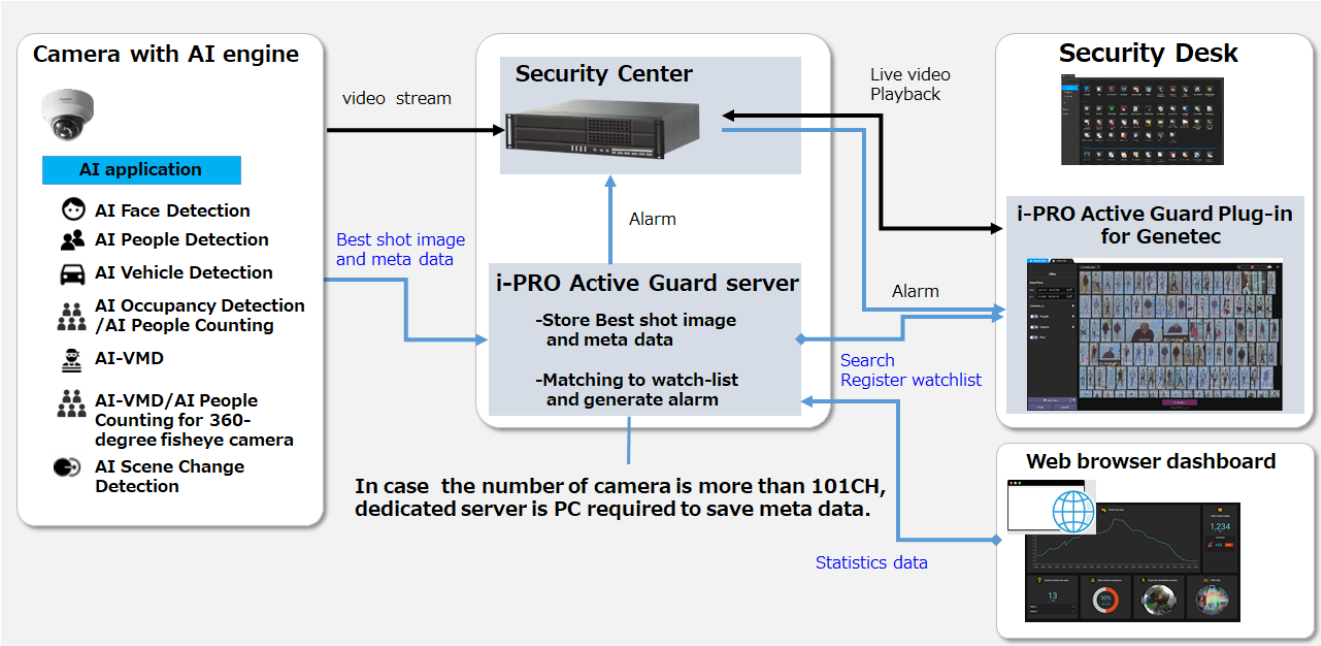
- Utilisez un mot de passe qui n'a jamais été utilisé pour protéger votre réseau contre les fuites ou le vol d'informations.

1.8. Précaution d’emploi

- L’administrateur doit gérer correctement les informations d’authentification telles que les caméras, les enregistreurs, les logiciels clients, Windows, les bases de données, etc. afin de ne pas divulguer à des tiers.
- Toujours changer les mots de passe pour les caméras, les enregistreurs, les logiciels clients, etc. à partir des valeurs par défaut et effectuez une gestion appropriée.
- Appliquez les informations d’authentification pour chaque utilisateur et ne partagez pas.
- Définissez les privilèges d’accès de l’utilisateur de manière appropriée.
- Assurez-vous de gérer correctement la connexion à l’aide de la fonction de déconnexion automatique, etc. afin que les tiers n’opèrent pas involontairement en le laissant connecté.
- Lors du téléchargement de l’application, veuillez télécharger à partir du site officiel.
- L’administrateur doit gérer correctement les données exportées à l’aide de la fonction d’exportation afin qu’il n’y ait pas de fuite vers des tiers.
- Lors de la réparation, de l’élimination ou du transfert du PC, il est possible que des informations soient laissées sur le disque dur, etc. Par conséquent, veuillez gérer par une méthode appropriée telle que la destruction physique du disque dur. En outre, si vous utilisez des supports externes, supprimez-les à l’avance et gérez-les afin qu’ils ne fuient pas à des tiers.
- Si les informations d’authentification sont perdues, le système doit être initialisé. Conservez correctement les informations d’authentification dans un endroit où seules les personnes autorisées peuvent les consulter.
- Il est recommandé de sauvegarder et de gérer régulièrement les données de configuration du système.
- Réglez l’heure des périphériques du système, tels que les caméras, les enregistreurs et les PC, à l’aide d’un serveur NTP, etc.
- Veuillez gérer correctement la date d’expiration du certificat de serveur préparé par le client.
- Pour Windows, appliquez le dernier correctif de sécurité. Veuillez également configurer Windows correctement en fonction de votre environnement.
- Les bases de données peuvent être corrompues par des arrêts forcés / pannes de courant ou des pannes de système / pannes système dues à des interruptions de courant.
Dans ce cas, le phénomène suivant peut se produire. Le logiciel serveur i-PRO Active Guard ne démarre pas, les fonctions telles que la recherche, la notification d’alarme ou l’enregistrement de la montre ne seront pas utilisées.
Les données endommagées ne peuvent pas être récupérées, il est donc fortement recommandé d’installer un onduleur en cas de panne de courant.

2. Introduction à i-PRO Active Guard

2.1. Vue d’ensemble du système



L’application AI ou la fonction AI sur les processeurs transmettent le flux vidéo à Security Center et transmettent les meilleures images et métadonnées au serveur i-PRO Active Guard.

Le serveur i-PRO Active Guard stocke ces données et génère également une alarme lorsque le visage ou les personnes correspondent à la liste de surveillance.

i-PRO Active Guard Plug-in for Genetec (ci-après dénommé « Plug-in »), qui est le logiciel plug-in de Security Desk , peut rechercher des images prises de vue, enregistrer une liste de surveillance, afficher des vidéos en direct, des vidéos enregistrées.

En visualisant les données statistiques de l’application IA sur le navigateur Web, il peut également être utilisé pour la Business Intelligence.

2.2. Composants logiciels et version prise en charge

Fonction IA de la caméra

- AI Face Detection: Logiciel extension de la caméra. V1. La version 11 ou ultérieure est prise en charge.
- AI People Detection: Logiciel extension de la caméra. V1. La version 11 ou ultérieure est prise en charge.
  - V1. La version 40 ou ultérieure est requise pour utiliser la détection automatique des attributs de personnes à partir d'images.
- AI Vehicle Detection: Logiciel extension de la caméra. V1. La version 11 ou ultérieure est prise en charge.
  - V1. 40 ou version ultérieure est requis pour utiliser la détection automatique des attributs du véhicule à partir d'images.
- AI Occupancy Detection/AI People Counting : Logiciel exten sion de la caméra. V1. 60 ou version ultérieure est pris en charge.
- AI-VMD: Logiciel extension de la caméra. V2. 0 0ou version ultérieure est pris en charge.
  - La version 3.00 ou ultérieure est requise pour le tableau de bord de comptage de personnes ou de véhicules.
  - La version 3.20 ou ultérieure est requise pour afficher les noms de zone/ligne définis dans la caméra.

- Classification sonore AI: fonction de micrologiciel de la caméra.
- AI-VMD/AI People Counting for 360-degree fisheye camera: Logiciel extension de la caméra. V1. La version 21 ou ultérieure est prise en charge.
  - La version 1.50 ou ultérieure est requise pour afficher les noms de zone/ligne définis dans la caméra.
- AIS cene Change Detection: Logiciel extension de la caméra. La version 1.00 ou ultérieure est prise en charge.
- AI Processing Relay: Logiciel extension de la caméra. La version 1.00 ou ultérieure est prise en charge.

Veuillez consulter https://i-pro.com/global/en/surveillance/products/i-pro-ai-application/ pour plus d'informations .

Pour l'intégration avec le logiciel d'extension tiers, reportez-vous à 7.2la section .

Micrologiciel des caméras

Les caméras avec moteur AI (ci-après dénommées « caméra ») sont prises en charge.

Veuillez également vérifier les modèles de caméras pris en charge sur VMS.

Modèle de caméra	Version
WV-S1136,WV-S2136,WV-S2136L,WV-S2236L	1.11 ou version ultérieure
WV-S1536L, WV-S1536LN, WV-S1536LTN,WV-S2536L,WV-S2536LN, ,WV-S2536LTN	1.11 ou version ultérieure
WV-X1571L,WV-X2571L,WV-X2271L,WV-X1551L,WV-X2551L	1.50 ou ultérieure
WV-S4576L,WV-S4176,WV-S4576LM,WV-S4156,WV-S4556L,WV-S4556LM	1.01 ou version ultérieure
WV-S8543,WV-S8543G,WV-S8543L,WV-S8543LG, WV-S8544,WV-S8544G,WV-S8544L,WV-S8544LG, WV-S8563L,WV-S8563LG,WV-S8564L,WV-S8564LG, WV-S8573L,WV-S8573LG,WV-S8574L,WV-S8574LG	1.01 ou version ultérieure
WV-S15500-V3L, WV-S15500-V3LN, WV-S15500-V3LN1, WV-S15500-V3LK,WV-S15600-V2L, WV-S15600-V2LN,WV-S15700-V2L, WV-S15700-V2LN, WV-S15700-V2LK,WV-S22500-V3L, WV-S22500-V3LG, WV-S22500-V3L1, WV-S22600-V2L, WV-S22600-V2LG,WV-S22700-V2L, WV-S22700-V2LG, WV-S22700-V2L1, WV-S25500-V3L,WV-S25500-V3LN, WV-S25500-V3LG, WV-S25500-V3LN1,WV-S25600-V2L, WV-S25600-V2LN, WV-S25600-V2LG,WV-S25700-V2L, WV-S25700-V2LN, WV-S25700-V2LG,WV-S25700-V2LN1,	1.00 ou version ultérieure
WV-S71300-F3	1.10 ou version ultérieure
WV-S61301-Z2,WV-S61302-Z4,WV-S65340-Z2N,WV-S65340-Z2K,WV-S65340-Z4N,WV-S65340-Z4K	1.00 ou version ultérieure

Veuillez consulter https://i-pro.com/global/en/surveillance/training-support/support/technical-information<Control No:C0103> pour plus d’informations.

VMS et i-PRO Active Guard serveur / plug-in

Logiciel	Version
Security Center Genetec	SC 5.10.1.0 ou version ultérieure
Serveur i-PRO Active Guard / Plug-in i-PRO Active Guard pour Genetec	V1.0.0 ou ultérieure

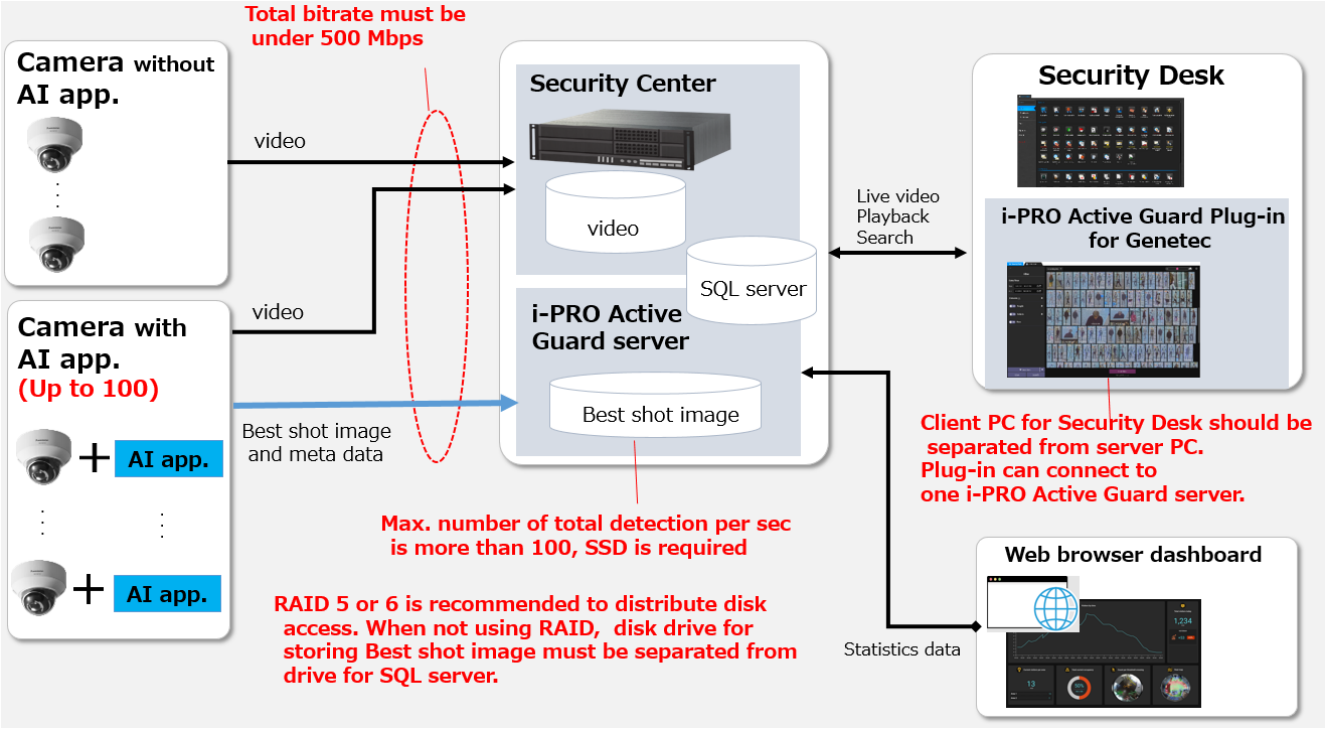
3. Conception du système

3.1. Architecture du système

Deux architectures système sont sélectionnables en fonction du nombre de caméras et de la fréquence à laquelle la caméra détecte les objets ou de la taille de stockage, etc.

	Serveur i-PRO Active Guard installé avec Security Center	Serveur i-PRO Active Guard installé En serveur dédié
Le nombre de caméras	100 (AI Face Detection est jusqu'à 20)	300 (AI Face Detection est jusqu'à 60)
Débit binaire total	500Mbps pour la vidéo et les meilleures images	500 Mbps pour les meilleures images prises

3.1.Un serveur i-PRO Active Guard installé sur PC avec Security Center



Il existe certaines conditions pour installer le serveur i-PRO Active Guard sur le PC serveur avec Security Center.

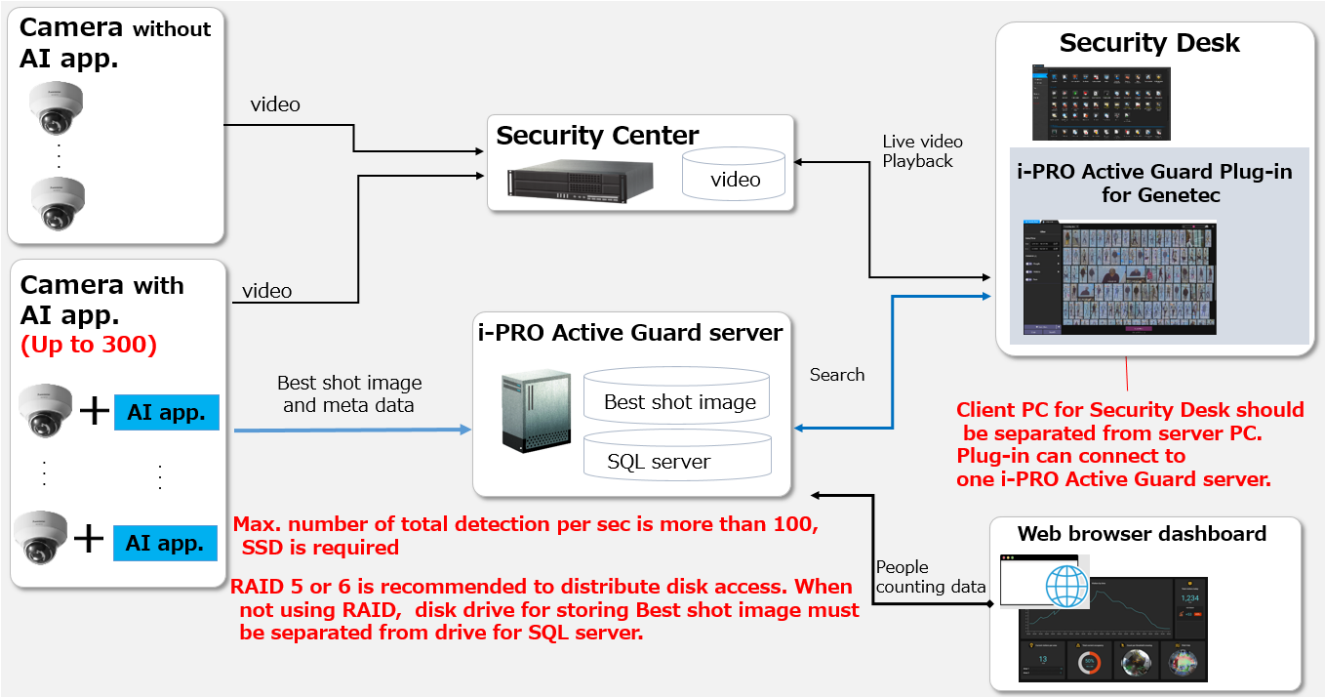
(1) Le nombre de caméras avec moteur AI est jusqu'à 100.
La caméra avec détection de visage AI est jusqu'à 20.

(2) Le débit binaire total reçu par le PC serveur doit être inférieur à 500 Mbit/s. Le débit binaire des données vidéo et les meilleures images doivent être calculés.
Le débit binaire des meilleures images peut être calculé en 3.3.

(3) RAID 5 ou 6 est recommandé pour distribuer l'accès au disque. Lorsque vous n'utilisez pas RAID, le lecteur de disque pour stocker l'image Best shot doit être séparé du lecteur pour stocker la vidéo et SQL Server.

(4) Le PC client doit être séparé du PC serveur. Le plug-in peut se connecter à un serveur i-PRO Active Guard.

3.1.B Serveur i-PRO Active Guard installé sur un serveur dédié



Lorsque le serveur i-PRO Active Guard est installé sur un serveur dédié,

(1) Le nombre de caméras avec moteur AI est jusqu'à 300.
La caméra avec détection de visage AI est jusqu'à 60.

(2) RAID 5 ou 6 est recommandé pour distribuer l'accès au disque. Lorsque vous n'utilisez pas RAID, le lecteur de disque pour stocker l'image Best shot doit être distinct du lecteur pour SQL Server.

(3) Le PC client doit être séparé du PC serveur. Le plug-in peut se connecter à un serveur i-PRO Active Guard.

3.2. Configuration système requise

3.2.1 Configuration requise pour le serveur i-PRO Active Guard

Configuration matérielle requise

	Exigence
Jusqu'à 100 caméras Serveur i-PRO Active Guard installé avec Security Center	• Intel® Xeon® Silver 4210 2,2 GHz ou supérieur • 32 Go de RAM ou plus • Système d'exploitation 64 bits Microsoft® Windows Server 2016 Standard Microsoft® Windows Server 2019 Standard Microsoft® Windows Server 2022 Standard Centre de données Microsoft® Windows Server 2016 Centre de données Microsoft® Windows Server 2019 Centre de données Microsoft® Windows Server 2022 • Carte d'interface réseau GbE
Jusqu'à 100 caméras Serveur i-PRO Active Guard installé sur un serveur dédié	• Intel® Core™ i7-9700 (4,9 GHz, 8 cœurs 8 threads) ou supérieur • 32 Go de RAM ou plus • Système d'exploitation 64 bits Microsoft® Windows 10 Professionnel Microsoft® Windows 10 Entreprise Microsoft® Windows 10 Éducation Microsoft® Windows 10 Professionnel Éducation * version 2004 ou ultérieure Microsoft® Windows 11 Professionnel Microsoft® Windows 11 Entreprise Microsoft® Windows 11 Éducation Microsoft® Windows 11 Professionnel Éducation Microsoft® Windows Server 2016 Standard Microsoft® Windows Server 2019 Standard Microsoft® Windows Server 2022 Standard Centre de données Microsoft® Windows Server 2016 Centre de données Microsoft® Windows Server 2019 Centre de données Microsoft® Windows Server 2022 • Carte d'interface réseau GbE
Jusqu'à 300 caméras Serveur i-PRO Active Guard installé sur un serveur dédié	• Intel® Xeon® Silver 4208 2,1 GHz (8 cœurs 16 threads) ou supérieur • 32 Go de RAM ou plus • Système d'exploitation 64 bits Microsoft® Windows Server 2016 Standard Microsoft® Windows Server 2019 Standard Microsoft® Windows Server 2022 Standard

	Exigence
	Centre de données Microsoft® Windows Server 2016 Centre de données Microsoft® Windows Server 2019 Centre de données Microsoft® Windows Server 2022 • Carte d'interface réseau GbE

Configuration logicielle commune requise

Catégorie	Logiciels pris en charge
Moteurs de base de données	• SQL Server 2014/2016 Express/Standard Edition SQL Server 2016 Express E dition est installé lors de l'installation du serveur i-PRO Active Guard. La procédure de mise à niveau est illustrée à 5.10la .
Navigateur Web pour l'outil de configuration	•Microsoft Edge 85 ou version ultérieure •Chrome 83 ou version ultérieure •Firefox 95 ou version ultérieure

Considérations relatives au lecteur de disque

Lorsque le nombre maximal de détections dépasse 100 objets par seconde pour toutes les caméras, un SSD est requis pour stocker les données. Voir 3.3 en détail. Si vous utilisez un disque dur, les données ne seront pas stockées et le système deviendra instable.

RAID 5 ou 6 est recommandé pour distribuer l'accès au disque. Lorsque vous n'utilisez pas RAID, le lecteur de disque pour stocker l'image Best shot doit être distinct du lecteur pour SQL Server.

Considérations relatives la base de données

SQL Server Express Edition a la limitation que la taille maximale de la base de données est de 10 Go, donc la taille de disque utilisée estimée pour la base de données du visage, des personnes et du véhicule doit être inférieure à 8 Go. Vérifiez 3.3 si l'édition Express est suffisante.

3.2.2 Configuration requise pour le plug-in

Exigence (recommandé)
● Intel® Core™ i7-9700 (4,9 GHz, 8 cœurs 8 threads) ou supérieur ● 8 Go de RAM ou mieux ● Système d'exploitation : Microsoft Windows 10 Pro (64 bits), Microsoft®® Windows 11 Pro (64 bits) ● Disque SSD de 120 Go pour les applications OS et Security Center, avec un minimum de 6 Go d'espace disque disponible pour installer l'application cliente Security Center ● Carte d'interface réseau GbE ● Carte vidéo NVIDIA® GTX 1660

Veuillez également consulter le manuel du Security Center.

3.3. Comment déterminer l'architecture du système

Afin de déterminer le dimensionnement du serveur Active Guard un calculateur dédié est disponible sur notre site internet :

https://i-pro.com/products_and_solutions/en/surveillance/learning-and-support/tools/calculators

Remarques :

Dans le cas d'une caméra multi-capteurs, un logiciel d'extension peut être installé pour chaque caméra et chaque caméra doit être enregistrée sur le serveur i-PRO Active Guard.

Pour calculer le débit binaire des Best shot, le nombre de logiciels d'extension (Face, People, Vehicle et People Counting for for 360-degree fisheye camera) devrait être envisagée. Étant donné que la quantité de données de comptage par AI-VMD, AI Occupancy Detection / AI People Counting, AI Scene Change Detection est faible, il n'est pas nécessaire de le considérer. Plusieurs logiciels d'extension peuvent être installés sur chaque caméra.

Lorsque le nombre maximal de détections au total est inférieur à 100, un disque dur ou un SSD sont utilisables comme périphérique de stockage.
Lorsque le nombre maximum de détections au total est supérieur à 100, un SSD est requis.

Si le débit binaire total reçu par le PC serveur dépasse 500 Mbps, le serveur i-PRO Active Guard doit être installé sur un PC serveur dédié .

Lorsque la « taille de disque utilisée estimée pour la base de données » est inférieure à 8 Go, SQL Server Express Edition ou Standard Edition peut être utilisé. Lorsque plus de 8 Go, SQL Server Express Edition ne peut pas être utilisé en raison de la limitation d'Express Edition. L'édition Standard est indispensable. (Reportez-vous à 5.10)

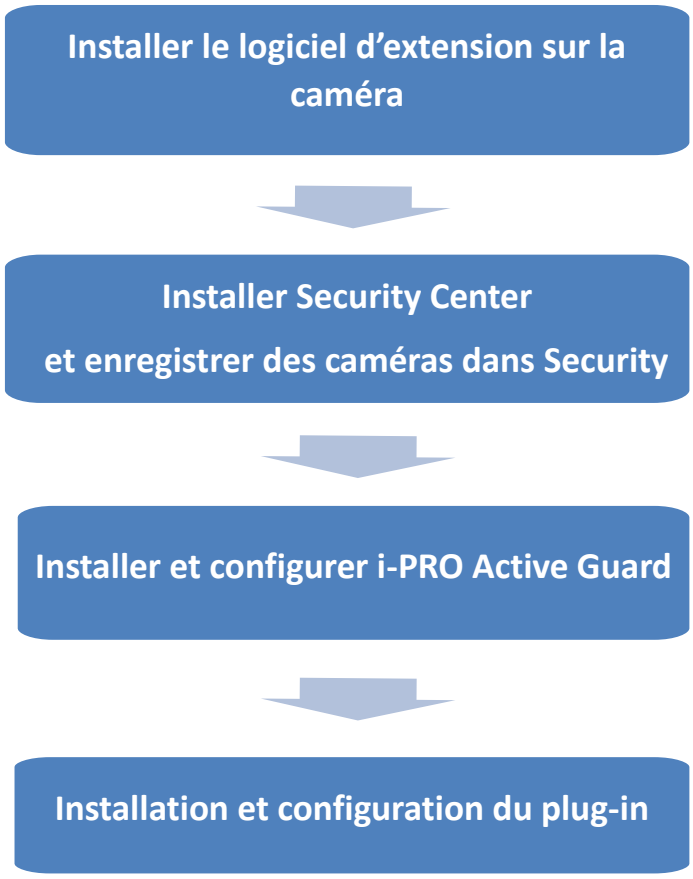
3.4. Ports utilisés dans le serveur i-PRO Active Guard

Le tableau suivant répertorie les ports réseau par défaut utilisés par le serveur i-PRO Active Guard. Ces ports doivent être autorisés à partir des configurations de pare-feu.

Numéros deports	Protocole	Utilisation des ports
1435	TCP	Connexion au serveur SQL
8090	HTTP	Connexion du plug-in client
8091	HTTPS	Connexion du plug-in client
8092	HTTPS	Connexion à l'outil de configuration Web
50000	TCP	Communication interne des processus
50002	TCP	Communication interne des processus

4. Installation et configuration

Vue d’ensemble de la procédure



4.1. Installez le logiciel d’extension sur la caméra et configurez à l’aide d’iCT

Téléchargez le logiciel d’extension et se référer au manuel de https://i-pro.com/global/en/surveillance/training-support/documentation-database-list/

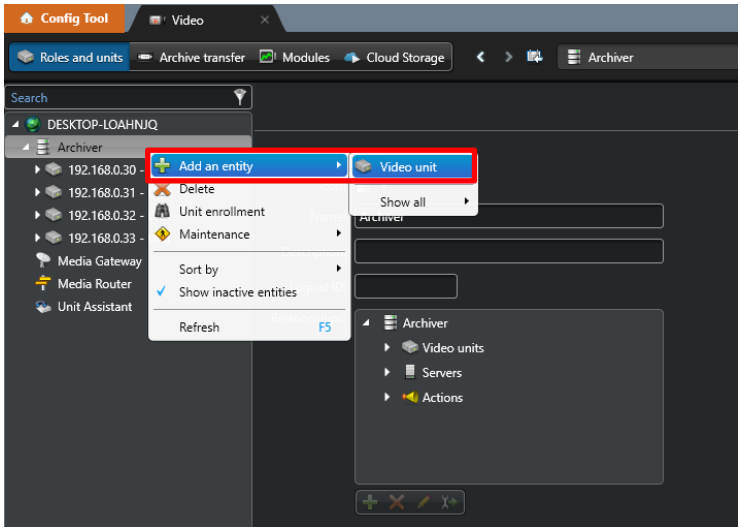
4.2. Installer et configurer Security Center

Installez le logiciel serveur VMS et enregistrez la caméra AI auprès du client VMS.
Installez le plug-in sur Security Desk.
Enregistrer la caméra dans MAP en tant que paramètre Option

4.2.1. Installer et enregistrer des caméras dans Security Center

La procédure détaillée concernant l'installation et la configuration de base de Security Center sont indiquées dans le manuel de Security Center.

Après l'installation, enregistrez les caméras AI dans Security Center à l'aide de Config Tool.
(Security Center Genetec – [Outil de configuration] – [Vidéo] – [Caméras])



4.2.2. Installer le plug-in dans Security Center

Download l'installateur de https://i-pro.com/global/en/surveillance/training-support/documentation-database-list/
Installez le logiciel « i-PRO Active Guard Plug-in for Genetec » sur le PC sur lequel Genetec Security Center est installé.

4.2.2.1. Installer

ÉTAPE 1

Démarrez « Panneau de configuration » - « Outils d'administration » - « Services ».
Sélectionnez « Genetec Server » et « Arrêter » dans le menu contextuel.

ÉTAPE 2

Lancez le programme d'installation exécutable en tant qu'administrateur.
Cliquez sur le bouton [Suivant], puis cochez la case [J'accepte les termes du contrat de licence], puis cliquez sur le bouton [Installer]

Lorsque la fenêtre Installation terminée s’affiche, cliquez sur le bouton [Terminer].

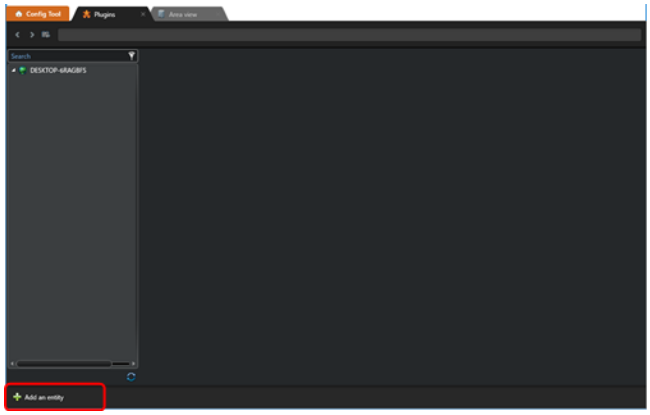
ÉTAPE 3

Démarrer « Panneau de configuration » - « Outils d’administration » - « Services »

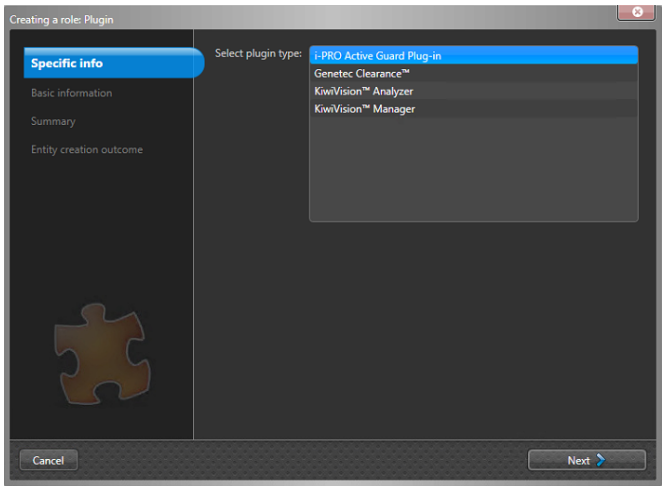
Sélectionnez « Genetec Server » et « Démarrer » dans le menu contextuel.

4.2.2.2. Configurer le plug-in pour Security Center

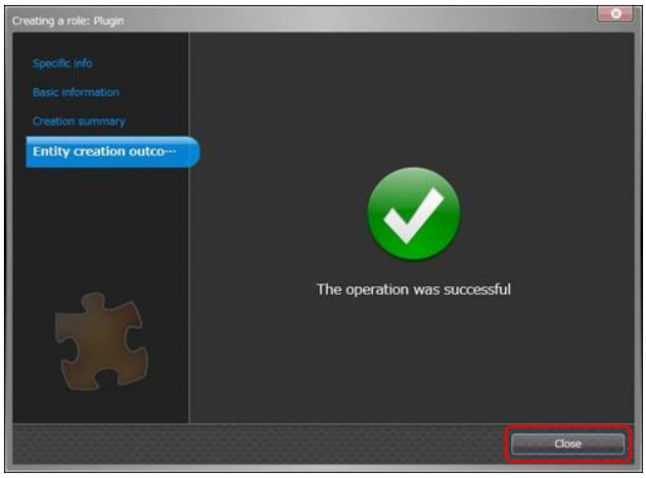
Connectez Config Tool à Security Center. Dans le site Config Tool, cliquez sur [Plugins] dans le menu [Tâches].



Cliquez sur le bouton [Ajouter une entité] en bas à gauche de l’écran.



Sélectionnez [plug-in i-PRO Active Guard] et [Suivant].



Installez en suivant l’écran et [Fermer] lorsque vous avez terminé.

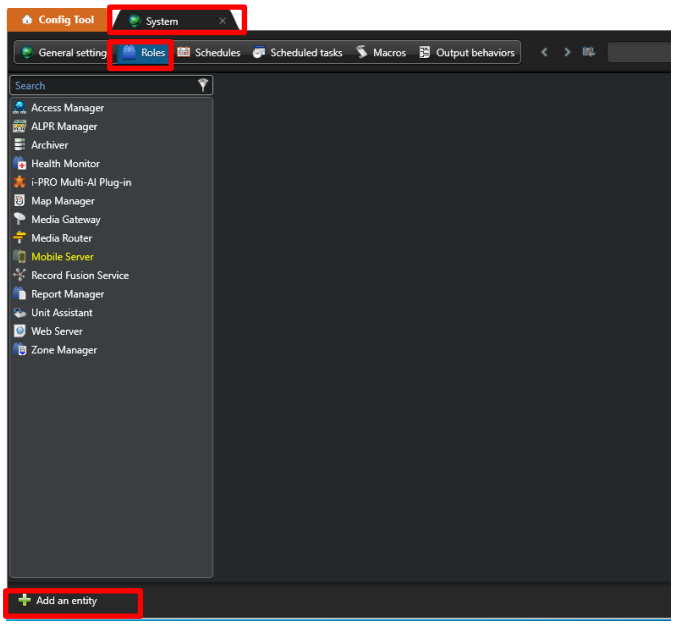
.

4.2.3. Configurer le SDK Web

ÉTAPE 1

[Outil de configuration] – [Système] - [Rôles] bouton.

Cliquez sur le bouton [Ajouter une entité] en bas à gauche de l'écran et sélectionnez le [SDK Web].



Cliquez sur le bouton [Suivant] dans [Informations de base], le bouton [Créer] dans [Résumé de la création] et le bouton [Fermer] dans [Résultat de la création de l'entité].

ÉTAPE 2

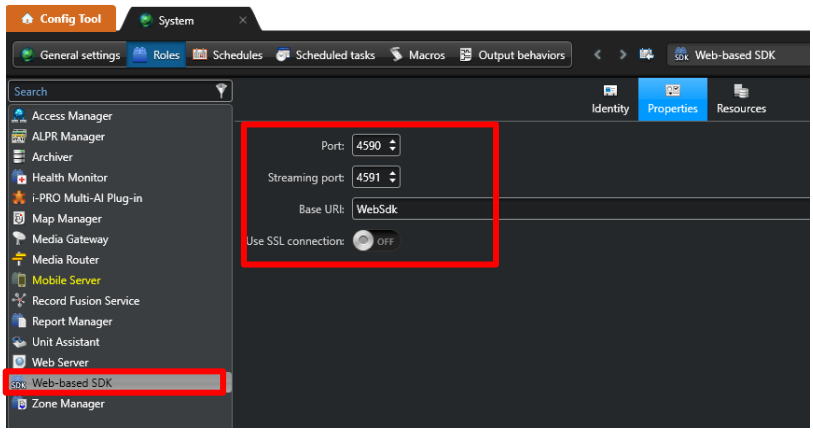
Vérifiez que [SDK Web] est affiché.

Cliquez sur [Propriétés] dans [SDK Web] et définissez comme suit.

Port : 4590

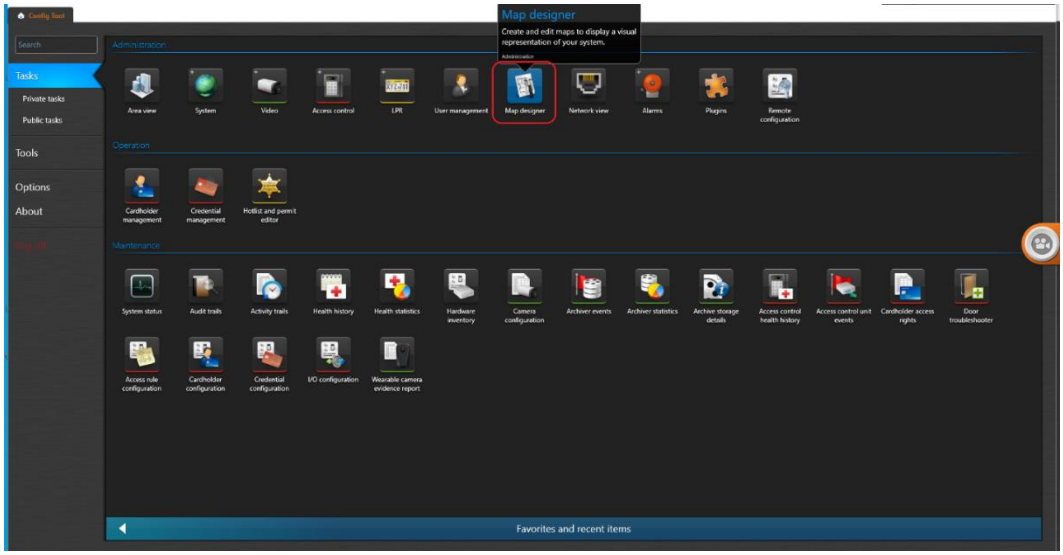
Base URI : WebSdk

Utiliser une connexion SSL peut être utilisé lors de l'utilisation de connexions SSL.



4.2.4. Enregistrer des caméras sur Map (facultatif)

À l'aide de cartes, l'opérateur peut facilement trouver l'emplacement de chaque meilleure image sur l'écran du plug-in.
Consultez le manuel d'utilisation de Security Center en détail.
([Outil de configuration] – [Concepteur de carte])



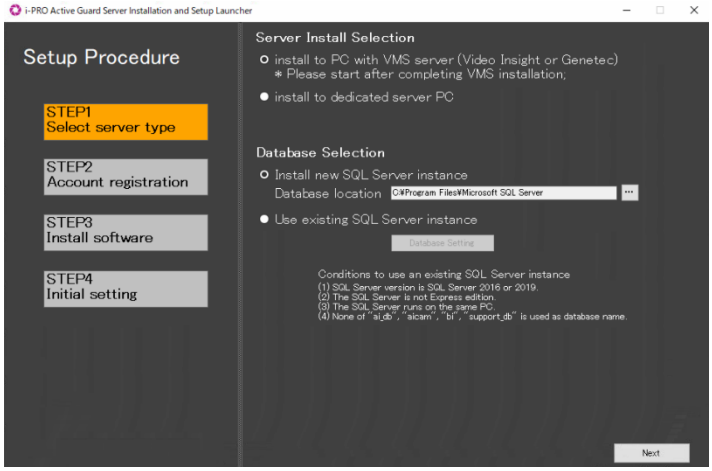
4.3. Installer et configurer le serveur i-PRO Active Guard

Download l'installateur de https://i-pro.com/global/en/surveillance/training-support/documentation-database-list/
Installez le logiciel serveur i-PRO Active Guard. La configuration après l'installation peut être effectuée à partir du navigateur Web.

4.3.1. Installer

Exécutez « MultiAIStartup.exe » en tant qu'administrateur (la longueur du chemin d'accès au fichier doit être inférieure à 120).

Lorsque .NET Framework 4.8 n'est pas installé sur le PC, il sera automatiquement installé et l'écran principal de l'outil d'installation s'affichera après l'installation.
Vérifiez [Accepter] pour la durée de la licences et [OK].

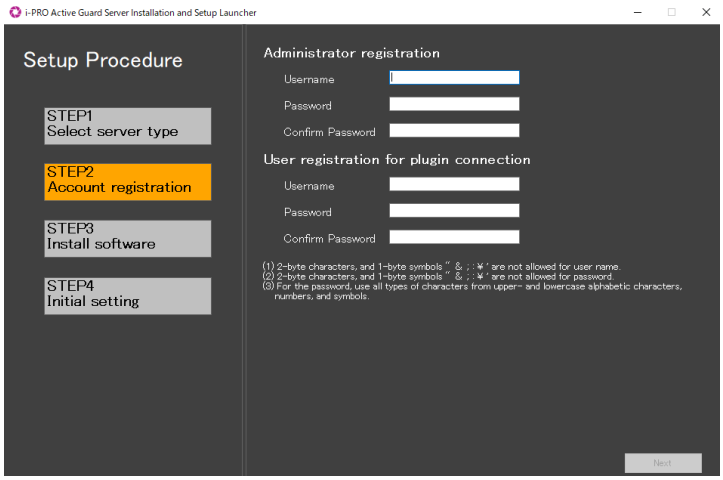


・Sélection de l'installation du serveur
Sélectionnez [installer sur un PC avec un serveur VMS] ou [installer sur un PC serveur dédié].

Remarque
Lorsque vous installez le serveur i-PRO Active Guard sur un PC avec un serveur VMS, vous devez installer le logiciel du serveur VMS à l'avance.

・Sélection de base de données
Sélectionnez [Installer une nouvelle instance SQL Server] ou [Utiliser une instance SQL Server existante].
Remarque
Si vous choisissez [Installer une nouvelle instance SQL Server], vous devez définir l'emplacement de la base de données.
Si vous choisissez [Utiliser une instance SQL Server existante], vous devez sélectionner les paramètres de base de données existants et les informations d'identification d'entrée.

Cliquez sur [Suivant].

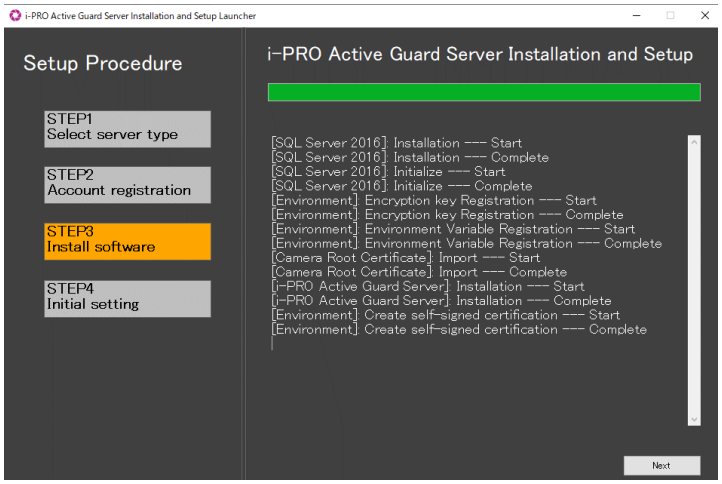


Enregistrez les informations d'identification et cliquez sur [Suivant].

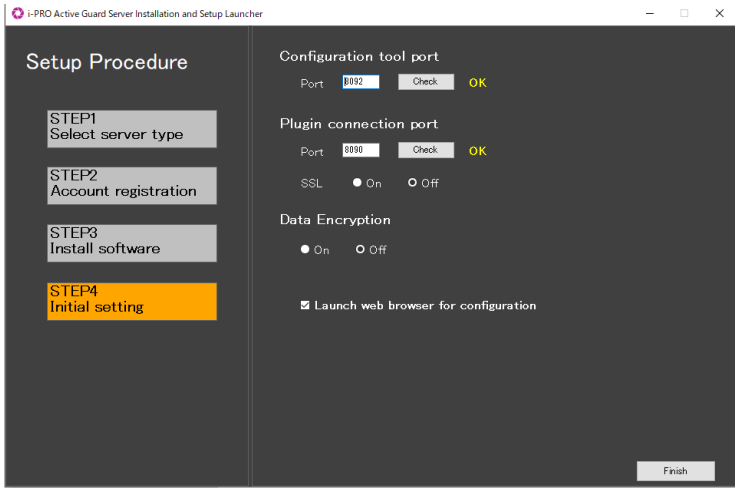
Remarque
Notez le mot de passe que vous avez entré et conservez-le en lieu sûr.

Lorsque vous oubliez le compte Administrateur, vous pouvez le réinitialiser (reportez-vous à 5.9la section).

Lorsque vous oubliez le compte d'utilisateur, vous pouvez le réinitialiser (reportez-vous à 4.3.7.2la section).



Installation démarre et le bouton [Suivant] apparaîtra lorsque vous aurez terminé. Cliquez sur [Suivant].



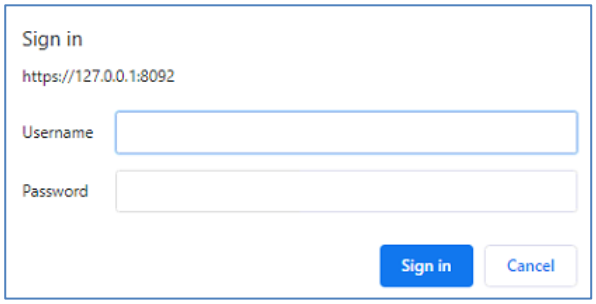
Configurez le numéro de port, SSL et le chiffrement des données et [Terminer].

Remarque Lorsque l’option Activé est sélectionnée pour Chiffrement des données, les données de l’image sont chiffrées. Ce paramètre ne peut pas être modifié après l’installation. La réinstallation est requise lorsque vous souhaitez modifier une fois l’installation terminée.

4.3.2. Configuration du serveur i-PRO Active Guard

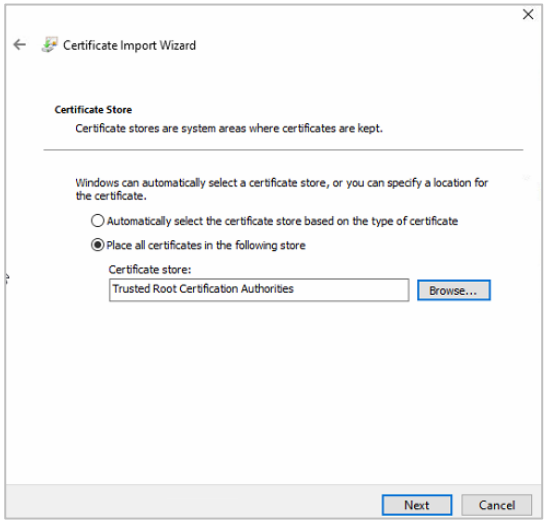
4.3.2.1. Ouverture de session

Accédez à https://<ip>:8092 à l'aide de Google Chrome, Microsoft Edge ou Firefox.
Informations d'identification d'entrée.

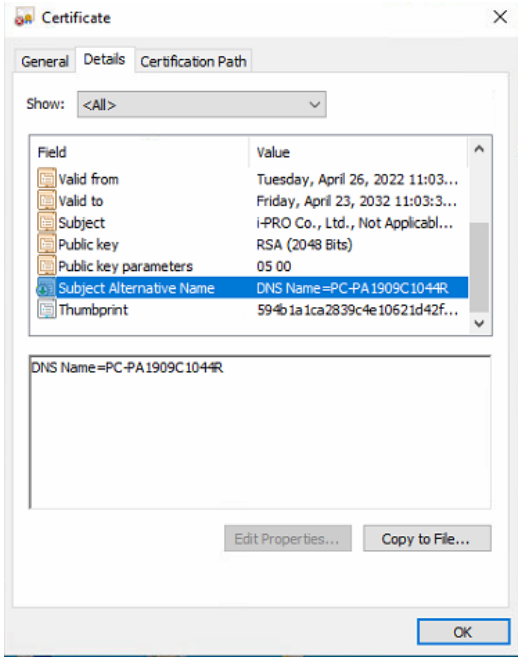


Remarque
Les informations d'identification et le numéro de port configurés par l'outil 4.3.1 d'installation sont utilisés.
Le serveur i-PRO Active Guard utilise un certificat auto-signé pour l'accès Web.
Lorsque la fenêtre d'alerte de sécurité s'affiche, click[avancé] et [Passer à <ip> (dangereux)].

Il est possible d'empêcher l'affichage de l'avertissement en effectuant la procédure suivante pour chaque PC client accessible.
1) C opy « C:\MultiAI\apache24\conf\server.crt » dans i-PRO Active Guard serveur PC à PC client.
2) Double-cliquez sur le fichier et cliquez sur « Installer le certificat ».
3) Sélectionnez « Machine locale » pour l'emplacement du magasin
4) Sélectionnez « Placer tous les certificats dans le magasin suivant » et « Autorités de certification racines de confiance ».



5) Confirmez « Autre nom du sujet » à partir de « Détails ». Nom DNS=xxxx est affiché.

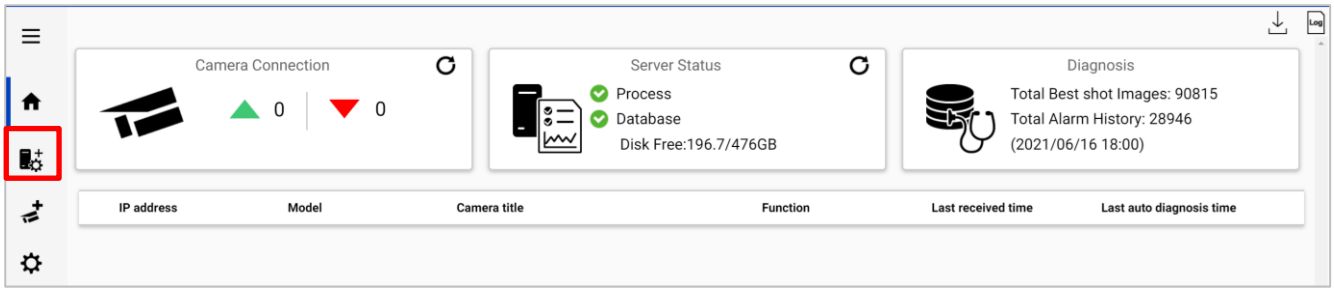


6) Ouvrez « C: \ Windows \ System32 \ drivers \ etc \ hosts » et ajoutez l'adresse IP du serveur i-PRO Active Guard et xxxx (nom DNS).
ex. 192.168.0.125 PC-PA1909C1044R

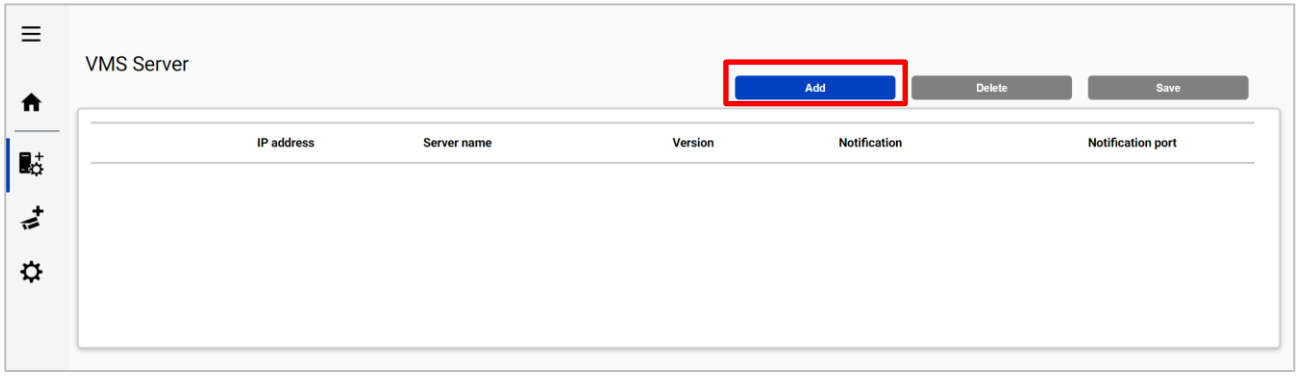
7) Accédez à https:// xxxx:8092 à l'aide d'un navigateur Web.

4.3.2.2. Enregistrer VMS

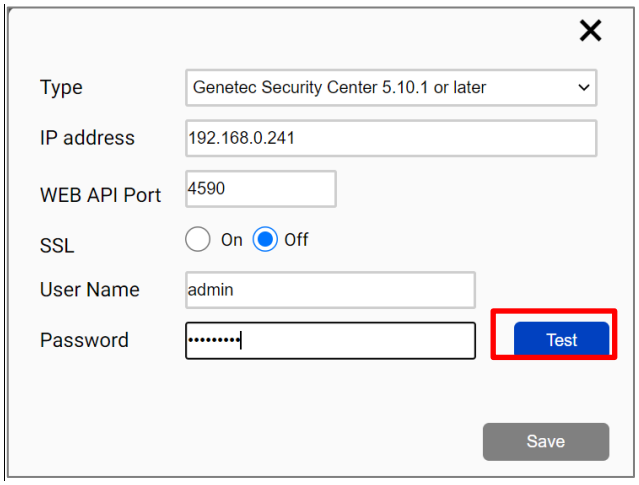
Cliquez sur  (Enregistrer VMS)



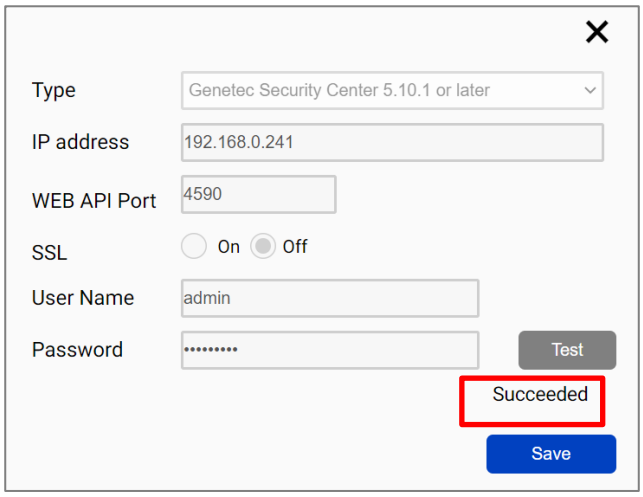
Cliquez sur [Ajouter]



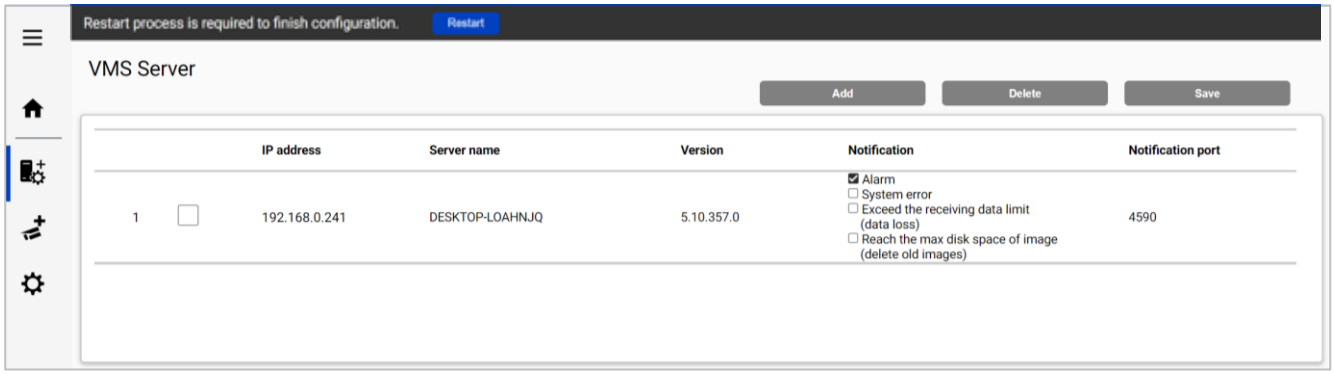
Entrez les informations du Security Center et cliquez sur Test



Lorsque Succeeded est affiché, cliquez sur Enregistrer



Confirmer que le serveur VMS est enregistré

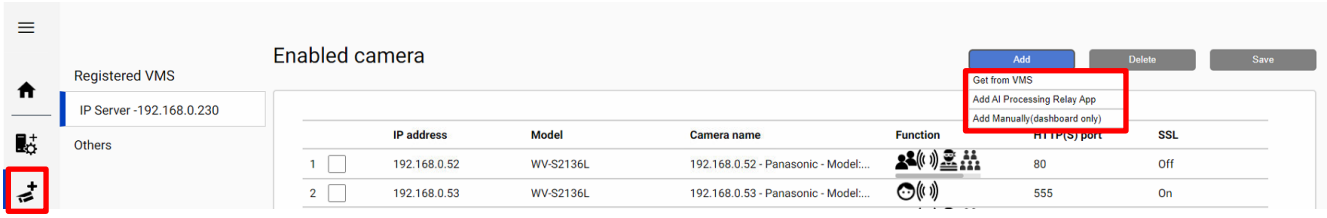


Remarque : Le bouton Redémarrer apparaîtra en haut de l'écran, mais vous n'avez pas besoin de cliquer maintenant. Vous devez cliquer sur Redémarrer après avoir terminé toutes les autres configurations.

4.3.2.3. Enregistrer les caméras

Cliquez sur  (Enregistrer les caméras)

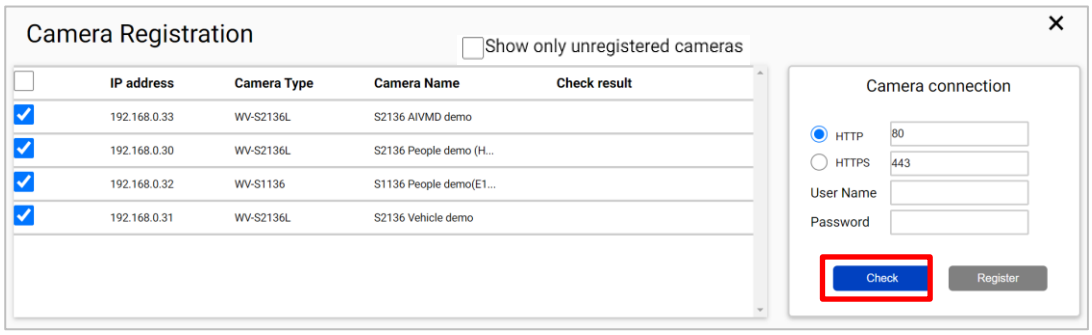
Sélectionnez [Ajouter] - [Obtenir à partir de VMS]



Remarque

- Lorsque la caméra est sélectionnée dans [Ajouter une application de relais de traitement AI], seules les caméras auxquelles l'application AI Processing Relay a été ajoutée peuvent être enregistrées. Configurez les caméras que vous souhaitez relayer dans le navigateur de configuration de l'appareil photo et enregistrez-les à l'avance dans VMS. Entrez l'adresse IP de la caméra, les informations d'identification, [Vérifier] et [Enregistrer].
- Lorsque la caméra est enregistrée à partir de [Ajouter manuellement (tableau de bord uniquement)], seule la fonction de tableau de bord peut être utilisée. Le plug-in ne peut pas utiliser l'appareil photo. Entrez l'adresse IP de la caméra, les informations d'identification, [Vérifier] et [Enregistrer].

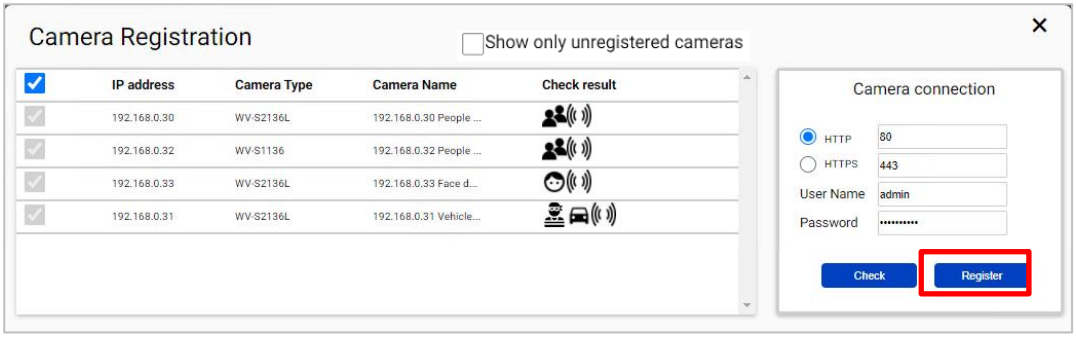
Toutes les caméras i-PRO (y compris les caméras non prises en charge) sont affichées.
Entrez les informations d'identification de la caméra et cliquez sur [Cocher].



Remarque

La caméra peut être triée par [adresse IP], [Type de caméra] ou [Nom de la caméra].
Les caméras non enregistrées peuvent être filtrées en cochant [Afficher uniquement les caméras non enregistrées].

L'icône représentant la fonction AI est affichée pour les caméras AI prises en charge.
Cliquez sur [S'inscrire].



(Détection de personnes AI)

(AI Détection de véhicule)

(Détection de visage AI)

(AI-VMD)

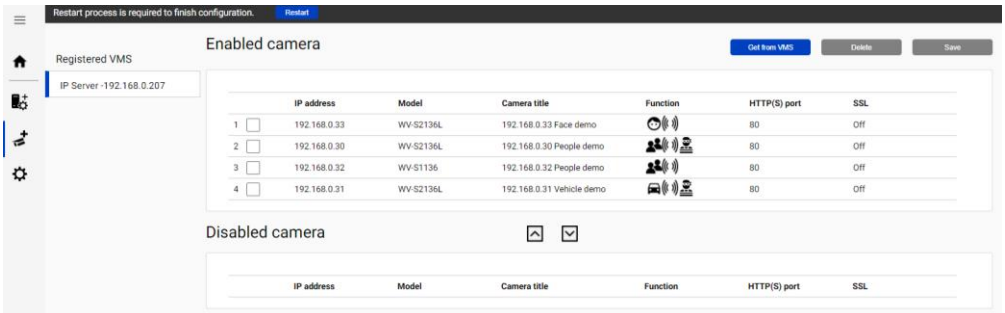
(Classification AI Sound)

(AI People Counting)

(Comptage de véhicules AI)

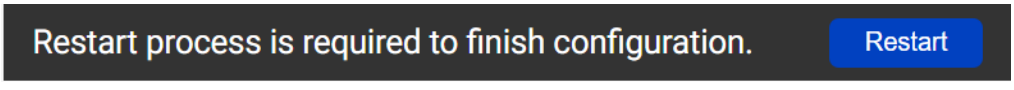
(AIS cene Détection de changement)

Confirmer que les caméras sont enregistrées



4.3.3. Redémarrer le processus pour appliquer les modifications

* Pour toute modification de configuration, un processus de redémarrage est requis.
Lorsque vous avez terminé toute la configuration. Cliquez sur « Redémarrer » dans la barre d'affichage ci-dessus ou sur l'écran d'accueil.

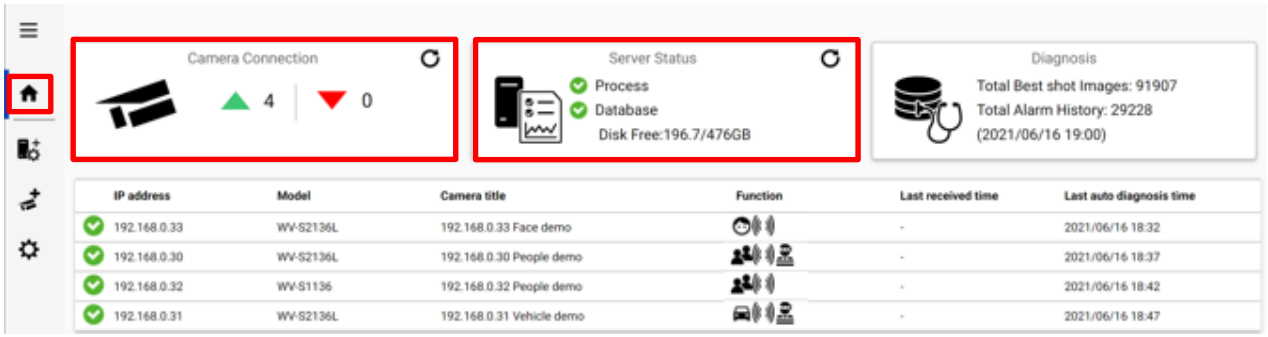


4.3.4. Vérifier

Cliquez sur (Accueil)

- Vérifiez la connexion caméra

Vérifiez que toutes les caméras enregistrées sont connectées.



désigne le nombre de caméras connectées. (session de métadonnées entre la caméra et le serveur i-PRO Active Guard).

désigne le nombre de caméras déconnectées. Lorsque la déconnexion est détectée, confirmez la connexion réseau à la caméra.

- Vérifier l’état du serveur

Vérifier Processus et base de données affiche l’état vert.

4.3.5. Configuration du système (facultatif)

Cliquez sur (Configurer le système) et modifiez les paramètres si nécessaire.

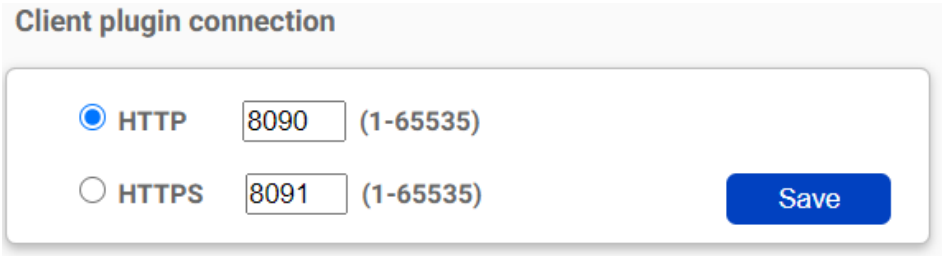
4.3.5.1. Général

Sélectionnez [Auto], [Anglais] ou [Japonais] pour [Langue]. (Valeur par défaut : Auto).
Cochez ou décochez [Envoyer des données anonymes pour améliorer le logiciel et l'expérience utilisateur].

Remarque Lorsque la configuration de la langue du navigateur Web est autre que l'anglais ou le japonais, l'anglais est affiché.

4.3.5.2. Connexion du plug-in client

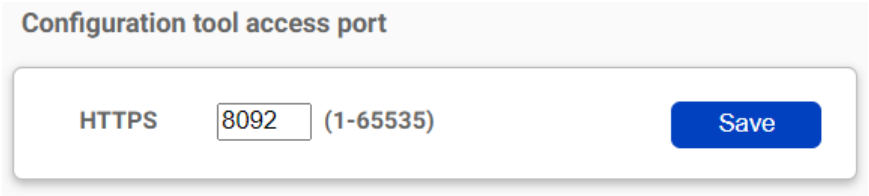
Sélectionnez [HTTP] ou [HTTPS] et le numéro de port (par défaut : défini par l'outil d'installation at 4.3.1)



Remarque Pour une communication sécurisée, HTTPS est recommandé.

4.3.5.3. Accès à la page de configuration

Numéro de port pour l'outil de configuration (par défaut : défini par l'outil d'installation à 4.3.1)



Remarque Lorsque vous modifiez et redémarrez le logiciel à , vous devez accéder à 4.3.3https://<ip>:<port> en utilisant un nouveau numéro de port. Prenez note de ne pas oublier.

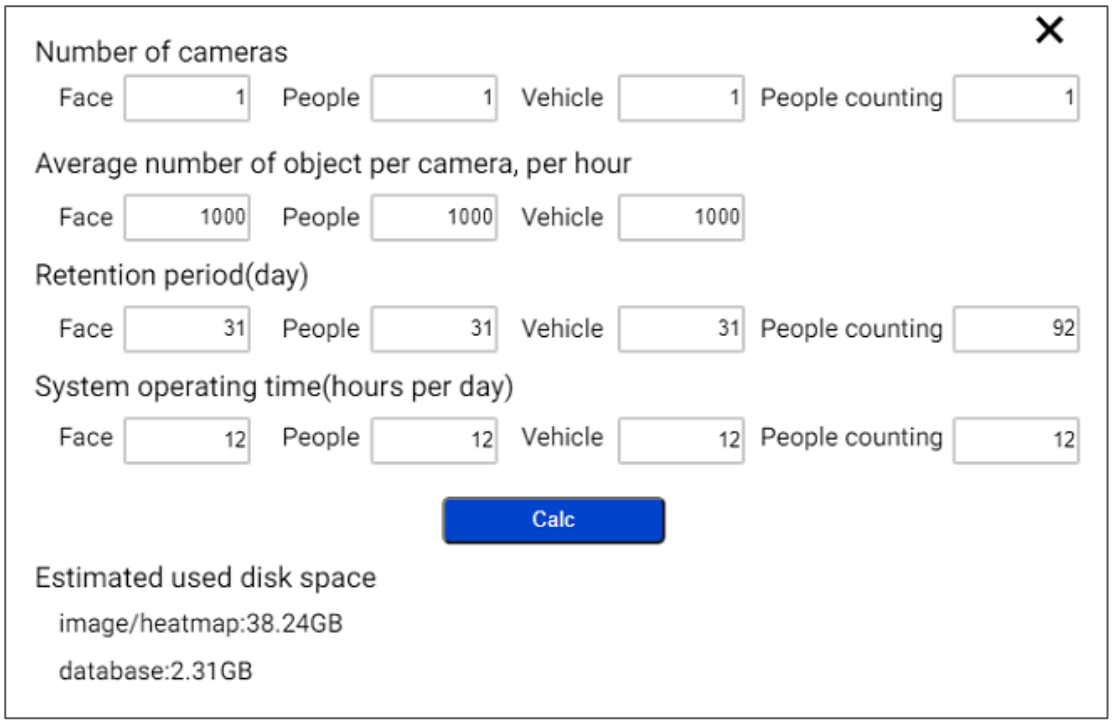
4.3.5.4. Base de données

Configuration item	commentaire
Stockage d'images dans une base de données	Toutes les données (par défaut) : Stockez toutes les données, y compris les images. Uniquement les données d'alarme et de statistiques : stockez uniquement les données d'alarme et de statistiques Données statistiques uniquement : stocker uniquement les données statistiques
Période de conservation	[Pour l'image/les statistiques du visage, l'image/les statistiques, l'image/les statistiques du véhicule et l'historique des alarmes] Utilisation de SQL Server Express Edition : 1 à 31 jours (par défaut : 31) peut être défini Utilisation de SQL Server Standard Edition :1 – 366 jours (par défaut : 366) peut être défini [Pour le nombre de personnes/véhicules , y compris les statistiques sur les cartes thermiques] Utilisation de SQL Server Express Edition : 1 – 92 jours (par défaut : 92) peut être défini Utilisation de SQL Server Standard Edition :1 – 366 jours (par défaut : 366) peut être défini Remarque Les données après la période de conservation seront supprimées la nuit (0h00 ~ 3h30). Si le serveur est arrêté, les données ne peuvent pas être supprimées, de sorte que les nouvelles données peuvent ne pas être stockées en raison du manque d'espace de stockage.
Sauvegarde CSV	Activer/Désactiver peut être configuré. (Valeur par défaut : Désactiver) Lorsque l'option est activée et que la période de rétention des données de comptage de personnes expire, les données sont supprimées de SQL Server, mais automatiquement sauvegardées en tant que fichier CSV. Les données du fichier CSV ne peuvent pas être affichées sur le tableau de bord. Remarque Lorsque cette option est activée, [Utilisation maximale du lecteur de stockage d'images] est également activée automatiquement.
Utilisation maximale du lecteur de stockage d'images(*)	Activer/Désactiver et la taille de données 10- 2000 (Go) peut être configurée. (Valeur par défaut : Désactiver) Remarque

	Lorsque cette option est activée et que l'espace disque utilisé du lecteur pour stocker les meilleures images dépasse la valeur du paramètre, l'ancienne image est automatiquement supprimée. Cela fonctionne toutes les heures. Vous pouvez gérer la taille des données à l'aide de cette configuration stockée par le serveur i-PRO Active Guard. L'espace disque utilisé est égal au volume total moins l'espace libre.
Chemin d'enregistrement des données d'image	Chemin d'enregistrement des images (par défaut : C:\MultiAI\Image) Remarque Lorsque vous modifiez le chemin d'enregistrement, toutes les données d'image existantes ne peuvent pas être utilisées à partir du plug-in.
Chemin d'accès à l'enregistrement des données SQL Server	Le chemin d'enregistrement des données SQL Server est indiqué parinstall tool à 4.3.1. Vous ne pouvez pas modifier cela après l'installation.
Fréquence maximale de réception Données d'objet (par seconde)	50 -300 (Default: 100) Remarque : Si le nombre de données d'objet de toutes les caméras dépasse la valeur, ces données d'objet seront supprimées pour réduire l'accès au disque afin que le système soit stable. SSD est requis en cas de 100 ou plus. Lorsque vous définissez plus de 100 à l'aide du disque dur, le système sera instable.
Cryptage des données	On/Off est affiché set par install tool à 4.3.1. Vous ne pouvez pas modifier cela après l'installation.

* Une calculatrice simple peut être utilisée en cliquant sur 

Entrez les paramètres de votre système et cliquez sur Calc.
L'estimation de l'espace disque utilisé est affichée.



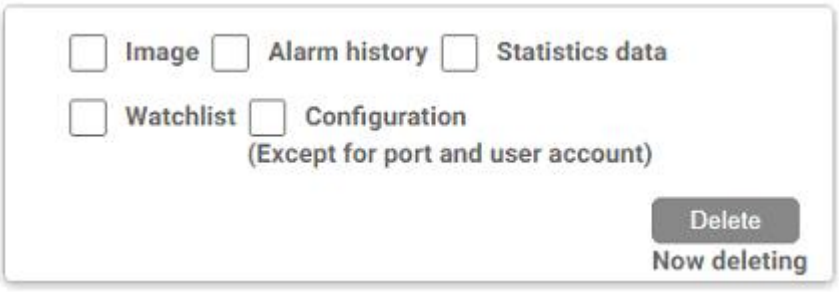
Remarque

L’espace disque utilisé estimé n’est qu’une référence. La taille réelle des données dépend fortement de l’environnement réel.

4.3.5.5. Initialisation

Image: supprimez les Best shot images.
Historique des alarmes : supprimez un historique des alarmes.
Données statistiques : supprimez les données statistiques, y compris les données de carte thermique.
Liste de surveillance : supprimez une liste de surveillance LL Face, une liste de surveillance de personnes et une liste de surveillance de véhicules . Voir le manuel d'utilisation sur la liste de surveillance.
Configuration : supprimez toutes les données d'enregistrement (VMS, caméra et journaux) à l'exception du port et du compte utilisateur.

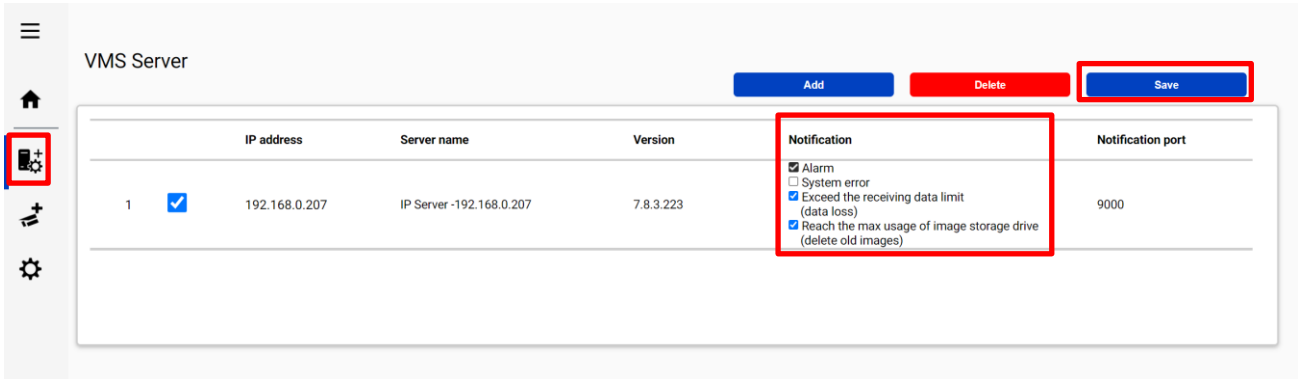
Remarque
La suppression de l'image peut prendre du temps en fonction du nombre d'images. Lors de la suppression, le bouton sera le suivant. Veuillez mettre à jour la page pour confirmer le dernier statut.



4.3.6. Notification au serveur VMS (facultatif)

Certaines alarmes liées à une défaillance du serveur i-PRO Active Guard peuvent être activées.
Les actions côté VMS peuvent également être configurées (4.7 Configuration personnalisée de l'alarme (en option))

Cliquez sur  (Enregistrer VMS)



Cochez les éléments suivants que vous souhaitez et enregistrez.

Erreur système

Erreur détectée par le serveur i-PRO Active Guard. (ex. erreur de connexion de caméra entre la caméra et le serveur i-PRO Active Guard.)

Dépasse la limite de données de réception (perte de données)

Lorsque les données dépassent la valeur de paramètre « Fréquence maximale de réception des données d'objet (par seconde) » configurée à 4.3.5.4.

Atteindre l'espace disque maximum de l'image (supprimer les anciennes images)

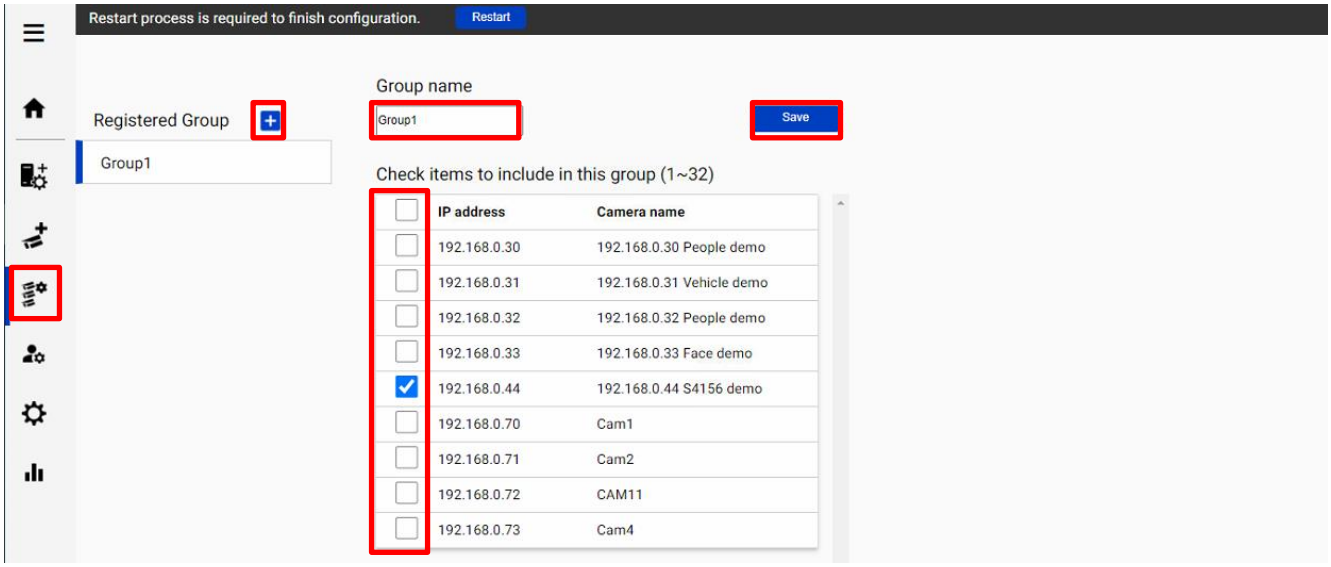
Lorsque l'utilisation du lecteur de stockage d'images dépasse la valeur de paramètre « Utilisation maximale du lecteur de stockage d'images (Go) » configurée à 4.3.5.4.

4.3.7. Configuration du tableau de bord (facultatif)

4.3.7.1. Configuration du groupe de caméras

Lors de l'affichage du graphique sur le tableau de bord, il est possible de l'afficher sous forme d'informations statistiques pour chaque groupe composé de plusieurs caméras au lieu d'informations statistiques pour chaque caméra.

Click  (groupe de caméras).



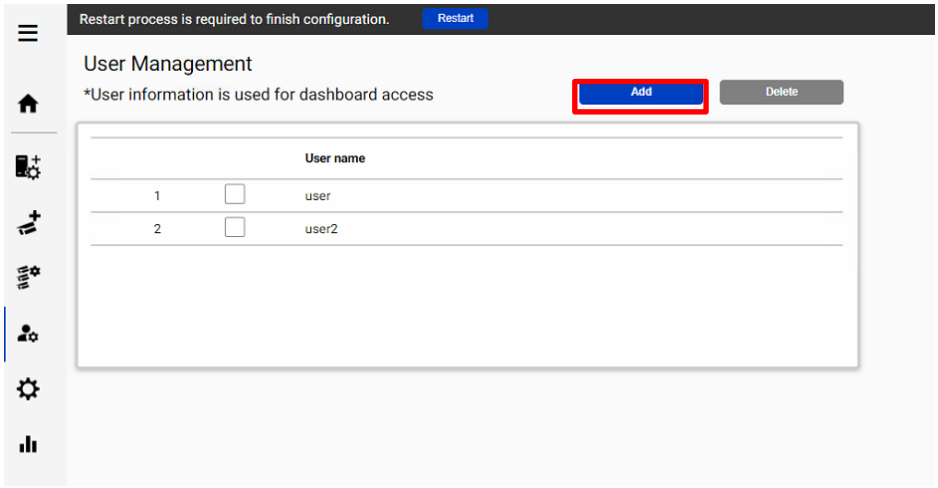
Cliquez sur le bouton [+], entrez le nom du groupe, vérifiez la présence de caméras et [Enregistrer].

Remarque Jusqu'à 16 groupes peuvent être configurés.
Pour supprimer un groupe de caméras, cliquez dessus avec le bouton droit de la souris et sélectionnez [Supprimer le groupe de caméras].

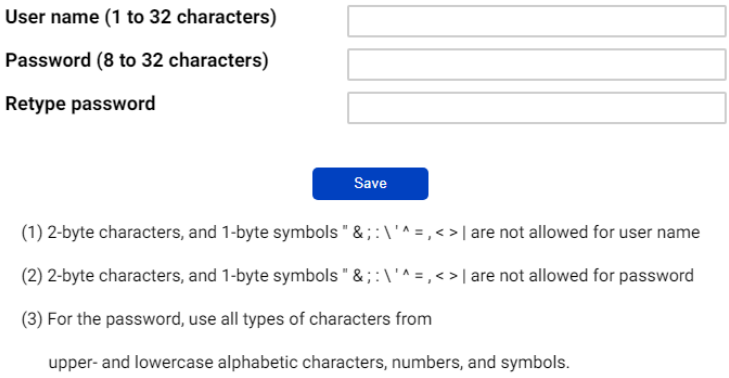
4.3.7.2. Gestion des utilisateurs

En enregistrant plusieurs utilisateurs, il est possible de personnaliser l'affichage du tableau de bord pour chaque utilisateur.

Cliquez sur  (Gestion des utilisateurs) et [Ajouter].



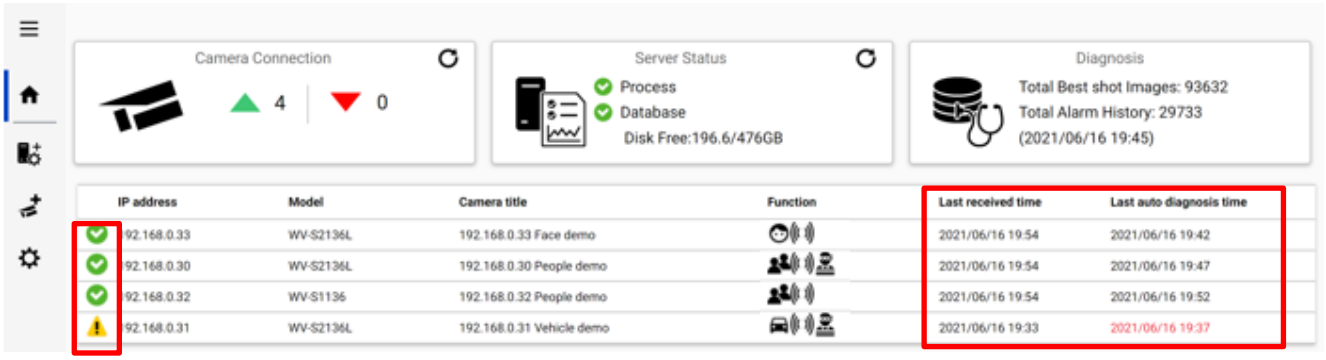
Entrez [Nom d'utilisateur], [Mot de passe] et [Retaper le mot de passe], puis [Enregistrer]



Note : Les informations utilisateur peuvent également être utilisées pour la connexion Plug-in.
[Nom d'utilisateur] défini par l'outil d'installation à 4.3.1 est affiché par défaut. [Mot de passe] n'est pas affiché.
Si vous oubliez le mot de passe, supprimez l'utilisateur et enregistrez-vous à nouveau.

4.3.8. Plus d’informations sur le statut (facultatif)

4.3.8.1. Connexion de la caméra



: La caméra est connectée.

: La caméra n’est pas connectée.

: l’appareil photo est connecté, mais la dernière erreur de résultat de diagnostic automatique.

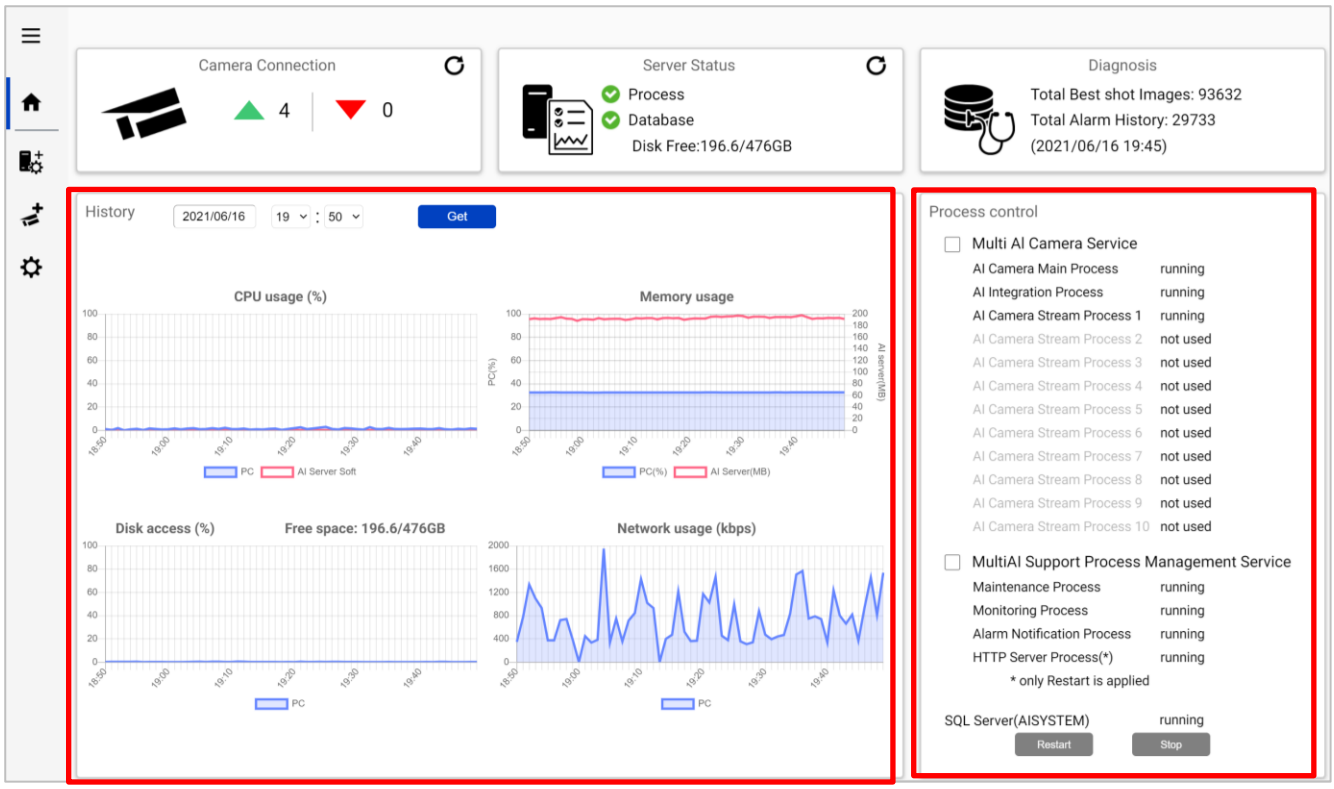
La session de métadonnées est connectée, mais l’application d’IA côté caméra peut ne pas fonctionner correctement. Vérifiez que l’application AI côté caméra est installée, que le réglage de la planification est activé et vérifiez également si « Dernière heure de réception ».

« **Heure** de la dernière réception » indique l’heure de détection de la dernière fois que la caméra a détecté le visage, les personnes, le véhicule ou l’alarme. Si ce temps est plus long que lorsque la caméra a capturé des objets, l’application d’IA côté caméra peut ne pas fonctionner correctement.

« **Dernière heure de diagnostic automatique** » est la dernière heure à laquelle le serveur i-PRO Active Guard a testé la connexion à la caméra et à la base de données. Le test s’exécute toutes les 5 minutes pour une caméra dans l’ordre. En cas d’erreur, l’heure est affichée en rouge. Dans ce cas, cochez la case Journal et confirmez l’état de la caméra ou de la base de données.

Remarque Lorsque le paramètre de planification pour l’application AI est désactivé, le dernier diagnostic automatique échoue. Si c’est prévu, veuillez ignorer cet indicateur.

4.3.8.2. État du serveur



Historique

L'historique montre l'utilisation du processeur, l'utilisation de la mémoire, l'accès au disque et l'utilisation du réseau du serveur i-PRO Active Guard. L'utilisation du processeur et l'utilisation de la mémoire affichent la valeur totale dans le PC et le serveur i-PRO Active Guard.
Les données d'une heure à compter de la date spécifiée sont affichées. Sélectionnez la date et obtenez pour la date précédente (dans les 31 jours peuvent être affichés).

Ces données peuvent être utilisées pour vérifier si les performances du PC sont stables après l'installation ou l'enquête sur le problème du système.

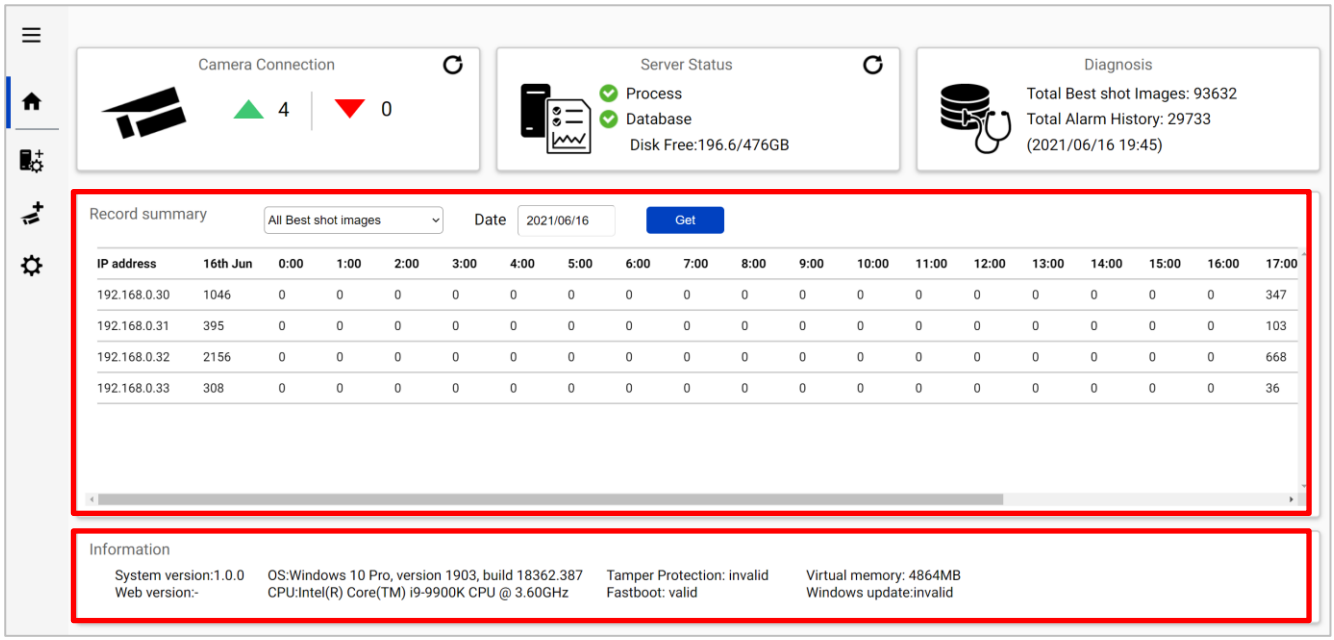
Remarque Les données peuvent ne pas s'afficher correctement lorsque le PC est éteint ou que le logiciel serveur i-PRO Active Guard est arrêté pendant un certain temps.

Contrôle des processus

Les processus liés au serveur i-PRO Active Guard peuvent être redémarrés ou arrêtés. Lorsque le système est en cours d'exécution, veuillez vérifier que tous les processus affichent « en cours d'exécution » ou « non utilisé ».
(Le nombre de « AI Camera Stream Process x » utilisé dépend du nombre de caméras enregistrées.)
Lorsqu'il est nécessaire de redémarrer le PC, cochez « Multi AI Camera Service » et « Support Process Management Service » sont arrêtés (voir 5.6.1également).

Lorsque l'enquête sur les problèmes du système est requise, vérifiez l'état et essayez de redémarrer.

4.3.8.3. Diagnostic



Résumé du dossier

Le résumé de l'enregistrement indique le nombre de données reçues de chaque caméra à la date spécifiée.

Les éléments sélectionnables dépendent de la caméra enregistrée et de l'application d'IA.

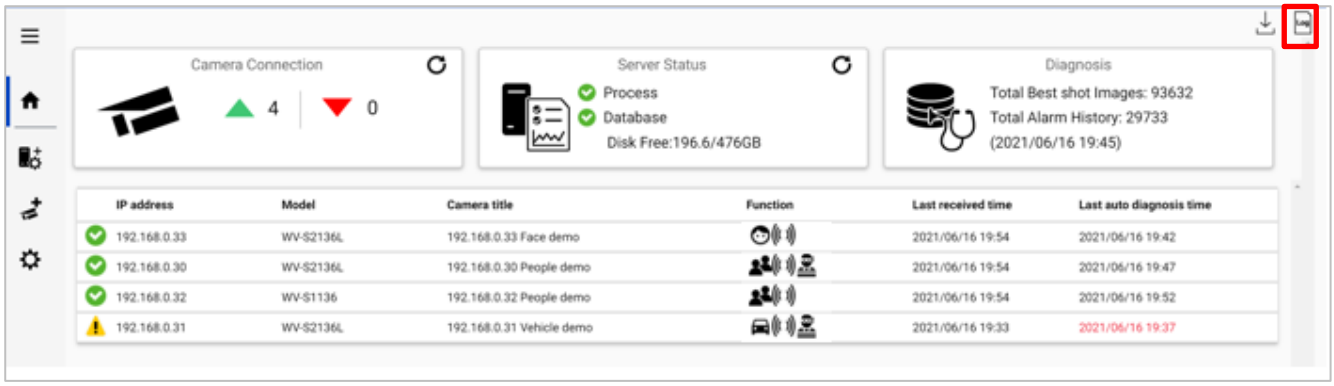
*Articles sélectionnables

- Toutes les meilleures images prises
- Visage Meilleures images
- Personnes Meilleures images prises
- Véhicule Meilleures images
- Toutes les alarmes
- Détection de visage enregistrée
- Détection des personnes enregistrées
- AI-VMD
- Détection sonore
- Détection d'occupation IA
- Détection de véhicule enregistré
- Détection de changement de scène AI

Informations

La version du logiciel, le système d'exploitation, la configuration Windows sont affichés.

4.3.8.4. Journal d’affichage

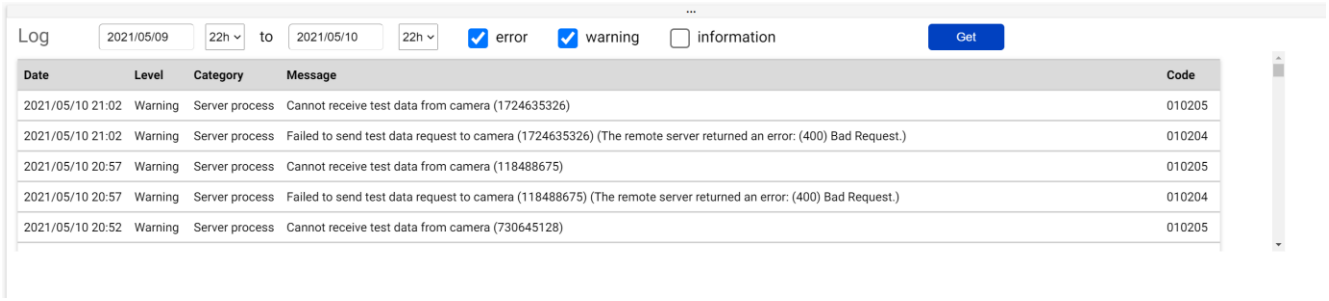


Cliquez 

pour afficher les journaux.

Un aperçu de l’erreur système peut être affiché. Sélectionnez la date et le niveau d’erreur (erreur, avertissement et informations) et cliquez sur Obtenir.

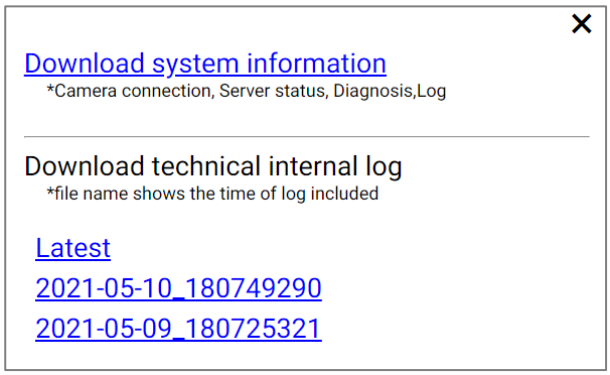
Les détails de chaque message et dépannage pour le code sont affichés sur .6.Résolution des problèmes



Remarque Un maximum de 1000 journaux peut être affiché en même temps.

4.3.8.5. Télécharger le journal

Cliquez pour télécharger le journal.



Télécharger les informations système

Téléchargez Camera Connection, Server Status, Diagnosis et Log chargés à l'écran au format json.

Télécharger le journal technique interne

Télécharger le journal détaillé. Le nom de fichier « aaaa-mm-dd_hhmmssfff » indique l'heure du journal incluse. Les fichiers journaux sont compressés automatiquement en fonction de la durée ou de la taille et le nom du fichier indique l'heure de compression.

Ex. « 2021-05-10_180749290 » inclut les journaux de 2021-05-09 18:07:25.321 à 2021-05-10 18:07:49.290 sur cet exemple.

4.3.9. Paramètre Windows

Une configuration Windows complète est nécessaire pour que le travail du serveur i-PRO Active Guard soit stable.
L'emplacement de la configuration peut varier en fonction du système d'exploitation.

4.3.9.1. Désactiver la protection en temps réel et la protection contre les falsifications

Ceci est nécessaire pour que le serveur i-PRO Active Guard conserve les performances de base.

Dans le cas de Windows 10,
(Démarrer – Paramètres – Système – Mise à jour et sécurité – Sécurité Windows – Protection contre les virus et les menaces – Protection contre les virus et les menaces – Paramètres de protection contre les virus et les menaces – Gérer les paramètres)
Désactivez la « Protection en temps réel » et la « Protection contre les falsifications ».
Serveur Windows Le système d'exploitation n'a pas de fonction de protection contre les falsifications.

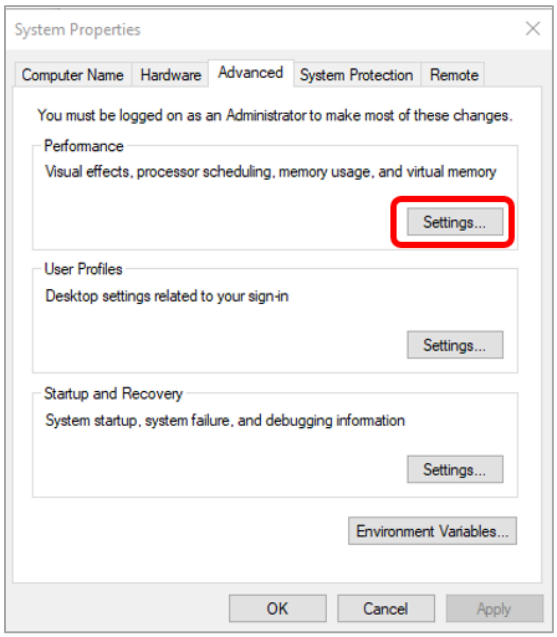
4.3.9.2. Désactiver le service Windows Update

Les mises à jour Windows sont importantes pour maintenir le système à jour, mais la mise à jour automatique peut entraîner un redémarrage non planifié et certaines nouvelles fonctionnalités de Windows peuvent influencer le serveur i-PRO Active Guard. Pour éviter les redémarrages ou les influences imprévus, désactivez le service de mise à jour Windows.

Dans le cas de Windows 10,
Démarrer - Outils d'administration Windows - Services - clic droit « Windows Update » - Propriétés - sélectionnez « Désactivé » pour « Type de démarrage » et cliquez sur OK.

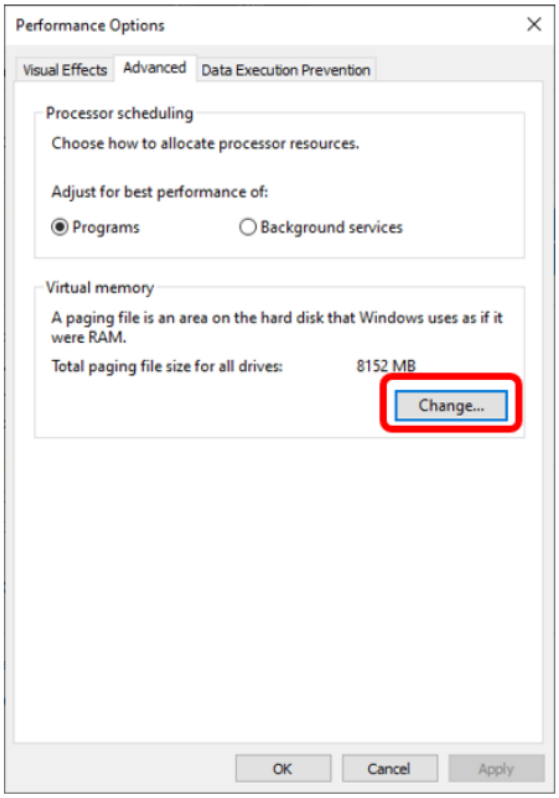
4.3.9.3. Paramètre de mémoire virtuelle

Si la mémoire virtuelle est insuffisante, la base de données peut s'arrêter.
Suivez les procédures ci-dessous pour vérifier le paramètre de mémoire virtuelle



Dans le cas de Windows 10,
Démarrer – Système Windows – Panneau de configuration – Système et sécurité – Système – Paramètres système avancés

Sélectionnez Paramètres



Sélectionnez l'onglet « Avancé » sur l'écran « Options de performance » et cliquez sur « Modifier... » de Mémoire virtuelle.

Vérifiez que l'option « Gérer automatiquement la taille du fichier d'échange pour tous les lecteurs » est cochée sur l'écran « Mémoire virtuelle ».
Cochez-le et cliquez sur le bouton « OK ».

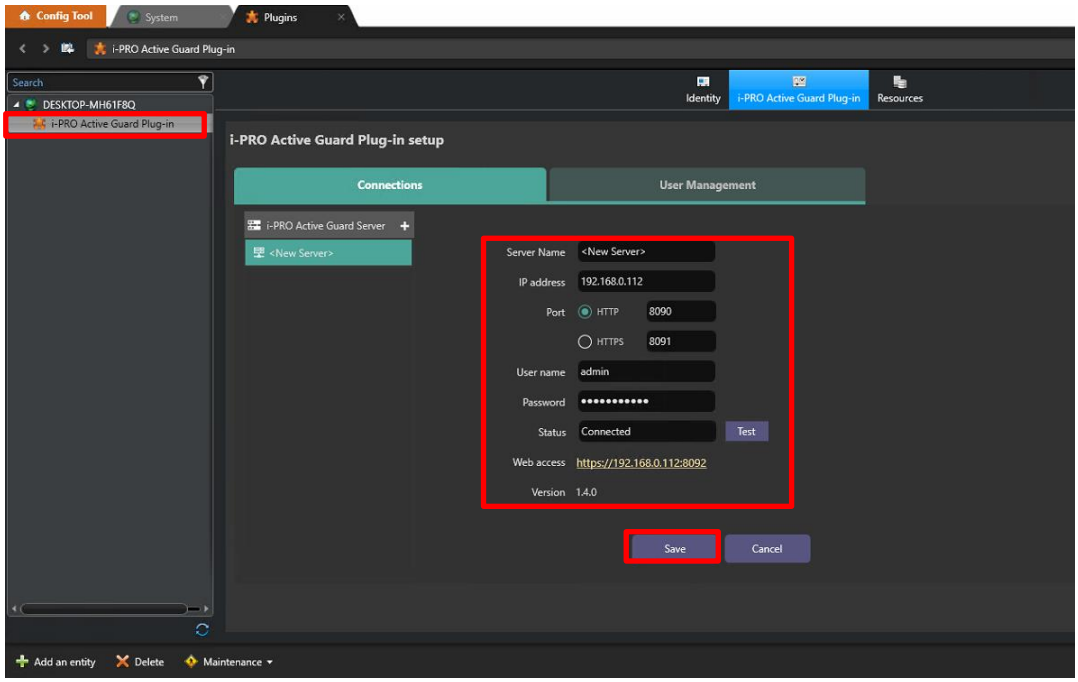
4.4. Installation et configuration du plug-in pour Security Desk

4.4.1. Installer le plug-in sur Security Desk

Installer le plug-in sur le PC qui est Security Desk est installé en se référant à la section 4.2.2.1.

4.4.2. Connexion au serveur i-PRO Active Guard

Connectez Config Tool à Security Center. Sélectionnez [Plugin], [i-PRO Active Guard Plugin]. Entrez les informations du serveur Active Guard et cliquez sur [Test], puis sur [Enregistrer].

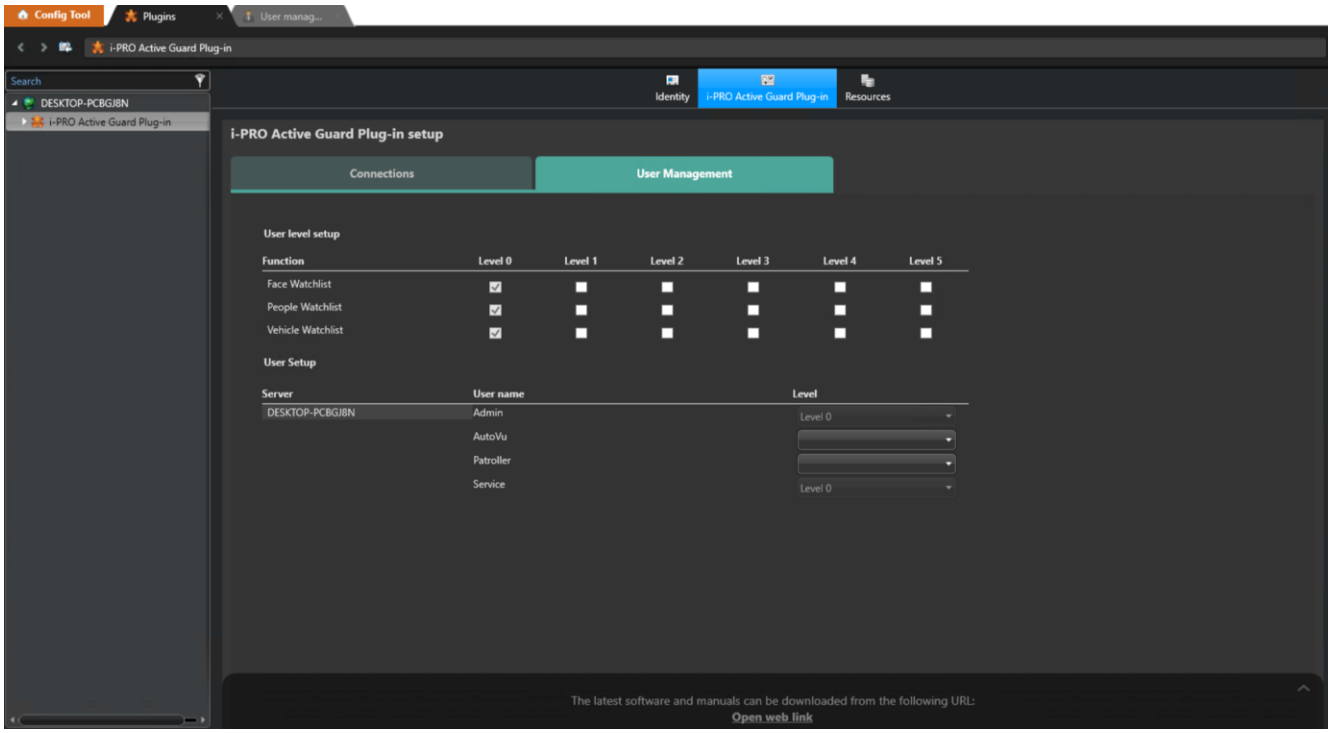


Remarque Si le test a échoué, veuillez vérifier que les informations d’identification sont correctes.

4.4.3. Gestion des utilisateurs (facultatif)

4.4.3.1. Privilèges pour une fonction spécifique au plug-in

Configurez User Management pour l'accès [Face Watchlist], [People Watchlist] et [Vehicle Watchlist]. Vous devez également configurer les paramètres utilisateur ([Outil de configuration]-[Gestion des utilisateurs] - [Privilèges]) pour que les administrateurs ne soient pas dans la liste de surveillance des utilisateurs.



4.4.3.2. Privilèges requis pour utiliser le plugin pour les non-administrateurs

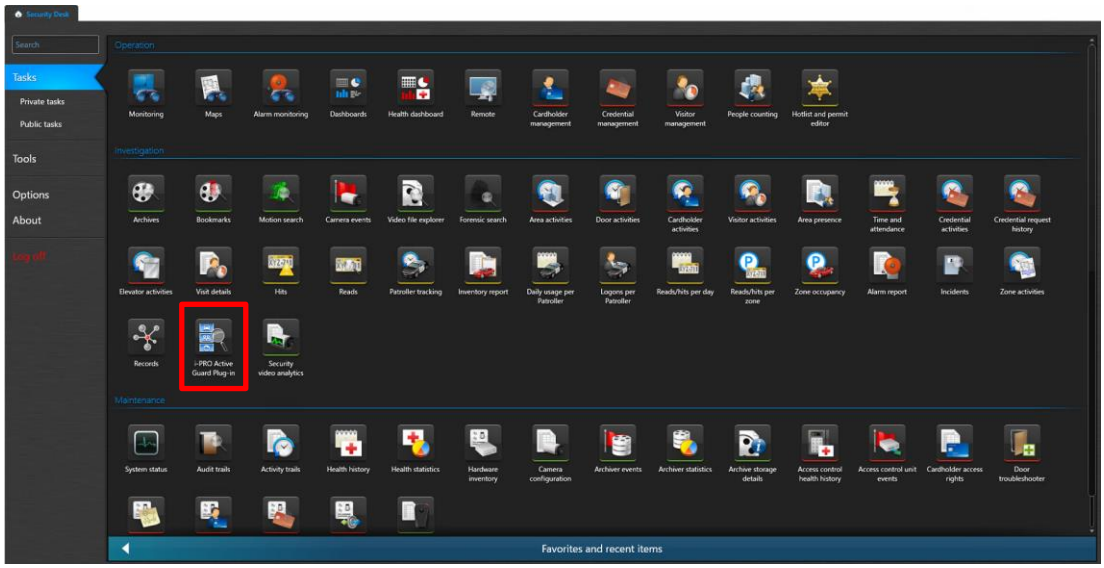
Si un non-administrateur utilise ce logiciel, les privilèges suivants doivent être définis sur [Autoriser] au moins.

- [Privilèges d'application] – [Bureau de sécurité]
- [Privilèges de tâche] – [Administration] – [Plugins]
- [Privilèges d'action] – [Caméras]

En plus de cela, vous devrez peut-être accorder plus de privilèges en fonction des fonctionnalités de Security Center que vous utilisez.

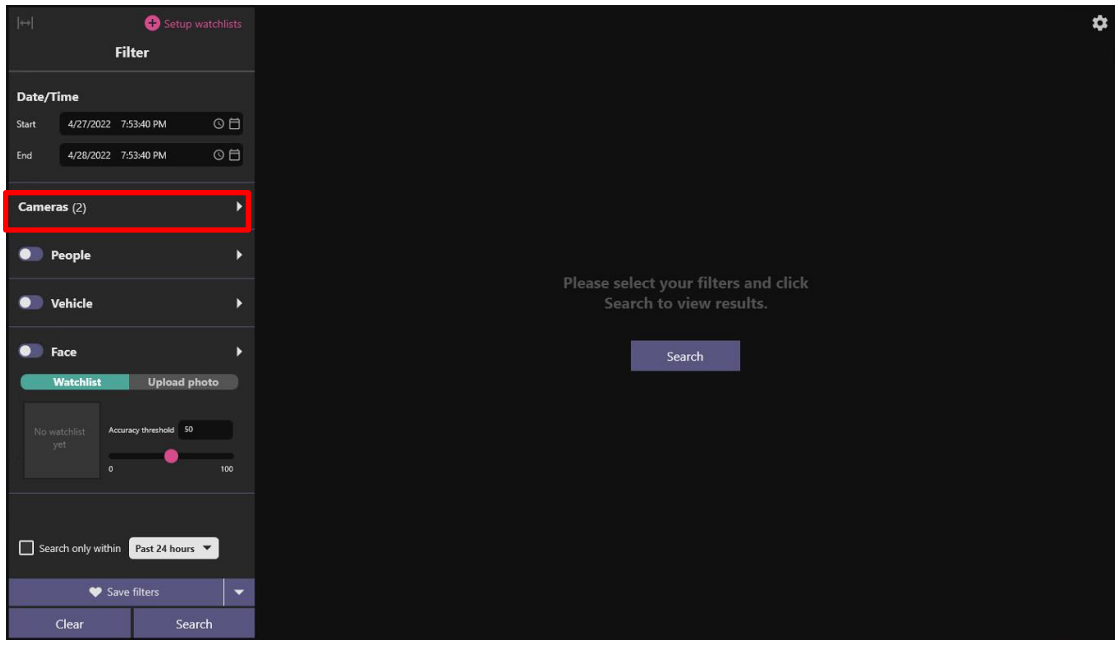
4.4.4. Vérifier

Démarrez Security Desk et sélectionnez [i-PRO Active Guard Plug-in].



Lorsque le numéro est affiché pour « Caméras (x) », la connexion a réussi.

* x signifie le nombre de caméras sur lesquelles le logiciel d’extension Face, People ou Vehicle est installé.

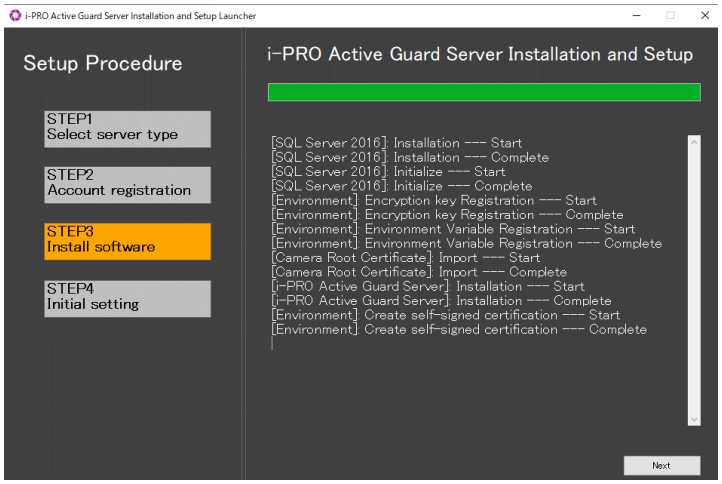


Lorsqu’un appareil photo a détecté un objet, vous pouvez rechercher les meilleures images prises en cliquant sur Rechercher.

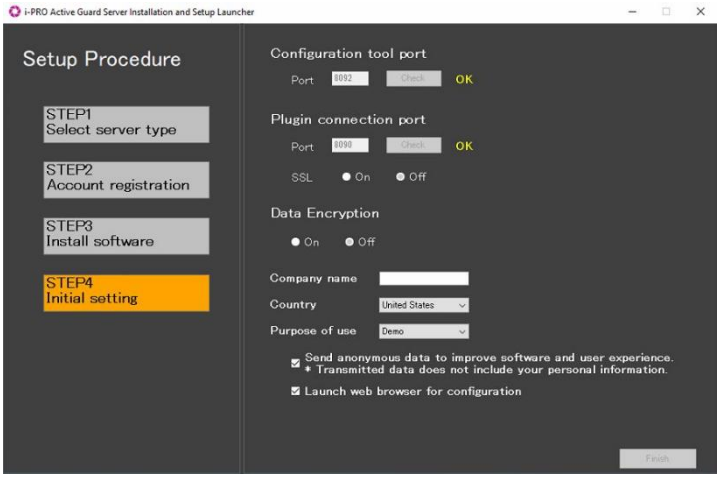
4.5. Mise à niveau du serveur i-PRO Active Guard

[Important]
Lors de la mise à niveau de la version du serveur i-PRO Active Guard, ne désinstallez pas la version déjà installée. Si vous le désinstallez, vous ne pourrez pas utiliser les données passées.

Exécutez « MultiAIStartupGV.exe » en tant qu'administrateur (la longueur du chemin d'accès au fichier doit être inférieure à 120).
Vérifiez [Accepter] pour la durée de la licences et [OK].



Installation démarre et le bouton [Suivant] apparaîtra lorsque vous aurez terminé. Cliquez [Suivant].



Cliquez sur [Terminer].

4.6. Plug-in de mise à niveau

ÉTAPE 1

Démarrez « Panneau de configuration » - « Outils d'administration » - « Services ».

Sélectionnez « Genetec Server » et « Arrêter » dans le menu contextuel.

ÉTAPE 2

Lancez le programme d'installation exécutable en tant qu'administrateur.

Cliquez sur le bouton [Suivant], puis cochez la case [J'accepte les termes du contrat de licence], puis cliquez sur le bouton [install]

Lorsque la fenêtre Installation terminée s'affiche, cliquez sur le bouton [Terminer].

ÉTAPE 3

Démarrer « Panneau de configuration » - « Outils d'administration » - « Services »

Sélectionnez « Genetec Server » et « Démarrer » dans le menu contextuel.

4.7. Configuration personnalisée de l’alarme (en option)

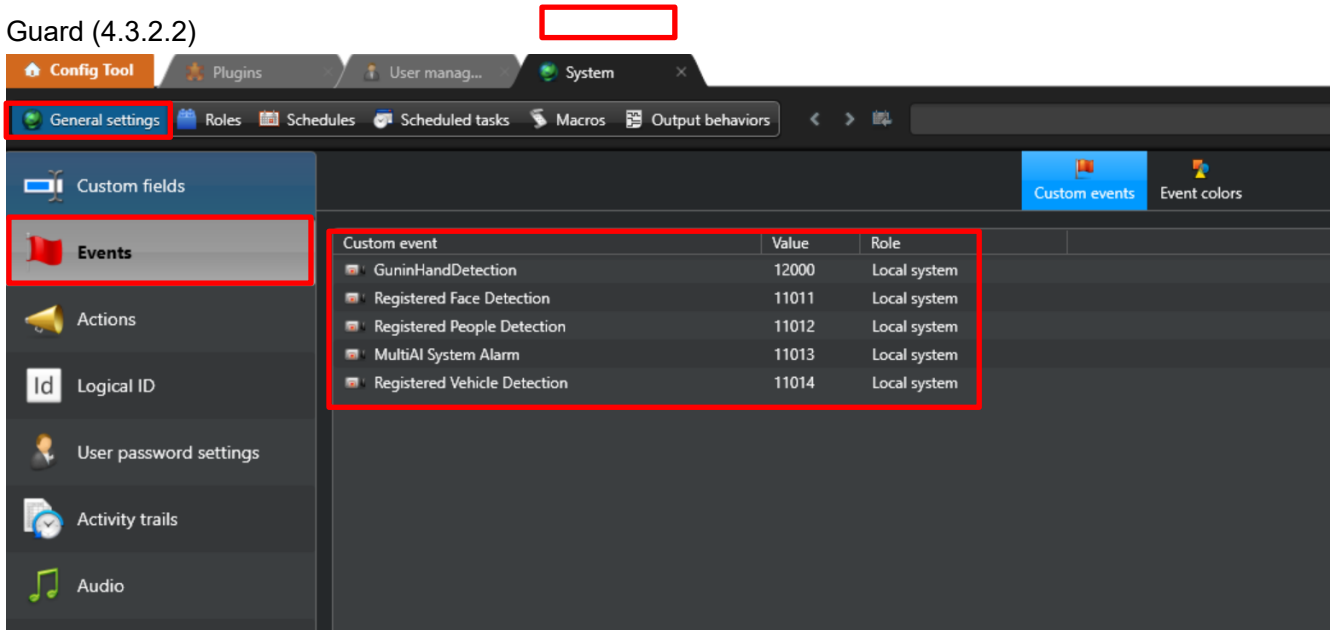
La détection de visage enregistrée, la détection de personnes enregistrées et l’alarme système du serveur i-PRO Active Guard peuvent être utilisées comme événement personnalisé sur Security Center.

ÉTAPE 1

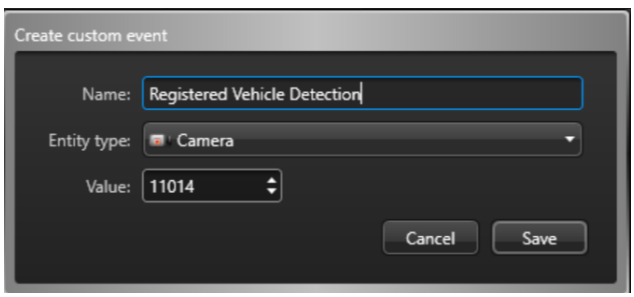
Connectez Config Tool à Security Center. Sélectionnez [Système] - [Paramètres généraux] - [Événements].

Confirmez que « Détection de visage enregistrée », « Détection de personnes enregistrées », « Détection de véhicule enregistré » et « Alarme système multi-IA » existent.

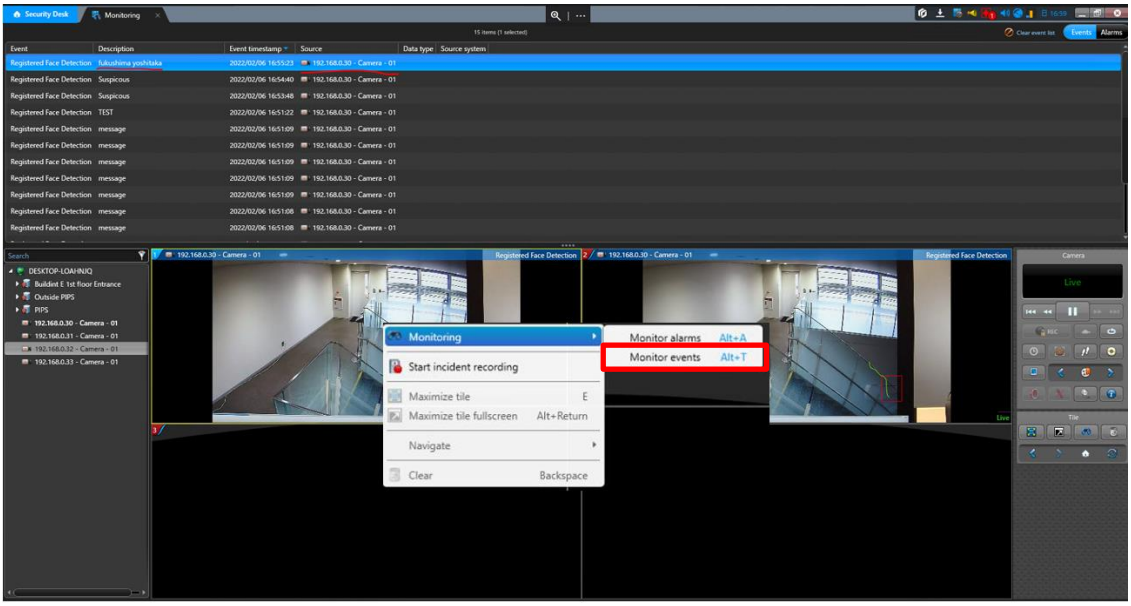
Ceux-ci sont ajoutés automatiquement lorsque Security Center est enregistré sur le serveur i-PRO Active Guard (4.3.2.2)



Remarque　Si vous mettez à jour votre serveur de la version 1.51 ou antérieure à la version 1.60 ou ultérieure, la fonction « Détection de véhicule enregistré » ne sera pas ajoutée automatiquement. Si vous souhaitez l’ajouter, veuillez créer un événement personnalisé manuellement.



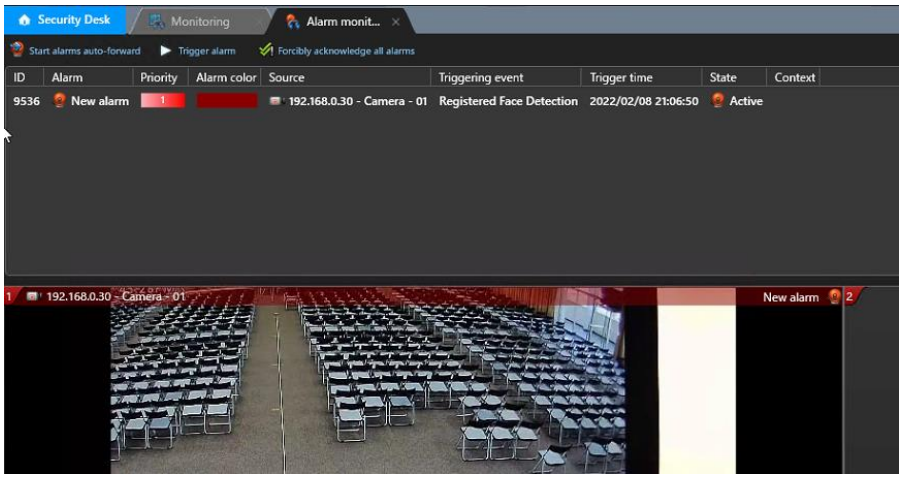
En activant [Surveillance] – [Surveiller les événements], « Détection des visages enregistrés » et « Détection des personnes enregistrées » seront affichés.



La détection de visage enregistrée, la détection de personnes enregistrées et l'alarme système du serveur i-PRO Active Guard peuvent également être affichées comme « Alarme » en configurant [Alarme] et [Actions],

ÉTAPE 2

Sélectionnez le paramètre [Actions]. Définissez [Quand] sur l'événement personnalisé ajouté à l'étape 1 et sélectionnez la caméra pour la source de l'événement. Et sélectionnez [Action] dans le menu déroulant. (Les autres éléments de paramètre dépendent de [Action].)



Remarque Pour utiliser Multi-AI System Alarm, vous devez également activer la configuration i-PRO Active Guard (reportez-vous à la section 4.3.6).

5. Lors du changement de composant système

5.1. Ajouter un périphérique système

5.1.1. Ajouter une caméra

ÉTAPE 1

Enregistrez des caméras AI sur le serveur Security Center à l'aide de Security Desk (reportez-vous à 4.2.1la section).

ÉTAPE 2

Enregistrer des caméras AI sur le serveur i-PRO Active Guard (voir 4.3.2.3)

ÉTAPE 3

Processus de redémarrage (voir 4.3.3)

5.2. Supprimer le périphérique système

5.2.1. Supprimer l'appareil photo

ÉTAPE 1

Vérifiez la caméra et [Supprimer] à partir de l'écran Enregistrer les caméras.

Les données existantes de la caméra sélectionnée ne seront pas disponibles.

ÉTAPE 2

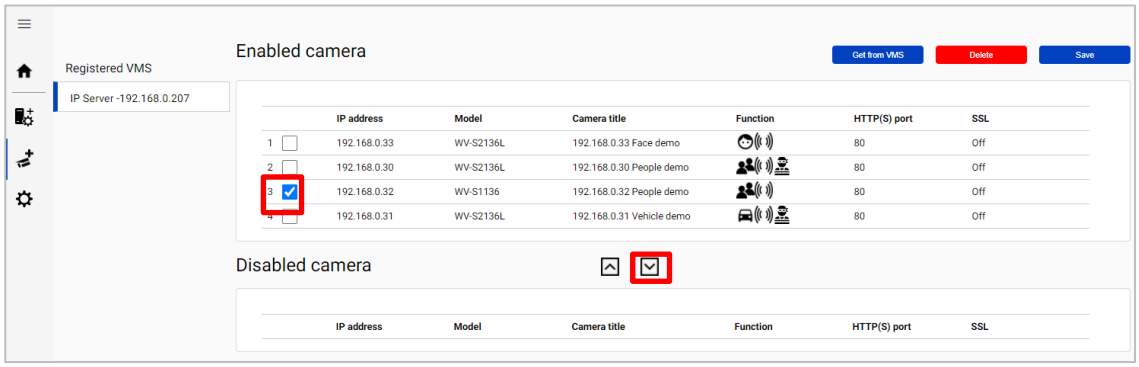
Processus de redémarrage (voir 4.3.3)

5.2.2. Désactiver la caméra

Lorsque vous souhaitez désactiver temporairement des caméras spécifiques, ce qui signifie qu'il est possible que vous souhaitiez rechercher ultérieurement les données existantes de la caméra, configurez la caméra sur Caméra désactivée.

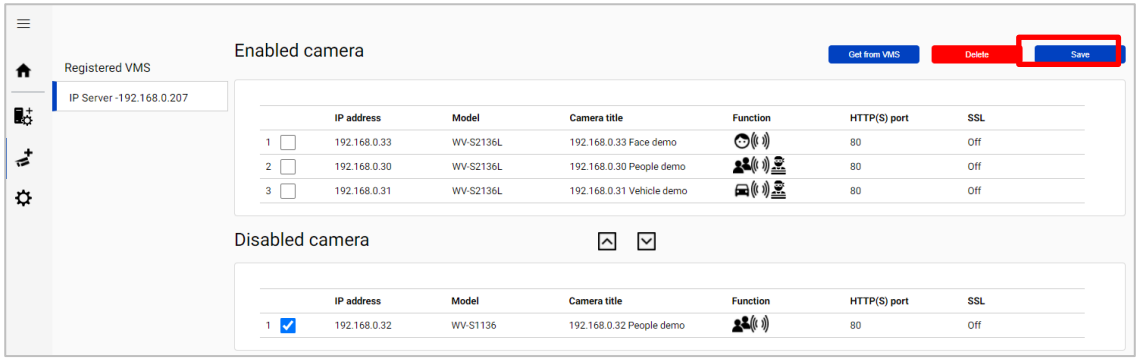
ÉTAPE 1

Vérifiez la caméra et passez à Caméra désactivée à partir de l'écran Enregistrer les caméras.
Les données existantes de la caméra sélectionnée ne seront pas disponibles tant que la caméra est désactivée.



ÉTAPE 2

[Enregistrer]



ÉTAPE 3

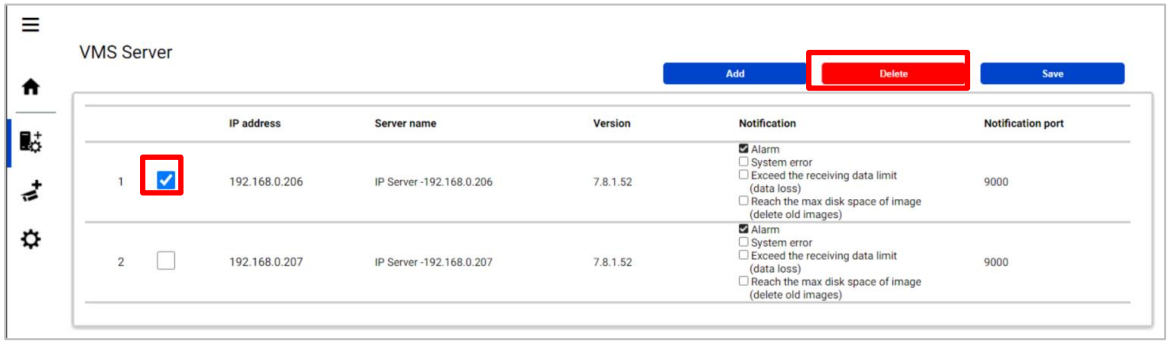
Processus de redémarrage (voir 4.3.3)

Lorsque vous souhaitez utiliser à nouveau l'appareil photo et les données existantes de l'appareil photo, passez à Appareil photo activé et [Enregistrer].
Les données existantes de la caméra seront disponibles tant que la période de rétention n'est pas dépassée à partir du plug-in.

5.2.3. Supprimer Security Center

ÉTAPE 1

Vérifiez le serveur et [Supprimer] à partir de l'écran Enregistrer VMS.
Les caméras appartenant au serveur sélectionné sont également supprimées et les données sortantes ne seront pas recherchées à partir du plug-in.
Lorsque le même serveur VMS est à nouveau enregistré, les données existantes deviennent disponibles.
Les meilleures images et la base de données associée seront supprimées lorsque la période de rétention dépasse.



ÉTAPE 2

Processus de redémarrage (voir 4.3.3)

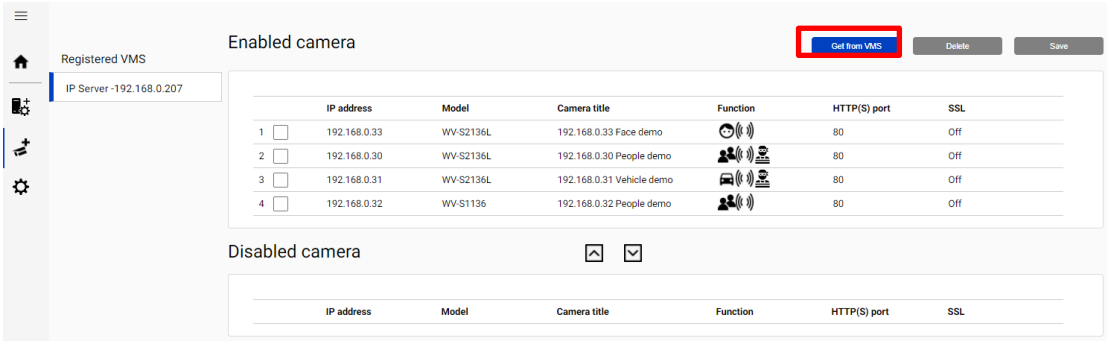
5.3. Ajouter ou modifier le logiciel d’extension de la caméra

ÉTAPE 1

Installez ou modifiez le logiciel d’extension à l’aide d’iCT. (Reportez-vous à 4.1)

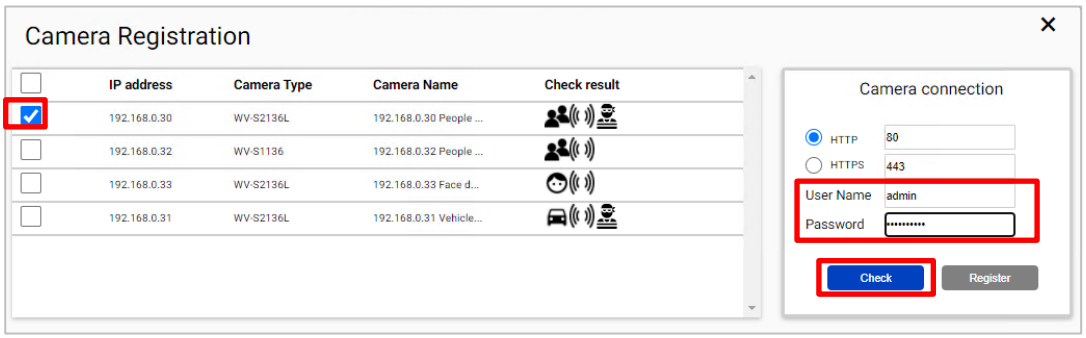
ÉTAPE 2

Cliquez sur [Obtenir de VMS] sur l’écran Enregistrer les caméras.



ÉTAPE 3

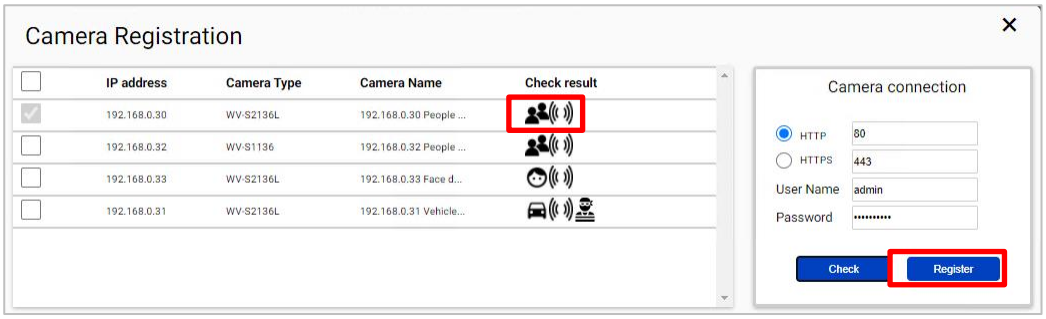
Sélectionnez l’appareil photo et les informations d’identification d’entrée, puis [Cocher].



ÉTAPE4

Vérifiez que les icônes de Vérifier le résultat sont modifiées et [Enregistrer].

Dans cet exemple, AI-VMD est désinstallé (voir 4.3.2.3 à propos de la signification des icônes).



ÉTAPE5

Processus de redémarrage (voir 4.3.3)

5.4. Désinstaller le système

5.4.1. Désinstaller le plug-in du PC client

ÉTAPE 1

Ouvrez la fenêtre Programmes et fonctionnalités (à partir du Panneau de configuration).

ÉTAPE 2

Trouvez [Multi AI Plugins] et [Désinstaller].

5.4.2. Désinstaller le serveur i-PRO Active Guard

ÉTAPE 1

Ouvrez la fenêtre Programmes et fonctionnalités (à partir du Panneau de configuration).

ÉTAPE 2

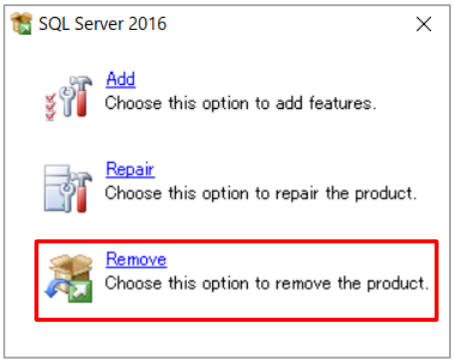
Trouvez [Multi AI Plugins – Server] et [Désinstaller].

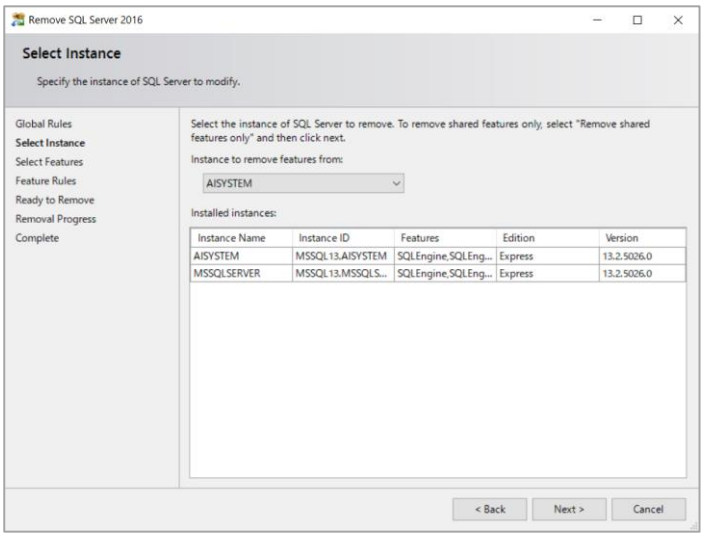
Supprimez le dossier « C:\MultiAI » s'il existe.

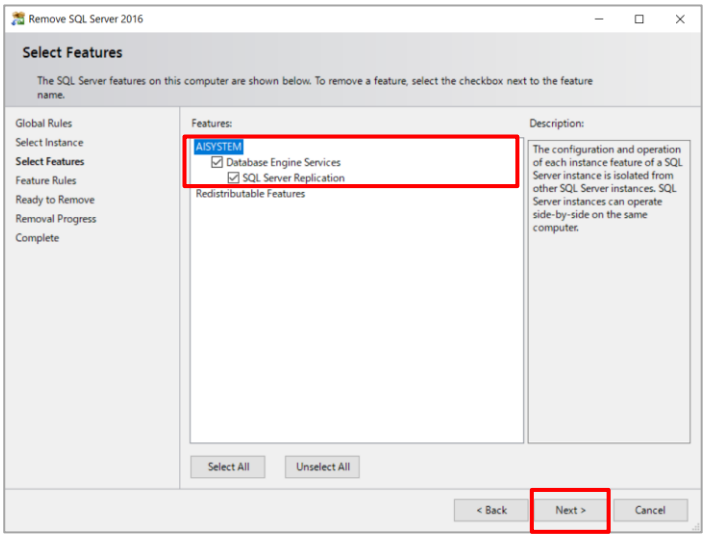
ÉTAPE 3

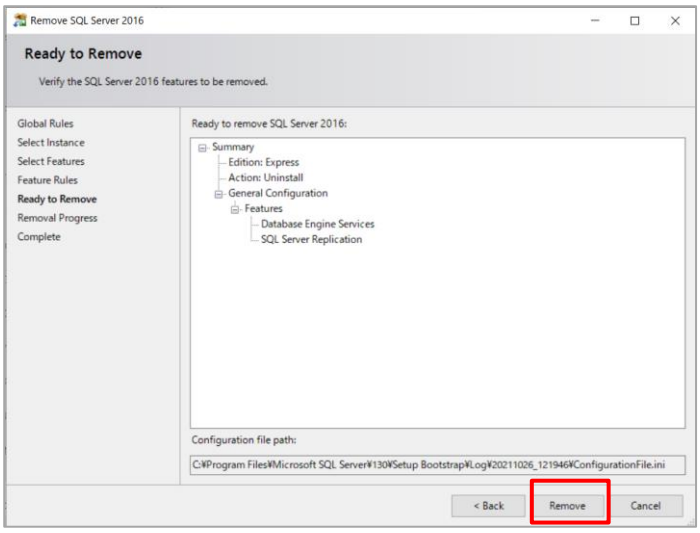
Recherchez [Microsoft SQL Server 2016 (64 bits)] et [Désinstaller].

Sélectionnez [Supprimer] et supprimez l'instance « AISYSTEM ».


SQL Server 2016
Add
Choose this option to add features.
Repair
Choose this option to repair the product.
Remove
Choose this option to remove the product.


Remove SQL Server 2016
Select Instance
Specify the instance of SQL Server to modify.
Global Rules
Select Instance
Select Features
Feature Rules
Ready to Remove
Removal Progress
Complete
Select the instance of SQL Server to remove. To remove shared features only, select "Remove shared features only" and then click next.
Instance to remove features from:
AISYSTEM
Installed instances:
Instance Name
Instance ID
Features
Edition
Version
AISYSTEM
MSSQL13.AISYSTEM
SQLEngine,SQLEng...
Express
13.2.5026.0
MSSQLSERVER
MSSQL13.MSSQLS...
SQLEngine,SQLEng...
Express
13.2.5026.0
< Back
Next >
Cancel


Remove SQL Server 2016
Select Features
The SQL Server features on this computer are shown below. To remove a feature, select the checkbox next to the feature name.
Global Rules
Select Instance
Select Features
Feature Rules
Ready to Remove
Removal Progress
Complete
Features:
AISYSTEM
Database Engine Services
SQL Server Replication
Redistributable Features
Description:
The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on the same computer.
Select All
Unselect All
< Back
Next >
Cancel



Remarque

- L'instance SQL Server utilisée par VMS n'est pas supprimée. Seule l'instance du serveur i-PRO Active Guard est supprimée.
- Le nom d'instance « AISYSTEM » est le nom par défaut. Si vous avez spécifié un nom d'instance comme décrit dans la section 4.3.1, remplacez « AISYSTEM » par le nom d'instance spécifié dans les sections suivantes.

ÉTAPE4

Supprimez « C:\Program Files\Microsoft SQL Server\MSSQL13. AYSYSTEM ».

5.5. Modifier l'adresse IP

5.5.1. Modifier l'adresse IP de la caméra

ÉTAPE 1

Modifier l'adresse IP de la caméra

ÉTAPE 2

Lorsque vous souhaitez conserver les données enregistrées existantes et les meilleures images de l'appareil photo,
mettre à jour l'adresse IP et enregistrer à partir du Security Center ([Outil de configuration] – [Vidéo] – [Paramètre de propriété de l'unité Vidéo]).
Une fois les caméras supprimées de Security Center et réenregistrer la caméra en utilisant une nouvelle adresse IP, les données existantes ne seront pas disponibles.

ÉTAPE 3

Supprimer la caméra du serveur i-PRO Active Guard (voir 5.2.1)

ÉTAPE4

Enregistrez à nouveau la caméra (reportez-vous à 4.3.2.3la section).

ÉTAPE5

Redémarrer le processus (reportez-vous à 4.3.3la section).

5.5.2. Modifier l’adresse IP du Security Center

Les données enregistrées existantes et les meilleures images sont disponibles après le changement d’adresse IP.

ÉTAPE 1

Changement Adresse IP du Security Center.

ÉTAPE 2

Supprimer Security Center du serveur i-PRO Active Guard (voir 5.2.3)

ÉTAPE 3

Enregistrez à nouveau le Security Center (reportez-vous à 4.3.2.2la section).

ÉTAPE4

Redémarrer le processus (reportez-vous à 4.3.3la section).

5.5.3. Modifier l’adresse IP du serveur i-PRO Active Guard

Les données enregistrées existantes et les meilleures images sont disponibles après le changement d’adresse IP.

ÉTAPE 1

Modifiez l’adresse IP du serveur i-PRO Active Guard.

ÉTAPE 2

Mettez à jour la configuration de la connexion au serveur i-PRO Active Guard à partir du plug-in (reportez-vous à 4.4.2la section).

5.6. Sauvegarde et restauration des données

Les données d'image et la base de données associée peuvent être sauvegardées manuellement. Il est important de noter que la réinstallation du serveur i-PRO Active Guard nécessite la même version du logiciel pour la réinstallation à partir de la sauvegarde en raison des différences dans chaque version de base de données.

5.6.1. Processus de sauvegarde

ÉTAPE 1

Démarrer – Outils d'administration Windows – Planificateur de tâches. Faites un clic droit et désactivez « AliveMonitoringProcess »

ÉTAPE 2

Démarrer – Outils d'administration Windows – Services.
Cliquez avec le bouton droit et arrêtez pour « MultiAICameraService »,
« MultiAISupportProcessManagementService » et « SQL Server(AISYSTEM) », respectivement.

ÉTAPE 3

Accédez à Chemin d'enregistrement des données SQL Server (set par install tool at 4.3.1.) .
Copiez « ai_db.mdf », « aicam.mdf », « support_db.mdf », ai_db_log.ldf », « aicam_log.ldf »,
« support_db_log.ldf », « bi.mdf » et « bi_log.ldf » dans un emplacement sûr (c'est-à-dire : une clé USB, un périphérique NAS, un autre serveur, etc.).

ÉTAPE4

Copiez le dossier « C:\MultiAI\Image » dans unemplacement sûr.
Si vous avez modifié le chemin d'enregistrement des données d'image, copiez le dossier.
Copiez le dossier « C:\MultiAI\Backup\WebConfig » dans unemplacement sûr.

ÉTAPE5

Tapez « regedit » dans le menu Démarrer et exécutez. Cliquez avec le bouton droit sur deux dossiers et exportez vers un emplacement sûr, respectivement.
« \HKEY_LOCAL_MACHINE\SOFTWARE\Panasonic\AiSystem » ou
« \HKEY_LOCAL_MACHINE\SOFTWARE\i-PRO\AiSystem ».

« \HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Panasonic\AiSystem » ou
« \HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ i-PRO \AiSystem ».

ÉTAPE6

Démarrer – Outils d'administration Windows – Services.
Cliquez avec le bouton droit et exécutez pour « MultiAICameraService »,
« MultiAISupportProcessManagementService » et « SQL Server (AISYSTEM) », respectivement.

ÉTAPE7

Démarrer – Outils d'administration Windows – Planificateur de tâches. Faites un clic droit et activez « AliveMonitoringProcess »

5.6.2. Processus de restauration

ÉTAPE 1

Démarrer – Outils d'administration Windows – Planificateur de tâches. Faites un clic droit et désactivez « AliveMonitoringProcess »

ÉTAPE 2

Démarrer – Outils d'administration Windows – Services.
Cliquez avec le bouton droit et arrêtez pour « MultiAICameraService »,
« MultiAISupportProcessManagementService » et « SQL Server(AISYSTEM) », respectivement.

ÉTAPE 3

Copiez les fichiers enregistrés « ai_db.mdf », « aicam.mdf », « support_db.mdf », ai_db_log.ldf »,
« aicam_log.ldf », « support_db_log.ldf », « bi.mdf » et « bi_log.ldf » dans « C:\Program Files\Microsoft SQL Server\MSSQL13. AISYSTEM\MSSQL\DATA » et remplacer les fichiers existants.

ÉTAPE4

Copiez le dossier enregistré « Image » dans « C:\MultiAI » et remplacez les fichiers existants.
Copiez le dossier enregistré « WebConfig » dans « C:\MultiAI\Backup » et remplacez les fichiers existants.

ÉTAPE5

Double-cliquez sur le fichier d'exportation du Registre enregistré. Cela réinstallera les clés de Registre.

ÉTAPE6

Démarrer – Outils d'administration Windows – Services.
Faites un clic droit et exécutez pour « SQL Server (AISYSTEM) ».

ÉTAPE7

Exécutez « C:\MultiAI\tools\restore_user\restore_user.bat » en tant qu'administrateur

Remarque
Si vous définissez le nom de l'instance SQL Server sur autre chose que « AISYSTEM », remplacez le nom d'instance dans le fichier bat par « AISYSTEM » par le nom d'instance que vous avez défini et exécutez le fichier.

ÉTAPE 8
Faites un clic droit et exécutez pour « MultiAICameraService »,
« MultiAISupportProcessManagementService », respectivement.

ÉTAPE 9
Démarrer – Outils d'administration Windows – Planificateur de tâches. Faites un clic droit et activez « AliveMonitoringProcess ».

5.7. Procédure pour déplacer l'emplacement du serveur i-PRO Active Guard du PC de Security Center vers le PC du serveur dédié

L'emplacement du serveur i-PRO Active Guard peut être déplacé du PC de Security Center vers le PC du serveur dédié, par exemple,lorsque le nombre de caméras est augmenté ou lorsque la répartition de la charge de traitement est nécessaire.

5.7.1. Préparation des données et des informations de compte

ÉTAPE 1
Préparez les informations de compte administrateur du serveur i-PRO Active Guard existant lors de l'installation.
Si vous oubliez le compte administrateur, réinitialisez-le (reportez-vous à 5.9la section).

ÉTAPE 2
Données de sauvegarde (reportez-vous à 5.6.1)

5.7.2. Installez le serveur i-PRO Active Guard sur un nouveau PC et restaurez les données

ÉTAPE 1

Installez le serveur i-PRO Active Guard sur un nouveau PC en tant que PC serveur dédié (reportez-vous à 4.3.1la section).

Remarque Les informations de compte que vous avez définies lors de l'installation seront écrasées dans le processus de restauration (reportez-vous à l'étape 2).

ÉTAPE 2

Restaurer les données (reportez-vous à 5.6.2)

ÉTAPE 3

Exécutez « C:\MultiAI\tools\init_dedicated_server.bat » en tant qu'administrateur

ÉTAPE4

Démarrer – Outils d'administration Windows – Services.
Faites un clic droit et redémarrez pour « MultiAICameraService »,
« MultiAISupportProcessManagementService ».

5.8. Procédure pour redémarrer/arrêter le PC serveur i-PRO Active Guard

Par mesure de sécurité, il est recommandé d'arrêter les services avant de redémarrer l'ordinateur.

ÉTAPE 1

Arrêtez le processus du serveur i-PRO Active Guard (reportez-vous à 4.3.8.2la section).

ÉTAPE 2

Redémarrez ou arrêtez.

5.9. Réinitialiser le compte administrateur

Lorsque vous oubliez les informations d'identification de l'administrateur pour accéder à la configuration, vous devez réinitialiser sur le PC que le serveur i-PRO Active Guard est installé.

Exécutez « C:\MultiAI\tools\ChangeAdminPassword\ChangeAdminPassword.exe » en tant qu’administrateur et définissez les informations d’identification.

5.10. Mettre à niveau SQL Server vers Standard Edition

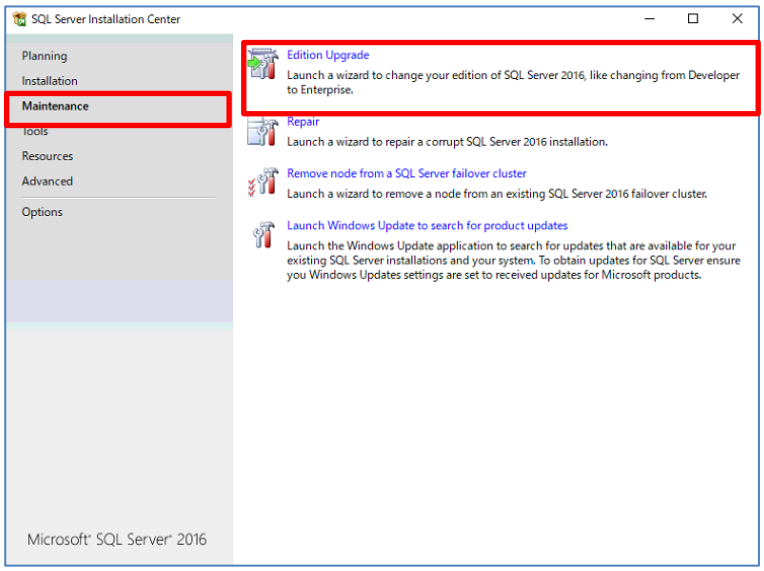
Vous pouvez déterminer si vous avez besoin de Standard Edition à partir de 3.3.
Si vous en avez besoin, veuillez suivre les étapes ci-dessous pour effectuer la mise à niveau après l’achat de la licence.
Le logiciel serveur i-PRO Active Guard doit être installé à l’avance.

ÉTAPE 1

Démarrez [installation.exe] à partir du support d’installation de SQL Server Standard Edition.

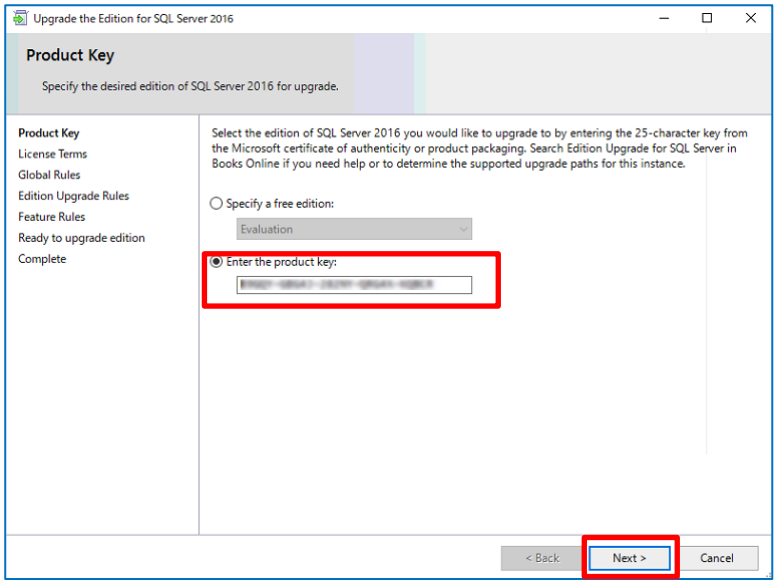
ÉTAPE 2

Sélectionnez [Mise à niveau de l’édition] dans Maintenance.



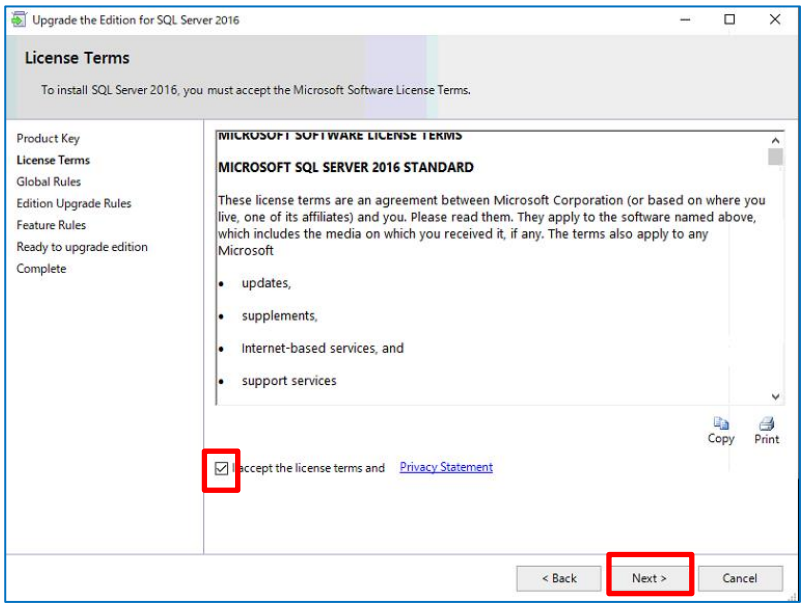
ÉTAPE 3

Vérifiez que la clé de produit est affichée et cliquez sur [Suivant].



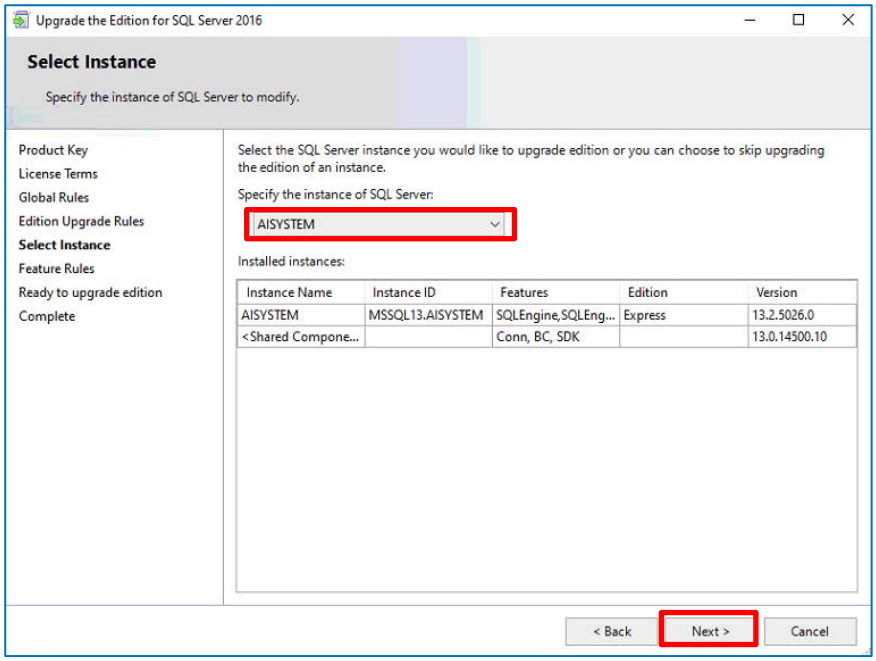
ÉTAPE4

Vérifiez la durée de la licence et cliquez sur [Suivant].



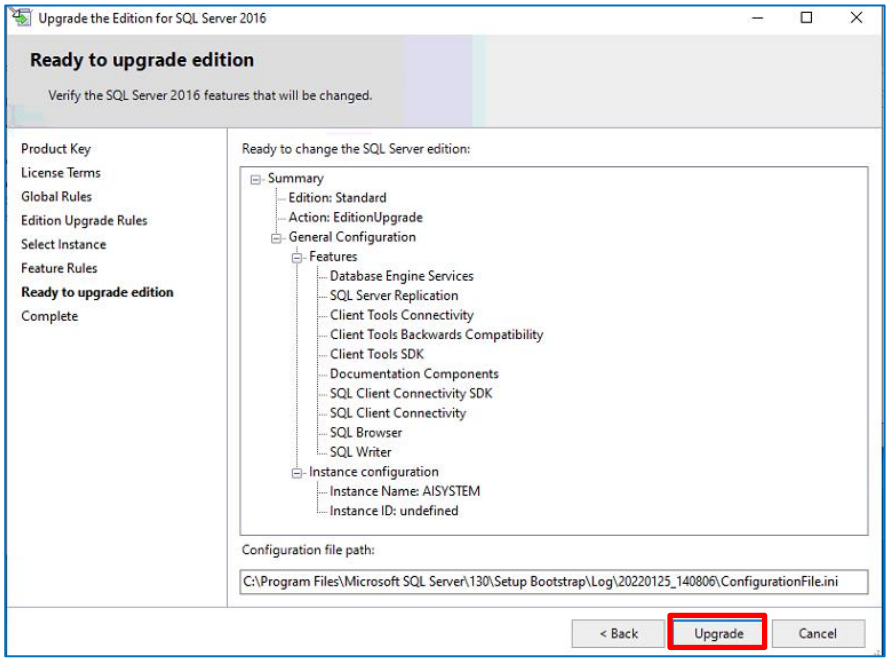
ÉTAPE5

Sélectionnez [AISYSTEM] par exemple et cliquez sur [Suivant].



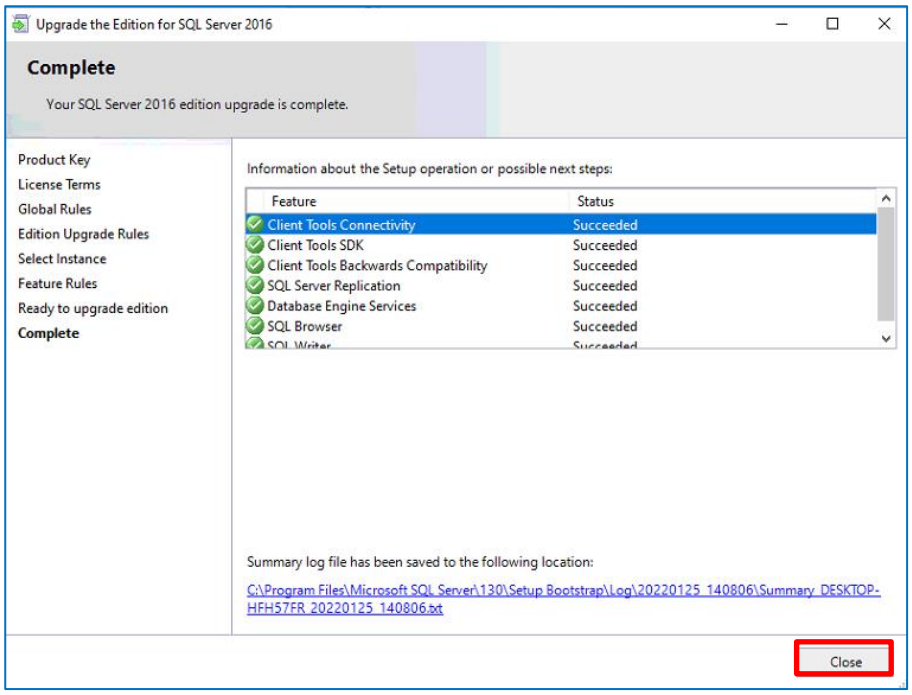
ÉTAPE6

Cliquez sur [Mettre à niveau]



ÉTAPE7

Cliquez sur [Fermer]



6. Résolution des problèmes

6.1. Dépannage pour l'installation et la configuration

Problème	Cause et solution	Parrainer
Echec de l'installation de SQL Server	Certaines données ont peut-être été utilisées dans le passé. Désinstallez le programme lié à SQL Server 2016 si VMS utilise une autre version de SQL Server, supprimez le dossier C:\Program Files\Microsoft SQL Server\MSSQL13. AISYSTEM et supprimez le dossier C:\MultiAI si vous l'avez déjà installé.	5.4.2
	Vérifiez si la longueur du chemin d'accès au fichier du package d'installation est inférieure à 120 et lancez le programme d'installation en tant qu'administrateur.	4.3.1
	Lorsque vous utilisez Window 10 , version 20H2 et le navigateur Microsoft Edge de n'importe quelle version de 84.0.522.52 à 86.0.622.55, exécutez « Windows update ». Réf.https://docs.microsoft.com/en-us/troubleshoot/sql/install/error-set-up-update-instances	-
Impossible d'installer le logiciel serveur VMS après l'installation du serveur i-PRO Active Guard	Lorsque vous installez le serveur i-PRO Active Guard sur un PC avec un serveur VMS, vous devez installer le logiciel du serveur VMS à l'avance. Si le serveur i-PRO Active Guard est installé avant cela, désinstallez le serveur i-PRO Active Guard et le serveur SQL, puis installez le serveur VMS.	4.3.1 **Erreur ! Source du renvoi introuvable.**
Impossible d'accéder à la configuration i-PRO Active Guard.	Avez-vous accédé à http://<ip>:8092 ? « https://<ip>:8092 » est correct. Lorsque vous définissez un autre numéro de port, qu'un autre logiciel utilise 8092 ou que vous avez modifié après l'installation, entrez le numéro de port.	4.3.2.1

	Le navigateur pris en charge est Microsoft Edge 85 (ou version ultérieure), Chrome 83 (ou version ultérieure) et Firefox 95 (ou version ultérieure).	3.2
	Veuillez confirmer que le service associé est en cours d'exécution sur le PC que le serveur i-PRO Active Guard est installé. Démarrer – Outils d'administration Windows – Services. « MultiAICameraService », « MultiAISupportProcessManagementService » et « SQL Server(AISYSTEM) » Si vous êtes arrêté, cliquez avec le bouton droit de la souris et exécutez	5.6.1
Impossible de se connecter à la configuration i-PRO Active Guard	Si vous oubliez le compte administrateur, réinitialisez le compte du PC sur lequel le serveur i-PRO Active Guard est installé.	5.9
Impossible d'enregistrer VMS.	Vérifiez si l'adresse IP, le port, le protocole et les informations d'identification sont corrects.	4.3.2.2
	Vérifiez si web-SDK est activé à partir de Config tool sur Security Center et	4.2.3
	La version prise en charge de Security Center est SC 5.10.1.0 ou version ultérieure	2.2
Impossible d'enregistrer les caméras	Vérifiez si l'adresse IP, le port, le protocole et les informations d'identification sont corrects.	-
	Vérifiez si le logiciel d'extension est installé à l'avance sur l'appareil photo.	4.1
	Vérifiez si les caméras sont enregistrées à l'avance dans Security Center.	4.2.1
	Vérifiez si « Digest » est utilisé pour l'authentification côté caméra. ([Paramètres] - [Utilisateur mng.] - [Authentification de l'utilisateur.])	-
Visage Les images de personnes ou de véhicules ne peuvent pas être recherchées à partir du plug-in (la caméra n'est pas	L'enregistrement de la caméra sur le serveur i-PRO Active Guard doit être effectué après l'enregistrement de la caméra dans Security Center. Lorsque vous redonnez la caméra au Security Center après l'enregistrement sur le serveur i-PRO Active Guard, vous devez également réenregistrer la caméra sur le	5.2.1 **Erreur ! Source du renvoi introuvable.**

affichée pour la liste des caméras).	serveur i-PRO Active Guard (supprimer, puis enregistrer à nouveau).	
Visage Les images de personnes ou de véhicules ne peuvent pas être recherchées à partir du plug-in (le nombre de résultats de recherche est 0).	L'état de réception de chaque caméra peut être confirmé à partir de la configuration i-PRO Active Guard. Vérifiez la connexion réseau entre la caméra et le serveur i-PRO Active Guard, l'heure de la dernière réception, l'heure du dernier diagnostic. Si le résultat n'est pas attendu, vérifiez si le réglage de la planification côté caméra pour le logiciel d'extension est activé.	4.3.8.1
	Vérifiez l'état du processus du serveur i-PRO Active Guard. Si un processus est arrêté, redémarrez-le.	4.3.8.2
	Vérifiez si le réglage de la planification côté caméra pour le logiciel d'extension est activé.	-
	Problèmes de configuration dans un environnement réseau multiple Vérifiez si la caméra est connectée à un réseau qui n'est pas local au serveur.	-
	Problèmes de configuration du pare-feu. Vérifiez si le programme du serveur i-PRO Active Guard est répertorié dans « Applications et fonctionnalités autorisées » pour les paramètres du pare-feu.	-
Impossible de se connecter à partir de Plug-in au serveur i-PRO Active Guard.	Vérifiez si l'adresse IP, le port, le protocole et les informations d'identification sont corrects. Le port et les informations d'identification peuvent être modifiés à partir de la configuration i-PRO Active Guard.	4.3.5.2 4.4.2
Le temps de lecture est incorrect.	Vérifiez si l'heure PC du serveur i-PRO Active Guard et du serveur VMS est synchronisée lorsque le serveur i-PRO Active Guard est installé sur un serveur dédié.	-
La détection de visage enregistrée ou les personnes enregistrées détectention ne peut pas être affichée	Vérifiez si des événements et des actions personnalisés (par exemple, déclencher une alarme) sont configurés.	4.7
	Vérifiez si le serveur i-PRO Active Guard détecte l'alarme à partir du diagnostic sur la configuration i-PRO Active Guard. Si une alarme existe, vérifiez l'état du processus du serveur i-PRO Active Guard.	4.3.8.3
L'alarme système ne peut pas être affichée	Vérifiez si des événements et des actions personnalisés (par exemple, déclencher une alarme) sont configurés.	4.7

6.2. Dépannage après mise en production

Lorsque le problème se produit après le démarrage du système, vous pouvez confirmer le code d'erreur sur la configuration i-PRO Active Guard (voir 4.3.8.4)

Problème	Code d'erreur	Cause et solution
Le processus serveur est arrêté lors de la configuration i-PRO Active Guard	514 à 517	Les services liés au serveur i-PRO Active Guard n'existent pas. Veuillez réinstaller le serveur i-PRO Active Guard
	1025 – 1028 4097 – 4100 4354,4357, 4610,4611	Le processus lié au serveur i-PRO Active Guard n'a pas pu démarrer. Redémarrez manuellement le serveur i-PRO Active Guard (reportez-vous à 4.3.8.2la section). Lorsque le processus s'arrête à nouveau, téléchargez les journaux (reportez-vous à 4.3.8.5) et contactez l'administrateur système.
Déconnexion de la caméra	4355,4356,4358	Vérifiez la connexion réseau entre la caméra et le serveur i-PRO Active Guard. Vérifier le fonctionnement de la caméra (enregistrement sur VMS et surveillance en direct) Si le problème persiste après le redémarrage manuel de la caméra et du serveur i-PRO Active Guard (reportez-vous à), téléchargez les journaux (reportez-vous à 4.3.8.24.3.8.5) et contactez l'administrateur système.
Visage Les images de personnes ou de véhicules ne peuvent pas être recherchées à partir du plug-in (le nombre de résultats de recherche est 0).	66052,66053	L'état de réception de chaque caméra peut être confirmé à partir de la configuration i-PRO Active Guard. Vérifiez la connexion réseau entre la caméra et le serveur i-PRO Active Guard, l'heure de la dernière réception, l'heure du dernier diagnostic. Si le résultat n'est pas attendu, vérifiez si le réglage de la planification côté caméra pour le logiciel d'extension est activé.
Fausse détection (Le visage, les personnes ou le	-	Pour éviter toute fausse détection, configurez la zone de masque à l'aide d'iCT (reportez-vous à 4.1la section).

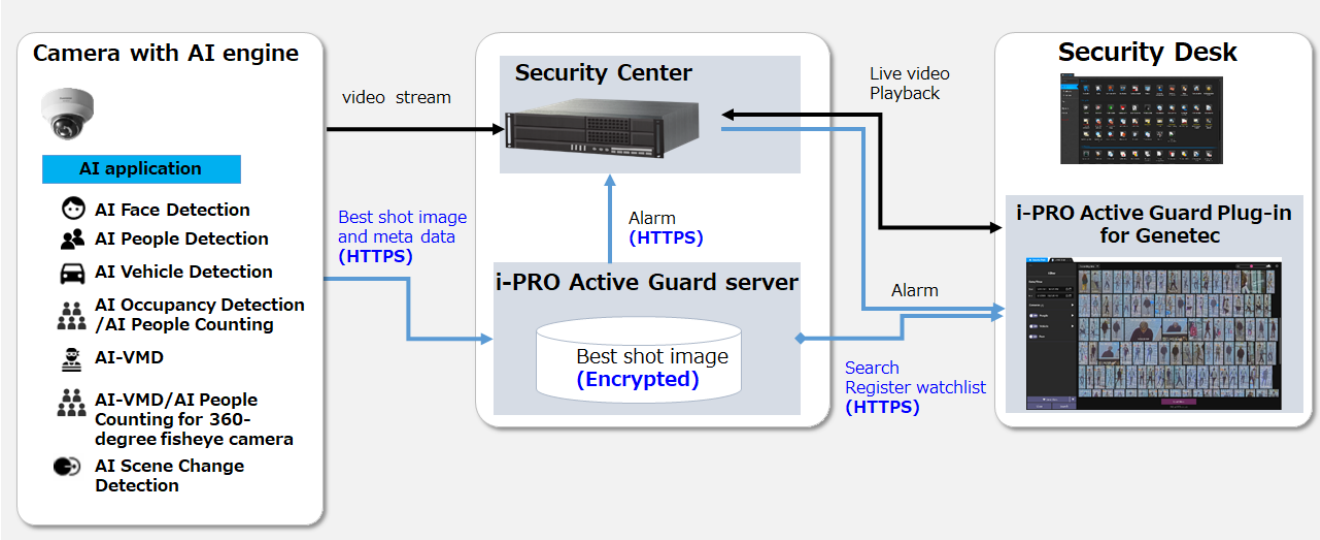
véhicule ne sont pas fouillés)		
Utilisation élevée du processeur, utilisation de la mémoire ou accès disque	65793,65794 65796,65797	Vérifiez l'état du processeur ou de la mémoire (reportez-vous à 4.3.8.2) et confirmez si l'utilisation par le logiciel serveur i-PRO Active Guard est élevée. Si l'utilisation du serveur i-PRO Active Guard est élevée, pour réduire la charge, configurez la zone de masque côté caméra à l'aide de iCT (reportez-vous à) ou « Fréquence maximale de réception des données d'objet (par seconde) » (Reportez-vous à 4.3.5.44.1) Si l'utilisation du serveur i-PRO Active Guard est faible et celle du PC entier est élevée, vérifiez l'influence d'autres logiciels. Lorsque le serveur i-PRO Active Guard est installé avec le logiciel VMS, vérifiez l'état du logiciel VMS.
Atteindre l'espace disque maximum de l'image (supprimer les anciennes images)	65795	Les anciennes images ont été supprimées en dépassant les paramètres de « Utilisation maximale du lecteur de stockage d'images ». Si vous devez stocker des données pour la « Période de rétention », configurez la zone de masque côté caméra à l'aide de iCT (reportez-vous à 4.1) pour réduire le nombre de détections.

7. Annexes

7.1. Guide sur les systèmes sécurisés

Pour garantir des communications cryptées dans des environnements critiques, le système sécurisé a été créé en tant que couche de sécurité supplémentaire pour l'application. Ce document décrit comment activer et configurer un système sécurisé.

La communication entre les caméras et le serveur i-PRO Active Guard peut être cryptée via le protocole HTTPS.
La communication entre Security Center et le serveur i-PRO Active Guard peut être chiffrée via le protocole HTTPS.
La communication entre le serveur i-PRO Active Guard et le plug-in peut être cryptée via le protocole HTTPS.
Les meilleures images enregistrées sur le serveur i-PRO Active Guard peuvent être cryptées. Le cryptage des données ne peut être configuré que lorsque vous installez le serveur i-PRO Active Guard.



7.1.1. HTTPS entre la caméra et le serveur i-PRO Active Guard

ÉTAPE 1

Ouvrez le navigateur Web de l'appareil photo (*voir les instructions pour chaque marque et modèle*). [Configuration] – [Réseau] – [Avancé] – [HTTPS], sélectionnez [HTTPS] dans la zone de liste Connexions.

ÉTAPE 2

Lorsque vous enregistrez une caméra sur le serveur i-PRO Active Guard, sélectionnez HTTPS (reportez-vous à 4.3.2.3).

7.1.2. HTTPS entre le serveur i-PRO Active Guard et le plug-in

ÉTAPE 1

Configurez HTTPS pour [Connexion au plug-in client] sur la configuration i-PRO Active Guard (reportez-vous à 4.3.5.2) et le processus de redémarrage.

ÉTAPE 2

Configurer la connexion HTTPS sur le paramètre du plug-in (voir 4.4.2)

7.1.3. HTTPS entre VMS et le serveur i-PRO Active Guard

ÉTAPE 1

Sélectionnez « utiliser la connexion SSL » dans l'outil de configuration (voir 4.2.3)

ÉTAPE 2

Lorsque vous enregistrez VMS sur le serveur i-PRO Active Guard, sélectionnez HTTPS (reportez-vous à 4.3.2.2).

7.1.4. Cryptage des meilleures images

Le chiffrement activé/désactivé ne peut être configuré que lors de l'installation du serveur i-PRO Active Guard (reportez-vous à 4.3.1la section).
Lorsque les données sont cryptées, l'image peut être vue à partir du logiciel plug-in. Un autre logiciel ne peut pas ouvrir le fichier.

7.2. Open source software

Ce produit utilise un logiciel open source.
Pour plus de détails concernant les licences, lisez licence.txt inclus dans le package d'installation..

7.3. Comment utiliser le logiciel d'extension 3rd party

Le logiciel d'extension de caméra 3rd party développé pour la caméra i-PRO peut être utilisé dans le système i-PRO Active Guard. Tousles logiciels d'extension 3rd ne peuvent pas être utilisés, un logiciel qui implémente une intégration spécifique peut être utilisé. Vous pouvez vérifier le logiciel d'extension qui peut être connecté à i-PRO Active Guard à partir de la liste des applications lors de sa sortie.

Ce document n'inclut pas l'installation ou la configuration du logiciel d'extension 3rd party lui-même et inclut d'autres procédures après eux.

7.3.1. Version logicielle requise

Serveur i-PRO Active Guard : v1.6.1 ou version ultérieure.

7.3.2. Configuration du serveur i-PRO Active Guard

Cette section décrit les étapes requises pour enregistrer la caméra avec le logiciel d'extension tiers 3rd sur le serveur i-PRO Active Guard et recevoir les données d'événement.

ÉTAPE 1
Modifiez le fichier de configuration pour enregistrer le logiciel d'extension.
Ostylo le fichier « C:\MultiAI\Backup\3rdpartyApp.config » dans le PC sur lequel le logiciel serveur i-PRO Active Guard est installé.

Entrez le nom du logiciel d'extension, le nom de l'événement et l'ID d'événement personnalisé, puis activez également la ligne en supprimant « ; » au début de la ligne.
Ex.
application_name_1 = « SampleApplication »
event_name_1 = « SampleDetection »
genetec_custom_event_id_1 = 12000

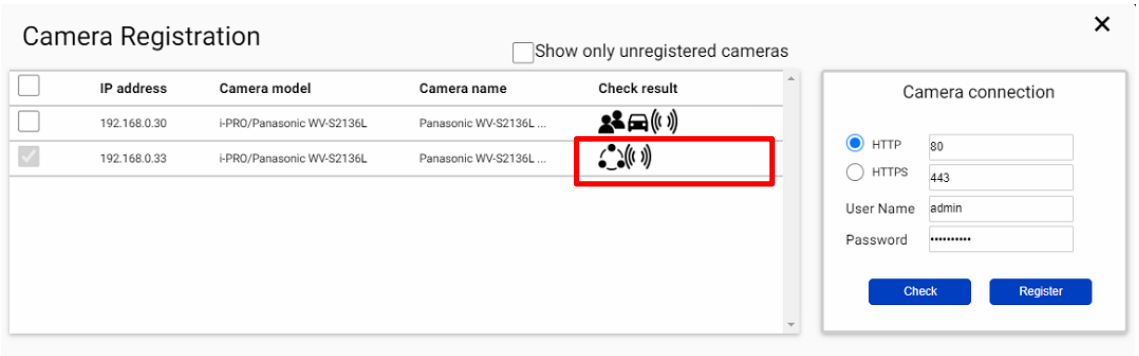
Save et fermez le fichier après modification.

Remarque
Jusqu'à 10 logiciels d'extension et 10 événements peuvent être enregistrés dans un système.

Le nom du logiciel d'extension et le nom de l'événement du logiciel d'extension seront affichés dans la liste des applications lors de la publication. Cela ne fonctionnera pas si un autre nom est configuré.

ÉTAPE 2

Register caméra au serveur i-PRO Active Guard (voir 4.3.2.3).

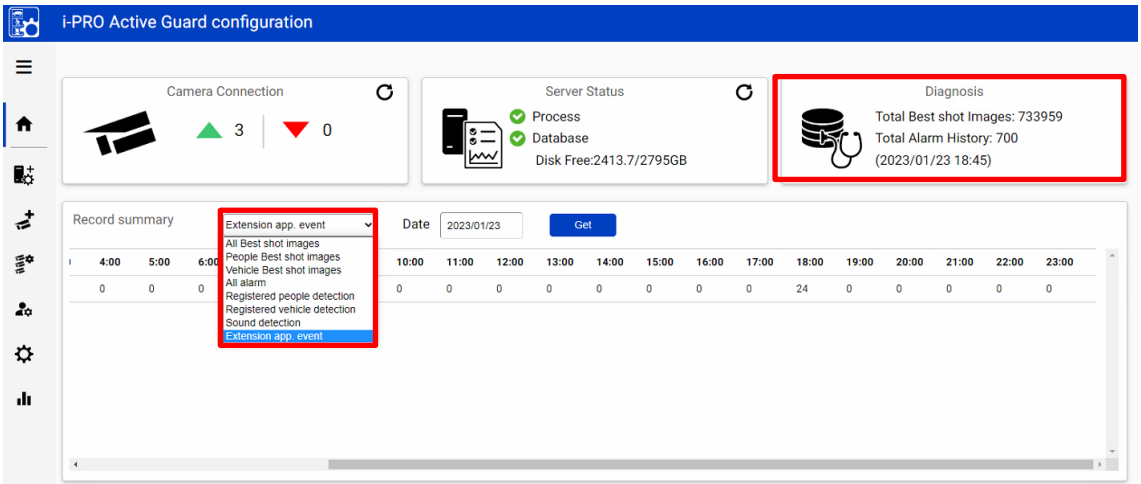


Lorsque le logiciel d'extension 3rd party est installé dans la caméra sélectionnée, l'icône sera affichée dans le [Vérifier le résultat]. Si l'icône n'est pas affichée, veuillez vérifier si le fichier de configuration est correctement édité.

ÉTAPE 3

Vérifiez si un événement s'est produit (facultatif).

[Extension app. event] peut être sélectionné pour confirmer le nombre de détection. (Reportez-vous à **Erreur ! Source du renvoi introuvable.**)

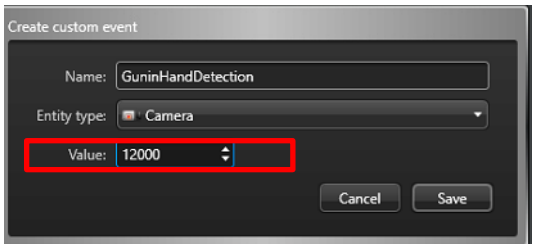


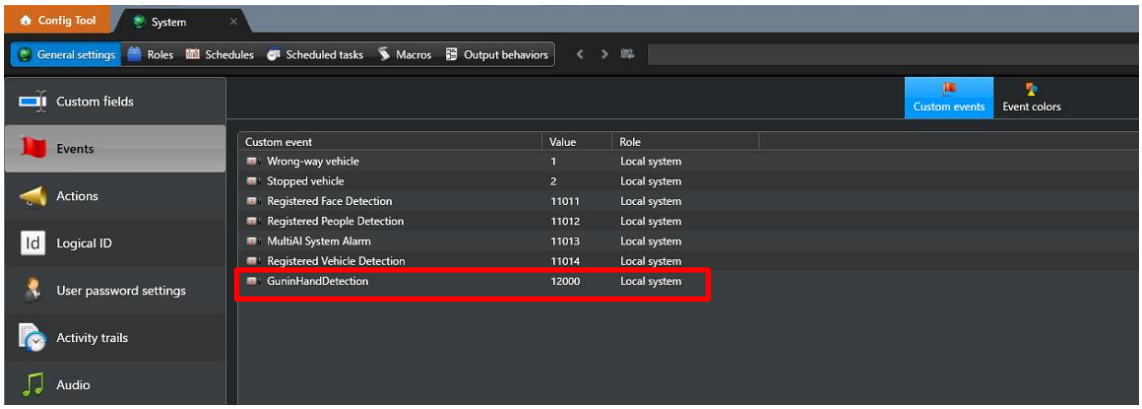
* Il faut environ 15 minutes pour qu'un événement apparaisse à l'écran après qu'il se soit produit.

7.3.3. Configurer l’événement personnalisé (obligatoire)

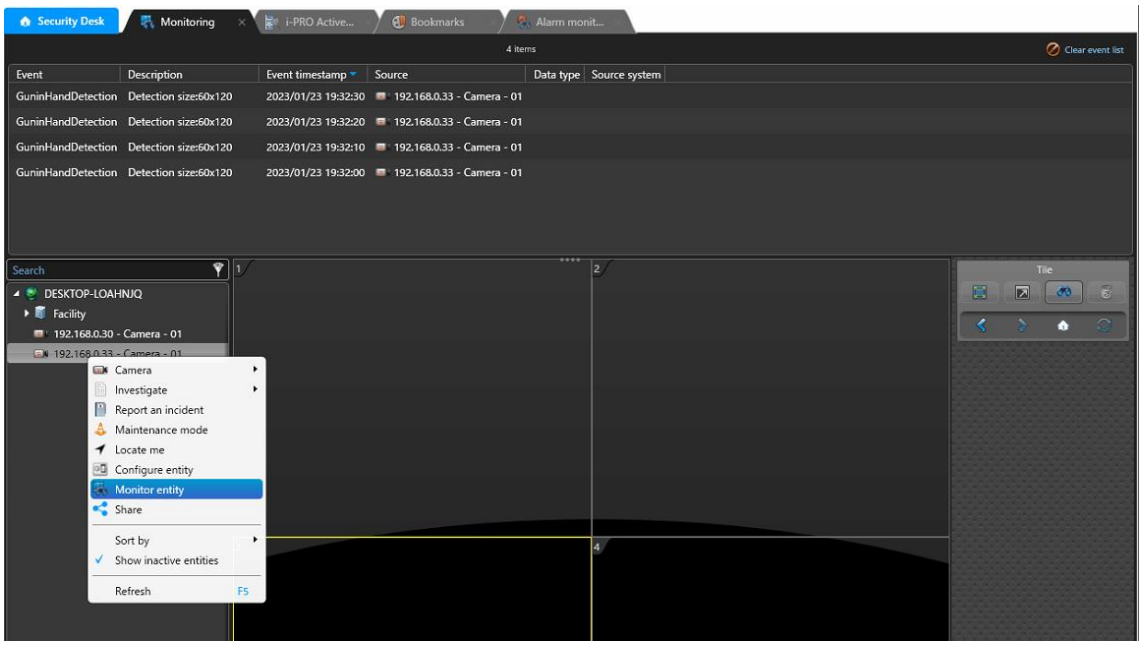
Semblable à la procédure décrite dans 4.7, l’événement logiciel d’extension 3rd party peut être utilisé comme événement personnalisé.

Ajoutez un événement logiciel d’extension avec la valeur. La valeur doit correspondre à la valeur configurée dans « C:\MultiAI\Backup\3rdpartyApp.config » côté serveur i-PRO Active Guard.

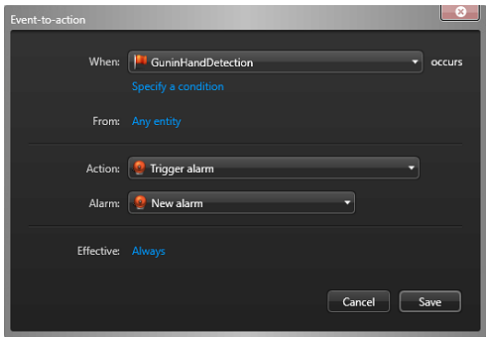


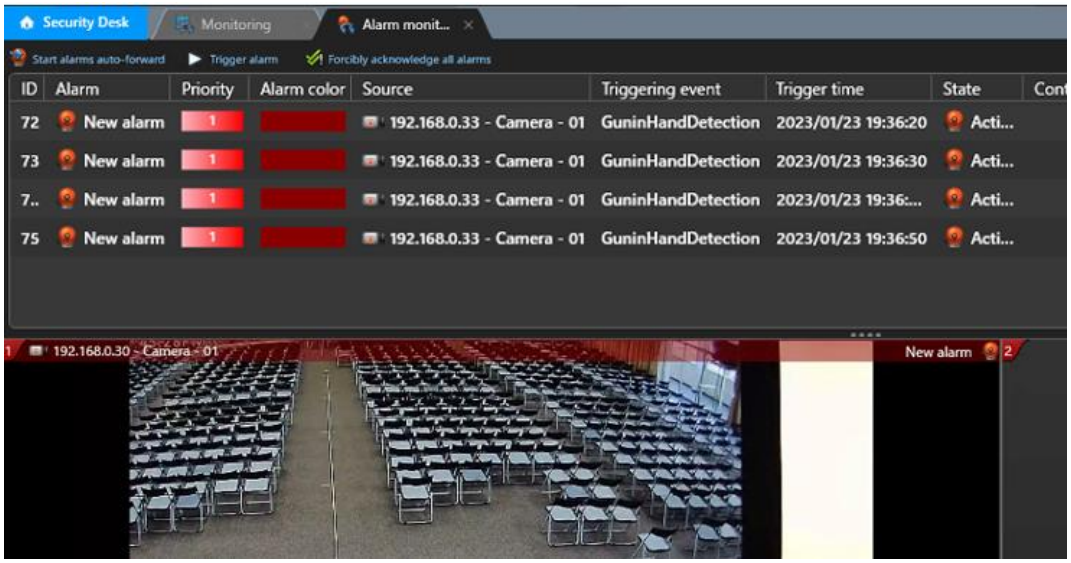


En activant [Surveillance] – [Entité Moniteur], l’événement logiciel d’extension sera affiché.



Configurer les actions (facultatif).





7.4. Spécifications

Les détails des spécifications sont les suivants.

Design	Caméra prise en charge	Caméra réseau i-PRO avec moteur d'IA
	Nombre de caméras	1 à 100 CH lorsqu'il est installé avec un serveur VMS (AI Face Detection est jusqu'à 20) 1 à 300CH lorsqu'il est installé sur un serveur dédié (AI Face Detection est jusqu'à 60)
	Nombre de clients	Aucune limitation (en fonction de la limitation du PMV)
	Nombre d'enregistrements serveur	- (seul le serveur principal doit être enregistré)
	Nombre de i-PRO Active Guard serveur par client	Aucune limitation (en fonction de la capacité de l'ensemble du système)

Applications IA supportées	Pour plugin	Détection de visage AI / Détection de personnes AI / Détection de véhicule IA
	Pour le tableau de bord	Détection de visage AI, détection de personnes AI, détection de véhicule AI, AI-VMD / AI People Counting pour caméra fisheye à 360 degrés, AI-VMD, AI Détection d'occupation
Stockage	Période de conservation	Limite max. 31 jours pour les données faciales, de personnes ou de véhicules / Max. 92 jours pour les données de comptage de personnes * Max. 366 jours en mettant à niveau SQL Server Standard Edition ou supérieure
Recherche de poste	Filtre	Personnes, Véhicule (attribut, date et heure, caméra, direction du déplacement) Visage (visage, date et heure et appareil photo similaires)
	Recherche similaire	Oui (par les mêmes informations d'attribut) * Personnes et véhicule (par les mêmes informations d'attribut) et visage
	Sort	Descendant, ascendant, pertinence (visage, personnes et véhicule)
Alarme	Alarme de liste de surveillance	Jusqu'à 1 000 visages, Jusqu'à 12 attributs de personnes, Jusqu'à 12 attributs de véhicule
	Alarme de détection	AI-VMD, AI Sound Classification sont pris en charge dans Genetec Security Center et Security Desk (pas de plugin)
	Fonction associée	
Lecture/ Exportation	Lecture	Lire des vidéos à l'époque des meilleurs Prise de vue en mode complet et multi-vues
	Exporter une vidéo	Enregistrer la meilleure image prise de vue, Exporter la vidéo à partir du serveur d'enregistrement
	Exporter le résultat de la recherche	HTML
Tableau de bord	Navigateur pris en charge	Microsoft Edge, Google Chrome et Firefox
	Graphique	Comptage des personnes, statistiques d'occupation et carte thermique lors de l'utilisation de AI-VMD / AI People Counting pour caméra fisheye à 360 degrés. Comptage de personnes et comptage de véhicules lors de l'utilisation de l'AI-VMD. Comptage de personnes et statistiques d'occupation lors de

		l’utilisation de la détection d’occupation par IA. L’intervalle de mise à jour des données est d’au moins 15 secondes pour le comptage des personnes/véhicules et de 1 min pour la carte thermique. Statistiques sur l’âge et le sexe lors de l’utilisation de la détection faciale par IA. L’intervalle de mise à jour des données est de 1 min minimum. Les personnes attribuent des statistiques lors de l’utilisation de la détection de personnes par IA. L’intervalle de mise à jour des données est de 1 min minimum. Statistiques des attributs de véhicule lors de l’utilisation de la détection de véhicule IA. L’intervalle de mise à jour des données est de 1 min minimum.
	Personnaliser	Contenu, taille d’affichage, emplacement de chaque graphique. 3 Les mises en page par utilisateur peuvent être enregistrées et 24 utilisateurs peuvent être enregistrés. (Jusqu’à 4 utilisateurs peuvent être connectés en même temps) Thème de couleur d’affichage de base (sombre ou clair) Type de graphique linéaire (ligne droite / ligne lissée), nom de ligne/zone pour le comptage