



AXIS Q1656-DLE Radar-Video Fusion Camera

Manuel d'utilisation

Table des matières

Vue d'ensemble de la solution	5
.....	5
Pourquoi la fusion ?.....	5
Description de la fusion radar-vidéo.....	5
Installation	7
Mode aperçu	7
Guide d'installation	7
Considérations de performance.....	7
Où installer le produit	7
Couverture radar	9
Couverture de la fusion radar-vidéo.....	11
Installation de zone.....	13
Exemples d'installation de zone.....	13
Cas d'utilisation de la surveillance de zone	14
Installation routière.....	16
Exemples d'installation routière	16
Cas d'utilisation de la surveillance routière.....	18
MISE EN ROUTE	21
Trouver le périphérique sur le réseau	21
Prise en charge navigateur.....	21
Ouvrir l'interface web du périphérique.....	21
Créer un compte administrateur	21
Mots de passe sécurisés	22
Vérifiez que personne n'a saboté le logiciel du dispositif.....	22
Vue d'ensemble de l'interface web	22
Configurer votre périphérique.....	23
Paramètres de base	23
Régler l'image.....	23
Sélectionner le mode d'exposition	23
Optimiser l'éclairage IR	23
Bénéficier de l'illuminateur IR dans des conditions de faible luminosité avec le mode nocturne	23
Réduire le bruit dans des conditions de faible luminosité	24
Réduire le flou de mouvement dans les conditions de faible luminosité	24
Maximiser les détails dans une image	24
Gérer les scènes avec un fort contre-jour	25
Stabiliser une image tremblante avec la stabilisation d'image	25
Masquer des parties de l'image avec des masques de confidentialité.....	25
Afficher une incrustation d'image.....	26
Afficher la vidéo en direct du radar à l'image.....	26
Ajouter les noms des rues et la direction de la boussole sur l'image.....	26
Enregistrer et regarder la vidéo	27
Afficher et enregistrer la vidéo.....	27
Réduire la bande passante et le stockage	27
Configurer le stockage réseau	27
Configurer le radar.....	28
Sélectionner un profil de radar.....	28
Régler la hauteur de montage.....	28
Valider la hauteur de montage	28
Calibrez une carte de référence.....	29
Définir des zones de détection	30
Calibrer automatiquement le périphérique	32
Afficher une incrustation de texte avec l'angle d'inclinaison du radar.....	32
Configurer AXIS Object Analytics	33

Créer un scénario	33
Utiliser la vitesse pour le déclenchement.....	33
Sélectionner la sensibilité de détection	34
Réduire les fausses alarmes	34
Définir des règles pour les événements	35
Économiser l'énergie lorsqu'aucun mouvement est détecté	35
Déclencher une alarme si une personne ouvre l'enceinte.....	36
Envoyer un e-mail si le radar est recouvert d'un objet métallique.....	36
Contrôler une caméra PTZ avec le radar	37
Utiliser MQTT pour envoyer des données radar	39
Enregistrer une vidéo lorsque la caméra détecte un objet.....	39
Fournir une indication visuelle d'un événement en cours.....	40
Afficher une incrustation de texte dans le flux vidéo lorsque le périphérique détecte un objet	40
Enregistrer une vidéo lorsqu'un détecteur infrarouge passif détecte un mouvement.....	41
Enregistrer une vidéo lorsque la caméra détecte des bruits forts	42
Détecter les sabotages avec le signal d'entrée.....	43
Audio	43
Ajouter de l'audio à votre enregistrement.....	43
L'interface web.....	44
État	44
Vidéo	46
Installation	48
Image.....	50
Flux.....	57
Incrustations.....	60
Masques de confidentialité.....	62
Radar.....	62
Paramètres	62
Flux.....	64
Calibrage de la carte	66
Zones d'exclusion	67
Scénarios.....	68
Incrustations.....	69
Suivi automatique PTZ du radar.....	71
Calibrage automatique.....	72
Fonctions d'analyse	73
AXIS Object Analytics.....	73
AXIS Image Health Analytics.....	73
Visualisation des métadonnées.....	73
Configuration des métadonnées	73
Audio.....	74
Paramètres du périphérique	74
Flux.....	74
Clips audio.....	75
Amélioration audio	75
Enregistrements.....	75
Applications	77
Système	77
Heure et emplacement.....	77
Réseau	79
Sécurité.....	83
Comptes.....	88
Événements	90
MQTT	95
Stockage	98
Profils de flux.....	100

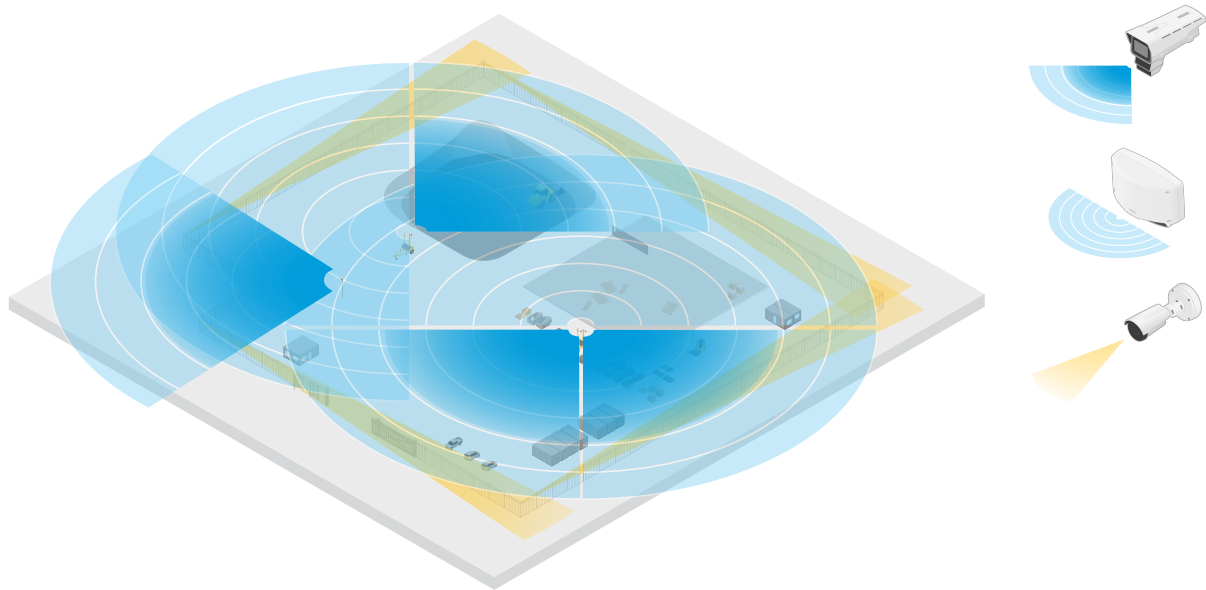
ONVIF.....	101
Détecteurs	104
Accessoires	104
Edge-to-Edge.....	105
Journaux	106
Plain Config	107
Maintenance	108
Maintenance.....	108
dépannage.....	109
En savoir plus	110
Connexions longues distances	110
Modes de capture.....	110
Mise au point à distance et zoom.....	111
Masques de confidentialité	111
Incrustations	111
Diffusion et stockage.....	112
Formats de compression vidéo	112
Quel est le lien entre les paramètres d'image, de flux et de profil de flux ?.....	112
Commande du débit binaire.....	113
Applications	114
AXIS Object Analytics.....	114
AXIS Image Health Analytics.....	114
Visualisation des métadonnées.....	115
Cybersécurité.....	115
Système d'exploitation signé.....	115
Démarrage sécurisé.....	115
Axis Edge Vault	115
Module TPM.....	115
Identifiant du périphérique Axis	115
Vidéo signée	116
Caractéristiques techniques	117
Gamme de produits	117
Voyants DEL.....	118
Avertisseur	118
Signal sonore de l'assistant de mise au point	118
Emplacement pour carte SD	118
Boutons	118
Bouton de commande	118
Interrupteur d'alarme d'intrusion.....	119
Connecteurs	119
Connecteur réseau.....	119
Connecteur audio	119
Connecteur E/S.....	119
Connecteur d'alimentation	120
Connecteur RS485/RS422.....	121
Recherche de panne	122
Réinitialiser les paramètres par défaut.....	122
Options d'AXIS OS	122
Vérifier la version actuelle d'AXIS OS.....	122
Mettre à niveau AXIS OS.....	123
Problèmes techniques, indications et solutions	123
Facteurs ayant un impact sur la performance	126
Contacter l'assistance.....	126

Vue d'ensemble de la solution

Une caméra de fusion radar-vidéo est une caméra visuelle équipée d'un module radar entièrement intégré. Par conséquent, elle peut utiliser le radar et la vidéo – séparément ou ensemble – pour détecter et classer des objets.

Les avantages d'une fusion radar-vidéo sont des détections et des classifications plus précises et moins de fausses alarmes. La fusion des deux technologies se matérialise dans AXIS Object Analytics, qui est l'interface principale utilisée pour accéder à la fusion radar-vidéo et la configurer.

L'AXIS Q1656-DLE détecte et classe les objets dans de vastes zones avec une profondeur, et vous pouvez l'utiliser pour la surveillance de zones ou la surveillance de routes. De plus, l'AXIS Q1656-DLE fonctionne bien dans la conception d'un site associée à d'autres périphériques. Dans la mesure où la plage de détection du radar est plus étendue que le champ de vision dans l'AXIS Q1656-DLE, combinez-la avec des caméras PTZ avec éclairage IR pour obtenir une confirmation visuelle dans la plage de détection complète du radar. Ou combinez-la avec des caméras thermiques qui peuvent détecter et classer des objets dans des zones longues et étroites.



Exemple de chantier de construction où deux radars autonomes couvrent les zones ouvertes du site tandis que quatre caméras de fusion radar-vidéo couvrent les zones ouvertes les plus complexes. En outre, quatre caméras thermiques couvrent les couloirs étroits le long de la clôture.

Pourquoi la fusion ?

Utilisées seules, la vidéo et le radar ont leurs propres atouts et limites :

- Généralement, la vidéo fournit des classifications plus précises lorsque le contraste est suffisant et que l'objet se déplace à proximité de la caméra. Elle fournit également plus de classifications granulaires que le radar. Cependant, une caméra a besoin de conditions d'éclairage adéquates pour une bonne vision.
- Quant au radar, il peut détecter des objets même dans des conditions d'éclairage difficiles, et sa plage de détection et de classification est plus étendue. Quelles que soient les conditions météorologiques, le radar peut mesurer la vitesse d'un objet en mouvement, sa direction et la distance qui le sépare de l'objet. Cependant, l'absence de confirmation visuelle risque de fragiliser les classifications radar. Les objets ondulants et les surfaces réfléchissantes peuvent déclencher de fausses alarmes et doivent être pris en compte dans le cadre de la conception du site et de la configuration du radar.

Les deux technologies de la caméra de fusion radar-vidéo peuvent évidemment être utilisées seules, mais elles sont plus puissantes lorsque les analyses des deux technologies interagissent pour assurer des détections et des classifications plus fiables.

Description de la fusion radar-vidéo

Ce produit fusionne les données radar avec les données vidéo de deux manières :

- **Fusion visuelle** : Les détections et classifications radar sont fusionnées dans l'image vidéo. Cela permet de visualiser les données radar dans le flux vidéo lorsque l'analyse vidéo n'est pas disponible. Par exemple, si un objet apparaît à une distance de 50 m (164 pi), il peut être trop petit pour l'analyse vidéo à détecter, mais le radar peut l'identifier. Dans ce cas, la détection radar est fusionnée dans le plan de l'image et peut être utilisée pour déclencher des alarmes dans l'application AXIS Object Analytics.
- **Fusion analytique** : Les détections et les classifications du radar sont fusionnées avec les détections et les classifications de l'analyse vidéo. Cela donne au dispositif une sortie analytique combinée où les forces respectives des deux technologies sont fusionnées. Il utilise la distance et la vitesse du radar, et la position et la classe de la vidéo. Lorsque l'objet dans l'exemple ci-dessus se rapproche, il est également détecté par l'analyse vidéo. La détection radar est ensuite fusionnée avec la sortie de l'analyse vidéo pour produire une sortie de meilleure qualité, et avec plus d'informations, que ce que les technologies peuvent fournir séparément.

Installation



Vidéo d'installation du périphérique.

Mode aperçu

Ce mode est idéal pour les installateurs au moment de régler la vue de la caméra pendant l'installation. Aucune connexion n'est requise pour accéder à la vue de la caméra en mode aperçu. Il n'est disponible que dans la configuration d'usine pour une durée limitée à partir de la mise sous tension de l'appareil.



Cette vidéo démontre comment utiliser le mode aperçu.

Guide d'installation

Le guide d'installation et d'autres documents relatifs à ce produit sont disponibles sur le site axis.com/products/axis-q1656-dle/support#support-resources

Considérations de performance

Où installer le produit

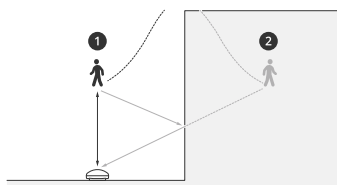
Pour obtenir la meilleure couverture vidéo et radar, le produit doit être correctement monté. Tenez compte des éléments suivants lors du montage d'une caméra de fusion radar-vidéo :

Surveillance des zones ou des routes

Ce produit est conçu pour la surveillance de zones ouvertes et vous pouvez l'utiliser pour la surveillance de zones ou la surveillance routière. Pour des exemples d'installation et des cas d'utilisation, voir et .

Éviter les objets solides et réfléchissants

Les objets solides et métalliques peuvent affecter les performances du radar du dispositif AXIS Q1656-DLE. La plupart des objets solides (tels que les murs, les clôtures, les arbres ou les grands buissons) situés dans le champ de vision créeront un angle mort (ombre radar) derrière eux. Les objets métalliques dans le champ de vision provoquent des reflets qui affectent la capacité du radar à effectuer des classifications. Cette situation peut générer des traces fantômes et de fausses alarmes dans le flux radar.



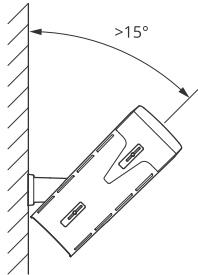
- 1 Détection réelle
- 2 Détection par réflexion (traces fantômes)

Pour plus d'informations sur la manière de manipuler les objets solides et réfléchissants dans la zone de couverture du radar, voir .

Position de montage

Installez le produit sur un mât stable ou à un endroit d'un mur où il n'y a pas d'autres objets ou d'installations. Les objets à une distance de 1 m (3 pi) à gauche et à droite du produit, qui réfléchissent les ondes radio, affectent les performances du radar dans AXIS Q1656-DLE.

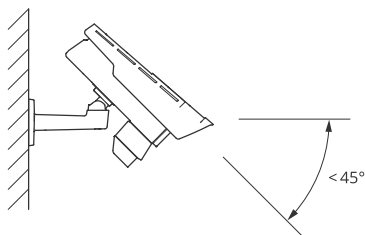
Si vous installez le produit contre un mur, il doit être orienté à l'opposé du mur à au moins 15°.



De plus, la hauteur de montage affecte la distance de détection et la portée de la vidéo et du radar.

Angle d'inclinaison

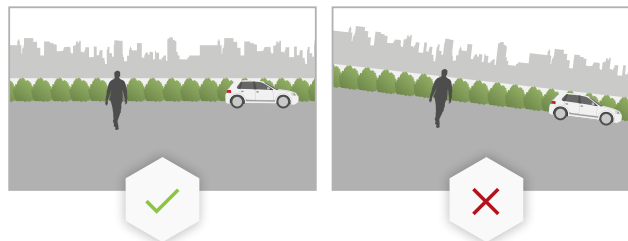
Le produit doit être orienté suffisamment vers le sol de sorte que le centre de l'image se trouve sous l'horizon. L'inclinaison de montage recommandée oscille entre 15 et 45°.



Vous pouvez ajouter une incrustation dans la vidéo en direct du radar qui indique l'angle d'inclinaison du produit. Pour des instructions, voir .

Angle de roulis

L'angle de roulis du produit doit être pratiquement égal à zéro, ce qui signifie que l'image doit être au même niveau que l'horizon.



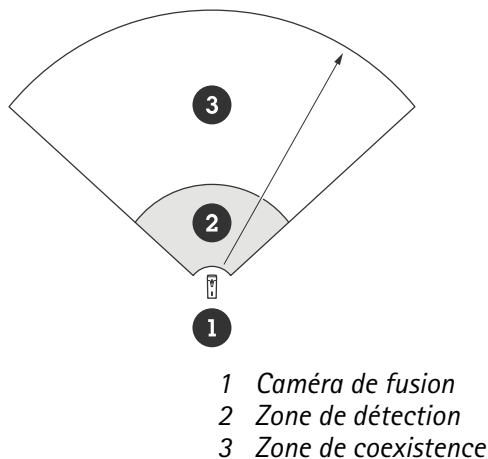
Coexistence

Si vous montez plus de huit radars ou caméras de fusion radar-vidéo Axis fonctionnant sur la bande de fréquences de 60 GHz l'un à côté de l'autre, ils risquent d'interférer l'un avec l'autre. Pour éviter les interférences, consultez .

Installer plusieurs radars Axis

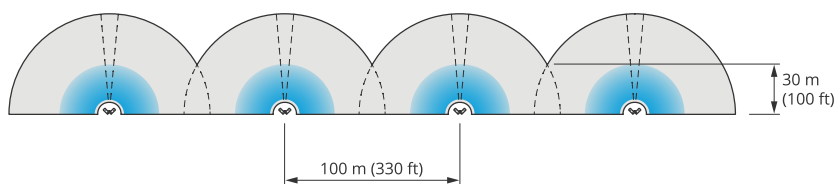
Coexistence

Les ondes radio du radar dans AXIS Q1656-DLE continuent au-delà de la zone de détection et peuvent interférer avec d'autres radars jusqu'à 350 m (380 yd). Il s'agit d'une zone de coexistence.



Le radar AXIS Q1656-DLE fonctionne sur la bande de fréquence de 60 GHz. Jusqu'à huit radars ou caméras de fusion radar-vidéo Axis fonctionnant sur la bande de fréquence de 60 GHz peuvent être installés à proximité les uns des autres, ou face à face, sans causer de problèmes. L'algorithme de coexistence intégré peut trouver un créneau de temps et un canal de fréquence qui minimise les interférences.

Si une installation comporte plus de huit dispositifs radar fonctionnant sur la même bande de fréquences et que de nombreux dispositifs sont orientés à l'opposé les uns des autres, il existe moins de risques d'interférences. En général, les interférences radar ne provoquent pas l'arrêt du fonctionnement du radar. Même en cas d'interférence, un algorithme d'atténuation des interférences intégré tente de réparer le signal radar. Un avertissement concernant les interférences devrait se produire dans un environnement où de nombreux radars fonctionnent sur la même bande de fréquences dans la même zone de coexistence. Le principal impact des interférences est la détérioration des performances de détection et la présence occasionnelle de traces fantômes.



Quatre paires de radars AXIS Q1656-DLE montés côte à côte.

Vous pouvez combiner la caméra de fusion radar-vidéo avec des radars Axis fonctionnant sur une autre bande de fréquences sans avoir à vous soucier de leur coexistence. Les périphériques Axis qui utilisent différentes bandes de fréquence n'interfèrent pas l'un avec l'autre.

Couverture radar

Le radar du dispositif AXIS Q1656-DLE a un champ de détection horizontal de 95°. La portée de détection du radar dépend de facteurs tels que la scène, la hauteur de montage et l'angle d'inclinaison du produit, ainsi que la taille et la vitesse des objets en mouvement.

La plage de détection dépend également du **profil de surveillance** que vous sélectionnez. Vous pouvez utiliser l'AXIS Q1656-DLE pour la surveillance de zone ou de route et deux profils du radar sont optimisés pour chacun des scénarios :

- **Area monitoring profile** (Profil de surveillance d'espace) : Le radar suit et classe les personnes, les véhicules et les objets inconnus qui se déplacent à des vitesses inférieures à 55 km/h (34 mph). Pour plus d'informations sur la plage de détection, consultez .
- **Road monitoring profile** (Profil de surveillance routière) : Le radar suit et classe principalement les véhicules qui se déplacent à des vitesses jusqu'à 200 km/h (125 mph). Pour plus d'informations sur la plage de détection, consultez .

Remarque

Lorsque le radar et la vidéo sont combinés dans AXIS Object Analytics, l'AXIS Q1656-DLE peut classer les sous-catégories de véhicules (bus, voitures, vélos, autobus, camions et autres).

Sélectionnez la zone ou le profil de surveillance dans l'interface Web du produit. Pour des instructions, voir .

Zone de couverture

Le champ de détection horizontal du radar de ce dispositif est de 95°. La surface du champ de vision correspond à 2700 m² (29 000 pi²) pour les humains et à 6 100 m² (65 600 pi²) pour les véhicules.

Remarque

Une couverture de zone optimale s'applique lorsque le produit est monté à 3,5–7 m (11–23 pi). La hauteur de montage influe sur l'ampleur de l'angle mort sous le radar.

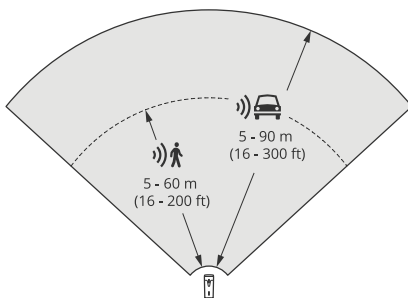
Plage de détection de zone

La plage de détection est la distance à laquelle un objet peut être suivi et déclencher une alarme. Elle est mesurée entre une limite proche de la détection (proximité du périphérique à laquelle elle peut être assurée) et une limite de détection éloignée (distance du périphérique à laquelle une détection peut être assurée).

Le **profil de surveillance de zone** est optimisé pour la détection humaine. En outre, il vous permettra également de suivre des véhicules et d'autres objets se déplaçant à une vitesse pouvant atteindre 55 km/h (34 mph) avec une précision de +/- 2 km/h (1,25 mph).

Lorsque le montage est à une hauteur d'installation optimale, les plages de détection sont les suivantes :

- 5 à 60 m (16 à 200 pi.) lors de la détection d'un humain
- 5 à 90 m (16 à 300 pi.) lors de la détection d'un véhicule



Remarque

- Saisissez la hauteur de montage sur l'interface Web du produit lors du calibrage du radar.
- La plage de détection est impactée par la scène et l'angle d'inclinaison du produit.
- La plage de détection est impactée par le type et la taille de l'objet en déplacement.

La plage de détection du radar a été mesurée dans les conditions suivantes :

- La portée a été mesurée le long du sol.
- L'objet correspondait à une personne mesurant 170 cm (5 pi 7 po).
- La personne marchait directement devant le radar.
- Les valeurs étaient mesurées lorsque la personne entrait dans la zone de détection.
- La sensibilité du radar était réglée sur **Medium (Moyen)**.

Hauteur de montage	Inclinaison de 15°	Inclinaison de 20°	Inclinaison de 25°	Inclinaison de 30°	Inclinaison de 35°	Inclinaison de 40°	Inclinaison de 45°
3,5 m (11 pi)	6,0–60+ m (19–196+ pi)	5,0–60+ m (16–196+ pi)	4,0–60+ m (13–196+ pi)	4,0–60 m (13–196 pi)	4,0–55 m (13–180 pi)	4,0–40 m (13–131 pi)	4,0–30 m (13–98 pi)
4,5 m (14 pi)	6,0–60+ m (19–196+ pi)	6,0–60+ m (19–196+ pi)	5,0–60+ m (16–196+ pi)	4,0–60+ m (13–96+ pi)	4,0–60 m (13–196 pi)	4,0–45 m (13–147 pi)	4,0–40 m (13–131 pi)
6 m (19 pi)	10–60+ m (32–196+ pi)	9,0–60+ m (29–196+ pi)	7,0–60+ m (22–196+ pi)	6,0–60+ m (19–196+ pi)	6,0–60 m (19–196 pi)	5,0–55 m (16–180 pi)	5,0–55 m (16–180 pi)
8 m (26 pi)	16–60 m (52–196 pi)	14–60 m (45–196 pi)	10–60 m (32–196 pi)	8,0–60+ m (26–196+ pi)	8,0–60+ m (26–196+ pi)	7,0–60 m (22–196 pi)	7,0–60 m (22–196 pi)
10 m (32 pi)	21–60 m (68–196 pi)	19–60 m (62–196 pi)	14–60 m (45–196 pi)	12–60+ m (39–196+ pi)	10–60+ m (32–196+ pi)	9,0–60 m (29–196 pi)	9,0–60 m (29–196 pi)
12 m (39 pi)	25–60 m (82–196 pi)	23–60 m (75–196 pi)	19–60 m (62–196 pi)	16–60+ m (52–196+ pi)	13–60+ m (42–196+ pi)	11–60 m (36–196 pi)	11–55 m (36–180 pi)

Remarque

- Le réglage de la sensibilité radar sur **Faible** diminue la plage de détection de 20 %, alors que la valeur **Élevé** augmente la plage de détection de 20 %.
- Dans les installations où l'on s'attend à ce que de petits animaux apparaissent en dehors de la zone de fusion, mais toujours dans la zone de détection du radar, vous pouvez réduire le nombre de fausses alarmes en définissant la sensibilité radar sur **Low (Faible)**. Néanmoins ce choix limite la plage de détection.

Plage de détection routière

Le **profil de surveillance routière** est optimisé pour la détection des véhicules et fournit une précision de vitesse de +/- 2 km/h (1,24 mph) lors de la surveillance de véhicules se déplaçant à une vitesse de 200 km/h (125 mph).

La hauteur de montage de la caméra de fusion radar-vidéo et la vitesse du véhicule auront un impact sur la portée de détection du radar. Lorsqu'il est monté à une hauteur d'installation optimale, le radar détecte les véhicules qui s'approchent et s'éloignent avec une précision de vitesse de +/- 2 km/h (1,24 mph) dans les plages suivantes :

- 25 à 100 m (82 à 328 pi) pour les véhicules qui se déplacent à une vitesse de 50 km/h (31 mph).
- 40 à 80 m (131 à 262 pi) pour les véhicules qui se déplacent à une vitesse de 100 km/h (62 mph).
- 50 à 70 m (164 à 230 pi) pour les véhicules qui se déplacent à une vitesse de 200 km/h (125 mph).

Remarque

Afin de minimiser le risque de détections manquées de véhicules roulant à grande vitesse, configurez un scénario dans le radar qui se déclenche en fonction des types d'objets **Véhicule** et **Inconnu**. Pour plus d'informations sur la configuration d'un scénario, consultez .

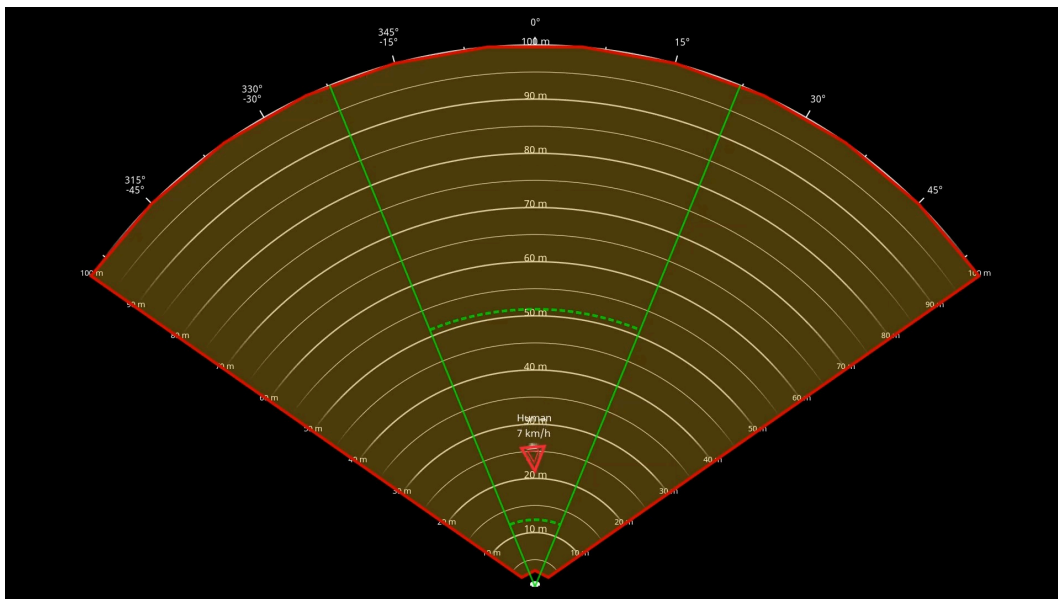
Couverture de la fusion radar-vidéo

La zone de fusion analytique, dans laquelle un objet peut être détecté et classé par les deux technologies, dépend des facteurs suivants :

- La hauteur d'installation de la caméra.
- L'angle d'inclinaison de la caméra.
- Le niveau de zoom de l'objectif de la caméra.
- Les conditions d'éclairage de l'environnement, et la lumière fournie par la caméra elle-même et les autres périphériques du site.
- La distance par rapport à l'objet en mouvement.

Une fois la caméra de fusion radar-vidéo installée, la couverture du radar est fixe. Toutefois, le champ de vision de la caméra dépend du niveau de zoom de l'objectif.

Deux lignes vertes dans le flux radar qui représentent le champ de vision approximatif de la caméra permettent de visualiser le champ de vision de la caméra par rapport à la couverture radar. Les lignes s'ajustent lorsque la caméra effectue un zoom avant ou arrière. De plus, deux lignes pointillées qui représentent la zone de vision approximative de la caméra apparaissent. La ligne pointillée la plus proche du périphérique représente la limite proche de la détection, tandis que la ligne plus éloignée représente la limite de détection éloignée.



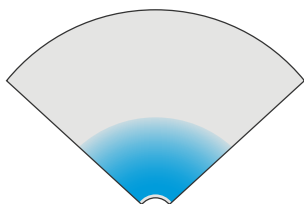
Les lignes continues de couleur verte représentent le champ de vision approximatif de la caméra, tandis que les lignes pointillées vertes désignent les limites de détection proches et éloignées approximatives.

Exemples de niveau de zoom

La taille de la zone de fusion des analyses dépend du niveau de zoom de l'objectif du dispositif AXIS Q1656-DLE. Les deux extrêmes du niveau de zoom sont décrits ci-dessous.

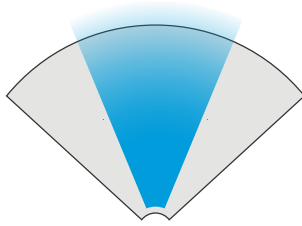
Zoom arrière de l'objectif (largeur maximale) :

Lorsque l'objectif de l'AXIS Q1656-DLE est zoomé vers l'arrière au maximum, les objets peuvent être trop petits pour être détectés dans le cadre de l'analyse vidéo. Dans ce scénario, il est probable que les objets soient détectés par le radar grâce à sa large couverture, mais pas par l'analyse vidéo. Pour établir une confirmation visuelle dans l'ensemble de la plage de détection du radar, vous pouvez appairer l'AXIS Q1656-DLE avec une ou plusieurs caméras PTZ.



Zoom avant de l'objectif (limite télé max.)

Lorsque l'objectif est zoomé vers l'avant au maximum, il limite considérablement le champ de vision de la caméra. Dans la mesure où les objets lointains sont agrandis par rapport à une utilisation du zoom arrière maximal de l'objectif, cela signifie toutefois que les objets peuvent être détectés par l'analyse vidéo à une distance beaucoup plus grande de l'appareil. Dans ce scénario, il est donc possible que les objets soient détectés par l'analyse vidéo, mais pas par l'analyse radar.



Afin d'optimiser les chances de classification précise d'un objet à la fois par le radar et l'analyse vidéo, réglez le zoom dans la mesure du possible de sorte que les objets de la zone d'intérêt soient suffisamment grands pour être détectés par l'analyse vidéo.

Détections et classifications du radar-vidéo

Dans la mesure où AXIS Q1656-DLE peut détecter et classer des objets à l'aide d'un radar et de la vidéo, ou de l'une de ces technologies seulement, plusieurs facteurs doivent être pris en compte.

- Si deux personnes marchent à proximité l'une de l'autre et sont détectées par le radar (mais pas par l'analyse vidéo), elles seront classées comme une seule personne et une zone de délimitation unique apparaît autour d'elles. Lorsqu'elles pénètrent la zone de fusion analytique et que la confirmation visuelle est assurée, elles sont classées de manière précise. La différenciation spatiale du radar dans le dispositif AXIS Q1656-DLE est de 3 m (9 pi).
- Si un objet se trouve en dehors du champ de vision de la caméra, l'AXIS Q1656-DLE ne peut pas fusionner ce qu'il a détecté ou classé dans le plan d'image. En conséquence, l'AXIS Object Analytics ne peut pas déclencher d'alarme. Pour déclencher une alarme lorsqu'un objet est détecté par le radar uniquement, configurez un scénario dans l'interface web du radar et utilisez les conditions permettant de déclencher un mouvement dans le scénario du radar.
- Les zones d'exclusion que vous ajoutez dans l'interface Web du radar sont globales, ce qui signifie que tout mouvement détecté dans ces zones est toujours ignoré – même si la zone d'exclusion se chevauche avec la zone de fusion d'analyses dans AXIS Object Analytics. Les zones d'exclusion que vous ajoutez dans AXIS Object Analytics, cependant, ignoreront uniquement les mouvements dans les scénarios d'AXIS Object Analytics.

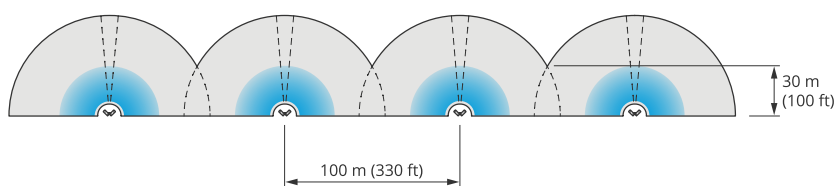
Installation de zone

Pour obtenir les meilleures performances radar dans les installations de surveillance d'espace, sélectionnez le **profil de surveillance d'espace** dans le dispositif AXIS Q1656-DLE. Pour en savoir plus, voir .

Exemples d'installation de zone

Vous pouvez placer plusieurs caméras de fusion radar-vidéo côte à côte pour créer une clôture virtuelle, le long ou autour d'un bâtiment.

Pour une couverture radar à 180°, placez deux AXIS Q1656-DLE l'une à côté de l'autre. Lorsque vous installez plus d'une paire de caméras de fusion radar-vidéo côte à côte, nous vous recommandons de les placer avec un espacement de 100 m (330 pi) entre chaque paire, comme illustré dans l'exemple.



Quatre paires de radars AXIS Q1656-DLE montés côte à côte.

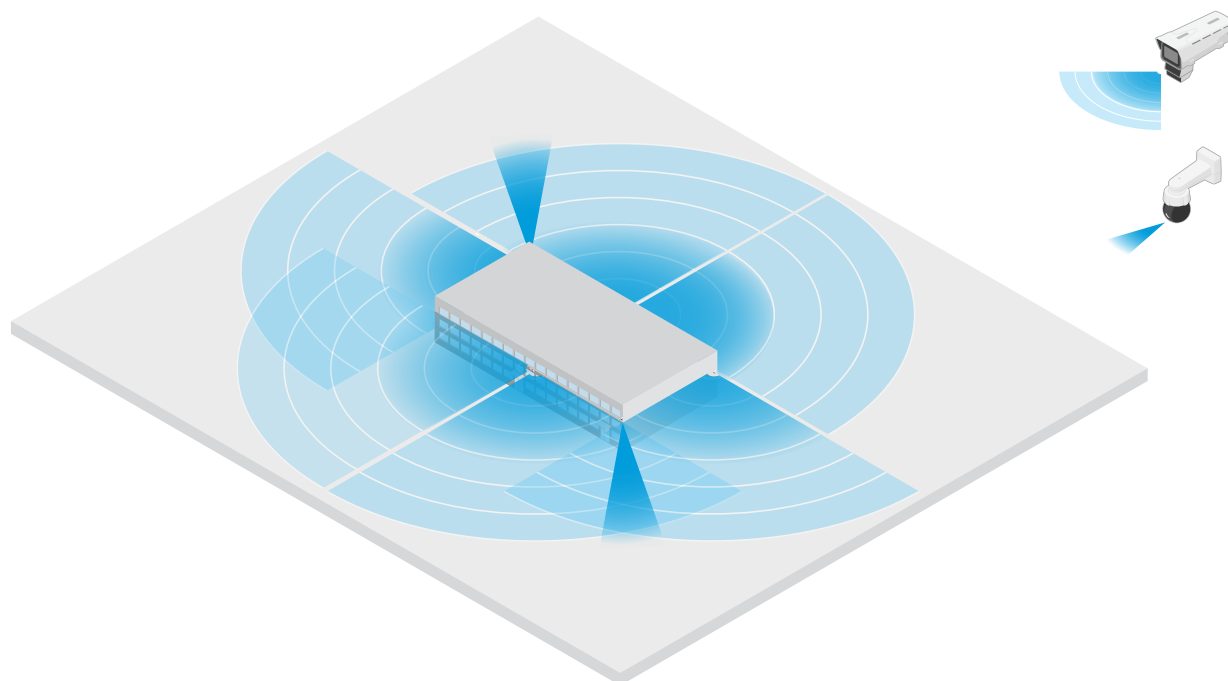
Vous pouvez installer jusqu'à huit caméras de fusion radar-vidéo ensemble sans interférences entre les radars. Pour plus d'informations sur le positionnement des radars Axis à proximité les uns des autres, consultez .

Cas d'utilisation de la surveillance de zone

Couvrir un champ ouvert autour d'un bâtiment

Une entreprise logée dans un immeuble de bureaux doit protéger les locaux contre les intrusions et les actes de vandalisme, notamment après les heures de bureau, lors des vacances et des week-ends. Pour couvrir la zone autour du bâtiment, elle installe un ensemble de caméras de fusion radar-vidéo et de caméras PTZ. Elle configure les caméras de fusion radar-vidéo de manière à déclencher une alarme lorsque des humains et des véhicules approchent du bâtiment. Pour obtenir des détections et des classifications aussi fiables que possible, elle sélectionne une sensibilité de détection AXIS Object Analytics adaptée à la zone. Pour plus d'informations sur la sensibilité de la détection, consultez .

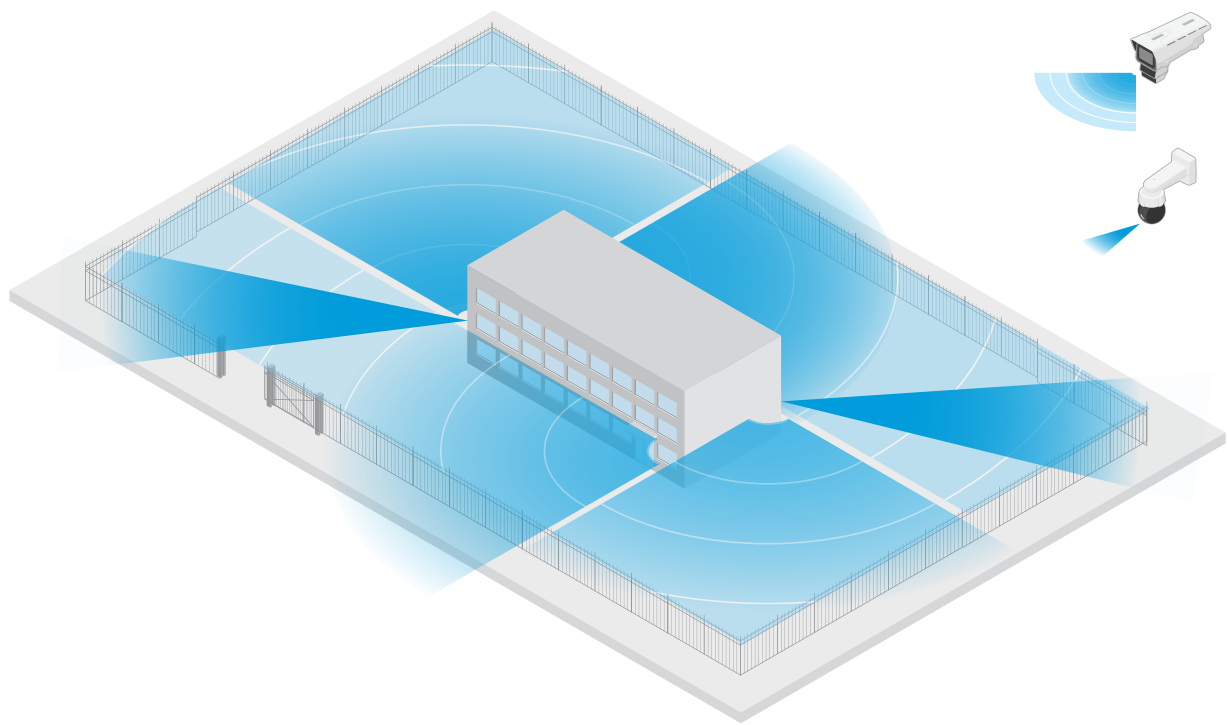
Pour être sûre d'obtenir une confirmation visuelle des intrus potentiels dans la plage de détection complète du radar, elle ajoute deux caméras PTZ avec IR intégré aux coins opposés du bâtiment. Les radars orientent les caméras PTZ via *AXIS Radar Autotracking for PTZ*, et l'IR intégré fournit également plus de lumière pour les caméras radar-vidéo fusion, ce qui permet de détecter et d'identifier des intrus sur une plus grande distance.



Couvrir un bâtiment clôturé

Un entrepôt qui conserve normalement les marchandises dans les locaux est entouré d'une clôture pour éloigner les intrus. Pour détecter les intrus potentiels, elle installe une combinaison de caméras de fusion radar-vidéo et de caméras PTZ avec IR intégré pour sécuriser les locaux. Les caméras de fusion radar-vidéo fournissent des détections fiables et des alarmes de déclenchement, tandis que les caméras PTZ étendent la couverture visuelle. Les caméras PTZ avec IR intégré apportent également plus de lumière aux caméras de fusion radar-vidéo, ce qui permet de détecter et d'identifier des intrus à une plus grande distance.

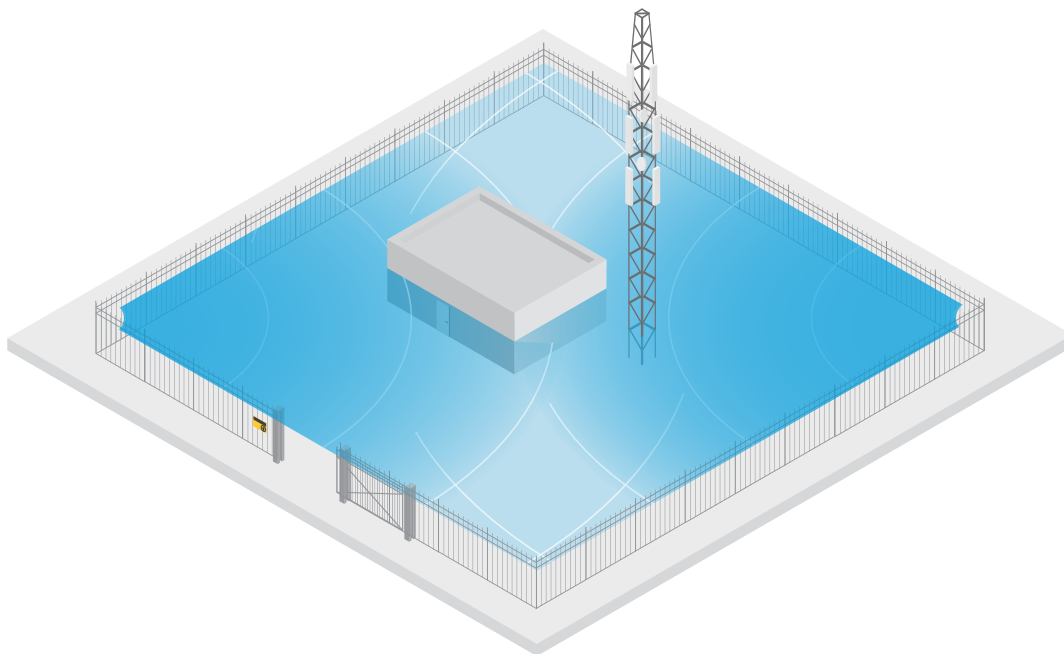
Dans cette scène, la zone à l'extérieur de la clôture n'est pas couverte, car c'est une zone très fréquentée qui peut déclencher de fausses alarmes. Dans les scènes avec moins d'activité, la zone à l'extérieur de la clôture peut également être couverte. Dans une telle scène, il serait possible de configurer les caméras pour déclencher des lumières externes lorsque des mouvements sont détectés à l'extérieur de la clôture pour dissuader les intrus potentiels. Elles pourraient également déclencher une alarme lorsque des intrus sont effectivement détectés à l'intérieur de la clôture. Pour pouvoir détecter un mouvement à l'extérieur de la clôture, les caméras doivent être suffisamment montées en hauteur.



Couvrir une ressource critique

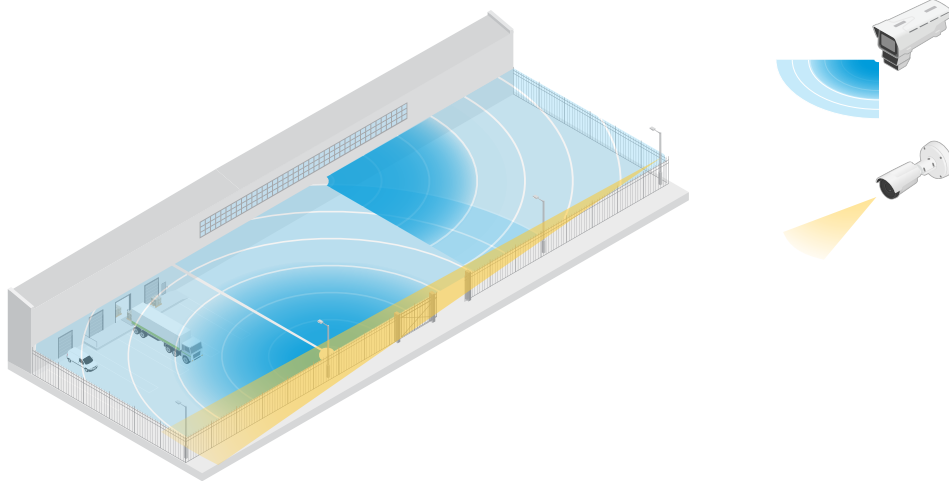
Un abri télécom contenant des équipements critiques et des câblages est entouré d'une clôture pour éloigner les intrus. Pour éviter toute sabotage, une protection supplémentaire est nécessaire. Comme il est important de maintenir au minimum les fausses alarmes, elle installe deux caméras radar-vidéo fusion dans les coins opposés du site. Les caméras peuvent ensemble couvrir l'abri, les antennes et le sol. Grâce à la technologie radar et vidéo utilisée dans les caméras de fusion radar-vidéo, les caméras peuvent fournir des détections et des classifications fiables des intrus potentiels.

Il est possible de placer les caméras radar-vidéo en fusion les unes en face des autres de cette manière sans interférences entre les radars. Cependant, pour être sûr que la technologie vidéo fournisse des détections et des classifications précises, de bonnes conditions d'éclairage sont nécessaires.



Couvrir la zone autour d'un quai de chargement

Le quai de chargement d'un bâtiment commercial est enserré par une clôture pour protéger les locaux. Pour des raisons de sécurité supplémentaires, la société installe une caméra thermique et trois caméras de fusion radar-vidéo sur le site. Pour détecter les intrus potentiels, elle installe une caméra thermique le long de la clôture. Pour détecter les intrus qui ont réussi à passer la clôture, elle installe deux des caméras de fusion radar-vidéo sur un poteau faisant face aux quais de chargement. Ces caméras sont capables de détecter et de classer des personnes et des véhicules qui se déplacent autour des quais et peuvent déclencher une alarme après les heures de travail. Pour détecter tout intrus traversant la zone avec le point de retournement sur le côté droit, elle installe une caméra radar-vidéo de fusion supplémentaire orientée vers la zone. Enfin, la caméra thermique peut également aider à détecter les tentatives de sabotage des deux caméras installées à proximité de la clôture.



Installation routière

Pour obtenir les meilleures performances radar dans les installations routières, sélectionnez le **profil de surveillance routière** dans le dispositif AXIS Q1656-DLE. Pour en savoir plus, voir .

Exemples d'installation routière

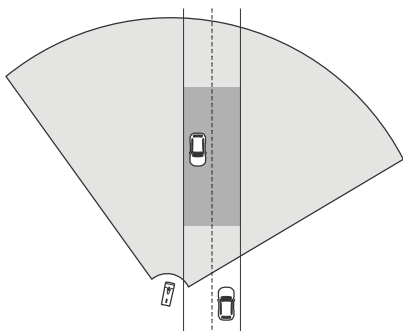
En cas de surveillance des routes et des autoroutes, assurez-vous de monter la caméra de fusion radar-vidéo à une hauteur suffisante afin d'éviter les angles morts (ombre radar) derrière les véhicules.

Remarque

La taille de l'ombre radar dépend de la hauteur de montage de la caméra de fusion radar-vidéo, ainsi que de la hauteur et de la distance du véhicule par rapport au radar. Par exemple, lorsqu'un véhicule haut de 4,5 m (15 pi) se trouve à 50 m (164 pi) d'une caméra de fusion radar-vidéo montée à une hauteur de 8 m (26 pi), l'ombre radar derrière le véhicule est de 50 m (164 pi). Toutefois, si la caméra de fusion radar-vidéo est montée à une hauteur de 12 m (39 pi), l'ombre derrière le même véhicule ne sera que de 23 m (74 pi).

Monté sur un côté

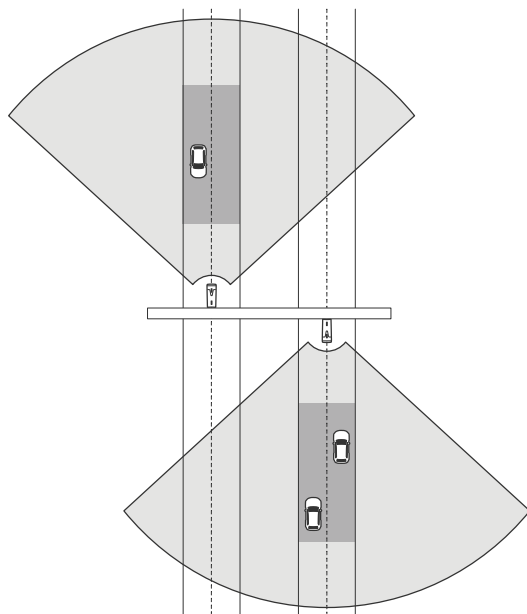
Pour surveiller les véhicules le long d'une route, vous pouvez monter la caméra de fusion radar-vidéo sur le côté de la route (sur un mât, par exemple). Dans ce type d'installation, nous recommandons un angle panoramique max. de 25°.



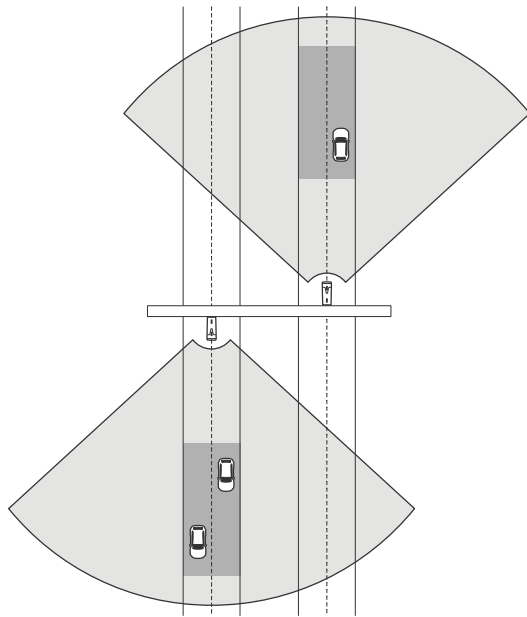
Pour que le radar de l'AXIS Q1656-DLE mesure les vitesses élevées avec précision, positionnez la caméra de fusion radar-vidéo à une distance latérale de 10 m (32 pi) des véhicules. Pour plus d'informations sur la portée de détection et la précision de la vitesse, consultez .

Monté au centre

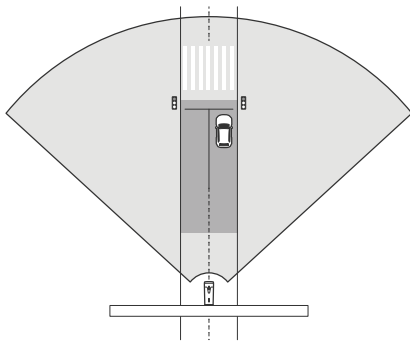
Pour surveiller les véhicules sur une route à plusieurs voies, vous pouvez monter un ou plusieurs caméras de fusion radar-vidéo sur un portique au-dessus de la route.



Le même type d'installation est possible si vous souhaitez surveiller des véhicules qui s'éloignent de la caméra de fusion radar-vidéo, au lieu de rouler vers elle.



Vous pouvez également placer la caméra de fusion radar-vidéo sur une allée donnant sur un passage pour piétons avec des feux de signalisation, par exemple pour enregistrer les vitesses des véhicules ou détecter des infractions de vitesse.

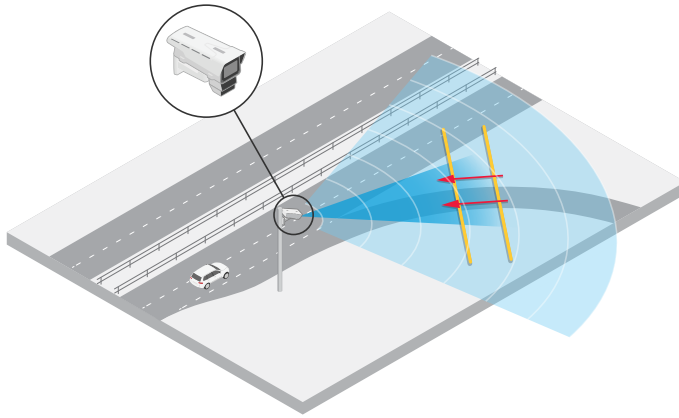


Pour que le radar de l'AXIS Q1656-DLE mesure les vitesses élevées avec précision, positionnez la caméra de fusion radar-vidéo à une distance latérale de 10 m (32 pi) des véhicules. Pour plus d'informations sur la portée de détection et la précision de la vitesse, consultez .

Cas d'utilisation de la surveillance routière

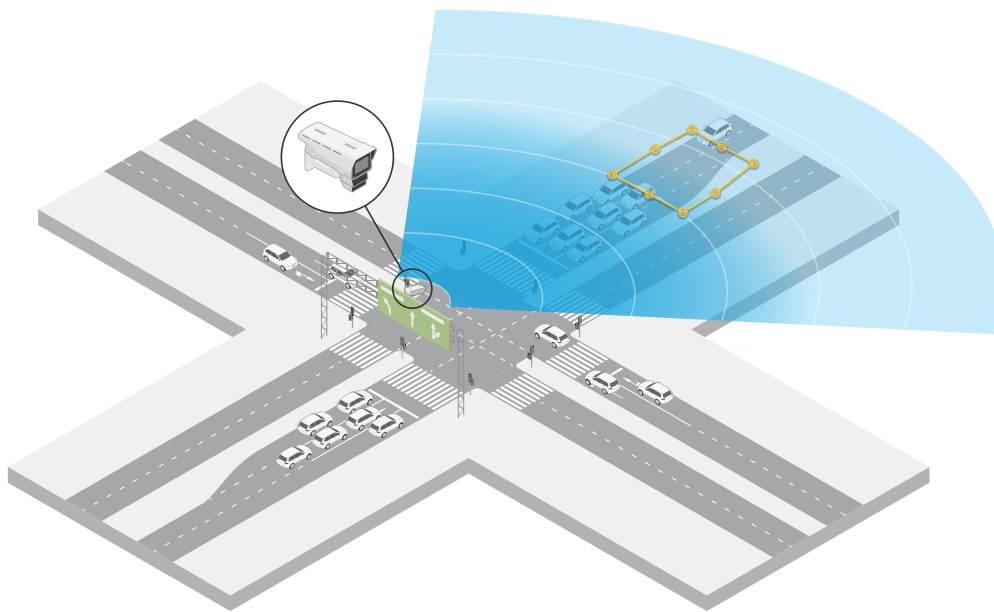
Détection de véhicules roulant dans le mauvais sens sur une bretelle d'autoroute

Pour détecter et identifier les véhicules roulant dans le mauvais sens sur une bretelle d'autoroute, le contrôle du trafic monte l'AXIS Q1656-DLE sur un poteau faisant face à la bretelle. Pour des détections fiables, il définit un scénario de franchissement de ligne dans l'interface Web du dispositif et le configure de sorte que les véhicules doivent traverser deux lignes pour déclencher une alarme. Dans le scénario radar, il positionne les deux lignes sur la bretelle comme indiqué dans l'illustration, et précise le sens de conduite et les vitesses de déclenchement. Dans cette configuration, le radar déclenche l'alarme et la caméra peut fournir une identification visuelle du véhicule sur la bretelle. Pour plus d'informations sur la configuration d'un scénario radar, consultez .



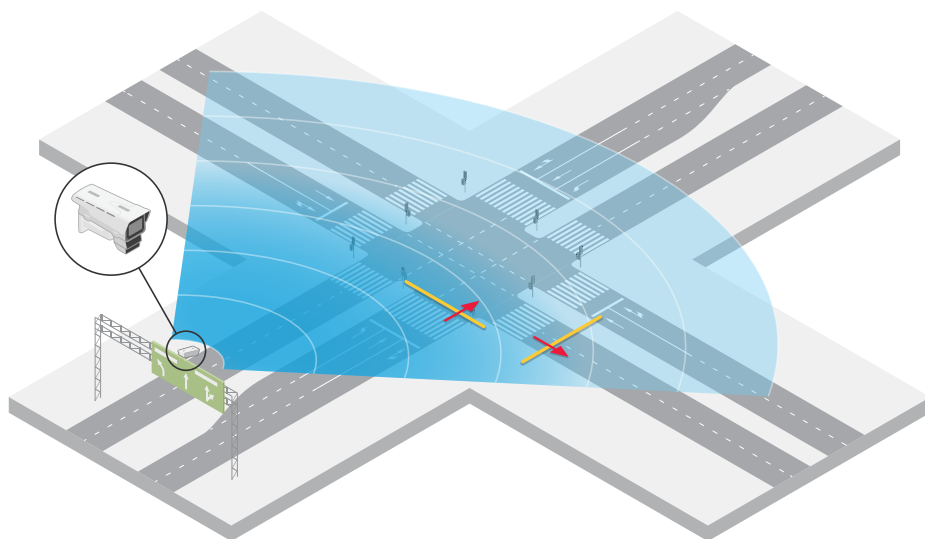
Surveillance du flux de trafic à une intersection : formation de bouchons

Pour surveiller comment et quand des bouchons se forment à une intersection très fréquentée, le contrôle de la circulation installe l'AXIS Q1656-DLE sur un portique au-dessus de l'intersection. Il définit un objet dans le scénario de zone dans AXIS Object Analytics qui va déclencher un mouvement de véhicules dans une zone. Il élabore un scénario de façon à couvrir uniquement la partie de la route conduisant à l'intersection et sélectionne une sensibilité de détection adaptée à la scène. Pour déclencher une alarme lorsque des bouchons commencent à se former, la condition de déclenchement porte sur les véhicules qui se déplacent à des vitesses inférieures à 5 km/h (3 mph). Pour plus d'informations sur la configuration d'un scénario AXIS Object Analytics et la sélection d'une sensibilité de détection adaptée, consultez .



Surveillance du flux de trafic à une intersection : direction

Pour obtenir un aperçu du flux de trafic et de la direction prise par les véhicules à une intersection très fréquentée, le contrôle de la circulation installe l'AXIS Q1656-DLE sur un portique au-dessus de la route conduisant à l'intersection. Il définit un scénario de franchissement de ligne dans les pages radar de l'interface Web du dispositif où les véhicules doivent traverser deux lignes pour déclencher une alarme. Dans le scénario radar configuré, la première des deux lignes est placée sur les voies conduisant à l'intersection, juste après le passage pour piétons afin d'éviter que les véhicules s'arrêtent à la ligne. La deuxième ligne est placée sur les voies allant vers la droite. Les véhicules doivent traverser les deux lignes dans la direction spécifiée pour déclencher une alarme. Pour éviter un déclenchement sur plusieurs véhicules par franchissement, la durée minimale de déclenchement dans le scénario radar va de 2 à 0 secondes.



Pour surveiller le flux de trafic dans toutes les directions, ils créent un scénario radar pour chaque direction. Pour plus d'informations sur la configuration d'un scénario radar, consultez .

Remarque

Dans ce scénario radar, les véhicules qui traversent les lignes ne sont pas comptés. Vous pouvez plutôt utiliser le système d'événements dans l'interface Web du dispositif pour effectuer le comptage. Un moyen de compter les véhicules consiste à envoyer un message MQTT à chaque déclenchement du scénario radar et de compter les déclencheurs du côté du destinataire de MQTT.

MISE EN ROUTE

Trouver le périphérique sur le réseau

Pour trouver les périphériques Axis présents sur le réseau et leur attribuer des adresses IP sous Windows®, utilisez AXIS IP Utility ou AXIS Device Manager. Ces applications sont gratuites et peuvent être téléchargées via axis.com/support.

Pour plus d'informations sur la détection et l'assignation d'adresses IP, accédez à *Comment assigner une adresse IP et accéder à votre périphérique*.

Prise en charge navigateur

Vous pouvez utiliser le périphérique avec les navigateurs suivants :

	Chrome™	Firefox®	Edge™	Safari®
Windows®	recommandé	recommandé	✓	
macOS®	recommandé	recommandé	✓	✓
Linux®	recommandé	recommandé	✓	
Autres systèmes d'exploitation	✓	✓	✓	✓*

*Pour utiliser l'interface Web AXIS OS avec iOS 15 ou iPadOS 15, allez à **Settings (Paramètres) > Safari > Advanced (Avancé) > Experimental Features (Fonctions expérimentales)** et désactivez NSURLConnection Websocket.

Ouvrir l'interface web du périphérique

1. Ouvrez un navigateur et saisissez l'adresse IP ou le nom d'hôte du périphérique Axis. Si vous ne connaissez pas l'adresse IP, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau.
2. Saisissez le nom d'utilisateur et le mot de passe. Si vous accédez pour la première fois au périphérique, vous devez créer un compte administrateur. Cf. .

Pour une description de tous les contrôles et options que vous rencontrez dans l'interface Web du périphérique, consultez

Créer un compte administrateur

La première fois que vous vous connectez à votre périphérique, vous devez créer un compte administrateur.

1. Saisissez un nom d'utilisateur.
2. Entrez un mot de passe. Cf. .
3. Saisissez à nouveau le mot de passe.
4. Acceptez le contrat de licence.
5. Cliquez sur **Ajouter un compte**.

Important

Le périphérique n'a pas de compte par défaut. Si vous perdez le mot de passe de votre compte administrateur, vous devez réinitialiser le périphérique. Cf. .

Mots de passe sécurisés

Important

Les périphériques Axis envoient le mot de passe initial en texte clair sur le réseau. Pour protéger votre appareil après la première connexion, configurez une connexion HTTPS sécurisée et cryptée, puis modifiez le mot de passe.

Le mot de passe de l'appareil est la principale protection de vos données et services. Les périphériques Axis n'imposent pas de stratégie de mot de passe, car ils peuvent être utilisés dans différents types d'installations.

Pour protéger vos données, nous vous recommandons vivement de respecter les consignes suivantes :

- Utilisez un mot de passe comportant au moins 8 caractères, de préférence créé par un générateur de mot de passe.
- Prenez garde à ce que le mot de passe ne soit dévoilé à personne.
- Changez le mot de passe à intervalles réguliers, au moins une fois par an.

Vérifiez que personne n'a saboté le logiciel du dispositif.

Pour vous assurer que le périphérique dispose de son système AXIS OS d'origine ou pour prendre le contrôle total du périphérique après une attaque de sécurité :

1. Réinitialisez les paramètres par défaut. Cf. .
Après la réinitialisation, le démarrage sécurisé garantit l'état du périphérique.
2. Configurez et installez le périphérique.

Vue d'ensemble de l'interface web

Cette vidéo vous donne un aperçu de l'interface web du périphérique.



Interface Web des périphériques Axis

Configurer votre périphérique

Paramètres de base

Définir la fréquence de la ligne d'alimentation

1. Allez à Vidéo > Installation > Fréquence de la ligne d'alimentation.
2. Cliquez sur **Change (Modifier)**.
3. Sélectionnez une fréquence de la ligne d'alimentation et cliquez sur **Enregistrer et redémarrer**.

Définir le mode de capture

1. Accédez à Vidéo > Installation > Mode de capture.
2. Cliquez sur **Change (Modifier)**.
3. Sélectionnez un mode de capture et cliquez sur **Enregistrer et redémarrer**.
Voir aussi .

Régler l'image

Cette section fournit des instructions sur la configuration de votre périphérique. Pour en savoir plus sur certaines fonctions, accédez à .

Sélectionner le mode d'exposition

Pour améliorer la qualité d'image pour des scènes de surveillance spécifiques, utilisez des modes d'exposition. Les modes d'exposition vous permettent de contrôler l'ouverture, la vitesse d'obturation et le gain. Accédez à Vidéo > Image > Exposure (Vidéo > Image > Exposition) et sélectionnez l'un des modes d'exposition suivants :

- Dans la plupart des cas, sélectionnez le mode d'exposition **Automatic (Automatique)**.
- Pour les environnements avec des éclairages artificiels, par exemple un éclairage fluorescent, sélectionnez **Flicker-free (Sans clignotement)**.
Sélectionnez la même fréquence que la fréquence de la ligne d'alimentation.
- Pour les environnements avec des éclairages artificiels et vifs, par exemple des éclairages fluorescents en extérieur de nuit ou le soleil pendant la journée, sélectionnez **Flicker-reduced (Clignotement réduit)**.
Sélectionnez la même fréquence que la fréquence de la ligne d'alimentation.
- Pour verrouiller les paramètres d'exposition actuels, sélectionnez **Hold current (Conserver les paramètres actuels)**.

Optimiser l'éclairage IR

En fonction de l'environnement d'installation et des conditions autour de la caméra, par exemple des sources lumineuses externes dans la scène, vous pouvez parfois améliorer la qualité de l'image en réglant manuellement l'intensité des LED. Si vous avez des problèmes avec les reflets produits par les LED, vous pouvez essayer d'en réduire l'intensité.

1. Accédez à Vidéo > Image > Day-night mode (Mode jour-nuit).
2. Activez **Allow illumination (Autoriser l'éclairage)**.
3. Cliquez sur  dans la vidéo en direct et sélectionnez **Manual (Manuel)**.
4. Réglez l'intensité.

Bénéficier de l'illuminateur IR dans des conditions de faible luminosité avec le mode nocturne

Votre caméra utilise la lumière visible pour générer des images en couleur pendant la journée. Mais lorsque la lumière visible diminue, les images en couleur deviennent moins lumineuses et claires. Si vous basculez en mode nocturne lorsque cela se produit, la caméra utilise à la fois la lumière visible et la lumière infrarouge proche pour

fournir des images noir et blanc lumineuses et détaillées. Vous pouvez configurer la caméra pour qu'elle bascule en mode nocturne automatiquement.

1. Accédez à **Video > Image > Day-night mode (Vidéo > Image > Mode jour et nuit)** et assurez-vous que **IR cut filter (Masque IR)** est défini sur **Auto**.
2. Pour utiliser l'illuminateur IR intégré lorsque la caméra est en mode nocturne, activez **Autoriser l'éclairage** et **Synchroniser l'éclairage IR**.

Réduire le bruit dans des conditions de faible luminosité

Pour réduire le bruit dans des conditions de faible luminosité, vous pouvez ajuster les paramètres suivants :

- Ajustez le compromis entre le bruit et le flou de mouvement. Accédez à **Video > Image > Exposure (Vidéo > Image > Exposition)** et déplacez le curseur **Blur-noise trade-off (Compromis flou-bruit)** vers **Low noise (Bruit faible)**.
- Réglez le mode d'exposition sur **Automatique**.

Remarque

Une valeur maximale d'obturateur élevée peut générer des flous de mouvement.

- Pour ralentir la vitesse d'obturation, réglez **Obturateur max.** sur la valeur la plus élevée possible.

Remarque

Lorsque vous réduisez le gain maximal, l'image peut devenir plus sombre.

- Définissez le gain maximal sur une valeur inférieure.
- S'il existe un curseur **Aperture (Ouverture)**, déplacez-le vers **Open (Ouvert)**.
- Réduisez la netteté dans l'image sous **Vidéo > Image > Apparence**.

Réduire le flou de mouvement dans les conditions de faible luminosité

Pour réduire le flou de mouvement dans les conditions de faible luminosité, réglez un ou plusieurs des paramètres suivants dans **Video > Image > Exposure (Vidéo > Image > Exposition)** :

Remarque

Lorsque vous augmentez le gain, le bruit de l'image augmente également.

- Réglez **Max shutter (Exposition max)** sur une durée plus courte et **Max gain (Gain max)** sur une valeur plus élevée.

Si vous rencontrez encore des problèmes avec le flou de mouvement :

- Augmentez le niveau d'illumination dans la scène.
- Montez la caméra de sorte que les objets se déplacent vers elle ou s'éloignent d'elle plutôt d'aller sur les côtés.

Maximiser les détails dans une image

Important

Si vous maximisez les détails dans une image, le débit binaire augmentera probablement et vous obtiendrez peut-être une fréquence d'image réduite.

- Assurez-vous de sélectionner le mode de capture avec la résolution la plus élevée.
- Accédez à **Video > Stream > General (Vidéo > Flux > Général)** et définissez une compression aussi basse que possible.
- Sous l'image de la vidéo en direct, cliquez sur  et dans **Format vidéo**, sélectionnez **MJPEG**.
- Accédez à **Vidéo > Flux > Zipstream** et sélectionnez **Désactivé**.

Gérer les scènes avec un fort contre-jour

La plage dynamique est la différence des niveaux d'illumination dans une image. Dans certains cas, la différence entre les zones les plus sombres et les plus éclairées peut être significative. Le résultat est souvent une image où les zones sombres ou éclairées sont visibles. La plage dynamique étendue (WDR) rend visibles les zones éclairées et sombres dans l'image.



Image sans WDR.



Image avec WDR.

Remarque

- La fonction WDR peut provoquer des artefacts dans l'image.
 - La fonction WDR n'est peut-être pas disponible pour tous les modes de capture.
1. Accédez à **Video > Image > Wide dynamic range (Vidéo > Image > Plage dynamique étendue)**.
 2. Activez WDR.
 3. Utilisez le curseur **Local contrast (Contraste local)** pour ajuster le niveau de WDR.
 4. Si vous rencontrez encore des problèmes, accédez à **Exposure (Exposition)** et ajustez **Exposure zone (Zone d'exposition)** pour couvrir le domaine d'intérêt.

Découvrez-en plus sur la fonction WDR et son utilisation à l'adresse axis.com/web-articles/wdr.

Stabiliser une image tremblante avec la stabilisation d'image

La stabilisation d'image peut être utilisée dans les environnements où le produit est installé à un endroit exposé et soumis à des vibrations, par exemple, en plein vent ou à proximité d'une route au trafic intense.

Cette fonction rend l'image plus fluide, plus régulière et moins floue. Il réduit également la taille de fichier de l'image compressée et réduit le débit binaire du flux vidéo.

Remarque

Lorsque vous activez la stabilisation d'image, l'image est légèrement rognée, ce qui diminue la résolution maximale.

1. Accédez à **Vidéo > Installation > Correction de l'image**.
2. Activez la stabilisation de l'image.

Masquer des parties de l'image avec des masques de confidentialité

Vous pouvez créer un ou plusieurs masques de confidentialité pour masquer des parties de l'image.

1. Accédez à **Video (Vidéo) > Privacy masks (Masques de confidentialité)**.
2. Cliquez sur .
3. Cliquez sur le nouveau masque et saisissez un nom.
4. Réglez la taille et la position du masque de confidentialité en fonction de vos besoins.
5. Pour changer la couleur de tous les masques de confidentialité, cliquez sur **Privacy masks (Masques de confidentialité)** et sélectionnez une couleur.

Consultez aussi

Afficher une incrustation d'image

Vous pouvez ajouter une image en tant qu'incrustation dans le flux vidéo.

1. Allez à **Vidéo > Incrustations**.
2. Sélectionnez **Image** et cliquez sur .
3. Cliquez sur **Images**.
4. Glissez-déplacez une image.
5. Cliquez sur **Upload (Télécharger)**.
6. Cliquez sur **Gérer l'incrustation**.
7. Sélectionnez l'image et une position. Vous pouvez également faire glisser l'image en incrustation dans la vidéo en direct pour modifier la position.

Afficher la vidéo en direct du radar à l'image

Utilisez les commandes à l'écran pour visualiser la vidéo en direct et le radar dans le même flux.

1. Accédez à **Video > Image (Vidéo > Image)**.
2. Cliquez sur  dans la vidéo en direct pour accéder aux commandes à l'écran du produit.
3. Sélectionnez **Commandes prédéfinies**.
4. Activez **Radar Picture-in-Picture**.
5. Cliquez sur **Activer Picture-in-Picture**.
6. Pour modifier la taille de la projection radar, cliquez sur **Redimensionner Picture-in-Picture**.
7. Pour modifier la position de la projection radar, cliquez sur **Déplacer Picture-in-Picture**.

Ajouter les noms des rues et la direction de la boussole sur l'image

Remarque

Le nom de la rue et la direction de la boussole seront visibles sur tous les flux vidéo et les enregistrements.

1. Accédez à **Apps (Applications)**.
2. Sélectionnez **Axis-Orientation Aid (Aide à l'orientation Axis)**.
3. Cliquez sur **Ouvrir**.
4. Pour ajouter un nom de rue, cliquez sur **Add text (Ajouter du texte)** et modifiez le texte pour qu'il corresponde à la rue.
5. Pour ajouter une boussole, cliquez sur **Add compass (Ajouter une boussole)** et modifiez la boussole pour qu'elle corresponde à l'image.

Enregistrer et regarder la vidéo

Record video directly from the camera (Enregistrer une vidéo directement depuis la caméra)

1. Accédez à **Video > Image** (Vidéo > Image).

2. Pour commencer un enregistrement, cliquez sur .

Si vous n'avez configuré aucun stockage, cliquez sur  et sur . Pour obtenir des instructions sur la configuration du stockage réseau, consultez

3. Pour arrêter l'enregistrement, cliquez de nouveau sur .

Regarder la vidéo

1. Accédez à **Recordings** (Enregistrements).

2. Cliquez sur  en regard de votre enregistrement dans la liste.

Afficher et enregistrer la vidéo

Cette section fournit des instructions sur la configuration de votre périphérique. Pour en savoir plus sur le fonctionnement de la diffusion et du stockage, accédez à .

Réduire la bande passante et le stockage

Important

La réduction de la bande passante peut entraîner une perte de détails dans l'image.

1. Accédez à **Video > Stream** (Vidéo > Flux).

2. Cliquez sur  dans la vidéo en direct.

3. Sélectionnez **Video format (Format vidéo)** AV1 si votre périphérique le prend en charge. Sinon, sélectionnez H.264.

4. Accédez à **Video > Stream > General** (Vidéo > Flux > Général) et augmentez la valeur de **Compression**.

5. Accédez à **Vidéo > Flux > Zipstream** et procédez comme suit (une ou plusieurs fois) :

Remarque

Les paramètres de Zipstream sont utilisés pour tous les encodages vidéo à l'exception de MJPEG.

- Sélectionnez l'intensité de Zipstream à utiliser.
- Activez **Optimize for storage (Optimiser le stockage)**. Ce système ne peut être utilisé que si le logiciel de gestion vidéo prend en charge les images B.
- Activez l'option **Dynamic FPS (IPS dynamique)**.
- Activez l'option **Dynamic GOP (GOP dynamique)** et définissez une valeur de longueur de GOP **Upper limit (Limite supérieure)** élevée.

Remarque

La plupart des navigateurs Web ne prennent pas en charge le décodage H.265 et, de ce fait, le périphérique ne le prend pas en charge dans son interface Web. À la place, vous pouvez utiliser un système de gestion vidéo ou une application qui prend en charge le décodage H.265.

Configurer le stockage réseau

Pour stocker des enregistrements sur le réseau, vous devez configurer votre stockage réseau.

1. Accédez à **System (Système) > Storage (Stockage)**.

2. Cliquez sur  **Add network storage (Ajouter un stockage réseau)** sous **Network storage (Stockage réseau)**.

3. Saisissez l'adresse IP du serveur hôte.
4. Saisissez le nom de l'emplacement partagé sur le serveur hôte sous **Network Share (Partage réseau)**.
5. Saisissez le nom d'utilisateur et le mot de passe.
6. Sélectionnez la version SMB ou conservez **Auto**.
7. Sélectionnez **Ajouter un partage sans test** si vous rencontrez des problèmes de connexion temporaires, ou si le partage n'est pas encore configuré.
8. Cliquez sur **Ajouter**.

Configurer le radar

Remarque

La caméra de fusion radar-vidéo est calibrée en usine de sorte que la caméra et le module radar sont parfaitement alignés. Afin de ne pas annuler le calibrage et l'alignement, évitez de déplacer ou de retirer l'objectif, l'unité optique ou le module radar.

Sélectionner un profil de radar

Le radar de cette caméra de fusion radar-vidéo a deux profils : l'un est optimisé pour la surveillance de zone, et l'autre est optimisé pour la surveillance des routes. sélectionnez le profil adapté à votre type d'installation.

Dans l'interface web :

1. Accédez à **Radar > Paramètres > Détection**.
2. Sélectionnez un profil sous **Profils radar**.

Régler la hauteur de montage

Régler la hauteur de montage du périphérique dans l'interface web du radar. Cela permet au radar de détecter et de mesurer correctement la vitesse des objets qui passent.

Mesurez le plus précisément possible la hauteur entre le sol et le périphérique. Pour les scènes comportant des surfaces inégales, ajoutez la valeur qui représente la hauteur moyenne de la scène.

Remarque

Si la hauteur est définie de façon incorrecte, les zones de délimitation qui apparaissent dans **AXIS Object Analytics** en cas de détection d'un objet n'apparaissent pas dans la position précise.

1. Accédez à **Radar > Settings > General (Radar > Paramètres > Général)**.
2. Définissez la hauteur sous le paramètre **Mounting height (Hauteur de montage)**.

Vous pouvez également définir la hauteur de montage dans **AXIS Object Analytics**. Le réglage de la hauteur à un endroit permet de remplir automatiquement la hauteur de montage de l'autre.

1. Accédez à **Apps > AXIS Object Analytics (Applications > AXIS Object Analytics)**.
2. Activez l'application et cliquez sur **Ouvrir**.
3. Cliquez sur **Paramètres**.
4. Définissez la hauteur sous le paramètre **Mounting height (Hauteur de montage)**.

Valider la hauteur de montage

Pour valider que vous avez mesuré et réglé la bonne hauteur de montage du dispositif, ajoutez une incrustation enrichie dans la vidéo en direct de la caméra. L'incrustation consiste en des cadres de délimitation projetés autour des objets en mouvement.

1. Accédez à **Video > Image (Vidéo > Image)**.
2. Cliquez sur  dans la vidéo en direct pour accéder aux commandes à l'écran du dispositif.

3. Développez **Predefined controls (Commandes prédéfinies)**.
4. Activez **Augmented overlay (radar) (Incrustation augmentée (radar))**.
5. Cliquez sur **Toggle augmented bounding boxes (Activer/désactiver les zones de délimitation augmentées)**.
6. Demandez à quelqu'un de se déplacer dans la scène que vous surveillez et vérifiez dans la vidéo en direct de la caméra que le cadre de délimitation est projeté autour de l'objet en mouvement, et non au-dessus, au-dessous ou à côté.
7. Si nécessaire, mesurez à nouveau la hauteur de montage, ajustez les paramètres et revérifiez.

Désactivez l'incrustation augmentée une fois la validation terminée.

Remarque

Si la scène présente des variations d'altitude, utilisez la fonction d'étalonnage automatique pour améliorer la précision des cadres de délimitation d'après les détections radar. Pour en savoir plus, consultez .

Calibrez une carte de référence

Chargez une carte de référence pour faciliter la visualisation des déplacements des objets détectés. Vous pouvez utiliser un plan de mise à la terre ou une photo aérienne qui montre la zone couverte par le radar. Calibrez la carte pour que le champ de vision du radar corresponde à la position, à la direction et à l'échelle de la carte, et effectuez un zoom sur la carte si vous êtes intéressé(e) par une partie spécifique du champ de vision du radar.

Vous pouvez soit utiliser un assistant de configuration qui vous guide pas à pas dans le calibrage de la carte, soit modifier chaque paramètre individuellement.

Utilisez l'assistant de configuration :

1. Accédez à **Radar > Calibrage de la carte**.
2. Cliquez sur **Setup assistant (Assistant de configuration)** et suivez les instructions.

Pour supprimer la carte chargée et les paramètres que vous avez ajoutés, cliquez sur **Reset calibration (Réinitialiser le calibrage)**.

Edit each setting individually (Modifier chaque paramètre individuellement) :

La carte s'étalonnera progressivement après que vous ayez ajusté chaque paramètre.

1. Allez à **Radar > Map calibration (Calibrage de la carte) > Map (Carte)**.
2. Sélectionnez l'image que vous souhaitez charger ou glissez-déplacez-la dans la zone prévue à cet effet. Pour réutiliser une image de carte avec ses paramètres de panoramique et de zoom actuels, cliquez sur **Download map (Télécharger la carte)**.
3. Sous **Rotate map (Rotation de la carte)**, utilisez le curseur pour faire pivoter la carte en position.
4. Allez à **Scale and distance on a map (Échelle et distance sur une carte)** et cliquez sur deux points prédéterminés sur la carte.
5. Sous **Distance (Distance)**, ajoutez la distance réelle entre les deux points que vous avez ajoutés à la carte.
6. Allez à **Pan and zoom map (Carte panoramique et zoom)** et utilisez les boutons pour effectuer un panoramique sur l'image de la carte ou un zoom avant et arrière sur l'image de la carte.

Remarque

La fonction zoom ne modifie pas le champ de vision du radar. Même si certaines parties du champ de vision sont hors de vue après avoir effectué un zoom, le radar détectera toujours les objets en mouvement dans l'ensemble du champ de vision. La seule façon d'exclure les mouvements détectés est d'ajouter des zones d'exclusion. Pour en savoir plus, consultez .

7. Allez à **Radar position (Position du radar)** et utilisez les boutons pour déplacer ou faire pivoter la position du radar sur la carte.

Pour supprimer la carte chargée et les paramètres que vous avez ajoutés, cliquez sur **Reset calibration (Réinitialiser le calibrage)**.



La vidéo montre un exemple d'étalonnage d'une carte de référence dans un radar Axis ou une caméra combinée radar-vidéo.

Définir des zones de détection

Pour déterminer où détecter les mouvements, vous pouvez ajouter une ou plusieurs zones de détection. Utilisez différentes zones pour déclencher différentes actions.

Il existe deux types de zones :

- Un **scénario** (anciennement « zone à inclure ») est une zone dans laquelle les objets en mouvement déclenchent des règles. Le scénario par défaut correspond à l'ensemble du champ de vision du radar.
- Une **exclude zone (zone à exclure)** est une zone dans laquelle les objets en mouvement sont ignorés. Utilisez des zones à exclure s'il existe des zones à l'intérieur d'un scénario qui déclenchent un grand nombre d'alarmes indésirables.

Ajouter des scénarios

Un scénario combine des conditions de déclenchement et des paramètres de détection qui vous permettent de créer des règles dans le système d'événement. Ajoutez des scénarios pour créer différentes règles correspondant aux différentes parties de la scène.

Pour ajouter un scénario :

1. Accédez à **Radar > Scenarios (Radar > Scénarios)**.
2. Cliquez sur **Ajouter un scénario**.
3. Saisissez le nom du scénario.
4. Indiquez si vous souhaitez déclencher un événement sur des objets se déplaçant dans une zone ou des objets franchissant une ou deux lignes.

Pour déclencher un événement sur des objets en mouvement dans une zone :

1. Sélectionnez **Mouvement dans la zone**.
2. Cliquez sur **Next (Suivant)**.
3. Sélectionnez le type de zone à inclure dans le scénario.
Utilisez la souris pour déplacer et définir la zone afin qu'elle couvre la partie souhaitée de l'image radar ou de la carte de référence.
4. Cliquez sur **Next (Suivant)**.
5. Ajoutez des paramètres de détection.
1. Ajoutez des secondes jusqu'à ce que le déclencheur se déclenche après sous **Ignorer les objets de courte durée**.
2. Sélectionnez le type d'objet sur lequel il doit se déclencher sous **Déclencheur sur type d'objet**.
3. Ajoutez une plage pour la limite de vitesse sous **Speed limit (Limite de vitesse)**.
6. Cliquez sur **Next (Suivant)**.
7. Définissez la durée minimale de l'alarme sous **la durée minimale du déclenchement**.
8. Cliquez sur **Save (Enregistrer)**.

Pour déclencher un événement sur des objets franchissant une ligne :

1. Sélectionnez **Line crossing (Franchissement de la ligne)**.
2. Cliquez sur **Next (Suivant)**.

3. Positionnez la ligne dans la scène.
Utilisez la souris pour déplacer et définir la ligne.
4. Pour modifier le sens de la détection, activez **Change direction (Changer de direction)**.
5. Cliquez sur **Next (Suivant)**.
6. Ajoutez des paramètres de détection.
 - 6.1. Ajoutez des secondes jusqu'à ce que le déclencheur se déclenche après sous **Ignorer les objets de courte durée**.
 - 6.2. Sélectionnez le type d'objet sur lequel il doit se déclencher sous **Déclencheur sur type d'objet**.
 - 6.3. Ajoutez une plage pour la limite de vitesse sous **Speed limit (Limite de vitesse)**.
7. Cliquez sur **Next (Suivant)**.
8. Définissez la durée minimale de l'alarme sous **la durée minimale du déclenchement**.
La valeur par défaut est définie sur 2 secondes. Si vous souhaitez que le scénario se déclenche à chaque fois qu'un objet traverse la ligne, réduisez la durée à 0 seconde.
9. Cliquez sur **Save (Enregistrer)**.

Pour déclencher un événement sur des objets franchissant deux lignes :

1. Sélectionnez **Line crossing (Franchissement de la ligne)**.
2. Cliquez sur **Next (Suivant)**.
3. Pour que l'objet traverse deux lignes de sorte que l'alarme se déclenche, activez **Require crossing of two lines (Exiger le franchissement de deux lignes)**.
4. Positionnez les lignes dans la scène.
Utilisez la souris pour déplacer et définir la ligne.
5. Pour modifier le sens de la détection, activez **Change direction (Changer de direction)**.
6. Cliquez sur **Next (Suivant)**.
7. Ajoutez des paramètres de détection.
 - 7.1. Définissez la limite de temps entre le franchissement de la première et de la deuxième ligne sous **Max time between crossings (Temps max. entre les franchissements)**.
 - 7.2. Sélectionnez le type d'objet sur lequel il doit se déclencher sous **Déclencheur sur type d'objet**.
 - 7.3. Ajoutez une plage pour la limite de vitesse sous **Speed limit (Limite de vitesse)**.
8. Cliquez sur **Next (Suivant)**.
9. Définissez la durée minimale de l'alarme sous **la durée minimale du déclenchement**.
La valeur par défaut est définie sur 2 secondes. Si vous souhaitez que le scénario se déclenche à chaque fois qu'un objet a traversé les deux lignes réduisez la durée à 0 seconde.
10. Cliquez sur **Save (Enregistrer)**.

Ajouter des zones d'exclusion

Les zones d'exclusion comprennent des objets en mouvement qui sont ignorés. Ajoutez des zones d'exclusion pour ignorer, par exemple, les feuillages ondulants au bord d'une route. Vous pouvez également ajouter des zones d'exclusion pour ignorer les traces fantômes générées par des matériaux réfléchissant les ondes radar (une clôture métallique, par exemple).

Pour ajouter une zone à exclure :

1. Accédez à **Radar > Exclude zones (Radar > Zones d'exclusion)**.
2. Cliquez sur **Add exclude zone (Ajouter une zone d'exclusion)**.
Utilisez la souris pour déplacer et définir la zone afin qu'elle couvre la partie souhaitée de la vue radar ou de la carte de référence.

Calibrer automatiquement le périphérique

Le calibrage automatique de la caméra de fusion radar-vidéo améliore la précision des matrices de caractères qui apparaissent autour des objets détectés dans AXIS Object Analytics. Avec le calibrage automatique, le périphérique utilise des informations de la vidéo, comme la hauteur et la précision angulaire, pour améliorer le positionnement des matrices de caractères en fonction des détections radar.

Remarque

Le calibrage automatique n'affecte pas les détections ; il a uniquement un impact sur la visualisation des matrices de caractères.

Pour calibrer la hauteur :

1. Allez à **Radar > autocalibration > elevation (Radar > Calibrage automatique > Hauteur)**.
2. Activer l'option **Autocalibration (Calibrage automatique)**.
Le calibrage automatique est effectué lorsque les données de calibrage sont disponibles.
3. Sélectionnez une option de lissage (**Smoothing**).
 - Si votre scène présente peu de différences de hauteur, laissez l'option **Smoothing (Lissage)** définie sur **High (Élevé)**.
 - Si votre scène est vallonnée ou en pente, ou si elle contient des escaliers ou des bâtiments de grande hauteur, définissez **Smoothing (Lissage)** sur **Low (Faible)** pour maintenir les différences de hauteur.
4. Visualisez le résultat du calibrage dans l'interface Web à l'aide des options suivantes :
 - **Show elevation pattern (Afficher la configuration de la hauteur)** indique la distance verticale entre le sol et la caméra dans un modèle de points colorés.
 - **Show color legend (Afficher la légende des couleurs)** affiche une légende contenant les couleurs du modèle de hauteur et la distance verticale que représente chaque couleur.
 - **Show reference area (Afficher la zone de référence)** indique la zone sur laquelle repose le calibrage.

Pour le calibrage de l'azimut :

1. Allez à **Radar > Autocalibration > Azimuth (Radar > Calibrage automatique > Azimut)**.
2. Activer l'option **Autocalibration (Calibrage automatique)**.
Le calibrage automatique est effectué lorsque les données de calibrage sont disponibles.

Afficher une incrustation de texte avec l'angle d'inclinaison du radar

Vous pouvez ajouter une incrustation dans la vidéo en direct du radar qui indique l'angle d'inclinaison du radar. Elle s'avère utile dans le cadre de l'installation ou lorsque vous devez connaître l'angle d'inclinaison du périphérique.

Remarque

L'incrustation de l'angle d'inclinaison affiche la valeur « 90 » lorsque le périphérique est horizontal. Si la valeur indiquée dans l'incrustation est « 75 », l'angle d'inclinaison du radar est de 15° sous de la ligne d'horizon.

1. Accédez à **Radar > Incrustations**.
2. Sélectionnez **Text (Texte)** et cliquez sur **+**.
3. Saisissez **#op**.
Vous pouvez également cliquer sur **Modificateur** et sélectionner **#op** dans la liste.
4. Sélectionnez une position. Vous pouvez également faire glisser le champ d'incrustation dans la vidéo en direct pour modifier la position.

Configurer AXIS Object Analytics

AXIS Object Analytics est une application basée sur l'IA qui détecte et classe les objets en mouvement. C'est également l'interface principale pour configurer la fusion radar-vidéo dans le dispositif AXIS Q1656-DLE. La sortie en temps réel de la fusion est visible uniquement dans le flux vidéo faisant partie d'un scénario configuré dans l'application.

Créez un scénario

Utilisez des scénarios dans AXIS Object Analytics pour définir les paramètres de détection et les conditions de déclenchement de votre caméra de fusion radar-vidéo.

1. Dans l'interface Web du périphérique, allez à **Apps > AXIS Object Analytics**.
2. Lancez l'application et cliquez sur **Open (Ouvrir)**.
3. Dans l'écran d'accueil, cliquez sur **Pas à pas** et suivez la procédure de configuration recommandée.
4. Dans **Considérations**, lisez les informations et cliquez sur **Terminer**.
5. Cliquez sur **+ Nouveau scénario**.

Remarque

Par défaut, les scénarios **Objet dans la zone** et **Franchissement de ligne** utilisent à la fois l'entrée vidéo et l'entrée radar. Les autres scénarios de AXIS Object Analytics utilisent uniquement l'entrée vidéo.

6. Sélectionnez un scénario en fonction de vos besoins.
7. Sélectionnez le type d'objet que vous souhaitez que l'application détecte.
8. Configurez votre scénario.
9. Vérifiez vos paramètres, puis cliquez sur **Terminer**.

Remarque

Pour obtenir des matrices de caractère autour des objets en mouvement, allez à **Settings (Paramètres)** et activez **Metadata overlay (Incrustation de métadonnées)**. Lorsque vous créez deux scénarios, dont l'un utilise à la fois l'entrée vidéo et l'entrée radar et l'autre uniquement l'entrée vidéo, l'objet en mouvement sera entouré par deux matrices de caractères. Ce comportement est attendu.

Vous avez créé un scénario dans AXIS Object Analytics. Pour modifier le scénario et appliquer des paramètres supplémentaires, cliquez sur **Ouvrir**. Pour les scénarios qui utilisent à la fois une entrée radar et une entrée vidéo, vous pouvez utiliser la vitesse pour déclencher et sélectionner une sensibilité de détection. Pour plus d'instructions, consultez :

-
-

Pour en savoir plus sur AXIS Object Analytics et ses paramètres généraux, consultez le manuel d'utilisation *AXIS Object Analytics*.

Remarque

Certaines des considérations et fonctions décrites dans le manuel d'utilisation AXIS Object Analytics ne s'appliquent pas aux caméras de fusion radar-vidéo.

Utiliser la vitesse pour le déclenchement

Si vous avez créé un scénario **Objet dans la zone** ou **Franchissement de ligne** dans AXIS Object Analytics, vous pouvez déclencher un scénario sur des objets en mouvement à des vitesses comprises dans une plage définie (ou une plage supérieure ou inférieure).

1. Accédez à **Apps > AXIS Object Analytics (Applications > AXIS Object Analytics)**.
2. Lancez l'application et cliquez sur **Open (Ouvrir)**.
3. Sélectionnez le scénario à modifier et cliquez sur **Open (Ouvrir)**.

4. Accédez à la **Object speed (Vitesse de l'objet)** et activez **Use speed to trigger (Utiliser la vitesse pour le déclenchement)**.
5. Définissez la plage de vitesses pour laquelle déclencher un scénario.
6. Pour déclencher un scénario sur des vitesses supérieures et inférieures à la plage que vous avez définie, cliquez sur **Invert (Inverser)**.

Sélectionner la sensibilité de détection

Le choix de la sensibilité de détection permet de décider si vous souhaitez déclencher un événement sur des détections assurées par la vidéo ou le radar, ou les détections effectuées par les deux. Vous pouvez également laisser le périphérique lui-même, en fonction des algorithmes de fusion, décider s'il doit s'appuyer sur l'une des deux technologies, ou les deux.

Cette option est disponible dans les scénarios **Objet dans la zone** et **Franchissement de ligne**.

1. Accédez à **Apps > AXIS Object Analytics (Applications > AXIS Object Analytics)**.
2. Lancez l'application et cliquez sur **Open (Ouvrir)**.
3. Sélectionnez le scénario à modifier et cliquez sur **Open (Ouvrir)**.
4. Accédez à **Detection sensitivity (Sensibilité de détection)** et sélectionnez l'une des options suivantes :
 - **Sensibilité faible:** Il faut que le radar et la caméra détectent l'objet. Cela réduit le risque de fausses alarmes, mais augmente le risque de détections manquées. Pour être certain que les objets peuvent être détectés par les deux technologies, il faut que la scène ne soit pas trop complexe. Les conditions d'éclairage doivent être bonnes, la zone de détection doit se situer dans la plage de détection des deux technologies, et l'absence d'éléments perturbateurs, tels que des arbres ou des buissons, est préférable.
 - **Automatic (Automatique) :** Permet à l'application de décider si le radar et la caméra ou un seul d'entre eux sont requis pour détecter l'objet. Il s'agit de l'option par défaut.
 - **Sensibilité élevée:** Il faut que le radar ou la caméra détecte l'objet. Cela augmente le risque de fausses alarmes, mais réduit le risque de détections manquées. Les conditions d'éclairage et la taille de la zone de détection sont moins importantes lorsque vous sélectionnez une sensibilité élevée, car vous n'avez besoin que de l'une des technologies pour détecter l'objet.

Remarque

Vous pouvez améliorer la précision des matrices de caractères qui apparaissent autour des objets détectés dans AXIS Object Analytics grâce à la fonction de calibrage automatique. Le calibrage automatique n'affecte pas les détections ; il a uniquement un impact sur la visualisation des matrices de caractères.

Pour en savoir plus, consultez .

Réduire les fausses alarmes

Si vous obtenez trop de fausses alarmes, vous pouvez filtrer certains types de mouvements ou d'objets, modifier la couverture ou régler la sensibilité de détection. Étudiez les paramètres les mieux adaptés à votre environnement.

- Réglez la sensibilité de détection de l'application AXIS Object Analytics : Accédez à **Applications > AXIS Object Analytics**, ouvrez un scénario et sélectionnez une **sensibilité de détection** inférieure.
 - **Sensibilité faible:** Il faut que le radar et la caméra détectent l'objet. Réduction du risque de fausses alarmes, mais risque accru de détections manquées.
 - **Automatic (Automatique) :** Permet à l'application de décider si le radar et la caméra ou un seul d'entre eux sont requis pour détecter l'objet.
 - **Sensibilité élevée:** Il faut que le radar ou la caméra détecte l'objet. Risque accru de fausses alarmes mais risque réduit de détections manquées.
- Réglage de la sensibilité de détection du radar :

Accédez à **Radar > Paramètres > Détection** et sélectionnez une **Sensibilité de détection** inférieure. Cela diminue le risque de fausses alarmes, mais peut également faire manquer des mouvements au radar.

- **Faible** : Utilisez cette sensibilité en présence d'un grand nombre d'objets métalliques ou de gros véhicules dans la zone. Le radar prendra plus de temps pour suivre et classer les objets. Cela peut réduire la portée de détection, en particulier pour les objets qui se déplacent rapidement.
- **Moyenne** : Ce sont les paramètres par défaut.
- **Élevée** : Utilisez cette sensibilité en présence d'un champ ouvert sans objets métalliques devant le radar. Cela augmente la portée de détection des êtres humains.
- **Modification des scénarios et des zones d'exclusion** :
Si un scénario inclut des surfaces dures, comme une paroi métallique, il peut y avoir des réflexions qui causent plusieurs détections pour un seul objet physique. Vous pouvez soit modifier la forme du scénario, soit ajouter une zone d'exclusion qui ignore certaines parties du scénario. Pour en savoir plus, consultez et .
- **Déclencher sur des objets traversant deux lignes au lieu d'une** :
Si un scénario de franchissement de ligne inclut des objets ondulants ou des animaux qui se déplacent, il existe un risque qu'un objet passe la ligne et déclenche une fausse alarme. Dans ce cas, vous pouvez configurer le scénario de déclenchement uniquement lorsqu'un objet a traversé deux lignes. Pour en savoir plus, consultez .
- **Filtrer sur mouvement** :
 - Accédez à **Radar > Paramètres > Détection** et sélectionnez **Ignorer les objets ondulants**. Ce paramètre réduit les fausses alarmes déclenchées par les arbres, les buissons et les mâts dans la zone de couverture.
 - Accédez à **Radar > Settings > Detection (Radar > Paramètres > Détection)** et sélectionnez **Ignore swaying objects (Ignorer les petits objets)**. Ce paramètre minimise les fausses alarmes en cas de présence de petits objets dans la zone de couverture (chats et lapins, par exemple).
- **Filtrer sur temps** :
 - Accédez à **Radar > Scenarios (Radar > Scénarios)**.
 - Sélectionnez un scénario, puis cliquez sur  pour modifier ses paramètres.
 - Sélectionnez une valeur supérieure en **Secondes jusqu'au déclenchement**. Il s'agit du délai entre le moment où le radar commence à suivre un objet et celui où il peut déclencher une alarme. Le minuteur démarre lorsque le radar détecte la première fois l'objet, non quand l'objet pénètre dans la zone spécifiée dans le scénario.
- **Filtrer sur type d'objet** :
 - Accédez à **Radar > Scenarios (Radar > Scénarios)**.
 - Sélectionnez un scénario, puis cliquez sur  pour modifier ses paramètres.
 - Pour éviter les déclenchements sur des types d'objets spécifiques, désélectionnez les types d'objets qui ne doivent pas déclencher d'événements dans ce scénario.

Remarque

Le réglage du type d'objet n'affecte que le radar. Il est ignoré par AXIS Object Analytics.

Définir des règles pour les événements

Pour plus d'informations, consultez notre guide *Premiers pas avec les règles pour les événements*.

Économiser l'énergie lorsqu'aucun mouvement est détecté

Cet exemple explique comment activer le mode d'économie d'énergie lorsqu'aucun mouvement n'est détecté dans la scène.

Remarque

Lorsque vous activez le mode économie d'énergie, la plage d'éclairage infrarouge est réduite.

Assurez-vous que AXIS Object Analytics est en cours d'exécution :

1. Accédez à **Apps > AXIS Object Analytics (Applications > AXIS Object Analytics)**.
2. Démarrez l'application si elle n'est pas déjà en cours d'exécution.
3. Assurez-vous d'avoir configuré l'application en fonction de vos besoins.

Créez une règle :

1. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sous **Application**, sélectionnez **Object Analytics**.
4. Sélectionnez **Invert this condition (Inverser cette condition)**.
5. Dans la liste des actions, sous **Power saving mode (Mode d'économie d'énergie)**, sélectionnez **Use power saving mode while the rule is active (Utiliser le mode d'économie d'énergie pendant que la règle est active)**.
6. Cliquez sur **Save (Enregistrer)**.

Déclencher une alarme si une personne ouvre l'enceinte

Cet exemple explique comment déclencher une alarme si quelqu'un ouvre l'enceinte ou le boîtier du périphérique.

Ajouter un destinataire :

1. Accédez à **System > Events > Recipients (Système > Événements > Destinataires)** et cliquez sur **Add recipient (Ajouter un destinataire)**.
2. Entrez le nom du destinataire de l'e-mail.
3. Sélectionnez **Email (E-mail)**.
4. Entrez l'adresse e-mail à laquelle envoyer l'e-mail.
5. La caméra ne dispose pas de son propre serveur de messagerie, elle devra donc se connecter à un autre serveur de messagerie pour pouvoir envoyer des messages. Remplissez le reste des informations en fonction de votre fournisseur d'e-mail.
6. Pour envoyer un e-mail de test, cliquez sur **Test**.
7. Cliquez sur **Save (Enregistrer)**.

Créez une règle :

8. Accédez à **System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
9. Saisissez le nom de la règle.
10. Dans la liste des conditions, sélectionnez **Casing open (Boîtier ouvert)**.
11. Dans la liste des actions, sélectionnez **Send notification to email (Envoyer la notification par e-mail)**.
12. Sélectionnez un destinataire de la liste.
13. Saisissez un objet et un message pour l'e-mail.
14. Cliquez sur **Save (Enregistrer)**.

Envoyer un e-mail si le radar est recouvert d'un objet métallique

Cet exemple explique comment créer une règle de notification par e-mail si quelqu'un altère le fonctionnement du radar en le couvrant d'un objet métallique (feuille ou plaque métallique, par exemple).

Remarque

L'option de création de règles en cas de sabotage du radar est proposée à partir de la version d'AXIS OS 11.11.

Ajouter un destinataire d'e-mails :

1. Accédez à **System > Events > Recipients (Système > Événements > Destinataires)** et cliquez sur **Add recipient (Ajouter un destinataire)**.
2. Entrez le nom du destinataire de l'e-mail.
3. Sélectionnez **Email (E-mail)**.
4. Entrez l'adresse e-mail à laquelle envoyer l'e-mail.
5. La caméra ne dispose pas de son propre serveur de messagerie, elle devra donc se connecter à un autre serveur de messagerie pour pouvoir envoyer des messages. Remplissez le reste des informations en fonction de votre fournisseur d'e-mail.
6. Pour envoyer un e-mail de test, cliquez sur **Test**.
7. Cliquez sur **Save (Enregistrer)**.

Créez une règle :

8. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
9. Saisissez le nom de la règle.
10. Dans la liste des conditions, sous **Device status (État du périphérique)**, sélectionnez **Radar data failure (Échec des données radar)**.
11. Sous **Reason (Raison)**, sélectionnez **Tampering (Sabotage)**.
12. Dans la liste des actions, sous **Notifications**, sélectionnez **Send notification to email (Envoyer une notification par e-mail)**.
13. Sélectionnez le destinataire que vous avez créé.
14. Saisissez un objet et un message pour l'e-mail.
15. Cliquez sur **Save (Enregistrer)**.

Contrôler une caméra PTZ avec le radar

Il est possible d'utiliser les informations du radar sur la position des objets pour qu'une caméra PTZ suive des objets. Cela peut être effectué de deux façons :

- . L'option intégrée est adaptée lorsqu'une caméra PTZ et un radar sont montés très près l'un de l'autre.
- . L'application Windows est idéale si vous souhaitez utiliser plusieurs caméras PTZ et radars pour le suivi des objets.

Remarque

Utilisez un serveur NTP pour synchroniser l'heure sur les caméras et l'ordinateur Windows. Si les horloges sont désynchronisées, vous pouvez observer des retards dans le suivi ou un suivi fantôme.

Contrôler une caméra PTZ à l'aide du service intégré de suivi automatique du radar

Le service intégré de suivi automatique du radar crée une solution bord à bord où le radar contrôle directement la caméra PTZ. Il est compatible avec toutes les caméras PTZ d'Axis.

Remarque

Vous pouvez utiliser le service intégré de suivi automatique du radar pour connecter un radar à une caméra PTZ. Pour une configuration avec plusieurs radars ou caméras PTZ, utilisez **AXIS Radar Autotracking for PTZ**. Pour plus d'informations, consultez la section .

Ces instructions portent sur le couplage du radar avec une caméra PTZ, le calibrage des deux dispositifs et la configuration du suivi des objets.

Avant de commencer :

- Définissez la zone d'intérêt et évitez les alarmes intempestives en configurant des zones à exclure dans le radar. Veillez à exclure les zones comportant des matériaux réfléchissant le signal radar ou des objets

ondulants, comme le feuillage, afin d'éviter que la caméra PTZ ne suive des objets non pertinents. Pour des instructions, voir .

Pour appairer le radar à la caméra PTZ, procédez comme suit :

1. Accédez à **Système > Bord à bord > Appairage PTZ**.
2. Saisissez l'adresse IP, le nom d'utilisateur et le mot de passe de la caméra PTZ.
3. Cliquez sur **Connect (Connecter)**.
4. Cliquez sur **Configure Radar autotracking (Configurer le suivi automatique du radar)** ou accédez à **Radar > Radar PTZ autotracking (Radar > Suivi automatique du radar)** pour configurer le suivi automatique du radar.

Pour calibrer le radar et la caméra PTZ, procédez comme suit :

5. Accédez à **Radar > Radar PTZ autotracking (Radar > Suivi automatique du radar)**.
6. Pour définir la hauteur de montage de la caméra, accédez à **Camera mounting height (Hauteur de montage de la caméra)**.
7. Pour effectuer un panoramique avec la caméra PTZ de sorte qu'elle pointe dans la même direction que le radar, accédez à **Pan alignment (Alignement panoramique)**.
8. Si vous devez ajuster l'inclinaison pour compenser la déclivité d'un terrain en pente, accédez à **Ground incline offset (Décalage de l'inclinaison du sol)** et ajoutez une valeur de décalage en degrés.

Pour configurer le suivi PTZ, procédez comme suit :

9. Accédez à **Track (Suivre)** et sélectionnez cette option si vous souhaitez suivre des personnes, des véhicules et/ou des objets inconnus.
10. Pour commencer à suivre des objets avec la caméra PTZ, activez la fonction **Tracking (Suivi)**. Le suivi zoome automatiquement sur un objet ou un groupe d'objets pour les garder dans la vue de la caméra.
11. Activez la fonction **Changement d'objet** si vous prévoyez que plusieurs objets ne rentrent pas dans la vue de la caméra. Grâce à ce réglage, le radar donne la priorité aux objets à suivre.
12. Pour déterminer le nombre de secondes pendant lesquelles chaque objet doit être suivi, définissez la **durée de maintien de l'objet**.
13. Si vous souhaitez que la caméra PTZ revienne à sa position initiale lorsque le radar ne suit plus aucun objet, activez la fonction **Revenir à l'accueil**.
14. Pour déterminer le temps de pause de la caméra PTZ sur la dernière position connue des objets suivis avant le retour à la position initiale, définissez le **délai d'expiration du retour à l'accueil**.
15. Pour ajuster le zoom de la caméra PTZ, réglez le zoom sur le curseur.

Contrôler une caméra PTZ avec AXIS Radar Autotracking for PTZ

Basée sur serveur, la solution AXIS Radar Autotracking for PTZ est capable de gérer différentes configurations dans le cadre du suivi d'objets :

- Contrôlez plusieurs caméras PTZ avec un radar.
- Contrôlez une caméra PTZ avec plusieurs radars.
- Contrôlez plusieurs caméras PTZ avec plusieurs radars.
- Contrôlez une caméra PTZ avec un radar lorsqu'ils sont montés dans différentes positions couvrant la même zone.

L'application est compatible avec un ensemble spécifique de caméras PTZ. Pour plus d'informations, consultez la page axis.com/products/axis-radar-autotracking-for-ptz#compatible-products.

Téléchargez l'application et reportez-vous au manuel d'utilisation pour en savoir plus sur la configuration de l'application. Pour plus d'informations, consultez la page axis.com/products/axis-radar-autotracking-for-ptz/support.

Utiliser MQTT pour envoyer des données radar

Utilisez la caméra de fusion radar-vidéo avec l'application AXIS Speed Monitor pour collecter des données radar pour les objets détectés et les transmettre via MQTT.

Cet exemple explique comment configurer un client MQTT sur le périphérique où vous avez installé AXIS Speed Monitor, et comment créer une condition de publication des données radar recueillies dans AXIS Speed Monitor en tant que charge utile pour un courtier MQTT.

Avant de commencer :

- Installez AXIS Speed Monitor dans votre caméra de fusion radar-vidéo, ou installez-la dans une caméra que vous connectez au radar de la caméra de fusion radar-vidéo.
Pour plus d'informations, consultez le *manuel d'utilisation d'AXIS Speed Monitor*.
- Définissez un courtier MQTT et obtenez son adresse IP, son nom d'utilisateur et son mot de passe.
Pour en savoir plus sur MQTT et les courtiers MQTT, consultez *AXIS OS Knowledge Base*.

Pour configurer le client MQTT dans l'interface Web du périphérique sur laquelle AXIS Speed Monitor est installé :

1. Allez à **Système > MQTT > Client MQTT > Courtier** et saisissez les informations suivantes :
 - **Hôte** : l'adresse IP du courtier
 - **Client ID** (ID du client) : Identifiant du dispositif
 - **Protocol (Protocole)** : protocole sur lequel le courtier est défini
 - **Port** : numéro de port utilisé par le courtier
 - **Username (Nom d'utilisateur)** et **Password (Mot de passe)** du courtier
2. Cliquez sur **Save (Enregistrer)** et **Connect (Connecter)**.

Créez une condition de publication des données radar en tant que charge utile pour le courtier MQTT :

3. Accédez à **Système > MQTT > Publication MQTT** et cliquez sur **+ Ajouter condition**.
4. Dans la liste des conditions, sous **Application**, sélectionnez **Speed Monitor : Track exited zone** (Moniteur de vitesse : Suivi de la sortie de zone).

Désormais, le périphérique peut envoyer des informations sur les suivis radar pour chaque objet en mouvement qui sort d'un scénario. Chaque objet possède ses propres paramètres de suivi radar, par exemple `rmd_zone_name`, `tracking_id`, et `trigger_count`. Vous trouverez la liste complète des paramètres dans le *manuel d'utilisation d'AXIS Speed Monitor*.

Enregistrer une vidéo lorsque la caméra détecte un objet

Cet exemple explique comment configurer la caméra pour démarrer l'enregistrement sur la carte SD lorsque la caméra détecte un objet. L'enregistrement inclut cinq secondes avant la détection et une minute après la fin de la détection.

Avant de commencer :

- Assurez-vous d'avoir une carte SD installée.

Assurez-vous que AXIS Object Analytics est en cours d'exécution :

1. Accédez à **Apps > AXIS Object Analytics (Applications > AXIS Object Analytics)**.
2. Démarrez l'application si elle n'est pas déjà en cours d'exécution.
3. Assurez-vous d'avoir configuré l'application en fonction de vos besoins.

Créez une règle :

1. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sous **Application**, sélectionnez **Object Analytics**.
4. Dans la liste des actions, sous **Recordings (Enregistrements)**, sélectionnez **Record video while the rule is active (Enregistrer la vidéo tant que la règle est active)**.

5. Dans la liste des options de stockage, sélectionnez **SD_DISK (DISQUE_SD)**.
6. Sélectionnez une caméra et un profil de flux.
7. Réglez la durée pré-buffer sur 5 secondes.
8. Réglez la durée post-tampon sur 1 minute.
9. Cliquez sur **Save (Enregistrer)**.

Fournir une indication visuelle d'un événement en cours

Vous avez la possibilité de connecter AXIS I/O Indication LED à votre caméra réseau. Cette LED peut être configurée pour s'allumer lorsque certains événements se produisent dans la caméra. Par exemple, pour informer les personnes qu'un enregistrement vidéo est en cours.

Matériel requis

- AXIS I/O Indication LED
- Une caméra vidéo sur IP Axis

Remarque

Pour obtenir des instructions sur le raccordement d'AXIS I/O Indication LED, consultez le guide d'installation fourni avec le produit.

L'exemple suivant montre comment configurer une règle qui allume AXIS I/O Indication LED pour indiquer que la caméra enregistre.

1. Accédez **System > Accessories > I/O ports (Système > Accessoires > Port d'E/S)**.
2. Pour le port sur lequel vous avez raccordé le AXIS I/O Indication LED, cliquez sur  pour régler la direction sur **Output (Sortie)**, puis cliquez sur  pour régler le statut normal sur **Circuit open (Circuit ouvert)**.
3. Accédez à **System > Events (Système > Événements)**.
4. Créez une nouvelle règle.
5. Sélectionnez la **Condition** qui doit être satisfaite pour déclencher le démarrage de l'enregistrement par la caméra. Cela peut, par exemple, être un programme ou une détection de mouvement.
6. Dans la liste des actions, sélectionnez **Record video (Enregistrer la vidéo)**. Sélectionnez un espace de stockage. Sélectionnez un profil de flux ou créez-en un nouveau. Configurez également le **Prebuffer (Pré-tampon)** et le **Postbuffer (Post-tampon)** selon le besoin.
7. Sauvegardez la règle.
8. Créez une deuxième règle et sélectionnez la même **Condition** que dans la première règle.
9. Dans la liste des actions, sélectionnez **Toggle I/O while the rule is active (Basculer l'E/S tant que la règle est active)**, puis sélectionnez le port sur lequel AXIS I/O Indication LED est raccordé. Réglez l'état sur **Active (Actif)**.
10. Sauvegardez la règle.

D'autres scénarios où AXIS I/O Indication LED peut être utilisé sont, par exemple :

- Configurez la LED pour qu'elle s'allume lorsque la caméra démarre, afin d'indiquer la présence de la caméra. Sélectionnez **System ready (Système prêt)** comme condition.
- Configurez la LED pour qu'elle s'allume lorsque le flux de données en direct est actif afin d'indiquer qu'une personne ou un programme accède à un flux de données provenant de la caméra. Sélectionnez **Live stream accessed (Accès au flux de données en direct)** comme condition.

Afficher une incrustation de texte dans le flux vidéo lorsque le périphérique détecte un objet

Cet exemple explique comment afficher le texte « Mouvement détecté » lorsque le périphérique détecte un objet.

Assurez-vous que AXIS Object Analytics est en cours d'exécution :

1. Accédez à **Apps > AXIS Object Analytics (Applications > AXIS Object Analytics)**.
2. Démarrez l'application si elle n'est pas déjà en cours d'exécution.
3. Assurez-vous d'avoir configuré l'application en fonction de vos besoins.

Ajoutez l'incrustation de texte :

1. Allez à **Vidéo > Incrustations**.
2. Sous **Overlays (Incrustations)**, sélectionnez **Text (Texte)** et cliquez sur **+**.
3. Saisissez #D dans le champ de texte.
4. Choisissez la taille et l'apparence du texte.
5. Pour positionner l'incrustation de texte, cliquez sur  et sélectionnez une option.

Créez une règle :

1. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sous **Application**, sélectionnez **Object Analytics**.
4. Dans la liste des actions, sous **Overlay text (Texte d'incrustation)**, sélectionnez **Use overlay text (Utiliser le texte d'incrustation)**.
5. Sélectionner un canal vidéo.
6. Dans **Text (Texte)**, saisissez « Motion detected (Mouvement détecté »).
7. Définissez la durée.
8. Cliquez sur **Save (Enregistrer)**.

Remarque

Si vous mettez le texte de superposition à jour, il sera automatiquement mis à jour de manière dynamique sur tous les flux vidéo.

Enregistrer une vidéo lorsqu'un détecteur infrarouge passif détecte un mouvement

Cet exemple explique comment connecter un capteur infrarouge passif (normalement fermé) au périphérique et pour démarrer l'enregistrement vidéo lorsque le détecteur détecte un mouvement.

Matériel requis

- Câble à 3 fils (mise à la terre, alimentation, E/S)
- Capteur infrarouge passif, normalement fermé

AVIS

Déconnectez le périphérique de l'alimentation avant de raccorder les câbles. Reconnectez-la à l'alimentation lorsque toutes les connexions sont réalisées.

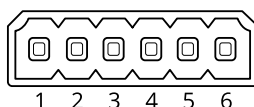
Connecter les câbles au connecteur d'E/S du périphérique

Remarque

Pour des informations sur le connecteur d'E/S, voir .

1. Branchez le câble de mise à la terre sur la broche 1 (Terre/-).
2. Branchez le câble d'alimentation sur la broche 2 (sortie 12 V CC).
3. Branchez le câble d'E/S sur la broche 3 (entrée E/S).

Connecter les câbles au connecteur d'E/S du détecteur infrarouge passif



1. Reliez l'autre extrémité du câble de mise à la terre sur la broche 1 (Terre/-).
2. Reliez l'autre extrémité du câble d'alimentation sur la broche 2 (entrée CC/+).
3. Reliez l'autre extrémité du câble d'E/S sur la broche 3 (sortie E/S).

Configurez le port d'E/S sur l'interface web du périphérique.

1. Accédez **System > Accessories > I/O ports (Système > Accessoires > Port d'E/S)**.
2. Cliquez sur  pour définir la direction sur Input (Entrée) pour le port 1.
3. Donnez un nom descriptif au module d'entrée, par exemple « Détecteur infrarouge passif ».
4. Pour déclencher un événement chaque fois que le capteur infrarouge passif détecte un mouvement, cliquez sur  pour définir l'état normal sur circuit fermé.

Création d'une règle

1. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sélectionnez **PIR detector (Détecteur infrarouge passif)**.
4. Dans la liste des actions, sous **Recordings (Enregistrements)**, sélectionnez **Record video while the rule is active (Enregistrer la vidéo tant que la règle est active)**.
5. Dans la liste des options de stockage, sélectionnez **SD_DISK (DISQUE_SD)**.
6. Sélectionnez une caméra et un profil de flux.
7. Réglez la durée pré-buffer sur 5 secondes.
8. Réglez la durée post-tampon sur 1 minute.
9. Cliquez sur **Save (Enregistrer)**.

Enregistrer une vidéo lorsque la caméra détecte des bruits forts

Cet exemple explique comment configurer la caméra pour commencer l'enregistrement sur la carte SD cinq secondes avant qu'elle détecte un bruit fort et l'arrêter deux minutes après.

Remarque

Les instructions suivantes nécessitent qu'un microphone soit raccordé à l'entrée audio.

Activez l'audio :

1. Configurez le profil de flux pour inclure l'audio, voir .

Activez la détection audio :

1. Accédez à **System > Detectors > Audio detection (Système > Détecteurs > Détection audio)**.
2. Réglez le niveau sonore selon vos besoins.

Créez une règle :

1. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sous **Audio (Audio)**, sélectionnez **Audio Detection (Détection audio)**.
4. Dans la liste des actions, sous **Recordings (Enregistrements)**, sélectionnez **Record video (Enregistrer la vidéo)**.
5. Dans la liste des options de stockage, sélectionnez **SD_DISK (DISQUE_SD)**.
6. Sélectionnez le profil de flux où l'audio a été activé.
7. Réglez la durée pré-buffer sur 5 secondes.
8. Réglez la durée post-tampon sur 2 minutes.
9. Cliquez sur **Save (Enregistrer)**.

Détecter les sabotages avec le signal d'entrée

Cet exemple explique comment envoyer un e-mail lorsque le signal d'entrée est coupé ou court-circuité. Pour plus d'informations sur le connecteur d'E/S, voir .

1. Allez à **System (Système) > Accessories (Accessoires) > Ports E/S** et activez **Supervised (Supervisés)** pour le port approprié.

Ajouter un destinataire d'e-mails :

1. Accédez à **System (Système) > Events (Événements) > Recipients (Destinataires)** et ajoutez un destinataire.
2. Entrez le nom du destinataire de l'e-mail.
3. Sélectionnez **Email (E-mail)**.
4. Entrez l'adresse e-mail à laquelle envoyer l'e-mail.
5. Le dispositif ne dispose pas de son propre serveur de messagerie, elle doit donc se connecter à un autre serveur de messagerie pour envoyer des messages. Remplissez le reste des informations en fonction de votre fournisseur d'e-mail.
6. Pour envoyer un e-mail de test, cliquez sur **Test**.
7. Cliquez sur **Save (Enregistrer)**.

Créez une règle :

1. Accédez à **System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sous **I/O (E/S)**, sélectionnez **Supervised input tampering is active (Le sabotage d'entrée supervisée est actif)**.
4. Sélectionner le port approprié.
5. Dans la liste des actions, sous **Notifications**, sélectionnez **Send notification to email (Envoyer une notification à un e-mail)**, puis sélectionnez le destinataire dans la liste.
6. Saisissez un objet et un message pour l'e-mail.
7. Cliquez sur **Save (Enregistrer)**.

Audio

Ajouter de l'audio à votre enregistrement

Activez l'audio :

1. Accédez à **Video (Vidéo) > Stream (Flux) > Audio** et incluez l'audio.
2. Si le périphérique possède plus d'une source d'entrée, sélectionnez la bonne source dans **Source**.
3. Accédez à **Audio > Device settings (Paramètres du périphérique)** et activez la bonne source d'entrée.
4. Si vous modifiez la source d'entrée, cliquez sur **Apply changes (Appliquer les modifications)**.

Modifiez le profil de flux utilisé pour l'enregistrement :

5. Accédez à **System > Stream profiles (Système > Profils de flux)** et sélectionnez le profil de flux.
6. Sélectionnez **Include audio (Inclure l'audio)** et activez-le.
7. Cliquez sur **Save (Enregistrer)**.

L'interface web

Pour accéder à l'interface web, saisissez l'adresse IP du périphérique dans un navigateur Web.

Remarque

La prise en charge des fonctionnalités et des paramètres décrits dans cette section varie d'un périphérique à l'autre. Cette icône  indique que la fonction ou le paramètre n'est disponible que sur certains périphériques.



Affichez ou masquez le menu principal.



Accédez aux notes de version.



Accédez à l'aide du produit.



Changez la langue.



Définissez un thème clair ou foncé.



Le menu utilisateur contient :

- les informations sur l'utilisateur connecté.
-  **Change account (Changer de compte)** : Déconnectez-vous du compte courant et connectez-vous à un nouveau compte.
-  **Log out (Déconnexion)** : Déconnectez-vous du compte courant.



Le menu contextuel contient :

- **Analytics data (Données d'analyse)** : acceptez de partager les données de navigateur non personnelles.
- **Feedback (Commentaires)** : partagez vos commentaires pour nous aider à améliorer votre expérience utilisateur.
- **Legal (Informations légales)** : Affichez des informations sur les cookies et les licences.
- **About (À propos)** : affichez les informations sur le périphérique, dont la version d'AXIS OS et le numéro de série.

État

Sécurité

Indique les types d'accès au périphérique actifs et les protocoles de cryptage utilisés, et si les applications non signées sont autorisées. Les recommandations concernant les paramètres sont basées sur le Guide de renforcement AXIS OS.

Guide de renforcement : Accédez au *Guide de renforcement AXIS OS* où vous pouvez en apprendre davantage sur la cybersécurité sur les périphériques Axis et les meilleures pratiques.

État de la synchronisation horaire

Affiche les informations de synchronisation NTP, notamment si le périphérique est synchronisé avec un serveur NTP et le temps restant jusqu'à la prochaine synchronisation.

Paramètres NTP : Affichez et mettez à jour les paramètres NTP. Cliquez pour accéder à la page **Heure et emplacement** où vous pouvez changer les paramètres NTP.

Enregistrements en cours

Affiche les enregistrements en cours et leur espace de stockage désigné.

Enregistrements : Afficher les enregistrements en cours et filtrés ainsi que leur source. Pour en savoir plus, consultez



Affiche l'espace de stockage où l'enregistrement est enregistré.

Infos sur le dispositif

Affiche les informations sur le périphérique, dont la version d'AXIS OS et le numéro de série.

Upgrade AXIS OS (Mettre à niveau AXIS OS) : Mettez à niveau le logiciel sur votre périphérique. Vous accédez à la page de maintenance où vous pouvez effectuer la mise à niveau.

Clients connectés

Affiche le nombre de connexions et de clients connectés.

View details (Afficher les détails) : Affichez et mettez à jour la liste des clients connectés. La liste affiche l'adresse IP, le protocole, le port, l'état et le protocole PID/processus de chaque connexion.

AXIS Image Health Analytics

Affiche l'état de l'application préinstallée AXIS Image Health Analytics et indique si l'application a détecté des problèmes.

Go to apps (Aller à Applications) : Allez à la page **Apps (Applications)** où vous pouvez gérer vos applications installées.

Open application (Ouvrir l'application) : Ouvrez AXIS Image Health Analytics dans un nouvel onglet du navigateur.

Vidéo



Cliquez pour lire le flux vidéo en direct.



Cliquez pour arrêter le flux vidéo en direct.



Cliquez pour faire une capture d'écran du flux vidéo en direct. Le fichier est enregistré dans le dossier « Téléchargements » de votre ordinateur. Le nom du fichier image est [snapshot_YYYY_MM_DD_HH_MM_SS.jpg]. La taille réelle de la capture d'image dépend de la compression appliquée par le moteur spécifique du navigateur web dans lequel la capture d'image est reçue. Par conséquent, la taille de la capture d'image peut varier par rapport au réglage de compression réel configuré sur le périphérique.



Cliquez pour afficher les ports de sortie E/S. Utilisez le commutateur pour ouvrir ou fermer le circuit d'un port, par exemple pour tester des périphériques externes.



Cliquez pour activer ou désactiver manuellement l'éclairage infrarouge.



Cliquez pour activer ou désactiver manuellement la lumière blanche.



Cliquez pour accéder aux commandes à l'écran :

- **Commandes prédéfinies** : Activez cette option pour utiliser les commandes disponibles à l'écran.

- **Commandes personnalisées** : Cliquez sur  **Add custom control (Ajouter une commande personnalisée)** pour ajouter une commande à l'écran.



Démarre le lavage. Lorsque la séquence démarre, la caméra se déplace à la position configurée. Lorsque la séquence de lavage complète est terminée, la caméra revient à sa position précédente. Cette icône est visible uniquement lorsque le dispositif de lavage est connecté et configuré.



Démarre l'essuyage.



Cliquez et sélectionnez une position préréglée pour y accéder dans la vidéo en direct. Vous pouvez aussi cliquer sur **Configuration** pour aller à la page des positions préréglées.



Ajoute ou supprime une zone de rappel mise au point. Lorsque vous ajoutez une zone de rappel mise au point, la caméra enregistre les paramètres de mise au point pour cette portée de panoramique/inclinaison spécifique. Lorsque vous avez configuré une zone de rappel mise au point et que la caméra pénètre sans cette zone de la vidéo en direct, la caméra rappelle la mise au point précédemment enregistrée. Cela suffit à couvrir la moitié de la zone pour que la caméra rappelle la mise au point.



Cliquez pour sélectionner une ronde de contrôle, puis cliquez sur **Start (Démarrer)** pour lire la ronde de contrôle. Vous pouvez aussi cliquer sur **Configuration** pour aller à la page des rondes de contrôle.



Cliquez pour activer manuellement la chaleur pendant une période sélectionnée.



Cliquez pour démarrer un enregistrement continu du flux vidéo en direct. Cliquez à nouveau pour arrêter l'enregistrement. Si un enregistrement est en cours, il reprend automatiquement après un redémarrage.



Cliquez pour afficher le stockage configuré pour le périphérique. Pour configurer le stockage dont vous avez besoin, vous devez être connecté en tant qu'administrateur.



Cliquez pour accéder à plus de paramètres :

- **Format vidéo** : sélectionnez le format d'encodage à utiliser dans la vidéo en direct.
- **Autoplay (Lecture automatique)** : Activez automatiquement un flux vidéo muet chaque fois que vous ouvrez le dispositif dans une nouvelle session.
- **Informations sur les flux client** : Activez cette option pour afficher des informations dynamiques sur le flux vidéo utilisé par le navigateur qui affiche le flux vidéo en direct. Les informations de débit binaire diffèrent des informations affichées dans une incrustation de texte, en raison de différentes sources d'informations. Le débit binaire dans les informations du flux client est celui de la dernière seconde, et il provient du pilote d'encodage du périphérique. Le débit binaire dans l'incrustation est le débit binaire moyen des 5 dernières secondes, et il provient du navigateur. Ces deux valeurs ne couvrent que le flux vidéo brut et non la bande passante supplémentaire générée lorsqu'il est transporté sur le réseau via UDP/TCP/HTTP.
- **Adaptive stream (Flux adaptatif)** : Activez cette option pour adapter la résolution d'image à la résolution d'affichage réelle du client d'affichage, afin d'améliorer l'expérience utilisateur et d'éviter une surcharge éventuelle du matériel du client. Le flux adaptatif est appliqué uniquement lors de l'affichage du flux vidéo en direct dans l'interface Web d'un navigateur. Lorsque le flux adaptatif est activé, la fréquence d'images maximale est de 30 ips. Si vous faites une capture d'image alors que le flux adaptatif est activé, la résolution d'image sélectionnée est celle utilisée par le flux adaptatif.
- **Level grid (Grille de niveau)** : Cliquez sur pour afficher la grille de niveau. La grille vous aide à décider si l'image est alignée horizontalement. Cliquez sur pour la masquer.
- **Compteur de pixels** : Cliquez sur pour afficher le compteur de pixels. faites glisser et redimensionnez le cadre pour contenir votre domaine d'intérêt. Vous pouvez également définir la taille en pixels du cadre dans les champs **Width (Largeur)** et **Height (Hauteur)**.
- **Refresh (Actualiser)** : Cliquez sur pour actualiser l'image arrêtée dans la vidéo en direct.
- **Commandes PTZ** : Activez cette option pour afficher les commandes PTZ dans la vidéo en direct.



Cliquez pour afficher la vidéo en direct en pleine résolution. Si la pleine résolution est plus grande que la taille de l'écran, utilisez l'image la plus petite pour vous déplacer dans l'image.



Cliquez pour afficher le flux vidéo en plein écran. Appuyez sur ESC pour quitter le mode plein écran.

Installation

Mode de capture ⓘ : Un mode de capture est une configuration prédéfinie qui définit la manière dont la caméra capture les images. Lorsque vous modifiez le mode de capture, cela peut affecter de nombreux autres paramètres, tels que les zones de visualisation et les masques de confidentialité.

Position de montage ⓘ : L'orientation de l'image peut varier en fonction du montage de la caméra.

Power line frequency (Fréquence d'alimentation) : Pour minimiser le scintillement de l'image, sélectionnez la fréquence utilisée dans votre région. Les régions américaines utilisent en général 60 Hz. Le reste du monde utilise principalement 50 Hz. Si vous n'êtes pas sûr de la fréquence de la ligne d'alimentation de votre région, vérifiez auprès des administrations locales.

Zoom ⓘ : Utilisez le curseur pour ajuster le niveau de zoom.

Mise au point automatique après zoom ⓘ : Allumer pour activer la mise au point automatique après avoir effectué un zoom.

Focus (Mise au point) : Utilisez le curseur pour régler manuellement la mise au point.

Autofocus (Mise au point automatique) : Cliquez pour permettre à la caméra d'effectuer une mise au point sur la zone sélectionnée. Si vous ne sélectionnez pas une zone de mise au point automatique, la caméra effectue la mise au point sur la totalité de la scène.

Autofocus area (Zone de mise au point automatique): Cliquez sur ⓘ pour afficher la zone de mise au point automatique. Cette zone doit inclure la zone d'intérêt.

Reset focus (Réinitialiser la mise au point) : Cliquez pour rétablir la position d'origine de la mise au point.

Remarque

Dans les environnements froids, le zoom et la mise au point peuvent prendre plusieurs minutes.

Correction d'image

Important

Nous vous recommandons de ne pas utiliser plusieurs fonctions de correction d'image en même temps, car cela peut entraîner des problèmes de performance.

Correction de la distorsion en barillet (CDB)  : Activez cette option pour obtenir une image plus droite en cas de distorsion en barillet. La distorsion en barillet est un effet de l'objectif qui fait apparaître l'image courbe et déformée vers l'extérieur. L'état est plus clair lorsque l'image est zoomée en arrière.

Crop (Recadrer)  : Utilisez le curseur pour ajuster le niveau de correction. Un niveau moins élevé implique que la largeur de l'image est conservée au détriment de la hauteur et de la résolution de l'image. Un niveau plus élevé implique que la hauteur et la résolution de l'image sont conservées au détriment de la largeur.

Remove distortion (Supprimer la distorsion)  : Utilisez le curseur pour ajuster le niveau de correction. Pucker (Contraction) implique que la largeur de l'image est conservée au détriment de la hauteur et de la résolution de l'image. Bloat (Dilatation) implique que la hauteur et de la résolution de l'image sont conservées au détriment de la largeur.

Image stabilization (Stabilisation d'image)  : Activez cette option pour obtenir des images plus stables et plus fluides, avec moins de flou. Nous vous recommandons d'utiliser la stabilisation d'image dans les environnements où le périphérique est installé à un endroit exposé et soumis à des vibrations, par exemple, en plein vent ou à proximité d'une route au trafic intense.

Focal length (Distance focale)  : Utilisez le curseur pour ajuster la distance focale. Une valeur plus élevée produit un grossissement plus élevé et un angle de vue plus étroit, tandis qu'une valeur plus faible produit un moindre grossissement et un angle de vue plus large.

Stabilizer margin (Marge du stabilisateur)  : Utilisez le curseur pour ajuster la taille de la marge du stabilisateur, qui détermine le niveau de vibration à stabiliser. Si le produit est monté dans un environnement subissant beaucoup de vibrations, déplacez le curseur vers **Max**. Résultat : une scène plus petite est capturée. Si l'environnement subit moins de vibrations, déplacez le curseur vers **Min**.

Focus breathing correction (Mise au point correction de la respiration)  : Activez-la pour que l'angle de vue reste constant pendant que vous changez la mise au point. Il se peut que vous ne puissiez pas effectuer un zoom avant aussi important lorsque cette fonction est activée.

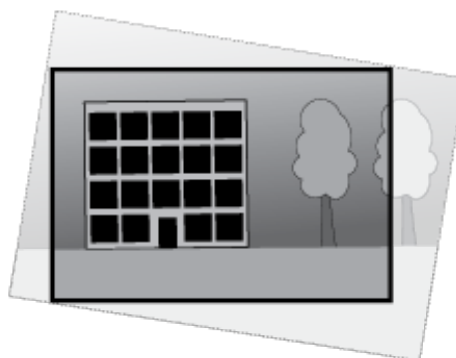
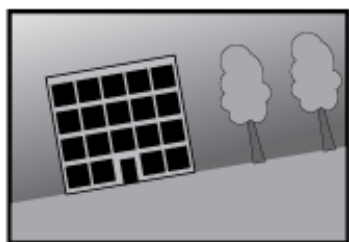
Straighten image (Image redressée)  : Activez cette option et utilisez le curseur pour redresser l'image horizontalement en la faisant pivoter et en la rognant numériquement. Cette fonctionnalité est particulièrement utile lorsqu'il n'est pas possible de monter la caméra exactement au niveau. Dans l'idéal, redressez l'image pendant l'installation.



: Cliquez pour afficher une grille de support dans l'image.



: Cliquez pour masquer la grille.



L'image avant et après avoir été redressée.

Image

Apparence

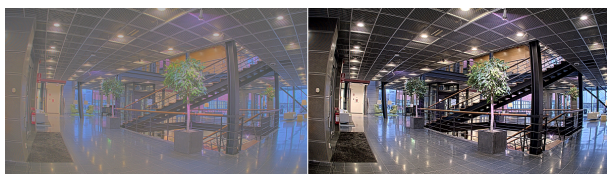
Scene profile (Profil de scène) ⓘ : Sélectionnez un profil de scène adapté à votre scénario de surveillance. Un profil de scène optimise les paramètres d'image, notamment le niveau de couleur, la luminosité, la netteté, le contraste et le contraste local, pour un environnement ou un objectif spécifiques.

- **Forensic (Médico-légal)** ⓘ : Adapté à des fins de surveillance.
- **Indoor (Intérieur)** ⓘ : Convient pour les environnements en intérieur.
- **Outdoor (Extérieur)** ⓘ : Convient pour les environnements en extérieur.
- **Vivid (Vif)** ⓘ : Utile à des fins de démonstration.
- **Traffic overview (Aperçu du trafic)** ⓘ : Convient à la surveillance du trafic de véhicules.
- **License plate (Plaque d'immatriculation)** ⓘ : Convient à la capture des plaques d'immatriculation.

Saturation : Utilisez le curseur pour ajuster l'intensité de la couleur. Vous pouvez, par exemple, obtenir une image en nuances de gris.



Contraste : Utilisez le curseur pour ajuster les différences entre les zones obscures et claires.



Luminosité : Utilisez le curseur pour ajuster l'intensité lumineuse. Cela peut rendre les objets plus visibles. La luminosité est appliquée après la capture de l'image et n'affecte pas les informations contenues dans l'image. Pour obtenir davantage de détails d'une zone sombre, il est parfois préférable d'accroître le gain ou le temps d'exposition.



Sharpness (Netteté) : Utilisez le curseur pour ajuster le contraste des contours des objets et les rendre plus visibles. Si vous augmentez la netteté, cela peut augmenter le débit binaire et l'espace de stockage nécessaire également.



Plage dynamique étendue (WDR)

WDR  : Activez cette option pour rendre visibles les zones éclairées et sombres dans l'image.

Local contrast (Contraste local)  : Utilisez le curseur pour ajuster le contraste de l'image. Une valeur plus élevée permet d'augmenter le contraste entre les zones sombres et lumineuses.

Tone mapping (Courbe des gammas)  : Utilisez le curseur pour ajuster la courbe des gammas appliquée à l'image. Si la valeur est fixée à zéro, seule la correction gamma standard est appliquée, tandis qu'une valeur supérieure augmente la visibilité dans la zone la plus sombre et la zone la plus lumineuse de l'image.

Balance des blancs

Une fois la température de couleur de la lumière entrante détectée par la caméra, il est possible de régler l'image afin que les couleurs paraissent plus naturelles. Si cela n'est pas suffisant, vous pouvez sélectionner une source de lumière qui convient.

Le réglage automatique de la balance des blancs réduit le risque de scintillement de couleur en s'adaptant progressivement aux changements. Si l'éclairage change, ou lorsque la caméra est allumée pour la première fois, cela peut prendre jusqu'à 30 secondes avant de s'adapter à une nouvelle source lumineuse. S'il y a plusieurs types de source de lumière dans une scène, et qu'elles ont une température de couleur différente, la source de lumière dominante agit comme une référence pour l'algorithme automatique de la balance des blancs. Ce comportement peut être contourné en choisissant un réglage fixe de la balance des blancs qui correspond à la source de lumière que vous souhaitez utiliser comme référence.

Light environment (Environnement lumineux) :

- **Automatic (Automatique)** : Identification et compensation automatiques pour la couleur de la source de lumière. C'est le réglage recommandé qui peut être utilisé dans la plupart des cas.
- **Automatic – outdoors (Automatique – extérieur)**  : Identification et compensation automatiques pour la couleur de la source de lumière. C'est le réglage recommandé qui peut être utilisé dans la plupart des cas à l'extérieur.
- **Custom – indoors (Personnalisé – intérieur)**  : Réglage fixe de la couleur pour une pièce avec une lumière artificielle autre qu'un éclairage fluorescent et bonne pour une température de couleur normale d'environ 2 800 K.
- **Custom – outdoors (Personnalisé – extérieur)**  : Réglage fixe de la couleur lorsque le temps est ensoleillé avec une température de couleur d'environ 5 500 K.
- **Fixed – fluorescent 1 (Fixe – fluorescent 1)** : Réglage fixe de la couleur pour un éclairage fluorescent avec une température de couleur d'environ 4 000 K.
- **Fixed – fluorescent 2 (Fixe – fluorescent 2)** : Réglage fixe de la couleur pour un éclairage fluorescent avec une température de couleur d'environ 3 000 K.
- **Fixed – indoors (Fixe – intérieur)** : Réglage fixe de la couleur pour une pièce avec une lumière artificielle autre qu'un éclairage fluorescent et bonne pour une température de couleur normale d'environ 2 800 K.
- **Fixed – outdoors 1 (Fixe – extérieur 1)** : Réglage fixe de la couleur lorsque le temps est ensoleillé avec une température de couleur d'environ 5 500 K.
- **Fixed – outdoors 2 (Fixe – extérieur 2)** : Réglage fixe de la couleur lorsque le temps est nuageux avec une température de couleur d'environ 6 500 K.
- **Street light – mercury (Lampadaire – mercure)**  : Réglage fixe de la couleur pour l'émission d'ultraviolets des ampoules à vapeur de mercure des lampadaires.
- **Street light – sodium (Lampadaire – sodium)**  : Réglage fixe de la couleur qui compense la couleur jaune orangée des ampoules à vapeur de sodium des lampadaires.
- **Hold current (Conserver les paramètres actuels)** : Conservez les paramètres actuels et ne compensez pas les changements de lumière.
- **Manual (Manuel)**  : Réglage fixe de la balance des blancs à l'aide d'un objet blanc. Faites glisser le cercle sur un objet que vous souhaitez que la caméra interprète comme blanc dans l'image en direct. Utilisez les curseurs **Balance des rouges** et **Balance des bleus** pour régler manuellement la balance des blancs.

Mode jour-nuit

Filtre infrarouge :

- **Auto** : Sélectionnez cette option pour activer et désactiver automatiquement le masque IR. lorsque la caméra est en mode jour, le masque IR est activé et bloque la lumière IR entrante ; en mode nuit, lorsque le masque IR est désactivé et la sensibilité à la lumière de la caméra augmente.

Remarque

- Certains appareils sont équipés de filtres passe-IR en mode nocturne. Le filtre passe-IR augmente la sensibilité à la lumière infrarouge, mais bloque la lumière visible.
- **Activé** : Sélectionnez cette option pour activer le masque IR. L'image est en couleurs, mais avec une sensibilité à la lumière réduite.
- **Désactivé** : Sélectionnez cette option pour désactiver le masque IR. L'image est en noir et blanc pour une meilleure sensibilité à la lumière.

Threshold (Seuil) : Utilisez le curseur pour régler le seuil d'éclairage auquel la caméra passe du mode jour au mode nuit.

- Faites glisser le curseur vers **Bright (Lumineux)** pour réduire le seuil du masque IR. La caméra passe en mode nocturne plus tôt.
- Faites glisser le curseur vers **Dark (Sombre)** pour augmenter le seuil du masque IR. La caméra passe en mode nocturne plus tard.

lumière IR

Si votre dispositif n'a pas d'éclairage intégré, ces contrôles ne sont disponibles que lorsque vous connectez un éclairage Axis compatible.

Autoriser l'éclairage : Activez cette option pour permettre à la caméra d'utiliser l'éclairage intégré en mode nuit.

Synchroniser l'éclairage : Activez cette option pour synchroniser automatiquement l'éclairage avec la lumière environnante. La synchronisation entre les modes jour et nuit fonctionne uniquement si le filtre infrarouge est réglé sur **Auto** ou **Désactivé**.

Automatic illumination angle (Angle d'éclairage automatique)  : Activez cette option pour utiliser un angle d'éclairage automatique. Désactivez-la pour régler manuellement l'angle d'éclairage.

Angle d'éclairage  : utilisez le curseur pour régler manuellement l'angle d'éclairage, par exemple, si l'angle doit être différent de l'angle de vue de la caméra. Si la caméra dispose d'un grand angle de vue, vous pouvez réduire l'angle d'éclairage (position de téléobjectif). Cela produira des coins sombres dans l'image.

IR wavelength (Longueur d'onde IR)  : Sélectionnez la longueur d'onde souhaitée pour la lumière IR.

Lumière blanche

Allow illumination (Autoriser l'éclairage)  : Activez cette option pour permettre à la caméra d'utiliser la lumière blanche en mode nuit.

Synchronize illumination (Synchroniser l'éclairage)  : Activez cette option pour synchroniser automatiquement la lumière blanche avec la lumière environnante.

Exposition

Sélectionnez un mode d'exposition afin de réduire rapidement les effets irréguliers sur l'image, tels que le clignotement produit par différents types de sources de lumière. Nous vous recommandons d'utiliser le mode d'exposition automatique ou la même fréquence que le réseau d'alimentation.

Exposure mode (Mode d'exposition) :

- **Automatic (Automatique)** : La caméra règle automatiquement l'ouverture, le gain et l'obturateur.
- **Automatic aperture (Ouverture automatique)** ⓘ : La caméra règle automatiquement l'ouverture et le gain. L'obturateur est fixe.
- **Automatic shutter (Obturateur automatique)** ⓘ : La caméra règle automatiquement l'obturateur et le gain. L'ouverture est fixe.
- **Conserver les paramètres actuels** : Verrouille les paramètres d'exposition en cours.
- **Flicker-free (Sans clignotement)** ⓘ : La caméra règle automatiquement l'ouverture et le gain et utilise uniquement les vitesses d'obturation suivantes : 1/50 s (50 Hz) et 1/60 s (60 Hz).
- **Flicker-free 50 Hz (Sans clignotement 50 Hz)** ⓘ : La caméra règle automatiquement l'ouverture et le gain et utilise la vitesse d'obturation 1/50 s.
- **Flicker-free 60 Hz (Sans clignotement 60 Hz)** ⓘ : La caméra règle automatiquement l'ouverture et le gain et utilise la vitesse d'obturation 1/60 s.
- **Flicker-reduced (Clignotement réduit)** ⓘ : Identique au mode sans clignotement à la différence que la caméra peut utiliser n'importe quelle vitesse d'obturation supérieure à 1/100 s (50 Hz) et 1/120 s (60 Hz) pour les scènes plus lumineuses.
- **Flicker-reduced 50 Hz (Clignotement réduit 50 Hz)** ⓘ : Identique au mode sans clignotement à la différence que la caméra peut utiliser n'importe quelle vitesse d'obturation supérieure à 1/100 s pour les scènes plus lumineuses.
- **Flicker-reduced 60 Hz (Clignotement réduit 60 Hz)** ⓘ : Identique au mode sans clignotement à la différence que la caméra peut utiliser n'importe quelle vitesse d'obturation supérieure à 1/120 s pour les scènes plus lumineuses.
- **Manual (Manuel)** ⓘ : L'ouverture, le gain et l'obturateur sont fixes.

Exposure zone (Zone d'exposition) ⓘ : Utilisez des zones d'exposition pour optimiser l'exposition dans une partie sélectionnée de la scène, par exemple la zone située en face d'une porte d'entrée.

Remarque

Les zones d'exposition sont liées à l'image originale (non tournée), et les noms des zones s'appliquent à l'image originale. Cela signifie par exemple que si le flux vidéo pivote à 90°, la zone **supérieure** devient la zone de **droite** dans le flux, et que la zone de **gauche** devient la zone **inférieure**.

- **Automatic (Automatique)** : Convient à la plupart des situations.
- **Center (Centre)** : Utilise une zone fixe au centre de l'image pour calculer l'exposition. La zone a une taille et une position fixes dans la Vidéo en direct.
- **Full (Complet)** ⓘ : Utilise la vidéo en direct entière pour calculer l'exposition.
- **Upper (Supérieur)** ⓘ : Utilise une zone avec une taille et une position fixes dans la partie supérieure de l'image pour calculer l'exposition.
- **Lower (Inférieur)** ⓘ : Utilise une zone avec une taille et une position fixes dans la partie inférieure de l'image pour calculer l'exposition.

- **Left (Gauche)**  : Utilisez une zone avec une taille et une position fixes dans la partie gauche de l'image pour calculer l'exposition.
- **Right (Droite)**  : Utilisez une zone avec une taille et une position fixes dans la partie droite de l'image pour calculer l'exposition.
- **Spot (Mesure sélective)** : Utilisez une zone avec une taille et une position fixes dans la vidéo en direct pour calculer l'exposition.
- **Personnalisé** : Utilisez une zone dans la vidéo en direct pour calculer l'exposition. Vous pouvez ajuster la taille et la position de la zone.

Max shutter (Obturbateur max.) : Sélectionnez la vitesse d'obturation afin d'améliorer la qualité des images. Les vitesses d'obturation lente (exposition plus longue) peuvent entraîner un flou de mouvement et une vitesse d'obturation trop rapide peut altérer la qualité de l'image. Pour une qualité optimale, réglez conjointement les options Obturbateur max. et Gain max.

Max gain (Gain max.) : Sélectionnez le gain max. approprié. Si vous augmentez le gain maximal, cela améliore le niveau visible de détails dans les images sombres, mais augmente aussi le niveau de bruit. Davantage de bruit peut avoir pour résultat une utilisation accrue de la bande passante et du stockage. Si vous définissez le gain maximal sur une valeur élevée, les images peuvent être très différentes si les conditions d'éclairage diffèrent fortement entre le jour et la nuit. Pour une qualité optimale, réglez conjointement les options Gain max. et Obturbateur max.

Exposition variable en fonction du mouvement  : Sélectionnez pour réduire le flou de mouvement dans les conditions de faible luminosité.

Compromis flou-bruit : Utilisez le curseur afin de régler la priorité entre le flou de mouvement et le bruit. Si vous souhaitez donner la priorité à une faible bande passante et avoir moins de bruit aux dépens de détails sur les objets en mouvement, déplacez le curseur vers **Low noise (Faible bruit)**. Si vous souhaitez donner la priorité aux détails sur les objets en mouvement aux dépens du bruit et de la bande passante, déplacez le curseur vers **Low motion blur (Flou des mouvements au ralenti)**.

Remarque

Vous pouvez changer l'exposition en réglant le temps d'exposition ou en réglant le gain. Si vous augmentez le temps d'exposition, il en résulte plus de flou de mouvement, et si vous augmentez le gain, cela entraîne plus de bruit. Si vous réglez **Blur-noise trade-off (Compromis flou-bruit)** sur **Low noise (Faible bruit)**, l'exposition automatique préférera des temps d'exposition plus longs à une augmentation du gain, et inversement si vous réglez le compromis sur **Low motion blur (Flou des mouvements au ralenti)**. Le gain et le temps d'exposition atteignent en définitive leurs valeurs maximales dans des conditions de faible luminosité, quelle que soit la priorité définie.

Lock aperture (Verrouiller l'ouverture)  : Activez cette option pour conserver la taille d'ouverture définie par le curseur **Aperture (Ouverture)**. Désactivez cette option pour permettre à la caméra de régler automatiquement la taille de l'ouverture. Vous pouvez, par exemple, verrouiller l'ouverture dans des scènes avec des conditions d'éclairage constantes.

Aperture (Ouverture)  : Utilisez le curseur pour ajuster la taille de l'ouverture, à savoir, quelle quantité de lumière passe à travers l'objectif. Pour permettre à davantage de lumière d'entrer dans le capteur et de produire ainsi une image plus lumineuse dans des conditions de faible luminosité, déplacez le curseur vers **Open (Ouvvert)**. Une grande ouverture réduit également la profondeur de champ, ce qui signifie que les objets proches ou éloignés de la caméra peuvent apparaître flous. Pour permettre une mise au point d'une plus grande partie de l'image, déplacez le curseur vers **Closed (Fermé)**.

Exposure level (Niveau d'exposition) : Utilisez le curseur pour ajuster l'exposition de l'image.

Defog (Désembuage)  : Activez cette option pour détecter l'effet de buée et le supprimer automatiquement afin de produire une image plus nette.

Remarque

Nous vous recommandons de ne pas activer l'option **Defog (Désembuage)** dans les scènes présentant un faible contraste, des variations de luminosité importantes et lorsque la mise au point automatique est erronée. Cela peut affecter la qualité d'image en augmentant, par exemple, le contraste. Par ailleurs, trop de lumière peut également avoir un impact négatif sur la qualité d'image lorsque le désembuage est actif.

Optique

Compensation de température  : Activez cette option si vous souhaitez que la position de mise au point soit corrigée en fonction de la température dans le système optique.

IR compensation  (compensation IR) : Activez cette option si vous souhaitez que la position de mise au point soit corrigée lorsque le masque IR est désactivé et lorsqu'il y a un illuminateur IR.

Calibrer le zoom et la mise au point : Cliquez pour réinitialiser l'optique et les paramètres de zoom et de mise au point sur la position d'usine par défaut. Vous devez effectuer cette opération si l'optique a perdu le calibrage pendant le transport ou si le périphérique a été exposé à des vibrations extrêmes.

Flux

Général

Résolution : Sélectionnez la résolution d'image convenant à la scène de surveillance. Une résolution plus élevée accroît les besoins en matière de bande passante et de stockage.

Fréquence d'images : Pour éviter les problèmes de bande passante sur le réseau ou réduire la taille du stockage, vous pouvez limiter la fréquence d'images à une valeur fixe. Si vous laissez la fréquence d'image à zéro, la fréquence d'image est maintenue à la fréquence la plus élevée possible dans les conditions actuelles. Une fréquence d'images plus élevée nécessite davantage de bande passante et de capacité de stockage.

P-frames (Trames P) : Une image P est une image prédite qui montre uniquement les changements dans l'image par rapport à l'image précédente. Saisissez le nombre de trames P souhaitées. Plus ce nombre est élevé, plus la bande passante nécessaire est faible. Toutefois, en cas d'encombrement du réseau, la qualité de la vidéo peut se détériorer sensiblement.

Compression : Utilisez le curseur pour ajuster la compression de l'image. Une compression élevée se traduit par un débit binaire et une qualité d'image inférieurs. Une faible compression améliore la qualité de l'image, mais utilise davantage de bande passante et de capacité de stockage lors de l'enregistrement.

Signed video (Vidéo signée)  : Activez cette option pour ajouter la fonction de vidéo signée à la vidéo. La vidéo signée protège la vidéo contre la falsification en ajoutant des signatures cryptographiques à la vidéo.

Zipstream

Zipstream est une technologie de réduction du débit binaire optimisée pour la vidéosurveillance qui réduit le débit binaire moyen dans un flux H.264 ou H.265 en temps réel. La technologie Axis Zipstream applique un débit binaire élevé dans les scènes comportant de nombreuses régions d'intérêt, par exemple, des objets en mouvement. Lorsque la scène est plus statique, Zipstream applique un débit binaire inférieur, ce qui réduit l'espace de stockage requis. Pour en savoir plus, voir la section *Diminuer le débit binaire avec Axis Zipstream*

Sélectionnez l'intensité de la réduction du débit binaire :

- **Désactivé** : Aucune réduction du débit binaire.
- **Faible** : Aucune dégradation visible de la qualité dans la plupart des scènes. Il s'agit de l'option par défaut et elle peut être utilisée dans tous les types de scènes pour réduire le débit binaire.
- **Moyenne** : Effets visibles dans certaines scènes, à savoir, moins de bruit, et un niveau de détails légèrement inférieur dans les régions de moindre intérêt (par exemple, absence de mouvement).
- **Élevée** : Effets visibles dans certaines scènes, à savoir, moins de bruit, et un niveau de détails inférieur dans les régions de moindre intérêt (par exemple, absence de mouvement). Nous recommandons ce niveau pour les périphériques connectés au cloud et les périphériques qui utilisent un stockage local.
- **Higher (Plus élevé)** : Effets visibles dans certaines scènes, à savoir, moins de bruit, et un niveau de détails inférieur dans les régions de moindre intérêt (par exemple, absence de mouvement).
- **Extrême** : Effet visible dans la plupart des scènes. Le débit binaire est optimisé pour le stockage le plus petit possible.

Optimiser pour le stockage : Activez cette option réduire le débit binaire tout en conservant la qualité.

L'optimisation ne s'applique pas au flux affiché sur le client Web. Ce système ne peut être utilisé que si votre VMS prend en charge des images B. L'activation de l'option **Optimiser pour le stockage** entraîne l'activation de l'option **GOP dynamique**.

Dynamic FPS (IPS dynamique) (images par seconde) : Activez cette option pour permettre une variation de la bande passante en fonction du niveau d'activité dans la scène. Davantage d'activité nécessite plus de bande passante.

Lower limit (Limite inférieure) : Saisissez une valeur pour ajuster la fréquence d'images entre le nombre d'ips minimal et le nombre d'ips par défaut du flux en fonction du mouvement de la scène. Nous vous recommandons d'utiliser une limite inférieure dans les scènes avec très peu de mouvement, où le nombre d'ips peut chuter à 1 ou moins.

Dynamic GOP (Group of Pictures) (Algorithme dynamique de groupe d'images (GOP) : Activez cette option pour ajuster dynamiquement l'intervalle entre les trames I en fonction du niveau d'activité dans la scène.

Upper limit (Limite supérieure) : Saisissez une longueur de GOP maximale, c'est-à-dire le nombre maximal de trames P entre deux trames I. Une image I est une image autonome qui ne dépend pas des autres images.

Commande du débit binaire

- **Moyenne** : Sélectionnez cette option pour ajuster automatiquement le débit binaire sur une période plus longue et fournir la meilleure qualité d'image possible en fonction du stockage disponible.
 -  Cliquez pour calculer le débit binaire cible en fonction du stockage disponible, de la durée de conservation et de la limite de débit binaire.
 - **Débit binaire cible** : Saisissez le Débit binaire cible souhaité.
 - **Retention time (Durée de conservation)** : Saisissez la durée de stockage en jours des enregistrements.
 - **Stockage** : Affiche le stockage estimé qui peut être utilisé pour le flux.
 - **Maximum bitrate (Débit binaire maximum)** : Activez cette option pour définir une limite de débit binaire.
 - **Bitrate limit (Limite de débit binaire)** : Saisissez une limite de débit binaire supérieure au débit binaire cible.
- **Maximum (Maximum)** : Sélectionnez cette option pour définir le débit binaire instantané maximum du flux en fonction de la bande passante de votre réseau.
 - **Maximum (Maximum)** : Saisissez le débit binaire maximum.
- **Variable (Variable)** : Sélectionnez cette option pour autoriser une variation du débit binaire en fonction du niveau d'activité dans la scène. Davantage d'activité nécessite plus de bande passante. Nous vous recommandons cette option dans la plupart des cas.

Audio

Include (Inclure) : Activez cette option pour utiliser l'audio dans le flux vidéo.

Source (Source)  : Sélectionnez la source audio à utiliser.

Stereo (Stéréo)  : Activez cette option pour inclure l'audio intégré ainsi que l'audio provenant d'un microphone externe.

Incrustations



: Cliquez pour ajouter une incrustation. Sélectionnez le type d'incrustation dans la liste déroulante :

- **Text (Texte)** : Sélectionnez pour afficher un texte intégré à l'image de la vidéo en direct et visible dans toutes les vues, tous les enregistrements et tous les instantanés. Vous pouvez saisir votre propre texte et inclure des modificateurs pré-configurés pour afficher automatiquement, par exemple, l'heure, la date, la fréquence d'image.
 -  : Cliquez pour ajouter le modificateur de date %F pour afficher le format aaaa-mm-jj.
 -  : Cliquez pour ajouter le modificateur d'heure %X pour afficher le format hh:mm:ss (format 24 heures).
 - **Modificateurs** : Cliquez pour sélectionner l'un des modificateurs de la liste et l'ajouter à la zone de texte. Par exemple, %a affiche le jour de la semaine.
 - **Size (Taille)** : Sélectionnez la taille de police souhaitée.
 - **Appearance (Apparence)** : Sélectionnez la couleur du texte et de l'arrière-plan, par exemple, du texte blanc sur fond noir (par défaut).
 -  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct.
- **Une image** : Sélectionnez pour afficher une image statique superposée au flux vidéo. Vous pouvez utiliser des fichiers .bmp, .png, .jpeg ou .svg. Pour charger une image, cliquez sur **Images**. Avant de charger une image, vous pouvez choisir les options suivantes :
 - **Scale with resolution (Mise à l'échelle)** : Sélectionnez cette option pour adapter automatiquement l'image d'incrustation à la résolution vidéo.
 - **Use transparency (Utiliser la transparence)** : Sélectionnez cette option et saisissez la valeur hexadécimale RVB pour cette couleur. Utilisez le format RRGGBB. Exemples de valeurs hexadécimales : FFFFFFFF pour blanc, 000000 pour noir, FF0000 pour rouge, 6633FF pour bleu et 669900 pour vert. Uniquement pour les images .bmp.
- **Scene annotation (Annotation de la scène)**  : Sélectionnez cette option pour afficher une incrustation de texte dans le flux vidéo qui reste dans la même position, même lorsque la caméra effectue un panoramique ou une inclinaison dans une autre direction. Vous pouvez choisir d'afficher l'incrustation uniquement dans certains niveaux de zoom.
 -  : Cliquez pour ajouter le modificateur de date %F pour afficher le format aaaa-mm-jj.
 -  : Cliquez pour ajouter le modificateur d'heure %X pour afficher le format hh:mm:ss (format 24 heures).
 - **Modificateurs** : Cliquez pour sélectionner l'un des modificateurs de la liste et l'ajouter à la zone de texte. Par exemple, %a affiche le jour de la semaine.
 - **Size (Taille)** : Sélectionnez la taille de police souhaitée.
 - **Appearance (Apparence)** : Sélectionnez la couleur du texte et de l'arrière-plan, par exemple, du texte blanc sur fond noir (par défaut).
 -  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct. L'incrustation est enregistrée et demeure dans les coordonnées de panoramique et d'inclinaison de cette position.
 - **Annotation entre les niveaux de zoom (%)** : Définissez les niveaux de zoom dans lesquels l'incrustation sera affichée.

- **Symbole de l'annotation** : Sélectionnez un symbole qui apparaît à la place de l'incrustation lorsque la caméra n'est pas dans les niveaux de zoom définis.
- **Streaming indicator (Indicateur de diffusion)**  : Sélectionnez cette image pour afficher une animation superposée au flux vidéo. L'animation indique que le flux vidéo est en direct, même si la scène ne contient pas de mouvement.
 - **Appearance (Apparence)** : Sélectionnez la couleur d'animation et la couleur de l'arrière-plan, par exemple, une animation de couleur rouge sur un fond transparent (par défaut).
 - **Size (Taille)** : Sélectionnez la taille de police souhaitée.
 -  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct.
- **Widget : Linegraph (Graphique linéaire)**  : Afficher un graphique qui montre l'évolution d'une valeur mesurée au fil du temps.
 - **Title (Titre)** : Entrez le nom du widget.
 - **Modificateur d'incrustation** : Sélectionnez un modificateur d'incrustation comme source de données. Si vous avez créé des incrustations MQTT, elles seront situées en fin de liste.
 -  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct.
 - **Size (Taille)** : Sélectionnez la taille de l'incrustation.
 - **Visible sur toutes les chaînes** : Désactivez cette option pour afficher uniquement sur la chaîne actuellement sélectionnée. Activez cette option pour afficher sur toutes les chaînes actives.
 - **Intervalle de mise à jour** : Choisissez le temps entre les mises à jour des données.
 - **Transparency (Transparence)** : Définissez la transparence de toute l'incrustation.
 - **Transparence de l'arrière-plan** : Définissez uniquement la transparence de l'arrière-plan de l'incrustation.
 - **Points** : Activez cette option pour ajouter un point à la ligne du graphique lorsque les données sont mises à jour.
 - **Axe des X**
 - **Label (Étiquette)** : Entrez le libellé de texte pour l'axe X.
 - **Fenêtre temporelle** : Entrez la durée pendant laquelle les données sont visualisées.
 - **Unité de temps** : Entrez une unité de temps pour l'axe des X.
 - **Axe des Y**
 - **Label (Étiquette)** : Entrez le libellé de texte pour l'axe Y
 - **Échelle dynamique** : Activez-le pour que l'échelle s'adapte automatiquement aux valeurs des données. Désactivez cette option pour saisir manuellement les valeurs d'une échelle fixe.
 - **Seuil d'alarme minimum et Seuil d'alarme maximum** : Ces valeurs ajouteront des lignes de référence horizontales au graphique, ce qui permettra de voir plus facilement quand la valeur des données devient trop élevée ou trop faible.
- **Widget : Meter (Mètre)**  : Afficher un graphique à barres affichant la valeur de données la plus récemment mesurée.
 - **Title (Titre)** : Entrez le nom du widget.
 - **Modificateur d'incrustation** : Sélectionnez un modificateur d'incrustation comme source de données. Si vous avez créé des incrustations MQTT, elles seront situées en fin de liste.

-  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct.
- **Size (Taille)** : Sélectionnez la taille de l'incrustation.
- **Visible sur toutes les chaînes** : Désactivez cette option pour afficher uniquement sur la chaîne actuellement sélectionnée. Activez cette option pour afficher sur toutes les chaînes actives.
- **Intervalle de mise à jour** : Choisissez le temps entre les mises à jour des données.
- **Transparency (Transparence)** : Définissez la transparence de toute l'incrustation.
- **Transparence de l'arrière-plan** : Définissez uniquement la transparence de l'arrière-plan de l'incrustation.
- **Points** : Activez cette option pour ajouter un point à la ligne du graphique lorsque les données sont mises à jour.
- **Axe des Y**
 - **Label (Étiquette)** : Entrez le libellé de texte pour l'axe Y
 - **Échelle dynamique** : Activez-le pour que l'échelle s'adapte automatiquement aux valeurs des données. Désactivez cette option pour saisir manuellement les valeurs d'une échelle fixe.
 - **Seuil d'alarme minimum et Seuil d'alarme maximum** : Ces valeurs ajouteront des lignes de référence horizontales au graphique à barres, ce qui permettra de voir plus facilement quand la valeur des données devient trop élevée ou trop faible.

Masques de confidentialité



: Cliquez pour créer un nouveau masque de confidentialité.

Privacy masks (Masques de confidentialité) : Cliquez pour modifier la couleur de tous les masques de confidentialité, ou pour supprimer définitivement tous les masques de confidentialité.

Taille de la cellule : Si vous choisissez la couleur mosaïque, les masques de confidentialité apparaissent comme des motifs pixellisés. Utilisez le curseur pour modifier la taille des pixels.



Mask x (Masque x) : Cliquez pour renommer, désactiver ou supprimer définitivement le masque.

Radar

Paramètres

Général

Transmission radar : Utilisez ceci pour éteindre complètement le module radar.



Canal : Si vous avez des problèmes d'interférence entre plusieurs dispositifs, sélectionnez le même canal pour quatre dispositifs proches les uns des autres. Pour la plupart des installations, sélectionnez **Auto** pour laisser les périphériques négocier automatiquement le canal à utiliser.

Hauteur de montage : Entrez la hauteur de montage du produit.

Remarque

Soyez aussi précis que possible lorsque vous entrez dans la hauteur de montage. Cela permet au dispositif de visualiser la détection radar à la bonne position dans l'image.

Détection

Sensibilité de détection : Sélectionnez la sensibilité du radar. Une valeur plus élevée vous permet d'avoir une plage de détection plus longue, mais le risque de fausses alarmes est également plus élevé. Une sensibilité inférieure réduit le nombre de fausses alarmes, mais peut réduire la plage de détection.

Profil du radar : Sélectionnez un profil adapté à votre domaine d'intérêt.

- **Surveillance de la zone** : Suivez les objets petits et grands qui se déplacent à des vitesses plus basses en zones ouvertes.
 - **Ignore stationary rotating objects (Ignorer les objets rotatifs stationnaires)**  : Activez cette fonction pour minimiser les fausses alarmes à l'aide d'objets stationnaires avec des mouvements rotatifs, tels que des ventilateurs ou des turbines.
 - **Ignorer les petits objets** : Allumez la caméra pour minimiser les fausses alarmes concernant de petits objets, tels que des chats ou des lapins.
 - **Ignorer les objets ondulants** : Activez cette option pour réduire le nombre de fausses alarmes provenant d'objets ondulants, tels que des arbres, des buissons ou des mâts de drapeau.
- **Contrôle des routes** : Suivre les véhicules qui se déplacent à des vitesses plus élevées dans les zones urbaines et les départementales
 - **Ignore stationary rotating objects (Ignorer les objets rotatifs stationnaires)**  : Activez cette fonction pour minimiser les fausses alarmes à l'aide d'objets stationnaires avec des mouvements rotatifs, tels que des ventilateurs ou des turbines.
 - **Ignorer les objets ondulants** : Activez cette option pour réduire le nombre de fausses alarmes provenant d'objets ondulants, tels que des arbres, des buissons ou des mâts de drapeau.

Voir

Légende d'information : activez pour afficher une légende contenant les types d'objet que le radar peut détecter et suivre. Faites glisser-déposer pour déplacer la légende d'informations.

Opacité de la zone : Sélectionnez le niveau d'opacité ou de transparence dans la zone de couverture.

Opacité du réseau : Sélectionnez le niveau d'opacité ou de transparence dans le réseau.

Palette de couleurs : Sélectionnez un thème pour la visualisation du radar.

Rotation  : sélectionnez l'orientation préférée de l'image radar.

Visualisation des objets

Durée du tracé : Sélectionnez la durée de tracé d'un objet suivi dans la vue radar.

Style d'icône : sélectionnez le style d'icône des objets suivis dans la vue radar. Pour les triangles ordinaires, sélectionnez **Triangle**. Pour les symboles représentatifs, sélectionnez **Symbole**. Les icônes pointent dans la direction du mouvement des objets suivis, quel que soit le style.

Afficher les informations avec l'icône : Sélectionnez les informations à afficher à côté de l'icône de l'objet tracé :

- **Type d'objet** : Affiche le type d'objet que le radar a détecté.
- **Probabilité de classification** : Indique à quel point le radar est sûr que la classification des objets est correcte.
- **Vitesse** : Affiche la vitesse de déplacement de l'objet.

Flux

Général

Résolution : Sélectionnez la résolution d'image convenant à la scène de surveillance. Une résolution plus élevée accroît les besoins en matière de bande passante et de stockage.

Fréquence d'images : Pour éviter les problèmes de bande passante sur le réseau ou réduire la taille du stockage, vous pouvez limiter la fréquence d'images à une valeur fixe. Si vous laissez la fréquence d'image à zéro, la fréquence d'image est maintenue à la fréquence la plus élevée possible dans les conditions actuelles. Une fréquence d'images plus élevée nécessite davantage de bande passante et de capacité de stockage.

P-frames (Trames P) : Une image P est une image prédite qui montre uniquement les changements dans l'image par rapport à l'image précédente. Saisissez le nombre de trames P souhaitées. Plus ce nombre est élevé, plus la bande passante nécessaire est faible. Toutefois, en cas d'encombrement du réseau, la qualité de la vidéo peut se détériorer sensiblement.

Compression : Utilisez le curseur pour ajuster la compression de l'image. Une compression élevée se traduit par un débit binaire et une qualité d'image inférieurs. Une faible compression améliore la qualité de l'image, mais utilise davantage de bande passante et de capacité de stockage lors de l'enregistrement.

Signed video (Vidéo signée)  : Activez cette option pour ajouter la fonction de vidéo signée à la vidéo. La vidéo signée protège la vidéo contre la falsification en ajoutant des signatures cryptographiques à la vidéo.

Zipstream

Zipstream est une technologie de réduction du débit binaire optimisée pour la vidéosurveillance qui réduit le débit binaire moyen dans un flux H.264 ou H.265 en temps réel. La technologie Axis Zipstream applique un débit binaire élevé dans les scènes comportant de nombreuses régions d'intérêt, par exemple, des objets en mouvement. Lorsque la scène est plus statique, Zipstream applique un débit binaire inférieur, ce qui réduit l'espace de stockage requis. Pour en savoir plus, voir la section *Diminuer le débit binaire avec Axis Zipstream*

Sélectionnez l'intensité de la réduction du débit binaire :

- **Désactivé** : Aucune réduction du débit binaire.
- **Faible** : Aucune dégradation visible de la qualité dans la plupart des scènes. Il s'agit de l'option par défaut et elle peut être utilisée dans tous les types de scènes pour réduire le débit binaire.
- **Moyenne** : Effets visibles dans certaines scènes, à savoir, moins de bruit, et un niveau de détails légèrement inférieur dans les régions de moindre intérêt (par exemple, absence de mouvement).
- **Élevée** : Effets visibles dans certaines scènes, à savoir, moins de bruit, et un niveau de détails inférieur dans les régions de moindre intérêt (par exemple, absence de mouvement). Nous recommandons ce niveau pour les périphériques connectés au cloud et les périphériques qui utilisent un stockage local.
- **Higher (Plus élevé)** : Effets visibles dans certaines scènes, à savoir, moins de bruit, et un niveau de détails inférieur dans les régions de moindre intérêt (par exemple, absence de mouvement).
- **Extrême** : Effet visible dans la plupart des scènes. Le débit binaire est optimisé pour le stockage le plus petit possible.

Optimiser pour le stockage : Activez cette option réduire le débit binaire tout en conservant la qualité.

L'optimisation ne s'applique pas au flux affiché sur le client Web. Ce système ne peut être utilisé que si votre VMS prend en charge des images B. L'activation de l'option **Optimiser pour le stockage** entraîne l'activation de l'option **GOP dynamique**.

Dynamic FPS (IPS dynamique) (images par seconde) : Activez cette option pour permettre une variation de la bande passante en fonction du niveau d'activité dans la scène. Davantage d'activité nécessite plus de bande passante.

Lower limit (Limite inférieure) : Saisissez une valeur pour ajuster la fréquence d'images entre le nombre d'ips minimal et le nombre d'ips par défaut du flux en fonction du mouvement de la scène. Nous vous recommandons d'utiliser une limite inférieure dans les scènes avec très peu de mouvement, où le nombre d'ips peut chuter à 1 ou moins.

Dynamic GOP (Group of Pictures) (Algorithme dynamique de groupe d'images (GOP) : Activez cette option pour ajuster dynamiquement l'intervalle entre les trames I en fonction du niveau d'activité dans la scène.

Upper limit (Limite supérieure) : Saisissez une longueur de GOP maximale, c'est-à-dire le nombre maximal de trames P entre deux trames I. Une image I est une image autonome qui ne dépend pas des autres images.

Commande du débit binaire

- **Moyenne** : Sélectionnez cette option pour ajuster automatiquement le débit binaire sur une période plus longue et fournir la meilleure qualité d'image possible en fonction du stockage disponible.
 -  Cliquez pour calculer le débit binaire cible en fonction du stockage disponible, de la durée de conservation et de la limite de débit binaire.
 - **Débit binaire cible** : Saisissez le Débit binaire cible souhaité.
 - **Retention time (Durée de conservation)** : Saisissez la durée de stockage en jours des enregistrements.
 - **Stockage** : Affiche le stockage estimé qui peut être utilisé pour le flux.
 - **Maximum bitrate (Débit binaire maximum)** : Activez cette option pour définir une limite de débit binaire.
 - **Bitrate limit (Limite de débit binaire)** : Saisissez une limite de débit binaire supérieure au débit binaire cible.
- **Maximum (Maximum)** : Sélectionnez cette option pour définir le débit binaire instantané maximum du flux en fonction de la bande passante de votre réseau.
 - **Maximum (Maximum)** : Saisissez le débit binaire maximum.
- **Variable (Variable)** : Sélectionnez cette option pour autoriser une variation du débit binaire en fonction du niveau d'activité dans la scène. Davantage d'activité nécessite plus de bande passante. Nous vous recommandons cette option dans la plupart des cas.

Audio

Include (Inclure) : Activez cette option pour utiliser l'audio dans le flux vidéo.

Source (Source)  : Sélectionnez la source audio à utiliser.

Stereo (Stéréo)  : Activez cette option pour inclure l'audio intégré ainsi que l'audio provenant d'un microphone externe.

Calibrage de la carte

Téléchargez et calibrez une carte de référence en utilisant le calibrage de la carte. Le résultat de l'étalonnage est une carte de référence qui affiche le champ de vision du radar à l'échelle appropriée, ce qui permet de voir plus facilement où se déplacent les objets.

Setup assistant (Assistant de configuration) : Cliquez pour ouvrir l'assistant de configuration qui vous guide pas à pas dans l'étalonnage.

Reset calibration (Réinitialiser le calibrage) : Cliquez pour supprimer l'image de la carte actuelle et la position du radar sur la carte.

Carte

Charger la carte : Sélectionnez ou glissez-déplacez l'image de la carte que vous souhaitez charger.

Download map (Télécharger la carte) : Cliquez pour télécharger la carte.

Rotate map (Rotation de la carte) : Utilisez le curseur pour faire pivoter l'image de la carte.

Échelle et distance sur la carte

Distance : Ajoutez la distance entre les deux points que vous avez ajoutés à la carte.

Effectuer un panoramique et un zoom sur la carte

Panoramique : Cliquez sur les boutons pour effectuer un panoramique de l'image de la carte.

Zoom (Zoom) : Cliquez sur les boutons pour effectuer un zoom avant ou arrière sur l'image de la carte.

Reset pan and zoom (Réinitialiser le panoramique et le zoom) : Cliquez pour supprimer les paramètres du panoramique et du zoom.

Position du radar

Position : Cliquez sur les boutons pour déplacer le radar sur la carte.

Rotation : Cliquez sur les boutons pour faire tourner le radar sur la carte.

Zones d'exclusion

Une **zone à exclure** est une zone dans laquelle les objets en mouvement sont ignorés. Utilisez des zones à exclure s'il existe des zones à l'intérieur d'un scénario qui déclenchent un grand nombre d'alarmes indésirables.



: Cliquez pour créer une zone à exclure.

Pour modifier une zone à exclure, sélectionnez-la dans la liste.

Track passing objects (Suivre le passage d'objets) : Activez cette option pour suivre les objets qui passent à travers la zone d'exclusion. Les objets qui passent conservent leurs ID de suivi et sont visibles dans toute la zone. Les objets qui apparaissent dans la zone d'exclusion ne seront pas suivis.

Zone shape presets (Préréglages de forme de zone) : Sélectionnez la forme initiale de la zone à exclure.

- **Cover everything (Tout couvrir)** : Sélectionnez cette option pour définir une zone d'exclusion couvrant l'intégralité de la zone de couverture radar.
- **Reset to box (Réinitialiser dans la case)** : Sélectionnez cette option pour placer une zone d'exclusion rectangulaire au milieu de la zone de couverture.

Pour modifier la forme de la zone, glissez-déplacez l'un des points sur les lignes. Pour retirer un point, effectuez un clic droit dessus.

Scénarios

Un scénario est une combinaison de conditions de déclenchement, ainsi que de paramètres de scène et de détection.



: Cliquez pour créer un nouveau scénario. Vous pouvez créer jusqu'à 20 scénarios.

Conditions du déclenchement : Sélectionnez l'état qui déclenche l'alarme.

- **Mouvements dans la zone** : Indiquez si vous souhaitez déclencher un scénario sur des objets se déplaçant dans une zone.
- **Franchissement de ligne** : Sélectionnez si vous souhaitez que le scénario se déclenche sur des objets traversant une ou deux lignes.

Scène : Définissez la zone ou les lignes dans le scénario où des objets en mouvement déclenchent des alarmes.

- Pour un mouvement dans une zone, sélectionnez une des formes prédéfinies afin de modifier la zone.
- Pour Line crossing (Franchissement de la ligne), faites glisser et déposez-la dans la scène. Pour créer plus de points sur une ligne, cliquez et faites glisser n'importe où. Pour retirer un point, effectuez un clic droit dessus.
 - **Exiger le franchissement de deux lignes** : Allumez-la si l'objet doit passer deux lignes avant que le scénario ne déclenche une alarme.
 - **Changer de direction** : Allumez si vous souhaitez que le scénario déclenche une alarme quand des objets traversent la ligne dans l'autre direction.

Paramètres de détection : Définissez le critère de déclenchement du scénario.

- Pour les mouvements dans la zone :
 - **Ignorer les objets passagers** : Définissez le délai en secondes entre le moment où le radar détecte l'objet et le moment où le scénario déclenche une alarme. Ce paramétrage peut contribuer à réduire le nombre de fausses alarmes.
 - **Déclencher sur le type d'objet** : Sélectionnez le type d'objets (humain, véhicule, inconnu) pour lesquels le scénario doit se déclencher.
 - **Limite de vitesse** : Le déclenchement s'opère sur des objets en mouvement à des vitesses comprises dans une plage spécifique.
 - **Inverser** : Sélectionnez cette fonction si vous souhaitez déclencher des vitesses supérieures ou inférieures à la limite de vitesse définie.
- Pour Line crossing (Franchissement de la ligne) :
 - **Ignorer les objets passagers** : Définissez le délai en secondes entre le moment où le radar détecte l'objet et le moment où le scénario déclenche une action. Ce paramétrage peut contribuer à réduire le nombre de fausses alarmes. Cette option n'est pas disponible pour les objets traversant deux lignes.
 - **Temps max. entre les franchissements** : Définissez la durée maximale entre la traversée de la première ligne et la deuxième ligne. Cette option est uniquement disponible pour les objets traversant deux lignes.
 - **Déclencher sur le type d'objet** : Sélectionnez le type d'objets (humain, véhicule, inconnu) pour lesquels le scénario doit se déclencher.
 - **Limite de vitesse** : Le déclenchement s'opère sur des objets en mouvement à des vitesses comprises dans une plage spécifique.
 - **Inverser** : Sélectionnez cette fonction si vous souhaitez déclencher des vitesses supérieures ou inférieures à la limite de vitesse définie.

Paramètres d'alarme : Définissez les critères pour l'alarme.

- **Durée minimale du déclencheur** : Définissez la durée minimale de l'alarme déclenchée.

Incrustations



: Cliquez pour ajouter une incrustation. Sélectionnez le type d'incrustation dans la liste déroulante :

- **Text (Texte)** : Sélectionnez pour afficher un texte intégré à l'image de la vidéo en direct et visible dans toutes les vues, tous les enregistrements et tous les instantanés. Vous pouvez saisir votre propre texte et inclure des modificateurs pré-configurés pour afficher automatiquement, par exemple, l'heure, la date, la fréquence d'image.
 -  : Cliquez pour ajouter le modificateur de date %F pour afficher le format aaaa-mm-jj.
 -  : Cliquez pour ajouter le modificateur d'heure %X pour afficher le format hh:mm:ss (format 24 heures).
 - **Modificateurs** : Cliquez pour sélectionner l'un des modificateurs de la liste et l'ajouter à la zone de texte. Par exemple, %a affiche le jour de la semaine.
 - **Size (Taille)** : Sélectionnez la taille de police souhaitée.
 - **Appearance (Apparence)** : Sélectionnez la couleur du texte et de l'arrière-plan, par exemple, du texte blanc sur fond noir (par défaut).
 -  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct.
- **Une image** : Sélectionnez pour afficher une image statique superposée au flux vidéo. Vous pouvez utiliser des fichiers .bmp, .png, .jpeg ou .svg. Pour charger une image, cliquez sur **Images**. Avant de charger une image, vous pouvez choisir les options suivantes :
 - **Scale with resolution (Mise à l'échelle)** : Sélectionnez cette option pour adapter automatiquement l'image d'incrustation à la résolution vidéo.
 - **Use transparency (Utiliser la transparence)** : Sélectionnez cette option et saisissez la valeur hexadécimale RVB pour cette couleur. Utilisez le format RRGGBB. Exemples de valeurs hexadécimales : FFFFFFFF pour blanc, 000000 pour noir, FF0000 pour rouge, 6633FF pour bleu et 669900 pour vert. Uniquement pour les images .bmp.
- **Scene annotation (Annotation de la scène)**  : Sélectionnez cette option pour afficher une incrustation de texte dans le flux vidéo qui reste dans la même position, même lorsque la caméra effectue un panoramique ou une inclinaison dans une autre direction. Vous pouvez choisir d'afficher l'incrustation uniquement dans certains niveaux de zoom.
 -  : Cliquez pour ajouter le modificateur de date %F pour afficher le format aaaa-mm-jj.
 -  : Cliquez pour ajouter le modificateur d'heure %X pour afficher le format hh:mm:ss (format 24 heures).
 - **Modificateurs** : Cliquez pour sélectionner l'un des modificateurs de la liste et l'ajouter à la zone de texte. Par exemple, %a affiche le jour de la semaine.
 - **Size (Taille)** : Sélectionnez la taille de police souhaitée.
 - **Appearance (Apparence)** : Sélectionnez la couleur du texte et de l'arrière-plan, par exemple, du texte blanc sur fond noir (par défaut).
 -  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct. L'incrustation est enregistrée et demeure dans les coordonnées de panoramique et d'inclinaison de cette position.
 - **Annotation entre les niveaux de zoom (%)** : Définissez les niveaux de zoom dans lesquels l'incrustation sera affichée.

- **Symbole de l'annotation** : Sélectionnez un symbole qui apparaît à la place de l'incrustation lorsque la caméra n'est pas dans les niveaux de zoom définis.
- **Streaming indicator (Indicateur de diffusion)**  : Sélectionnez cette image pour afficher une animation superposée au flux vidéo. L'animation indique que le flux vidéo est en direct, même si la scène ne contient pas de mouvement.
 - **Appearance (Apparence)** : Sélectionnez la couleur d'animation et la couleur de l'arrière-plan, par exemple, une animation de couleur rouge sur un fond transparent (par défaut).
 - **Size (Taille)** : Sélectionnez la taille de police souhaitée.
 -  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct.
- **Widget : Linegraph (Graphique linéaire)**  : Afficher un graphique qui montre l'évolution d'une valeur mesurée au fil du temps.
 - **Title (Titre)** : Entrez le nom du widget.
 - **Modificateur d'incrustation** : Sélectionnez un modificateur d'incrustation comme source de données. Si vous avez créé des incrustations MQTT, elles seront situées en fin de liste.
 -  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct.
 - **Size (Taille)** : Sélectionnez la taille de l'incrustation.
 - **Visible sur toutes les chaînes** : Désactivez cette option pour afficher uniquement sur la chaîne actuellement sélectionnée. Activez cette option pour afficher sur toutes les chaînes actives.
 - **Intervalle de mise à jour** : Choisissez le temps entre les mises à jour des données.
 - **Transparency (Transparence)** : Définissez la transparence de toute l'incrustation.
 - **Transparence de l'arrière-plan** : Définissez uniquement la transparence de l'arrière-plan de l'incrustation.
 - **Points** : Activez cette option pour ajouter un point à la ligne du graphique lorsque les données sont mises à jour.
 - **Axe des X**
 - **Label (Étiquette)** : Entrez le libellé de texte pour l'axe X.
 - **Fenêtre temporelle** : Entrez la durée pendant laquelle les données sont visualisées.
 - **Unité de temps** : Entrez une unité de temps pour l'axe des X.
 - **Axe des Y**
 - **Label (Étiquette)** : Entrez le libellé de texte pour l'axe Y
 - **Échelle dynamique** : Activez-le pour que l'échelle s'adapte automatiquement aux valeurs des données. Désactivez cette option pour saisir manuellement les valeurs d'une échelle fixe.
 - **Seuil d'alarme minimum et Seuil d'alarme maximum** : Ces valeurs ajouteront des lignes de référence horizontales au graphique, ce qui permettra de voir plus facilement quand la valeur des données devient trop élevée ou trop faible.
- **Widget : Meter (Mètre)**  : Afficher un graphique à barres affichant la valeur de données la plus récemment mesurée.
 - **Title (Titre)** : Entrez le nom du widget.
 - **Modificateur d'incrustation** : Sélectionnez un modificateur d'incrustation comme source de données. Si vous avez créé des incrustations MQTT, elles seront situées en fin de liste.

-  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct.
- **Size (Taille)** : Sélectionnez la taille de l'incrustation.
- **Visible sur toutes les chaînes** : Désactivez cette option pour afficher uniquement sur la chaîne actuellement sélectionnée. Activez cette option pour afficher sur toutes les chaînes actives.
- **Intervalle de mise à jour** : Choisissez le temps entre les mises à jour des données.
- **Transparency (Transparence)** : Définissez la transparence de toute l'incrustation.
- **Transparence de l'arrière-plan** : Définissez uniquement la transparence de l'arrière-plan de l'incrustation.
- **Points** : Activez cette option pour ajouter un point à la ligne du graphique lorsque les données sont mises à jour.
- **Axe des Y**
 - **Label (Étiquette)** : Entrez le libellé de texte pour l'axe Y
 - **Échelle dynamique** : Activez-le pour que l'échelle s'adapte automatiquement aux valeurs des données. Désactivez cette option pour saisir manuellement les valeurs d'une échelle fixe.
 - **Seuil d'alarme minimum et Seuil d'alarme maximum** : Ces valeurs ajouteront des lignes de référence horizontales au graphique à barres, ce qui permettra de voir plus facilement quand la valeur des données devient trop élevée ou trop faible.

Suivi automatique PTZ du radar

Apparez le radar à une caméra PTZ pour utiliser le suivi automatique radar. Pour établir la connexion, allez à **Système > Edge-to-Edge**.

Configurer les paramètres initiaux :

Camera mounting height (Hauteur de montage de la caméra) : distance entre le sol et la hauteur de la caméra PTZ montée.

Alignement panoramique : Faites un panoramique avec la caméra PTZ de sorte qu'elle pointe dans la même direction que le radar. Cliquez sur l'adresse IP de la caméra PTZ pour y accéder.

Enregistrer le décalage panoramique : Cliquez pour enregistrer l'alignement panoramique.

Décalage de l'inclinaison au sol : Utilisez le décalage de l'inclinaison au sol pour ajuster l'inclinaison de la caméra. Si le sol est en pente ou si la caméra n'est pas montée horizontalement, elle peut être orientée trop haut ou trop bas lorsqu'elle suit un objet.

Terminé : cliquez pour enregistrer vos paramètres et poursuivre la configuration.

Configurer le suivi automatique PTZ :

Suivi : sélectionnez cette option si vous souhaitez suivre des personnes, des véhicules et/ou des objets inconnus.

Suivi : activez cette option pour commencer à suivre des objets avec la caméra PTZ. Le suivi zoome automatiquement sur un objet ou un groupe d'objets pour les garder dans la vue de la caméra.

Changement d'objet : Si le radar détecte plusieurs objets qui ne rentrent pas dans la vue de la caméra PTZ, la caméra PTZ suit l'objet auquel le radar affecte la priorité la plus élevée et ignore les autres.

Durée de maintien de l'objet : Détermine la durée en secondes pendant laquelle la caméra PTZ suit chaque objet.

Revenir à l'accueil : Activez cette option pour que la caméra PTZ revienne à sa position initiale lorsque le radar ne suit plus aucun objet.

Revenir à l'expiration accueil : Détermine la durée pendant laquelle la caméra PTZ doit rester sur la dernière position connue des objets suivis avant le retour à la position initiale.

Zoom (Zoom) : Déplacez le curseur pour régler le zoom de la caméra PTZ.

Reconfigurer l'installation : Cliquez pour effacer tous les paramètres et revenir à la configuration initiale.

Calibrage automatique

Élévation

Status (Statut) : Indique si les données de calibrage sont disponibles ou non. La caméra et le radar recueillent les données de calibrage en continu.

Autocalibration (Calibrage automatique) : Activez cette option pour calibrer automatiquement la scène. Le calibrage automatique est effectué lorsque les données de calibrage sont disponibles. Vérifiez l'état de disponibilité.

Smoothing (Lissage) : Permet de lisser les différences de hauteur.

- **Élevée** : Le lissage doit être réglé sur **High (Élevé)** dans les scènes où les différences de hauteur sont faibles.
- **Faible** : Le lissage doit être réglé sur **Low (Faible)** dans les scènes où les différences de hauteur sont plus importantes, par exemple s'il y a des collines ou des escaliers.

Réinitialiser : Réinitialise le calibrage automatique et les données de calibrage recueillies.

Show elevation pattern (Afficher la configuration de la hauteur) : Activez cette option pour visualiser le calibrage. Affiche la distance verticale entre le sol et la caméra dans un schéma de points colorés. Le schéma est visible sur cette page uniquement, pas dans le flux vidéo ni dans le radar.

Show color legend (Afficher la légende des couleurs) : Activez cette option pour afficher une légende contenant les couleurs du modèle de hauteur et la distance verticale que représente chaque couleur. La légende est visible sur cette page uniquement, pas dans le flux vidéo ni dans le radar.

Couleur : Sélectionnez les couleurs pour le modèle de hauteur.

Show reference area (Afficher la zone de référence) : Activez cette option pour afficher la zone sur laquelle repose le calibrage. La zone est visible sur cette page uniquement, pas dans le flux vidéo ni dans le radar.

Azimut

Status (Statut) : Indique si les données de calibrage sont disponibles ou non. La caméra et le radar recueillent les données de calibrage en continu.

Autocalibration (Calibrage automatique) : Activez cette option pour calibrer automatiquement la scène. Le calibrage automatique est effectué lorsque les données de calibrage sont disponibles. Vérifiez l'état de disponibilité.

Réinitialiser : Réinitialise le calibrage automatique et les données de calibrage recueillies.

Fonctions d'analyse

AXIS Object Analytics

Start (Démarrer) : Cliquez pour démarrer AXIS Object Analytics. L'application s'exécute en arrière-plan et vous pouvez créer des règles pour les événements en fonction des paramètres actuels de l'application.

Open (Ouvrir) : Cliquez pour ouvrir AXIS Object Analytics. L'application s'ouvre dans un nouvel onglet du navigateur, où vous pouvez configurer ses paramètres.

- **Not installed (Non installé)** : AXIS Object Analytics n'est pas installé sur ce périphérique. Mettez à niveau le système d'exploitation AXIS vers la dernière version pour obtenir la dernière version de l'application.

AXIS Image Health Analytics

Start (Démarrer) : Cliquez pour lancer AXIS Image Health Analytics. L'application s'exécute en arrière-plan et vous pouvez créer des règles pour les événements en fonction des paramètres actuels de l'application.

Open (Ouvrir) : Cliquez pour ouvrir AXIS Image Health Analytics. L'application s'ouvre dans un nouvel onglet du navigateur, où vous pouvez configurer ses paramètres.

- **Not installed (Non installé)** : AXIS Image Health Analytics n'est pas installé sur ce périphérique. Mettez à niveau le système d'exploitation AXIS vers la dernière version pour obtenir la dernière version de l'application.

Visualisation des métadonnées

La caméra détecte les objets en mouvement et les classe en fonction du type d'objet. Dans la vue, un objet classé est entouré d'une matrice de caractères colorée et un ID lui est affecté.

Id : Numéro d'identification unique pour l'objet identifié et le type. Ce numéro s'affiche à la fois dans la liste et dans la vue.

Type : Classifie un objet en mouvement comme une personne, un visage, une voiture, un bus, un camion, un bicyclette ou une plaque d'immatriculation. La couleur de la matrice de caractères dépend de la classification de type.

Confiance : La barre indique le niveau de confiance dans la classification du type d'objet.

Configuration des métadonnées

Producteurs de métadonnées RTSP

Répertorient les applications qui diffusent des métadonnées et les canaux qu'elles utilisent.

Remarque

Ces paramètres concernent les flux de métadonnées RTSP qui utilisent ONVIF XML. Les changements effectués ici n'affectent pas la page de visualisation des métadonnées.

Producteur : L'application qui produit les métadonnées. L'application ci-dessous constitue la liste des types de métadonnées que l'application diffuse depuis le périphérique.

Canal : Canal utilisé par l'application. Sélectionnez cette option pour activer le flux de métadonnées. Désélectionnez-la pour des raisons de compatibilité ou de gestion des ressources.

Audio

Paramètres du périphérique

Entrée : Activer ou désactiver l'entrée audio. Indique le type d'entrée.

Input type (Type d'entrée) ⓘ : Sélectionnez le type d'entrée, par exemple s'il s'agit d'un microphone interne ou d'une entrée de ligne.

Power type (Type d'alimentation) ⓘ : Sélectionnez le type d'alimentation pour votre entrée.

Apply changes (Appliquer les modifications) ⓘ : Appliquez votre sélection.

Echo cancellation (Suppression d'écho) ⓘ : Activez cette option pour supprimer les échos lors d'une communication bidirectionnelle.

Séparer les contrôles du gain ⓘ : Activez cette option pour ajuster le gain séparément pour les différents types d'entrée.

Contrôle automatique du gain ⓘ : Activez cette option pour adapter dynamiquement le gain aux changements apportés au son.

Gain (Gain) : Utilisez le curseur pour modifier le gain. Cliquez sur l'icône du microphone pour le désactiver ou l'activer.

Sortie : Indique le type de sortie.

Gain (Gain) : Utilisez le curseur pour modifier le gain. Cliquez sur l'icône du haut-parleur pour le désactiver ou le réactiver.

Automatic volume control (Contrôle automatique du volume) ⓘ : Activez cette option pour que le périphérique règle automatiquement et dynamiquement le gain en fonction du niveau de bruit ambiant. Le contrôle automatique du volume affecte toutes les sorties audio, y compris la ligne et la bobine téléphonique.

Flux

Encodage : Sélectionnez l'encodage à utiliser pour le flux de la source d'entrée. Vous pouvez uniquement choisir l'encodage si l'entrée audio est allumée. Si l'entrée audio est hors tension, cliquez sur **Enable audio input (Activer l'entrée audio)** pour l'activer.

Clips audio

 **Add clip (Ajouter un clip)** : Ajoutez une nouveau clip audio. Vous pouvez utiliser des fichiers .au, .mp3, .opus, .vorbis, .wav.

 Lisez le clip audio.

 Arrêtez la lecture du clip audio.

 Le menu contextuel contient :

- **Rename (Renommer)** : Modifiez le nom du clip audio.
- **Create link (Créer un lien)** : Créez une URL qui, lorsqu'elle est utilisée, lit le clip audio sur le périphérique. Indiquez le volume et le nombre de lectures du clip.
- **Download (Télécharger)** : Téléchargez le clip audio sur votre ordinateur.
- **Supprimer** : Supprimez le clip audio du périphérique.

Amélioration audio

Entrée

Égalisateur audio graphique 10 bandes : Activez-le pour ajuster le niveau des différentes fréquences d'écoute dans un signal audio. Cette fonction est destinée aux utilisateurs avancés qui ont l'expérience de la configuration audio.

Plage de conversation  : choisissez la plage de fonctionnement pour collecter le contenu audio. Une augmentation de la plage opérationnelle entraîne une réduction des capacités simultanées de communication bidirectionnelle.

Amélioration vocale  : Activez-la pour élever la qualité du contenu vocal par rapport à d'autres sons.

Enregistrements

Enregistrements en cours : Afficher tous les enregistrements en cours sur le périphérique.

- Démarrer un enregistrement sur le périphérique.

 Choisir le périphérique de stockage sur lequel enregistrer.

- Arrêter un enregistrement sur le périphérique.

Les **enregistrements déclenchés** se terminent lorsqu'ils sont arrêtés manuellement ou lorsque le périphérique est arrêté.

Les **enregistrements continus** se poursuivent jusqu'à ce qu'ils soient arrêtés manuellement. Même si le périphérique est arrêté, l'enregistrement continue lorsque le périphérique démarre à nouveau.



Lire l'enregistrement.



Arrêter la lecture de l'enregistrement.



Afficher ou masquer les informations et les options sur l'enregistrement.

Définir la plage d'exportation : Si vous souhaitez uniquement exporter une partie de l'enregistrement, entrez une durée. Notez que si vous travaillez dans un fuseau horaire différent de l'emplacement du périphérique, la durée est basée sur le fuseau horaire du périphérique.

Crypter : Sélectionnez un mot de passe pour l'exportation des enregistrements. Il ne sera pas possible d'ouvrir le fichier exporté sans le mot de passe.



Cliquez pour supprimer un enregistrement.

Exporter : Exporter la totalité ou une partie de l'enregistrement.



Cliquez pour filtrer les enregistrements.

From (Du) : Afficher les enregistrements effectués au terme d'une certaine période.

To (Au) : Afficher les enregistrements jusqu'à une certaine période.

Source (Source) ⓘ : Afficher les enregistrements en fonction d'une source. La source fait référence au capteur.

Event (Événement) : Afficher les enregistrements en fonction d'événements.

Stockage : Afficher les enregistrements en fonction d'un type de stockage.

Applications



Add app (Ajouter une application) : Installer une nouvelle application.

Find more apps (Trouver plus d'applications) : Trouver d'autres applications à installer. Vous serez redirigé vers une page d'aperçu des applications Axis.

Allow unsigned apps (Autoriser les applications non signées)  : Activez cette option pour autoriser l'installation d'applications non signées.



Consultez les mises à jour de sécurité dans les applications AXIS OS et ACAP.

Remarque

Les performances du périphérique peuvent être affectées si vous exécutez plusieurs applications en même temps.

Utilisez le commutateur en regard du nom de l'application pour démarrer ou arrêter l'application.

Open (Ouvrir) : Accéder aux paramètres de l'application. Les paramètres disponibles dépendent de l'application. Certaines applications n'ont pas de paramètres.



Le menu contextuel peut contenir une ou plusieurs des options suivantes :

- **Licence Open-source** : Affichez des informations sur les licences open source utilisées dans l'application.
- **App log (Journal de l'application)** : Affichez un journal des événements de l'application. Le journal est utile lorsque vous contactez le support.
- **Activate license with a key (Activer la licence avec une clé)** : si l'application nécessite une licence, vous devez l'activer. Utilisez cette option si votre périphérique n'a pas accès à Internet. Si vous n'avez pas de clé de licence, accédez à axis.com/products/analytics. Vous avez besoin d'un code de licence et du numéro de série du produit Axis pour générer une clé de licence.
- **Activate license automatically (Activer la licence automatiquement)** : si l'application nécessite une licence, vous devez l'activer. Utilisez cette option si votre périphérique a accès à Internet. Vous avez besoin d'un code de licence pour activer la licence.
- **Désactiver la licence** : Désactivez la licence pour la remplacer par une autre, par exemple, lorsque vous remplacez une licence d'essai par une licence complète. Si vous désactivez la licence, vous la supprimez aussi du périphérique.
- **Settings (Paramètres)** : configurer les paramètres.
- **Supprimer** : supprimez l'application de manière permanente du périphérique. Si vous ne désactivez pas d'abord la licence, elle reste active.

Système

Heure et emplacement

Date et heure

Le format de l'heure dépend des paramètres de langue du navigateur Web.

Remarque

Nous vous conseillons de synchroniser la date et l'heure du périphérique avec un serveur NTP.

Synchronization (Synchronisation) : sélectionnez une option pour la synchronisation de la date et de l'heure du périphérique.

- **Automatic date and time (manual NTS KE servers) (Date et heure automatiques (serveurs NTS KE manuels))** Synchronisez avec les serveurs d'établissement de clés NTP sécurisés connectés au serveur DHCP.
 - **Serveurs NTS KE manuels** : saisissez l'adresse IP d'un ou de deux serveurs NTP. Si vous utilisez deux serveurs NTP, le périphérique synchronise et adapte son heure en fonction des entrées des deux serveurs.
 - **Max NTP poll time (Délai maximal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente maximale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
 - **Min NTP poll time (Délai minimal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente minimale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
- **Automatic date and time (NTP servers using DHCP) (Date et heure automatiques (serveurs NTP utilisant DHCP))** : synchronisez avec les serveurs NTP connectés au serveur DHCP.
 - **Serveurs NTP de secours** : saisissez l'adresse IP d'un ou de deux serveurs de secours.
 - **Max NTP poll time (Délai maximal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente maximale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
 - **Min NTP poll time (Délai minimal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente minimale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
- **Automatic date and time (serveurs NTP manuels) (Date et heure automatiques (serveur NTP manuel))** : synchronisez avec les serveurs NTP de votre choix.
 - **Serveurs NTP manuels** : saisissez l'adresse IP d'un ou de deux serveurs NTP. Si vous utilisez deux serveurs NTP, le périphérique synchronise et adapte son heure en fonction des entrées des deux serveurs.
 - **Max NTP poll time (Délai maximal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente maximale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
 - **Min NTP poll time (Délai minimal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente minimale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
- **Custom date and time (Date et heure personnalisées)** : Réglez manuellement la date et l'heure. Cliquez sur **Get from system (Récupérer du système)** pour récupérer les paramètres de date et d'heure une fois de votre ordinateur ou de votre périphérique mobile.

Fuseau horaire : sélectionnez le fuseau horaire à utiliser. L'heure est automatiquement réglée pour l'heure d'été et l'heure standard.

- **DHCP** : Adopte le fuseau horaire du serveur DHCP. Pour que cette option puisse être sélectionnée, le périphérique doit être connecté à un serveur DHCP.
- **Manuel** : Sélectionnez un fuseau horaire dans la liste déroulante.

Remarque

Le système utilise les paramètres de date et heure dans tous les enregistrements, journaux et paramètres système.

Localisation du périphérique

Indiquez où se trouve le dispositif. Le système de gestion vidéo peut utiliser ces informations pour placer le dispositif sur une carte.

- **Format** : Sélectionnez le format à utiliser lorsque vous saisissez la latitude et la longitude de votre périphérique.
- **Latitude** : Les valeurs positives indiquent le nord de l'équateur.
- **Longitude** : Les valeurs positives indiquent l'est du premier méridien.
- **En-tête** : Saisissez l'orientation de la boussole à laquelle fait face le périphérique. 0 indique le nord.
- **Étiquette** : Saisissez un nom descriptif pour votre périphérique.
- **Enregistrer** : Cliquez pour enregistrer l'emplacement de votre périphérique.

Paramètres régionaux

Paramétrez le système de mesure à utiliser pour tous les paramètres système.

Metric (m, km/h) (Métrique) : Sélectionnez pour que la distance soit mesurée en mètres et la vitesse en kilomètres par heure.

U.S. customary (ft, mph) (Américain standard) : Sélectionnez pour que la distance soit mesurée en pieds et la vitesse en miles par heure.

Réseau

IPv4

Assign IPv4 automatically (Assigner IPv4 automatiquement) : Sélectionnez cette option pour laisser le routeur réseau attribuer une adresse IP au périphérique automatiquement. Nous recommandons l'IP automatique (DHCP) pour la plupart des réseaux.

Adresse IP : Saisissez une adresse IP unique pour le périphérique. Des adresses IP statiques peuvent être affectées au hasard dans des réseaux isolés, à condition que chaque adresse soit unique. Pour éviter les conflits, nous vous recommandons de contacter votre administrateur réseau avant d'attribuer une adresse IP statique.

Masque de sous-réseau : Saisissez le masque de sous-réseau pour définir les adresses à l'intérieur du réseau local. Toute adresse en dehors du réseau local passe par le routeur.

Routeur : Saisissez l'adresse IP du routeur par défaut (passerelle) utilisé pour connecter les appareils qui sont reliés à différents réseaux et segments de réseaux.

L'adresse IP statique est la solution de secours si le protocole DHCP n'est pas disponible : Sélectionnez cette option pour ajouter une adresse IP statique à utiliser comme solution de secours si DHCP n'est pas disponible et que vous ne pouvez pas assigner une adresse IP automatiquement.

Remarque

Si DHCP n'est pas disponible et que le périphérique utilise une solution de secours d'adresse statique, cette dernière est configurée avec une portée limitée.

IPv6

Assign IPv6 automatically (Assigner IPv6 automatiquement) : Sélectionnez cette option pour activer IPv6 et laisser le routeur réseau attribuer une adresse IP au périphérique automatiquement.

Nom d'hôte

Attribuer un nom d'hôte automatiquement : Sélectionnez cette option pour laisser le routeur réseau attribuer un nom d'hôte au périphérique automatiquement.

Nom d'hôte : Saisissez manuellement le nom d'hôte afin de l'utiliser comme autre façon d'accéder au périphérique. Le rapport du serveur et le journal système utilisent le nom d'hôte. Les caractères autorisés sont les suivants : A-Z, a-z, 0-9 et -.

Activez les mises à jour DNS dynamiques : Autorisez votre périphérique à mettre automatiquement à jour les enregistrements de son serveur de noms de domaine chaque fois que son adresse IP change.

Register DNS name (Enregistrer le nom DNS) : Saisissez un nom de domaine unique qui pointe vers l'adresse IP de votre périphérique. Les caractères autorisés sont les suivants : A-Z, a-z, 0-9 et -.

TTL : le TTL (Time to Live) paramètre la durée pendant laquelle un enregistrement DNS reste valide jusqu'à ce qu'il doive être mis à jour.

Serveurs DNS

Affecter DNS automatiquement : Sélectionnez cette option pour laisser le serveur DHCP assigner automatiquement des domaines de recherche et des adresses de serveur DNS au périphérique. Nous recommandons le DNS automatique (DHCP) pour la plupart des réseaux.

Domaines de recherche : Lorsque vous utilisez un nom d'hôte qui n'est pas entièrement qualifié, cliquez sur **Ajouter un domaine de recherche (Add search domain)** et saisissez un domaine dans lequel rechercher le nom d'hôte utilisé par le périphérique.

Serveurs DNS : Cliquez sur **Add DNS server (Serveur DNS principal)** et saisissez l'adresse IP du serveur DNS. Cela assure la conversion de noms d'hôte en adresses IP sur votre réseau.

HTTP et HTTPS

Le protocole HTTPS permet le cryptage des demandes de consultation de pages des utilisateurs, ainsi que des pages envoyées en réponse par le serveur Web. L'échange crypté des informations est régi par l'utilisation d'un certificat HTTPS, garantissant l'authenticité du serveur.

Pour utiliser HTTPS sur le périphérique, vous devez installer un certificat HTTPS. Accédez à **System > Security (Système > Sécurité)** pour créer et installer des certificats.

Autoriser l'accès via : Sélectionnez cette option si un utilisateur est autorisé à se connecter au périphérique via HTTP, HTTPS, ou les deux protocoles HTTP et HTTPS.

Remarque

Si vous affichez des pages Web cryptées via HTTPS, il se peut que vos performances baissent, en particulier lorsque vous faites une requête de page pour la première fois.

Port HTTP : Entrez le port HTTP à utiliser. Le périphérique autorise le port 80 ou tout port de la plage 1024-65535. Si vous êtes connecté en tant qu'administrateur, vous pouvez également saisir n'importe quel port de la plage 1-1023. Si vous utilisez un port de cette plage, vous recevez un avertissement.

Port HTTPS : Entrez le port HTTPS à utiliser. Le périphérique autorise le port 443 ou tout port de la plage 1024-65535. Si vous êtes connecté en tant qu'administrateur, vous pouvez également saisir n'importe quel port de la plage 1-1023. Si vous utilisez un port de cette plage, vous recevez un avertissement.

Certificat : Sélectionnez un certificat pour activer HTTPS pour le périphérique.

Proxy mondiaux

Http proxy (Proxy HTTP) : Spécifiez un hôte ou une adresse IP de proxy mondial selon le format autorisé.

Https proxy (Proxy HTTPS) : Spécifiez un hôte ou une adresse IP de proxy mondial selon le format autorisé.

Formats autorisés pour les proxys HTTP et HTTPS :

- `http(s)://hôte:port`
- `http(s)://utilisateur@hôte:port`
- `http(s)://utilisateur:motdepasse@hôte:port`

Remarque

Redémarrez le dispositif pour appliquer les paramètres du proxy mondial.

No proxy (Aucun proxy) : Utilisez **No proxy (Aucun proxy)** pour contourner les proxys mondiaux. Saisissez l'une des options de la liste ou plusieurs options séparées par une virgule :

- Laisser vide
- Spécifier une adresse IP
- Spécifier une adresse IP au format CIDR
- Indiquer un nom de domaine, par exemple : `www.<nom de domaine>.com`
- Indiquer tous les sous-domaines d'un domaine spécifique, par exemple `.<nom de domaine>.com`

Protocoles de découverte de réseau

Bonjour® Activez cette option pour effectuer une détection automatique sur le réseau.

Nom Bonjour : Saisissez un pseudonyme qui sera visible sur le réseau. Le nom par défaut est le nom du périphérique et l'adresse MAC.

UPnP® : Activez cette option pour effectuer une détection automatique sur le réseau.

Nom UPnP : Saisissez un pseudonyme qui sera visible sur le réseau. Le nom par défaut est le nom du périphérique et l'adresse MAC.

WS-Discovery : Activez cette option pour effectuer une détection automatique sur le réseau.

LLDP et CDP : Activez cette option pour effectuer une détection automatique sur le réseau. La désactivation de LLDP et CDP peut avoir une incidence sur la négociation de puissance PoE. Pour résoudre tout problème avec la négociation de puissance PoE, configurez le commutateur PoE pour la négociation de puissance PoE matérielle uniquement.

Connexion au cloud en un clic

One-Click Cloud Connect (O3C) associé à un service O3C fournit un accès Internet simple et sécurisé à des vidéos en direct et enregistrées accessibles depuis n'importe quel lieu. Pour plus d'informations, voir axis.com/end-to-end-solutions/hosted-services.

Autoriser O3C :

- **Un clic** : Ce sont les paramètres par défaut. Maintenez le bouton de commande enfoncé sur le périphérique pour établir une connexion avec un service O3C via Internet. Vous devez enregistrer le périphérique auprès du service O3C dans les 24 heures après avoir appuyé sur le bouton de commande. Sinon, le périphérique se déconnecte du service O3C. Une fois l'enregistrement du périphérique effectué, **Always (Toujours)** est activé et le périphérique reste connecté au service O3C.
- **Toujours** : Le périphérique tente en permanence d'établir une connexion avec un service O3C via Internet. Une fois que vous êtes inscrit, il reste connecté au service O3C. Utilisez cette option si le bouton de commande du périphérique est hors de portée.
- **Non** : Désactive le service O3C.

Proxy settings (Paramètres proxy) : si besoin, saisissez les paramètres proxy à connecter au serveur proxy.

Hôte : Saisissez l'adresse du serveur proxy.

Port : Saisissez le numéro du port utilisé pour l'accès.

Identifiant et mot de passe : Si nécessaire, saisissez un nom d'utilisateur et un mot de passe pour le serveur proxy.

Authentication method (Méthode d'authentification) :

- **Base** : Cette méthode est le schéma d'authentification le plus compatible pour HTTP. Elle est moins sécurisée que la méthode **Digest**, car elle envoie le nom d'utilisateur et le mot de passe non cryptés au serveur.
- **Digest** : Cette méthode est plus sécurisée car elle transfère toujours le mot de passe crypté à travers le réseau.
- **Auto** : Cette option permet au périphérique de sélectionner la méthode d'authentification selon les méthodes prises en charge. Elle donne priorité à la méthode **Digest** sur la méthode **Base**.

Clé d'authentification propriétaire (OAK) : Cliquez sur **Get key (Récupérer la clé)** pour récupérer la clé d'authentification du propriétaire. Cela n'est possible que si le périphérique est connecté à Internet sans pare-feu ni proxy.

SNMP

Le protocole SNMP (Simple Network Management Protocol) autorise la gestion à distance des périphériques réseau.

SNMP : Sélectionnez la version de SNMP à utiliser.

- **v1 et v2c :**
 - **Communauté en lecture :** Saisissez le nom de la communauté disposant d'un accès en lecture seule à tous les objets SNMP pris en charge. La valeur par défaut est **publique**.
 - **Communauté en écriture :** Saisissez le nom de la communauté disposant d'un accès en lecture ou en écriture seule à tous les objets SNMP pris en charge (à l'exception des objets en lecture seule). La valeur par défaut est **écriture**.
 - **Activer les déroutements :** Activez cette option pour activer les rapports de déroutement. Le périphérique utilise les déroutements pour envoyer des messages à un système de gestion concernant des événements importants ou des changements de statut. Dans l'interface Web, vous pouvez configurer des déroutements pour SNMP v1 et v2c. Les déroutements sont automatiquement désactivés si vous passez à SNMP v3 ou si vous désactivez SNMP. Si vous utilisez SNMP v3, vous pouvez configurer les déroutements via l'application de gestion SNMP v3.
 - **Adresse de déroutement :** Entrez l'adresse IP ou le nom d'hôte du serveur de gestion.
 - **Communauté de déroutement :** saisissez la communauté à utiliser lors de l'envoi d'un message de déroutement au système de gestion.
 - **Déroutements :**
 - **Démarrage à froid :** Envoie un message de déroutement au démarrage du périphérique.
 - **Lien vers le haut :** Envoie un message d'interruption lorsqu'un lien change du bas vers le haut.
 - **Link down (Lien bas) :** Envoie un message d'interruption lorsqu'un lien passe du haut vers le bas.
 - **Échec de l'authentification :** Envoie un message de déroutement en cas d'échec d'une tentative d'authentification.

Remarque

Tous les déroutements Axis Video MIB sont activés lorsque vous activez les déroutements SNMP v1 et v2c. Pour plus d'informations, reportez-vous à *AXIS OS Portal > SNMP*.

- **v3 :** SNMP v3 est une version plus sécurisée qui fournit un cryptage et mots de passe sécurisés. Pour utiliser SNMP v3, nous vous recommandons d'activer HTTPS, car le mot de passe est envoyé via ce protocole. Cela empêche également les tiers non autorisés d'accéder aux déroutements v1 et v2c SNMP non cryptés. Si vous utilisez SNMP v3, vous pouvez configurer les déroutements via l'application de gestion SNMP v3.
 - **Mot de passe pour le compte « initial » :** Saisissez le mot de passe SNMP du compte nommé « initial ». Bien que le mot de passe puisse être envoyé sans activer le protocole HTTPS, nous ne le recommandons pas. Le mot de passe SNMP v3 ne peut être configuré qu'une fois, et de préférence seulement lorsque le protocole HTTPS est activé. Une fois le mot de passe configuré, le champ de mot de passe ne s'affiche plus. Pour reconfigurer le mot de passe, vous devez réinitialiser le périphérique aux paramètres des valeurs par défaut.

Sécurité

Certificats

Les certificats sont utilisés pour authentifier les périphériques d'un réseau. Le périphérique prend en charge deux types de certificats :

- **Certificats serveur/client**
Un certificat serveur/client valide l'identité du périphérique et peut être auto-signé ou émis par une autorité de certification (CA). Un certificat auto-signé offre une protection limitée et peut être utilisé avant l'obtention d'un certificat CA émis.
- **Certificats CA**
Un certificat CA permet d'authentifier un certificat d'homologue, par exemple pour valider l'identité d'un serveur d'authentification lorsque le périphérique se connecte à un réseau protégé par IEEE 802.1X. Le périphérique dispose de plusieurs certificats CA préinstallés.

Les formats suivants sont pris en charge :

- Formats de certificats : .PEM, .CER et .PFX
- Formats de clés privées : PKCS#1 et PKCS#12

Important

Si vous réinitialisez le périphérique aux valeurs par défaut, tous les certificats sont supprimés. Les certificats CA préinstallés sont réinstallés.



Add certificate (Ajouter un certificat) : Cliquez pour ajouter un certificat. Un guide étape par étape s'ouvre.

- **More (Plus)** : Afficher davantage de champs à remplir ou à sélectionner.
- **Keystore sécurisé** : Sélectionnez cette option pour utiliser **Trusted Execution Environment (SoC TEE)** (Environnement d'exécution de confiance), **Secure element** (Élément sécurisé) ou **Trusted Platform Module 2.0** (Module TPM 2.0) afin de stocker de manière sécurisée la clé privée. Pour plus d'informations sur le keystore sécurisé à sélectionner, allez à help.axis.com/en-us/axis-os#cryptographic-support.
- **Type de clé** : Sélectionnez l'algorithme de cryptage par défaut ou un autre algorithme dans la liste déroulante pour protéger le certificat.



Le menu contextuel contient :

- **Certificate information (Informations sur le certificat)** : Affichez les propriétés d'un certificat installé.
- **Delete certificate (Supprimer certificat)** : supprimez le certificat.
- **Create certificate signing request (Créer une demande de signature du certificat)** : créez une demande de signature du certificat pour l'envoyer à une autorité d'enregistrement afin de demander un certificat d'identité numérique.

Secure keystore (Keystore sécurisé) :

- **Trusted Execution Environment (SoC TEE)** (Environnement d'exécution de confiance) : Sélectionnez cette option pour utiliser le TEE du SoC pour le keystore sécurisé.
- **Secure element (CC EAL6+)** : Sélectionnez cette touche pour utiliser l'élément sécurisé pour le keystore sécurisé.
- **Module de plateforme sécurisée 2.0 (CC EAL4+, FIPS 140-2 niveau 2)** : Sélectionnez TPM 2.0 pour le keystore sécurisé.

Politique cryptographique

La politique cryptographique définit la manière dont le cryptage est utilisé pour protéger les données.

Active (Actif) : Sélectionnez la politique cryptographique à appliquer au périphérique :

- **Default — OpenSSL (Par défaut — OpenSSL) :** Équilibre entre sécurité et performance pour une utilisation générale.
- **FIPS — Policy to comply with FIPS 140–2 (FIPS — Politique de conformité à la norme FIPS 140–2) :** Cryptage de haute sécurité conforme à la norme FIPS 140–2 pour les industries réglementées.

Contrôle d'accès réseau et cryptage

Norme IEEE 802.1x

La norme IEEE 802.1x est une norme IEEE servant au contrôle de l'admission au réseau basé sur les ports en fournissant une authentification sécurisée des périphériques réseau câblés et sans fil. IEEE 802.1x repose sur le protocole EAP (Extensible Authentication Protocol).

Pour accéder à un réseau protégé par IEEE 802.1x, les périphériques réseau doivent s'authentifier. L'authentification est réalisée par un serveur d'authentification, généralement un serveur RADIUS (par exemple le Service d'Authentification Internet de Microsoft et FreeRADIUS).

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec est une norme IEEE pour la sécurité du contrôle d'accès au support (MAC) qui définit la confidentialité et l'intégrité des données sans connexion pour les protocoles indépendants de l'accès au support.

Certificats

Lorsqu'il est configuré sans certificat CA, la validation du certificat du serveur est désactivée et le périphérique essaie de s'authentifier indépendamment du réseau auquel il est connecté.

En cas d'utilisation d'un certificat, lors de l'implémentation Axis, le périphérique et le serveur d'authentification s'authentifient avec des certificats numériques à l'aide de EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

Pour permettre au périphérique d'accéder à un réseau protégé par des certificats, vous devez installer un certificat client signé sur le périphérique.

Authentication method (Méthode d'authentification) : Sélectionnez un type EAP utilisé pour l'authentification.

Certificat client : Sélectionnez un certificat client pour utiliser IEEE 802.1x. Le serveur d'authentification utilise le certificat CA pour valider l'identité du client.

Certificats CA : Sélectionnez les certificats CA pour valider l'identité du serveur d'authentification. Si aucun certificat n'est sélectionné, le périphérique essaie de s'authentifier indépendamment du réseau auquel il est connecté.

Identité EAP : Saisissez l'option Identity (Identité) de l'utilisateur associée au certificat du client.

Version EAPOL : sélectionnez la version EAPOL utilisée dans votre commutateur réseau.

Utiliser IEEE 802.1x : Sélectionnez cette option pour utiliser le protocole IEEE 802.1x.

Ces paramètres ne sont disponibles que si vous utilisez IEEE 802.1x PEAP-MSCHAPv2 comme méthode d'authentification :

- **Mot de passe :** Saisissez le mot de passe pour l'identité de votre utilisateur.
- **Version Peap :** sélectionnez la version Peap utilisée dans votre commutateur réseau.
- **Étiquette :** Sélectionnez 1 pour utiliser le cryptage EAP du client ; sélectionnez 2 pour utiliser le cryptage PEAP client. Sélectionnez l'étiquette que le commutateur réseau utilise lors de l'utilisation de Peap version 1.

Ces paramètres sont uniquement disponibles si vous utilisez IEEE 802.1ae MACsec (CAK statique/clé pré-partagée) comme méthode d'authentification :

- **Nom principal de l'association de connectivité du contrat de clé :** Saisissez le nom de l'association de connectivité (CKN). Il doit y avoir 2 à 64 caractères hexadécimaux (divisibles par 2). La CKN doit être configurée manuellement dans l'association de connectivité et doit correspondre aux deux extrémités de la liaison pour activer initialement MACsec.
- **Clé de l'association de connectivité du contrat de clé :** Saisissez la clé de l'association de connectivité (CAK). Elle doit faire 32 ou 64 caractères hexadécimaux. La CAK doit être configurée

manuellement dans l'association de connectivité et doit correspondre aux deux extrémités de la liaison pour activer initialement MACsec.

Empêcher les attaques par force brute

Blocage : Activez cette option pour bloquer les attaques par force brute. Une attaque par force brute utilise l'essai-erreur pour deviner les informations de connexion ou les clés de cryptage.

Période de blocage : Saisissez le nombre de secondes pour bloquer une attaque par force brute.

Conditions de blocage : Saisissez le nombre d'échecs d'authentification autorisés par seconde avant le démarrage du blocage. Vous pouvez définir le nombre d'échecs autorisés à la fois au niveau de la page et au niveau du périphérique.

Pare-feu

Activate (Activer) : Activez le pare-feu.

Politique par défaut : Sélectionnez l'état par défaut du pare-feu.

- **Autoriser :** Permet toutes les connexions au périphérique. Cette option est définie par défaut.
- **Refuser :** Refuse toutes les connexions au périphérique.

Pour faire des exceptions à la politique par défaut, vous pouvez créer des règles qui permettent ou refusent les connexions au périphérique depuis des adresses, des protocoles et des ports spécifiques.

- **Adresse :** Saisissez une adresse au format IPv4/IPv6 ou CIDR à laquelle vous souhaitez autoriser ou refuser l'accès.
- **Protocol (Protocole) :** Sélectionnez un protocole auquel vous souhaitez autoriser ou refuser l'accès.
- **Port :** Saisissez un numéro de port auquel vous souhaitez autoriser ou refuser l'accès. Vous pouvez ajouter un numéro de port entre 1 et 65535.
- **Politique :** Sélectionnez la politique de la règle.



: Cliquez pour créer une autre règle.

Ajouter des règles : Cliquez pour ajouter les règles que vous avez définies.

- **Temps en secondes :** Fixez une limite de temps pour tester les règles. La limite de temps par défaut est définie sur 300 secondes. Pour activer immédiatement les règles, réglez le temps sur 0 secondes.
- **Confirmer les règles :** Confirmez les règles et leur limite de temps. Si vous avez fixé une limite de temps de plus d'une seconde, les règles seront actives pendant ce temps. Si vous avez paramétré le temps sur 0, les règles seront immédiatement actives.

Règles en attente : Un aperçu des dernières règles testées que vous devez encore confirmer.

Remarque

Les règles avec une limite de temps apparaissent sous **Règles actives** jusqu'à ce que la minuterie affichée s'arrête ou jusqu'à ce que vous les confirmiez. Si vous ne les confirmez pas, elles apparaissent sous **Règles en attente** une fois la minuterie terminée, et le pare-feu revient aux paramètres précédemment définis. Si vous les confirmez, elles remplacent les règles actives actuelles.

Confirmer les règles : Cliquez pour activer les règles en cours.

Règles actives : Un aperçu des règles en cours d'exécution sur le périphérique.



: Cliquez pour supprimer une règle active.



: Cliquez pour supprimer toutes les règles, en attente ou actives.

Certificat AXIS OS avec signature personnalisée

Pour installer le logiciel de test ou tout autre logiciel personnalisé d'Axis sur le périphérique, vous avez besoin d'un certificat AXIS OS avec signature personnalisée. Le certificat vérifie que le logiciel est approuvé à la fois par le propriétaire du périphérique et par Axis. Le logiciel ne peut être exécuté que sur un périphérique précis, identifié par son numéro de série unique et son ID de puce. Seul Axis peut créer des certificats AXIS OS avec signature personnalisée, car il détient la clé pour les signer.

Install (Installer) : Cliquez pour installer le certificat. Vous devez installer le certificat avant d'installer le logiciel.



Le menu contextuel contient :

- **Delete certificate (Supprimer certificat)** : supprimez le certificat.

Comptes

Comptes



Add account (Ajouter un compte) : cliquez pour ajouter un nouveau compte. Vous pouvez ajouter jusqu'à 100 comptes.

Compte : Saisissez un nom de compte unique.

New password (Nouveau mot de passe) : Saisissez un mot de passe pour le nom de compte. Les mots de passe doivent comporter entre 1 et 64 caractères. Seuls les caractères ASCII imprimables (codes 32 à 126) sont autorisés dans le mots de passe, comme les lettres, les chiffres, les signes de ponctuation et certains symboles.

Repeat password (Répéter le mot de passe) : Saisissez à nouveau le même mot de passe.

Privilèges :

- **Administrator (Administrateur)** : accès sans restriction à tous les paramètres. Les administrateurs peuvent également ajouter, mettre à jour et supprimer les autres comptes.
- **Operator (Opérateur)** : accès à tous les paramètres à l'exception de :
 - Tous les paramètres **System (Système)**.



Le menu contextuel contient :

Mettre à jour le compte : modifiez les propriétés du compte.

Supprimer un compte : Supprimez le compte. Vous ne pouvez pas supprimer le compte root.

Accès anonyme

Autoriser le visionnage anonyme : activez cette option pour autoriser toute personne à accéder au périphérique en tant qu'utilisateur sans se connecter avec un compte.

Allow anonymous PTZ operating (Autoriser les opérations anonymes)  : activez cette option pour autoriser les utilisateurs anonymes à utiliser le panoramique, l'inclinaison et le zoom sur l'image.

Comptes SSH

 **Add SSH account (Ajouter un compte SSH)** : cliquez pour ajouter un nouveau compte SSH.

- **Activer le protocole SSH** : Activez-la pour utiliser le service SSH.

Compte : Saisissez un nom de compte unique.

New password (Nouveau mot de passe) : Saisissez un mot de passe pour le nom de compte. Les mots de passe doivent comporter entre 1 et 64 caractères. Seuls les caractères ASCII imprimables (codes 32 à 126) sont autorisés dans le mots de passe, comme les lettres, les chiffres, les signes de ponctuation et certains symboles.

Repeat password (Répéter le mot de passe) : Saisissez à nouveau le même mot de passe.

Commentaire : Saisissez un commentaire (facultatif).

 Le menu contextuel contient :

Mettre à jour le compte SSH : modifiez les propriétés du compte.

Supprimer un compte SSH : Supprimez le compte. Vous ne pouvez pas supprimer le compte root.

Hôte virtuel

 **Add virtual host (Ajouter un hôte virtuel)** : Cliquez pour ajouter un nouvel hôte virtuel.

Activé : Sélectionnez cette option pour utiliser cet hôte virtuel.

Nom du serveur : Entrez le nom du serveur. N'utilisez que les nombres 0-9, les lettres A-Z et le tiret (-).

Port : Entrez le port auquel le serveur est connecté.

Type : Sélectionnez le type d'authentification à utiliser. Sélectionnez **Base**, **Digest** ou **Open ID**.

 Le menu contextuel contient :

- **Update (Mettre à jour)** : Mettez à jour l'hôte virtuel.
- **Supprimer** : Supprimez l'hôte virtuel.

Désactivé : Le serveur est désactivé.

Configuration OpenID

Important

S'il vous est impossible de vous connecter à l'aide d'OpenID, utilisez les identifiants Digest ou de base qui vous ont servi lors de la configuration d'OpenID pour vous connecter.

Client ID (Identifiant client) : Saisissez le nom d'utilisateur OpenID.

Proxy sortant: Saisissez l'adresse proxy de la connexion OpenID pour utiliser un serveur proxy.

Demande de l'administrateur : Saisissez une valeur pour le rôle d'administrateur.

URL du fournisseur : Saisissez le lien Web pour l'authentification du point de terminaison de l'API. Le format doit être `https://[insérer URL]/.well-known/openid-configuration`

Demande de l'opérateur : Saisissez une valeur pour le rôle d'opérateur.

Demande obligatoire : Saisissez les données qui doivent être dans le jeton.

Demande de l'observateur : Saisissez la valeur du rôle de l'observateur.

Utilisateur distant : Saisissez une valeur pour identifier les utilisateurs distants. Elle permet d'afficher l'utilisateur actuel dans l'interface Web du périphérique.

Portées : Portées en option qui pourraient faire partie du jeton.

Partie secrète du client : Saisissez le mot de passe OpenID.

Enregistrer : Cliquez pour enregistrer les valeurs OpenID.

Activer OpenID : Activez cette option pour fermer la connexion actuelle et autoriser l'authentification du périphérique depuis l'URL du fournisseur.

Événements

Règles

Une règle définit les conditions requises qui déclenche les actions exécutées par le produit. La liste affiche toutes les règles actuellement configurées dans le produit.

Remarque

Vous pouvez créer jusqu'à 256 règles d'action.



Ajouter une règle : Créez une règle.

Nom : Nommez la règle.

Attente entre les actions : Saisissez la durée minimale (hh:mm:ss) qui doit s'écouler entre les activations de règle. Cela est utile si la règle est activée, par exemple, en mode jour/nuit, afin d'éviter que de faibles variations d'éclairage pendant le lever et le coucher de soleil activent la règle à plusieurs reprises.

Condition (Condition) : Sélectionnez une condition dans la liste. Une condition doit être remplie pour que le périphérique exécute une action. Si plusieurs conditions sont définies, toutes doivent être satisfaites pour déclencher l'action. Pour plus d'informations sur des conditions spécifiques, consultez *Get started with rules for events (Consulter les règles pour les événements)*.

Utiliser cette condition comme déclencheur : Sélectionnez cette option pour que cette première condition fonctionne uniquement comme déclencheur de démarrage. Cela signifie qu'une fois la règle activée, elle reste active tant que toutes les autres conditions sont remplies, quel que soit l'état de la première condition. Si vous ne sélectionnez pas cette option, la règle est simplement active lorsque toutes les conditions sont remplies.

Inverser cette condition : Sélectionnez cette option si vous souhaitez que cette condition soit l'inverse de votre sélection.



Add a condition (Ajouter une condition) : Cliquez pour ajouter une condition supplémentaire.

Action : Sélectionnez une action dans la liste et saisissez les informations requises. Pour plus d'informations sur des actions spécifiques, consultez *Get started with rules for events (Consulter les règles pour les événements)*.

Destinataires

Vous pouvez configurer votre périphérique pour qu'il informe des destinataires lorsque des événements surviennent ou lorsque des fichiers sont envoyés.

Remarque

Si vous avez paramétré votre périphérique pour qu'il utilise le protocole FTP ou SFTP, ne modifiez pas et ne supprimez pas le numéro de séquence unique qui est ajouté aux noms de fichiers. Dans ce cas, une seule image par événement peut être envoyée.

La liste affiche tous les destinataires actuellement configurés dans le produit, ainsi que des informations sur leur configuration.

Remarque

Vous pouvez créer jusqu'à 20 destinataires.



Add a recipient (Ajouter un destinataire) : Cliquez pour ajouter un destinataire.

Nom : Entrez le nom du destinataire.

Type : Choisissez dans la liste :

- **FTP** 
 - **Hôte** : Entrez l'adresse IP du serveur ou son nom d'hôte. Si vous saisissez un nom d'hôte, assurez-vous qu'un serveur DNS est spécifié sous **System > Network > IPv4 and IPv6** (**Système > Réseau > IPv4 et IPv6**).
 - **Port** : Saisissez le numéro de port utilisé par le serveur FTP. Le numéro par défaut est 21.
 - **Dossier** : Saisissez le chemin d'accès au répertoire dans lequel vous souhaitez stocker des fichiers. Si ce répertoire n'existe pas déjà sur le serveur FTP, un message d'erreur s'affiche lors du chargement des fichiers.
 - **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
 - **Mot de passe** : Entrez le mot de passe pour la connexion.
 - **Utiliser un nom de fichier temporaire** : Sélectionnez cette option pour télécharger des fichiers avec des noms de fichiers temporaires, générés automatiquement. Les fichiers sont renommés comme vous le souhaitez une fois le chargement terminé. Si le chargement est abandonné/interrompu, vous n'obtenez pas de fichiers corrompus. Cependant, vous obtiendrez probablement toujours les fichiers temporaires. Vous saurez ainsi que tous les fichiers qui portent le nom souhaité sont corrects.
 - **Utiliser une connexion FTP passive** : dans une situation normale, le produit demande simplement au serveur FTP cible d'ouvrir la connexion de données. Le périphérique initie activement le contrôle FTP et la connexion de données vers le serveur cible. Cette opération est normalement nécessaire si un pare-feu est présent entre le périphérique et le serveur FTP cible.
- **HTTP**
 - **URL** : Saisissez l'adresse réseau du serveur HTTP et le script qui traitera la requête. Par exemple, `http://192.168.254.10/cgi-bin/notify.cgi`.
 - **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
 - **Mot de passe** : Entrez le mot de passe pour la connexion.
 - **Proxy** : Activez cette option et saisissez les informations requises si un serveur proxy doit être fourni pour la connexion au serveur HTTP.
- **HTTPS**
 - **URL** : Saisissez l'adresse réseau du serveur HTTPS et le script qui traitera la requête. Par exemple, `https://192.168.254.10/cgi-bin/notify.cgi`.
 - **Validate server certificate (Valider le certificat du serveur)** : Sélectionnez cette option pour valider le certificat qui a été créé par le serveur HTTPS.
 - **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
 - **Mot de passe** : Entrez le mot de passe pour la connexion.
 - **Proxy** : Activez cette option et saisissez les informations requises si un serveur proxy doit être fourni pour la connexion au serveur HTTPS.
- **Stockage réseau** 

Vous pouvez ajouter un stockage réseau comme un NAS (Unité de stockage réseaux) et l'utiliser comme destinataire pour stocker des fichiers. Les fichiers sont stockés au format de fichier Matroska (MKV).

 - **Hôte** : Saisissez l'adresse IP ou le nom d'hôte du stockage réseau.

- **Partage** : Saisissez le nom du partage sur le serveur hôte.
- **Dossier** : Saisissez le chemin d'accès au répertoire dans lequel vous souhaitez stocker des fichiers.
- **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
- **Mot de passe** : Entrez le mot de passe pour la connexion.
- **SFTP** 
 - **Hôte** : Entrez l'adresse IP du serveur ou son nom d'hôte. Si vous saisissez un nom d'hôte, assurez-vous qu'un serveur DNS est spécifié sous **System > Network > IPv4 and IPv6** (**Système > Réseau > IPv4 et IPv6**).
 - **Port** : Saisissez le numéro de port utilisé par le serveur SFTP. Le numéro par défaut est 22.
 - **Dossier** : Saisissez le chemin d'accès au répertoire dans lequel vous souhaitez stocker des fichiers. Si ce répertoire n'existe pas déjà sur le serveur SFTP, un message d'erreur s'affiche lors du chargement des fichiers.
 - **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
 - **Mot de passe** : Entrez le mot de passe pour la connexion.
 - **Type de clé publique hôte SSH (MD5)** : Entrez l'empreinte de la clé publique de l'hôte distant (une chaîne hexadécimale à 32 chiffres). Le client SFTP prend en charge les serveurs SFTP utilisant SSH-2 avec les types de clé hôte RSA, DSA, ECDSA et ED25519. RSA est la méthode préférée pendant la négociation, suivie par ECDSA, ED25519 et DSA. Assurez-vous d'entrer la bonne clé MD5 utilisée par votre serveur SFTP. Bien que le périphérique Axis prenne en charge les clés de hachage MD5 et SHA-256, nous recommandons l'utilisation de SHA-256 en raison de sa sécurité supérieure à celle de MD5. Pour plus d'informations sur la manière de configurer un serveur SFTP avec un périphérique Axis, accédez à la page *Portail AXIS OS*.
 - **Type de clé publique hôte SSH (SHA256)** : Entrez l'empreinte de la clé publique de l'hôte distant (une chaîne codée Base64 à 43 chiffres). Le client SFTP prend en charge les serveurs SFTP utilisant SSH-2 avec les types de clé hôte RSA, DSA, ECDSA et ED25519. RSA est la méthode préférée pendant la négociation, suivie par ECDSA, ED25519 et DSA. Assurez-vous d'entrer la bonne clé MD5 utilisée par votre serveur SFTP. Bien que le périphérique Axis prenne en charge les clés de hachage MD5 et SHA-256, nous recommandons l'utilisation de SHA-256 en raison de sa sécurité supérieure à celle de MD5. Pour plus d'informations sur la manière de configurer un serveur SFTP avec un périphérique Axis, accédez à la page *Portail AXIS OS*.
 - **Utiliser un nom de fichier temporaire** : Sélectionnez cette option pour télécharger des fichiers avec des noms de fichiers temporaires, générés automatiquement. Les fichiers sont renommés comme vous le souhaitez une fois le chargement terminé. Si le chargement est abandonné ou interrompu, vous n'obtenez pas de fichiers corrompus. Cependant, vous obtiendrez probablement toujours les fichiers temporaires. Vous saurez que tous les fichiers qui portent le nom souhaité sont corrects.
- **SIP or VMS (SIP ou VMS)**  :
 - SIP** : Sélectionnez cette option pour effectuer un appel SIP.
 - VMS** : Sélectionnez cette option pour effectuer un appel VMS.
 - **Compte SIP de départ** : Choisissez dans la liste.
 - **Adresse SIP de destination** : Entrez l'adresse SIP.
 - **Test (Tester)** : Cliquez pour vérifier que vos paramètres d'appel fonctionnent.
- **Envoyer un e-mail**
 - **Envoyer l'e-mail à** : Entrez l'adresse e-mail à laquelle envoyer les e-mails. Pour entrer plusieurs adresses e-mail, séparez-les par des virgules.
 - **Envoyer un e-mail depuis** : Saisissez l'adresse e-mail du serveur d'envoi.

- **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur du serveur de messagerie. Laissez ce champ vierge si le serveur de messagerie ne nécessite pas d'authentification.
- **Mot de passe** : Entrez le mot de passe du serveur de messagerie. Laissez ce champ vierge si le serveur de messagerie ne nécessite pas d'authentification.
- **Serveur e-mail (SMTP)** : Saisissez le nom du serveur SMTP, par exemple, smtp.gmail.com, smtp.mail.yahoo.com.
- **Port** : Saisissez le numéro de port du serveur SMTP, en utilisant des valeurs comprises dans la plage 0-65535. La valeur par défaut est 587.
- **Cryptage** : Pour utiliser le cryptage, sélectionnez SSL ou TLS.
- **Validate server certificate (Valider le certificat du serveur)** : Si vous utilisez le cryptage, sélectionnez cette option pour valider l'identité du périphérique. Le certificat peut être auto-signé ou émis par une autorité de certification (CA).
- **Authentification POP** : Activez cette option pour saisir le nom du serveur POP, par exemple, pop.gmail.com.

Remarque

Certains fournisseurs de messagerie possèdent des filtres de sécurité destinés à empêcher les utilisateurs de recevoir ou de visionner une grande quantité de pièces jointes et de recevoir des emails programmés, etc. Vérifiez la politique de sécurité de votre fournisseur de messagerie électronique pour éviter que votre compte de messagerie soit bloqué ou pour ne pas manquer de messages attendus.

- **TCP**
 - **Hôte** : Entrez l'adresse IP du serveur ou son nom d'hôte. Si vous saisissez un nom d'hôte, assurez-vous qu'un serveur DNS est spécifié sous **System > Network > IPv4 and IPv6** (**Système > Réseau > IPv4 et IPv6**).
 - **Port** : Saisissez le numéro du port utilisé pour accès au serveur.

Test : Cliquez pour tester la configuration.



Le menu contextuel contient :

Afficher le destinataire : cliquez pour afficher les détails de tous les destinataires.

Copier un destinataire : Cliquez pour copier un destinataire. Lorsque vous effectuez une copie, vous pouvez apporter des modifications au nouveau destinataire.

Supprimer le destinataire : Cliquez pour supprimer le destinataire de manière définitive.

Calendriers

Les calendriers et les impulsions peuvent être utilisés comme conditions dans les règles. La liste affiche tous les calendriers et impulsions actuellement configurés dans le produit, ainsi que des informations sur leur configuration.



Add schedule (Ajouter un calendrier) : Cliquez pour créer un calendrier ou une impulsion.

Déclencheurs manuels

Vous pouvez utiliser le déclencheur manuel pour déclencher manuellement une règle. Le déclencheur manuel peut être utilisé, par exemple, pour valider des actions pendant l'installation et la configuration du produit.

MQTT

MQTT (message queuing telemetry transport) est un protocole de messagerie standard pour l'Internet des objets (IoT). Conçu pour simplifier l'intégration IoT, il est utilisé dans de nombreux secteurs pour connecter des dispositifs distants avec une empreinte de code réduite et une bande passante réseau minimale. Le client MQTT du logiciel des périphériques Axis peut simplifier l'intégration des données et des événements produits sur le périphérique dans les systèmes qui ne sont pas un logiciel de gestion vidéo (VMS).

Configurez le périphérique en tant que client MQTT. La communication MQTT est basée sur deux entités, les clients et le courtier. Les clients peuvent envoyer et recevoir des messages. Le courtier est responsable de l'acheminement des messages entre les clients.

Pour en savoir plus sur MQTT, consultez *AXIS OS Knowledge base*.

ALPN

ALPN est une extension TLS/SSL qui permet de choisir un protocole d'application au cours de la phase handshake de la connexion entre le client et le serveur. Cela permet d'activer le trafic MQTT sur le même port que celui utilisé pour d'autres protocoles, tels que HTTP. Dans certains cas, il n'y a pas de port dédié ouvert pour la communication MQTT. Une solution consiste alors à utiliser ALPN pour négocier l'utilisation de MQTT comme protocole d'application sur un port standard, autorisé par les pare-feu.

Client MQTT

Connect (Connexion) : Activez ou désactivez le client MQTT.

Status (Statut) : Affiche le statut actuel du client MQTT.

Courtier

Hôte : Saisissez le nom d'hôte ou l'adresse IP du serveur MQTT.

Protocol (Protocole) : Sélectionnez le protocole à utiliser.

Port : Saisissez le numéro de port.

- 1883 est la valeur par défaut pour MQTT sur TCP
- 8883 est la valeur par défaut pour MQTT sur SSL.
- 80 est la valeur par défaut pour MQTT sur WebSocket.
- 443 est la valeur par défaut pour MQTT sur WebSocket Secure.

Protocole ALPN : Saisissez le nom du protocole ALPN fourni par votre fournisseur MQTT. Cela ne s'applique qu'aux normes MQTT sur SSL et MQTT sur WebSocket Secure.

Username (Nom d'utilisateur) : Saisissez le nom d'utilisateur utilisé par le client pour accéder au serveur.

Mot de passe : Saisissez un mot de passe pour le nom d'utilisateur.

Client ID (Identifiant client) : Entrez un identifiant client. L'identifiant client est envoyé au serveur lorsque le client s'y connecte.

Clean session (Nettoyer la session) : Contrôle le comportement lors de la connexion et de la déconnexion. Lorsque cette option est sélectionnée, les informations d'état sont supprimées lors de la connexion et de la déconnexion.

Proxy HTTP : URL d'une longueur maximale de 255 octets. Vous pouvez laisser le champ vide si vous ne souhaitez pas utiliser de proxy HTTP.

Proxy HTTPS : URL d'une longueur maximale de 255 octets. Vous pouvez laisser le champ vide si vous ne souhaitez pas utiliser de proxy HTTPS.

Keep alive interval (Intervalle Keep Alive) : Permet au client de détecter quand le serveur n'est plus disponible sans devoir observer le long délai d'attente TCP/IP.

Timeout (Délai d'attente) : Intervalle de temps en secondes pour permettre l'établissement d'une connexion. Valeur par défaut : 60

Préfixe de rubrique du périphérique : Utilisé dans les valeurs par défaut pour le sujet contenu dans le message de connexion et le message LWT sur l'onglet MQTT client (Client MQTT), et dans les conditions de publication sur l'onglet MQTT publication (Publication MQTT).

Reconnect automatically (Reconnexion automatique) : Spécifie si le client doit se reconnecter automatiquement en cas de déconnexion.

Message de connexion

Spécifie si un message doit être envoyé lorsqu'une connexion est établie.

Send message (Envoyer message) : Activez cette option pour envoyer des messages.

Use default (Utiliser les valeurs par défaut) : Désactivez cette option pour saisir votre propre message par défaut.

Topic (Rubrique) : Saisissez la rubrique du message par défaut.

Payload (Charge utile) : Saisissez le contenu du message par défaut.

Retain (Conserver) : Sélectionnez cette option pour conserver l'état du client sur cette Rubrique.

QoS : Modifiez la couche QoS pour le flux de paquets.

Message Dernière Volonté et Testament

Last Will Testament (LWT) permet à un client de fournir un testament avec ses identifiants lors de sa connexion au courtier. Si le client se déconnecte incorrectement plus tard (peut-être en raison d'une défaillance de sa source d'alimentation), il peut laisser le courtier délivrer un message aux autres clients. Ce message LWT présente la même forme qu'un message ordinaire. Il est acheminé par le même mécanisme.

Send message (Envoyer message) : Activez cette option pour envoyer des messages.

Use default (Utiliser les valeurs par défaut) : Désactivez cette option pour saisir votre propre message par défaut.

Topic (Rubrique) : Saisissez la rubrique du message par défaut.

Payload (Charge utile) : Saisissez le contenu du message par défaut.

Retain (Conserver) : Sélectionnez cette option pour conserver l'état du client sur cette Rubrique.

QoS : Modifiez la couche QoS pour le flux de paquets.

Publication MQTT

Utiliser le préfixe de rubrique par défaut : Sélectionnez cette option pour utiliser le préfixe de rubrique par défaut, défini dans la rubrique du périphérique dans l'onglet **MQTT client (Client MQTT)**.

Inclure le nom de rubrique : Sélectionnez cette option pour inclure la rubrique qui décrit l'état dans la rubrique MQTT.

Inclure les espaces de noms de rubrique : Sélectionnez cette option pour inclure des espaces de noms de rubrique ONVIF dans la rubrique MQTT.

Inclure le numéro de série : Sélectionnez cette option pour inclure le numéro de série du périphérique dans la charge utile MQTT.



Add condition (Ajouter condition) : Cliquez pour ajouter une condition.

Retain (Conserver) : Définit les messages MQTT qui sont envoyés et conservés.

- **Aucun** : Envoyer tous les messages comme non conservés.
- **Property (Propriété)** : Envoyer seulement les messages avec état comme conservés.
- **All (Tout)** : Envoyer les messages avec état et sans état, comme conservés.

QoS : Sélectionnez le niveau souhaité pour la publication MQTT.

Abonnements MQTT



Add subscription (Ajouter abonnement) : Cliquez pour ajouter un nouvel abonnement MQTT.

Subscription filter (Filtre d'abonnements) : Saisissez le sujet MQTT auquel vous souhaitez vous abonner.

Use device topic prefix (Utiliser le préfixe de rubrique du périphérique) : Ajoutez le filtre d'abonnement comme préfixe au sujet MQTT.

Subscription type (Type d'abonnement) :

- **Stateless (Sans état)** : Sélectionnez cette option pour convertir les messages MQTT en message sans état.
- **Stateful (Avec état)** : Sélectionnez cette option pour convertir les messages MQTT dans une condition. La charge utile est utilisée comme état.

QoS : Sélectionnez le niveau souhaité pour l'abonnement MQTT.

Incrustations MQTT

Remarque

Connectez-vous à un courtier MQTT avant d'ajouter des modificateurs d'incrustation MQTT.



Add overlay modifier (Ajouter modificateur d'incrustation) : Cliquez pour ajouter un modificateur d'incrustation.

Filtre rubrique : Ajoutez le sujet MQTT contenant les données que vous souhaitez afficher dans l'incrustation.

Champ de données : Spécifiez la clé de l'incrustation de message que vous souhaitez afficher dans l'incrustation, en supposant que le message soit au format JSON.

Modificateur : Utilisez le modificateur résultant lorsque vous créez l'incrustation.

- Les modificateurs qui commencent par **#XMP** affichent toutes les données reçues à partir du sujet.
- Les modificateurs qui commencent par **#XMD** affichent les données spécifiées dans le champ de données.

Stockage

Stockage réseau

Ignore (Ignorer) : Activez cette option pour ignorer le stockage réseau.

Add network storage (Ajouter un stockage réseau) : cliquez pour ajouter un partage réseau où vous pouvez enregistrer les enregistrements.

- **Adresse :** saisissez l'adresse IP ou le nom du serveur hôte, en général une unité NAS (unité de stockage réseau). Nous vous conseillons de configurer l'hôte pour qu'il utilise une adresse IP fixe (autre que DHCP puisqu'une adresse IP dynamique peut changer) ou d'utiliser des noms DNS. Les noms Windows SMB/CIFS ne sont pas pris en charge.
- **Network Share (Partage réseau) :** Saisissez le nom de l'emplacement partagé sur le serveur hôte. Chaque périphérique possédant son propre dossier, plusieurs périphériques Axis peuvent utiliser le même partage réseau.
- **User (Utilisateur) :** si le serveur a besoin d'un identifiant de connexion, saisissez le nom d'utilisateur. Pour vous connecter à un serveur de domaine précis, entrez DOMAIN\username.
- **Mot de passe :** si le serveur a besoin d'un identifiant de connexion, saisissez le mot de passe.
- **Version SMB:** Sélectionnez la version du protocole SMB pour la connexion au NAS. Si vous sélectionnez **Auto**, le périphérique essaie de négocier l'une des versions SMB sécurisées : 3.02, 3.0 ou 2.1. Sélectionnez 1.0 ou 2.0 pour vous connecter à un NAS plus ancien qui ne prend pas en charge les versions supérieures. Vous pouvez en savoir plus sur l'assistance SMB sur les périphériques Axis [ici](#).
- **Ajouter un partage sans test :** Sélectionnez cette option pour ajouter le partage réseau même si une erreur est découverte lors du test de connexion. L'erreur peut correspondre, par exemple, à l'absence d'un mot de passe alors que le serveur en a besoin.

Remove network storage (Supprimer le stockage réseau) : Cliquez pour démonter, dissocier et supprimer la connexion au partage réseau. Tous les paramètres du partage réseau sont supprimés.

Dissocier : Cliquez pour dissocier et déconnecter le partage réseau.

Bind (Associer) : cliquez pour lier et connecter le partage réseau.

Unmount (Démonter) : Cliquez pour démonter le partage réseau.

Mount (Monter) : cliquez pour monter le partage réseau.

Write protect (Protection en écriture) : activez cette option pour arrêter l'écriture sur le partage réseau et éviter la suppression des enregistrements. Vous ne pouvez pas formater un partage réseau protégé en écriture.

Retention time (Durée de conservation) : choisissez la durée de conservation des enregistrements, pour réduire le nombre d'anciens enregistrements ou pour respecter les réglementations en matière de stockage de données. Si le stockage réseau est saturé, les anciens enregistrements sont supprimés avant la fin de la période sélectionnée.

Outils

- **Test connection (Tester la connexion) :** testez la connexion au partage réseau.
- **Format :** Formatez le partage réseau, comme dans le cas où vous devez effacer rapidement toutes les données, par exemple. CIFS est l'option de système de fichiers disponible.

Use tool (Utiliser l'outil) : cliquez pour activer l'outil sélectionné.

Stockage embarqué

Important

Risque de perte de données et d'enregistrements corrompus. Ne retirez pas la carte SD tant que le périphérique fonctionne. Démontez la carte SD avant de la retirer.

Unmount (Démonter) : cliquez pour retirer la carte SD en toute sécurité.

Write protect (Protection en écriture) : Activez cette option pour empêcher l'écriture sur la carte SD et la suppression d'enregistrements. Vous ne pouvez pas formater une carte SD protégée en écriture.

Autoformat (Formater automatiquement) : Activez cette option pour formater automatiquement une carte SD récemment insérée. Le système de fichiers est formaté en ext4.

Ignore (Ignorer) : Activez cette option pour arrêter le stockage des enregistrements sur la carte SD. Si vous ignorez la carte SD, le périphérique ne reconnaît plus son existence. Le paramètre est uniquement accessible aux administrateurs.

Retention time (Durée de conservation) : Choisissez la durée de conservation des enregistrements, pour réduire le nombre d'anciens enregistrements ou respecter les réglementations en matière de stockage de données. Lorsque la carte SD est pleine, les anciens enregistrements sont supprimés avant que leur durée de conservation ne soit écoulée.

Outils

- **Check (Vérifier)** : Vérifiez les erreurs sur La carte SD.
- **Repair (Réparer)** : Réparez les erreurs dans le système de fichiers.
- **Format** : Formatez la carte SD pour changer de système de fichiers et effacer toutes les données. Vous ne pouvez formater la carte SD qu'avec le système de fichiers ext4. Vous avez besoin d'une application ou d'un pilote ext4 tiers pour accéder au système de fichiers depuis Windows®.
- **Crypter** : Utilisez cet outil pour formater la carte SD et activer le cryptage. Il supprime toutes les données stockées sur la carte SD. Toutes les nouvelles données stockées sur la carte SD seront chiffrées.
- **Decrypt (Décrypter)** : Utilisez cet outil pour formater la carte SD sans cryptage. Il supprime toutes les données stockées sur la carte SD. Aucune nouvelle donnée stockée sur la carte SD ne sera chiffrée.
- **Modifier le mot de passe** : Modifiez le mot de passe exigé pour crypter la carte SD.

Use tool (Utiliser l'outil) : cliquez pour activer l'outil sélectionné.

Déclencheur d'usure : Définissez une valeur pour le niveau d'usure de la carte SD auquel vous voulez déclencher une action. Le niveau d'usure est compris entre 0 et 200 %. Une carte SD neuve qui n'a jamais été utilisée a un niveau d'usure de 0 %. Un niveau d'usure de 100 % indique que la carte SD est proche de sa durée de vie prévue. Lorsque le niveau d'usure atteint 200 %, le risque de dysfonctionnement de la carte SD est élevé. Nous recommandons de régler le seuil d'usure entre 80 et 90 %. Cela vous laisse le temps de télécharger les enregistrements et de remplacer la carte SD à temps avant qu'elle ne s'use. Le déclencheur d'usure vous permet de configurer un événement et de recevoir une notification lorsque le niveau d'usure atteint la valeur définie.

Profils de flux

Un profil de flux est un groupe de paramètres qui affectent le flux vidéo. Ces profils de flux s'utilisent dans différentes situations, par exemple, lorsque vous créez des événements et utilisez des règles d'enregistrement.



Add stream profile (Ajouter un profil de flux) : Cliquez pour créer un nouveau profil de flux.

Aperçu : Aperçu du flux vidéo avec les paramètres de profil de flux sélectionnés. L'aperçu est mis à jour en cas de modification des paramètres de la page. Si votre périphérique offre différentes zones de visualisation, vous pouvez en changer dans la liste déroulante de la partie inférieure gauche de l'image.

Nom : Nommez votre profil.

Description : Ajoutez une description pour votre profil.

Codec vidéo : Sélectionnez le codec vidéo applicable au profil.

Résolution : Pour une description de ce paramètre, consultez .

Fréquence d'images : Pour une description de ce paramètre, consultez .

Compression : Pour une description de ce paramètre, consultez .

Zipstream  : Pour une description de ce paramètre, consultez .

Optimize for storage (Optimiser pour le stockage)  : Pour une description de ce paramètre, consultez .

Dynamic FPS (IPS dynamique)  : Pour une description de ce paramètre, consultez .

Dynamic GOP (Groupe dynamique d'image dynamique)  : Pour une description de ce paramètre, consultez .

Mirror (Miroir)  : Pour une description de ce paramètre, consultez .

GOP length (Longueur de GOP)  : Pour une description de ce paramètre, consultez .

Bitrate control (Contrôle du débit binaire) : Pour une description de ce paramètre, consultez .

Include overlays (Inclure les incrustations)  : Sélectionnez le type d'incrustations à inclure. Pour plus d'informations sur l'ajout d'incrustations, consultez .

Include audio (Inclure l'audio)  : Pour une description de ce paramètre, consultez .

ONVIF

Comptes ONVIF

ONVIF (Open Network Video Interface Forum) est une norme mondiale qui permet aux utilisateurs finaux, aux intégrateurs, aux consultants et aux fabricants de tirer pleinement parti des possibilités inhérentes à la technologie de vidéo sur IP. ONVIF permet une interopérabilité entre des produits de fournisseurs différents, une flexibilité accrue, un coût réduit et des systèmes à l'épreuve du temps.

Lorsque vous créez un compte ONVIF, vous activez automatiquement la communication ONVIF. Utilisez le nom de compte et le mot de passe pour toute communication ONVIF avec le périphérique. Pour plus d'informations, consultez la communauté des développeurs Axis sur axis.com.



Add accounts (Ajouter des comptes) : Cliquez pour ajouter un nouveau compte ONVIF.

Compte : Saisissez un nom de compte unique.

New password (Nouveau mot de passe) : Saisissez un mot de passe pour le nom de compte. Les mots de passe doivent comporter entre 1 et 64 caractères. Seuls les caractères ASCII imprimables (codes 32 à 126) sont autorisés dans le mots de passe, comme les lettres, les chiffres, les signes de ponctuation et certains symboles.

Repeat password (Répéter le mot de passe) : Saisissez à nouveau le même mot de passe.

Role (Rôle) :

- **Administrator (Administrateur)** : accès sans restriction à tous les paramètres. Les administrateurs peuvent également ajouter, mettre à jour et supprimer les autres comptes.
- **Operator (Opérateur)** : accès à tous les paramètres à l'exception de :
 - Tous les paramètres **System (Système)**.
 - Ajout d'applications.
- **Compte média** : Permet d'accéder au flux de données vidéo uniquement.



Le menu contextuel contient :

Mettre à jour le compte : modifiez les propriétés du compte.

Supprimer un compte : Supprimez le compte. Vous ne pouvez pas supprimer le compte root.

Profils médiatiques ONVIF

Un profil médiatique ONVIF se compose d'un ensemble de configurations que vous pouvez utiliser pour modifier les réglages du flux multimédia. Pour créer de nouveaux profils, vous avez le choix d'utiliser votre propre ensemble de configurations ou des profils préconfigurés pour une configuration rapide.



Add media profile (Ajouter un profil média : Cliquez pour ajouter un nouveau profil médiatique ONVIF.

Nom du profil : ajoutez un nom pour le profil multimédia.

Video source (Source vidéo) : sélectionnez la source vidéo adaptée à votre configuration.

- **Sélectionner une configuration :** sélectionnez une configuration définie par l'utilisateur dans la liste. Les configurations proposées dans la liste déroulante correspondent aux canaux vidéo du périphérique, y compris les multi-vues, les zones de visualisation et les canaux virtuels.

Video encoder (Encodeur vidéo) : sélectionnez le format d'encodage vidéo adapté à votre configuration.

- **Sélectionner une configuration :** sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres d'encodage. Les configurations proposées dans la liste déroulante servent d'identifiants / de noms à la configuration de l'encodeur vidéo. Sélectionnez l'utilisateur 0 à 15 pour appliquer vos propres paramètres, ou sélectionnez l'un des utilisateurs par défaut pour utiliser des paramètres prédéfinis correspondant à un format d'encodage spécifique.

Remarque

Activez l'audio sur le périphérique pour pouvoir sélectionner une source audio et une configuration d'encodeur audio.

Audio source (Source audio)  : sélectionnez la source d'entrée audio adaptée à votre configuration.

- **Sélectionner une configuration :** sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres audio. Les configurations proposées dans la liste déroulante correspondent aux entrées audio du périphérique. Si le périphérique dispose d'une entrée audio, il s'agit de l'utilisateur 0. Si le périphérique dispose de plusieurs entrées audio, d'autres utilisateurs apparaissent dans la liste.

Audio encoder (Encodeur audio)  : sélectionnez le format d'encodage audio adapté à votre configuration.

- **Sélectionner une configuration :** sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres d'encodage audio. Les configurations proposées dans la liste déroulante servent d'identifiants / de noms à la configuration de l'encodeur audio.

Audio decoder (Décodeur audio)  : sélectionnez le format de décodage audio adapté à votre configuration.

- **Sélectionner une configuration :** sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres. Les configurations proposées dans la liste déroulante servent d'identifiants / de noms à la configuration.

Sortie audio  : sélectionnez le format de sortie audio adapté à votre configuration.

- **Sélectionner une configuration :** sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres. Les configurations proposées dans la liste déroulante servent d'identifiants / de noms à la configuration.

Métadonnées : sélectionnez les métadonnées à inclure dans votre configuration.

- **Sélectionner une configuration :** sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres de métadonnées. Les configurations proposées dans la liste déroulante servent d'identifiants / de noms à la configuration des métadonnées.

PTZ  : sélectionnez les paramètres PTZ adaptés à votre configuration.

- **Sélectionner une configuration** : sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres PTZ. Les configurations proposées dans la liste déroulante correspondent aux canaux vidéo du périphérique avec prise en charge des fonctions PTZ.

Créer : cliquez pour enregistrer vos paramètres et créer le profil.

Cancel (Annuler) : cliquez pour annuler la configuration et effacer tous les paramètres.

profil_x : cliquez sur le nom du profil pour ouvrir et modifier le profil préconfiguré.

Détecteurs

Détection de sabotage

Le détecteur de sabotage de la caméra génère une alarme lorsque la scène change, par exemple lorsque son objectif est obstrué ou aspergé de peinture ou que sa mise au point est fortement dérégulée, et que le délai défini dans **Délai de déclenchement** s'est écoulé. Le détecteur de sabotage ne s'active que lorsque la caméra n'a pas bougé pendant au moins 10 secondes. Pendant cette période, le détecteur configure un modèle de scène qu'il utilisera comme comparaison pour détecter un sabotage dans les images actuelles. Afin que le modèle de scène soit correctement configuré, assurez-vous que la caméra est mise au point, que les conditions d'éclairage sont correctes et que la caméra n'est pas dirigée sur une scène sans contours, par exemple un mur vide. La détérioration de caméra peut servir à déclencher des actions.

Délai de déclenchement : Saisissez la durée minimale pendant que les conditions de sabotage doivent être actives avant le déclenchement de l'alarme. Ceci peut permettre d'éviter les fausses alarmes si des conditions connues affectent l'image.

Trigger on dark images (Déclencheur sur images sombres) : Il est très difficile de générer des alarmes lorsque l'objectif de la caméra est aspergé de peinture, car il est impossible de distinguer cet événement d'autres situations où l'image s'assombrit de la même façon, par exemple lorsque les conditions d'éclairage varient. Activez ce paramètre pour générer des alarmes dans tous les cas où l'image devient sombre. Lorsque ce paramètre est désactivé, le périphérique ne génère aucune alarme lorsque l'image devient sombre.

Remarque

Pour la détection des tentatives de sabotage dans les scènes statiques et non encombrées.

Détection audio

Ces paramètres sont disponibles pour chaque entrée audio.

Sound level (Niveau sonore) : Réglez le niveau sonore sur une valeur comprise entre 0 et 100, où 0 correspond à la plus grande sensibilité et 100 à la plus faible. Utilisez l'indicateur **Activité** pour vous guider lors du réglage du niveau sonore. Lorsque vous créez des événements, vous pouvez utiliser le niveau sonore comme condition. Vous pouvez choisir de déclencher une action si le niveau sonore est supérieur, inférieur ou différent de la valeur définie.

Détection des chocs

Shock detector (Détecteur de chocs) : Activez cette option pour générer une alarme si le périphérique est heurté par un objet ou s'il subit un acte de vandalisme.

Sensitivity level (Niveau de sensibilité) : Déplacez le curseur pour ajuster le niveau de sensibilité auquel le périphérique doit générer une alarme. Une valeur faible signifie que le périphérique génère une alarme uniquement si le choc est puissant. Une valeur élevée signifie que l'appareil génère une alarme même si l'acte de vandalisme est n'est pas brutal.

Accessoires

Ports E/S

Utilisez une entrée numérique pour connecter les périphériques externes pouvant basculer entre un circuit ouvert et un circuit fermé, tels que les capteurs infrarouge passifs, les contacts de porte ou de fenêtre et les détecteurs de bris de verre.

Utilisez une sortie numérique pour raccorder des périphériques externes, comme des relais ou des voyants. Vous pouvez activer les périphériques connectés par l'interface de programmation VAPIX® ou par l'interface Web.

Port

Nom : modifiez le texte pour renommer le port.

Direction :  indique que le port est un port d'entrée.  indique qu'il s'agit d'un port de sortie. Si le port est configurable, vous pouvez cliquer sur les icônes pour modifier entre l'entrée et la sortie.

État normal : Cliquez sur  pour un circuit ouvert, et  pour un circuit fermé.

État actuel : Indique l'état actuel du port. L'entrée ou la sortie est activée lorsque l'état actuel diffère de l'état normal. Une entrée sur le périphérique a un circuit ouvert lorsqu'elle est déconnectée ou lorsque la tension est supérieure à 1 V CC.

Remarque

Lors du redémarrage, le circuit de sortie est ouvert. Lorsque le redémarrage est terminé, le circuit repasse à la position normale. Si vous modifiez un paramètre sur cette page, les circuits de sortie repassent à leurs positions normales quels que soient les déclencheurs actifs.

Supervisé  : Activez cette option pour pouvoir détecter et déclencher des actions si quelqu'un touche aux périphériques d'E/S numériques. En plus de détecter si une entrée est ouverte ou fermée, vous pouvez également détecter si quelqu'un l'a altérée (c'est-à-dire coupée ou court-circuitée). La supervision de la connexion nécessite des composants supplémentaires (résistances de fin de ligne) dans la boucle d'E/S externe.

Edge-to-Edge

Appairage

L'appairage vous permet d'utiliser un périphérique Axis compatible comme s'il faisait partie du périphérique principal.

Appairage audio vous permet d'effectuer un appairage avec un haut-parleur ou un microphone du réseau. Une fois appairé, le haut-parleur réseau joue le rôle de périphérique de sortie audio permettant de lire des clips audio et de transmettre des sons via la caméra. Le microphone réseau capte les sons de la zone environnante et les retranscrit comme entrée audio, utilisable dans les flux et les enregistrements multimédia.

Important

Pour que cette fonction soit opérationnelle avec un logiciel de gestion vidéo (VMS), vous devez d'abord appairer la caméra avec le haut-parleur ou le microphone, puis ajouter la caméra à votre VMS.

Définissez une limite « Attendre entre les actions » dans la règle d'événement lorsque vous utilisez un périphérique audio appairé en réseau dans une règle d'événement avec « Détection audio » en tant que condition et « Lecture de clips audio » comme action. Cela vous permettra d'éviter une détection de boucle si le microphone de capture capte l'audio du haut-parleur.



Ajouter : Ajoutez un périphérique à appairer.

Sélectionner le type d'appairage : Sélectionnez dans la liste déroulante.

Appairage du haut-parleur : Sélectionnez cette option pour appairer un haut-parleur réseau.



Appairage de microphone : Sélectionnez cette option pour appairer un microphone.

Adresse : Saisissez le nom d'hôte ou l'adresse IP du haut-parleur réseau.

Username (Nom d'utilisateur) : Saisissez le nom d'utilisateur.

Mot de passe : Saisissez un mot de passe pour l'utilisateur.

Close (Fermer) : Cliquez pour effacer le contenu de tous les champs.

Connect (Connexion) : Cliquez pour établir une connexion avec le périphérique à appairer.

L'appairage PTZ vous permet d'appairer un radar avec une caméra PTZ pour utiliser le suivi automatique. Le suivi automatique du radar permet à la caméra PTZ de suivre les objets à partir d'informations du radar sur les positions des objets.



Ajouter : Ajoutez un périphérique à appairer.

Sélectionner le type d'appairage : Sélectionnez dans la liste déroulante.

Adresse : Entrez le nom d'hôte ou l'adresse IP de la caméra PTZ.

Username (Nom d'utilisateur) : Saisissez le nom d'utilisateur de la caméra PTZ.

Mot de passe : Saisissez le mot de passe de la caméra PTZ.

Close (Fermer) : Cliquez pour effacer le contenu de tous les champs.

Connect (Connexion) : Cliquez pour établir une connexion à la caméra PTZ.

Configurer le suivi automatique du radar : Cliquez pour ouvrir et configurer le suivi automatique. Vous pouvez également accéder à **Radar > Radar PTZ autotracking (Radar > Suivi automatique du radar)** pour le configurer.

Journaux

Rapports et journaux

Rapports

- **View the device server report (Afficher le rapport du serveur de périphériques)** : Affichez des informations sur le statut du produit dans une fenêtre contextuelle. Le journal d'accès figure également dans le rapport de serveur.
- **Download the device server report (Télécharger le rapport du serveur de périphériques)** : Il crée un fichier .zip qui contient un fichier texte du rapport de serveur complet au format UTF-8 et une capture d'image de la vidéo en direct actuelle. Joignez toujours le fichier .zip du rapport de serveur lorsque vous contactez le support.
- **Download the crash report (Télécharger le rapport d'incident)** : Téléchargez une archive avec des informations détaillées sur l'état du serveur. Le rapport d'incident contient des informations figurant dans le rapport de serveur ainsi que des informations de débogage détaillées. Ce rapport peut aussi contenir des informations sensibles comme le suivi réseau. L'opération de génération du rapport peut prendre plusieurs minutes.

Journaux

- **View the system log (Afficher le journal système)** : cliquez pour afficher les informations sur les événements système tels que le démarrage du périphérique, les avertissements et les messages critiques.
- **View the access log (Afficher le journal d'accès)** : cliquez pour afficher tous les échecs d'accès au périphérique, par exemple si un mot de passe erroné a été utilisé.

Journal système à distance

Syslog est une norme de journalisation des messages. Elle permet de séparer le logiciel qui génère les messages, le système qui les stocke et le logiciel qui les signale et les analyse. Chaque message est étiqueté avec un code de fonction qui donne le type de logiciel générant le message et le niveau de gravité assigné.



Serveur : cliquez pour ajouter un nouvel serveur.

Hôte : saisissez le nom d'hôte ou l'adresse IP du serveur.

Format : Sélectionnez le format de message de journal système à utiliser.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocole) : Sélectionnez le protocole à utiliser :

- UDP (Le port par défaut est 514)
- TCP (Le port par défaut est 601)
- TLS (Le port par défaut est 6514)

Port : Modifiez le numéro de port pour utiliser un autre port.

Severity (Gravité) : sélectionnez les messages à envoyer lorsqu'ils sont déclenchés.

CA certificate set (Initialisation du certificat CA) : affichez les paramètres actuels ou ajoutez un certificat.

Plain Config

Plain config (Configuration simple) est réservée aux utilisateurs avancés qui ont l'expérience de la configuration des périphériques Axis. La plupart des paramètres peuvent être configurés et modifiés à partir de cette page.

Maintenance

Maintenance

Restart (Redémarrer) : Redémarrez le périphérique. Cela n'affecte aucun des paramètres actuels. Les applications en cours d'exécution redémarrent automatiquement.

Restore (Restaurer) : la plupart des paramètres sont rétablis aux valeurs par défaut. Ensuite, vous devez reconfigurer le périphérique et les applications, réinstaller toutes les applications qui ne sont pas préinstallées et recréer les événements et les préreglages.

Important

Les seuls paramètres enregistrés après la restauration sont les suivants :

- le protocole Boot (DHCP ou statique) ;
- l'adresse IP statique ;
- Routeur par défaut
- Masque de sous-réseau
- les réglages 802.1X.
- Réglages O3C
- Adresse IP du serveur DNS

Factory default (Valeurs par défaut) : tous les paramètres sont rétablis aux valeurs par défaut. Réinitialisez ensuite l'adresse IP pour rendre le périphérique accessible.

Remarque

Tous les logiciels des périphériques Axis sont signés numériquement pour garantir que seuls les logiciels vérifiés sont installés sur le périphérique. Cela permet d'accroître le niveau minimal de cybersécurité globale des périphériques Axis. Pour plus d'informations, consultez le livre blanc Axis Edge Vault sur le site axis.com.

AXIS OS upgrade (Mise à niveau d'AXIS OS) : procédez à la mise à niveau vers une nouvelle version d'AXIS OS. Les nouvelles versions peuvent comporter des améliorations de certaines fonctionnalités, des résolutions de bogues et de nouvelles fonctions. Nous vous conseillons de toujours utiliser la version d'AXIS OS la plus récente. Pour télécharger la dernière version, accédez à axis.com/support.

Lors de la mise à niveau, vous avez le choix entre trois options :

- **Standard upgrade (Mise à niveau standard)** : procédez à la mise à niveau vers la nouvelle version d'AXIS OS.
- **Factory default (Valeurs par défaut)** : mettez à niveau et remettez tous les paramètres sur les valeurs par défaut. Si vous choisissez cette option, il est impossible de revenir à la version précédente d'AXIS OS après la mise à niveau.
- **AutoRollback (Restauration automatique)** : mettez à niveau et confirmez la mise à niveau dans la durée définie. Si vous ne confirmez pas, le périphérique revient à la version précédente d'AXIS OS.

AXIS OS rollback (Restauration d'AXIS OS) : revenez à la version d'AXIS OS précédemment installée.

dépannage

Reset PTR (Réinitialiser le PTR)  : réinitialisez le PTR si, pour une quelconque raison, les paramètres **Pan** (Panoramique), **Tilt** (Inclinaison), ou **Roll** (Roulis) ne fonctionnent pas comme prévu. Les moteurs PTR sont toujours calibrés dans une nouvelle caméra. Mais le calibrage peut être perdu, par exemple, si la caméra perd de l'alimentation ou si les moteurs sont déplacés manuellement. Lors de la réinitialisation du PTR, la caméra est re-calibrée et reprend sa position d'usine par défaut.

Calibration (Calibrage)  : Cliquez sur **Calibrate** (Calibrer) pour recalibrer les moteurs de panoramique, d'inclinaison et de roulis à leurs positions par défaut.

Ping : Pour vérifier si le périphérique peut atteindre une adresse spécifique, entrez le nom d'hôte ou l'adresse IP de l'hôte que vous souhaitez pinger et cliquez sur **Start** (Démarrer).

Port check (Contrôle des ports) : Pour vérifier la connectivité du périphérique à une adresse IP et à un port TCP/UDP spécifiques, entrez le nom d'hôte ou l'adresse IP et le numéro de port que vous souhaitez vérifier et cliquez sur **Start** (Démarrer).

Trace réseau

Important

Un fichier de suivi réseau peut contenir des informations sensibles, comme des certificats ou des mots de passe.

Un fichier de suivi réseau contribue à dépanner les problèmes en enregistrant l'activité sur le réseau.

Trace time (Durée du suivi) : Sélectionnez la durée du suivi en secondes ou en minutes puis cliquez sur **Download** (Télécharger).

En savoir plus

Connexions longues distances

Ce produit prend en charge les installations à câbles à fibre optique via un convertisseur de média. Les installations à câbles à fibre optique présentent de nombreux avantages tels que :

- Connexion longues distances
- Grande vitesse
- Longue durée de vie
- Grande capacité de transmission de données
- Immunité aux interférences électromagnétiques

Pour en savoir plus sur les installations de câbles à fibre optique, consultez le livre blanc « Long distance surveillance – Fiber-optic communication in network video » (Surveillance longue distance : communication par fibre optique dans le domaine de la vidéo sur IP), accessible sur la page axis.com/learning/white-papers.

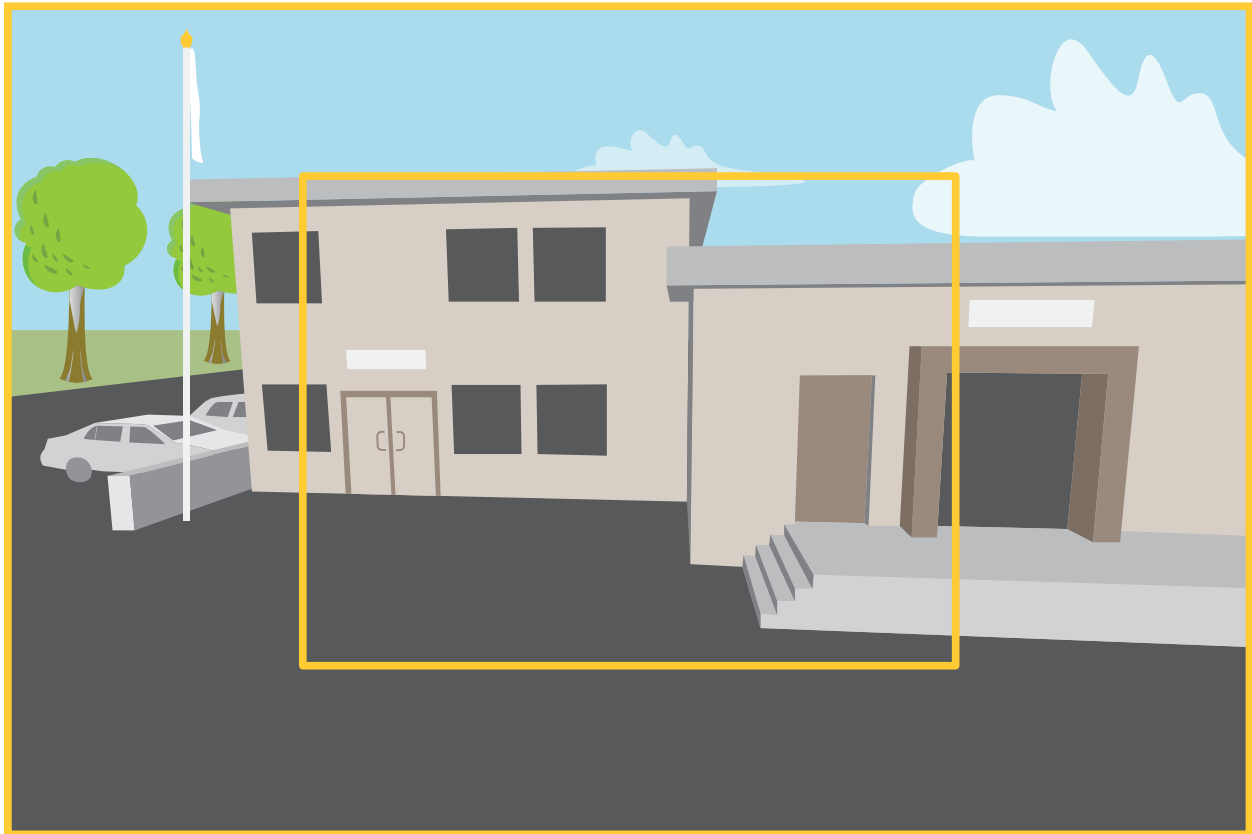
Pour plus d'informations sur l'installation du convertisseur de média, consultez le guide d'installation de ce produit.

Modes de capture

Un mode de capture est une configuration prédéfinie qui définit la manière dont la caméra capture les images.

- Le paramètre du mode de capture peut affecter la résolution maximale et la fréquence d'images maximale disponibles dans le périphérique.
- Le mode de capture avec une résolution inférieure à la résolution maximale peut réduire le champ de vision.
- Le mode de capture influe également sur la vitesse d'obturation, qui à son tour influe sur la sensibilité à la lumière. En effet, un mode de capture avec une fréquence d'image maximale élevée présente une sensibilité à la lumière réduite, et inversement.
- Certains modes de capture ne permettent pas d'utiliser la fonction WDR.

Le mode de capture à plus faible résolution peut être échantillonné à partir de la résolution d'origine, ou être recadré à partir de l'original, auquel cas le champ de vision peut également être affecté.



L'image montre comment le champ de vision et le rapport d'aspect peuvent changer entre deux modes de capture différents. Le mode de capture à choisir dépend des exigences en matière de fréquence d'images et de résolution de la configuration de surveillance spécifique. Pour connaître les spécifications des modes de capture disponibles, consultez la fiche technique du produit sur le site axis.com.

Mise au point à distance et zoom

La fonction de mise au point et de zoom à distance vous permet de régler la mise au point et le zoom de votre caméra depuis un ordinateur. Il s'agit d'un moyen pratique pour s'assurer que la mise au point, l'angle de vue et la résolution de la scène sont optimisés sans devoir se rendre sur le lieu d'installation de la caméra.

Masques de confidentialité

Un masque de confidentialité est une zone définie par l'utilisateur couvrant une partie de la zone surveillée. Les masques de confidentialité se présentent sous forme de blocs de couleur opaque ou de mosaïque sur le flux de données vidéo.

Vous verrez le masque de confidentialité sur toutes les captures d'écran, vidéos enregistrées et flux en direct.

Vous pouvez utiliser l'interface de programmation (API) VAPIX® pour masquer les masques de confidentialité.

Important

Si vous utilisez plusieurs masques de confidentialité, cela peut affecter les performances du produit.

Vous pouvez créer plusieurs masques de confidentialité. Chaque masque peut comporter de 3 à 10 points d'ancrage.

Incrustations

Les incrustations se superposent au flux vidéo. Elles sont utilisées pour fournir des informations supplémentaires lors des enregistrements, telles que des horodatages, ou lors de l'installation et de la configuration d'un produit. Vous pouvez ajouter du texte ou une image.

L'indicateur de flux vidéo est un autre type d'incrustation. Il vous indique que le flux vidéo est en direct.

Diffusion et stockage

Formats de compression vidéo

Choisissez la méthode de compression à utiliser en fonction de vos exigences de visualisation et des propriétés de votre réseau. Les options disponibles sont les suivantes :

Motion JPEG

Remarque

Pour garantir la prise en charge du codec audio Opus, le flux Motion JPEG est toujours envoyé via RTP.

Motion JPEG, ou MJPEG, est une séquence vidéo numérique qui se compose d'une série d'images JPEG individuelles. Ces images s'affichent et sont actualisées à une fréquence suffisante pour créer un flux présentant un mouvement constamment mis à jour. Pour permettre à l'observateur de percevoir la vidéo en mouvement, la fréquence doit être d'au moins 16 images par seconde. Une séquence vidéo normale est perçue à 30 (NTSC) ou 25 (PAL) images par seconde.

Le flux Motion JPEG consomme beaucoup de bande passante, mais fournit une excellente qualité d'image, tout en donnant accès à chacune des images du flux.

H.264 ou MPEG-4 Partie 10/AVC

Remarque

H.264 est une technologie sous licence. Le produit Axis est fourni avec une licence client permettant d'afficher les flux de données vidéo H.264. Il est interdit d'installer d'autres copies du client sans licence. Pour acheter d'autres licences, contactez votre revendeur Axis.

H.264 peut réduire la taille d'un fichier vidéo numérique de plus de 80 % par rapport à Motion JPEG et de plus de 50 % par rapport aux anciens formats MPEG, sans affecter la qualité d'image. Le fichier vidéo occupe alors moins d'espace de stockage et de bande passante réseau. La qualité vidéo à un débit binaire donné est également nettement supérieure.

H.265 ou MPEG-H Partie 2/HEVC

H.265 peut réduire la taille d'un fichier vidéo numérique de plus de 25 % par rapport à H.264, sans affecter la qualité d'image.

Remarque

- H.265 est une technologie sous licence. Le produit Axis est fourni avec une licence client permettant d'afficher les flux de données vidéo H.265. Il est interdit d'installer d'autres copies du client sans licence. Pour acheter d'autres licences, contactez votre revendeur Axis.
- La plupart des navigateurs Web ne prennent pas en charge le décodage H.265 et, de ce fait, la caméra ne le prend pas en charge dans son interface Web. À la place, vous pouvez utiliser un système de gestion vidéo ou une application prenant en charge l'encodage H.265.

Quel est le lien entre les paramètres d'image, de flux et de profil de flux ?

L'onglet **Image (Image)** contient les paramètres de la caméra qui affectent tous les flux vidéo provenant du produit. Si vous modifiez un élément dans cet onglet, cela affecte immédiatement tous les flux vidéo et tous les enregistrements.

L'onglet **Stream (Flux)** contient les paramètres des flux vidéo. Vous obtenez ces paramètres si vous sollicitez un flux vidéo provenant du produit sans spécifier la résolution ou la fréquence d'image, par exemple. Lorsque vous modifiez les paramètres dans l'onglet **Stream (Flux)**, cela n'affecte pas les flux en cours, mais prend effet lorsque vous lancez un nouveau flux.

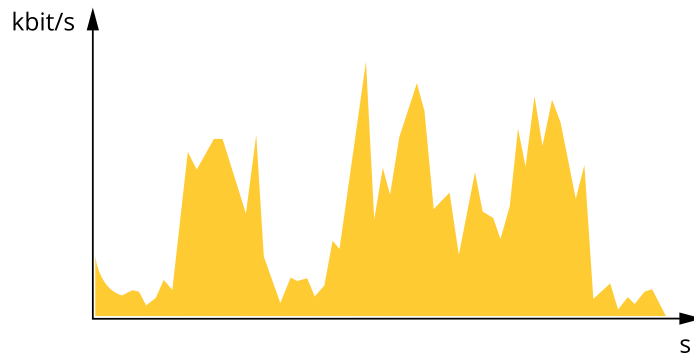
Les paramètres **Stream profiles (Profils de flux)** dépassent les paramètres de l'onglet **Stream (Flux)**. Si vous sollicitez un flux avec un profil de flux spécifique, le flux contient les paramètres de ce profil. Si vous sollicitez un flux sans spécifier de profil de flux ou sollicitez un profil de flux qui n'existe pas dans le produit, le flux contient les paramètres de l'onglet **Stream (Flux)**.

Commande du débit binaire

Le contrôle du débit binaire permet de gérer la consommation de bande passante du flux vidéo.

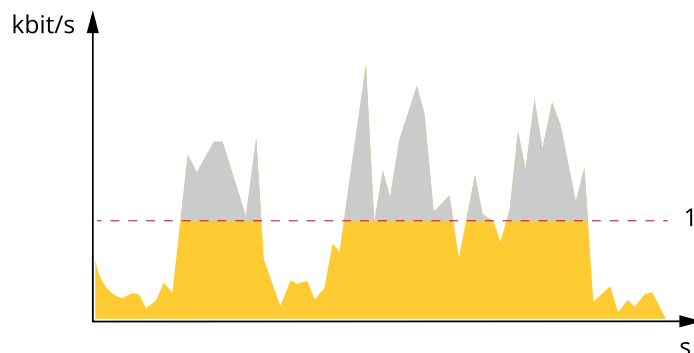
Débit binaire variable (VBR)

Le débit binaire variable permet de faire varier la consommation de bande passante en fonction du niveau d'activité dans la scène. Plus l'activité est intense, plus vous avez besoin de bande passante. Avec un débit binaire variable, une qualité d'image constante est garantie, mais vous devez être sûr d'avoir des marges de stockage.



Débit binaire maximal (MBR)

Le débit binaire maximal permet de définir un débit binaire cible pour gérer les limitations de débit binaire du système. Vous pouvez observer une baisse de la qualité d'image ou de la fréquence d'images lorsque le débit binaire instantané est maintenu en dessous du débit binaire cible spécifié. Vous pouvez choisir de donner la priorité soit à la qualité d'image, soit à la fréquence d'image. Nous vous conseillons de configurer le débit binaire cible sur une valeur plus élevée que le débit binaire attendu. Vous bénéficiez ainsi d'une marge si l'activité dans la scène est élevée.

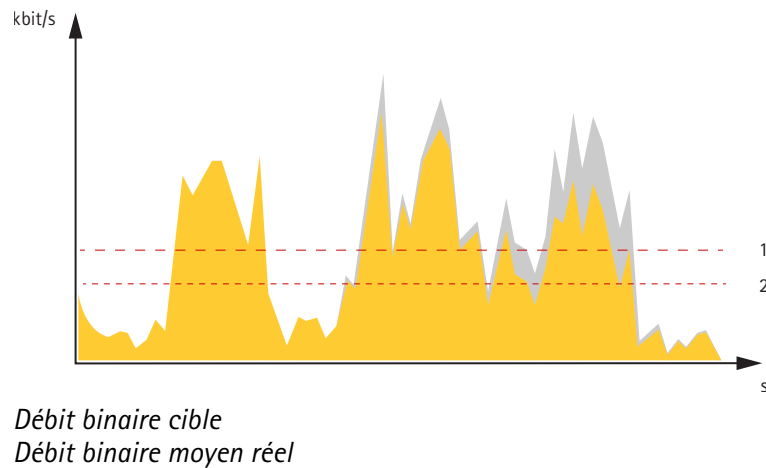


1 Débit binaire cible

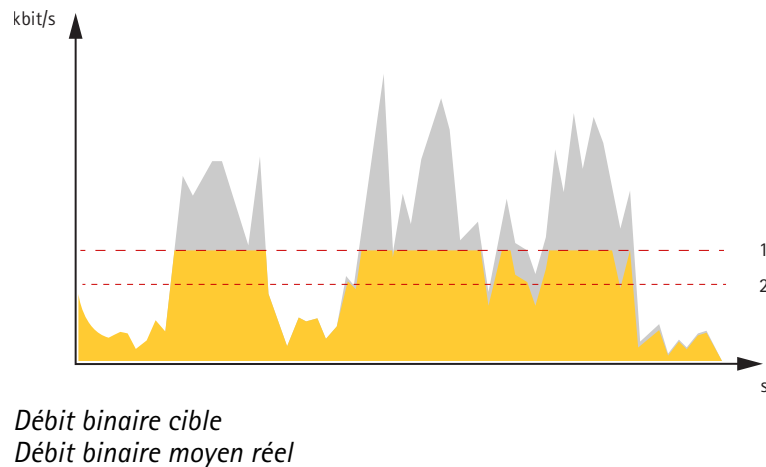
Débit binaire moyen (ABR)

Avec le débit binaire moyen, le débit binaire est automatiquement ajusté sur une période de temps plus longue. Vous pouvez ainsi atteindre la cible spécifiée et obtenir la meilleure qualité vidéo en fonction du stockage disponible. Le débit binaire est plus élevé dans les scènes présentant une activité importante que dans les scènes statiques. Vous avez plus de chances d'obtenir une meilleure qualité d'image dans les scènes avec beaucoup d'activité si vous utilisez l'option de débit binaire moyen. Vous pouvez définir le stockage total requis pour stocker le flux vidéo pendant une durée spécifiée (durée de conservation) lorsque la qualité d'image est ajustée pour atteindre le débit binaire cible spécifié. Spécifiez les paramètres du débit binaire moyen de l'une des façons suivantes :

- Pour calculer l'estimation du stockage nécessaire, définissez le débit binaire cible et la durée de conservation.
- Pour calculer le débit binaire moyen en fonction du stockage disponible et de la durée de conservation requise, utilisez la calculatrice de débit binaire cible.



Vous pouvez également activer le débit binaire maximum et spécifier un débit binaire cible dans l'option de débit binaire moyen.



Applications

Les applications vous permettent de tirer pleinement avantage de votre périphérique Axis. AXIS Camera Application Platform (ACAP) est une plateforme ouverte qui permet à des tiers de développer des outils d'analyse et d'autres applications pour les périphériques Axis. Les applications, téléchargeables gratuitement ou moyennant le paiement d'une licence, peuvent être préinstallées sur le périphérique.

Pour rechercher les manuels utilisateur des applications Axis, consultez le site help.axis.com.

Remarque

- Plusieurs applications peuvent être exécutées en même temps, mais il se peut que certaines applications ne soient pas compatibles entre elles. Il est possible que certaines combinaisons d'applications nécessitent trop de puissance de calcul ou de ressources mémoire lorsqu'elles sont exécutées en parallèle. Vérifiez que les applications fonctionnent ensemble avant le déploiement.

AXIS Object Analytics

AXIS Object Analytics est une application d'analyse préinstallée sur la caméra. Elle détecte les objets en mouvement dans la scène et les classe, par exemple, en tant que personnes ou véhicules. Vous pouvez configurer l'application pour qu'elle envoie des alarmes sur différents types d'objets. Pour en savoir plus sur le fonctionnement de l'application, consultez le *manuel d'utilisation d'AXIS Object Analytics*.

AXIS Image Health Analytics

AXIS Image Health Analytics est une application basée sur l'IA qui peut être utilisée pour détecter les dégradations ou tentatives d'altération d'images. L'application analyse et apprend le comportement de la scène pour détecter le flou ou la sous-exposition de l'image, ou pour détecter une vue obstruée ou redirigée. Vous

pouvez configurer l'application pour qu'elle envoie des événements pour chacune de ces détections et déclenche des actions par le biais du système d'événements de la caméra ou d'un logiciel tiers.

Pour en savoir plus sur le fonctionnement de l'application, consultez le *manuel d'utilisation d'AXIS Image Health Analytics*.

Visualisation des métadonnées

Des métadonnées analytiques sont disponibles pour les objets en mouvement dans la scène. Les classes d'objets pris en charge sont visualisées dans le flux vidéo via une boîte de mesure entourant l'objet, ainsi que des informations sur le type d'objet et le niveau de confiance de la classification. Pour en savoir plus sur la configuration et la consommation des métadonnées analytiques, consultez le *guide d'intégration AXIS Scene Metadata*.

Cybersécurité

Pour obtenir des informations spécifiques sur la cybersécurité, consultez la fiche technique du produit sur le site axis.com.

Pour des informations plus détaillées sur la cybersécurité dans AXIS OS, lisez le *guide du durcissement d'AXIS OS*.

Système d'exploitation signé

Le système d'exploitation signé est mis en œuvre par le fournisseur du logiciel, qui signe l'image d'AXIS OS avec une clé privée. Lorsque la signature est associée au système d'exploitation, le périphérique valide le logiciel avant de l'installer. Si le périphérique détecte que l'intégrité du logiciel est compromise, la mise à niveau d'AXIS OS est rejetée.

Démarrage sécurisé

L'amorçage sécurisé est un processus d'amorçage constitué d'une chaîne ininterrompue de logiciels validés par cryptographie, commençant dans la mémoire immuable (ROM d'amorçage). Basé sur l'utilisation d'un système d'exploitation signé, le démarrage sécurisé garantit qu'un périphérique ne peut démarrer qu'avec le logiciel autorisé.

Axis Edge Vault

Axis Edge Vault fournit une plateforme de cybersécurité matérielle qui protège les périphériques Axis. Elle garantit leur identité et leur intégrité, et protège vos informations sensibles contre tout accès non autorisé. Elle repose sur des bases solides constituées de modules de calcul cryptographique (élément sécurisé et TPM) et d'une sécurité SoC (TEE et démarrage sécurisé), associés au savoir-faire en matière de sécurité des dispositifs périphériques.

Module TPM

Le TPM (Trusted Platform Module : module de plateforme de confiance) est un composant qui procure des fonctions cryptographiques pour protéger les informations contre les accès non autorisés. Il est toujours activé et vous ne pouvez modifier aucun paramètre.

Identifiant du périphérique Axis

Être capable de vérifier l'origine du périphérique est essentiel pour instaurer la confiance dans l'identité du périphérique. Pendant la production, avec Axis Edge Vault, un certificat d'identifiant de périphérique Axis unique, provisionné en usine et conforme IEEE 802.1AR est assigné à chaque périphérique. Ceci fonctionne comme un passeport pour prouver l'origine du périphérique. L'identifiant de périphérique est stocké de façon permanente dans un fichier de clés sécurisé sous la forme d'un certificat signé par le certificat racine Axis. L'ID du dispositif peut être utilisé par l'infrastructure informatique du client pour l'intégration automatique et l'identification sécurisée des dispositifs.

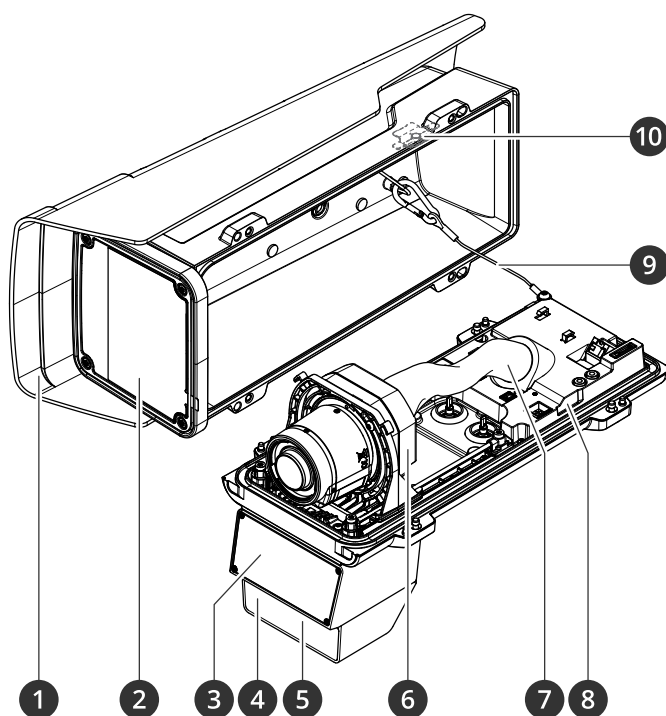
Vidéo signée

La signature vidéo garantit que les preuves vidéo peuvent être confirmées intactes sans avoir à démontrer la chaîne de possession du fichier vidéo. Chaque caméra utilise sa clé de signature de vidéo unique, qui est stockée dans un fichier de clés sécurisé, pour ajouter une signature dans le flux vidéo. À la lecture, le lecteur vidéo indique si la vidéo est intacte. La signature vidéo permet de remonter la vidéo jusqu'à l'origine de la caméra et de vérifier qu'elle n'a pas été modifiée après avoir quitté la caméra.

Pour en savoir plus sur les fonctionnalités de cybersécurité des périphériques Axis, accédez à axis.com/learning/white-papers et lancez une recherche sur la cybersécurité.

Caractéristiques techniques

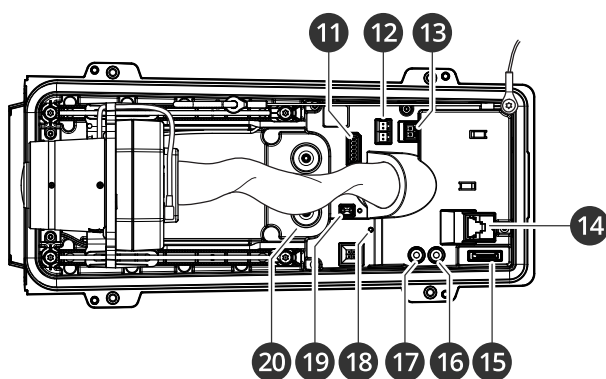
Gamme de produits



- 1 Protection étanche
- 2 Fenêtre
- 3 Radar
- 4 Capteur de luminosité
- 5 LED d'illumination IR
- 6 Unité optique
- 7 Couvercle de câble
- 8 Capteur d'alarme d'intrusion
- 9 Câble de sécurité
- 10 Aimant d'alarme d'intrusion

AVIS

Ne soulevez pas le produit dans le couvercle de câble.



- 1 Connecteur E/S
- 2 Connecteur RS485/422
- 3 Connecteur d'alimentation
- 4 Connecteur réseau (PoE)
- 5 Emplacement pour carte microSD
- 6 Sortie audio

- 7 Entrée audio
- 8 DEL d'état
- 9 Bouton de commande
- 10 Joint de câble M20 (x2)

Voyants DEL

Remarque

- Le voyant d'état peut clignoter lorsqu'un événement est actif.
- Les voyants s'éteignent lorsque vous fermez le boîtier.

DEL d'état	Indication
Éteint	Branchement et fonctionnement normal.
Vert	Vert et fixe pendant 10 secondes pour indiquer un fonctionnement normal après le démarrage.
Orange	Fixe pendant le démarrage. Clignote pendant les mises à niveau du logiciel du périphérique ou le rétablissement des valeurs par défaut configurées en usine.
Orange / Rouge	Clignote en orange/rouge en cas d'indisponibilité ou de perte de la connexion réseau.
Rouge	Échec de la mise à niveau du logiciel du périphérique.

Avertisseur

Signal sonore de l'assistant de mise au point

Remarque

Valable uniquement pour les objectifs à diaphragme P, DC ou manuel en option.

Avertisseur	Objectif
Intervalle rapide	Réglage optimal
Intervalle intermédiaire	Réglage moins optimal
Intervalle lent	Réglage médiocre

Emplacement pour carte SD

Ce périphérique est compatible avec les cartes microSD/microSDHC/microSDXC.

Pour des recommandations sur les cartes SD, rendez-vous sur axis.com.

 Les logos microSD, microSDHC et microSDXC sont des marques commerciales de SD-3C LLC. microSD, microSDHC, microSDXC sont des marques commerciales ou des marques déposées de SD-3C, LLC aux États-Unis et dans d'autres pays.

Boutons

Bouton de commande

Le bouton de commande permet de réaliser les opérations suivantes :

- Réinitialisation du produit aux paramètres d'usine par défaut. Cf. .

- Connexion à un service one-click cloud connection (O3C) sur Internet. Pour vous connecter, appuyez et relâchez le bouton, puis attendez que la LED de status clignote trois fois en vert.

Interrupteur d'alarme d'intrusion

Utilisez le commutateur d'alarme d'intrusion pour recevoir une notification lorsqu'une personne ouvre le boîtier du périphérique. Créez une règle pour que le périphérique exécute une action lorsque le commutateur est activé. Cf. .

Connecteurs

Connecteur réseau

Connecteur Ethernet RJ45 avec Power over Ethernet Plus (PoE+).

Connecteur audio

- **Entrée audio** – entrée de 3,5 mm pour microphone mono ou signal d'entrée mono (le canal de gauche est utilisé pour le signal stéréo).
- **Entrée audio** – entrée de 3,5 mm pour microphone numérique, microphone mono analogique ou signal d'entrée mono (le canal de gauche est utilisé pour le signal stéréo).
- **Sortie audio** – sortie de 3,5 mm (niveau de ligne) qui peut être connectée à un système de sonorisation ou à un haut-parleur actif avec amplificateur intégré. Un connecteur stéréo doit être utilisé pour la sortie audio.



Entrée audio

1 Pointe	2 Anneau	3 Manchon
Microphone déséquilibré (avec ou sans alimentation à électret) ou entrée de ligne	Alimentation à électret si sélectionnée	Terre
Microphone équilibré (avec ou sans alimentation fantôme) ou entrée de ligne, signal « chaud »	Microphone équilibré (avec ou sans alimentation fantôme) ou entrée de ligne, signal « froid »	Terre
Signal numérique	Alimentation en boucle si sélectionnée	Terre

Sortie audio

1 Pointe	2 Anneau	3 Manchon
Canal 1, ligne déséquilibrée, mono	Canal 1, ligne déséquilibrée, mono	Terre

Connecteur E/S

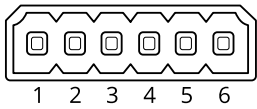
Utilisez le connecteur d'E/S avec des périphériques externes, associés aux applications telles que la détection de mouvement, le déclenchement d'événements et les notifications d'alarme. En plus du point de référence 0 V CC et de l'alimentation (sortie 12 V CC), le connecteur d'E/S fournit une interface aux éléments suivants :

Entrée numérique – Pour connecter des dispositifs pouvant passer d'un circuit ouvert à un circuit fermé, par exemple capteurs infrarouge passifs, contacts de porte/fenêtre et détecteurs de bris de verre.

Entrée supervisée – Permet la détection de sabotage sur une entrée numérique.

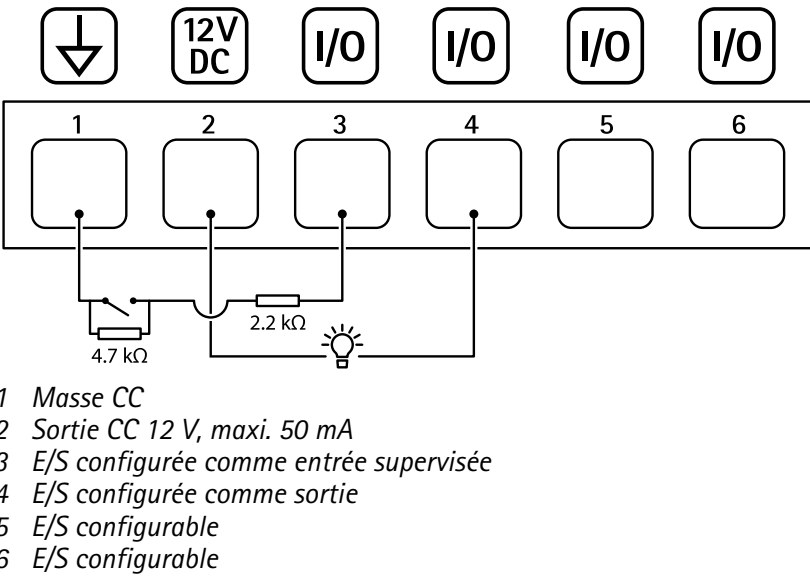
Sortie numérique – Permet de connecter des dispositifs externes, comme des relais ou des voyants. Les périphériques connectés peuvent être activés par l'interface de programmation VAPIX®, via un événement ou à partir de l'interface web du périphérique.

Bloc terminal à 6 broches



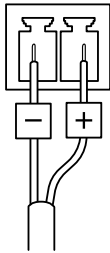
Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1		0 V CC
Sortie CC	2	Cette broche peut également servir à l'alimentation de matériel auxiliaire. Remarque : cette broche ne peut être utilisée que comme sortie d'alimentation.	12 V CC Charge maximale = 50 mA
Configurable (entrée ou sortie)	3–6	Entrée numérique ou entrée supervisée – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver. Pour utiliser une entrée supervisée, installez des résistances de fin de ligne. Consultez le schéma de connexion pour plus d'informations sur la connexion des résistances.	0 à 30 V CC max.
		Sortie numérique – Connexion interne à la broche 1 (masse CC) en cas d'activation, et flottante (déconnectée) en cas de désactivation. En cas d'utilisation avec une charge inductive, par exemple un relais, connectez une diode en parallèle à la charge pour assurer la protection contre les transitoires de tension.	0 à 30 V CC max., drain ouvert, 100 mA

Exemple:



Connecteur d'alimentation

Bloc terminal à 2 broches pour l'entrée d'alimentation CC. Utilisez une source d'alimentation limitée (LPS) conforme aux exigences de Très basse tension de sécurité (TBTS) dont la puissance de sortie nominale est limitée à ≤100 W ou dont le courant de sortie nominal est limité à ≤5 A.

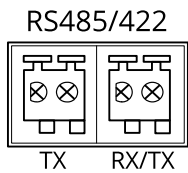


Connecteur RS485/RS422

Blocs terminaux à 2 broches pour interface série RS485/RS422.

Le port série peut être configuré pour la prise en charge de :

- RS485 semi-duplex sur deux fils
- RS485 duplex intégral sur quatre fils
- RS422 simplex sur deux fils
- RS422 full-duplex sur quatre fils pour communication point à point



Fonction	Remarques
RS485/RS422 TX(A)	Paire TX pour RS422 et RS485 à 4 fils
RS485/RS422 TX(B)	
RS485A alt RS485/422 RX (A)	Paire RX pour tous les modes (RX/TX combiné pour RS485 à 2 fils)
RS485B alt RS485/422 RX (B)	

Recherche de panne

Réinitialiser les paramètres par défaut

■ AVERTISSEMENT

Ce produit est susceptible d'émettre un rayonnement optique dangereux. Cela peut être nocif pour les yeux. Ne regardez jamais directement la lampe en fonctionnement.

Important

La restauration des paramètres par défaut doit être effectuée avec prudence. Cette opération restaure tous les paramètres par défaut, y compris l'adresse IP.

Pour réinitialiser l'appareil aux paramètres d'usine par défaut :

1. Déconnectez l'alimentation de l'appareil.
2. Remettez le produit sous tension en maintenant le bouton de commande enfoncé. Cf. .
3. Maintenez le bouton de commande enfoncé pendant 15-30 secondes, jusqu'à ce que le voyant d'état à LED passe à l'orange et clignote.
4. Relâchez le bouton de commande. Le processus est terminé lorsque le voyant d'état à LED passe au vert. Si aucun serveur DHCP n'est disponible sur le réseau, l'adresse IP du périphérique est définie par défaut sur l'une des valeurs suivantes :
 - Périphériques dotés d'AXIS OS 12.0 ou d'une version ultérieure : Obtenu à partir du sous-réseau de l'adresse lien-local (169.254.0.0/16)
 - Périphériques équipés d'AXIS OS 11.11 ou d'une version antérieure : 192.168.0.90/24
5. Utilisez les logiciels d'installation et de gestion pour attribuer une adresse IP, configurer le mot de passe et accéder au périphérique.
Les logiciels d'installation et de gestion sont disponibles sur les pages d'assistance du site axis.com/support.

Vous pouvez également rétablir les paramètres d'usine par défaut via l'interface web du périphérique. Accédez à **Maintenance > Factory default (Valeurs par défaut)** et cliquez sur **Default (Par défaut)**.

Options d'AXIS OS

Axis permet de gérer le logiciel du périphérique conformément au support actif ou au support à long terme (LTS). Le support actif permet d'avoir continuellement accès à toutes les fonctions les plus récentes du produit, tandis que le support à long terme offre une plateforme fixe avec des versions périodiques axées principalement sur les résolutions de bogues et les mises à jour de sécurité.

Il est recommandé d'utiliser la version d'AXIS OS du support actif si vous souhaitez accéder aux fonctions les plus récentes ou si vous utilisez des offres système complètes d'Axis. Le support à long terme est recommandé si vous utilisez des intégrations tierces, qui ne sont pas continuellement validées par rapport au dernier support actif. Avec le support à long terme, les produits peuvent assurer la cybersécurité sans introduire de modification fonctionnelle ni affecter les intégrations existantes. Pour plus d'informations sur la stratégie de logiciel du périphérique Axis, consultez axis.com/support/device-software.

Vérifier la version actuelle d'AXIS OS

Le système Axis OS utilisé détermine la fonctionnalité de nos périphériques. Lorsque vous devez résoudre un problème, nous vous recommandons de commencer par vérifier la version actuelle d'AXIS OS. En effet, il est possible que la toute dernière version contienne un correctif pouvant résoudre votre problème.

Pour vérifier la version actuelle d'AXIS OS :

1. Allez à l'interface web du périphérique > **Status (Statut)**.
2. Sous **Device info (Informations sur les périphériques)**, consultez la version d'AXIS OS.

Mettre à niveau AXIS OS

Important

- Les paramètres préconfigurés et personnalisés sont enregistrés lors de la mise à niveau du logiciel du périphérique (à condition qu'il s'agisse de fonctions disponibles dans le nouvel AXIS OS), mais Axis Communications AB n'offre aucune garantie à ce sujet.
- Assurez-vous que le périphérique reste connecté à la source d'alimentation pendant toute la durée du processus de mise à niveau.

Remarque

La mise à niveau vers la dernière version d'AXIS OS de la piste active permet au périphérique de bénéficier des dernières fonctionnalités disponibles. Lisez toujours les consignes de mise à niveau et les notes de version disponibles avec chaque nouvelle version avant de procéder à la mise à niveau. Pour obtenir la dernière version d'AXIS OS et les notes de version, rendez-vous sur axis.com/support/device-software.

1. Téléchargez le fichier AXIS OS sur votre ordinateur. Celui-ci est disponible gratuitement sur axis.com/support/device-software.
2. Connectez-vous au périphérique en tant qu'administrateur.
3. Accédez à **Maintenance > AXIS OS upgrade (Mise à niveau d'AXIS OS)** et cliquez sur **Upgrade (Mettre à niveau)**.

Une fois la mise à niveau terminée, le produit redémarre automatiquement.

Problèmes techniques, indications et solutions

Si vous ne trouvez pas les informations dont vous avez besoin ici, consultez la section consacrée au dépannage sur la page axis.com/support.

Problèmes de mise à niveau d'AXIS OS

Échec de la mise à niveau d'AXIS OS	En cas d'échec de la mise à niveau, le périphérique recharge la version précédente. Le problème provient généralement du chargement d'un fichier AXIS OS incorrect. Vérifiez que le nom du fichier AXIS OS correspond à votre périphérique, puis réessayez.
Problèmes survenant après la mise à niveau d'AXIS OS	Si vous rencontrez des problèmes après la mise à niveau, revenez à la version installée précédemment à partir de la page Maintenance .

Problème de configuration de l'adresse IP

Le périphérique se trouve sur un sous-réseau différent.	Si l'adresse IP du périphérique et l'adresse IP de l'ordinateur utilisé pour accéder au périphérique se trouvent sur des sous-réseaux différents, vous ne pourrez pas configurer l'adresse IP. Contactez votre administrateur réseau pour obtenir une adresse IP.
---	---

L'adresse IP est utilisée par un autre périphérique.	Déconnectez le périphérique Axis du réseau. Exécutez la commande ping (dans une fenêtre de commande/DOS, entrez <code>ping</code> et l'adresse IP du périphérique) : - Si vous recevez : <code>Reply from <IP address>: bytes=32; time=10...</code>, cela signifie que l'adresse IP est peut-être déjà utilisée par un autre périphérique sur le réseau. Obtenez une nouvelle adresse IP auprès de l'administrateur réseau, puis réinstallez le périphérique. - Si vous recevez : <code>Request timed out</code>, cela signifie que l'adresse IP est disponible pour une utilisation avec le périphérique Axis. Vérifiez tous les câbles et réinstallez le périphérique.
Conflit d'adresse IP possible avec un autre périphérique sur le même sous-réseau	L'adresse IP statique du périphérique Axis est utilisée avant la configuration d'une adresse dynamique par le serveur DHCP. Cela signifie que des problèmes d'accès au périphérique sont possibles si un autre périphérique utilise la même adresse IP statique par défaut.

Impossible d'accéder au périphérique à partir d'un navigateur Web

Connexion impossible	Lorsque HTTPS est activé, assurez-vous que le protocole correct (HTTP ou HTTPS) est utilisé lorsque vous tentez de vous connecter. Il est possible que vous deviez saisir manuellement <code>http</code> ou <code>https</code> dans la barre d'adresse du navigateur. Si vous perdez le mot de passe pour le compte root d'utilisateur, les paramètres d'usine par défaut du périphérique devront être rétablis. Cf. .
L'adresse IP a été modifiée par DHCP.	Les adresses IP obtenues auprès d'un serveur DHCP sont dynamiques et peuvent changer. Si l'adresse IP a été modifiée, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau. Identifiez le périphérique à partir de son numéro de modèle ou de série ou de son nom DNS (si le nom a été configuré). Si nécessaire, une adresse IP statique peut être attribuée manuellement. Pour plus d'instructions, consultez la page axis.com/support.
Erreur de certification avec IEEE 802.1X	Pour que l'authentification fonctionne correctement, la date et l'heure du périphérique Axis doivent être synchronisées avec un serveur NTP. Accédez à System > Date and time (Système > Date et heure).

Le périphérique est accessible localement, mais pas en externe.

Pour accéder au périphérique en externe, nous vous recommandons d'utiliser l'une des applications pour Windows® suivantes :

- AXIS Camera Station 5 : version d'essai gratuite de 30 jours, application idéale pour les systèmes de petite taille et de taille moyenne.
- AXIS Camera Station Pro : version d'essai gratuite de 90 jours, application idéale pour les systèmes de petite taille et de taille moyenne.

Pour obtenir des instructions et des téléchargements, accédez à axis.com/vms.

Connexion impossible via le port 8883 avec MQTT sur SSL

Le pare-feu bloque le trafic via le port 8883, car ce dernier est considéré comme non sécurisé.

Dans certains cas, le serveur/courtier ne fournit pas de port spécifique pour la communication MQTT. Il peut toujours être possible d'utiliser MQTT sur un port qui sert normalement pour le trafic HTTP/HTTPS.

- Si le serveur/courtier prend en charge WebSocket/WebSocket Secure (WS/WSS), généralement sur le port 443, utilisez plutôt ce protocole. Vérifiez auprès du fournisseur de serveur/courtier si WS/WSS est pris en charge, ainsi que le port et le chemin d'accès de la base à utiliser.
- Si le serveur/courtier prend en charge ALPN, l'utilisation de MQTT peut être négociée sur un port ouvert, tel que 443. Vérifiez auprès de votre fournisseur de serveur/courtier si le protocole ALPN est pris en charge et quels sont le protocole et le port ALPN à utiliser.

Les problèmes de la fusion radar-vidéo

La zone de délimitation ne couvre pas l'objet avec précision

S'il n'y a pas de détection par analyse vidéo, la caméra montrera la projection de la détection radar dans l'image, ce qui n'est pas aussi précis qu'une matrice de caractères d'analyse vidéo. Cela peut également être dû à des différences d'élévation dans la scène, comme une route en pente, une colline ou une dépression.

Si la zone de délimitation est trop haute ou trop basse, assurez-vous que la hauteur d'installation est correctement réglée. Vous pouvez également améliorer la précision des matrices de caractères grâce à la fonction de calibrage automatique. Pour utiliser le calibrage automatique, allez à **Radar > Autocalibration (Calibrage automatique)**.

La matrice de caractères indique 1 personne alors qu'il y a effectivement 2 personnes.

Si deux personnes marchent à proximité l'une de l'autre et ne sont détectées que par le radar, elles seront classées comme une seule personne et une zone de délimitation unique apparaît. Lorsqu'elles entrent dans la zone de fusion analytique, elles sont classées avec précision.

La zone de délimitation déplace sa position lors du suivi d'un objet

Lorsque l'analyse radar et l'analyse caméra détectent le même objet, ou si seule l'analyse caméra détecte l'objet, la zone de délimitation sera dessinée autour de l'objet en utilisant les informations de la caméra.

Si la détection vidéo est perdue, la zone de délimitation sera dessinée à la position de la projection radar, ce qui est moins précis. Une fois la détection vidéo récupérée, la matrice de caractères sera à nouveau dessinée à la position correcte.

Vous pouvez également améliorer la précision des matrices de caractères grâce à la fonction de calibrage automatique. Pour utiliser le calibrage automatique, allez à **Radar > Autocalibration (Calibrage automatique)**.

Je n'obtiens pas la même distance de détection que celle indiquée dans le manuel

Plusieurs facteurs influent sur la distance de détection :

- Vérifiez que la hauteur correcte est saisie dans les paramètres.
- En fonction de l'angle d'approche de l'objet vers le point d'installation, la distance de détection peut varier. Dans les parties extérieures du champ de vision, la sensibilité de détection est plus faible du point de vue du radar. Pensez à orienter la caméra AXIS Q1656-DLE dans le sens où l'intrus est censé s'éloigner le plus.

Comment puis-je minimiser les fausses alarmes ?	Voici quelques astuces permettant de minimiser les fausses alarmes : • Assurez-vous que la scène est bien éclairée pour maximiser la probabilité de détection de l'analyse vidéo. • Réglez la sensibilité sur Low (Faible) dans l'application AXIS Object Analytics. Il faut donc que les analyses vidéo et radar concordent avant de déclencher une alarme. • Utilisez des zones d'exclusion dans le radar pour ignorer les sources connues de fausses détections, telles que la végétation ondulante et les bâtiments. • Configurez le radar de façon à utiliser une sensibilité faible. • Utilisez les zones d'exclusion de l'application AXIS Object Analytics. • L'herbe du site doit rester courte.
Interférence radar	Le dispositif utilise l'un des deux canaux radar. Dans chaque canal, jusqu'à quatre radars peuvent négocier la meilleure façon d'utiliser cette fréquence. Parfois, vous pouvez voir un message d'avertissement concernant les interférences de la caméra, malgré cette fonctionnalité. Vous pouvez alors sélectionner manuellement un canal pour chaque dispositif. Les dispositifs qui sont physiquement proches les uns des autres doivent être réglés sur le même canal. Cela permet aux dispositifs d'éviter plus facilement les interférences.

Facteurs ayant un impact sur la performance

Les principaux facteurs à prendre en compte sont les suivants :

- Une utilisation intensive du réseau en raison de l'inadéquation des infrastructures affecte la bande passante.

Contacter l'assistance

Si vous avez besoin d'aide supplémentaire, accédez à axis.com/support.

T10180975_fr

2025-04 (M22.2)

© 2022 – 2025 Axis Communications AB