AXIS Perimeter Defender

AXIS Perimeter Defender
AXIS Perimeter Defender PTZ Autotracking

Manuel d'utilisation

Table des matières

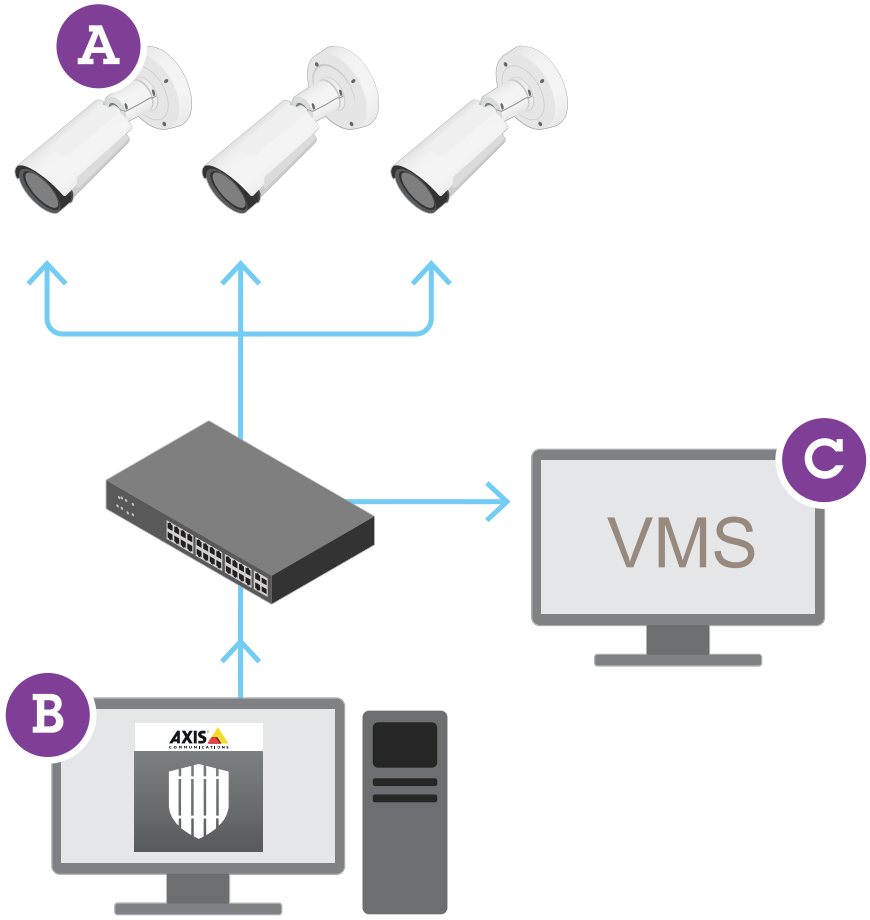
AXIS Perimeter Defender

AXIS Perimeter Defender est une application de surveillance et de protection de périmètre. Cette application est idéale pour la protection d'un périmètre de haute sécurité dans lequel il est nécessaire de renforcer le système de contrôle d'accès physique avec une détection fiable des intrusions.

AXIS Perimeter Defender est principalement conçu pour la protection des zones dites stériles, par exemple, le long d'une clôture marquant une frontière. Le terme « zone stérile » se réfère à une zone dans laquelle personne n'est censé pénétrer.

Utilisez AXIS Perimeter Defender en extérieur pour :

- Détecter des personnes en mouvement.
- Détecter des véhicules en mouvement, sans faire de distinction entre les types de véhicules.



Cette caméra peut fonctionner en mode calibrage, en mode IA, ou en combinant les deux modes. Si vous choisissez de l'exécuter en mode IA uniquement, le montage de la caméra est plus flexible et vous n'avez pas besoin de calibrer les caméras.

AXIS Perimeter Defender se compose d'une interface de bureau (B), à partir de laquelle vous installez et configurez l'application sur les caméras (A). Vous pouvez ensuite configurer le système pour envoyer des alarmes au logiciel de gestion vidéo (C).

AXIS Perimeter Defender PTZ Autotracking est un plug-in de l'application AXIS Perimeter Defender qui utilise la même interface de bureau. Avec le plug-in, vous associez une caméra visuelle ou thermique fixe à une caméra PTZ Axis Q-line. Vous pouvez ensuite maintenir une couverture de détection continue sur une scène avec la

caméra fixe, tandis que la caméra PTZ effectue un suivi automatique et propose des vues plus rapprochées des objets détectés.

Important

AXIS Perimeter Defender PTZ Autotracking nécessite un calibrage des caméras fixes et PTZ.

AXIS Perimeter Defender propose les types de scénarios de détection suivants :

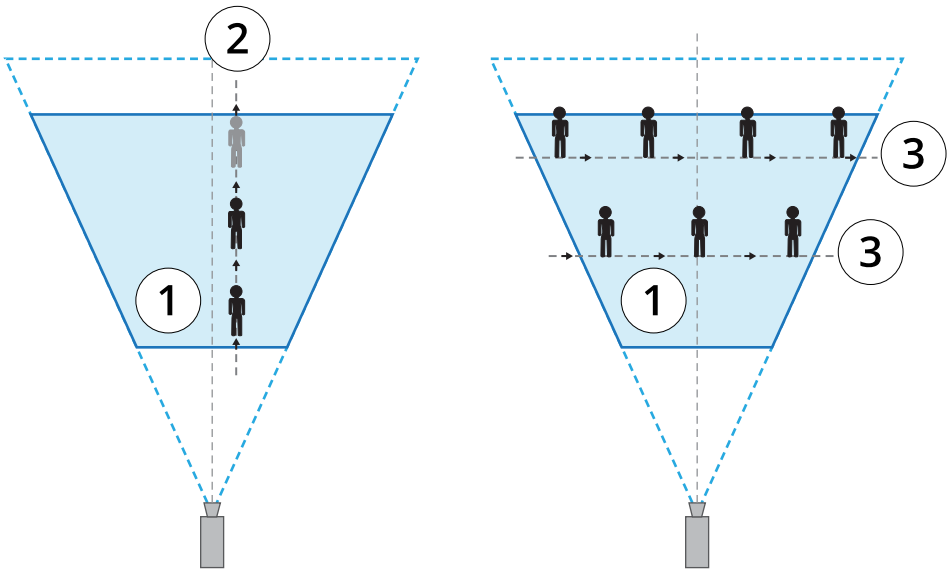
- **Intrusion** : déclenche une alarme lorsqu'une personne ou un véhicule entre dans une zone définie au sol (depuis n'importe quelle direction et selon n'importe quelle trajectoire).
- **Loitering (Maraudage)** : déclenche une alarme lorsqu'une personne ou un véhicule reste dans une zone définie au sol pendant une durée prédéfinie en secondes.
- **Zone-crossing (Franchissement de zone)** : déclenche une alarme lorsqu'une personne ou un véhicule traverse deux zones définies au sol ou plus dans un ordre donné.
- **Conditional (Conditionnel)** : déclenche une alarme lorsqu'une personne ou un véhicule entre dans une zone définie au sol sans traverser d'abord une ou plusieurs autres zones définies au sol.

Comment cela fonctionne-t-il ?

Détection d'objets

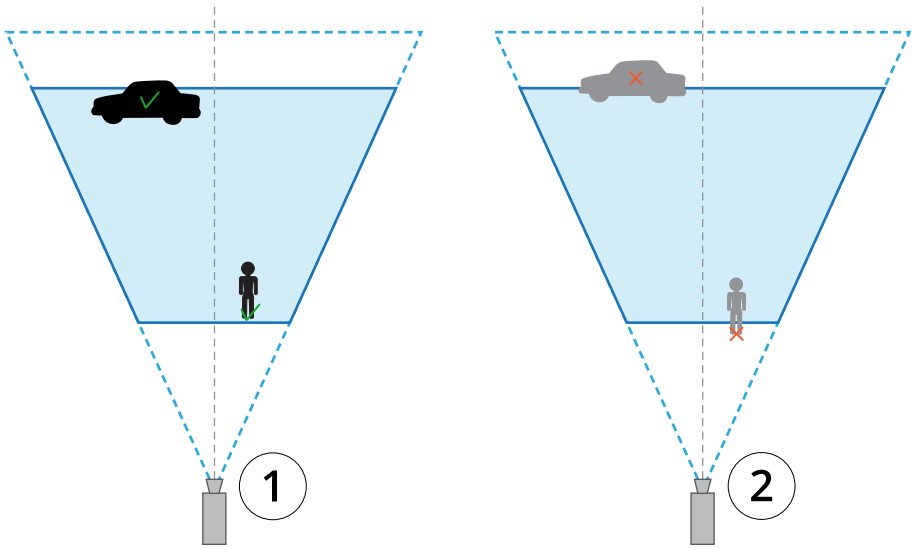
AXIS Perimeter Defender peut détecter des personnes ou des véhicules en mouvement. Pour permettre la détection :

- Une personne ou un véhicule doit être complètement visible dans la zone de détection pendant au moins trois secondes.
- Un véhicule peut mesurer jusqu'à 12 mètres de long. (en mode IA, il n'y a pas de longueur maximale).
- Les personnes ou les véhicules doivent être en mouvement perceptible dans le champ de vision de la caméra. En pratique, cela signifie que le taux de détection d'une personne s'approchant ou s'éloignant de la caméra en ligne droite est inférieur à celui d'une personne marchant perpendiculairement au champ de vision de la caméra.



1 Zone de détection
2 Personne s'éloignant de la caméra
3 Personnes marchant perpendiculairement au champ de vision de la caméra

- Le point de détection doit se trouver à l'intérieur de la zone de détection. Le point de détection se situe aux pieds d'une personne ou au centre d'un véhicule.



1 Point de détection à l'intérieur de la zone de détection
2 Point de détection à l'extérieur de la zone de détection

Une fois le véhicule ou la personne détecté, AXIS Perimeter Defender continue de le suivre, même s'il est partiellement masqué (par exemple, si le corps d'une personne est masqué par une voiture mais sa tête reste visible).

Si une personne ou un véhicule détecté s'immobilise pendant quelques secondes, AXIS Perimeter Defender interrompt le suivi. Si le mouvement reprend après moins de 15 secondes, l'application poursuit le suivi. Si la personne se trouvait dans une zone de franchissement, il n'est pas garanti que le scénario se déclenche correctement.

Comment fonctionne PTZ Autotracking ?

AXIS Perimeter Defender PTZ Autotracking associe une caméra fixe et une caméra PTZ. Lorsque la caméra fixe détecte des personnes ou des véhicules en mouvement, elle envoie les données de localisation des objets à la caméra PTZ associée. Tant que les objets restent dans le champ de vision de la caméra fixe, la caméra PTZ peut suivre automatiquement les objets et effectuer un zoom pour les garder en vue.

Conditions susceptibles de retarder ou de faire manquer des détections

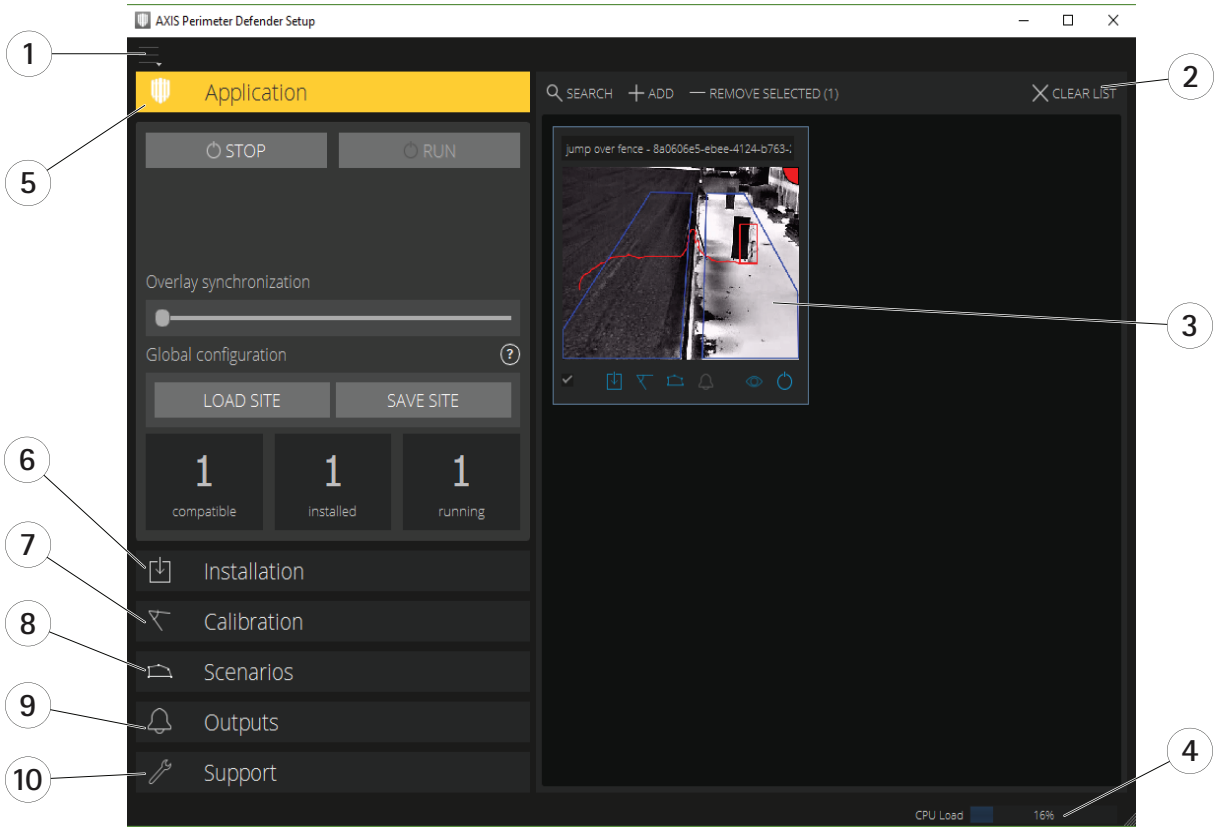
- Brouillard
- Lumière éclairant directement la caméra
- Éclairage inapproprié
- Image trop bruyante

Situations susceptibles de déclencher de fausses alarmes

- Personnes ou véhicules partiellement cachés. Par exemple, une petite fourgonnette qui apparaît derrière un mur peut ressembler à une personne, car la partie visible est haute et étroite.
- Insectes sur l'objectif de la caméra. Notez que les caméras jour/nuit à éclairage infrarouge attirent les insectes et les araignées.
- Phares de voiture dans des conditions de forte pluie.
- Animaux d'une taille similaire à celle d'un humain, notamment si les types d'approche supplémentaires accroupissement/marche à quatre pattes ou roulement ont été sélectionnés dans l'onglet **Scenarios** (Scénarios).
- Éclairage intense produisant des ombres.

L'interface utilisateur

L'interface d'AXIS Perimeter Defender vous permet, par exemple, d'étalonner les dispositifs, de configurer des scénarios et d'effectuer des actions pour plusieurs dispositifs. La configuration à distance permet de procéder à la configuration depuis n'importe quel endroit disposant d'une connexion réseau.



1 *Paramètres d'interface, on page 7*
2 *Gestion des périphériques. Cf. Ajout de périphériques, on page 17.*
3 *Vidéo en direct, on page 8*
4 *Indicateur de charge de l'UC. Cf. Charge CPU, on page 11.*
5 *Onglet Application, on page 9*
6 *Onglet Installation, on page 10*
7 *Onglet Calibrage, on page 10*
8 *Onglet Scénarios, on page 10*
9 *Onglet Sortie, on page 11*
10 *Onglet Assistance, on page 11*

Paramètres d'interface

Le menu des paramètres d'interface contient les éléments suivants :

Préférences répertoires –

Chemin de configuration du périphérique : sélectionnez l'emplacement de stockage des fichiers temporaires et de la vidéo de calibrage.

Chemin de configuration du site : sélectionnez l'emplacement de stockage des fichiers à partir des chemins de chargement.

Mots de passe – Consultez les mots de passe utilisés et ajoutez-en de nouveaux. Les mots de passe ne sont pas enregistrés lorsque l'utilisateur quitte l'application.

Gérer les packages de clip de démonstration – Importez ou supprimez des clips de démonstration.

Activer le mode fréquence d'image maximale – Modifiez la fréquence d'image dans la vidéo en direct. Cf. *Charge CPU, on page 11*.

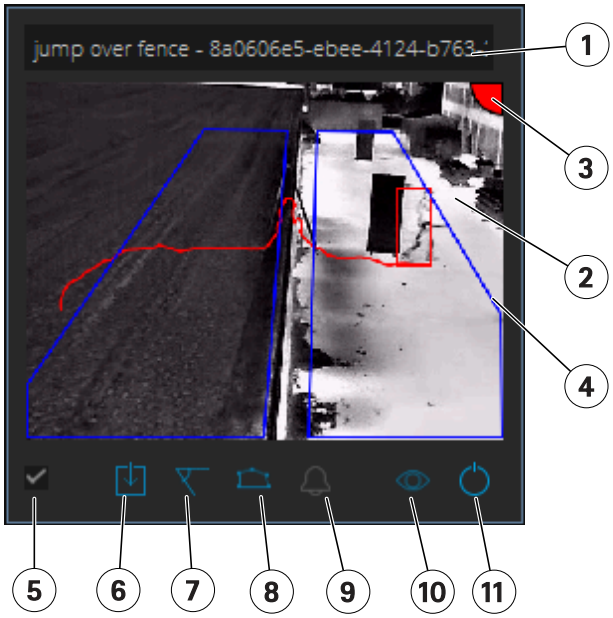
Affichage en pieds et pouces – Basculez entre les unités métriques et impériales.

Changer de langue – Changez la langue de l'application.

À propos de – Consultez la version d'AXIS Perimeter Defender Setup.

Vidéo en direct

Chaque périphérique connecté dispose d'une fenêtre de vidéo en direct dans l'interface principale. La vidéo en direct indique l'état du périphérique et permet un accès rapide aux fonctions principales.



1. Nom du dispositif – Cliquez pour modifier le nom du périphérique. Il contient toujours l'adresse IP et le numéro MAC du périphérique. Survolez le nom pour afficher le rapport d'aspect utilisé pour l'analyse, qui indique la couverture maximale du champ de vision, et pour vérifier si le périphérique utilise une connexion distante.

2. Image en direct – En mode Vue générale, la fréquence d'image est de 1 ips. Double-cliquez pour agrandir l'image et augmenter la fréquence d'image à 8 ips.

3. État de l'alarme – L'état de l'alarme est visible uniquement si l'incrustation est active et si AXIS Perimeter Defender est installé, configuré et exécuté. Le gris indique que la fonctionnalité d'alarme n'est pas active ou que les paramètres de configuration sont en cours de chargement. Le vert indique que la fonctionnalité d'alarme est active. Le rouge indique qu'une alarme a été déclenchée.

4. Zones de détection – Les zones de détection sont visibles uniquement si l'incrustation est active et si AXIS Perimeter Defender est installé, configuré et exécuté.

5. Case à cocher – Cette case à cocher permet la sélection de plusieurs périphériques.

6. Bouton d'état d'installation/d'accès rapide – Survolez cette zone pour afficher la version d'

AXIS Perimeter Defender installée sur le périphérique. Si l'icône est remplacée par , cela signifie qu'une version plus récente est disponible. Cliquez pour ouvrir l'onglet Installation pour le périphérique. Le gris indique que le périphérique n'est pas installé. L'orange indique que le dispositif est installé, mais ne dispose pas de licence valide. Le bleu indique que le dispositif est installé et dispose d'une licence valide.

7. Bouton d'état de calibrage/d'accès rapide – Cliquez pour ouvrir l'onglet Calibrage pour le périphérique. Le gris indique que le périphérique n'est pas calibré. Le bleu indique que le périphérique est calibré.

8. Bouton d'état des scénarios/d'accès rapide – Cliquez pour ouvrir l'onglet Scénarios pour le périphérique. Le gris indique qu'aucun scénario n'est défini. Le bleu indique qu'au moins un scénario est défini.

9. Bouton d'état des sorties/d'accès rapide – Cliquez pour ouvrir l'onglet Sortie pour le périphérique. Le gris indique qu'aucune sortie n'est configurée. Le bleu indique qu'au moins une sortie est configurée.

10. Bouton d'état d'incrustation/bascule – Cliquez pour activer/désactiver l'incrustation. Le gris indique que l'incrustation est inactive. Le bleu indique que l'incrustation est active. L'incrustation se présente sous la forme d'un cadre englobant autour des objets détectés, ainsi que sous la forme d'une traînée affichant la trajectoire des objets.

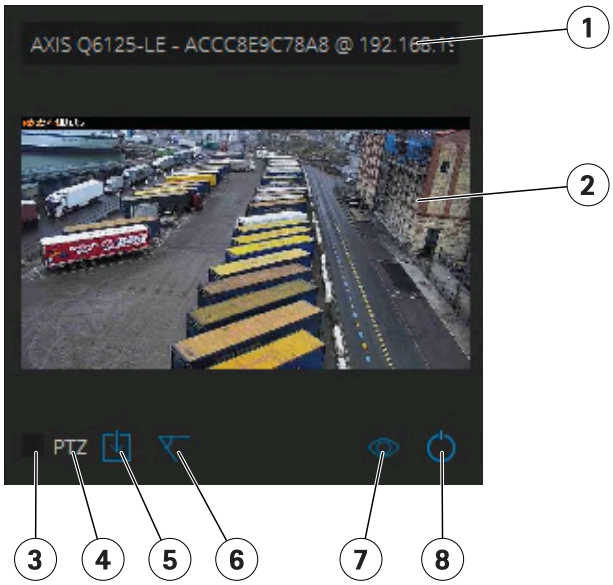
11. Bouton d'état d'exécution/bascule – Cliquez pour exécuter/arrêter l'application sur le périphérique. Le gris indique que l'application est arrêtée. Le bleu indique qu'elle est en cours d'exécution.

Remarque

L'incrustation est disponible uniquement si une connexion directe est disponible entre le périphérique et l'ordinateur de l'utilisateur, c'est-à-dire si aucun pare-feu ou dispositif similaire n'empêche la connexion au port d'incrustation sur le périphérique.

Vidéo en direct – PTZ Autotracking

La vidéo en direct des périphériques dotés d'AXIS Perimeter Defender PTZ Autotracking diffère légèrement de la vidéo en direct standard.



1 *Nom périphérique*
2 *Image en direct*
3 *Case à cocher*
4 *Indique que le périphérique utilise AXIS Perimeter Defender PTZ Autotracking*
5 *Bouton d'état d'installation/d'accès rapide*
6 *Bouton d'état de calibrage/d'accès rapide*
7 *Bouton d'état d'incrustation/bascule*
8 *Bouton d'état d'exécution/bascule*

Onglet Application

- **Run** (Exécuter) : lance l'analyse sur le ou les dispositifs sélectionnés.
- **Stop** (Arrêter) : arrête l'analyse sur le ou les dispositifs sélectionnés.
- **Charger le site** : permet de charger un site précédemment enregistré, c'est-à-dire des périphériques et leurs fichiers de configuration respectifs.
- **Enregistrer le site** : permet d'enregistrer le site actuel, c'est-à-dire toutes les informations des périphériques et leurs fichiers de configuration respectifs.
- **Synchronisation de l'incrustation** : contrôlez la synchronisation de l'incrustation des métadonnées d' AXIS Perimeter Defender. Ce curseur contrôle le délai entre l'incrustation des métadonnées et les images

reçues afin d'équilibrer la diffusion plus lente des images par rapport aux métadonnées. La valeur du curseur indique le délai défini pour la caméra actuellement sélectionnée. Si plusieurs caméras sont connectées, la valeur indiquée s'applique à la première caméra sélectionnée. La modification de la valeur du curseur modifie le délai pour toutes les caméras sélectionnées.

Vous pouvez également consulter le nombre de périphériques compatibles ajoutés, le nombre total de périphériques dotés d'AXIS Perimeter Defender et le nombre de périphériques sur lesquels l'analyse est en cours.

Onglet Installation

- **Application: Install** (Application : Installer) : permet d'installer l'application sur les dispositifs sélectionnés.
- **Application: Uninstall** (Application : Désinstaller) : permet de désinstaller l'application des dispositifs sélectionnés.
- **Licence: Install** (Licence : Installer) : permet d'installer la licence sur les dispositifs sélectionnés.

Onglet Calibrage

- **Automatique** : permet d'effectuer un calibrage automatique des périphériques sélectionnés.
- **Manuel** : permet d'effectuer un calibrage manuel des périphériques sélectionnés.

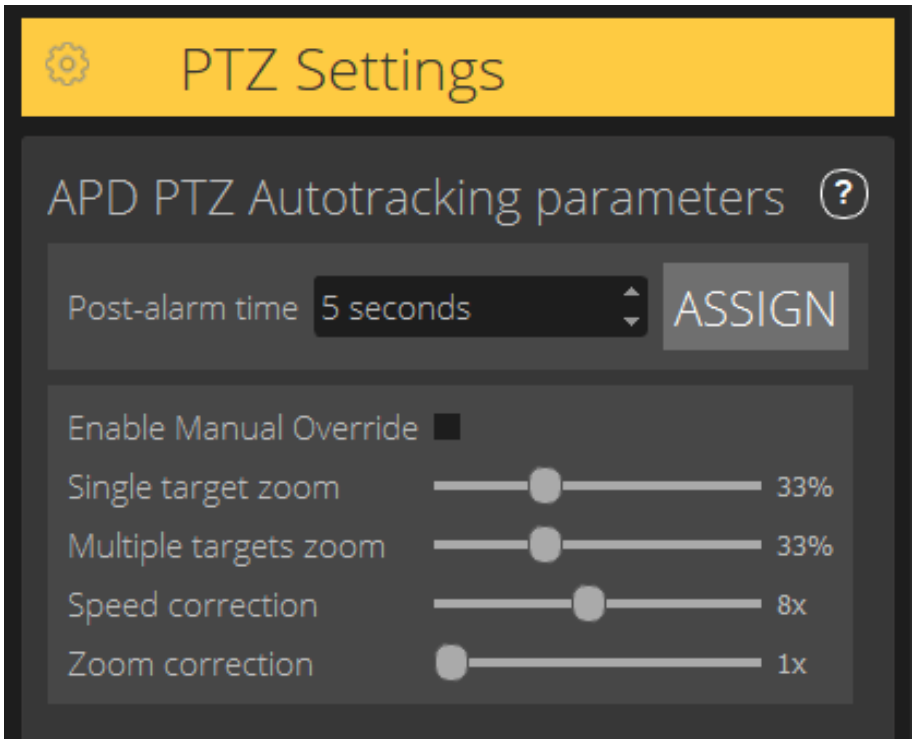
Onglet Scénarios

- **Paramètres globaux** : s'appliquent à tous les scénarios.
- **Scénarios avancés** : permet de créer des scénarios conditionnels, de détection des intrusions, de détection des rôdeurs et de franchissement de zone.

Onglet Paramètres de caméra PTZ

Remarque

Cet onglet s'affiche uniquement si vous disposez du plug-in AXIS Perimeter Defender PTZ Autotracking.



- **Durée post-alarme** : permet de définir le délai après lequel la caméra PTZ reprend sa position d'origine une fois que l'objet suivi a disparu de la vue.

- **Activer le mode manuel** : lorsque cette option est sélectionnée, l'opérateur peut prendre le contrôle de la caméra PTZ avec un joystick dans le VMS ou sur la page Web de la caméra.
- **Zoom sur cible unique** : permet d'ajuster le niveau de zoom pour suivre une cible unique. Une valeur plus élevée offre de meilleurs résultats d'identification, mais augmente également le risque de perdre des objets qui se déplacent rapidement.
- **Zoom sur cibles multiples** : permet d'ajuster le niveau de zoom pour suivre plusieurs cibles.
- **Correction de la vitesse** : permet d'ajuster la vitesse de suivi pour maintenir les objets qui se déplacent rapidement au centre de l'image de la caméra PTZ. Une valeur élevée peut rendre le suivi instable.
- **Correction du zoom** : une valeur plus élevée augmente le zoom arrière pour les objets qui se trouvent à proximité du bord du champ de vision de la caméra PTZ.

Onglet Sortie

- **Configurer** : permet d'ouvrir la page Web du périphérique pour créer et configurer des alarmes.
- **Alarme test** : permet de tester l'alarme configurée pour le périphérique.
- **Post-alarm time: Assign** (Heure de post-alarme : Assigner) : permet de définir l'heure de post-alarme.

Onglet Assistance

- **Charge** : permet de charger une configuration sauvegardée pour les périphériques sélectionnés. Cela s'avère particulièrement utile pour procéder à une restauration rapide après une panne de périphérique ou une désinstallation accidentelle. La configuration inclut les éléments suivants :

– Licence
– Paramètres
– Calibrage et scénarios
– Vidéo de calibrage

- **Enregistrer** : permet de créer une sauvegarde de la configuration des périphériques sélectionnés.
- **Effacer** : permet d'effacer le calibrage et les scénarios des périphériques sélectionnés. Cette option est utile si les caméras ont bougé, car les zones de calibrage et de détection ne sont alors plus valides.
- **Afficher le journal de l'application** : permet d'afficher le journal interne d'AXIS Perimeter Defender.
- **Exporter le journal d'assistance** : permet de générer un fichier d'assistance contenant des informations détaillées. Joignez toujours ce fichier à une demande d'assistance.

Charge CPU

Le témoin de charge du processeur indique en temps réel la charge actuelle du processeur de l'ordinateur. Lorsque la charge du processeur est excessive, il est possible qu'un ordinateur ou une application ne réponde pas. Assurez-vous de fermer les autres applications lorsque vous utilisez AXIS Perimeter Defender Setup pour optimiser l'allocation de votre processeur. Si la charge de l'UC est trop élevée et que vous essayez d'ajouter un périphérique, le système génère un avertissement.

Chaque dispositif ajouté consomme des ressources du processeur de l'ordinateur hôte pour décoder et afficher le flux vidéo. Pour limiter l'impact sur l'ordinateur hôte, les flux vidéo de périphériques ajoutés s'affichent par défaut à une fréquence d'image réduite (environ 1 ips). La fréquence d'image normale (environ 8 ips) est restaurée lorsque les flux sont optimisés ou pendant le processus de calibrage.

Important

Lorsque l'option **Enable full frame rate mode** (Activer le mode de fréquence d'image maximale) est activée, il est possible que l'interface ne réponde pas si vous vous connectez à un nombre important de caméras ou si vous utilisez un ordinateur peu puissant.

Affichage d'une démonstration d'AXIS Perimeter Defender

À des fins de démonstration, AXIS Perimeter Defender et AXIS Perimeter Defender PTZ Autotracking sont préinstallés avec des clips de démonstration qui peuvent être utilisés pour présenter les fonctionnalités d'analyse sans disposer d'une caméra installée et active. Les clips de démonstration présentent les types de résultats de détection et de suivi automatiques que vous pouvez obtenir dans différents environnements.

1. Accédez à **Application > Ajouter > Clips de démonstration** et effectuez l'une ou plusieurs des opérations suivantes :
   - Filtrez les clips de démonstration en fonction de leur type.
   - Sélectionnez au moins un clip de démonstration.
2. Pour ajouter les clips de démonstration, cliquez sur **Ajouter clips de démonstration sélectionnés**.

Une fois ajoutés, les clips de démonstration apparaissent sous forme de flux vidéo standard dans l'interface. Le calibrage est disponible et l'analyse est déjà activée de sorte que l'utilisateur puisse consulter immédiatement les résultats d'analyse et de suivi automatique sur le flux vidéo. Vous pouvez arrêter ou démarrer l'analyse et le suivi automatique en cliquant sur l'état d'exécution dans la vidéo en direct ou sur le bouton **Exécuter** ou **Arrêter** du volet de gauche.

Le calibrage et l'appariement peuvent être modifiés et réexécutés. De même, des scénarios de détection peuvent être ajoutés, supprimés et modifiés.

L'onglet **Assistance** du volet de gauche contient un bouton **Effacer** qui vous permet de rétablir les valeurs d'origine du calibrage et des scénarios. Il n'est pas possible de supprimer complètement le calibrage.

MISE EN ROUTE

Les processus d'installation d'AXIS Perimeter Defender et d'AXIS Perimeter Defender PTZ Autotracking diffèrent légèrement.

Premiers pas avec AXIS Perimeter Defender

Effectuez les étapes suivantes pour que votre site fonctionne avec AXIS Perimeter Defender :

1. Installez la caméra. Cf. *Installation de la caméra, on page 13*.
2. Téléchargez et installez le logiciel sur votre ordinateur. Cf. *Installation du logiciel sur l'ordinateur, on page 16*.
3. Connectez-vous à vos périphériques. Cf. *Ajout de périphériques, on page 17*.
4. Installez AXIS Perimeter Defender sur chaque périphérique. Cf. *Installation du logiciel sur des périphériques, on page 18*.

Remarque

Vous n'avez pas besoin de calibrer les périphériques exécutés en mode IA uniquement. Pour exécuter simultanément des périphériques en mode de calibrage et en mode IA, vous devez les calibrer.

5. Calibrez les périphériques. Cf. *Calibrage - AXIS Perimeter Defender, on page 19*.
6. Ajoutez des scénarios pour définir les règles de déclenchement d'alarmes. Cf. *Définition de scénarios, on page 26*.
7. Configurez les alarmes à envoyer. Cf. *Définition des sorties, on page 30*.

Premiers pas avec AXIS Perimeter Defender PTZ Autotracking

Effectuez les étapes suivantes pour que votre site fonctionne avec AXIS Perimeter Defender PTZ Autotracking :

1. Installez les caméras. Voir *Installation de la caméra, on page 13* et *Installation de la caméra PTZ, on page 16*.
2. Téléchargez et installez le logiciel sur votre ordinateur. Cf. *Installation du logiciel sur l'ordinateur, on page 16*.
3. Connectez-vous à vos périphériques. Cf. *Ajout de périphériques, on page 17*.
4. Installez AXIS Perimeter Defender version 2.5.0 ou ultérieure sur la caméra fixe et AXIS Perimeter Defender PTZ Autotracking sur la caméra PTZ. Cf. *Installation du logiciel sur des périphériques, on page 18*.
5. Calibrez les périphériques et configurez des scénarios. Cf. *Calibrage - PTZ Autotracking, on page 26*.
6. Associez les périphériques. Cf. *Appariement des caméras - PTZ Autotracking, on page 29*.
7. Configurez les alarmes à envoyer. Cf. *Définition des sorties, on page 30*.

Installation de la caméra

À propos de l'outil de conception

Pour définir le positionnement de la caméra sur site, nous vous recommandons d'utiliser l'outil de conception pour AXIS Perimeter Defender. Il tient compte des exigences des caméras Axis et d'AXIS Perimeter Defender. En outre, vous pouvez l'utiliser pour réaliser des installations doubles, c'est-à-dire pour utiliser deux caméras en association. L'outil vous aide à définir les réglages suivants :

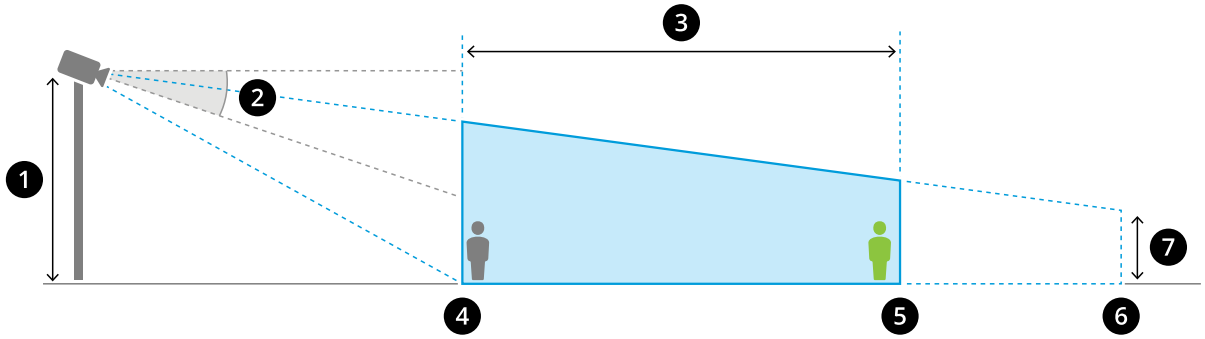
- Hauteur de montage de la caméra
- Angle d'inclinaison
- Distance de détection minimale
- Distance de détection maximale

Pour télécharger l'outil, veuillez aller à *axis.com/products/axis-perimeter-defender*.

Recommandations pour l'installation de la caméra

Remarque

Pour les caméras en mode IA uniquement, vous trouverez des recommandations de montage dans l'application.



Caméra correctement installée.

1 *Hauteur de montage*
2 *Inclinaison*
3 *Zone de détection*
4 *Distance de détection minimale*
5 *Distance de détection maximale*
6 *Distance du champ de vision*
7 *Hauteur du champ de vision*

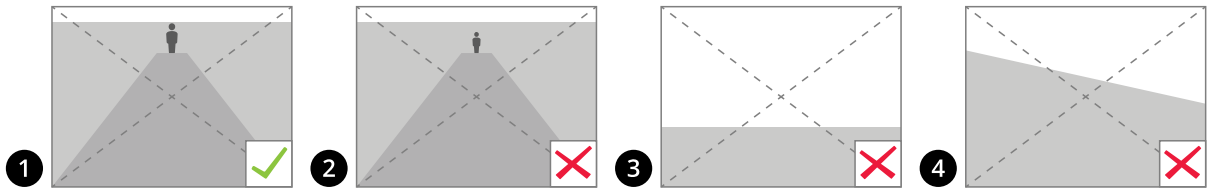
Hauteur de l'objet à la distance de détection maximale – Pour qu'une personne qui se tient debout soit détectée à la distance de détection maximale, la hauteur en pixels doit correspondre à au moins 5 % de la hauteur totale de l'image (3,5 % pour les caméras thermiques). Par exemple, si la hauteur de l'image visualisée est de 576 pixels, la hauteur d'une personne debout à la fin de la zone de détection doit être d'au moins 28 pixels (20 pixels pour les caméras thermiques).

Hauteur de l'objet à la distance de détection minimale – Pour qu'une personne qui se tient debout soit détectée à la distance de détection minimale, la hauteur en pixels ne peut pas être supérieure à 60 % de la hauteur totale de l'image.

Hauteur de l'objet en mode IA – Lorsque vous exécutez l'application en mode IA, les objets doivent avoir la même taille ou une taille plus grande que l'avatar à détecter.

Angle d'inclinaison – La caméra doit être orientée vers le sol de sorte que le centre de l'image se trouve sous l'horizon. Installez la caméra de sorte que la distance de détection minimale soit supérieure à la moitié de la hauteur d'installation de la caméra (distance de détection minimale > hauteur d'installation de la caméra / 2).

Angle de roulis – L'angle de roulis de la caméra doit être pratiquement égal à zéro.



1 *La hauteur de l'objet, l'angle d'inclinaison et l'angle de roulis sont appropriés.*
2 *La hauteur de l'objet à la distance de détection maximale est inférieure à 5 % de la hauteur de l'image (3,5 % pour les caméras thermiques).*
3 *Le centre de l'image se trouve au-dessus de la ligne d'horizon.*
4 *L'angle de roulis de la caméra n'est pas pratiquement égal à zéro.*

La distance de détection maximale dépend des éléments suivants :

- Type et modèle de la caméra
- Objectif de la caméra. Une distance focale plus élevée permet une distance de détection supérieure.
- Taille minimale en pixels d'un humain dans l'image à détecter. La hauteur en pixels d'une personne qui se tient debout doit correspondre à au moins 5 % de la hauteur de l'image pour les caméras visuelles et 3,5 % pour les caméras thermiques.
- Météo
- Éclairage
- Charge de caméra

Lorsque vous installez la caméra, tenez compte des éléments suivants :

- L'application tolère les légères vibrations de la caméra. Toutefois, la caméra est plus performante en l'absence de vibrations.
- Le champ de vision de la caméra doit être fixe.

Hauteur de montage

Pour atteindre une distance de détection donnée, outre la taille minimale requise des pixels, la caméra doit être placée à une hauteur minimale. Il n'y a pas de hauteur de montage maximale tant que les autres exigences, notamment l'angle d'inclinaison, sont respectées.

Distance de détection requise	Hauteur de montage minimale de la caméra
20 m (66 pi)	2,5 m (hauteur minimale admissible)
100 m (330 pi)	3m (10 pi.)
200 m (650 pi)	4 m (13 pi)
300 m (1000 pi)	5 m (16 pi)
500 m (1600 pi)	6 m (20 pi)

Exigences relatives à la scène

Remarque

Pour les caméras en mode IA uniquement, vous trouverez des recommandations relatives à la scène dans l'application.

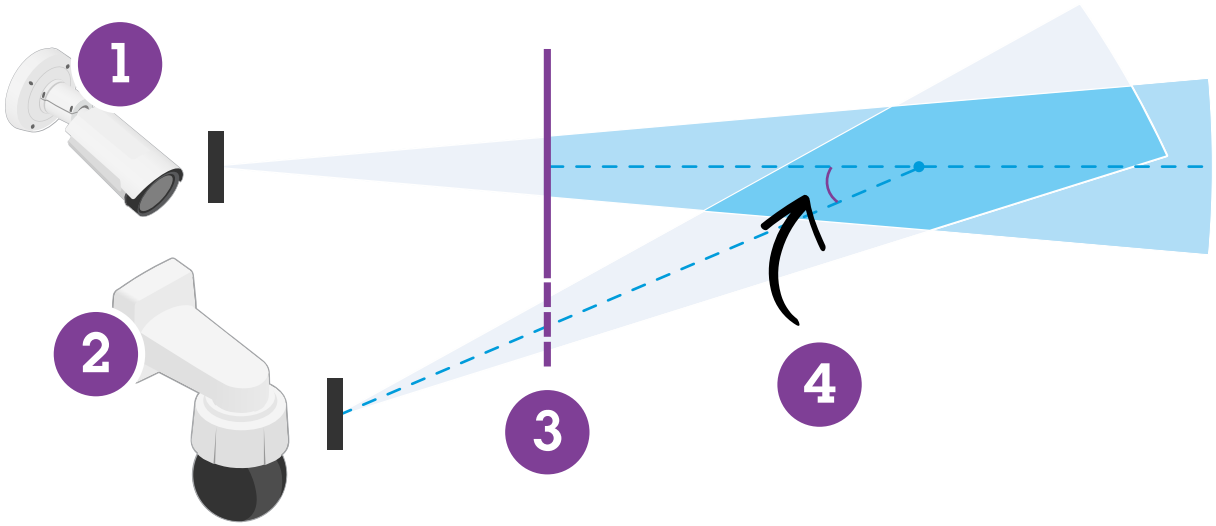
La zone de détection doit présenter les conditions suivantes :

- Vue claire
- Le sol doit être plat ou avec une légère pente
- L'éclairage n'est pas déclenché par le mouvement
- Vue claire
- Pour les caméras visuelles, le niveau des réglages d'éclairage et d'image doit être suffisant pour garantir un contraste correct entre les êtres humains et les véhicules et l'arrière-plan.
  - Lorsque vous utilisez une caméra Axis jour et nuit avec un éclairage artificiel, nous vous recommandons de définir au moins 50 lux dans l'intégralité de la zone de détection.
  - Lorsque vous utilisez des spots infrarouges externes, nous recommandons une distance de détection maximale de 80 m et une portée deux fois supérieure à la distance de détection maximale.
  - Lorsque vous utilisez un éclairage infrarouge intégré, la distance de détection maximale est limitée à 20 m, selon la caméra et l'environnement.
- Pour les caméras thermiques, un contraste élevé entre l'arrière-plan et le premier plan est nécessaire

Pour optimiser les performances de détection, AXIS Perimeter Defender détecte automatiquement la différence entre le jour et la nuit et utilise ces informations pour ajuster les algorithmes de détection. L'ajustement prend environ 24 heures, ce qui signifie que la détection de jour et de nuit sera optimale après 24 heures d'exécution de l'application.

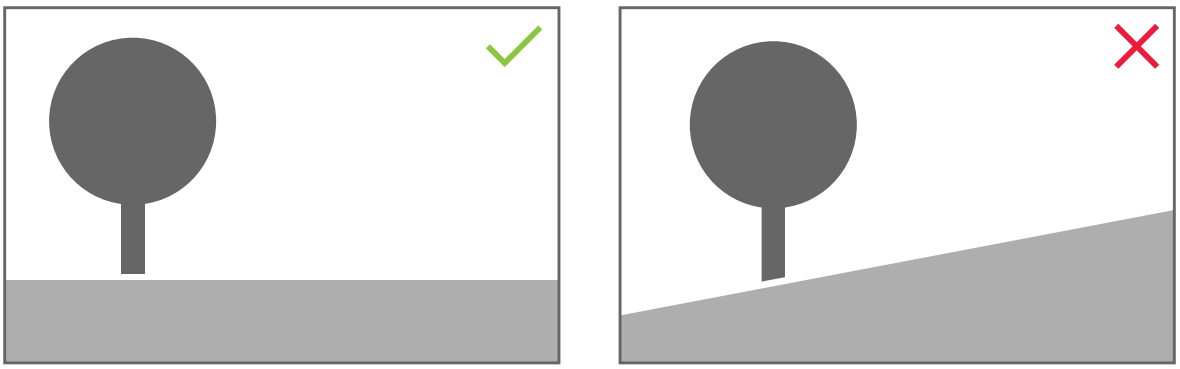
Installation de la caméra PTZ

Ce chapitre explique comment installer la caméra PTZ par rapport à la caméra fixe. Pour obtenir des instructions sur l'installation de la caméra fixe, voir *Installation de la caméra, on page 13*.



1 *Caméra réseau fixe*
2 *Caméra réseau PTZ*
3 *Distance de détection minimale*
4 *Angle entre les caméras*

- La position de départ préréglée de la caméra PTZ doit couvrir plus de 60 % de la zone de détection de la caméra fixe.
- Pour être suivie par la caméra PTZ, une personne qui se tient debout doit couvrir plus de 4 % de la hauteur d'image de la caméra PTZ.
- La caméra PTZ doit être placée avant la distance de détection minimale de la caméra fixe (C).
- L'angle entre la caméra fixe et la caméra PTZ doit être inférieur à 30° (D).



- Le sol doit être plat.

Installation du logiciel sur l'ordinateur

Les caméras exécutant AXIS Perimeter Defender doivent être accessibles via HTTP depuis l'ordinateur exécutant AXIS Perimeter Defender Setup Interface.

L'interface AXIS Perimeter Defender Setup Interface (requise uniquement pendant la phase de configuration) nécessite :

- Processeur Intel® Core™ 2 Duo ou supérieur
- Prise en charge d'Open GL
- Au moins 16 Go de RAM
- Windows® 10, Windows® 11 ou Win Server 2022
- Résolution d'écran d'au moins 1024 x 768

Notez que le nombre de caméras gérables par un seul ordinateur est limité. Par exemple, pour une machine équipée d'un processeur Intel® Core™ i5-1135G7 de 11e génération cadencé à 2,40 GHz, il est recommandé d'ajouter un maximum de 10 caméras et d'exécuter un étalonnage automatique simultané sur un maximum de 5 caméras.

Remarque

L'exécution de l'interface AXIS Perimeter Defender Setup Interface sur une machine virtuelle n'est pas prise en charge.

1. Téléchargez le logiciel AXIS Perimeter Defender depuis *axis.com/products/axis-perimeter-defender*
2. Installez le logiciel sur votre ordinateur.

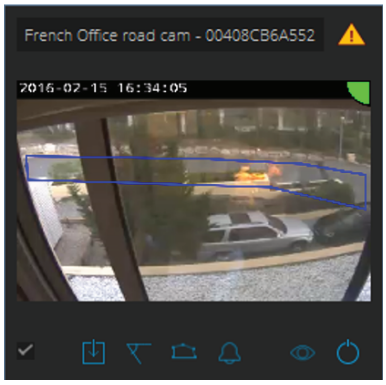
Ajout de périphériques

Vous pouvez ajouter des périphériques à l'application AXIS Perimeter Defender de trois façons différentes :

- Automatiquement par une analyse réseau. Cf. *Ajout automatique de périphériques, on page 18*.
- Manuellement en spécifiant les paramètres de connexion. Cf. *Ajout manuel de périphériques, on page 18*.
- Automatiquement en chargeant un site précédemment enregistré. Cf. *Chargement d'un site existant, on page 18*.

Après l'ajout d'un périphérique, vous pouvez consulter la liste de toutes les autres applications installées sur le périphérique. Nous vous recommandons d'arrêter toutes les applications non essentielles, car elles utilisent les ressources de l'UC de la caméra, ce qui affecte les performances d'AXIS Perimeter Defender et peut empêcher une installation correcte.

Si un périphérique ne dispose pas de suffisamment de ressources d'UC car d'autres applications sont en cours d'exécution, AXIS Perimeter Defender réduit la fréquence d'image. Si la fréquence d'image est inférieure à 5 images par seconde, un triangle d'avertissement jaune s'affiche en regard du nom du périphérique dans la vidéo en direct. Lorsque vous survolez le triangle, la fréquence d'image actuelle s'affiche.



Remarque

Une fréquence d'image inférieure à 5 ips peut réduire sensiblement les performances d'analyse de la vidéo, ce qui peut entraîner des détections manquées et incorrectes.

Pour en savoir plus, consultez *Charge CPU, on page 11*.

Ajout automatique de périphériques

Important

La fonctionnalité de recherche ne fonctionne pas sur tous les réseaux, c'est-à-dire qu'
AXIS Perimeter Defender Setup ne peut trouver que des périphériques connectés au même sous-réseau que celui du client exécutant le logiciel. Pour ajouter des périphériques connectés à un sous-réseau différent, procédez manuellement. La fonctionnalité de recherche peut également échouer si les routeurs ou les commutateurs réseau sont configurés pour filtrer la multidiffusion.

1. Pour rechercher des périphériques dans le réseau environnant, accédez à **Application**, puis cliquez sur **Rechercher**.
   Lorsque vous effectuez une recherche pour la première fois et qu'aucun mot de passe n'est disponible, une boîte de dialogue de mot de passe s'affiche. Sinon, le mot de passe disponible est utilisé pour la connexion aux périphériques.
2. Sélectionnez les périphériques et cliquez sur **Ajouter périphériques sélectionnés**.
   Si le mot de passe est correct, une image statique s'affiche pour guider l'utilisateur lors de la sélection des périphériques.

Ajout manuel de périphériques

1. Accédez à **Application**, puis cliquez sur **Ajouter**.
2. Entrez les informations suivantes :

- Adresse IP ou nom d'hôte du périphérique.
- Mot de passe racine du périphérique, car AXIS Perimeter Defender nécessite un accès racine.
- Port HTTP utilisé pour la connexion. Le port par défaut est le 80.
- Nom facultatif facilitant la reconnaissance du périphérique.
- Si le périphérique se trouve sur un réseau distant pour lequel la connexion peut être lente, cochez **Périphérique sur réseau distant**. Les connexions lentes qui ne sont pas configurées en tant que connexions distantes peuvent conduire à des calibrages défectueux ou incorrects.

Remarque

Pour les connexions à distance, l'utilisateur doit pouvoir se connecter au dispositif via HTTP. Veillez à configurer correctement le port HTTP. La configuration à distance peut échouer lorsque la connexion ne dispose pas d'une bande passante suffisante ou stable.

3. Cliquez sur **OK**.

Remarque

Si vous ne parvenez pas à ajouter une caméra à l'aide du nom d'hôte, vérifiez les paramètres réseau et DNS ou ajoutez le périphérique à l'aide de son adresse IP.

Chargement d'un site existant

Pour charger une configuration de site précédemment enregistrée :

1. Accédez à **Application**, puis cliquez sur **Charger le site**.
2. Recherchez et sélectionnez le fichier de configuration du site, puis cliquez sur **Ouvrir**. La vidéo en direct s'affiche automatiquement.

Installation du logiciel sur des périphériques

Vous devez installer AXIS Perimeter Defender sur chaque périphérique.

Si vous souhaitez vérifier quelle version d'AXIS Perimeter Defender est installée sur un périphérique, survolez la zone **État d'installation** dans la vidéo en direct.

Si AXIS Perimeter Defender n'est pas installé, toutes les icônes de la vidéo en direct sont grises.

Installation du logiciel sur un périphérique

1. Accédez à **Installation**.
2. Sélectionnez les périphériques sur lesquels vous souhaitez installer l'application.
3. Sélectionnez la dernière version disponible d'AXIS Perimeter Defender, puis cliquez sur **Installer**. AXIS Perimeter Defender est à présent installé sur les périphériques sélectionnés et démarre automatiquement.
4. Accédez à une licence et effectuez l'une des opérations suivantes :

– Si vous effectuez l'installation sur un seul dispositif : sélectionnez le fichier de licence du dispositif.

– Si vous effectuez l'installation sur plusieurs dispositifs : sélectionnez le dossier où sont stockés les fichiers de licence.

5. Cliquez sur **Installer**.

Calibrage - AXIS Perimeter Defender

Calibrage

Remarque

Vous n'avez pas besoin de calibrer les périphériques exécutés en mode IA uniquement. Pour exécuter simultanément des périphériques en mode de calibrage et en mode IA, vous devez les calibrer.

Pour permettre à AXIS Perimeter Defender d'interpréter correctement la scène, vous devez calibrer tous les périphériques. Au cours du calibrage, vous introduisez des points de référence qui fournissent des informations de profondeur et de hauteur au processeur. Vous définissez également la zone d'intérêt.

Le calibrage se compose de deux tâches :

1. Exécution d'un calibrage :
   – Automatique : recommandé dans la plupart des cas. Cf. *Exécution d'un calibrage automatique, on page 20*.
   – Manuel : recommandé si le calibrage automatique échoue sur une caméra, pour un ajustement ou lorsqu'il serait compliqué de traverser une scène comportant des objets de taille connue. Par exemple, il peut s'agir d'un périmètre distant avec une ligne de clôture composée de poteaux de clôture espacés régulièrement et d'une hauteur uniforme. Cf. *Calibrage manuel, on page 24*.
2. Vérifiez les résultats du calibrage. Cf. *Vérification de la qualité du calibrage , on page 21*.

Pour accélérer la configuration d'un site de grande taille, vous pouvez calibrer plusieurs périphériques simultanément. Vous pouvez effectuer un calibrage automatique ou manuel de la même manière que pour une seule caméra. Avant de calibrer plusieurs périphériques simultanément, tenez compte des éléments suivants :

- Le nombre maximal de périphériques que vous pouvez installer et configurer simultanément dépend de la puissance de l'UC et de la mémoire disponible sur votre ordinateur. Un nombre trop important de périphériques dans AXIS Perimeter Defender Setup peut entraîner des blocages. Lorsque l'avertissement de surcharge de l'UC s'affiche, installez et configurez un sous-ensemble de périphériques à l'aide de la fonction d'enregistrement de site.
- Le calibrage automatique de plusieurs périphériques nécessite davantage de ressources d'UC et de RAM que pour un seul périphérique. Sur les systèmes peu puissants, il est possible que l'ordinateur ne réponde pas pendant un certain temps ou que l'application se bloque. En cas de blocage, les vidéos capturées restent disponibles pour le calibrage d'une seule caméra.

Remarque

- AXIS Perimeter Defender prend en charge différents rapports d'aspect selon la résolution maximale fournie par la caméra. Vous devez donc répéter tous les calibrages précédents si vous modifiez la

résolution. Toutefois, si vous modifiez la résolution du flux sur la page Web de la caméra, il n'est pas nécessaire de refaire le calibrage.

- Nous vous recommandons d'utiliser le même rapport d'aspect d'image dans AXIS Perimeter Defender et dans le VMS pour garantir que les informations affichées s'adaptent au contenu de l'image. Pour connaître le rapport d'aspect, survolez le nom de la caméra dans la vidéo en direct.
- Si une caméra est déplacée après le calibrage, vous devez la recalibrer pour garantir des résultats d'analyse corrects.

Exécution d'un calibrage automatique

Le calibrage automatique vous permet de calibrer une ou plusieurs caméras en faisant traverser la scène de surveillance par une personne. La caméra collecte automatiquement les informations nécessaires à son calibrage.

Pour un calibrage automatique réussi :

- N'effectuez pas de calibrage lorsque de nombreuses personnes se trouvent dans le champ de vision.
- N'effectuez pas de calibrage lorsque de nombreux véhicules traversent le champ de vision.
- N'effectuez pas de calibrage lorsque d'autres objets se déplacent dans le champ de vision. Par exemple, des arbres ou des drapeaux dans le vent.
- Ne calibrez pas une caméra qui n'a pas été installée parallèlement au sol.
- La personne qui traverse la scène doit pouvoir couvrir l'ensemble du champ de vision de l'avant vers l'arrière. Si ce n'est pas possible, il est préférable de passer au calibrage manuel.
- Si la caméra se trouve sur un réseau distant, mais n'est pas connectée comme caméra distante, la personne qui traverse la scène doit marcher pendant environ 5 minutes pour qu'un nombre suffisant d'images soit capturé. En effet, la fréquence d'image des périphériques est généralement inférieure sur les réseaux distants.

1. Accédez à **Calibrage**.
2. Sélectionnez le ou les périphériques à calibrer.
3. Cliquez sur **Automatique**.
4. Définissez l'heure de début d'enregistrement. La capture doit commencer au moins 10 secondes avant que la personne qui traverse la scène entre dans le champ de vision.
5. Définissez la durée d'enregistrement. Tenez compte des points suivants :
   - La personne doit disposer de suffisamment de temps pour faire des allers-retours sur l'intégralité de la scène.
   - La durée de la vidéo influe sur le calcul du calibrage.
6. Entrez la taille (en cm) de la personne qui traverse la scène, puis cliquez sur **Capturer**.
   Pour réutiliser une vidéo précédemment capturée, cliquez sur **Utiliser la capture précédente**.
7. Laissez la personne traverser la scène conformément aux instructions suivantes :
   - Suivez une trajectoire en zigzag qui couvre autant que possible la zone de détection de l'avant à l'arrière de la scène. Nous recommandons d'opter pour une trajectoire en V dans le champ de vision.
   - Restez presque toujours entièrement visible dans le champ de vision.
   - Marchez lentement en ligne droite.
   - Gardez constamment une posture droite.
   - Arrêtez-vous 1 à 2 secondes 1 avant de changer de direction.

Exemple de séquence de marche.

8. Pour déterminer si le calibrage automatique a réussi, vérifiez si la personne est détectée avec précision. Cf. *Vérification de la qualité du calibrage , on page 21*.
9. Pour enregistrer le calibrage, cliquez sur **Accepter**.
   Pour effectuer un nouveau calibrage, cliquez sur **Nouveau**.
   Pour effectuer un calibrage manuel, cliquez sur **Manuel**.

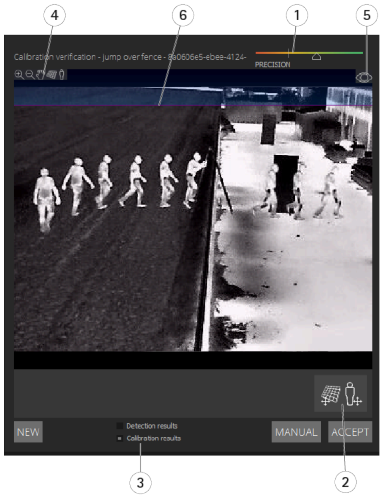
Lorsque vous avez accepté le calibrage, des bordures bleues indiquent la zone de détection maximale. La zone de détection maximale est la plus grande zone pouvant être surveillée. En dehors de cette zone, des intrus peuvent être détectés, mais sans aucune garantie.

Vérification de la qualité du calibrage

Après un calibrage, vous devriez voir la personne qui a traversé la scène à plusieurs positions. Si la personne n'est pas du tout visible, le calibrage automatique a échoué et doit être réexécuté.

Il existe plusieurs façons de vérifier la qualité du calibrage :

- Vérifiez l'indicateur de précision du calibrage. Il indique un niveau de précision calculé automatiquement qui détermine si la personne a bien couvert la scène et si elle a bien été détectée. Si l'indicateur de précision se situe dans la zone rouge, le calibrage a échoué et vous ne pouvez pas cliquer sur **Accepter**. Cf. *Calibrage manuel, on page 24*.
- Vous pouvez utiliser l'outil de grille. Cf. *Utilisation de la grille pour vérifier le calibrage, on page 22*.
- Vous pouvez utiliser l'outil d'avatar. Cf. *Utilisation de l'avatar pour vérifier le calibrage, on page 23*.
- Vous pouvez vérifier les résultats de la détection. Cf. *Utilisation des résultats de la détection pour vérifier le calibrage, on page 23*.



1 *Indicateur de précision du calibrage*
2 *Outils de grille et d'avatar*
3 *Vue dynamique ou statique*
4 *Modification de vue*
5 *Basculer entre l'image du calibrage et la vidéo en direct*
6 *Ligne d'horizon*

La ligne d'horizon représente l'extrémité visible du sol dans la scène. Lorsque vous définissez des scénarios, il n'est pas possible de placer des zones de scénario dans la zone bleue au-dessus de la ligne d'horizon, car cette zone se situe au-dessus du sol et les zones de scénario sont par définition au sol.

Utilisation de la grille pour vérifier le calibrage

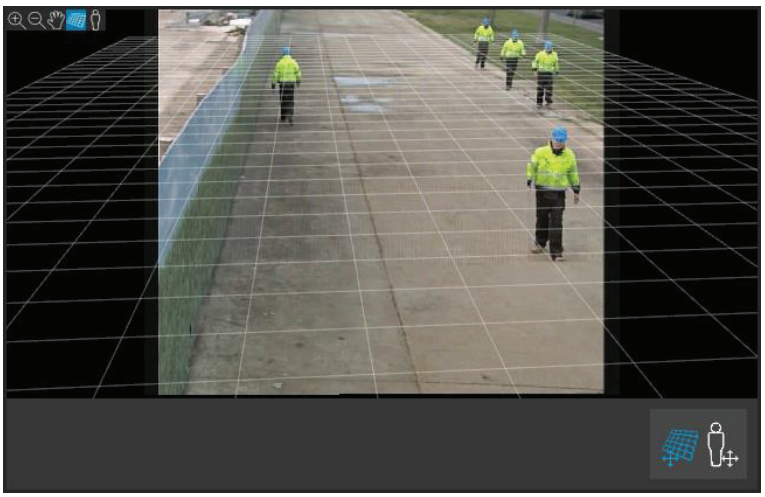
La grille doit correspondre à une grille carrée au sol. Pour basculer l'affichage de la grille, cliquez sur l'icône de modification de vue de la grille.

Important

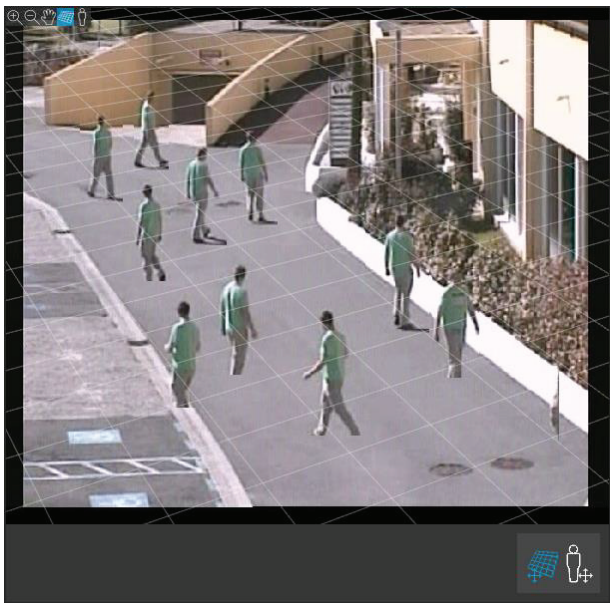
La grille n'affecte pas le calibrage. Il s'agit d'un outil qui permet de s'assurer que le calibrage est correct.

Pour tourner la grille, faites-la glisser dans le volet de prévisualisation. Essayez de l'aligner avec une structure de la scène pour déterminer si le résultat semble raisonnable.

Si la grille est parallèle au sol, ne présente pas de pente anormale et est parallèle à des artefacts créés par l'homme qui sont parallèles dans le monde réel après l'application de la rotation nécessaire à la grille, le calibrage est correct.



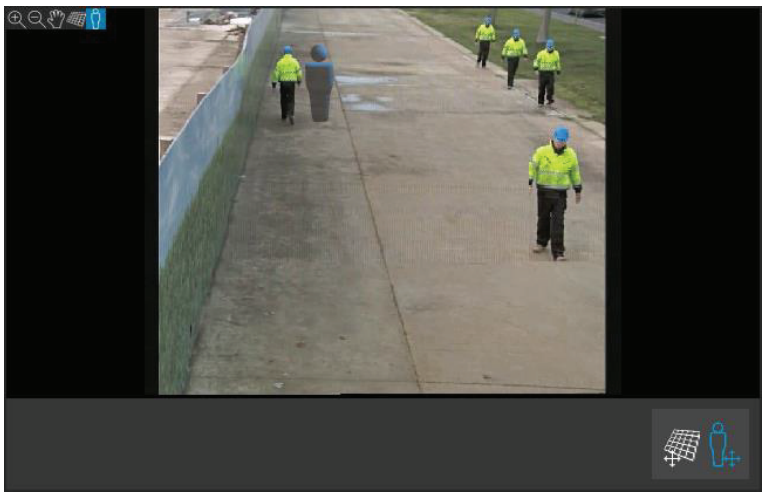
Exemple de grille correctement alignée avec les accotements de la route.



Exemple de grille mal alignée avec les accotements de la route.

Utilisation de l'avatar pour vérifier le calibrage

L'avatar vous permet de placer un avatar 3D de taille moyenne dans la scène. Pour basculer l'affichage de l'avatar, cliquez sur l'icône de modification de vue de l'avatar.



Sa taille dans le volet d'affichage correspond à la taille d'une personne moyenne à cette position, selon le calibrage actuel. En déplaçant l'avatar dans le volet, vous pouvez vous assurer que sa taille est raisonnable par rapport à d'autres objets ou personnes de la scène. Vérifiez l'avatar à différentes positions, car il peut être correctement dimensionné à une position, mais mal dimensionné ailleurs dans l'image.

Utilisation des résultats de la détection pour vérifier le calibrage

Vous pouvez utiliser les résultats de la détection pour vérifier comment fonctionnerait AXIS Perimeter Defender avec le calibrage actuel s'il recevait la vidéo d'une personne qui marche sous forme de flux en direct.

1. Passez des **résultats de calibrage** aux **résultats de détection**.
2. Vérifiez les détections des personnes ou des véhicules entrant sur la scène de surveillance :
   - Si le calibrage est correct, les personnes sont marquées d'un rectangle rouge et les véhicules d'un rectangle bleu.
   - Si le marquage des personnes ou des véhicules échoue fréquemment, cela signifie que le calibrage automatique a probablement échoué.

– Une zone rouge montre la zone limite de détection en fonction du calibrage calculé, c'est-à-dire la zone dans laquelle les conditions préalables sur la taille des personnes dans l'image ne sont pas respectées. Dans cette zone, la détection peut échouer en raison de la taille de la cible.

Remarque

- Si le calibrage calculé est incorrect, la zone rouge est également incorrecte.
- Si la personne est trop éloignée, elle peut ne pas être marquée. Une taille minimale est nécessaire pour que la détection fonctionne. Pour en savoir plus, consultez *Installation de la caméra, on page 13*.
- L'examen des résultats de la détection peut ne pas fonctionner sur des caméras connectées à distance, car la fréquence d'image de la capture est trop faible. Cela ne signifie pas que la configuration a échoué. Utilisez l'avatar et la grille pour vérifier le calibrage.

Calibrage manuel

Si vous n'avez pas tenté d'effectuer un calibrage automatique, vous devez capturer une courte vidéo et créer une image composite avant d'effectuer un calibrage manuel. Suivez les mêmes étapes que pour un calibrage automatique (*Exécution d'un calibrage automatique, on page 20*), mais sélectionnez **Manuel** au lieu d'**Automatique** dans l'onglet **Calibrage**. Pour créer l'image composite après avoir capturé une vidéo :

- Déplacez le curseur pour naviguer dans le clip vidéo.
- Aux positions clés, cliquez sur l'icône de caméra pour ajouter des images à l'image composite.

Assurez-vous que l'image composite reflète la section transversale complète de la scène : devant, derrière, à gauche et à droite.

Lorsque vous disposez d'une image composite créée manuellement ou automatiquement, vous pouvez poursuivre le calibrage manuel.

Le moteur de calibrage procède au calibrage en estimant les éléments suivants :

- Horizon
- Propagation (ou dispersion) des lignes verticales dans l'image
- Échelle de la scène

Lorsque vous effectuez un calibrage manuel, vous devez fournir ces informations au moteur de calibrage via les éléments de calibrage. Il existe trois types d'éléments de calibrage :

- Les **repères de personne** permettent de marquer la taille connue d'une personne moyenne à différentes positions dans la scène. Si vous avez déjà tenté un calibrage automatique, il est très probable que l'image affichée dans le volet de l'éditeur affiche plusieurs fois la même personne. Placez des repères de personne du sol vers le haut pour marquer la taille et la direction de la personne à une ou plusieurs positions. Un repère de personne doit démarrer au sol et être vertical dans le monde réel. La longueur d'un repère de personne dans le monde réel doit correspondre à la taille indiquée en regard du bouton **Personne** dans le volet de l'éditeur. Les repères de personne sont marqués d'un symbole bleu clair semi-transparent.
  Comment placer au mieux un repère de personne

– Nous vous recommandons de placer le repère sur une personne ayant les pieds joints.

– Si vous placez un repère sur une personne debout les pieds non joints, placez le point inférieur sur le sol à mi-distance entre les talons de la personne.

– Alignez le repère avec le torse de la personne. Cependant, si elle se penche dans une certaine direction, généralement en avant tout en marchant, essayez de compenser l'inclinaison en plaçant le repère plus verticalement. Utilisez tous les repères présents dans la scène pour vous aider, par exemple les arbres, les clôtures ou les lampadaires.

– Pour l'échelle de la scène, au moins un repère de personne avec la taille de la personne correspondante est nécessaire. Si aucune personne n'est visible dans la scène, vous pouvez ajouter un repère de personne sur un autre objet vertical de hauteur connue, par exemple, un poteau de clôture de 3 m, et définir la taille de la personne en fonction de la hauteur de l'objet.

- **Des lignes horizontales parallèles (lignes H)** sont utilisées pour marquer les lignes horizontales et parallèles connues dans la scène. Ces lignes peuvent se trouver au sol et/ou sur un mur, mais elles doivent toutes être parallèles. Si vous ajoutez des lignes horizontales parallèles, vous devez en ajouter au moins deux. Vous pouvez les placer sur les côtés ou les marques d'une route rectiligne, sur un ensemble de voies de chemin de fer rectilignes, sur une structure visible sur un mur ou sur la base et le sommet d'une rangée de poteaux de clôture. Les lignes H sont tracées en bleu clair.
- **Des lignes verticales (lignes V)** sont utilisées pour marquer les lignes verticales connues dans la scène. Une ligne V doit indiquer une structure verticale dans le monde réel. Il peut s'agir par exemple d'un poteau de clôture, du coin d'un bâtiment ou d'un panneau de signalisation. Une ligne V ne doit pas nécessairement commencer au sol. Les lignes V sont signalées en bleu foncé. Notez que les lignes V sont très sensibles, car une légère modification de l'orientation peut changer radicalement le calibrage. En règle générale, les lignes V doivent être inclinées sur la droite sur le côté droit de l'image et sur la gauche sur le côté gauche.

1 *Repères de personne*
2 *Lignes verticales (lignes V)*
3 *Lignes horizontales parallèles (lignes H)*
4 *Outils de grille et d'avatar*

Nombre d'éléments de calibrage

Lorsque vous ajoutez des repères de personne, des lignes H et des lignes V, il est généralement préférable d'en ajouter le plus possible. Le moteur de calibrage peut effectuer un calibrage avec seulement quelques lignes, mais généralement la qualité du calibrage s'améliore avec le nombre de lignes et de repères présents. Lorsque vous ajoutez des repères de personne, nous vous recommandons de les placer à la fois à proximité et à distance, à gauche et à droite.

Structures verticales dans l'image

Selon *Recommandations pour l'installation de la caméra, on page 14*, toutes les caméras doivent pointer légèrement vers le bas. En conséquence, toutes les structures verticales dans le monde réel semblent se disperser en queue de paon dans l'image. Cela signifie que tous les repères de personne et les lignes V doivent être inclinés vers le bord de l'image. Un repère sur la moitié droite de l'image doit être incliné vers la droite et repère sur la moitié gauche, vers la gauche. Au moins l'un des repères de personne ou l'une des lignes V placés doit être « correctement incliné » pour garantir le fonctionnement du calibrage.

L'indicateur de précision fournit un retour visuel sur le niveau et la qualité de détail ajoutés à la scène. Pour des calibrages manuels réussis, les balises doivent couvrir la scène de l'avant vers l'arrière et de gauche à droite. Ceci est indiqué par un indicateur de précision vert.

Qualité du calibrage

La qualité du calibrage peut être vérifiée avec les gestionnaires de grille ou d'avatar. Cf. *Vérification de la qualité du calibrage , on page 21*. Vous pouvez également cliquer sur **Examen**. Vous accédez ainsi au résultat de l'exécution d'AXIS Perimeter Defender sur la vidéo capturée à l'aide du calibrage manuel actuel.

Calibrage - PTZ Autotracking

Important

La qualité des résultats dépend de celle du calibrage. Suivez attentivement les directives et les instructions.

Remarque

Vous pouvez calibrer les deux caméras simultanément ou individuellement.

1. Sélectionnez la caméra fixe et la caméra PTZ.
2. Accédez à **Calibrage**, puis cliquez sur **Configurer la position de la caméra PTZ**. Une fenêtre contextuelle affichant la vue de la caméra fixe apparaît.
   La caméra PTZ applique les fonctions de panoramique, d'inclinaison et de zoom pendant un courant instant au démarrage de l'application.
3. Vérifiez que les vues des deux caméras sont alignées.
   Si ce n'est pas le cas, cliquez sur l'image de la vidéo en direct pour ajuster la vue de la caméra PTZ jusqu'à ce qu'elle corresponde à celle de la caméra fixe. Assurez-vous qu'il n'y a pas de roulement.
4. Cliquez sur **Configurer la position de la caméra PTZ**.
   Si le bouton n'est pas visible, déplacez la fenêtre contextuelle contenant la vue de la caméra fixe.
5. Cliquez sur **Automatique**.
6. Effectuez un calibrage automatique conformément aux instructions de la section *Exécution d'un calibrage automatique, on page 20*.
7. Utilisez l'avatar pour vérifier la qualité du calibrage de la caméra fixe. Cf. *Utilisation de l'avatar pour vérifier le calibrage, on page 23*.
   Si la qualité est satisfaisante, cliquez sur **Accepter**.
   Si elle est insuffisante, procédez à un calibrage manuel à l'aide de la vidéo du calibrage automatique. Cliquez sur **Manuel** et suivez les instructions de la section *Calibrage manuel, on page 24*.
8. Dans **Scénarios**, définissez les règles de déclenchement des alarmes. Cf. *Définition de scénarios, on page 26*.
9. Dans **Calibrage**, cliquez sur **Examen** dans la vidéo en direct de la caméra PTZ.
10. Utilisez l'avatar pour vérifier la qualité du calibrage de la caméra PTZ. Cf. *Utilisation de l'avatar pour vérifier le calibrage, on page 23*.
    Si la qualité est satisfaisante, cliquez sur **Accepter**.
    Si elle est insuffisante, procédez à un calibrage manuel à l'aide de la vidéo du calibrage automatique. Cliquez sur **Manuel** et suivez les instructions de la section *Calibrage manuel, on page 24*.
11. Appariez les caméras. Cf. *Appariement des caméras - PTZ Autotracking, on page 29*.

Définition de scénarios

Scénarios

AXIS Perimeter Defender inclut des scénarios de zone stériles courants que vous pouvez configurer pour sécuriser et contrôler des zones sensibles. Lors de l'étape d'étalonnage, la plage de détection maximale a été créée pour fournir un scénario par défaut de type intrusion/maraudage. Lors de cette étape, vous pouvez définir des scénarios de détection plus sophistiqués de trois types différents :

Remarque

Si vous utilisez AXIS Perimeter Defender 4.0, vous pouvez désormais configurer des scénarios sans l'application de bureau. Les modifications seront répercutées dans l'application de bureau. Pour en savoir plus, veuillez aller à *Interface web, on page 39*.

- Intrusion/maraudage. Veuillez consulter *Configuration du scénario de détection des intrusions/rôdeurs, on page 27*.

- Franchissement de zone. Veuillez consulter *Configuration du scénario de franchissement de zone, on page 28*.
- Scénario conditionnel. Cf. *Mise en place du scénario conditionnel, on page 28*

Si le symbole **!** apparaît en regard du nom d'un scénario, cela signifie que la configuration du scénario n'est pas terminée. Le plus souvent, il s'agit de sa zone de détection qui n'a pas encore été définie.

Paramètres globaux

Les paramètres globaux que vous définissez dans l'interface utilisateur s'appliquent à tous les scénarios.

Type de caméra – Pour les caméras visuelles, sélectionnez **Couleur – Jour/nuit**. Pour les caméras thermiques, le type de caméra thermique est automatiquement défini.

Remarque

- Des types d'approche supplémentaires peuvent augmenter le risque de fausses alarmes, par exemple causées par des animaux.
- Les types d'approche supplémentaires ne sont pas pris en charge pour les périphériques qui fonctionnent uniquement en mode IA.

Approche additionnelles – Sélectionnez les types que vous souhaitez inclure dans votre scénario de détection.

Environnement – Pour les périphériques dotés du mode IA, cochez **IA** pour activer ce mode. Vous pouvez utiliser **Headlights/vehicles in scene (Phares/véhicules dans la scène)** si la scène contient des véhicules, des phares ou des effets de phares tels que des reflets. Si vous utilisez ce paramètre, les performances peuvent parfois être réduites dans des conditions normales. Par défaut, tous les scénarios sont censés contenir des véhicules et, par conséquent, des phares. Vous pouvez utiliser **Insects/droplets on lens (Insectes/gouttelettes sur l'objectif)** pour ignorer les déclenchements dus aux gouttes de pluie ou aux insectes et réduire les fausses alarmes.

Sensibilité – Pour augmenter la sensibilité du système, déplacez le curseur vers la droite. Une sensibilité plus élevée réduit le risque de détections manquées, mais augmente le risque de fausses alarmes.

Filtrage par taille de cible – Pour les périphériques dotés du mode IA, vous pouvez filtrer les objets plus petits que la taille cible.

Paramètres temporels

Vous pouvez définir des paramètres de durée pour chaque scénario créé.

Temps minimum passé dans la zone – Définissez la durée que doit passer un objet dans une zone pour que celle-ci soit activée.

Zone étroite – Si la zone est étroite et peut être franchie en 1 à 2 secondes, il existe un risque d'alarmes manquées. Vous pouvez atténuer ce risque avec la fonction **Narrow zone (Zone étroite)**. Veuillez noter qu'elle ne peut pas être combinée avec **Min presence in zone (Présence minimale dans la zone)**.

Configuration du scénario de détection des intrusions/rôdeurs

Le scénario de détection des intrusions/rôdeurs est conçu pour déclencher une alarme lorsqu'un objet entre dans une certaine zone et y reste au-delà la durée prédéfinie.

Le scénario par défaut créé à l'étape de calibrage est de type détection des intrusions/rôdeurs et utilise la zone de détection maximale. Pour utiliser ce scénario en l'état, cliquez sur **Accepter** dans l'onglet **Scénarios**.

Pour modifier le scénario par défaut :

1. Accédez à **Scénarios > Scénarios avancés**.
2. Modifiez la zone de détection par défaut :
   – Pour déplacer des points existants dans la zone de détection, cliquez dessus et faites-les glisser à l'aide de la souris.

- Pour créer des points supplémentaires, cliquez sur l'un des segments existants et faites-le glisser avec la souris.

3. Sous **Détecter**, sélectionnez le type d'objet à détecter.
4. Sous **Paramètres de durée**, définissez le délai de détection des rôdeurs dans **Temps minimum passé dans la zone** si vous ne souhaitez pas qu'un objet déclenche une alarme dès son entrée dans la zone.
5. Si la zone est étroite et peut être franchie en 1 à 2 secondes et si vous souhaitez tout de même que les alarmes se déclenchent, sélectionnez **Narrow zone (Zone étroite)**. Ce paramètre ne peut pas être combiné avec **Min presence in zone (Présence minimale dans la zone)**. Pour en savoir plus, consultez *Paramètres temporels, on page 27*.
6. Pour charger les modifications apportées à la caméra et revenir à la vue principale, cliquez sur **Accepter**.

Configuration du scénario de franchissement de zone

Le scénario de franchissement de zone est conçu pour déclencher une alarme lorsqu'un objet traverse deux zones de détection dans un ordre donné.

Important

Le scénario de franchissement de zone comporte la limitation suivante : si l'objet qui déclenche le scénario cesse de se déplacer pendant quelques secondes dans la zone d'origine avant de passer à la zone finale, le scénario ne se déclenche pas.

Sous **Paramètres de durée**, vous pouvez définir une durée de présence minimale pour chacune des zones du scénario. Si T_A est la durée minimum dans la zone d'origine et T_B la durée dans la zone finale, une alarme ne se déclenche que si l'objet reste plus longtemps que T_A dans la zone d'origine et ensuite plus longtemps que T_B dans la zone finale.

1. Accédez à **Scénarios > Scénarios avancés**.
2. Cliquez sur **New** (nouveau), puis sélectionnez **Zone-crossing** (Franchissement de zone).
3. Créez deux zones de détection séparées d'au moins un mètre :
   - Pour créer une zone de détection, cliquez plusieurs fois dans l'image.
   - Pour terminer la zone, cliquez avec le bouton droit de la souris dans l'image.
4. Pour spécifier la direction de franchissement interdite, cliquez sur **Sélectionner l'origine**, puis cliquez sur l'une des zones.
5. Sous **Détecter**, sélectionnez le type d'objet à détecter.
6. Sous **Paramètres de durée**, définissez **Temps de présence minimal** pour au moins l'une des deux zones, si vous ne souhaitez pas activer une zone dès qu'un objet y pénètre.
7. Si la zone est étroite et peut être franchie en 1 à 2 secondes et si vous souhaitez tout de même que les alarmes se déclenchent, sélectionnez **Narrow zone (Zone étroite)**. Ce paramètre ne peut pas être combiné avec **Min presence in zone (Présence minimale dans la zone)**. Pour en savoir plus, consultez *Paramètres temporels, on page 27*.
8. Pour charger les modifications apportées à la caméra et revenir à la vue principale, cliquez sur **Accept** (Accepter).

Mise en place du scénario conditionnel

Le scénario conditionnel est conçu pour déclencher une alarme lorsqu'un objet entre dans une certaine zone sans en avoir traversé d'autres.

Sous **Paramètres de durée**, vous pouvez définir une durée de présence minimale pour chacune des zones du scénario. Si T_A est la durée minimum dans la zone autorisée et T_B la durée dans la zone d'intrusion, une alarme ne se déclenche que si l'objet :

- reste plus longtemps que T_B dans la zone d'intrusion sans être entré au préalable dans la zone autorisée.
- reste moins longtemps que T_A dans la zone autorisée, puis entre et reste plus longtemps que T_B dans la zone d'intrusion.

Aucune alarme ne se déclenche si l'objet :

- n'entre pas ou reste moins longtemps que T_B dans la zone d'intrusion.
- reste plus longtemps que T_A dans la zone autorisée, puis entre dans la zone d'intrusion (quelle que soit sa durée de séjour).

1. Accédez à **Scénarios > Scénarios avancés**.
2. Cliquez sur **Nouveau** et sélectionnez **Scénario conditionnel**.
3. Créez deux zones de détection ou plus séparées d'au moins un mètre :
   - Pour créer une zone de détection, cliquez plusieurs fois dans l'image.
   - Pour terminer la zone, cliquez avec le bouton droit de la souris dans l'image.
4. Pour spécifier la direction de passage autorisée, cliquez sur **Sélectionner une zone d'intrusion**, puis cliquez sur l'une des zones.
5. Sous **Détecter**, sélectionnez le type d'objet à détecter.
6. Sous **Paramètres de durée**, définissez **Temps de présence minimal** pour au moins l'une des deux zones, si vous ne souhaitez pas activer une zone dès qu'un objet y pénètre.
7. Si la zone est étroite et peut être franchie en 1 à 2 secondes et si vous souhaitez tout de même que les alarmes se déclenchent, sélectionnez **Narrow zone (Zone étroite)**. Ce paramètre ne peut pas être combiné avec **Min presence in zone (Présence minimale dans la zone)**. Pour en savoir plus, consultez *Paramètres temporels, on page 27*.
8. Pour charger les modifications apportées à la caméra et revenir à la vue principale, cliquez sur **Accept** (Accepter).

Appariement des caméras - PTZ Autotracking

Dans la configuration d'AXIS Perimeter Defender PTZ Autotracking, vous devez apparier la caméra fixe et la caméra PTZ pour vous assurer qu'un objet en mouvement sera suivi efficacement par la caméra PTZ.

Si vous avez effectué un calibrage automatique, vous pouvez effectuer les étapes décrites dans la section *Exécution d'un appariement automatique, on page 29* pour les deux caméras. Sinon, vous devez suivre les indications de la section *Exécution d'un appariement manuel, on page 30*.

Exécution d'un appariement automatique

Dans la vidéo d'appariement, les lignes rouges représentent la personne et le cadre orange représente l'image zoomée de la caméra PTZ.

1. Dans **Calibrage > Examen de l'appariement de la caméra PTZ**, vérifiez les vidéos d'appariement à partir des deux caméras :
   - Vérifiez que les lignes rouges dans les deux images sont alignées sur l'intégralité de la vidéo.
   - Vérifiez que les lignes rouges vont toujours des pieds à la tête de la personne.
   - Vérifiez que la personne est toujours centrée dans le cadre orange de la vidéo de la caméra PTZ.
2. Si les conditions de l'étape 1 sont respectées, sélectionnez **Examen de l'appariement interactif**.
   Si les conditions ne sont pas respectées, cliquez sur **Manuel** et suivez les étapes indiquées dans *Exécution d'un appariement manuel, on page 30*.
3. Déplacez le curseur pour naviguer dans le clip vidéo. Vérifiez que :
   - Les lignes bleues dans les deux images sont alignées sur l'intégralité de la vidéo.
   - La personne est toujours centrée dans le cadre orange de la vidéo de la caméra PTZ.
4. Si le cadre orange est absent de certaines scènes :
   4.1. Activez l'avatar dans l'image de la caméra fixe.
   4.2. Utilisez le curseur pour aller et venir dans la vidéo. Placez l'avatar sur la personne dans la vue de la caméra fixe et vérifiez que le point rouge se situe à ses pieds dans l'image de la caméra PTZ.

5. Si l'appariement automatique n'a pas ajouté de lignes bleues dans certaines scènes, cliquez sur **Manuel** et ajoutez manuellement les lignes rouges à la personne. Pour obtenir des instructions détaillées, voir *Exécution d'un appariement manuel, on page 30*.
6. Cliquez sur **Accepter**, puis sur **Quitter**.

Exécution d'un appariement manuel

Lorsque vous effectuez un appariement manuel, vous ajoutez des lignes rouges verticales des pieds à la tête de la personne qui a traversé la scène de surveillance lors de l'étape de calibrage. Vous devez ajouter des lignes sur l'intégralité de la vidéo afin de couvrir la totalité de la scène.

Si vous avez déjà effectué un appariement automatique, la vidéo contient déjà des lignes bleues.

Supprimez les lignes bleues et rouges qui :
- ne démarrent pas aux pieds de la personne ;
- ne rejoignent pas la tête de la personne ;
- n'ont pas de ligne correspondante dans l'image de la caméra PTZ.

Pour supprimer une ligne, cliquez dessus et appuyez sur Delete (Supprimer).

1. Déplacez le curseur pour naviguer vers une image du clip vidéo dans laquelle la personne est visible.
2. Ajoutez une ligne rouge à la personne dans l'image de la caméra fixe. Démarrez la ligne aux pieds de la personne. Un numéro d'ID est attribué à la ligne.
3. Ajoutez une ligne rouge correspondante au même objet dans l'image de la caméra PTZ. Vérifiez que le numéro d'ID correspond à celui de l'image de la caméra fixe.
4. Répétez les étapes 1 à 3 jusqu'à ce que vous ayez couvert l'intégralité de la scène.
   Lorsque le clip vidéo contient suffisamment de lignes pour un appariement valide :
   - le bouton **Accepter** devient actif ;
   - un cadre orange apparaît dans l'image de la caméra PTZ.
5. Vérifiez que la personne est toujours centrée dans le cadre orange. Si ce n'est pas le cas dans certaines scènes, ajoutez des lignes rouges.
6. Activez l'avatar dans l'image de la caméra fixe.
7. Déplacez le curseur pour naviguer dans le clip vidéo. Utilisez l'avatar pour vérifier que :
   - dans l'image de la caméra fixe, la taille de l'avatar correspond à la taille de la personne, dans différentes positions ;
   - dans l'image de la caméra PTZ, le point rouge se trouve au niveau des pieds de la personne ;
   - dans l'image de la caméra PTZ, la personne est toujours centrée dans le cadre orange.
8. Cliquez sur **Accept (Accepter)**. Si le bouton est inactif, vous devez d'abord ajouter des lignes rouges.
9. Cliquez sur **Quitter**.

Définition des sorties

Pour qu'AXIS Perimeter Defender déclenche des alarmes lorsqu'il détecte une intrusion, vous devez définir les règles appropriées. Le système peut envoyer des alarmes, par exemple, à un VMS.

AXIS Perimeter Defender peut envoyer des alarmes via différentes interfaces.

Depuis l'application :

- Notification d'alarme XML ou en texte clair sur TCP/IP
- Flux de métadonnées XML sur Multipart HTTP

Depuis le périphérique :

- Notifications de base en texte libre pour alarmes sur TCP/IP

- Sorties électriques (contacts secs ou humides)
- Notifications par e-mail
- Chargement FTP d'images d'alarme

Vous pouvez activer plusieurs interfaces simultanément.

Pour plus d'informations, voir *Sorties, on page 32*.

Pour définir des règles d'envoi d'alarmes à partir du périphérique :

1. Accédez à **Sorties**, puis cliquez sur **Configurer**. La page Web du périphérique s'ouvre dans un navigateur Web.
2. Créez une nouvelle règle d'action.
3. Dans la liste des déclencheurs, sélectionnez **Applications**, puis **AXISPerimeterDefender** et le scénario de déclenchement de l'action.

Remarque

Pour déclencher la même action pour tous les scénarios définis, sélectionnez **ALL_SCENARIOS**.

4. Dans la liste des actions, sélectionnez l'action à effectuer lorsque la condition est respectée.
5. Cliquez sur **OK**.

Pour plus d'informations sur la création de règles d'action, consultez le manuel d'utilisation du périphérique.

Configuration avancée

Sorties

Notifications d'alarme XML/texte

Cette interface permet à un destinataire TCP/IP de recevoir un message texte ou XML plus complet et descriptif pour chaque alarme. Par rapport à l'interface en texte libre, l'interface XML/texte offre les avantages suivants :

- Une notification est envoyée au début et à la fin de l'alarme et toutes les 10 secondes pendant l'alarme.
- Horodatage : Les notifications de début et de fin d'alarme contiennent un horodatage synchronisé à l'horloge de la caméra qui indique la date et l'heure exactes des événements.
- Type d'alarme : AXIS Perimeter Defender prend en charge plusieurs types d'alarme. Voir *Définition de scénarios, on page 26*. Les notifications XML/texte contiennent les informations relatives au type d'alarme déclenché. Attention : Le scénario de « franchissement de zone » est de type « passage », tandis que le scénario de « détection des rôdeurs » est de type « presence ».
- Zones concernées par la génération de l'alarme. Lorsque chaque scénario AXIS Perimeter Defender est associé à une ou plusieurs zones, les notifications XML/texte incluent la zone associée à l'alarme (par exemple, pour une alarme d'intrusion, la zone d'intrusion dans laquelle une personne a été détectée).

Par rapport à l'interface en texte libre, l'interface XML/texte présente les limites suivantes :

- Le texte du message est fixe et il n'existe pas de champs de texte libre.
- Chaque caméra ne prend en charge qu'un destinataire à la fois.

Le destinataire des notifications XML/texte reçoit quatre types de messages :

- AXIS Perimeter Defender envoie un message CONNECTION_TEST lorsque la notification XML est configurée pour vérifier que la communication avec le destinataire fonctionne comme prévu.
- Lorsqu'AXIS Perimeter Defender déclenche une alarme, il envoie un message ALARM_START.
- Pendant la durée de l'alarme, AXIS Perimeter Defender envoie un message « ALARM_IN_PROGRESS » toutes les 10 secondes. Tous ces messages ont la même balise GUID, identique à celle du message ALARM_START et des messages ALARM_STOP se rapportant à la même alarme.
- À la fin de l'alarme, AXIS Perimeter Defender envoie une alarme ALARM_STOP.

Pour obtenir une explication de ces messages aux formats XML et texte, voir *Exemples de format XML et texte, on page 32*.

Exemples de format XML et texte

Le format XML est le format par défaut pour les notifications TCP/IP. Néanmoins, si la taille de la notification est importante, un format texte générant des messages plus courts peut être utilisé. Pour sélectionner le format texte, sélectionnez l'option **Ne pas utiliser le format XML pour le paramètre d'alarmes** dans la page de configuration d'AXIS Perimeter Defender.

Exemple:
Par exemple, un message CONNECTION_TEST au format XML se présente comme suit :

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"          xmlns:xsd="http://www.w3.org/2001/XMLSchema"          VERSION=
"5.0.0"         ID="1"          TYPE="CONNECTION_TEST"          SENDER_IP=
"192.168.1.40"          SENDER_PORT="0">   <REFERENTIAL>45</REFERENTIAL></KEENEO_MESSAGE>
```

- VERSION est la version interne de la syntaxe et du protocole XML.
- ID est une identité numérique du message. Les ID ne sont pas nécessairement uniques ou consécutifs.
- TYPE est le type de message, ici « CONNECTION_TEST ». Le type de message détermine les sous-étiquettes du message (aucune pour les messages de type « CONNECTION_TEST »).
- SENDER_IP est l'adresse IP de la caméra Axis qui envoie la notification XML.

- SENDER_PORT est toujours défini sur 0 ; la caméra ne peut pas recevoir de messages entrants.
- REFERENTIAL est l'ID numérique associé à la caméra

Si le format texte est choisi, les messages de notification contiennent 7 champs chacun, séparés par le caractère de barre verticale « | ». Si un champ ne peut pas être spécifié (par exemple, il n'a pas de sens pour ce type de message), il est remplacé par « - ».

Les sept champs sont les suivants, dans l'ordre indiqué (entre parenthèses, le champ XML correspondant lorsque le format XML est sélectionné) :

1. ID numérique du message (attribut « ID » de l'en-tête XML « KEENEO_MESSAGE »).
2. Adresse IPv4 de la caméra (attribut « SENDER_IP » attribut de l'en-tête XML « KEENEO_MESSAGE »).
3. Numéro de référentiel associé à l'instance d'AXIS Perimeter Defender (balise « REFERENTIAL »).
4. Type de message (attribut « TYPE » de l'en-tête XML « KEENEO_MESSAGE »).
5. Type d'alarme (balise « TYPE »).
6. Nom du scénario qui a déclenché l'alarme (balise « SCENARIO_NAME »).
7. Horodatage (balise « TIMESTAMP »). Le format d'horodatage est le même que pour le format XML.

Le message CONNECTION_TEST précédent au format TEXT est le suivant :

```
1|192.168.1.40|45|CONNECTION_TEST|-|-|-
```

Exemple:
Un message ALARM_START au format XML se présente comme suit :

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"         xmlns:xsd="http://www.w3.org/2001/XMLSchema"         VERSION=
"5.0.0"         ID="9999"         TYPE="ALARM_START"         SENDER_IP=
"192.168.1.40"         SENDER_PORT="0">  <REFERENTIAL>0</REFERENTIAL>  <TYPE>INTRUSION</
TYPE>  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>  <EXTRA_DATA>zone=testzone</EXTRA_
DATA>  <TIMESTAMP>2014-03-01T21:24:12.114</TIMESTAMP>  <GUID>77acddf9-e0d4-402e-a497-
231aeee22788</GUID></KEENEO_MESSAGE>
```

- L'en-tête est le même que pour le message « CONNECTION_TEST ».
- Il s'agit d'un type de message « ALARM_START » possédant un ensemble de sous-balises.

– REFERENTIAL est l'ID numérique associé à la caméra.

– TYPE est le type d'alarme déclenchée par AXIS Perimeter Defender (dans cet exemple, « INTRUSION »). Les autres types possibles sont « PRESENCE », « PASSAGE » et « CONDITIONAL ».

– SCENARIO_NAME est le nom du scénario qui a déclenché l'alarme, tel que défini dans l'interface de configuration. Cf. *Configuration du scénario de détection des intrusions/rôdeurs, on page 27*

– EXTRA_DATA porte le nom de la zone (ou la liste des noms de zone) impliqué dans l'alarme, comme la zone d'intrusion.

– TIMESTAMP est la date et l'heure du démarrage de l'alarme, au format AAAA-MM-JJTHH:mm:sss.zzz, où :
  – AAAA est l'année en quatre chiffres (par exemple, 2014).
  – MM est le numéro du mois en 2 chiffres (par exemple, 01 pour janvier).
  – JJ est le numéro du jour en 2 chiffres (par exemple, 03 pour le 3).
  – T est une lettre fixe.
  – HH est l'heure au format 24 heures, de 00 à 23
  – mm correspond aux minutes en 2 chiffres, de 00 à 59
  – ss correspond aux secondes en 2 chiffres, de 00 à 59
  – zzz correspond aux millisecondes en 3 chiffres, de 000 à 999.
  AXIS Perimeter Defender utilise la date et l'heure internes de la caméra pour générer l'horodatage d'alarme. Il est donc important de synchroniser la caméra avec une horloge externe.

– GUID est un identifiant unique constant pour tous les messages liés à la même alarme (ALARM_START, ALARM_IN_PROGRESS et ALARM_STOP).

Voici l'équivalent du message ALARM_START au format texte :

```
9999|192.168.1.40|0|ALARM_START|INTRUSION|Intrusion-0|2014-03-01T21:24:12.114
```

Exemple:
Un message ALARM_IN_PROGRESS au format XML se présente comme suit :

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"          xmlns:xsd="http://www.w3.org/2001/XMLSchema"          VERSION=
"5.0.0"          ID="9999"          TYPE="ALARM_IN_PROGRESS"          SENDER_IP=
"192.168.1.40"          SENDER_PORT="0">   <REFERENTIAL>0</REFERENTIAL>   <TYPE>INTRUSION</
TYPE>   <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>   <GUID>77acddf9-e0d4-402e-a497-
231aeee22788</GUID></KEENEO_MESSAGE>
```

- L'en-tête est le même que pour les messages « CONNECTION_TEST » et « ALARM_START ».
- Il s'agit d'un type de message « ALARM_IN_PROGRESS » possédant un ensemble de sous-balises.

– REFERENTIAL est l'ID numérique associé à la caméra.

– TYPE est le type d'alarme déclenchée par AXIS Perimeter Defender. Il est identique à celui du message ALARM_START correspondant.

– SCENARIO_NAME est le nom du scénario qui a déclenché l'alarme. Il est identique à celui du message ALARM_START correspondant.

– Le GUID est le même que pour le message ALARM_START correspondant.

Message ALARM_IN_PROGRESS correspondant au format texte :

```
9999|192.168.1.40|0|ALARM_IN_PROGRESS|INTRUSION|Intrusion-0|-
```

Exemple:
Un message ALARM_STOP au format XML se présente comme suit :

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"          xmlns:xsd="http://www.w3.org/2001/XMLSchema"          VERSION=
"5.0.0"          ID="9999"          TYPE="ALARM_STOP"          SENDER_IP=
"192.168.1.40"          SENDER_PORT="0">   <REFERENTIAL>0</REFERENTIAL>   <TYPE>INTRUSION</
TYPE>   <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>   <EXTRA_DATA>zone=testzone</EXTRA_
DATA>   <TIMESTAMP>2014-03-01T21:24:26.304</TIMESTAMP>   <GUID>77acddf9-e0d4-402e-a497-
231aeee22788</GUID></KEENEO_MESSAGE>
```

- L'en-tête est le même que pour les messages précédents.
- Il s'agit d'un type de message « ALARM_STOP » possédant le même ensemble de sous-types que le message ALARM_START.

Message ALARM_IN_PROGRESS correspondant au format texte :

```
9999|192.168.1.40|0|ALARM_STOP|INTRUSION|Intrusion-0|2014-03-01T21:24:26.304
```

La connexion TCP/IP est toujours fermée après chaque message. Par conséquent, le destinataire doit toujours conserver la prise d'écoute ouverte pour recevoir d'autres notifications.

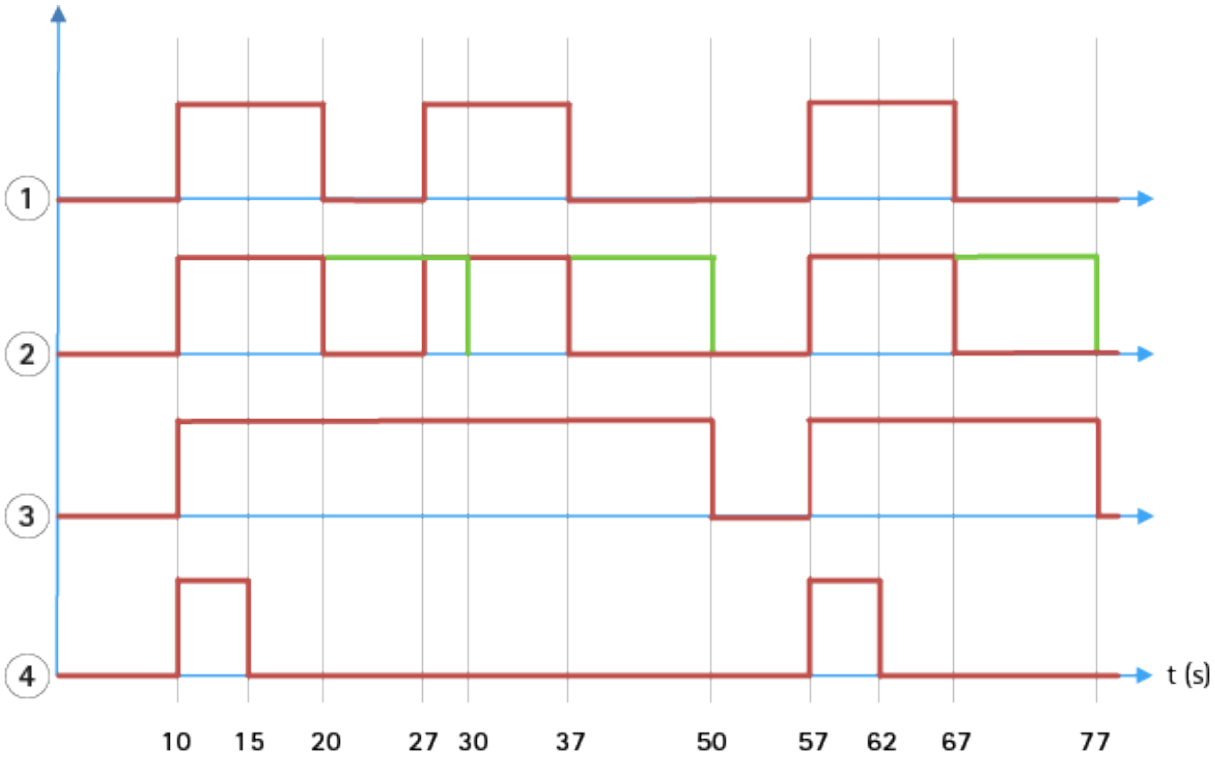
Erreurs de communication

Si le destinataire distant des notifications XML n'est pas joignable, par exemple en raison d'une déconnexion du réseau, AXIS Perimeter Defender commence à mettre en mémoire tampon les alarmes non envoyées en interne et essaie de les renvoyer régulièrement (au moins toutes les 10 secondes). Après un nombre consécutif d'échecs de l'envoi de nouveaux messages (l'échec de la nouvelle tentative d'envoi d'un message à partir de la mémoire tampon n'est pas pris en compte), AXIS Perimeter Defender déclare le destinataire comme « définitivement hors ligne » et interrompt l'envoi de notifications XML au destinataire. Le nombre d'échecs consécutifs est fixé à 20, ce qui correspond environ à 4 ou 5 alarmes d'intrusion d'une durée moyenne de 40 secondes chacune.
AXIS Perimeter Defender commence à renvoyer des notifications à ce destinataire si l'un des événements suivants se produit :

- AXIS Perimeter Defender est redémarré.
- La même valeur du paramètre « URL de diffusion des alarmes » est à nouveau enregistrée.

Maintien d'alarme

AXIS Perimeter Defender utilise la notion de « durée post-alarme ». Celle-ci se définit comme l'intervalle de temps après l'arrêt d'une alarme au cours duquel si une autre alarme est déclenchée, les deux alarmes sont fusionnées en une alarme unique.



1 Trois alarmes déclenchées par AXIS Perimeter Defender à 10, 27 et 57. Chaque alarme présente une durée de 10 secondes (l'intrus a mis 10 secondes pour traverser la zone d'intrusion).
2 Une durée post-alarme de 10 secondes est ajoutée.
3 Alarmes utilisant des notifications XML et des métadonnées XML.
4 Alarmes utilisant des notifications par e-mail, le chargement FTP d'images, des contacts électriques et des notifications TCP/IP de base.

(2) Une durée post-alarme de 10 secondes (en vert) augmente la durée de chaque alarme et aboutit à la fusion de deux alarmes séparées de 10 secondes maximum.

(3) Vous pouvez voir le nombre d'alarmes et leur durée, telles qu'elles ont été déclenchées par AXIS Perimeter Defender via des notifications XML et des métadonnées XML. La durée post-alarme peut être utilisée pour obtenir des alarmes plus longues mais moins nombreuses, au lieu d'alarmes plus courtes et consécutives.

(4) Pour les notifications par e-mail, le chargement FTP d'images, les contacts électriques et les notifications de base TCP/IP, le résultat de l'utilisation d'une durée post-alarme de 10 secondes est différent. Ces notifications tiennent compte du démarrage de l'alarme mais pas de l'arrêt. Il n'y a donc aucune notion de « durée d'alarme » lorsque vous utilisez ces notifications. Par conséquent, la durée post-alarme ne modifie pas la durée de la notification elle-même. Elle est toujours fixée à la valeur choisie par l'utilisateur lors de la configuration de la notification. Ainsi, lorsque les alarmes consécutives sont fusionnées en raison de la durée post-alarme, une seule notification est envoyée. Vous pouvez voir qu'AXIS Perimeter Defender fusionne les deux premières alarmes pour n'envoyer ensuite qu'une seule notification. Par conséquent, les notifications par e-mail, le téléchargement FTP d'images, les contacts électriques et les notifications TCP/IP de base s'appliquent uniquement à ces deux alarmes. Le graphique présente une durée fixe de 5 secondes pour ces notifications.

Configuration de la durée post-alarme

1. Ouvrez AXIS Perimeter Defender Setup.

2. Accédez à **Sorties**.
3. Modifiez le paramètre **Durée post-alarme**. La valeur par défaut est de 7 secondes.
4. Cliquez sur **Assigner**.

Métadonnées

Incrustation de métadonnées

L'incrustation de métadonnées gravées est une fonctionnalité qui permet d'effectuer des détections d'analyse à partir de flux en direct sélectionnés, et ce depuis la caméra. Les détections sont des incrustations graphiques qui se présentent sous la forme de cadres et de lignes de trajectoire. Les flux sont sélectionnés en fonction de leur résolution et d'une zone de visualisation si le périphérique prend en charge les zones de visualisation. Les métadonnées gravées s'affichent à la fois dans la vidéo en direct et pendant la relecture d'un enregistrement.

Incrustations de métadonnées gravées sur des flux sélectionnés

Par exemple, vous pouvez configurer l'application pour qu'elle ajoute des incrustations sur tous les flux ayant une résolution de 640x480. Dans ce cas, seuls les flux de cette résolution comporteront des incrustations, les autres ne seront pas modifiés.

Incrustations de métadonnées gravées sur des zones de visualisation sélectionnées

Lorsque cette fonction est prise en charge, vous pouvez également indiquer une zone de visualisation avec la résolution. Par exemple, vous pouvez choisir d'afficher des incrustations sur les flux provenant de la zone de visualisation n°3 à la résolution 1280x720. Dans ce cas, seuls les flux correspondant à cette configuration comporteront des incrustations, tandis que les autres flux resteront inchangés, y compris ceux provenant de la zone de visualisation n°3 mais dont la résolution est différente et ceux de résolution 1280x720 mais qui ne proviennent pas de la zone de visualisation n°3.

Ajout de métadonnées gravées au flux vidéo

Remarque

Cette fonction n'est disponible que sur les dispositifs dotés du logiciel version 7.30 ou ultérieure.

Cet exemple explique comment activer les incrustations de métadonnées sur tous les flux vidéo d'une résolution de 640x480. Les flux vidéo d'une autre résolution ne sont pas affectés.

1. Sélectionnez la caméra dans le volet contenant les vidéos en direct.
2. Accédez à **Sorties > Incrustation de métadonnées gravées**.
3. Sélectionnez **Activé**.
4. Dans la liste déroulante, sélectionnez la résolution 640 x 480.
5. Cliquez sur **Appliquer**.
6. Assurez-vous que les métadonnées s'affichent dans la vidéo en direct pour cette résolution.

L'intégration aux logiciels VMS

AXIS Perimeter Defender s'intègre parfaitement aux systèmes de gestion vidéo (VMS) suivants :

- Security Center de Genetec™
- XProtect® de Milestone

Pour des informations sur les versions de VMS prises en charge, veuillez consulter *axis.com/products/axis-perimeter-defender/support-and-documentation*.

Les alarmes déclenchées par AXIS Perimeter Defender sont automatiquement converties en événements dans le VMS, ce qui permet de déclencher un large éventail d'actions et d'exploiter toute la puissance du VMS. Simultanément, les métadonnées en direct générées par AXIS Perimeter Defender sont envoyées au VMS pour être affichées en direct et enregistrées. Par conséquent, les métadonnées sont également disponibles lors de la lecture des séquences vidéo enregistrées en mode relecture.

Un système automatisé de détection des intrusions est conçu pour déclencher des alarmes et fournir des informations permettant de faciliter l'intervention de sécurité. Cela peut inclure l'envoi d'une invite à un périphérique mobile ou l'affichage de l'événement d'alarme dans un VMS, peut-être avec le sujet à l'origine de l'événement d'alarme mis en évidence à l'écran.

Intégration d'un événement standard

AXIS Perimeter Defender capitalise sur les interfaces et capacités natives d'ACAP pour envoyer des alarmes et des informations supplémentaires à des dispositifs externes ou à des VMS. Les événements envoyés par AXIS Perimeter Defender peuvent être traduits en messages au VMS, en leur associant des règles d'action.

Les canaux d'alarme suivants entre la caméra et le VMS sont disponibles :

- Notifications de base en texte libre pour alarmes (TCP/IP)
- Sorties électriques (contacts secs ou humides)
- Notifications par e-mail
- Chargement FTP d'images d'alarme

Ces intégrations peuvent être configurées sur la caméra. Cf. *Maintien d'alarme, on page 35*.

Ponts VMS

Pour les systèmes de gestion vidéo suivants, nous fournissons des modules d'intégration pré-développés, appelés « ponts » :

- Milestone XProtect® 2014 et 2016 Corporate/Expert/Enterprise/Professional/Express. Les éditions Enterprise/Professional/Express ne prennent pas en charge les métadonnées (pas d'affichage en direct ou en relecture des métadonnées).
- Genetec™ Service Center 5.3 et 5.4 Pro/Enterprise/SV32/SV16

Les ponts offrent deux possibilités d'intégration :

- Création dans le VMS d'événements d'alarme personnalisés correspondant aux événements générés par AXIS Perimeter Defender.
- Affichage d'incrustations d'alarme ou de cadres, par-dessus des vidéos en direct et enregistrées (à l'exception de Milestone XProtect® Enterprise/Professional/Express).

Vous devez télécharger et installer les ponts VMS en tant qu'applications distinctes. Pour plus d'informations sur l'installation et la configuration d'un pont, consultez le manuel d'utilisation du pont en question.

Créer une règle dans AXIS Camera Station

Cette section explique comment intégrer AXIS Perimeter Defender à un système d'événement d'AXIS Camera Station. Vous apprendrez à effectuer les tâches suivantes :

- Configurer une règle AXIS Camera Station à déclencher en cas d'intrusion.
- Vérifier que la configuration est correcte.

1. Configurer et calibrer AXIS Perimeter Defender dans le logiciel de configuration AXIS Perimeter Defender. Pour obtenir de l'aide pour l'installation et le calibrage d'AXIS Perimeter Defender, reportez-vous au manuel d'utilisation d'AXIS Perimeter Defender ou à la *page du produit*.
2. Suivez les instructions de l'assistant d'**ajout de caméra** pour ajouter la caméra à AXIS Camera Station.
3. Configurez un déclencheur d'évènement de périphérique :
   3.1. Accédez à **Configuration** > **Enregistrements et événements** et ouvrez l'onglet **Règles avancées**.
   3.2. Créez une nouvelle règle et sélectionnez le déclencheur **Événement sur périphérique**.
   3.3. Sélectionnez la caméra sur laquelle AXIS Perimeter Defender est installé.

3.4. Dans la liste **Événement**, sélectionnez **AXISPerimeterDefender**.

3.5. Dans la liste **Fonction**, sélectionnez le nom de l'intrusion configurée (dans ce cas, « Intrusion-1 »). Si vous souhaitez déclencher la règle pour tous les scénarios configurés, sélectionnez **ALL_SCENARIOS**.

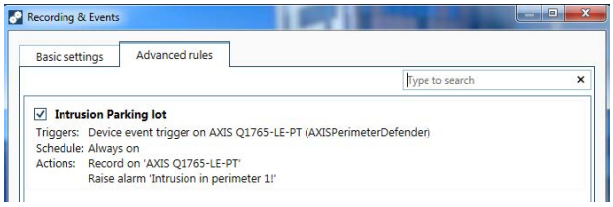
3.6. Sélectionnez **Oui** si le déclencheur doit être activé en cas d'intrusion. Lorsqu'une intrusion est détectée, la fenêtre Activité indique un changement d'état qui permet de vérifier si la configuration est correcte.

3.7. Cliquez sur **OK** et sur **Suivant** pour configurer les actions.

3.8. Dans la boîte de dialogue **Ajouter action**, vous pouvez ajouter une ou plusieurs actions pour la règle.

Dans cet exemple, nous ajoutons une action d'enregistrement et une action d'alarme.

3.9. Cliquez sur **Finish** (Terminer).



L'exemple présente une règle qui déclenche deux actions en cas d'intrusion.

4. Vérifiez que votre configuration est correcte en simulant une intrusion, par exemple, en pénétrant physiquement dans la zone surveillée.

Interface web

À partir de la version 4.0 d'AXIS Perimeter Defender, vous pouvez désormais accéder à une interface web qui vous permet de configurer des scénarios sans installer l'application de bureau.

Pour accéder à l'interface web :

- Ouvrez un navigateur web.
- Saisir l'adresse IP du dispositif
- Aller à Apps (Applications)
- Veuillez aller à **AXIS Perimeter Defender** dans la liste, puis cliquer sur **Open (Ouvrir)**.

Remarque

La fonction de calibrage n'est pas encore disponible dans l'interface web. Pour calibrer la caméra, veuillez utiliser l'application de bureau. Pour en savoir plus, veuillez aller à *Calibrage - AXIS Perimeter Defender, on page 19*.

Scénarios

Créer un scénario d'intrusion

Le scénario d'intrusion est conçu pour déclencher une alarme lorsqu'un objet entre dans une zone définie et y reste au-delà la durée définie.

Pour créer un scénario d'intrusion :

1. Veuillez aller à **Scenarios (Scénarios)** dans l'interface web.
2. Veuillez cliquer sur **+ Create (+ Créer)**.
3. Veuillez sélectionner **Intrusion**.
4. Veuillez cliquer sur **Select this template (Sélectionner ce modèle)**.
5. Définir un nom descriptif personnalisé pour le scénario
6. Veuillez sélectionner le type d'objets qui doivent déclencher une alarme.
7. Pour redessiner la zone de détection des défauts, veuillez faire glisser les points d'ancrage dans n'importe quelle direction. Une fois qu'un point d'ancrage a été déplacé, de nouveaux points d'ancrage seront créés pour permettre de personnaliser davantage la forme.
8. Si vous ne voulez pas qu'un objet déclenche une alarme dès qu'il entre dans la zone, veuillez définir, sous la **zone d'intrusion**, la **présence minimale dans la zone**.
9. Si la zone est étroite et peut être franchie en 1 à 2 secondes et si vous souhaitez tout de même que les alarmes se déclenchent, sélectionnez **Narrow zone (Zone étroite)**. Pour en savoir plus, consultez *Paramètres temporels, on page 27*.
10. Cliquez sur **Save (Enregistrer)**.

Créer un scénario de franchissement de zone

Le scénario de franchissement de zone est conçu pour déclencher un alarme lorsqu'un objet passe d'une zone prédéfinie à une zone restreinte.

Pour créer un scénario de franchissement de zone :

1. Veuillez aller à **Scenarios (Scénarios)** dans l'interface web.
2. Veuillez cliquer sur **+ Create (+ Créer)**.
3. Veuillez sélectionner **Zone crossing (Franchissement de zone)**.
4. Veuillez cliquer sur **Select this template (Sélectionner ce modèle)**.
5. Définir un nom descriptif personnalisé pour le scénario

6. Veuillez sélectionner le type d'objets qui doivent déclencher une alarme.
7. Pour redessiner les zones de défaut, veuillez faire glisser les points d'ancrage dans n'importe quelle direction. Une fois qu'un point d'ancrage a été déplacé, de nouveaux points d'ancrage seront créés pour permettre de personnaliser davantage la forme.
8. Si vous ne voulez pas qu'un objet déclenche une alarme dès qu'il entre dans la zone, veuillez définir, sous la **zone 1**, la **présence minimale dans la zone**.
9. Si la zone est étroite et peut être franchie en 1 à 2 secondes et si vous souhaitez tout de même que les alarmes se déclenchent, sélectionnez **Narrow zone (Zone étroite)**. Pour en savoir plus, consultez *Paramètres temporels, on page 27*.
10. Pour choisir la zone à restreindre, veuillez cliquer sur la flèche de direction située à côté de **Restricted zone entry (Entrée dans la zone restreinte)**. Par défaut, la **zone 2** est la zone restreinte.
11. Veuillez définir les paramètres de la **zone 2**.
12. Cliquez sur **Save (Enregistrer)**.

Créer un scénario conditionnel

Le scénario conditionnel vous permet de définir librement les conditions de déclenchement des alarmes dans une scène.

Pour créer un scénario conditionnel :

1. Veuillez aller à **Scenarios (Scénarios)** dans l'interface web.
2. Veuillez cliquer sur **+ Create (+ Créer)**.
3. Veuillez sélectionner **Conditional (Conditionnel)**.
4. Veuillez cliquer sur **Select this template (Sélectionner ce modèle)**.
5. Définir un nom descriptif personnalisé pour le scénario
6. Veuillez sélectionner le type d'objets qui doivent déclencher une alarme.
7. Si vous avez besoin de plus de zones que les zones de défaut, veuillez cliquer sur **+ Add zone (+ Ajouter une zone)**.
8. Veuillez choisir la zone d'intrusion dans le menu déroulant situé sous **Intrusion Zone (Zone d'intrusion)**. Les flèches indiquent la position des différentes zones par rapport à la zone d'intrusion choisie.
9. Pour redessiner les zones de défaut, veuillez faire glisser les points d'ancrage dans n'importe quelle direction. Une fois qu'un point d'ancrage a été déplacé, de nouveaux points d'ancrage seront créés pour permettre de personnaliser davantage la forme.
10. Si vous ne voulez pas qu'un objet déclenche une alarme dès qu'il entre dans la zone, veuillez définir la **présence minimale dans la zone**.
11. Si la zone est étroite et peut être franchie en 1 à 2 secondes et si vous souhaitez tout de même que les alarmes se déclenchent, sélectionnez **Narrow zone (Zone étroite)**. Pour en savoir plus, consultez *Paramètres temporels, on page 27*.
12. Cliquez sur **Save (Enregistrer)**.

Modifier des scénarios

Pour modifier un scénario que vous avez créé dans l'interface web ou dans l'application de bureau :

1. Veuillez aller à **Scenarios (Scénarios)** dans l'interface web.
2. Veuillez cliquer sur **Edit (Modifier)** pour le scénario que vous souhaitez modifier.
3. Veuillez cliquer sur **Save (Sauvegarder)** une fois que vous avez terminé.

Renommer des scénarios

Pour changer le nom de plusieurs scénarios à la fois :

1. Veuillez sélectionnez les scénarios que vous souhaitez renommer.
2. Veuillez cliquer sur **Rename (Renommer)**, désormais disponible dans le menu.
3. Veuillez changer les noms à votre guise.
4. Cliquez sur **Save (Enregistrer)**.

Supprimer des scénarios

Pour supprimer plusieurs scénarios à la fois :

1. Veuillez sélectionnez les scénarios que vous souhaitez supprimer.
2. Veuillez cliquer sur **Delete (Supprimer)**, désormais disponible dans le menu.
3. Pour confirmer, veuillez cliquer sur **Delete (Supprimer)**).

Paramètres

L'interface web intègre un panneau d'aide intégrée contenant des informations sur les différents paramètres de chaque page. Veuillez cliquer sur l'icône d'aide (?) pour accéder au panneau.

Recherche de panne

Pour que toutes les fonctionnalités soient opérationnelles, vous devez impérativement configurer les paramètres Axis suivants :

- Réseau / TCP-IP / Routeur de base/par défaut
- Réseau / TCP-IP / Avancé / Nom de domaine
- Réseau / TCP-IP / Serveur DNS principal
- Réseau / TCP-IP / Serveur DNS secondaire
- Réseau / TCP-IP / Adresse du serveur NTP
- Réseau / TCP-IP / SMTP (e-mail)
- Options système / Date et heure / Fuseau horaire
- Options système / Date et heure / Synchronisation avec le serveur NTP

Mise à jour vers la dernière version

Pour profiter des dernières améliorations sans devoir recalibrer le système et redéfinir les scénarios, nous vous recommandons d'effectuer la mise à niveau vers la dernière version d'AXIS Perimeter Defender.

1. Téléchargez et installez la dernière version d'AXIS Perimeter Defender.
2. Cliquez sur **Installer**. AXIS Perimeter Defender Setup effectue automatiquement les étapes nécessaires pour terminer l'installation :

– Sauvegarde du calibrage, des scénarios, des paramètres et de la licence existants.

– Installation de la nouvelle version.

– Restauration de la licence.

– Restauration du calibrage et des scénarios.

– Restauration des paramètres.

– Redémarrage des applications qui étaient en cours d'exécution.

Mettre à niveau le logiciel de la caméra

Remarque

Avant de mettre à niveau le logiciel de la caméra, enregistrez tous les paramètres d'AXIS Perimeter Defender. La mise à niveau du logiciel supprime l'application et ses paramètres de la caméra. Si les paramètres sont enregistrés, ils peuvent être restaurés à partir d'AXIS Perimeter Defender Setup.

1. Utilisez AXIS Perimeter Defender Setup pour enregistrer la configuration du site.
2. Mettez à niveau le logiciel de la caméra. Pour obtenir des instructions, reportez-vous au manuel d'utilisation de la caméra.
3. Démarrez AXIS Perimeter Defender Setup.
4. Utilisez l'option de chargement de site pour charger automatiquement la configuration de site enregistrée pour chaque caméra mise à niveau.

Résolution des problèmes d'installation

Problème	Cause possible	Solution
Un message Windows® indique qu'il est impossible d'installer le logiciel.	Le système d'exploitation de l'ordinateur portable ou du PC n'est pas compatible.	Vérifiez que le système d'exploitation Windows® correspond à celui spécifié dans les exigences.
Un message Windows® indique que l'installation est incorrecte.	Windows® Compatibility Assistant a détecté un problème d'installation potentiel.	Confirmez que l'installation est néanmoins correcte, puis poursuivez l'opération.
L'installation échoue lors de l'installation de XVID.	L'installation de XVID échoue en raison de la présence d'une ancienne installation partielle de XVID sur l'ordinateur.	Supprimez le dossier XVID dans C:\Program Files (x86), puis essayez à nouveau de procéder à l'installation.
Le package d'installation se bloque subitement après l'affichage de l'EULA. Un message d'erreur Windows® indique que l'application s'est arrêtée de manière inattendue. Il est impossible de fermer le package d'installation.	Un problème connu au niveau des packages d'installation entraîne le blocage de l'application dans certaines situations.	Ouvrez le Gestionnaire des tâches et arrêtez tous les processus « msiexec.exe ». Arrêtez ensuite le processus d'installation, puis redémarrez-le.

Résolution des problèmes de configuration

Problème	Cause possible	Solution
Problèmes d'ouverture d' AXIS Perimeter Defender.	Vous ne disposez pas de droits d'utilisateur Windows® suffisants.	Assurez-vous de disposer des droits d'administrateur.
La fonctionnalité de recherche ne trouve pas mes caméras.	Pare-feu	Les pare-feu et les logiciels antivirus peuvent parfois bloquer la détection de la caméra. Si nécessaire, configurez le pare-feu pour permettre le trafic réseau vers et depuis AXIS Perimeter Defender. Si le problème n'est pas résolu après cette configuration, réglez le pare-feu pour que les ports suivants soient autorisés : UDP port 5353 et TCP port 80.
	Problèmes d'adresse IP	Chaque dispositif du réseau doit avoir une adresse IP unique afin de communiquer avec les autres dispositifs. Avec AXIS Perimeter Defender, il est recommandé d'utiliser des adresses IP fixes pour les caméras. Assurez-vous que chaque périphérique IP sur le réseau possède sa propre adresse IP et n'utilise pas une adresse IP déjà attribuée.

Problème	Cause possible	Solution
	La caméra n'est pas disponible sur l'ordinateur de l'utilisateur.	Dans un navigateur, accédez à l'adresse IP de la caméra pour vérifier si elle est disponible. Si vous ne pouvez pas l'atteindre, cela signifie que la caméra n'a pas été installée correctement sur le réseau ou que l'ordinateur n'a pas accès à la caméra.
Il est impossible d'ajouter une caméra.	Les paramètres de connexion de la caméra (par exemple, adresse IP, mot de passe ou port HTTP) sont incorrects.	Vérifiez que les paramètres entrés sont corrects, puis répétez l'opération.
	La caméra ne peut pas être diffusée sur l'ordinateur de l'utilisateur.	Dans un navigateur, accédez à l'adresse IP de la caméra pour vérifier si elle est disponible. Si vous ne pouvez pas l'atteindre, cela signifie que la caméra n'a pas été installée correctement sur le réseau ou que l'ordinateur n'a pas accès au réseau sur lequel se trouve la caméra.
Perte de flux vidéo dans AXIS Perimeter Defender Setup.	La source vidéo n'est plus disponible.	La source vidéo a été interrompue et n'a pas été actualisée sur l'écran.
	Utilisez un navigateur pour vérifier si la caméra est disponible.	Cliquez sur la vignette sur laquelle le flux doit apparaître et redimensionnez l'interface. Le flux devrait être rétabli.
Le calibrage automatique ne fonctionne pas ou produit des résultats incorrects.	Les conditions préalables ne sont pas remplies.	Assurez-vous que les critères d'installation sont respectés. Cf. *Installation de la caméra, on page 13*.
	La caméra présente un mouvement de roulis.	Il n'est pas possible de calibrer une caméra présentant un mouvement de roulis.
	Connexion lente à une caméra non configurée comme caméra distante.	Connectez la caméra en tant que périphérique distant pour réduire les besoins en bande passante.
	Il y a d'autres objets en mouvement dans la scène utilisée pour le calibrage automatique, tels que des voitures, des arbres ou d'autres personnes.	Répétez le calibrage automatique ou calibrez le périphérique manuellement.
	Le champ de vision encombré cache souvent partiellement la personne qui marche devant la caméra.	Calibrez le périphérique manuellement.
	Le champ de vision est petit comme les entrées.	Calibrez le périphérique manuellement.

Problème	Cause possible	Solution
	La vidéo de capture n'a pas été enregistrée correctement en raison d'un espace disque insuffisant.	Vérifiez que l'espace disque disponible est suffisant et que l'application est autorisée à enregistrer la vidéo sur l'ordinateur sur lequel l'interface d' AXIS Perimeter Defender est en cours d'exécution.

Résolution des dysfonctionnements

Problème	Cause possible	Solution
L'application ne s'exécute pas même si la configuration est correcte.	Le logiciel de la caméra n'est pas à jour.	Vérifiez que le logiciel de la caméra est le plus récent.
L'incrustation ne s'affiche pas dans AXIS Perimeter Defender Setup même si l'analyse est en cours d'exécution.	L'application est bloquée après un démarrage ou un arrêt ou une mise à niveau du package d' AXIS Perimeter Defender.	Redémarrez la caméra.
	Un pare-feu bloque la connexion au port d'écoute des métadonnées de la caméra.	Configurez le pare-feu afin de permettre à l'interface de configuration de se connecter au port d'écoute des métadonnées de la caméra.
	Un programme antivirus bloque la réception de l'incrustation.	Configurez l'antivirus afin de permettre la réception de l'incrustation.
Aucune alarme n'est déclenchée dans AXIS Perimeter Defender Setup sur l'ordinateur de configuration même si l'analyse est en cours d'exécution et si l'incrustation est visible.	Bien que la cible se trouve dans la scène, elle ne correspond pas à un scénario conditionnel (par exemple, aucun déplacement d'une zone à l'autre dans le scénario de franchissement de zone).	Assurez-vous que le scénario est correctement spécifié, y compris les conditions.
	Détection médiocre.	Assurez-vous que les critères d'installation sont respectés. Cf. *Installation de la caméra, on page 13*. Assurez-vous également que le calibrage est assez précis et que la sensibilité est assez élevée.

Résolution des problèmes de performance

Problème	Cause possible	Solution
Les incrustations à l'écran et l'analyse s'activent et s'arrêtent sans cesse.	La charge du processeur de la caméra est trop élevée.	Solutions possibles : • Veillez à ne pas visualiser inutilement les flux de données, car chaque instance augmente la charge du processeur. • Si l'enregistrement sur détection de mouvement intégrée est activé, essayez de diminuer la qualité de l'enregistrement pour libérer la capacité du processeur. • Désactivez l'enregistrement par détection de mouvement et assurez-vous que la détection de mouvement est désactivée.
La fréquence d'image vidéo affichée est très faible.	Un trop grand nombre de visualisations de flux vidéo peut faire chuter la fréquence d'image en dessous des 8 ips par défaut.	Veillez à ne pas visualiser inutilement les flux de données, car chaque instance augmente la charge du processeur.
Une cible pénètre dans la zone stérile et déclenche plusieurs alertes.	La durée post-alarme est trop courte.	Ajustez la durée post-alarme. Accédez à AXIS Perimeter Defender Setup > **Sorties**.
Une cible potentielle entre dans la zone stérile, mais ne déclenche pas d'alerte, d'où une détection manquée.	Le contraste de l'objet par rapport à l'arrière-plan est trop faible.	Assurez-vous que les critères d'installation sont respectés. Cf. *Installation de la caméra, on page 13*.
	L'éclairage de la scène est inadéquat ou les performances de la caméra par faible luminosité sont insuffisantes.	Assurez-vous que les critères d'installation sont respectés. Cf. *Installation de la caméra, on page 13*.
	La sensibilité d'AXIS Perimeter Defender est trop faible.	Augmentez la sensibilité dans les paramètres de scénario globaux.
	La caméra a bougé, rendant le calibrage incorrect.	Refaites le calibrage.
	Le calibrage n'est pas assez précis.	Vérifiez le calibrage de la caméra. Accédez à AXIS Perimeter Defender Setup.
	Bien que la cible soit dans la scène, elle ne correspond pas à un scénario conditionnel. Par exemple, dans le scénario du	Assurez-vous que le scénario est correctement spécifié, y compris les conditions.

Problème	Cause possible	Solution
	franchissement de zone, l'objet ne passe pas d'une zone à une autre.	
La cible est détectée, mais sa classification est incorrecte (personne identifiée comme véhicule ou véhicule identifié comme personne).	La hauteur, le positionnement ou l'orientation de la caméra est incorrect.	Assurez-vous que les critères d'installation sont respectés. Cf. *Installation de la caméra, on page 13*.
	La caméra est trop éloignée de la zone.	Assurez-vous que les critères d'installation sont respectés. Cf. *Installation de la caméra, on page 13*.
	Le calibrage n'est pas assez précis.	Vérifiez le calibrage de la caméra. Accédez à AXIS Perimeter Defender Setup.
AXIS Perimeter Defender génère une alarme alors qu'aucune intrusion n'a lieu dans la zone stérile.	La sensibilité de l'analyse est trop élevée.	Diminuez la sensibilité. Accédez à AXIS Perimeter Defender Setup.
	Le calibrage n'est pas assez précis.	Vérifiez le calibrage de la caméra. Accédez à AXIS Perimeter Defender Setup.
	La caméra a bougé, rendant le calibrage incorrect.	Refaites le calibrage.
	Hauteur, positionnement ou orientation de la caméra incorrect.	Assurez-vous que les critères d'installation sont respectés. Cf. *Installation de la caméra, on page 13*.
	La caméra bouge, oscille ou vibre.	Stabilisez l'installation de la caméra.
	Végétation, drapeaux ou autres objets en mouvement à proximité de la caméra.	Retirez les éléments gênants du champ de vision de la caméra. AXIS Perimeter Defender ignore les objets qui se trouvent constamment dans la scène, mais qui sont éloignés de la caméra.
	Insectes sur l'objectif de la caméra ou à proximité.	Dissuadez les insectes d'approcher de l'objectif de la caméra.

À propos de ce manuel

Ce manuel s'adresse aux administrateurs et aux utilisateurs d'
AXIS Perimeter Defender. Il contient des consignes pour l'utilisation et la gestion du produit sur votre réseau. Une expérience préalable dans la mise en réseau sera utile pour l'utilisation de ce produit.

Avis de marques commerciales

T10068952_fr

2026-03 (M17.3)