

AXIS D2210-VE Radar

Table des matières

Installation	4
Considérations de performance.....	4
Où installer le produit	4
Installer plusieurs radars	5
Profils radar	7
Profil de surveillance de zone	7
Zone de couverture.....	7
Plage de détection de zone.....	7
Exemples d'installation de zone.....	8
Cas d'utilisation de la surveillance de zone	9
Profil de surveillance routière	10
Plage de détection routière.....	10
Exemples d'installation routière	10
Cas d'utilisation de la surveillance routière.....	12
MISE EN ROUTE	14
Trouver le périphérique sur le réseau	14
Prise en charge navigateur.....	14
Ouvrir l'interface web du périphérique.....	14
Créer un compte administrateur	14
Mots de passe sécurisés	15
Vérifiez que personne n'a saboté le logiciel du périphérique.....	15
Vue d'ensemble de l'interface web	15
Configurer votre périphérique.....	16
Sélectionner un profil de radar.....	16
Régler la hauteur de montage.....	16
Calibrez une carte de référence.....	16
Définir des zones de détection	17
Ajouter des scénarios.....	18
Ajouter des zones d'exclusion	19
Réduire les fausses alarmes.....	19
Régler l'image du radar.....	20
Afficher une incrustation d'image.....	20
Afficher une incrustation de texte	20
Afficher et enregistrer la vidéo.....	21
Réduire la bande passante et le stockage	21
Configurer le stockage réseau	21
Enregistrer et regarder la vidéo	22
Définir des règles pour les événements	22
Déclencher une action.....	22
Sauvegarder une vidéo depuis une caméra lorsqu'un mouvement est détecté.....	22
Sauvegarder la vidéo d'une caméra lorsqu'un véhicule roule dans le mauvais sens.....	23
Activer un balayage rouge sur le radar.....	24
Envoyer un e-mail si le radar est recouvert d'un objet métallique.....	25
Allumer un éclairage lorsqu'un mouvement est détecté	26
Contrôler une caméra PTZ avec le radar	26
Utiliser MQTT pour envoyer des données radar.....	28
L'interface web.....	29
État	29
Radar.....	30
Paramètres	30
Flux.....	32
Calibrage de la carte	32
Zones d'exclusion	33

Scénarios.....	34
Incrustations.....	35
Bande de LED dynamique	37
Suivi automatique PTZ du radar.....	37
Enregistrements.....	38
Applications	40
Système	40
Heure et emplacement.....	40
Réseau	42
Sécurité.....	46
Comptes.....	50
Événements	52
MQTT	57
Stockage	60
Profils de flux.....	62
ONVIF.....	63
Détecteurs	66
Accessoires	66
Edge-to-Edge.....	67
Journaux	68
Plain Config	69
Maintenance	69
Maintenance.....	69
dépannage.....	70
Valider votre installation	71
Valider l'installation du radar.....	71
Terminer la validation.....	72
En savoir plus.....	73
Diffusion et stockage.....	73
Formats de compression vidéo	73
Commande du débit binaire.....	73
Incrustations	75
Caractéristiques techniques	76
Gamme de produits	76
Voyants DEL.....	76
.....	76
Emplacement pour carte SD	77
Boutons	77
Bouton de commande	77
Connecteurs	77
Connecteur réseau (PoE in).....	77
Connecteur réseau (sortie PoE).....	77
Connecteur E/S.....	78
Connecteur d'alimentation	79
Nettoyer votre dispositif	80
Recherche de panne.....	81
Réinitialiser les paramètres par défaut.....	81
Vérifier la version actuelle d'AXIS OS.....	81
Mettre à niveau AXIS OS.....	81
Problèmes techniques, indications et solutions.....	82
Facteurs ayant un impact sur la performance	83
Contacter l'assistance.....	83

Installation

Cette vidéo montre un exemple d'installation du radar.

Pour obtenir des instructions complètes sur tous les scénarios d'installation ainsi que des informations de sécurité importantes, consultez le guide d'installation disponible sur axis.com/products/axis-d2210-ve-radar/support.

Pour regarder cette vidéo, accédez à la version Web de ce document.

Considérations de performance

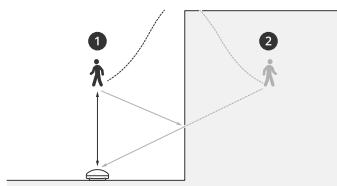
Où installer le produit

Surveillance des zones ou des routes

Le radar est conçu pour la surveillance de zones ouvertes et vous pouvez l'utiliser pour la surveillance de zones ou la surveillance routière. Il dispose de deux profils pour optimiser les performances de chacun des scénarios. Pour plus d'informations sur la plage de détection, les exemples d'installation et les cas d'utilisation, consultez .

Éviter les objets solides et réfléchissants

La plupart des objets solides (murs, clôtures, arbres ou grands buissons, notamment) situés dans la zone de couverture créent un angle mort (ombre radar) derrière lui. 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.



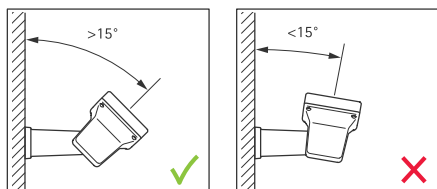
- 1 Détection réelle
- 2 Détection par réflexion (traces fantômes)

Pour plus d'informations sur la gestion des objets solides et réfléchissants, consultez .

Sur support mobile

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.

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

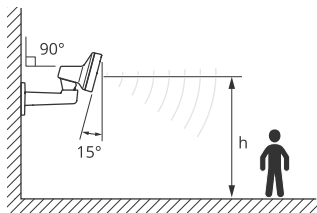


Angle de roulis

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

Angle d'inclinaison

Le radar peut être incliné de 0 à 30°, mais l'inclinaison recommandée pour le montage du dispositif est de 15°. Pour vous aider à obtenir une inclinaison de 15°, assurez-vous que la partie arrière du châssis est à niveau, comme le montre l'illustration.



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

Coexistence

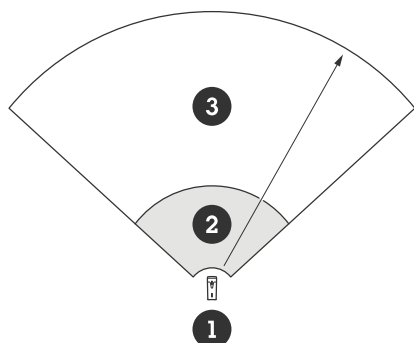
Si vous montez plus de huit radars Axis fonctionnant sur la bande de fréquences de 60 GHz l'un à côté de l'autre, ils risquent d'interférer l'un avec l'autre. Pour éviter les interférences, consultez .

Installer plusieurs radars

Installez plusieurs radars pour couvrir des zones telles que l'environnement d'un bâtiment ou la zone tampon en dehors d'une clôture.

Coexistence

Les ondes radio du radar 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.

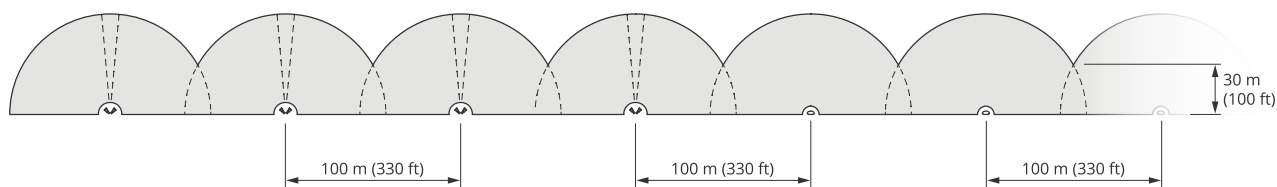


- 1 Radar
- 2 Zone de détection
- 3 Zone de coexistence

Ce radar fonctionne sur la bande de fréquence de 60 GHz. Jusqu'à huit radars 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 radars 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.

Les radars Axis qui utilisent différentes bandes de fréquence n'interfèrent pas l'un avec l'autre. Par exemple, vous pouvez combiner AXIS D2210-VE avec plusieurs AXIS D2110-VE Security Radar qui fonctionnent sur la bande de fréquences 24 GHz, sans interférences.



Quatre paires de radars AXIS D2210-VE et plusieurs AXIS D2110-VE Security Radars montés côte à côte.

Remarque

AXIS D2110-VE Security Radar nécessite une configuration supplémentaire lorsque plus de deux radars AXIS D2110-VE sont montés dans la même zone de coexistence. Pour en savoir plus, consultez le *manuel d'utilisation d'AXIS D2110-VE Security Radar*.

Environnement

Il existe également d'autres facteurs de conception à vérifier lors de l'installation de plusieurs radars sur un site, comme l'environnement, les objets ondulants, les mâts de drapeau et la végétation oscillante. Dans certains cas, vous devez filtrer les objets oscillants du flux radar pour éviter les fausses alarmes.

Profils radar

Le radar permet la surveillance de zones ou de routes. Deux profils sont optimisés pour chacun des scénarios :

- **Area monitoring profile** (Profil de surveillance d'espace) : Suivi des personnes, des véhicules et des objets inconnus qui se déplacent à des vitesses inférieures à 55 km/h (34 mph)
- **Road monitoring profile** (Profil de surveillance routière) : Suivi des véhicules principalement, qui se déplacent à des vitesses jusqu'à 200 km/h (125 mph)

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

Profil de surveillance de zone

Le profil de surveillance de zone est optimisé pour les objets qui se déplacent jusqu'à 55 km/h (34 mph). Ce profil vous permet de détecter si un objet est un être humain, un véhicule ou un élément inconnu. Une règle peut être définie pour déclencher une action lorsque l'un de ces objets est détecté. Pour suivre les véhicules qui se déplacent à des vitesses supérieures, utilisez le .

Zone de couverture

Le champ de détection horizontal du dispositif AXIS D2210-VE 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 radar 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.

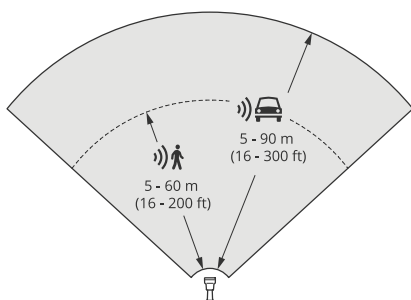
Plage de détection de zone

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 (1,24 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 1,70 m.
- 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)**.

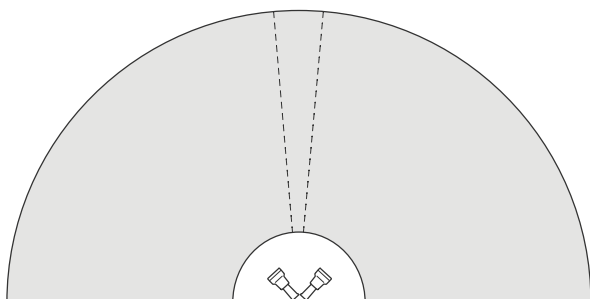
Hauteur de montage	Inclinaison de 0°	Inclinaison de 5°	Inclinaison de 10°	Inclinaison de 15°	Inclinaison de 20°	Inclinaison de 25°	Inclinaison de 30°
3,5 m (11 pi)	6,0–60+ m (19–196+ pi)	5,0–60+ m (16–196+ pi)	4,0–60+ m (13–196+ pi)	4,0–60 m (13–196 pi)	4,0–55 m (13– 180 pi)	4,0–40 m (13–131 pi)	4,0–30 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 %.

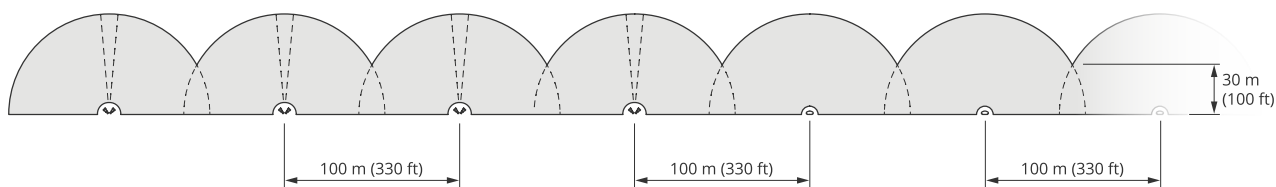
Exemples d'installation de zone

Pour créer une clôture virtuelle, par exemple le long ou autour d'un bâtiment, vous pouvez placer jusqu'à huit radars AXIS D2210-VE côte à côte. Lorsque vous placez deux radars AXIS D2210-VE l'un à côté de l'autre, vous obtenez un champ de vision de 180°.



Deux radars AXIS D2210-VE montés côte à côte pour une couverture à 180°.

Lorsque vous installez plusieurs paires de radars AXIS D2210-VE côte à côte, nous vous recommandons de les placer à 100 m (330 pi) les uns des autres.



Quatre paires de radars AXIS D2210-VE et plusieurs AXIS D2110-VE Security Radars montés avec un espacement de 100 m (330 pi). Les radars Axis qui utilisent différentes bandes de fréquence n'interfèrent pas l'un avec l'autre. Vous pouvez ainsi combiner le modèle AXIS D2210-VE, qui fonctionne sur la bande de fréquences de 60 GHz, avec AXIS D2110-VE Security Radar, qui fonctionne sur la bande de fréquences de 24 GHz dans la même zone de coexistence.

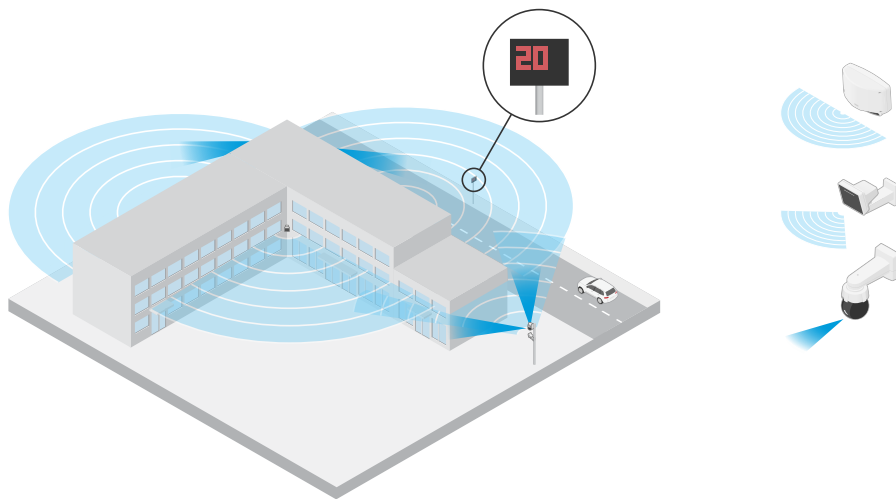
Pour en savoir plus sur la coexistence et les interférences, consultez .

Cas d'utilisation de la surveillance de zone

Couvrir la zone 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. Pour couvrir la zone autour du bâtiment, un ensemble de radars et de caméras PTZ doit être installé. L'entreprise utilise des AXIS D2110-VE Security Radars avec une couverture à 180° pour couvrir les longues parois du bâtiment et le radar AXIS D2210-VE Radar avec une couverture à 95° pour les parois et les coins plus courts. Elle configure les radars pour déclencher une alarme lorsque des personnes approchent du bâtiment après les heures de travail. Pour s'assurer d'obtenir une confirmation visuelle sur les intrus potentiels, deux caméras PTZ sont ajoutées. Les radars peuvent orienter les caméras PTZ via *AXIS Radar Autotracking for PTZ*.

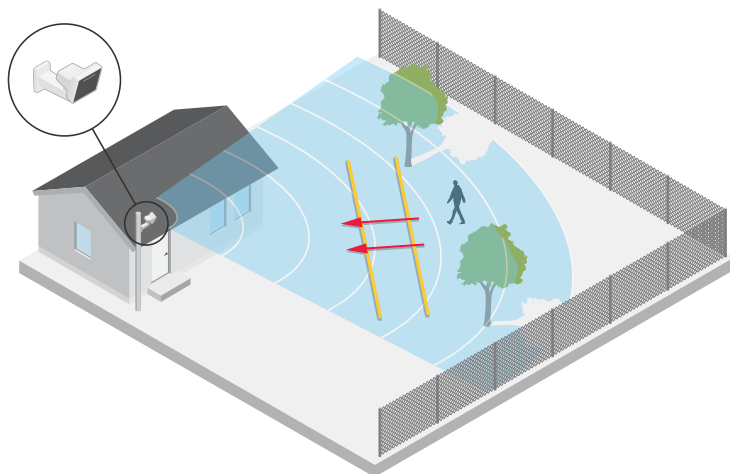
De plus, l'entreprise souhaite protéger les locaux pendant les heures de travail. Pour être sûrs que les véhicules qui traversent la route sur le côté du bâtiment ne dépassent pas les limites de vitesse, l'un des AXIS D2110-VE Security Radars est couplé à un panneau de vitesse de Microbus, en utilisant *AXIS Radar Integration for Microbus*.



Couvrir une scène complexe

Une entreprise qui conserve des équipements stratégiques à l'intérieur d'un bâtiment les protège avec une clôture pour éloigner les intrus. Pour éviter tout sabotage, une protection supplémentaire est nécessaire. Ils souhaitent qu'une alarme se déclenche lorsque des personnes s'approchent du bâtiment. Cependant, la scène comprend des arbres avec des branches ondulantes, une clôture métallique qui pourrait entraîner des reflets, et même des petits animaux qui se déplacent autour du site, ce qui est susceptible de déclencher de fausses alarmes.

Pour réduire le nombre de fausses alarmes, ils configurent un scénario dans l'interface Web du radar de sorte qu'un objet qui s'approche doit traverser deux lignes virtuelles avant le déclenchement d'une alarme. Ce réglage permet le déclenchement lorsque des objets se déplacent intentionnellement vers le bâtiment, tandis que les objets qui traversent l'une des lignes virtuelles par hasard sont filtrés.



Dans les sites dépourvus de clôtures, les deux lignes peuvent agir comme une clôture virtuelle. Pour en savoir plus sur l'ajout de deux lignes à un scénario dans l'interface Web du radar, consultez .

Profil de surveillance routière

Le profil de surveillance d'espace est optimisé pour suivre les véhicules qui se déplacent à une vitesse de 200 km/h (125 mph) sur les routes et autoroutes suburbaines. Pour suivre des personnes et des objets se déplaçant à des vitesses inférieures, utilisez le profil de surveillance de zone. Pour en savoir plus, consultez .

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 du radar et la vitesse du véhicule ont un impact sur la portée de détection. 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 .

Exemples d'installation routière

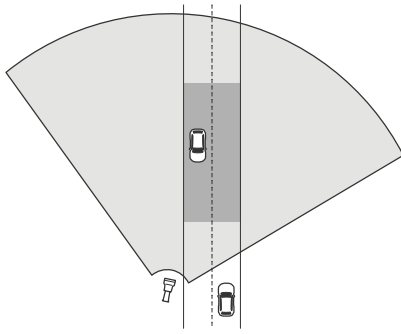
En cas de surveillance des routes et des autoroutes, assurez-vous de monter le radar à une hauteur suffisante afin d'éviter les angles morts (ombre radar) derrière les véhicules.

Remarque

La taille de l'ombre radar dépend de la hauteur de montage du radar, 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'un radar monté à une hauteur de 8 m (26 pi), l'ombre radar derrière le véhicule est de 50 m (164 pi). Toutefois, si le radar est monté 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

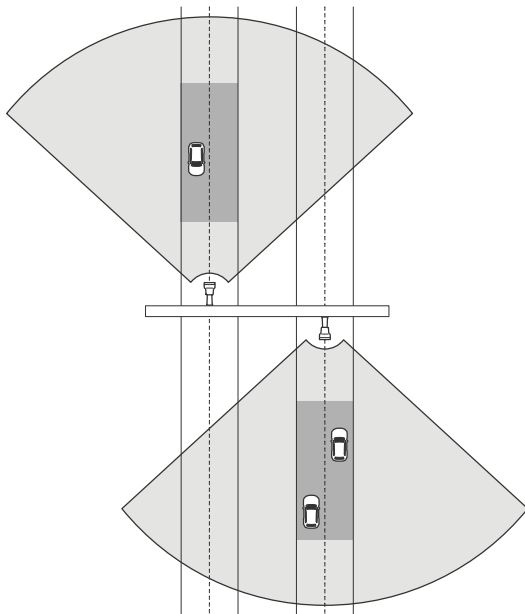
Pour surveiller les véhicules le long d'une route, vous pouvez monter le radar sur le côté de la route (sur un mât, par exemple). Dans ce type d'installation, nous recommandons un angle panoramique max. de 25°.



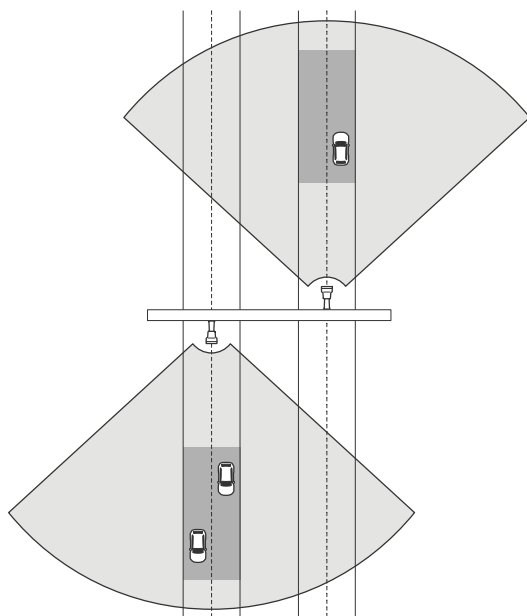
Pour mesurer précisément les vitesses élevées, positionnez le radar à une distance latérale de 10 m (32 pi) des véhicules. Pour plus d'informations sur la portée de détection et la précision de la vitesse, consultez .

Monté au centre

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



Le même type d'installation est possible si vous souhaitez surveiller des véhicules qui s'éloignent du radar, au lieu de rouler vers lui.



Pour mesurer précisément les vitesses élevées, positionnez le radar 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 .

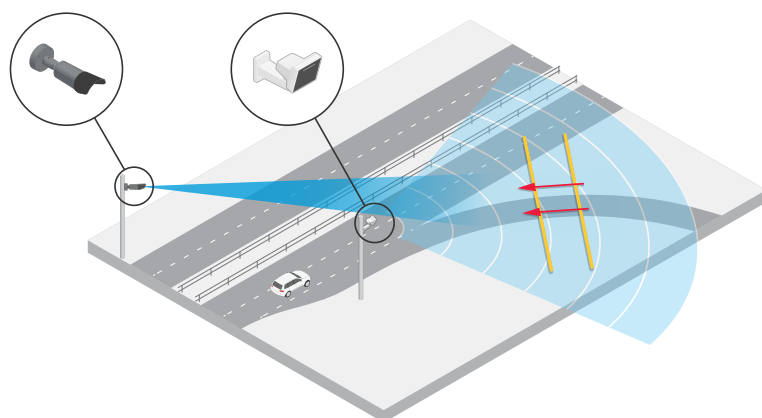
Cas d'utilisation de la surveillance routière

L'AXIS D2210-VE Radar et le profil de surveillance routière sont couramment utilisés pour suivre et mesurer la vitesse des véhicules. En outre, le radar associé à une caméra visuelle et l'application AXIS Speed Monitor permet de visualiser la vitesse des véhicules dans la vidéo en direct de la caméra ou d'enregistrer les pistes radar à des fins statistiques. Pour plus d'informations, consultez le *manuel d'utilisation d'AXIS Speed Monitor*.

Pour plus d'exemples de configuration du radar lors de l'utilisation du profil de surveillance routière, consultez les cas d'utilisation suivants :

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

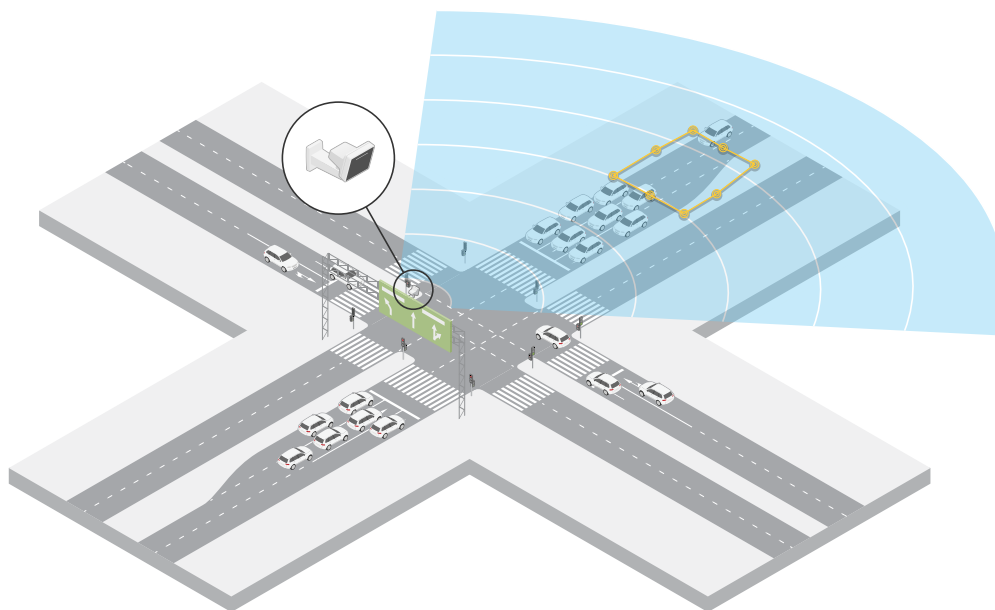
Pour détecter et identifier les véhicules roulant dans le mauvais sens sur une bretelle d'autoroute, les contrôles routiers utilisent des radars AXIS D2210-VE et des caméras cylindriques Axis. Ils montent le radar sur un poteau faisant face à la bretelle pour détecter les véhicules roulant dans le mauvais sens. Pour des détections fiables, ils configurent le radar de sorte que l'alarme se déclenche lorsque les véhicules traversent deux lignes. Dans ce scénario, ils positionnent les deux lignes sur la bretelle comme présenté dans l'illustration. Ils spécifient également le sens de la conduite et les vitesses qui déclenchent l'alarme. Lorsque le radar déclenche une alarme, la caméra cylindrique Axis peut fournir une identification visuelle du véhicule sur la bretelle.



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 un radar sur un portique au-dessus de l'intersection. Ils configurent un scénario dans l'interface Web du radar et le configurent de manière à déclencher une alarme lorsque des véhicules se

déplacent dans une zone. Le scénario est paramétré de façon à couvrir uniquement la partie de la route conduisant à l'intersection. 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).



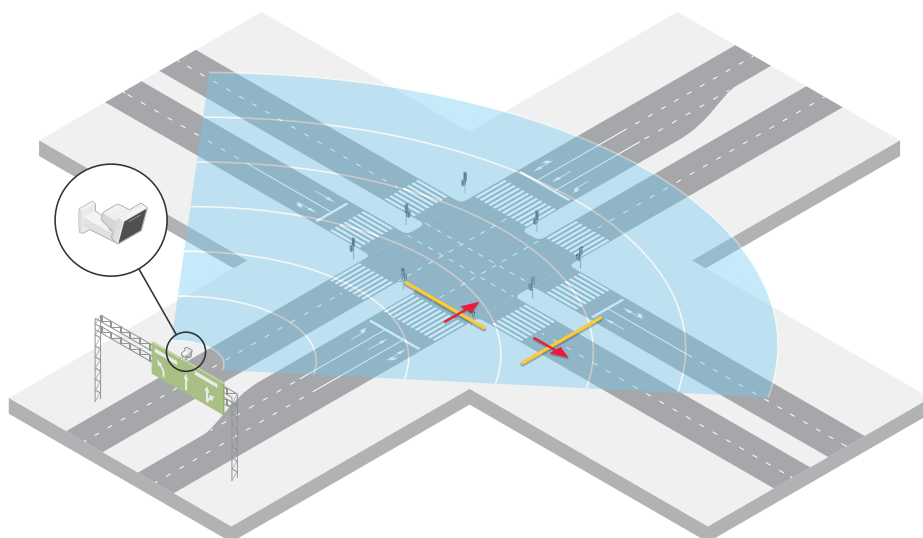
Surveillance du flux de trafic à une intersection : direction

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 un radar sur un portique au-dessus de la route conduisant à l'intersection. Ils définissent un scénario de franchissement de ligne dans l'interface Web du radar où les véhicules doivent traverser deux lignes pour déclencher une alarme. Dans le scénario configuré, la première des deux lignes est placée sur les voies conduisant à l'intersection, 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 va de 2 à 0 secondes.

Pour surveiller le flux de trafic dans toutes les directions, ils créent un scénario pour chaque direction.

Remarque

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

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.

Pour regarder cette vidéo, accédez à la version Web de ce document.

Interface Web des périphériques Axis

Configurer votre périphérique

Sélectionner un profil de radar

Dans l'interface web :

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

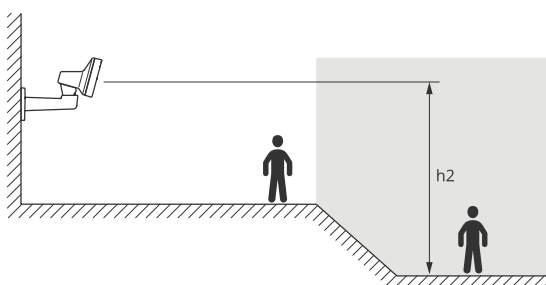
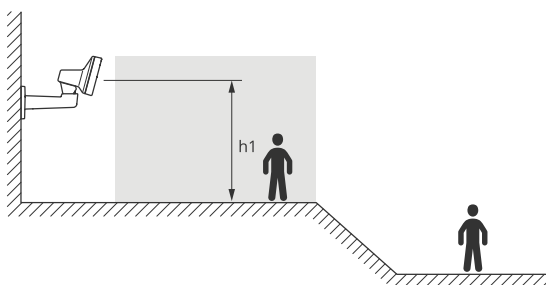
Régler la hauteur de montage

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

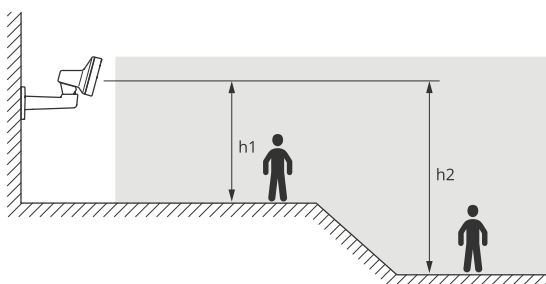
Mesurez le plus précisément possible la hauteur entre le sol et le radar. Pour les scènes comportant des surfaces inégales, ajoutez la valeur qui représente la hauteur moyenne de la scène.

Exemple:

La hauteur de montage (h_1 , h_2) varie en fonction de la zone d'intérêt.



Si la surface de la zone d'intérêt est irrégulière, ajoutez la hauteur moyenne (dans ce cas, $(h_1 + h_2) / 2$) lorsque vous configurez le radar.



Régler la hauteur de montage :

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

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)**.

Pour regarder cette vidéo, accédez à la version Web de ce document.

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.

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.

- 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. Le réglage de la sensibilité affecte toutes les zones.
 - **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 est disponible dans le profil de surveillance de la zone et permet de minimiser les fausses alarmes issues de la 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.

Régler l'image du radar

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

Afficher une incrustation d'image

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

1. Accédez à **Radar > 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 une incrustation de texte

Vous pouvez ajouter un champ de texte en tant qu'incrustation dans le flux de radar. Cette fonction est utile par exemple si vous souhaitez afficher la date, l'heure ou le nom d'une entreprise dans le flux vidéo.

1. Accédez à **Radar > Incrustations**.

2. Sélectionnez **Text (Texte)** et cliquez sur .
3. Saisissez le texte à afficher dans le flux vidéo.
4. Sélectionnez une position. Vous pouvez également faire glisser le champ de texte dans la vidéo en direct pour modifier la position.

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.

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 **Radar > Stream (Flux)**.
2. Cliquez sur  dans la vidéo en direct.
3. Sélectionnez **Video format (Format vidéo) H.264**.
4. Accédez à **Radar > Stream (Flux) > General (Général)** et augmentez la valeur de **Compression**.

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**.

Enregistrer et regarder la vidéo

Record video directly from the radar (Sauvegarder une vidéo directement depuis le radar)

1. Accédez à Radar > Stream (Flux).
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.

Définir des règles pour les événements

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

Déclencher une action

1. Accédez à System > Events (Système > Événements) et ajoutez une règle. La règle permet de définir quand le périphérique effectue certaines actions. Vous pouvez définir des règles comme étant programmées, récurrentes ou déclenchées manuellement.
2. Saisissez un **Name (Nom)**.
3. Sélectionnez la **Condition** qui doit être remplie pour déclencher l'action. Si plusieurs conditions sont définies pour la règle, toutes les conditions doivent être remplies pour déclencher l'action.
4. Sélectionnez quelle **Action** le périphérique doit exécuter lorsque les conditions sont satisfaites.

Remarque

Si vous modifiez une règle active, celle-ci doit être réactivée pour que les modifications prennent effet.

Remarque

Si vous modifiez la définition d'un profil de flux utilisé dans une règle, vous devez redémarrer toutes les règles qui utilisent ce profil de flux.

Sauvegarder une vidéo depuis une caméra lorsqu'un mouvement est détecté

Cet exemple explique comment configurer le radar et une caméra pour que la caméra commence l'enregistrement sur la carte SD cinq secondes avant que le radar détecte un mouvement et l'arrête une minute après.

Connectez les périphériques :

1. Connectez un câble depuis une sortie d'E/S du radar vers une entrée d'E/S de la caméra.

Configurez le port d'E/S du radar :

2. Accédez à System (Système) > Accessories (Accessoires) > I/O ports (Ports d'E/S) et configurez le port d'E/S en tant que sortie et sélectionnez l'état normal.

Créez une règle dans le radar :

3. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
4. Saisissez le nom de la règle.
5. Dans la liste des conditions, sélectionnez un scénario sous **Radar motion (Mouvement du radar)**. Pour configurer un scénario, consultez .
6. 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 connecté à la caméra.
7. Cliquez sur **Save (Enregistrer)**.

Configurez le port d'E/S de la caméra :

8. Accédez à **System (Système) > Accessories (Accessoires) > I/O ports (Ports d'E/S)** et configurez le port d'E/S en tant qu'entrée et sélectionnez l'état normal.

Créez une règle dans la caméra :

9. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
10. Saisissez le nom de la règle.
11. Dans la liste des conditions, sélectionnez **Digital input is active (L'entrée numérique est active)** puis sélectionnez le port qui doit déclencher la règle.
12. Dans la liste des actions, sélectionnez **Record video (Enregistrer la vidéo)**.
13. Dans la liste des options de stockage, sélectionnez **SD card (Carte SD)**.
14. Sélectionnez un profil de flux existant ou créez-en un.
15. Réglez le pré-tampon sur 5 secondes.
16. Réglez la durée post-tampon sur 1 minute.
17. Cliquez sur **Save (Enregistrer)**.

Sauvegarder la vidéo d'une caméra lorsqu'un véhicule roule dans le mauvais sens

Cet exemple explique comment configurer le radar et une caméra de sorte que la caméra démarre l'enregistrement sur une carte SD lorsque le radar détecte un véhicule qui roule dans le mauvais sens.

Avant de commencer

- Créez un scénario dans l'interface Web du radar qui se déclenche lors d'un franchissement de ligne et quand des véhicules franchissent deux lignes.
Pour en savoir plus, voir .
 - Veillez à positionner les deux lignes sur la voie de circulation à l'endroit où vous souhaitez détecter les véhicules roulant dans le mauvais sens. Utilisez une carte de référence, de type photo aérienne, pour voir plus facilement le déplacement des objets.
Pour en savoir plus, voir .
1. Créer deux destinataires dans le radar.
 - 1.1. Dans l'interface du périphérique du radar, accédez à **System > Events > Recipients (Système > Événements > Destinataires)** et ajoutez le premier destinataire.
 - 1.2. Ajoutez les informations suivantes :
 - **Nom** : Activer le port virtuel
 - **Type** : HTTP
 - **URL** : `http://<adresseIP>/axis-cgi/virtualinput/activate.cgi`
Remplacez <adresseIP> par l'adresse de la caméra dont vous souhaitez démarrer l'enregistrement.
 - Le nom d'utilisateur et le mot de passe de la caméra.
 - 1.1. Cliquez sur **Test (Tester)** pour vous assurer que toutes les données sont valides.
 - 1.2. Cliquez sur **Save (Enregistrer)**.

- 1.3. Ajouter un deuxième destinataire avec les informations suivantes :
 - Nom : Désactiver le port virtuel
 - Type : HTTP
 - URL : http://<adressesIP>/axis-cgi/virtualinput/deactivate.cgi
Remplacez <adressesIP> par l'adresse de la caméra.
 - Le nom d'utilisateur et le mot de passe de la caméra.
- 1.1. Cliquez sur **Test (Tester)** pour vous assurer que toutes les données sont valides.
- 1.2. Cliquez sur **Save (Enregistrer)**.
2. Créer deux règles dans le radar.
 - 2.1. Dans l'interface du périphérique du radar, accédez à **System > Events > Rules (Système > Événements > Règles)** et ajoutez la première règle.
 - 2.2. Ajoutez les informations suivantes :
 - Nom : Activer l'IO1 virtuel
 - Condition (Condition) : sélectionnez le scénario créé dans **Mouvement du radar**.
 - Action : **Notifications > Send notification through HTTP (Notifications > Envoyer une notification via HTTP)**
 - Destinataire : **Activer le port virtuel**
 - Query string suffix (Suffixe de la chaîne de requête) : **schemaversion=1&port=1**
 - 2.1. Cliquez sur **Save (Enregistrer)**.
 - 2.2. Ajoutez une autre règle avec les informations suivantes :
 - Nom : Désactiver l'IO1 virtuel
 - Condition (Condition) : sélectionnez le scénario créé dans **Mouvement du radar**.
 - Sélectionnez **Invert this condition (Inverser cette condition)**.
 - Action : **Notifications > Send notification through HTTP (Notifications > Envoyer une notification via HTTP)**
 - Destinataire : **Désactiver le port virtuel**
 - Query string suffix (Suffixe de la chaîne de requête) : **schemaversion=1&port=1**
 - 2.1. Cliquez sur **Save (Enregistrer)**.
3. Créez une règle dans la caméra.
 - 3.1. Dans l'interface de la caméra, accédez à **System > Events > Rules (Système > Événements > Règles)** et ajoutez une règle.
 - 3.2. Ajoutez les informations suivantes :
 - Nom : déclencher l'entrée virtuelle 1
 - Condition : **I/O > Digital Virtual input is active (E/S > L'entrée virtuelle est active)**
 - Port : 1
 - Action : **Recordings > Record video while the rule is active (Enregistrements > Sauvegarder la vidéo tant que la règle est active)**
 - Storage options (Options de stockage) : **SD_DISK**
 - Sélectionnez **Caméra** et un **Profil de flux**.
 - 3.1. Cliquez sur **Save (Enregistrer)**.

Activer un balayage rouge sur le radar

La bande de LED dynamique sur la face avant du radar permet d'indiquer que la zone est surveillée.

Cet exemple explique comment activer un éclairage de balayage rouge et comment définir un calendrier de sorte qu'il ne fonctionne qu'après les heures de travail en semaine.

Créer un programme :

1. Accédez à **System > Events > Schedules (Système > Événements > Calendriers)** et ajoutez un calendrier.
2. Saisissez le nom du calendrier.
3. Sous **Type**, sélectionnez **Calendrier**.
4. Sous **Récurrent**, sélectionnez **Quotidien**.
5. Définissez l'heure de début à 18:00.
6. Définissez l'heure de fin à 6:00.
7. Sous **Jours**, sélectionnez Lundi au vendredi.
8. Cliquez sur **Save (Enregistrer)**.

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 **Programmés et récurrents**, sélectionnez **Planifier**.
4. Sélectionnez le calendrier créé dans le menu déroulant **Schedule (Calendrier)**.
5. Dans la liste des actions, sous **Radar**, sélectionnez **Dynamic LED strip (Bande de LED dynamique)**.
6. Sélectionnez le modèle **Sweeping red (Balayage rouge)** dans le menu déroulant **Pattern (Modèle)**.
7. Réglez la durée sur 12 heures.
8. 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)**.

Allumer un éclairage lorsqu'un mouvement est détecté

Allumer un éclairage lorsqu'un intrus pénètre dans la zone de détection peut avoir un effet dissuasif et améliorer également la qualité d'image d'une caméra visuelle enregistrant l'intrusion.

Cet exemple explique comment configurer le radar et un projecteur pour que le projecteur s'allume lorsque le radar détecte un mouvement et s'éteigne après une minute.

Connectez les périphériques :

1. Branchez l'un des câbles du projecteur à l'alimentation électrique via le port relais du radar. Branchez l'autre câble directement entre l'alimentation électrique et le projecteur.

Configurez le port relais du radar :

2. Allez à **System (Système) > Accessories (Accessoires) > I/O ports (Ports d'E/S)** et sélectionnez **Open circuit (Circuit ouvert)** comme état normal du port relais.

Créez une règle dans le radar :

3. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
4. Saisissez le nom de la règle.
5. Dans la liste des conditions, sélectionnez un scénario sous **Radar motion (Mouvement du radar)**. Pour configurer un scénario, consultez .
6. Dans la liste des actions, sélectionnez **Toggle I/O once (Basculer l'E/S une fois)** puis sélectionnez le port relais.
7. Sélectionnez **Active (Actif)**.
8. Définissez la **Duration (Durée)**.
9. 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, les radars 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 le radar 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 radar ou installez-le sur une caméra que vous connectez à votre radar.
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*.

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

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.

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.

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.

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.

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.

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.

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.

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 indique 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.
- **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 indique 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. 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.
- **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.
 - **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.

- **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.

Bande de LED dynamique

Modèles de bande de LED dynamiques

Cette page permet de tester les modèles de la bande de LED dynamique.

Modèle : sélectionnez le modèle à tester.

Durée : indiquez la durée du test.

Test : cliquez pour démarrer le modèle à tester.

Arrêter : cliquez pour arrêter le test. Si vous quittez la page alors qu'un modèle est actif, il s'arrête automatiquement.

Pour activer un modèle à des fins d'indication ou de dissuasion, accédez à **System > Events (Système > Événements)** et créez une règle. Pour obtenir un exemple, consultez .

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.

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.



Allow root-privileged apps (Autoriser les applications privilégiées à la racine) : Activez cette option pour autoriser les applications dotées de privilèges root à accéder sans restriction au périphérique.



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.

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.

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`

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 dérouterments :** Activez cette option pour activer les rapports de dérouterment. Le périphérique utilise les dérouterments 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 dérouterments pour SNMP v1 et v2c. Les dérouterments sont automatiquement désactivés si vous passez à SNMP v3 ou si vous désactivez SNMP. Si vous utilisez SNMP v3, vous pouvez configurer les dérouterments via l'application de gestion SNMP v3.
 - **Adresse de dérouterment :** Entrez l'adresse IP ou le nom d'hôte du serveur de gestion.
 - **Communauté de dérouterment :** saisissez la communauté à utiliser lors de l'envoi d'un message de dérouterment au système de gestion.
 - **Dérouterments :**
 - **Démarrage à froid :** Envoie un message de dérouterment au démarrage du périphérique.
 - **Démarrage à chaud :** Envoie un message de dérouterment lorsque vous modifiez un paramètre SNMP.
 - **Lien vers le haut :** Envoie un message d'interruption lorsqu'un lien change du bas vers le haut.
 - **Échec de l'authentification :** Envoie un message de dérouterment en cas d'échec d'une tentative d'authentification.

Remarque

Tous les dérouterments Axis Video MIB sont activés lorsque vous activez les dérouterments 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 dérouterments v1 et v2c SNMP non cryptés. Si vous utilisez SNMP v3, vous pouvez configurer les dérouterments 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.

- **More (Plus)** : Afficher davantage de champs à remplir ou à sélectionner.
- **Keystore sécurisé** : Sélectionnez cette option pour utiliser **Secure element** ou **Trusted Platform Module 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) :

- **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.

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)**.
- **Viewer (Observateur)** : n'a pas le droit de modifier les paramètres.



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.

- **Restreindre l'accès root** : Activez pour limiter les fonctionnalités nécessitant l'accès root.
- **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 su MQTT, consultez *AXIS OS Portal*.

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, tapez `DOMAINE\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 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 compatible Axis comme s'il faisait partie du périphérique principal.

Appairage audio vous permet d'effectuer un appairage avec un haut-parleur ou un microphone 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.

Sélectionnez 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 la 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.

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).

Valider votre installation

Valider l'installation du radar

Remarque

Ce test vous aide à valider votre installation dans les conditions actuelles. Les performances quotidiennes de votre installation peuvent être affectées par des changements dans la scène.

Le radar est prêt à être utilisé dès son installation. Cependant, nous recommandons d'effectuer une validation avant de commencer à l'utiliser. Ceci peut augmenter la précision du radar en vous aidant à identifier tout problème avec l'installation ou à gérer les objets (tels que les arbres et les surfaces réfléchissantes) dans la scène.

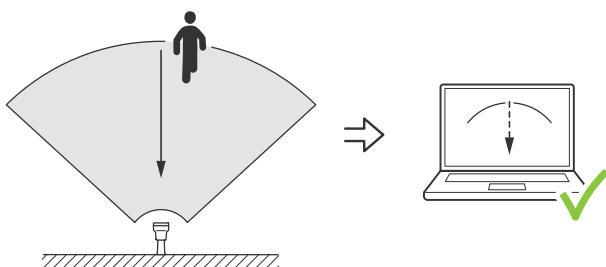
Commencez par avant de tenter la validation. Ensuite, procédez comme suit :

Check that there are no false detections (Vérifier l'absence de détections erronées)

1. Vérifiez que la zone de détection est exempte d'activités humaines.
2. Attendez quelques minutes pour vérifier que le radar ne détecte aucun objet statique dans la zone de détection.
3. En l'absence de détections indésirables, passez à l'étape 4.
4. En cas de détections indésirables, apprenez à filtrer certains types de mouvement ou d'objet, modifiez la couverture ou ajustez la sensibilité de la détection dans .

Vérifiez que le symbole et le sens du déplacement sont corrects lorsque le radar est approché de face

1. Accédez à l'interface Web du radar et enregistrez la session. Pour obtenir de l'aide pour ce faire, allez à .
2. Commencez jusqu'à 60 m (196 pi) en face du radar et marchez directement vers lui.
3. Vérifiez la session dans l'interface Web du radar. Le symbole d'une classification humaine doit apparaître lorsque vous êtes détecté.
4. Vérifiez que l'interface Web du radar indique le sens du déplacement correct.



Vérifiez que le symbole et le sens du déplacement sont corrects lorsque le radar est approché sur le côté

1. Accédez à l'interface Web du radar et enregistrez la session. Pour obtenir de l'aide pour ce faire, allez à .
2. Commencez à 30 m (98 pi) du radar et franchissez la zone de couverture radar.
3. Vérifiez que l'interface Web du radar affiche le symbole d'une classification humaine.
4. Vérifiez que l'interface Web du radar indique le sens du déplacement correct.

Créez un tableau similaire à celui ci-dessous pour vous aider à enregistrer les données de votre validation.

Test	Réussite/Échec	Commentaire
1. Vérifier l'absence de détections indésirables lorsque la zone est vide		
2a. Vérifier que l'objet est détecté avec le symbole correct		

(« Humain ») lorsque le radar est approché de face		
2b. Vérifier que le sens du déplacement est correct lorsque le radar est approché de face		
3a. Vérifier que l'objet est détecté avec le symbole correct (« Humain ») lorsque le radar est approché sur le côté		
3b. Vérifier que le sens du déplacement est correct lorsque le radar est approché sur le côté		

Terminer la validation

Une fois la première partie de la validation réussie, effectuez les tests suivants pour terminer la validation.

1. Vérifiez que le radar est configuré et que vous avez suivi les instructions.
2. Pour pousser davantage la validation, ajoutez et calibrez une carte de référence.
3. Définissez le scénario de radar qui doit se déclencher lors de la détection d'un objet approprié. Par défaut, **secondes jusqu'au déclenchement** est défini sur 2 secondes, mais vous pouvez modifier cette option dans l'interface Web si nécessaire.
4. Définissez le radar pour qu'il enregistre les données lors de la détection d'un objet approprié. Pour des instructions, voir .
5. Définissez **trial lifetime (Durée du tracé)** sur 1 heure pour dépasser largement le temps nécessaire pour vous lever de votre siège, faire le tour de la zone de surveillance et revenir à votre point de départ. **trail lifetime (Durée du tracé)** conserve le suivi dans la vidéo en direct du radar pendant le temps défini et, une fois la validation terminée, l'option peut être désactivée.
6. Marchez le long de la limite de la zone de couverture du radar et vérifiez que le chemin sur le système correspond bien à votre itinéraire.
7. Si vous n'êtes pas satisfait des résultats de la validation, calibrez de nouveau la carte de référence et répétez la validation.

En savoir plus

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

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

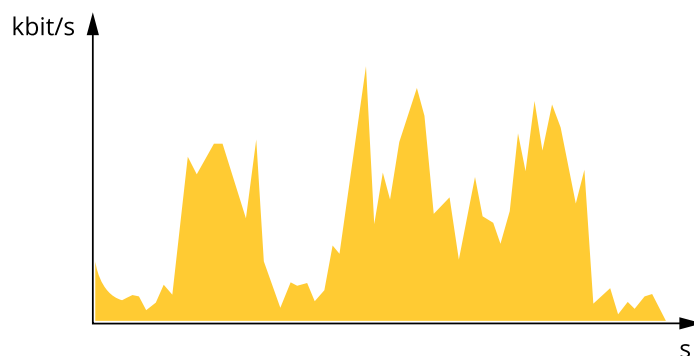
- H.265 est une technologie sous licence. Le produit Axis est fourni avec une licence client permettant d'afficher les flux de données vidéo H.265. Il est interdit d'installer d'autres copies du client sans licence. Pour acheter d'autres licences, contactez votre revendeur Axis.
- La plupart des navigateurs 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.

Commande du débit binaire

Le contrôle du débit binaire permet de gérer la consommation de bande passante du flux vidéo.

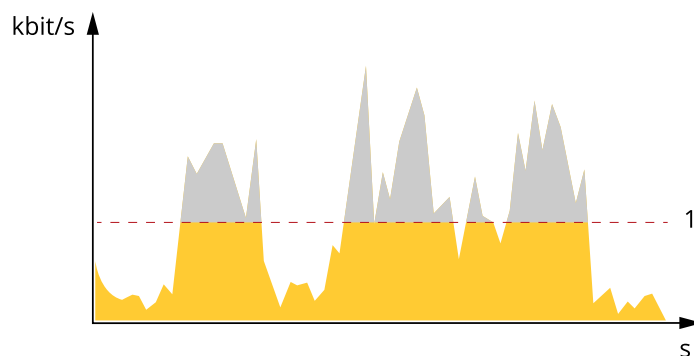
Débit binaire variable (VBR)

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 maximum 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.

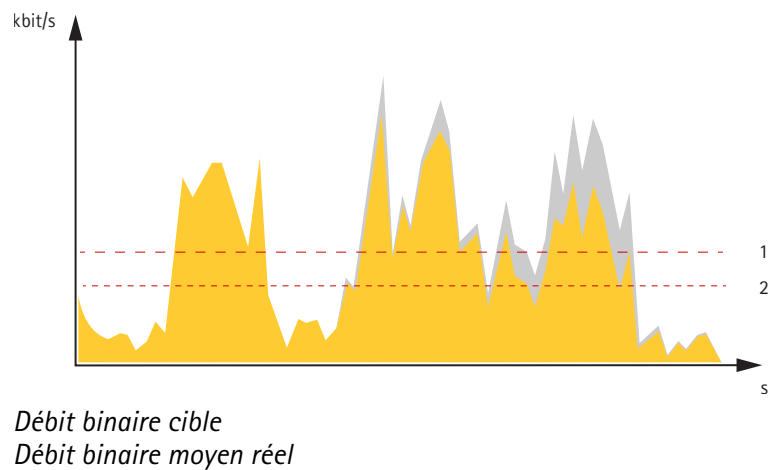


1 Débit binaire cible

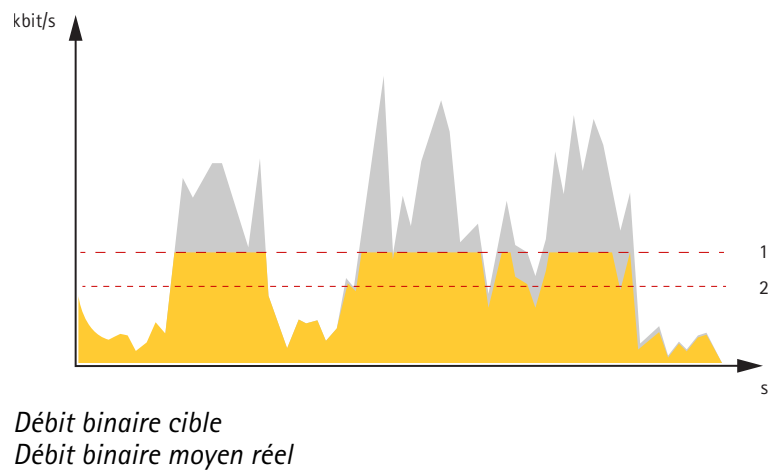
Débit binaire moyen (ABR)

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.

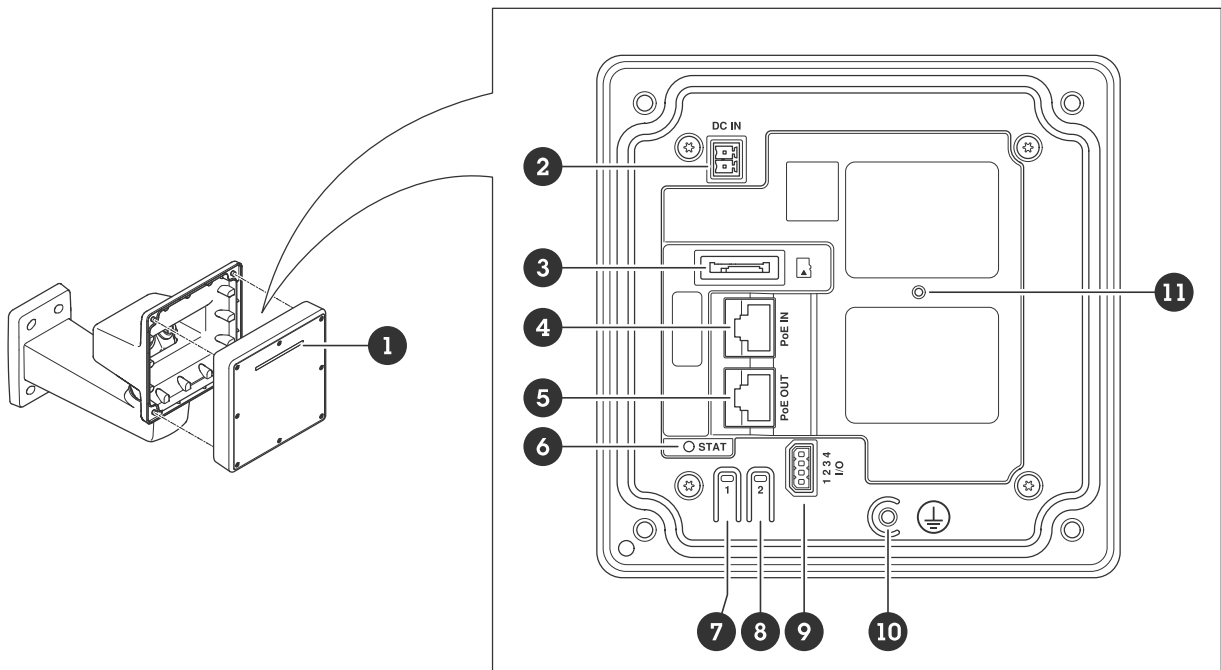


Incrustations

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.

Caractéristiques techniques

Gamme de produits



- 1 Bande de LED dynamique
- 2 Connecteur d'alimentation (CC)
- 3 Emplacement pour carte microSD
- 4 Connecteur réseau (PoE in)
- 5 Connecteur réseau (sortie PoE)
- 6 LED de statut
- 7 Bouton de commande
- 8 Bouton Action
- 9 Connecteur E/S
- 10 Vis de mise à la terre
- 11 Bouton de réinitialisation

Voyants DEL

Remarque

- Le voyant d'état peut clignoter lorsqu'un événement est actif.

DEL d'état	Indication
Vert	Vert et fixe en cas de fonctionnement normal.
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.
Rouge	Échec de la mise à niveau du logiciel du périphérique.

Modèles de bande de LED dynamiques
Rouge
Bleu
Vert

Jaune
Blanc
Rouge balayage
Bleu balayage
Vert balayage
Rouge, bleu, blanc clignotant

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 effectuer la connexion, maintenez le bouton enfoncé pendant environ 3 secondes jusqu'à ce que la DEL d'état clignote en vert.

Connecteurs

Connecteur réseau (PoE in)

Connecteur Ethernet RJ45 avec Power over Ethernet IEEE 802.3bt, Type 3 Classe 6.

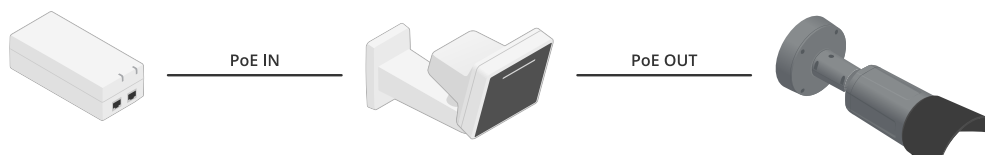
Remarque

Power over Ethernet IEEE 802.3bt, Type 3 Classe 6 est requis pour la sortie PoE. Si un deuxième périphérique n'est pas sous tension, Power over Ethernet IEEE 802.3at, Type 2 Classe 4 est suffisant.

Connecteur réseau (sortie PoE)

Connecteur Ethernet RJ45 avec une alimentation Power over Ethernet IEEE 802.3at, Type 2 Classe 4, 30 W max.

Utilisez ce connecteur pour alimenter un autre périphérique PoE, par exemple une caméra, un haut-parleur à pavillon ou un deuxième radar Axis.



Remarque

La sortie PoE est activée lorsque le radar est alimenté par un injecteur de 60 W (Power over Ethernet IEEE 802.3bt, type 3).

Remarque

Si le radar est alimenté par un injecteur de 30 W ou une alimentation CC, la sortie PoE est désactivée.

Remarque

La longueur maximale du câble Ethernet est de 100 m au total en combinant la sortie PoE et l'entrée PoE. Vous pouvez l'augmenter avec un extenseur PoE.

Remarque

Si le dispositif PoE connecté nécessite plus de 30 W, vous pouvez ajouter un injecteur de 60 W entre le port de sortie PoE sur le radar et le dispositif. L'injecteur alimentera le dispositif tandis que le radar fournira la connexion Ethernet.

Connecteur E/S

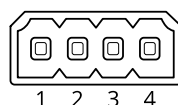
Utilisez le connecteur d'E/S avec des périphériques externes associés à des applications telles que le déclenchement d'événements et les notifications d'alarme. En plus du point de référence 0 V CC et de l'alimentation (sortie CC), le connecteur d'E/S fournit une interface aux éléments suivants :

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.

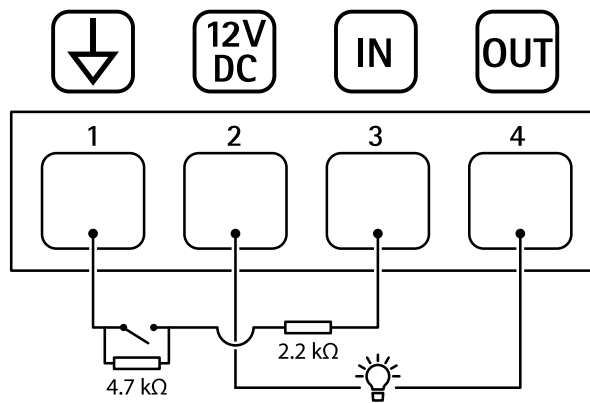
Sortie numérique – Permet de connecter des dispositifs externes, comme des relais ou des voyants. Les périphériques connectés peuvent être activés par l'interface de programmation VAPIX®, via un événement ou à partir de l'interface web du périphérique.

Bloc terminal à 4 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 = 25 mA
Entrée numérique	3	Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à max. 30 V CC
Sortie numérique	4	Connexion interne à la broche 1 (terre 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

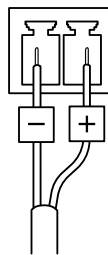
Exemple:



- 1 Masse CC
- 2 Sortie CC 12 V, maxi. 25 mA
- 3 Entrée supervisée
- 4 Sortie numérique

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.



Nettoyer votre dispositif

Vous pouvez nettoyer votre dispositif avec de l'eau tiède.

AVIS

- Les détergents peuvent endommager le dispositif. N'utilisez pas de produits chimiques tels que le nettoyant pour vitres ou l'acétone pour nettoyer votre dispositif.
 - Évitez de nettoyer en cas de lumière directe du soleil ou à des températures élevées, car cela peut entraîner des taches.
1. Utilisez une bombe d'air comprimé pour éliminer la poussière et la saleté non incrustée du dispositif.
 2. Si nécessaire, nettoyez le dispositif à l'aide d'un tissu microfibre doux humidifié avec de l'eau tiède.
 3. Pour éviter les taches, séchez le dispositif avec un chiffon propre et non abrasif.

Recherche de panne

Réinitialiser les paramètres par défaut

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).

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 la fenêtre de commande/DOS, saisissez <code>ping</code> et l'adresse IP du périphérique) : • Si vous recevez : Répondre à partir de <adresse IP>: bytes (octets)=32; time (temps)=10... , cela peut signifier que l'adresse IP est 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 : Request timed out, 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 Edge : application gratuite, idéale pour les petits systèmes ayant des besoins de surveillance de base.
- 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.
---	---

Facteurs ayant un impact sur la performance

Lors de la configuration de votre système, il est important de tenir compte du fait que certains réglages et situations affectent les besoins en bande passante nécessaire (le débit binaire).

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.

Contactez l'assistance

Si vous avez besoin d'aide supplémentaire, accédez à axis.com/support.

T10193646_fr

2025-01 (M13.2)

© 2023 – 2025 Axis Communications AB