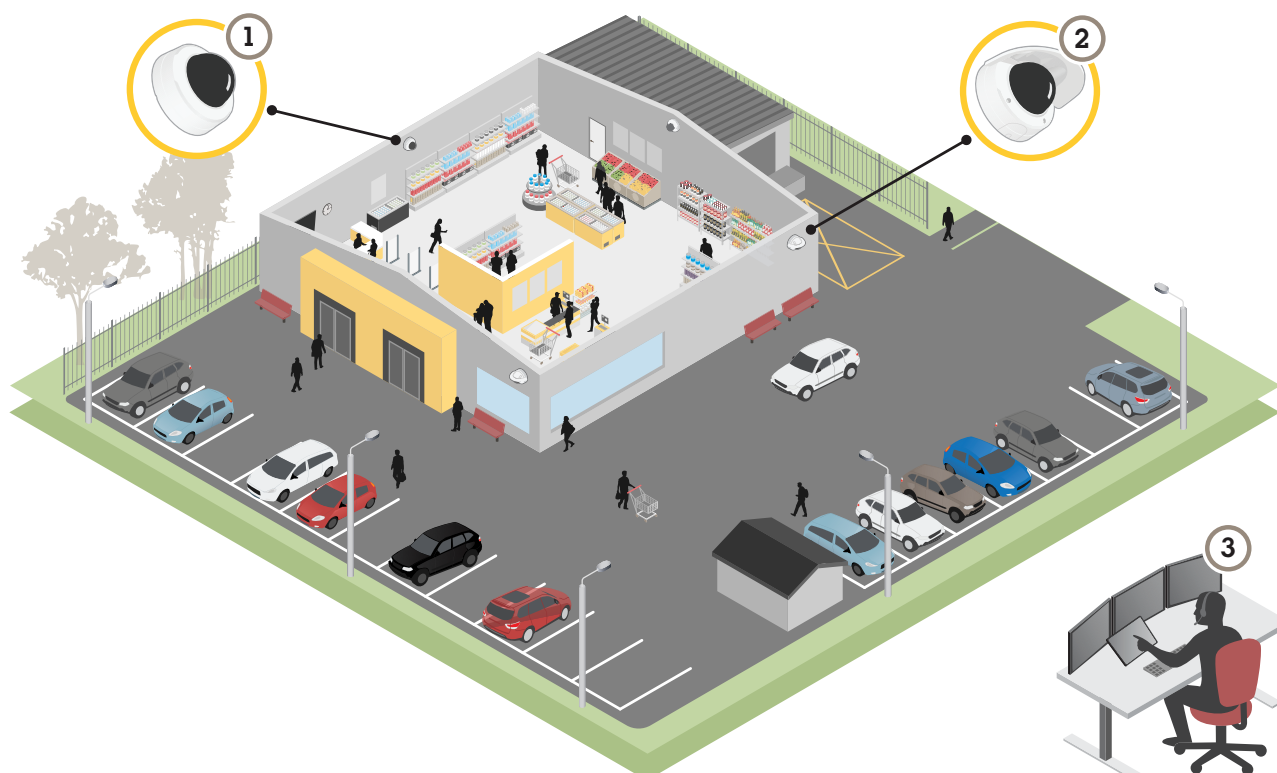


AXIS P3285-LVE Kit License Plate Verifier

Vue d'ensemble de la solution



- 1 *Caméra à dôme fixe pour l'intérieur*
- 2 *Caméra à dôme fixe pour l'extérieur*
- 3 *Centre de surveillance*

Installation

Mode aperçu

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



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

Cette vidéo démontre comment utiliser le mode aperçu.

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

✓ : Recommandé

* : Pris en charge avec limitations

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, veuillez utiliser 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. *Créer un compte administrateur*, on page 4.

Pour obtenir une description de toutes les fonctionnalités et de tous les paramètres de l'interface web des périphériques équipés d'AXIS OS, veuillez consulter l'*aide sur l'interface web d'AXIS OS*.

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. *Mots de passe sécurisés*, on page 5.
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. *Réinitialiser les paramètres par défaut*, on page 59.

Mots de passe sécurisés

Important

Utilisez HTTPS (activé par défaut) pour définir votre mot de passe ou d'autres configurations sensibles sur le réseau. HTTPS permet des connexions réseau sécurisées et cryptées, protégeant ainsi les données sensibles, telles que les mots 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. *Réinitialiser les paramètres par défaut, on page 59*.
Après la réinitialisation, le démarrage sécurisé garantit l'état du périphérique.
2. Configurez et installez le périphérique.

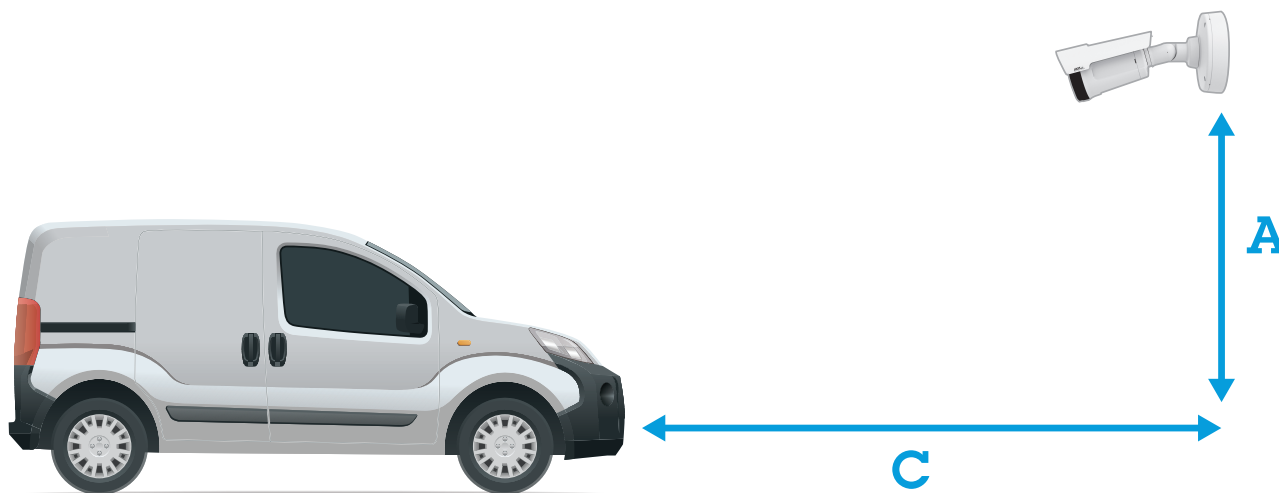
Configuration de base

Ces instructions de configuration sont valides dans tous les scénarios :

1. *Recommandations de montage de la caméra, on page 6*
2. *Assistant de configuration, on page 8*
3. *Régler le domaine d'intérêt, on page 10*
4. *Sélectionner une région, on page 11*
5. *Configurer le stockage d'événements, on page 11*

Recommandations de montage de la caméra

- Lorsque vous sélectionnez l'emplacement de montage, rappelez-vous que la lumière directe du soleil peut déformer l'image, par exemple, lors du coucher et du lever du soleil.
- La hauteur de montage d'une caméra dans un scénario de **Contrôle d'accès** doit être la moitié de la distance entre le véhicule et la caméra.
- La hauteur de montage de la caméra dans un scénario de **Flux libre** (reconnaissance de plaque d'immatriculation en cas de trafic lent) doit être inférieure à la moitié de la distance entre le véhicule et la caméra.



Distance de capture du **contrôle d'accès** : 2–7 m (6,6–23 pi). Cet exemple est basé sur l'AXIS P3265–LVE–3 License Plate Verifier kit.

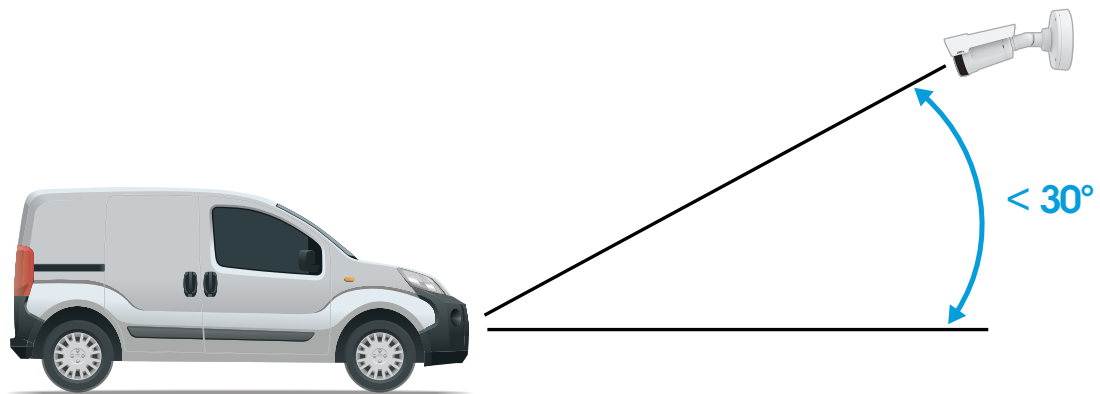
Distance de capture : (C)	Hauteur de montage (A)
2,0 m (6,6 pi)	1,0 m (3,3 pi)
3,0 m (9,8 pi)	1,5 m (4,9 pi)
4,0 m (13 pi)	2,0 m (6,6 pi)
5,0 m (16 pi)	2,5 m (8,2 pi)
7,0 m (23 pi)	3,5 m (11 pi)

Distance de capture en **flux libre** : 7–20 m (23–65 pi). Cet exemple est basé sur l'AXIS P1465–LE–3 License Plate Verifier kit.

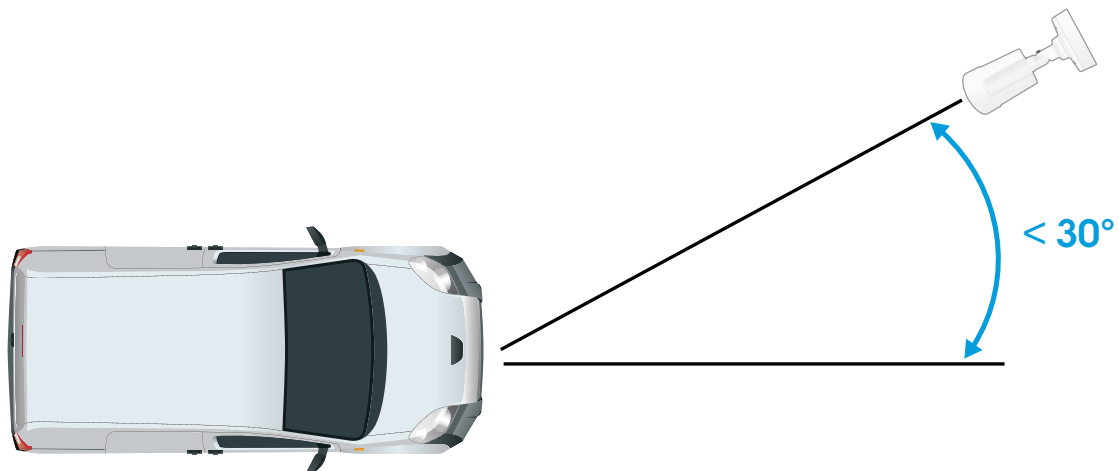
Distance de capture (C)	Hauteur de montage (A)
7,0 m (23 pi)	3,0 m (9,8 pi)

10,0 m (33 pi)	4,0 m (13 pi)
15,0 m (49 pi)	6,0 m (19,5 pi)
20,0 m (65 pi)	10,0 m (33 pi)

- L'angle de montage de la caméra doit être inférieur à 30° dans toute direction.

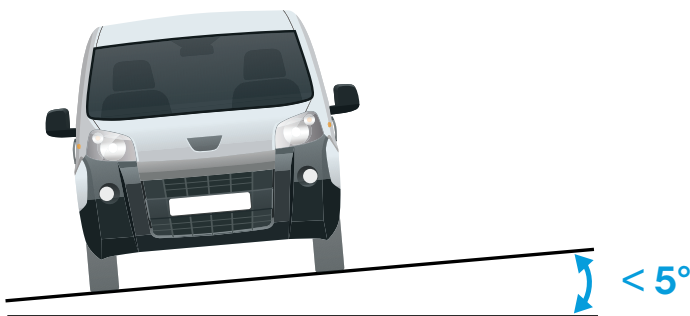


Angle de montage sur le côté.



Angle de montage montré ci-dessus.

- L'angle d'inclinaison horizontale de l'image de la plaque d'immatriculation doit être inférieur à 5°. Si l'image est inclinée de plus de 5°, nous vous recommandons d'ajuster la caméra, afin que la plaque d'immatriculation apparaisse horizontalement dans le flux de données en direct.



Angle de roulis.

Assistant de configuration

Lors de la première utilisation de l'application, configurez **Free flow (Flux libre)** ou **Access control (Contrôle d'accès)** en utilisant l'assistant de configuration. Si vous souhaitez changer quelque chose ultérieurement, veuillez aller à **Settings (Paramètres) > Maintenance** et sous **Setup assistant (Assistant de configuration)**, veuillez appuyer sur **Start (Démarrer)**.

Flux libre

Dans Flux libre, l'application peut détecter et lire les plaques d'immatriculation dans le trafic à basse vitesse sur les grandes voies d'accès, les centres-villes et dans des zones fermées, comme les campus, ports ou aéroports. Cela permet la recherche judiciaire basée sur la reconnaissance de plaques d'immatriculation et les événements déclenchés par reconnaissance de plaques d'immatriculation dans un VMS.

1. Sélectionnez **Flux libre** et cliquez sur **Next (Suivant)**.
2. Sélectionnez la rotation de l'image correspondant à la façon dont votre caméra est montée.
3. Sélectionnez le nombre de domaines d'intérêt. Notez qu'une zone peut détecter des plaques dans les deux directions.
4. Sélectionnez la région où se trouve la caméra.
5. Sélectionnez le type de capture.
 - **License plate crop (Découpage de plaque d'immatriculation)** sauvegarde uniquement la plaque d'immatriculation.
 - **Vehicle crop (Découpage de véhicule)** sauvegarde l'intégralité du véhicule capturé.
 - **Frame downsized 480x270 (Taille de l'image réduite à 480x270)** sauvegarde l'intégralité de l'image et réduit la résolution à 480x270.
 - **Full frame (Image complète)** sauvegarde l'intégralité de l'image en pleine résolution.
6. Faites glisser les points d'ancrage pour ajuster le domaine d'intérêt. Cf. *Régler le domaine d'intérêt, on page 10*.
7. Réglez la direction du domaine d'intérêt. Cliquez sur la flèche et faites pivoter, pour définir la direction. La direction détermine comment l'application enregistre les véhicules entrant ou sortant de la zone.
8. Cliquez sur **Next (Suivant)**
9. Dans la liste déroulante **Protocol (Protocole)**, sélectionnez l'un des protocoles suivants :
 - TCP
 - HTTP POST

10. Dans le champ **Server URL (URL du serveur)**, entrez l'adresse et le port du serveur au format suivant :
127.0.0.1:8080
11. Dans le champ **Device ID (ID du périphérique)**, tapez le nom du périphérique ou laissez-le tel quel.
12. Sous **Event types (Types d'événements)**, sélectionnez une ou plusieurs des options suivantes :
 - **New (Nouveau)** correspond à la première détection d'une plaque d'immatriculation.
 - **Update (Mettre à jour)** est une correction d'un caractère sur une plaque d'immatriculation précédemment détectée ou lorsqu'une direction est détectée alors que la plaque se déplace en étant suivie dans l'image.
 - **Lost (Perdu)** est le dernier événement suivi de la plaque d'immatriculation avant qu'elle sorte de l'image. Il contient également la direction de la plaque d'immatriculation.
13. Pour activer la fonction, sélectionnez **Send event data to server (Envoyer les données d'événement au serveur)**.
14. Pour réduire la bande passante lors de l'utilisation du protocole HTTP POST, vous pouvez sélectionner **Do not to send images through HTTP POST (Ne pas envoyer d'images via HTTP POST)**.
15. Cliquez sur **Next (Suivant)**.
16. Si vous avez déjà une liste de plaques d'immatriculation enregistrées, choisissez d'importer en tant que **liste de blocage** ou **liste d'autorisation**.
17. Cliquez sur **Finish (Terminer)**.

Contrôle d'accès

Utilisez l'assistant de configuration pour une configuration simple et rapide. Vous pouvez choisir de **Skip (Quitter)** pour quitter le guide à tout moment.

1. Sélectionnez **Access Control (Contrôle d'accès)** et cliquez sur **Suivant**.
2. Sélectionnez le type de contrôle d'accès à utiliser :
 - **E/S interne** si vous souhaitez conserver la gestion de la liste dans la caméra. Cf. *Ouvrir une barrière à des véhicules connus à l'aide du port d'E/S de la caméra, on page 34.*
 - **Controller (Contrôleur)** si vous souhaitez connecter un contrôleur de porte. Cf. .
 - **Relay (Relais)** si vous souhaitez vous connecter à un module relais. Cf. .
3. Dans la liste déroulante **Barrier mode (Liste des barrières)**, sous **Open from lists (Ouvrir à partir des listes)**, sélectionnez **Allowlist (Liste d'autorisation)**.
4. Dans la liste déroulante **Vehicle direction (Direction du véhicule)**, sélectionnez **out (sortie)**.
5. Dans la liste déroulante **ROI (Retour sur investissement)**, sélectionnez le domaine d'intérêt que vous souhaitez utiliser, ou si vous souhaitez tout utiliser.
6. Cliquez sur **Next (Suivant)**.

À la page **Paramètres d'image** :

1. Sélectionnez le nombre de domaines d'intérêt.
2. Sélectionnez la région où se trouve la caméra.
3. Sélectionnez le type de capture. Cf. *Régler les paramètres de capture d'image, on page 11.*
4. Faites glisser les points d'ancrage pour ajuster le domaine d'intérêt. Cf. *Régler le domaine d'intérêt, on page 10.*
5. Réglez la direction du domaine d'intérêt. La direction détermine comment l'application enregistre les véhicules entrant ou sortant de la zone.
6. Cliquez sur **Next (Suivant)**

À la page **Données des événements** :

Remarque

Pour plus de détails sur les paramètres, consultez : *Envoi d'informations sur les événements à un logiciel tiers, on page 43.*

1. Dans la liste déroulante **Protocol (Protocole)**, sélectionnez l'un des protocoles suivants :
 - TCP
 - HTTP POST
2. Dans le champ **Server URL (URL du serveur)**, entrez l'adresse et le port du serveur au format suivant : 127.0.0.1:8080.
3. Dans le champ **Device ID (ID du périphérique)**, tapez le nom du périphérique ou laissez-le tel quel.
4. Sous **Event types (Types d'événements)**, sélectionnez une ou plusieurs des options suivantes :
 - **New (Nouveau)** correspond à la première détection d'une plaque d'immatriculation.
 - **Update (Mettre à jour)** est une correction d'un caractère sur une plaque d'immatriculation précédemment détectée ou lorsqu'une direction est détectée alors que la plaque se déplace en étant suivie dans l'image.
 - **Lost (Perdu)** est le dernier événement suivi de la plaque d'immatriculation avant qu'elle sorte de l'image. Il contient également la direction de la plaque d'immatriculation.
5. Pour activer la fonction, sélectionnez **Send event data to server (Envoyer les données d'événement au serveur)**.
6. Pour réduire la bande passante lors de l'utilisation du protocole HTTP POST, vous pouvez sélectionner **Do not send images through HTTP POST (Ne pas envoyer d'images via HTTP POST)**.
7. Cliquez sur **Next (Suivant)**

À la page **Importer la liste du fichier .csv** :

1. Si vous avez déjà une liste de plaques d'immatriculation enregistrées, choisissez d'importer en tant que **liste de blocage** ou **liste d'autorisation**.
2. Cliquez sur **Finish (Terminer)**.

Accéder aux paramètres de l'application

1. Dans l'interface web de la caméra, accédez à **Applications**, démarrez l'application et cliquez sur **Ouvrir**.

Régler le domaine d'intérêt

Le domaine d'intérêt est la zone de vidéo en direct dans laquelle l'application recherche des plaques d'immatriculation. Pour des performances optimales, faites que le domaine d'intérêt soit le plus petite possible. Pour ajuster le domaine d'intérêt, effectuez les actions suivantes :

1. Accédez à **Settings (Paramètres)**.
2. Veuillez cliquer sur **Image**.
3. Veuillez cliquer sur **1:1** pour effectuer un zoom dans la zone où vous souhaitez surveiller le trafic ou gérer le contrôle d'accès.
4. Pour améliorer la vérification et les images capturées, veuillez cliquer sur **AF (Mise au point)**.
5. Pour que la caméra procède à une mise au point automatique sur les véhicules, veuillez cliquer sur **AF (Mise au point automatique)**. Pour régler la mise au point manuellement, veuillez utiliser le curseur.
6. Veuillez cliquer sur **Area of interest (Domaine d'intérêt)** pour l'afficher dans la zone de visualisation.
7. Pour déplacer le domaine d'intérêt, veuillez cliquer n'importe où dans le domaine pour le sélectionner, puis faites-le glisser jusqu'à l'endroit où les plaques d'immatriculation sont le plus visibles. Une fois que vous avez enregistré les paramètres, assurez-vous que la région d'intérêt n'ait pas bougé.
8. Pour ajuster le domaine d'intérêt, veuillez cliquer n'importe où dans le domaine pour le sélectionner, puis faites glisser les points d'ancrage surlignés en bleu.

- Pour réinitialiser le domaine d'intérêt, veuillez cliquer sur le bouton de réinitialisation situé dans le coin inférieur gauche, à côté de l'icône représentant un chiffre.
 - Pour ajouter des points d'ancrage, veuillez cliquer sur un des points d'ancrage forcés. Le point d'ancrage deviendra jaune, ce qui indique qu'il peut être manipulé. Les nouveaux points forcés sont automatiquement ajoutés à côté du point d'ancrage jaune. Le nombre maximal de points d'ancrage jaunes est de huit.
9. Cliquez n'importe où en dehors du domaine d'intérêt pour enregistrer vos modifications.
 10. Pour obtenir des informations correctes sur la direction dans le **Event log (Journal d'événements)**, vous devez faire pivoter la flèche pour qu'elle corresponde à la direction principale.
 - 10.1. Cliquez sur l'icône en forme de flèche.
 - 10.2. Sélectionnez le point d'ancrage et faites pivoter la flèche afin qu'elle s'aligne avec la direction principale.
 - 10.3. Cliquez en dehors du domaine d'intérêt pour enregistrer vos modifications.

Notez qu'une zone peut détecter des plaques dans les deux directions. Les informations sur la direction s'affichent dans la colonne **Direction**.

11. Pour vérifier si votre domaine d'intérêt est suffisamment grand pour obtenir les meilleurs résultats, veuillez utiliser le compteur de pixels.
 - Pour afficher le compteur de pixels, veuillez cliquer sur l'icône représentant une calculatrice.
 - Pour ajuster la zone du compteur de pixels en taille réelle, veuillez faire glisser le coin inférieur droit de la zone surlignée en jaune.
 - Pour déplacer la zone du compteur de pixels, veuillez cliquer n'importe où dans cette zone et la faire glisser à l'endroit souhaité.
- Pour ajouter un deuxième domaine d'intérêt, veuillez cliquer sur **+** à côté de 1.
- Si vous utilisez une caméra autonome, vous pouvez ajouter l'application définie selon les paramètres recommandés pour la reconnaissance de plaque d'immatriculation.
 1. Veuillez cliquer sur l'icône représentant une baguette magique et les paramètres seront optimisés pour la reconnaissance de plaque d'immatriculation.
 2. Veuillez cliquer sur le bouton du menu à côté de la baguette magique pour afficher les valeurs définies.

Sélectionner une région

1. Veuillez aller à **Settings (Paramètres) > Recognition (Reconnaissance)**.
2. Dans la liste déroulante **Region (Région)**, sélectionnez votre région.

Régler les paramètres de capture d'image

1. Accédez à **Paramètres > Image**.
2. Pour modifier la résolution des images capturées, veuillez aller à **Image resolution (Résolution d'image)**
3. Pour modifier la rotation de l'image capturée, veuillez aller à **Rotation**

Configurer le stockage d'événements

Un événement se compose de l'image capturée, de la plaque d'immatriculation, du numéro du domaine d'intérêt, de la direction du véhicule, de l'accès, de la date et de l'heure.

Cet exemple de cas d'utilisation explique comment stocker les événements de numéros de plaque d'immatriculation sur liste d'autorisation pendant 30 jours.

Conditions requises

- Caméra installée physiquement et connectée au réseau.
- AXIS License Plate Verifier opérationnel sur la caméra.

- Stockage interne ou carte SD installée dans la caméra.
- 1. Veuillez aller à **Settings (Paramètres) > Storage (Stockage)**.
- 2. Sous **Retain events (Conserver des événements)**, veuillez sélectionner **Allowlisted (Liste d'autorisations)**.
- 3. Sous **Retention period (Période de conservation)**, veuillez sélectionner **30 days (30 jours)**.
- 4. Pour modifier la rotation de l'image capturée, accédez à **Enregistrer l'image complète** :
 - **License plate crop (Découpage de plaque d'immatriculation)** sauvegarde uniquement la plaque d'immatriculation.
 - **Vehicle crop (Découpage de véhicule)** sauvegarde l'intégralité du véhicule capturé.
 - **Frame downsized 480x270 (Taille de l'image réduite à 480x270)** sauvegarde l'intégralité de l'image et réduit la résolution à 480x270.
 - **Full frame (Image complète)** sauvegarde l'intégralité de l'image en pleine résolution.

Remarque

Pour détecter une carte SD insérée lorsque l'application est en cours d'exécution, redémarrez l'application. Si une carte SD est installée dans la caméra, l'application choisit automatiquement la carte SD comme stockage par défaut.

AXIS License Plate Verifier utilise la mémoire interne des caméras pour enregistrer jusqu'à 1 000 événements, en utilisant les découpages de plaque d'immatriculation comme image. Si vous utilisez des images plus volumineuses, le nombre d'événements que vous pouvez enregistrer varie.

Une carte SD peut enregistrer jusqu'à 100 000 événements à l'aide de n'importe quel type d'image.

Configurer votre périphérique

La présente section couvre l'ensemble des configurations importantes qu'un installateur doit effectuer pour que le produit soit opérationnel une fois l'installation matérielle terminée.

Pour les utilisateurs de AXIS Camera Station

Configurer AXIS License Plate Verifier

Lorsqu'un périphérique est configuré avec AXIS License Plate Verifier, il est considéré comme une source de données externe dans le système de gestion vidéo. Vous pouvez connecter une vue à la source de données, rechercher les plaques d'immatriculation capturées par le périphérique et afficher l'image associée.

Paramètres de base

Définir le mode de capture

1. Accédez à Vidéo > Installation > Mode de capture.
2. Cliquez sur **Change (Modifier)**.
3. Sélectionnez un mode de capture et cliquez sur **Enregistrer et redémarrer**.
Voir aussi *Modes de capture*, on page 49.

Définir l'orientation

1. Accédez à Vidéo > Installation > Rotate (Vidéo > Installation > Pivoter).
2. Sélectionnez 0, 90, 180 ou 270 degrés.
Voir aussi *Surveiller les zones longues et étroites*, on page 16.

Régler l'image

Cette section fournit des instructions sur la configuration de votre périphérique. Pour en savoir plus sur certaines fonctions, accédez à *En savoir plus*, on page 49.

Mettre à niveau la caméra

Pour ajuster la vue par rapport à une zone de référence ou à un objet, utilisez la grille de niveau avec un ajustement mécanique de la caméra.

1. Allez à Vidéo (Vidéo) > Image (Image) > et cliquez sur .
2. Cliquez sur  pour afficher la grille de niveau.
3. Ajustez la caméra mécaniquement jusqu'à ce que la position de la zone de référence ou de l'objet soit alignée sur la grille de niveau.

Régler le zoom et la mise au point

Pour régler le zoom :

1. Allez à Vidéo > Installation et réglez le curseur de zoom.

Pour régler la mise au point :

1. Cliquez sur  pour afficher la zone de mise au point automatique.
2. Ajustez la zone de mise au point automatique pour couvrir la partie de l'image que vous souhaitez mettre au point.
Si vous ne sélectionnez pas une zone de mise au point automatique, la caméra effectue la mise au point sur la totalité de la scène. Nous vous conseillons d'effectuer la mise au point sur un objet statique.
3. Cliquez sur **Autofocus (Mise au point automatique)**.

4. Pour ajuster la mise au point, réglez le curseur de mise au point.

Réduire la durée du traitement d'image avec le mode faible latence

Vous pouvez optimiser la durée du traitement d'image de votre flux de données vidéo en direct en activant le mode faible latence. La latence de votre flux de données vidéo en direct est réduite au minimum. Lorsque vous utilisez un mode de faible latence, la qualité d'image est inférieure à celle d'ordinaire.

1. Allez à **System > Plain config (Système > Configuration normale)**.
2. Sélectionnez **ImageSource** dans la liste déroulante.
3. Accédez à **ImageSource/IO/Sensor > Low latency mode (Mode faible latence)** et sélectionnez **On (Activé)**.
4. Cliquez sur **Save (Enregistrer)**.

Sélectionner le mode d'exposition

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

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

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

Votre caméra utilise la lumière visible pour générer des images en couleur pendant la journée. Mais lorsque la lumière visible diminue, les images en couleur deviennent moins lumineuses et claires. Si vous basculez en mode nocturne lorsque cela se produit, la caméra utilise à la fois la lumière visible et la lumière infrarouge proche pour fournir des images noir et blanc lumineuses et détaillées. Vous pouvez configurer la caméra pour qu'elle bascule en mode nocturne automatiquement.

1. Accédez à **Video > Image > Day-night mode (Vidéo > Image > Mode jour et nuit)** et assurez-vous que **IR cut filter (Masque IR)** est défini sur **Auto**.
2. Pour définir le niveau d'éclairage auquel la caméra bascule en mode nocturne, déplacez le curseur **Threshold (Seuil)** vers **Bright (Clair)** ou **Dark (Foncé)**.
3. Pour utiliser l'illuminateur IR intégré lorsque la caméra est en mode nocturne, activez **Autoriser l'éclairage** et **Synchroniser l'éclairage IR**.

Remarque

Si vous définissez le commutateur pour que le mode nocturne s'active dans des conditions de plus grande clarté, l'image reste plus nette car il y a moins de bruit de faible luminosité. Si vous définissez le commutateur sur des conditions de plus grande obscurité, les couleurs de l'image sont conservées plus longtemps, mais il y a davantage de flou dans l'image en raison du bruit de faible luminosité.

Optimiser l'éclairage IR

Selon l'environnement d'installation et les conditions autour de la caméra tels que des sources de lumière externes par exemple, vous pouvez parfois améliorer la qualité d'image si vous ajustez manuellement l'intensité des LED. En cas de problèmes de reflets des voyants LED, vous pouvez essayer de réduire leur intensité.

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

Réduire le bruit dans des conditions de faible luminosité

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

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

Remarque

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

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

Remarque

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

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

Réduire le flou de mouvement dans les conditions de faible luminosité

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

Remarque

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

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

Remarque

Lorsque vous ouvrez l'ouverture, la profondeur de champ est plus superficielle.

- Déplacez le curseur **Aperture (Ouverture)** vers **Open (Ouvrir)**.

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

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

Gérer les scènes avec un fort contre-jour

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



Image sans WDR.



Image avec WDR.

Remarque

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

Découvrez-en plus sur la fonction WDR et son utilisation à l'adresse axis.com/solutions/wide-dynamic-range-wdr.

Compensation de la distorsion en barillet

La distorsion en barillet est un phénomène dans lequel des lignes droites apparaissent de plus en plus courbées près des bords de l'image. Un large champ de vision permet souvent de créer une distorsion en barillet dans une image. La correction de la distorsion en barillet compense cette distorsion.

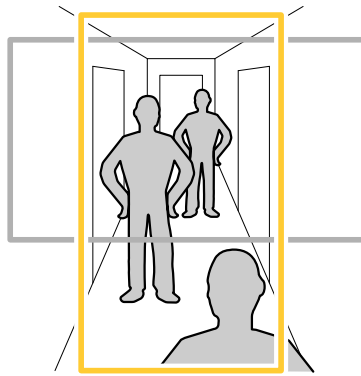
Remarque

La correction de la distorsion en barillet affecte la résolution de l'image et le champ de vision.

1. Accédez à **Vidéo > Installation > Correction de l'image**.
2. Activez **Barrel distortion correction (BDC) (Correction de la distorsion en barillet (CDB))**.

Surveiller les zones longues et étroites

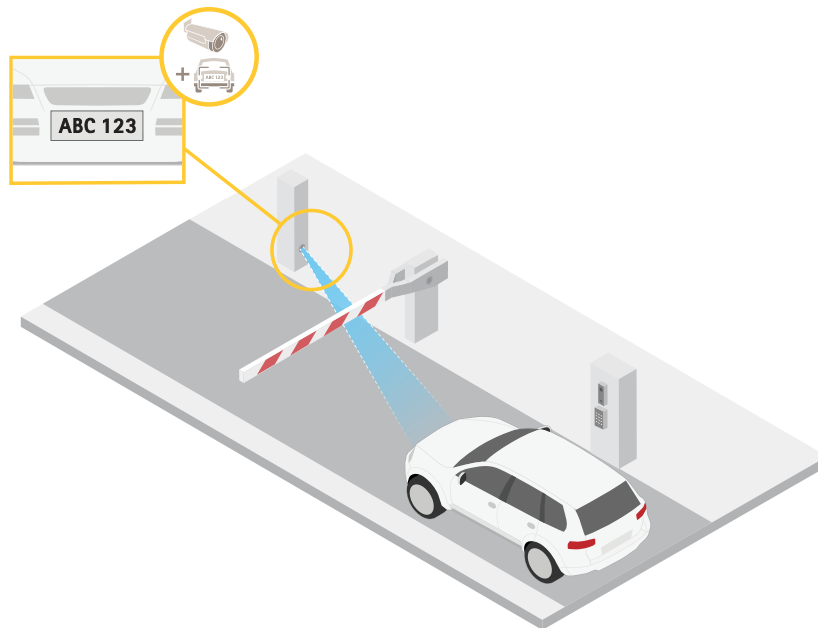
Utilisez le format Corridor pour mieux exploiter le champ de vision complet dans une zone longue et étroite, par exemple un escalier, un couloir, une route ou un tunnel.



1. Selon le périphérique, tournez la caméra ou l'objectif à 3 axes de la caméra à 90° ou 270°.
2. Si le périphérique n'a pas de rotation automatique de la vue, accédez à **Video > Installation (Vidéo > Installation)**.
3. Faites pivoter la vue à 90° ou 270°.

Vérifier la résolution en pixels

Pour vérifier qu'une partie définie de l'image contient suffisamment de pixels afin de, par exemple, reconnaître les plaques d'immatriculation, vous pouvez utiliser le compteur de pixels.



1. Accédez à **Video > Image (Vidéo > Image)**.
2. Cliquez sur .
3. Cliquez  pour **Pixel counter (Compteur de pixels)**.
4. Dans la vidéo en direct de la caméra, réglez la taille et la position du rectangle autour du domaine d'intérêt, par exemple l'endroit où vous pensez que les plaques d'immatriculation vont apparaître.
5. Vous pouvez voir le nombre de pixels sur chaque côté du rectangle et décider si les valeurs sont suffisantes pour vos besoins.

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

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

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

Consultez aussi *Masques de confidentialité, on page 50*

Afficher une incrustation d'image

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

1. Allez à **Vidéo > Incrustations**.
2. Cliquez sur **Manage images (Gérer les images)**.
3. Téléchargez une image ou faites-la glisser et déposez-la.
4. Cliquez sur **Upload (Télécharger)**.
5. Sélectionnez **Image** dans la liste déroulante et cliquez sur **+**.
6. Sélectionnez l'image et une position. Vous pouvez également faire glisser l'image en incrustation dans la vidéo en direct pour modifier la position.

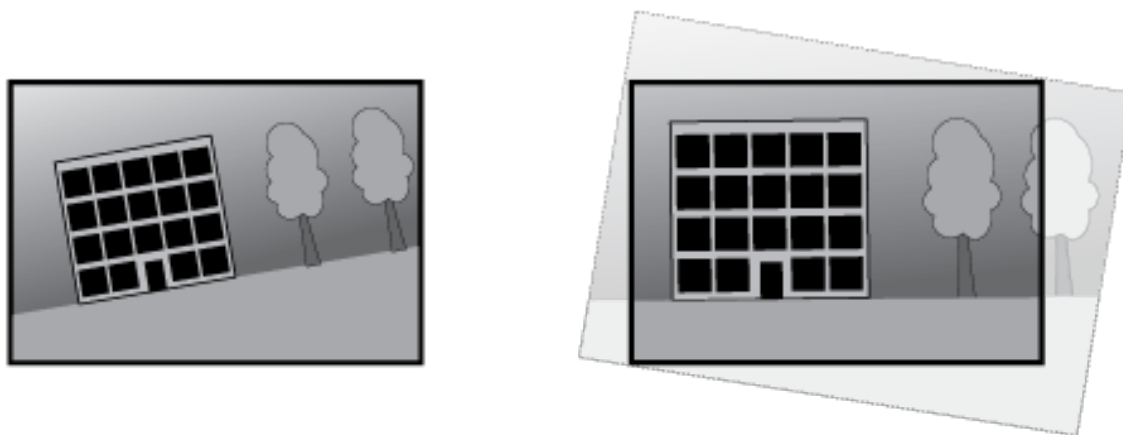
Afficher une incrustation de texte

Vous pouvez ajouter un champ de texte en tant qu'incrustation dans le flux vidéo. 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. Allez à **Vidéo > Incrustations**.
2. Sélectionnez **Text (Texte)** et cliquez sur **+**.
3. Tapez le texte que vous souhaitez afficher, ou sélectionnez des modificateurs pour afficher, par exemple, la date actuelle.
4. Sélectionnez une position. Vous pouvez également faire glisser l'incrustation dans la vidéo en direct pour modifier la position.

Redresser une image inclinée

Vous pouvez redresser une image inclinée en la faisant pivoter et en la rognant numériquement. En raison du rognage, une partie de l'image originale est perdue. Cette fonction est utile lors de l'installation.



L'illustration montre avant et après le redressement d'une image.

1. Accédez à Vidéo > Installation > Correction de l'image.
2. Activez **Straighten image (Redresser l'image)**.
3. Utilisez les commandes pour ajuster l'image.

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 *Diffusion et stockage*, on page 50.

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 Vidéo > Stream (Vidéo > Flux).
2. Cliquez sur  dans la vidéo en direct.
3. Sélectionnez **Video format (Format vidéo) AV1** si votre périphérique le prend en charge. Sinon, sélectionnez **H.264**.
4. Accédez à Vidéo > Stream > General (Vidéo > Flux > Général) et augmentez la valeur de **Compression**.
5. Accédez à Vidéo > Flux > Zipstream et procédez comme suit (une ou plusieurs fois) :

Remarque

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

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

Remarque

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

Configurer le stockage réseau

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

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

Enregistrer et regarder la vidéo

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

1. Accédez à **Video > Stream (Vidéo > 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 *Configurer le stockage réseau, on page 19*.
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.

Vérifiez que personne n'a saboté la vidéo.

Avec la vidéo signée, vous pouvez vous assurer que personne n'a saboté la vidéo enregistrée par la caméra.

1. Accédez à **Video > Stream > General (Vidéo > Flux > Général)** et activez **Signed video (Vidéo signée)**.
2. Enregistrez la vidéo directement sur le dispositif, ou utilisez AXIS Camera Station Pro ou un autre logiciel de gestion vidéo compatible. Pour obtenir des instructions sur AXIS Camera Station Pro, consultez le *manuel d'utilisation d'AXIS Camera Station Pro*.
3. Exportez la vidéo enregistrée.
4. Veuillez utiliser l'outil de *vérification des médias signés* d'Axis pour vérifier l'enregistrement.

Définir des règles pour les événements

Vous pouvez créer des règles pour que votre périphérique exécute une action lorsque certains événements se produisent. Une règle se compose de conditions et d'actions. Les conditions peuvent être utilisées pour déclencher les actions. Par exemple, le périphérique peut démarrer un enregistrement ou envoyer un e-mail lorsqu'il détecte un mouvement ou afficher un texte d'incrustation lorsque le périphérique enregistre.

Pour en savoir plus, consultez *Get started with rules for events (Commencer à utiliser 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** à exécuter lorsque les conditions sont satisfaites.

Enregistrer une vidéo lorsque la caméra détecte un objet

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

Avant de commencer :

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

Assurez-vous que AXIS Video Motion Detection est en cours d'exécution :

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

Créez une règle :

1. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sous **Applications**, sélectionnez **VMD4**.
4. Dans la liste des actions, sous **Recordings (Enregistrements)**, sélectionnez **Record video while the rule is active (Enregistrer la vidéo tant que la règle est active)**.
5. Dans la liste des options de stockage, sélectionnez **SD_DISK (DISQUE_SD)**.
6. Sélectionnez une caméra et un profil de flux.
7. Réglez la durée pré-buffer sur 5 secondes.
8. Réglez la durée post-tampon sur 1 minute.
9. Cliquez sur **Save (Enregistrer)**.

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

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

Assurez-vous que AXIS Video Motion Detection est en cours d'exécution :

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

Ajoutez l'incrustation de texte :

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

Créez une règle :

1. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.

3. Dans la liste des conditions, sous **Applications**, sélectionnez **VMD4**.
4. Dans la liste des actions, sous **Overlay text (Texte d'incrustation)**, sélectionnez **Use overlay text (Utiliser le texte d'incrustation)**.
5. Sélectionner un canal vidéo.
6. Dans **Text (Texte)**, saisissez « Motion detected (Mouvement détecté) ».
7. Définissez la durée.
8. Cliquez sur **Save (Enregistrer)**.

Remarque

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

Fournir une indication visuelle d'un événement en cours

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

Matériel requis

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

Remarque

AXIS I/O Indication LED doit être connecté à un port de sortie.

Remarque

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

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

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

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

- Configurez la LED pour qu'elle s'allume lorsque la caméra démarre, afin d'indiquer la présence de la caméra. Sélectionnez **System ready (Système prêt)** comme condition.

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

Déclencher une notification lors de l'ouverture de l'enceinte

Cet exemple explique comment configurer une notification par e-mail lorsque le boîtier ou l'enveloppe du périphérique est ouvert.

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)** comme type de notification.
4. Saisissez l'adresse électronique du destinataire.
5. Saisissez l'adresse électronique à partir de laquelle vous souhaitez que la caméra envoie des notifications.
6. Indiquez les données de connexion du compte de messagerie d'envoi, ainsi que le nom d'hôte SMTP et le numéro de port.
7. Pour tester la configuration de votre e-mail, cliquez sur **Test (Test)**.
8. Cliquez sur **Save (Enregistrer)**.

Créer une règle :

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

Déclencher une notification en cas de sabotage de l'objectif de la caméra.

Cet exemple explique comment configurer une notification par e-mail lorsque l'objectif de la caméra est peint au pistolet, recouvert ou brouillé.

Activer la détection de sabotage :

1. Accédez à **System (Système) Detectors (DéTECTEURS) > Camera tampering (Sabotage)**.
2. Définissez une valeur pour **Délai de déclenchement**. La valeur indique le temps qui doit s'écouler avant qu'un e-mail soit envoyé.
3. Activez **Trigger on dark images (Déclencheur sur images sombres)** pour détecter si l'objectif est aspergé, recouvert ou si sa mise au point est fortement dérégulée.

Ajouter un destinataire d'e-mails :

4. Accédez à **System (Système) > Events (Événements) > Recipients (Destinataires)** et ajoutez un destinataire.
5. Entrez le nom du destinataire de l'e-mail.
6. Sélectionnez **Email (E-mail)** comme type de notification.
7. Saisissez l'adresse électronique du destinataire.
8. Saisissez l'adresse électronique à partir de laquelle vous souhaitez que la caméra envoie des notifications.

9. Indiquez les données de connexion du compte de messagerie d'envoi, ainsi que le nom d'hôte SMTP et le numéro de port.
10. Pour tester la configuration de votre e-mail, cliquez sur **Test (Test)**.
11. Cliquez sur **Save (Enregistrer)**.

Créez une règle :

12. Accédez à **System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
13. Saisissez le nom de la règle.
14. Dans la liste des conditions, sous **Video (Vidéo)**, sélectionnez **Tampering (Sabotage)**.
15. Dans la liste des actions, sous **Notifications**, sélectionnez **Send notification to email (Envoyer une notification à un e-mail)**, puis sélectionnez le destinataire dans la liste.
16. Saisissez un objet et un message pour l'e-mail.
17. Cliquez sur **Save (Enregistrer)**.

Connexion à une sirène-stroboscope.

L'appairage réseau vous permet d'appairer une caméra à un périphérique Axis compatible équipé d'un éclairage et d'une sirène. Une fois appairée, la caméra peut configurer et gérer les deux périphériques.

Appairer la caméra à une sirène-stroboscope :

1. Allez à **System > Edge-to-edge > Pairing (Système > Complet > Appairage)**.
2. Cliquez sur  **Add (Ajouter)** et sélectionnez le type d'appairage **Network pairing (Appairage réseau)** dans la liste déroulante.
3. Entrez l'adresse IP, le nom d'utilisateur et le mot de passe de la sirène-stroboscope.
4. Cliquez sur **Connect (Connecter)**. Un message de confirmation s'affiche.

Pour trouver des périphériques directement sur le réseau, cliquez sur **Discover devices (Détecter les périphériques)**.

Remarque

- La liste affiche tous les périphériques Axis détectés, et pas seulement ceux qui peuvent être appairés.
- Une icône d'information s'affiche pour les périphériques qui ont déjà été appairés. Passez la souris sur l'icône pour obtenir des informations sur les appairages déjà actifs.
- Veuillez vous assurer que les périphériques appairés utilisent la même version d'AXIS OS.

Important

- Seuls les périphériques sur lesquels Bonjour est activé peuvent être détectés. Pour activer Bonjour pour un périphérique, veuillez ouvrir son interface web et aller à **System (Système) > Network (Réseau) > Network discovery protocols (Protocoles de détection de réseaux)**.

Gérer les listes

Ajouter une plaque d'immatriculation détectée à la liste

Une plaque d'immatriculation peut être ajoutée directement à une liste, après avoir été détectée par l'application.

1. Veuillez cliquer sur **Home (Accueil)**.
2. Veuillez aller à la **Live (vidéo en direct)**.
3. Veuillez cliquer sur l'icône en forme de flèche sur la plaque d'immatriculation enregistrée dans la liste.
4. Veuillez cliquer sur **Append plate to list (Ajouter une plaque à la liste)**.
5. Veuillez sélectionner la liste à laquelle vous souhaitez ajouter la plaque d'immatriculation dans le dialogue.
6. Cliquez sur **Append (Annexe)**.

Remarque

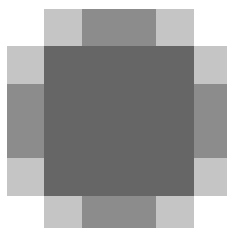
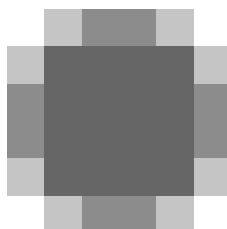
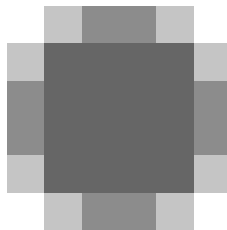
Veuillez vous assurer que les symboles <, > et & ne sont pas utilisés dans la plaque d'immatriculation ou la description.

Ajouter des descriptions aux plaques d'immatriculation

Pour ajouter une description à une plaque d'immatriculation dans la liste :

- Accédez à **List Management (Gestion des listes)**.

- Veuillez sélectionner la plaque d'immatriculation et cliquer sur



, puis sélectionner **Edit (Modifier)** dans le menu déroulant.

- Veuillez taper les informations pertinentes dans le champ **Description**.
- Cliquez sur **Save (Enregistrer)**.

Remarque

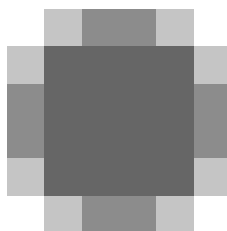
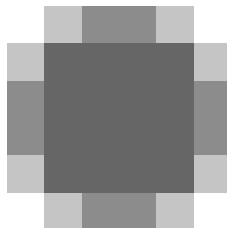
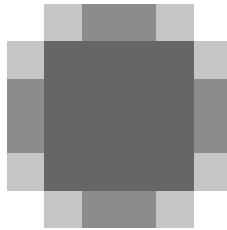
Assurez-vous que les symboles <, > et & ne sont pas utilisés dans les plaques d'immatriculation ou les descriptions.

Personnaliser les noms de la liste

Vous pouvez changer le nom de l'une des listes, pour vous adapter à votre cas d'utilisation spécifique.

1. Accédez à **List Management (Gestion des listes)**.

2. Veuillez cliquer sur



à côté de la liste que vous souhaitez changer.

3. Veuillez sélectionner **Edit (Modifier)**.
4. Tapez le nom de la liste.
5. Cliquez sur **Submit (Envoyer)**.

Le nouveau nom de liste sera mis à jour dans toutes les configurations existantes.

Importer les numéros de plaque d'immatriculation sur liste d'autorisation

Vous pouvez importer les numéros de plaque d'immatriculation sur liste d'autorisation depuis un fichier .csv sur l'ordinateur. En plus du numéro de plaque d'immatriculation, vous pouvez également ajouter des commentaires pour chaque numéro de plaque d'immatriculation dans le fichier .csv.

La structure du fichier .csv doit se présenter comme suit : `license plate, date, description`

Exemple:

Seulement la plaque d'immatriculation : `AXIS123`

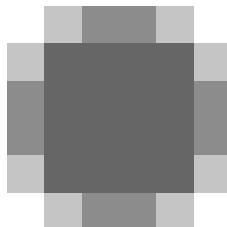
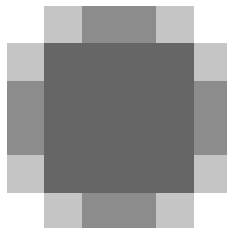
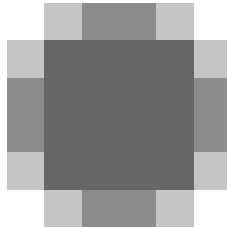
Plaque d'immatriculation + description : `AXIS123, , John Smith`

Plaque d'immatriculation + date + description : `AXIS123, 2022-06-08, John Smith`

Remarque

Assurez-vous que les symboles <, > et & ne sont pas utilisés dans les plaques d'immatriculation ou les descriptions.

1. Accédez à List Management (Gestion des listes)
2. Veuillez cliquer sur



à côté de **Allowlist (Liste d'autorisation)** et sélectionner **Import (Importer)** dans le menu déroulant.

3. Recherchez et sélectionnez un fichier .csv sur l'ordinateur.
4. Cliquez sur **OK**.
5. Vérifiez que les numéros de plaque d'immatriculation importés s'affichent dans **Allowlist (Liste d'autorisation)**.

Partager les listes de plaques d'immatriculation avec d'autres caméras

Vous pouvez partager les listes de plaques d'immatriculation avec d'autres caméras sur le réseau. La synchronisation remplace toutes les listes de plaques d'immatriculation en cours dans les autres caméras.

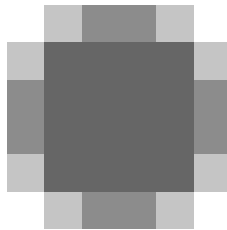
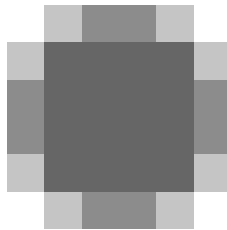
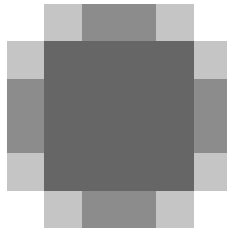
1. Veuillez aller à List management (Gestion des listes) > List synchronization (Synchronisation des listes).

2. Sous **Remote connected devices (Périphériques connectés à distance)**, veuillez taper l'adresse IP, le nom d'utilisateur et le mot de passe.
3. Cliquez sur **Ajouter**.
4. Veuillez cliquer sur **Synchronize list (Synchroniser la liste)**.
5. Vérifiez que la date et l'heure de **Last sync (Dernière synchro)** sont mises à jour en conséquence.

Listes des programmations

Les listes peuvent être programmées pour être actives uniquement à certains moments de la semaine. Pour programmer une liste :

- Accédez à **List Management (Gestion des listes)**.
- Veuillez cliquer sur



à côté de la liste que vous souhaitez changer.

- Veuillez sélectionner **Schedule (Programmer)** dans le menu déroulant.
- Sélectionnez l'heure de début et de fin et le jour où la liste doit être active.
- Cliquez sur le bouton à côté de **Enabled (Activé)**.
- Cliquez sur **Save (Enregistrer)**.

Paramètres supplémentaires

Configurer l'incrustation de texte

Une incrustation de texte permet d'afficher les informations d'événement suivantes dans la vue en direct : weekday, month, time, year, license plate number.

1. Accédez à Paramètres > Image.
2. Activez Texte overlay (Incrustation de texte).
3. Veuillez sélectionner Timestamp and license plate (Horodatage et plaque d'immatriculation) ou License plate only (Plaque d'immatriculation uniquement).
4. Réglez Overlay duration (Durée de l'incrustation) sur une valeur comprise entre 1 et 9 secondes.
5. Vérifiez que l'incrustation s'affiche dans la vidéo en direct.

Détecter les plaques d'immatriculation dans des conditions de faible éclairage

L'algorithme attribue à chaque détection un score appelé « seuil de confiance ». Les détections dont le score est inférieur au niveau sélectionné ne s'affichent pas dans la liste d'événements.

Pour les scènes à faible luminosité, il est possible de définir un seuil de confiance plus bas, ce qui permettra de détecter davantage de plaques.

1. Veuillez aller à Settings (Paramètres)> Recognition (Reconnaissance).
2. Veuillez ajuster le curseur sous Confidence threshold (Seuil de confiance).
3. Vérifiez que l'algorithme détecte les plaques d'immatriculation conformément aux attentes.

Autoriser moins de caractères sur les plaques d'immatriculation

L'application a un nombre de caractères minimal par défaut pour pouvoir détecter une plaque d'immatriculation. Le nombre minimal de caractères par défaut est 5. Vous pouvez configurer l'application pour qu'elle détecte des plaques d'immatriculation avec moins de caractères.

1. Veuillez aller à Settings (Paramètres)> Recognition (Reconnaissance).
2. Sous Number of characters (Nombre de caractères), veuillez ajuster le curseur pour définir le nombre minimum de caractères que vous souhaitez autoriser.
3. Vérifiez que l'application détecte les plaques d'immatriculation conformément aux attentes.

Autoriser uniquement les correspondances exactes de plaques d'immatriculation

L'algorithme de reconnaissance autorise automatiquement un écart d'un caractère lors de la comparaison de la plaque d'immatriculation détectée avec la liste d'autorisation ou la liste de blocage. Cependant, certains scénarios nécessitent une correspondance exacte de tous les caractères de la plaque d'immatriculation.

1. Accédez à List Management (Gestion des listes).
2. Cliquez sur Correspondance exacte.
3. Vérifiez que l'application reconnaît les plaques d'immatriculation conformément aux attentes.

Autoriser un écart de plusieurs caractères lors de la reconnaissance des plaques d'immatriculation

L'algorithme de reconnaissance autorise automatiquement un écart d'un caractère lors de la comparaison de la plaque d'immatriculation détectée avec la liste d'autorisation ou la liste de blocage. Cependant, vous pouvez autoriser un écart de plusieurs caractères.

1. Veuillez aller à Settings (Paramètres)> Recognition (Reconnaissance).

2. Sous **Allowed character deviation (Écart de caractère autorisé)**, sélectionnez le nombre de caractères autorisés à être différents.
3. Vérifiez que l'application reconnaît les plaques d'immatriculation conformément aux attentes.

Donner un accès limité aux opérateurs

Les opérateurs peuvent se voir accorder un accès limité à l'application à l'aide d'une URL. De cette manière, ils n'ont accès qu'au **Journal des événements** et à la **Gestion de la liste**. L'URL se trouve dans **Paramètres > User rights (Droits d'utilisateur)**.

Configurer une connexion sécurisée

Pour protéger la communication et les données entre les périphériques, par exemple, entre la caméra et le contrôleur de porte, configurez une connexion sécurisée avec HTTPS, en utilisant des certificats.

1. Accédez à **Paramètres > Security (Sécurité)**.
2. Sous HTTPS, veuillez sélectionner **Self-signed (Auto-signé)** ou **CA-signed (Signé CA)**.

Remarque

Pour en savoir plus sur HTTPS et son utilisation, veuillez consulter .

Enregistrer et restaurer les paramètres des applications

Vous pouvez sauvegarder et restaurer les paramètres de l'application liés à la capture d'image, à la sécurité, à la détection et à l'intégration. En cas de problème, vous pouvez maintenant restaurer les paramètres que vous avez sauvegardés.

Pour sauvegarder les paramètres de l'application :

- Accédez à **Paramètres > Maintenance**.
- Veuillez cliquer sur **Download back up configuration (Télécharger la configuration de sauvegarde)**.

Un fichier JSON sera téléchargé vers votre dossier de téléchargements.

Pour restaurer les paramètres de l'application :

- Accédez à **Paramètres > Maintenance**.
- Cliquez sur **Restore configuration (Restaurer la configuration)**.

Sélectionnez le fichier JSON contenant la sauvegarde.

Le paramètre est restauré automatiquement.

Effacer tous les événements

Une fois l'application configurée, il peut être bon de effacer les enregistrements des images ou des plaques capturées à partir du processus de configuration.

Pour effacer toutes les images et plaques de la base de données :

Accédez à **Paramètres > Maintenance**.

- Cliquez sur **Clear all recognition results (Effacer tous les résultats de reconnaissance)**.
- Cliquez sur **Yes (Oui)**.

Utilisation de ports virtuels comme actions de déclenchement

Les ports virtuels peuvent être utilisés avec le contrôle d'accès pour déclencher tout type d'action. Cet exemple explique comment configurer AXIS License Plate Verifier avec le port d'E/S de la caméra pour afficher une incrustation de texte à l'aide d'un port virtuel.

Conditions requises

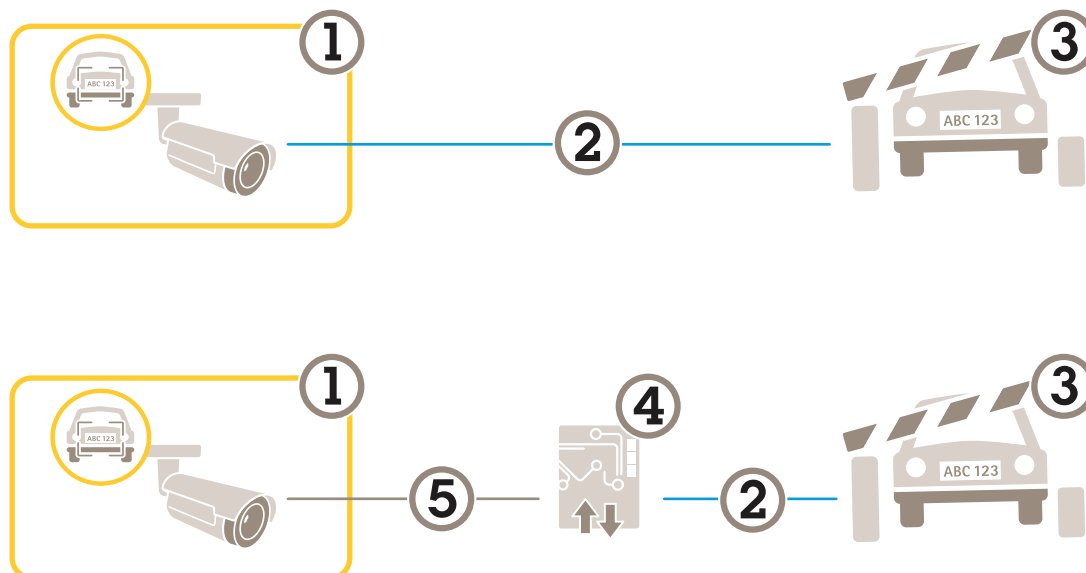
- Caméra installée physiquement et connectée au réseau.

- AXIS License Plate Verifier opérationnel sur la caméra.
 - Les câbles entre la barrière et le port d'E/S de la caméra sont connectés.
 - Configuration de base effectuée. Cf. .
1. Allez sur la page Web de l'application et sélectionnez l'onglet **Settings (Paramètres)**.
 2. Accédez à **Contrôle d'accès**.
 3. Sous **Access control (Contrôle d'accès)**, veuillez sélectionner **Internal I/O (E/S interne)**.
 4. Sélectionnez le n° de sortie E/S.
 5. Sélectionnez un port dans la liste déroulante **Port virtuel**.
 6. Sous **Barrier mode (Mode pare-feu)**, veuillez sélectionner **Open to all (Ouvrir à tous)**.
 7. Sous **Vehicle direction (Direction du véhicule)**, veuillez sélectionner **Any (N'importe laquelle)**.
 8. Veuillez sélectionner le **Area of interest (Domaine d'intérêt)** que vous souhaitez utiliser.
 9. Sur la page web de la caméra, accédez à **Système > Événements**.
 10. Cliquez sur **Add rule (Ajouter une règle)**.
 11. Sous **Condition**, sélectionnez **L'entrée virtuelle est active** et le numéro de port que vous avez choisi.
 12. Sous **Action**, sélectionnez **Utiliser une incrustation de texte**.
 13. Sélectionnez **Canaux vidéo**.
 14. Entrez le texte que vous souhaitez afficher.
 15. Ajoutez la durée du texte.
 16. Cliquez sur **Save (Enregistrer)**.
 17. Allez à **Vidéo > Incrustations**.
 18. Accédez à **Incrustations**.
 19. Sélectionnez **Texte** dans le menu déroulant et cliquez sur **+**.
 20. Entrez #D ou sélectionnez le modificateur dans la liste déroulante **Modifiers (Modificateurs)**.
 21. Vérifiez que l'incrustation de texte s'affiche lorsqu'un véhicule entre dans la région d'intérêt dans la vidéo en direct.

Scénario d'entrée et de sortie de véhicules

Dans ce scénario, l'application lit la plaque d'immatriculation du véhicule capturée par la caméra et la compare avec une liste de numéros de plaque d'immatriculation autorisés ou non autorisés dans la caméra.

Ce scénario nécessite que l'application soit intégrée à une caméra avec support E/S ou à un module relais E/S réseau pour ouvrir et fermer la barrière.



Deux paramètres sont possibles pour le scénario d'entrée et de sortie de véhicules.

- 1 Caméra Axis avec AXIS License Plate Verifier
- 2 Communication E/S
- 3 Barrière
- 4 Module relais E/S Axis
- 5 Communication IP

Ouvrir une barrière à des véhicules connus à l'aide d'un module relais

Cet exemple de cas d'utilisation explique comment configurer AXIS License Plate Verifier avec un module relais pour ouvrir une barrière à un véhicule connu circulant dans une région d'intérêt (ROI) spécifique, par exemple dans un parking.

Conditions requises :

- Caméra installée physiquement et connectée au réseau.
 - AXIS License Plate Verifier opérationnel sur la caméra.
 - Les câbles entre la barrière et le module relais sont connectés.
 - Configuration de base effectuée. Cf. .
1. Accédez à la page web de la caméra, puis allez dans **Settings (Paramètres)** et ouvrez **AXIS License Plate Verifier**.
 2. Allez sur la page Web du module relais et assurez-vous que le port du module est bien connecté au port E/S de la caméra.
 3. Copiez l'adresse IP du module relais.
 4. Revenez à **AXIS License Plate Verifier**.
 5. Accédez à **Settings > Access control (Paramètres > Contrôle d'accès)**.
 6. Accédez à **Type**, et sélectionnez **Relay (Relais)** dans la liste déroulante.
 7. Dans la liste déroulante **I/O output (Sortie E/S)**, sélectionnez le port d'E/S connecté à la barrière.

8. Dans la liste déroulante **Barrier mode (Liste des barrières)**, sélectionnez **Open from lists (Ouvrir à partir des listes)**, puis cochez la case **Allowlist (Liste d'autorisation)**.
9. Dans la liste déroulante **Vehicle direction (Direction du véhicule)**, sélectionnez **in (entrée)**.
10. Dans la liste déroulante **ROI**, sélectionnez le domaine d'intérêt qui couvre la voie de circulation.
11. Saisissez les informations suivantes :
 - l'adresse IP du module relais au format 192.168.0.0
 - le nom d'utilisateur du module relais
 - le mot de passe du module relais
12. Pour vérifier que la connexion est établie, cliquez sur **Connect (Connexion)**.
13. Pour activer la connexion, cliquez sur **Turn on integration (Activer l'intégration)**.
14. Accédez à l'onglet **List management (Gestion des listes)**.
15. Saisissez le numéro de plaque d'immatriculation dans le champ **Allowlist (Liste d'autorisation)**.

Remarque

Les ports d'entrée 1 à 8 sur le module relais correspondent aux ports 1 à 8 de la liste déroulante. Cependant, les ports 1 à 8 sur le module relais correspondent aux ports 9 et 16 de la liste déroulante. Ceci est valable même si le module relais dispose de 8 ports uniquement.

16. Vérifiez que l'application identifie le numéro de plaque d'immatriculation dans la liste d'autorisation comme un véhicule connu et que la barrière s'ouvre.

Ouvrir une barrière à des véhicules connus à l'aide du port d'E/S de la caméra

Cet exemple explique comment configurer AXIS License Plate Verifier avec le port d'E/S de la caméra, pour ouvrir une barrière à véhicule connu entrant, par exemple, dans un parking.

Conditions requises

- Caméra installée physiquement et connectée au réseau.
 - AXIS License Plate Verifier opérationnel sur la caméra.
 - Les câbles entre la barrière et le port d'E/S de la caméra sont connectés.
 - Configuration de base effectuée. Cf. .
1. Veuillez aller à la page web de l'application et à **Home (Accueil)**, et ajouter les plaques d'immatriculation détectées à une liste. Voir *Ajouter une plaque d'immatriculation détectée à la liste, on page 25*
 2. Pour modifier les listes directement, veuillez aller à **List management (Gestion des listes)**.
 3. Saisissez les numéros des plaques d'immatriculation autorisées dans le champ **Liste d'autorisation**.
 4. Accédez à **Settings (Paramètres)**.
 5. Sous **Access control (Contrôle d'accès)**, veuillez sélectionner **Internal I/O (E/S interne)**.
 6. Sélectionnez le n° de sortie E/S.
 7. Sous **Barrier mode (Mode pare-feu)**, veuillez sélectionner **Open from lists (Ouvrir à partir des listes)**, puis cocher **Allowlist (Liste d'autorisations)**.
 8. Dans la liste déroulante **Vehicle direction (Direction du véhicule)**, sélectionnez **in (entrée)**.
 9. Sous **Area of interest (Domaine d'intérêt)**, veuillez sélectionner le domaine d'intérêt que vous souhaitez utiliser, ou si vous souhaitez les utiliser tous.
 10. Vérifiez que l'application identifie le numéro de plaque d'immatriculation dans la liste d'autorisation comme un véhicule connu et que la barrière s'ouvre.

Remarque

Vous pouvez changer le nom de l'une des listes, pour vous adapter à votre cas d'utilisation spécifique.

Recevoir une notification concernant un véhicule non autorisé

Cet exemple explique comment configurer l'application, pour que la caméra envoie une notification lorsqu'un événement se produit.

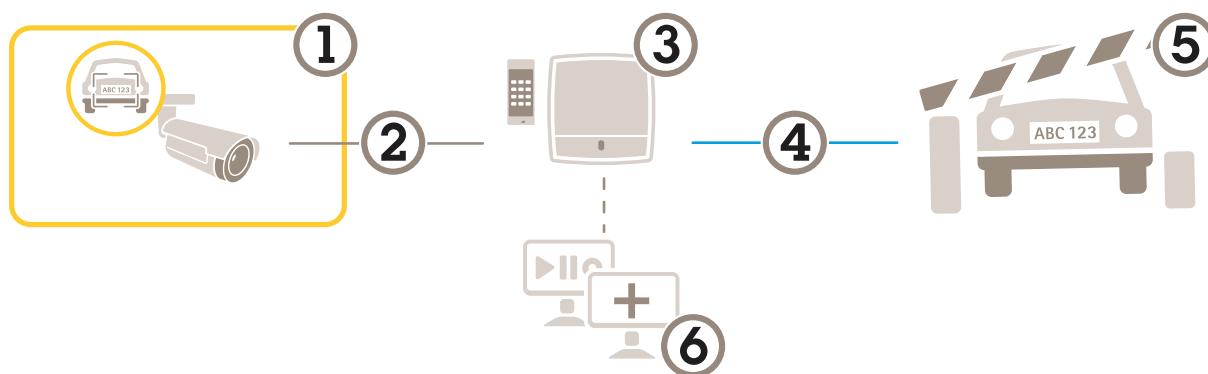
Conditions requises

- Configuration de base effectuée. Cf. .
- 1. Accédez à **List Management (Gestion des listes)**.
- 2. Saisissez le numéro de plaque d'immatriculation dans le champ **Blocklist (Liste de blocage)**.
- 3. Accédez à la page Web de la caméra.
- 4. Allez à **Settings > Events (Paramètres > Événements)** et définissez une règle d'action avec l'application comme condition et une notification comme action.
- 5. Vérifiez que l'application identifie le numéro de plaque d'immatriculation ajouté comme véhicule non autorisé et que la règle d'action s'exécute comme prévu.

Scénario de contrôle d'accès des véhicules

Dans ce scénario de contrôle d'accès des véhicules, l'application peut être connectée à un contrôleur de porte réseau Axis et configurer les règles d'accès, créer un calendrier des heures d'accès et gérer facilement l'accès des véhicules non seulement pour les salariés, mais également, par exemple, pour les visiteurs et les fournisseurs.

Utilisez un système impliquant un contrôleur de porte et un lecteur de carte d'accès pour la sauvegarde. Pour configurer le contrôleur de porte et le lecteur de carte, consultez la documentation utilisateur sur axis.com



- 1 Caméra Axis avec AXIS License Plate Verifier
- 2 Communication IP
- 3 Commande de porte réseau Axis avec lecteur de carte
- 4 Communication E/S
- 5 Barrière
- 6 Logiciel tiers optionnel

Connecter la caméra à un contrôleur de porte

Dans cet exemple, nous avons connecté la caméra à une commande de porte réseau, ce qui signifie que la caméra fonctionne comme un capteur. La caméra transmet les informations au contrôleur qui analyse les informations et déclenche les événements.

Remarque

Lorsque vous passez de AXIS License Plate Verifier à AXIS Entry Manager, assurez-vous d'actualiser les pages Web pour accéder à tous les paramètres.

Conditions requises

- Caméra et contrôleur de porte installés physiquement et connectés au réseau.
- AXIS License Plate Verifier opérationnel sur la caméra.
- Configuration de base effectuée. Cf. .



Comment rendre opérationnelle l'application avec le contrôleur de porte AXIS A1001.

Configuration du matériel sur AXIS Entry Manager

1. Allez sur AXIS Entry Manager et lancez une nouvelle configuration du matériel dans **Configuration**.
2. Dans le menu configuration du matériel, renommez la commande de porte réseau par « Gate controller ».
3. Cliquez sur **Next (Suivant)**.
4. Dans le menu **Configure locks connected to this controller (Configurer les verrous connectés à ce contrôleur)**, désactivez l'option **Door monitor (Moniteur de porte)**.

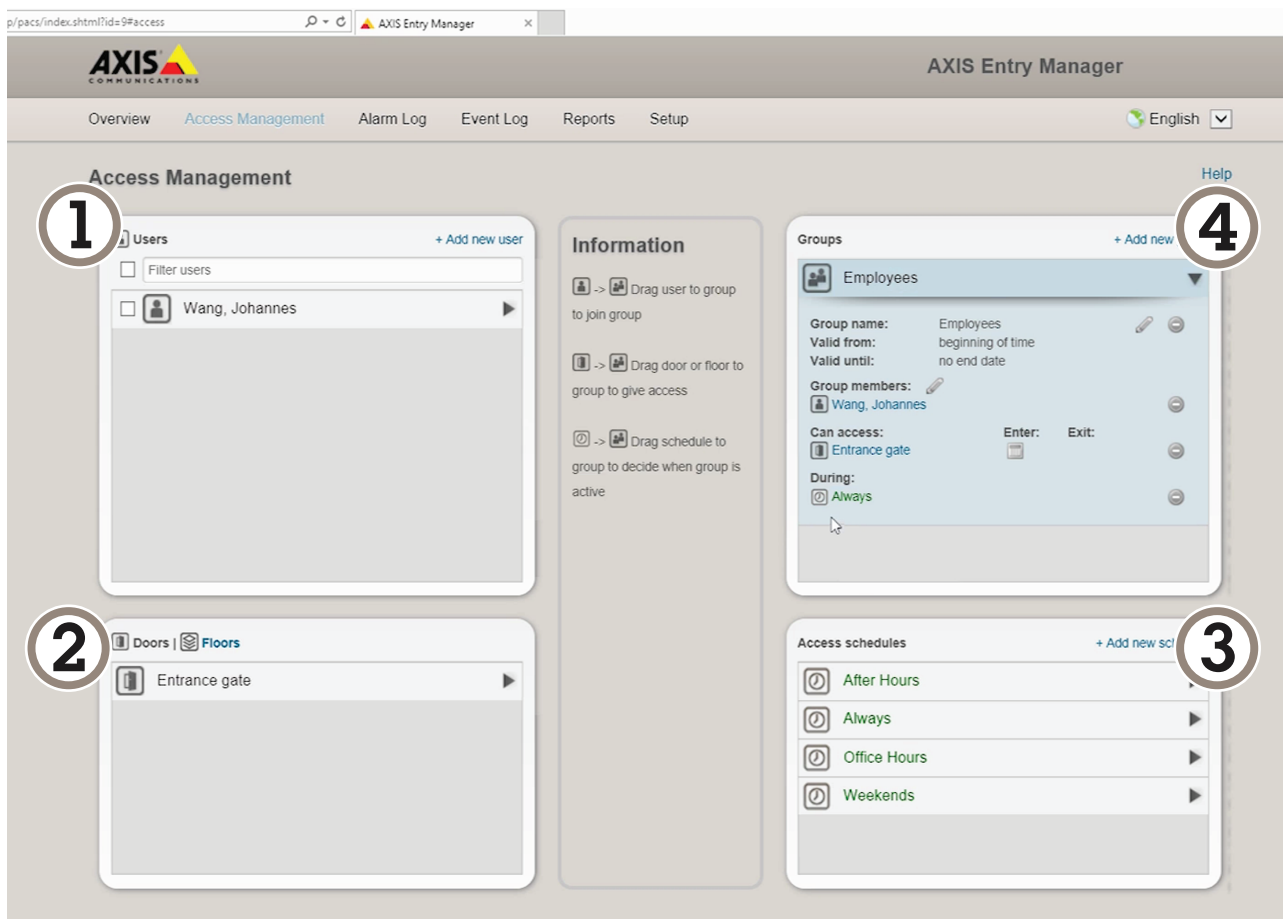
5. Cliquez sur **Next (Suivant)**.
6. Dans le menu **Configure readers connected to this controller (Configurer les lecteurs connectés à ce contrôleur)**, désactivez l'option **Exit reader (Lecteur de sortie)**.
7. Cliquez sur **Finish (Terminer)**.

Configuration sur AXIS License Plate Verifier

1. Allez sur la page Web **AXIS License Plate Verifier**.
2. Accédez à **Settings > Access control (Paramètres > Contrôle d'accès)**.
3. Accédez à **Type** et sélectionnez **Controller (Contrôleur)** dans la liste déroulante.
4. Saisissez les informations suivantes :
 - l'adresse IP du contrôleur au format 192.168.0.0
 - le nom d'utilisateur pour le contrôleur
 - le mot de passe pour le contrôleur
5. Cliquez sur **Connect (Connecter)**.
6. Si la connexion est établie, « Gatecontroller » s'affiche dans la liste déroulante **Network Door Controller name (Nom de contrôleur de porte réseau)**. Sélectionnez « Gatecontroller ».
7. Dans la liste déroulante **Reader name (Nom du lecteur)**, sélectionnez le lecteur connecté à la porte « Gatecontroller », par exemple « Reader Entrance » (Lecteur entrée). Ces noms peuvent être changés dans **AXIS Entry Manager**.
8. Pour activer la connexion, sélectionnez **Turn on integration (Activer l'intégration)**.
9. Saisissez un numéro de plaque d'immatriculation de l'utilisateur, ou utilisez le numéro par défaut, dans le champ de test et cliquez sur **Test integration (Tester l'intégration)**. Vérifiez que le test a réussi.

Configurez les utilisateurs, groupes, portes et programmations dans AXIS Entry Manager

1. Accédez à **AXIS Entry Manager**.
2. Accédez à **Access Management (Gestion des accès)**.
3. Allez dans **Doors > Add identification type (Portes > Ajouter un type d'identification)**.
4. Dans la liste déroulante **Credentials needed (Identifiants nécessaires)**, sélectionnez **License plate only (Plaque d'immatriculation uniquement)**.
5. Pour définir les limites d'utilisation du type d'identification, glissez et déposez une **Programmation** sur la porte.
6. Ajoutez des utilisateurs et, pour chaque utilisateur ajoutez l'identifiant **License plate (Plaque d'immatriculation)**.
7. Cliquez à nouveau sur **Add credential (Ajouter des identifiants)** puis saisissez la plaque d'immatriculation.
8. Cliquez sur **Add new group (Ajouter nouveau groupe)** et ajoutez les informations.
9. Pour ajouter des utilisateurs à un groupe, glissez et déposez les **Users (Utilisateurs)** dans le groupe.
10. Pour autoriser l'accès à certains utilisateurs, glissez et déposez **Door (Porte)** dans le groupe d'utilisateurs.
11. Pour limiter le temps d'accès, glissez et déposez **Schedule (programme)** dans le groupe.



Vue d'ensemble de l'interface utilisateur AXIS Entry Manager.

- 1 Utilisateurs
- 2 Portes
- 3 Programmes
- 4 Groupes d'utilisateurs

Se connecter à AXIS Secure Entry

Cet exemple décrit la connexion d'un contrôleur de porte Axis dans AXIS Camera Station et AXIS Secure Entry avec AXIS Licence Plate Verifier.

Conditions requises

- Caméra et contrôleur de porte installés physiquement et connectés au réseau.
- AXIS License Plate Verifier opérationnel sur la caméra.
- AXIS Camera Station version client 5.49.449 et versions suivantes.
- Configuration de base effectuée. Cf. .

Dans **AXIS Camera Station**, voir *Add a reader (Ajouter un lecteur)*.

Dans l'application **AXIS License Plate Verifier** :

1. Dans l'onglet **Settings (Paramètres)**, allez à **Configuration wizard (Assistant de configuration)** et cliquez sur **Start (Démarrer)**.
2. Sélectionnez **Access Control (Contrôle d'accès)**.
3. Sélectionnez **Secure Entry (Entrée sécurisée)**, puis cliquez sur **Next (Suivant)**.

Dans **AXIS Camera Station** :

4. Tapez l'adresse IP du contrôleur de porte, disponible dans la liste des périphériques dans **AXIS Camera Station > Configuration > Other Devices (Autres périphériques)**.

5. Pour ajouter une clé d'authentification, allez à **AXIS Camera Station > Configuration > Encrypted communication (Communication cryptée)**.
6. Allez à **External Peripheral Authentication Key (Clé d'authentification de périphérique externe)** et cliquez sur **Show authentication key (Afficher la clé d'authentification)**.
7. Cliquez sur **Copy key (Copier la clé)**.

Dans l'application **AXIS License Plate Verifier** :

8. Allez à **Authentication key (Clé d'authentification)** dans l'assistant de configuration et collez la clé.
9. Cliquez sur **Connect (Connecter)**.
10. Sélectionnez **Door controller name (Nom du contrôleur de porte)** dans le menu déroulant.
11. Sélectionnez le **Reader name (Nom du lecteur)** dans le menu déroulant.
12. Cochez **Turn on integration (Activer l'intégration)**.
13. Cliquez sur **Next (Suivant)**.
14. Réglez le domaine d'intérêt. Voir *Régler le domaine d'intérêt, on page 10*.
15. Cliquez sur **Next (Suivant)** deux fois, puis cliquez sur **Finish (Terminer)**.

Scénario de circulation libre avec mesure de la vitesse

Dans un scénario de circulation libre avec mesure de la vitesse, la caméra est appairée à un radar Axis via la technologie bord à bord. La caméra couvre deux voies et lit les plaques d'immatriculation des véhicules qui passent ; le radar appairé couvre les deux mêmes voies pour mesurer la vitesse des véhicules. En outre, l'application *AXIS Speed Monitor* peut visualiser la vitesse maximale dans chaque voie grâce à des incrustations dans la vidéo en direct de la caméra.

Pour en savoir plus sur la technologie bord à bord, consultez *Technologie Edge-to-edge*, on page 53.

Conditions requises :

- Un kit de vérification AXIS License Plate Verifier et un radar *AXIS D2210-VE Radar* installés et connectés au réseau

Configurer le scénario

Le scénario se déroule en quatre étapes : configuration de la caméra, couplage et configuration du radar, et enfin utilisation d'*AXIS Speed Monitor* pour ajouter des incrustations.

Avant de commencer :

- Vérifiez que la caméra et le radar sont orientés vers le même domaine d'intérêt.
- Assurez-vous que la caméra et le radar sont synchronisés. Pour vérifier l'état, allez à **Installation > Time sync status (État de la synchronisation horaire)** sur chaque périphérique.
- Assurez-vous que la deuxième zone de visualisation de la caméra (**View area 2 (Zone de visualisation 2)**) n'est pas utilisée, car le radar l'utilisera après l'appairage.

Configurer la caméra :

1. Configurez la caméra conformément aux instructions figurant dans .
2. Veillez à sélectionner le flux de circulation lorsque vous suivez l'assistant de configuration. Pour en savoir plus, consultez *Flux libre*, on page 8.

Appairer la caméra à un radar :

1. Dans l'interface Web de la caméra, accédez à **System > Edge-to-edge > Radar pairing (Système > Technologie bord à bord > Appairage de radar)**.
2. Saisissez le nom de l'hôte, le nom d'utilisateur et le mot de passe permettant d'accéder au radar.
3. Cliquez sur **Connect (Connecter)** pour appairer les périphériques.
Une fois la connexion établie, les paramètres du radar sont disponibles dans l'interface Web de la caméra.

Remarque

La résolution par défaut du radar couplé est de 1280x720. Conservez la résolution par défaut du radar dans l'interface web de la caméra, et si vous l'ajoutez à un VMS.

Configurer le radar :

1. Dans l'interface Web de la caméra, accédez à **Radar > Scénarios**.
2. Ajoutez un scénario sur le radar qui couvre une voie et un autre scénario qui couvre l'autre voie.
3. Pour les deux scénarios, sélectionnez **Movement in area (Mouvement dans la zone)**, déclenchez un scénario sur **Vehicles (Véhicules)** et définissez une **Speed limit (Limite de vitesse)**.
Pour plus d'informations, allez à *Add scenarios (Ajouter des scénarios)* dans le manuel d'utilisation d' *AXIS D2210-VE Radar*.

Remarque

Pour ajouter des incrustations contenant des informations sur les plaques d'immatriculation via *AXIS License Plate Verifier*, veillez à les ajouter avant d'intégrer des incrustations dans *AXIS Speed Monitor*.

Utilisez *AXIS Speed Monitor* pour ajouter des incrustations de vitesse :

1. Téléchargez et installez *AXIS Speed Monitor* sur votre caméra.

2. Ajoutez une incrustation pour chaque voie qui affiche la vitesse maximale dans la vidéo en direct de la caméra.
Pour obtenir des instructions d'installation et de configuration, consultez le *manuel d'utilisation d'AXIS Speed Monitor*.

Rechercher des événements spécifiques

Utilisez la fonction de recherche pour rechercher des événements à l'aide de plusieurs critères.

1. Veuillez aller à la page web de l'application et sélectionner la page **Search (Rechercher)**.
2. Sélectionnez la date dans les menus du calendrier **From (Du)** et **To (Au)**.
3. Veuillez cliquer sur le menu déroulant **AOI (Domaine d'intérêt)** pour sélectionner le domaine d'intérêt à inclure dans la recherche.
4. Sélectionnez **Direction** pour filtrer par entrée ou par sortie.
5. Saisissez la plaque d'immatriculation dans le champ **Plate (Plaque)**, si vous voulez rechercher une plaque.
6. Pour identifier les plaques d'immatriculation appartenant à un pays spécifique, veuillez sélectionner un pays dans la liste déroulante **Country (Pays)**.
7. Pour filtrer les images en fonction de la vue du véhicule, veuillez sélectionner **Front (Avant)** ou **Rear (Arrière)** dans la liste déroulante **Vehicle view (Vue du véhicule)**.
8. Pour filtrer les résultats de recherche en fonction de la marque, du modèle, du type ou de la couleur du véhicule, veuillez sélectionner ce que vous recherchez dans les menus déroulants **Vehicle details (Détails du véhicule)**.
9. Veuillez cliquer sur **Apply filters (Appliquer les filtres)** pour afficher les résultats de recherche.

Exporter et partager des résultats de recherche

Pour exporter des résultats de recherche sous forme de fichier CSV avec les statistiques à ce moment-là, cliquez sur **Exporter** afin d'enregistrer les résultats sous forme de fichier CSV.

Pour copier l'API sous forme de lien qui pourra être utilisé pour exporter les données vers des systèmes tiers, cliquez sur **Copy search link (Copier le lien de recherche)**.

Intégration

Utiliser des profils pour pousser les événements vers plusieurs serveurs

Avec les profils, vous pouvez pousser un événement vers différents serveurs en utilisant différents protocoles en même temps. Pour utiliser les profils :

1. Veuillez aller à **Integration (Intégration)** et à la page **Push events (Événements push)**.
2. Veuillez sélectionner **Profile 1 (Profil 1)**.
3. Configurez la règle. Cf. *Envoi d'informations sur les événements à un logiciel tiers, on page 43*.
4. Tester la règle.
5. Veuillez sélectionner un nouvel onglet de profil pour configurer une nouvelle règle.

Envoi d'informations sur les événements à un logiciel tiers

Remarque

L'application envoie les informations d'événement au format JSON. Pour plus d'informations, *connectez-vous à l'aide de votre compte MyAxis*, accédez à la *AXIS VAPIX Library* et sélectionnez **AXIS License Plate Verifier**

Cette fonction permet d'intégrer un logiciel tiers en envoyant les données d'événement via TCP ou HTTP POST.

Avant de commencer :

- La caméra doit être installée physiquement et connectée au réseau.
 - AXIS License Plate Verifier doit être opérationnel sur la caméra.
1. Accédez à **Integration (Intégration) > Push events (Événements Push)**.
 2. Sélectionner un profil vierge
 3. Dans la liste déroulante **Protocol (Protocole)**, veuillez sélectionner **HTTP POST**.
 4. Dans le champ **Server URL (URL du serveur)**, entrez l'adresse et le port du serveur au format suivant :
127.0.0.1:8080
 5. Saisissez le nom d'utilisateur et le mot de passe.
 6. Si vous utilisez un proxy, veuillez l'activer et taper le nom d'hôte, le nom d'utilisateur et le mot de passe.
 7. Dans le champ **Device ID (ID du périphérique)**, tapez le nom du périphérique ou laissez-le tel quel.
 8. Veuillez sélectionner la direction de déclenchement des événements push sous **Push conditions (Conditions push)**.
 9. Sous **LPR Event types (Types d'événements de reconnaissance de plaques d'immatriculation)**, sélectionnez une ou plusieurs des options suivantes :
 - **New (Nouveau)** correspond à la première détection d'une plaque d'immatriculation.
 - **Update (Mettre à jour)** est une correction d'un caractère sur une plaque d'immatriculation précédemment détectée ou lorsqu'une direction est détectée alors que la plaque se déplace en étant suivie dans l'image.
 - **Lost (Perdu)** est le dernier événement suivi de la plaque d'immatriculation avant qu'elle sorte de l'image. Il contient également la direction de la plaque d'immatriculation.
 - **Conditional (Conditionnel)** envoie un événement pour un objet lorsque les conditions sont satisfaites.
 10. Pour réduire la bande passante lors de l'utilisation de HTTP POST, vous pouvez sélectionner **Do not send images (Ne pas envoyer d'images)**.
 11. Veuillez activer le **tampon d'événements** afin de mettre les événements en mémoire tampon si le serveur tombe en panne, et de les envoyer lorsque le serveur redevient disponible.

12. Pour inclure le recadrage de la plaque d'immatriculation en plus de l'image si vous avez choisi cette option sous **Retention settings (Paramètres de conservation)**, veuillez sélectionner **Send two images (Envoyer deux images)**.
13. Pour envoyer les événements au format multipart plutôt qu'au format base64, veuillez sélectionner **Multipart**.
14. Veuillez cliquer sur **Test (Tester)** pour tester l'intégration avec une plaque d'immatriculation virtuelle.
15. Pour activer la fonctionnalité, veuillez sélectionner **Activate (Activer)**.

Remarque

Pour pousser les événements à l'aide de HTTP POST, vous pouvez utiliser un en-tête d'autorisation à la place d'un nom d'utilisateur et d'un mot de passe, veuillez aller à **Auth-Header (En-tête d'autorisation)**, et ajouter un chemin à une API d'authentification.

Envoyer des images de plaques d'immatriculation à un serveur

Avec cette fonction, vous pouvez pousser les images des plaques d'immatriculation vers un serveur via FTP.

Avant de commencer :

- La caméra doit être installée physiquement et connectée au réseau.
 - AXIS License Plate Verifier doit être opérationnel sur la caméra.
1. Accédez à **Integration (Intégration) > Push events (Événements Push)**.
 2. Dans la liste déroulante **Protocol (Protocole)**, sélectionnez **FTP**.
 3. Dans le champ **Server URL (URL du serveur)**, saisissez l'adresse du serveur au format suivant : `ftp://10.21.65.77/LPR`.
 4. Tapez le nom d'utilisateur et mot de passe du serveur FTP.
 5. Sélectionnez les modificateurs de chemin d'accès et de nom pour les noms de fichiers.
 6. Dans le champ **Device ID (ID du périphérique)**, tapez le nom du périphérique. Un dossier avec ce nom sera créé pour les images. Les images sont créées selon le format suivant : `horodatage_zone d'intérêt_direction_IDvoiture_texte plaque d'immatriculation_pays.jpg`.
 7. Veuillez sélectionner la direction de déclenchement des événements push sous **Push conditions (Conditions push)**.
 8. Sous **Event types (Types d'événements)**, sélectionnez une ou plusieurs des options suivantes :
 - **New (Nouveau)** correspond à la première détection d'une plaque d'immatriculation.
 - **Update (Mettre à jour)** est une correction d'un caractère sur une plaque d'immatriculation précédemment détectée ou lorsqu'une direction est détectée alors que la plaque se déplace en étant suivie dans l'image.
 - **Lost (Perdu)** est le dernier événement suivi de la plaque d'immatriculation avant qu'elle sorte de l'image. Il contient également la direction de la plaque d'immatriculation.
 - **Conditional (Conditionnel)** envoie un événement pour un objet lorsque les conditions sont satisfaites.

Remarque

La direction n'est incluse que dans le nom de fichier lorsque l'option **Perdu or mettre à jour** est sélectionnée.

9. Veuillez cliquer sur **Test (Tester)** pour tester l'intégration avec une plaque d'immatriculation virtuelle.
10. Pour activer la fonctionnalité, veuillez cliquer sur **Activate (Activer)**.

Remarque

Notez que l'image varie en fonction du type de mode de capture sélectionné, voir *Régler les paramètres de capture d'image, on page 11*.

Remarque

Si les événements push échouent, l'application renverra au serveur jusqu'aux 100 premiers événements ayant échoué.

Lorsque vous utilisez le protocole FTP dans les événements push vers un serveur Windows, n'utilisez pas %c, qui donne la date et l'heure, pour nommer les images. Cela est dû au fait que Windows n'accepte pas les noms définis par la fonction %c pour la date et l'heure. Notez que cela ne pose pas de problème lorsque vous utilisez un serveur Linux.

Intégration directe avec 2N

Cet exemple décrit l'intégration directe avec un périphérique IP 2N.

Configurez un compte sur votre périphérique 2N :

1. Allez à 2N IP Verso.
2. Allez à **Services > HTTP API > Compte 1**.
3. Sélectionnez **Activer le compte**.
4. Sélectionnez **Accès à la caméra**.
5. Sélectionnez **reconnaissance des plaques d'immatriculation**.
6. Copiez l'adresse IP.

Dans l'application AXIS License Plate Verifier :

1. Allez à **Integration (Intégration) > Direct integration (Intégration directe)**.
2. Veuillez sélectionner **2N IP Device (Périphérique IP 2N)**.
3. Ajoutez l'adresse IP ou l'URL au périphérique 2N.
4. Tapez vos nom d'utilisateur et mot de passe.
5. Sélectionnez **Type de connexion**.
6. Sélectionnez l'objet d'utilisation de la **barrière**.
7. Cliquez sur **Enable integration (Activer intégration)**.
8. Veuillez sélectionner la direction des véhicules.
9. Pour activer la fonctionnalité, veuillez sélectionner **Activate (Activer)**.

Pour vérifier l'intégration, cela fonctionne :

1. Allez à 2N IP Verso.
2. Allez à **Status (État) > Events (Événements)**.

Intégration avec Genetec Security Center

Cet exemple décrit la configuration d'une intégration directe avec le Security Center de Genetec.

Dans le Genetec Security Center :

1. Accédez à **Overview (Aperçu)**.
2. Vérifiez que **Base de données, Service d'annuaire et Licence** sont en ligne. Si ce n'est pas le cas, exécutez tous les services Genetec et SQLEXPRESS dans Windows.
3. Accédez à **Outil de configuration Genetec > Plug-ins**.
4. Cliquez sur **Ajouter une entité**.
5. Accédez à **Plug-in** et sélectionnez **Plug-in LPR**.
6. Cliquez sur **Next (Suivant)**.
7. Cliquez sur **Next (Suivant)**.
8. Cliquez sur **Next (Suivant)**.
9. Sélectionnez le plug-in LPR que vous avez ajouté et accédez à **Sources de données**.

Sous ALPR lit l'API :

10. Cochez l'option **Activé**.
11. Dans le champ **Nom**, entrez : **API REST de plug-in**.
12. Dans le champ **API path prefix** (Préfixe du chemin de l'API), entrez : **lpr**.
13. Dans le champ **Port REST**, sélectionnez **443**.
14. Dans le champ **Hôte WebSDK**, entrez : **localhost**.
15. Dans le champ **Port WebSDK**, sélectionnez **443**.
16. Cochez la case **Autoriser les certificats auto-signés**.

Sous **Source de données des événements du centre de sécurité** :

17. Cochez l'option **Activé**.
18. Dans le champ **Nom**, entrez **Événements Lpr du centre de sécurité**.
19. Dans la section **Fréquence de traitement**, sélectionnez **5 secondes** dans le menu déroulant.
20. Accédez à l'onglet **Puits de données**.
21. Cliquez sur **+**.
22. Dans le champ **Type**, sélectionnez **Base de données**.
23. **Choisir et configurer la base de données**.
 - Cochez l'option **Activé**.
 - Dans la section **Source**, sélectionnez **API REST de plug-in et Événements ALPR natifs**.
 - Dans le champ **Nom**, entrez **Base de données de lectures**.
 - Dans la section **Inclure**, sélectionnez **Lectures, Hits et Images**.
 - Accédez à l'onglet **Ressources**.
 - Cliquez sur **Supprimer la base de données**, puis sur **Créer une base de données**.

Créer un utilisateur d'API :

24. Accédez à **Outil de configuration > Gestion des utilisateurs**.
25. Cliquez sur **Ajouter une entité**.
26. Sélectionnez **Utilisateur**.
27. Saisissez un nom d'utilisateur et un mot de passe. Laissez les autres champs inchangés.
28. Sélectionnez l'utilisateur ajouté et accédez à l'onglet **Privilèges**.
29. Vérifiez que tout ce qui se trouve sous **Privilèges d'application**.
30. Cochez la case **API de lecture ALPR tierce partie**.
31. Cliquez sur **Appliquer**.

Dans l'application **AXIS License Plate Verifier** :

1. Veuillez aller à **Integration (Intégration) > Direct integration (Intégration directe)**.
2. Veuillez sélectionner **Genetec Security Center**.
3. Dans le champ **URL/IP**, entrez votre adresse selon ce modèle : `https://server-address/api/v1/lpr/lpringestion/reads`.
4. Entrez vos nom d'utilisateur et mot de passe Genetec.
5. Sélectionnez **Type de connexion**.
6. Pour activer la fonctionnalité, veuillez sélectionner **Activate (Activer)**.
7. Veuillez cliquer sur **Test (Tester)** pour tester l'intégration avec une plaque d'immatriculation virtuelle.
8. Si vous avez choisi **HTTPS**, veuillez aller à l'onglet **Settings (Paramètres)**.
9. Sous **Sécurité > HTTPS**.
10. Sélectionnez **Auto-signé**, ou **Signé par l'AC** en fonction des paramètres dans Genetec Security Center.

Dans le Genetec Security Center :

1. Accédez à **Bureau Genetec Security**.
2. Sous **Investigation**, cliquez sur **Lectures**.
3. Accédez à l'onglet **Lectures**.
4. Filtrez le résultat en fonction de vos besoins.
5. Cliquez sur **Générer un rapport**.

Remarque

Vous pouvez également consulter la documentation de Genetec sur l'intégration de plug-ins ALPR tiers. *Vous pouvez le faire ici (inscription obligatoire).*

L'interface web

Pour en savoir plus sur toutes les fonctionnalités et tous les paramètres disponibles dans l'interface web des périphériques équipés d'AXIS OS, consultez l'*Aide sur l'interface web d'AXIS OS*.

En savoir plus

Zone d'affichage

Une zone de visualisation est une partie détournée d'une vue d'ensemble. Vous pouvez diffuser et stocker des zones de visualisation au lieu de la vue complète afin de réduire les besoins en bande passante et en stockage. Si vous activez la fonction PTZ pour une zone de visualisation, vous pouvez effectuer un panoramique, une inclinaison ou un zoom à l'intérieur de celle-ci. En utilisant les zones de visualisation, vous pouvez supprimer des parties de la vue complète, par exemple, le ciel.

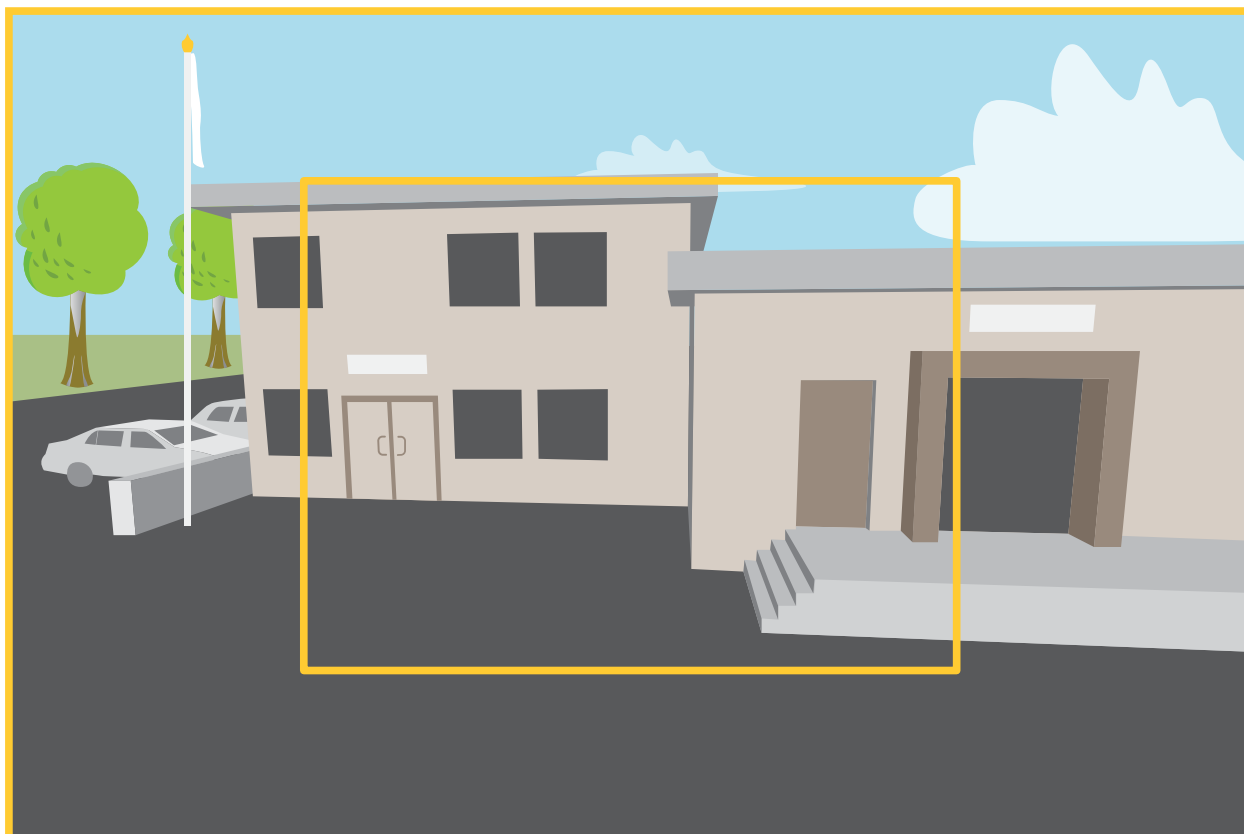
Lorsque vous configurez une zone de visualisation, nous vous recommandons de définir la résolution du flux vidéo sur la même taille ou sur une taille inférieure à celle de la zone de visualisation. Si vous définissez la résolution de flux vidéo plus grande que la taille de la zone de visualisation, elle implique une vidéo mise à l'échelle numériquement après la capture du capteur, qui nécessite plus de bande passante sans ajouter les informations sur l'image.

Modes de capture

Un mode de capture est une configuration prédéfinie qui définit la manière dont la caméra capture les images.

- Le paramètre du mode de capture peut affecter la résolution maximale et la fréquence d'images maximale disponibles dans le périphérique.
- Le mode de capture avec une résolution inférieure à la résolution maximale peut réduire le champ de vision.
- Le mode de capture influe également sur la vitesse d'obturation, qui à son tour influe sur la sensibilité à la lumière. En effet, un mode de capture avec une fréquence d'image maximale élevée présente une sensibilité à la lumière réduite, et inversement.
- Certains modes de capture ne permettent pas d'utiliser la fonction WDR.

Le mode de capture à plus faible résolution peut être échantillonné à partir de la résolution d'origine, ou être recadré à partir de l'original, auquel cas le champ de vision peut également être affecté.



L'image montre comment le champ de vision et le rapport d'aspect peuvent changer entre deux modes de capture différents.

Le mode de capture à choisir dépend des exigences en matière de fréquence d'images et de résolution de la configuration de surveillance spécifique. Pour connaître les spécifications des modes de capture disponibles, consultez la fiche technique du produit sur le site axis.com.

Mise au point à distance et zoom

La fonction de mise au point et de zoom à distance vous permet de régler la mise au point et le zoom de votre caméra depuis un ordinateur. Il s'agit d'un moyen pratique pour s'assurer que la mise au point, l'angle de vue et la résolution de la scène sont optimisés sans devoir se rendre sur le lieu d'installation de la caméra.

Masques de confidentialité

Un masque de confidentialité est une zone définie par l'utilisateur qui empêche les utilisateurs de visualiser une partie de la zone surveillée. Dans le flux vidéo, les masques de confidentialité se présentent sous forme de blocs de couleur opaque.

Un masque de confidentialité est une zone définie par l'utilisateur couvrant une partie de la zone surveillée. Les masques de confidentialité se présentent sous forme de blocs de couleur opaque ou de mosaïque sur le flux de données vidéo.

Vous verrez le masque de confidentialité sur toutes les captures d'écran, vidéos enregistrées et flux en direct.

Vous pouvez utiliser l'interface de programmation (API) VAPIX® pour masquer les masques de confidentialité.

Important

Si vous utilisez plusieurs masques de confidentialité, cela peut affecter les performances du produit.

Vous pouvez créer plusieurs masques de confidentialité. Chaque masque peut comporter de 3 à 10 points d'ancrage.

Important

Définissez le zoom et la mise au point avant de créer un masque de confidentialité.

Incrustations

Remarque

Les incrustations ne sont pas incluses dans le flux vidéo lorsque vous utilisez des appels SIP.

Les incrustations se superposent au flux vidéo. Elles sont utilisées pour fournir des informations supplémentaires lors des enregistrements, telles que des horodatages, ou lors de l'installation et de la configuration d'un produit. Vous pouvez ajouter du texte ou une image.

L'indicateur de flux vidéo est un autre type d'incrustation. Il vous indique que le flux vidéo est en direct.

Remarque

Les incrustations sont incluses dans tous les flux vidéo, à l'exception des appels SIP lorsque la connexion s'effectue via PoE classe 3.

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.

AV1

AV1 (AOMedia Video 1) est un format de codage vidéo sans licence optimisé pour la diffusion en continu. AV1 active les flux de données vidéo de haute qualité, même dans les environnements à bande passante limitée. En réduisant le débit binaire d'une vidéo, AV1 préserve la qualité de la vidéo tout en minimisant l'utilisation des données.

AV1 prend en charge les principaux navigateurs, systèmes d'exploitation d'ordinateurs et plates-formes mobiles.

Remarque

AV1 nécessite une plus grande puissance de traitement pour l'encodeur et le décodeur par rapport à d'autres codecs.

Quel est le lien entre les paramètres d'image, de flux et de profil de flux ?

L'onglet **Image (Image)** contient les paramètres de la caméra qui affectent tous les flux vidéo provenant du produit. Si vous modifiez un élément dans cet onglet, cela affecte immédiatement tous les flux vidéo et tous les enregistrements.

L'onglet **Stream (Flux)** contient les paramètres des flux vidéo. Vous obtenez ces paramètres si vous sollicitez un flux vidéo provenant du produit sans spécifier la résolution ou la fréquence d'image, par exemple. Lorsque vous modifiez les paramètres dans l'onglet **Stream (Flux)**, cela n'affecte pas les flux en cours, mais prend effet lorsque vous lancez un nouveau flux.

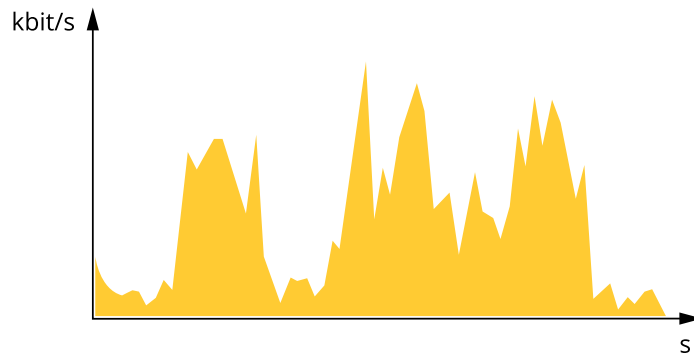
Les paramètres **Stream profiles (Profils de flux)** outrepassent les paramètres de l'onglet **Stream (Flux)**. Si vous sollicitez un flux avec un profil de flux spécifique, le flux contient les paramètres de ce profil. Si vous sollicitez un flux sans spécifier de profil de flux ou sollicitez un profil de flux qui n'existe pas dans le produit, le flux contient les paramètres de l'onglet **Stream (Flux)**.

Commande du débit binaire

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

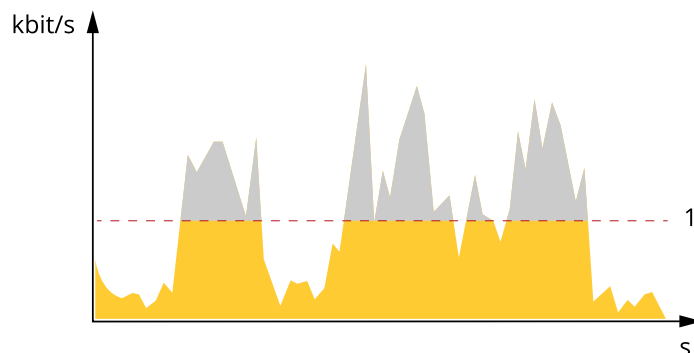
Débit binaire variable (VBR)

Le débit binaire variable permet de faire varier la consommation de bande passante en fonction du niveau d'activité dans la scène. Plus l'activité est intense, plus vous avez besoin de bande passante. Avec un débit binaire variable, une qualité d'image constante est garantie, mais vous devez être sûr d'avoir des marges de stockage.



Débit binaire maximal (MBR)

Le débit binaire maximal permet de définir un débit binaire cible pour gérer les limitations de débit binaire du système. Vous pouvez observer une baisse de la qualité d'image ou de la fréquence d'images lorsque le débit binaire instantané est maintenu en dessous du débit binaire cible spécifié. Vous pouvez choisir de donner la priorité soit à la qualité d'image, soit à la fréquence d'image. Nous vous conseillons de configurer le débit binaire cible sur une valeur plus élevée que le débit binaire attendu. Vous bénéficiez ainsi d'une marge si l'activité dans la scène est élevée.

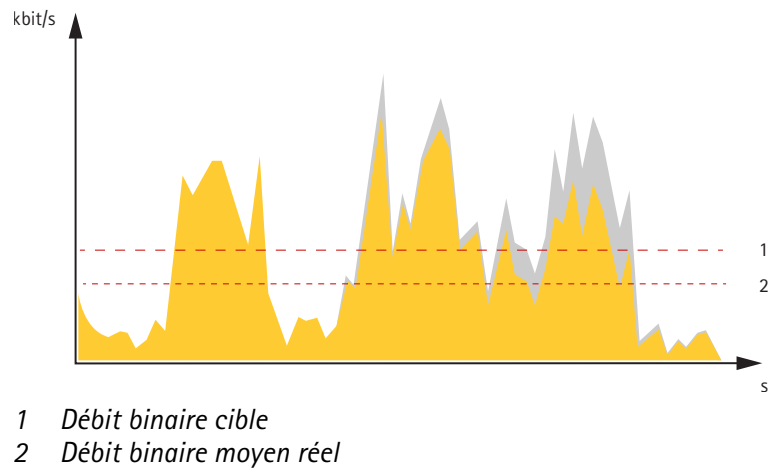


1 Débit binaire cible

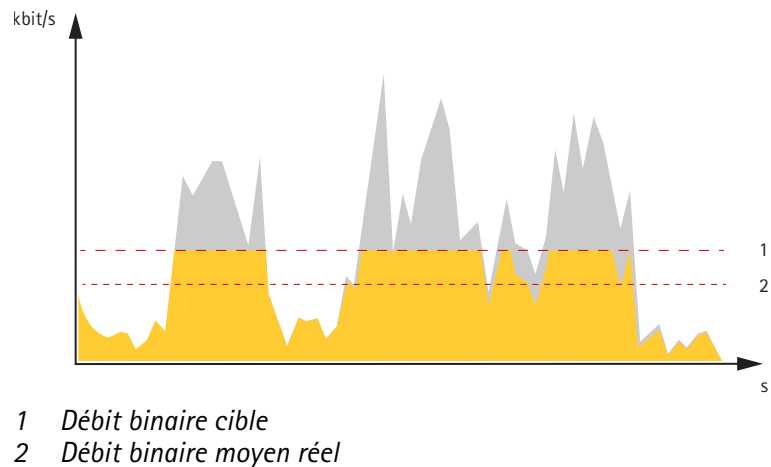
Débit binaire moyen (ABR)

Avec le débit binaire moyen, le débit binaire est automatiquement ajusté sur une période de temps plus longue. Vous pouvez ainsi atteindre la cible spécifiée et obtenir la meilleure qualité vidéo en fonction du stockage disponible. Le débit binaire est plus élevé dans les scènes présentant une activité importante que dans les scènes statiques. Vous avez plus de chances d'obtenir une meilleure qualité d'image dans les scènes avec beaucoup d'activité si vous utilisez l'option de débit binaire moyen. Vous pouvez définir le stockage total requis pour stocker le flux vidéo pendant une durée spécifiée (durée de conservation) lorsque la qualité d'image est ajustée pour atteindre le débit binaire cible spécifié. Spécifiez les paramètres du débit binaire moyen de l'une des façons suivantes :

- Pour calculer l'estimation du stockage nécessaire, définissez le débit binaire cible et la durée de conservation.
- Pour calculer le débit binaire moyen en fonction du stockage disponible et de la durée de conservation requise, utilisez la calculatrice de débit binaire cible.



Vous pouvez également activer le débit binaire maximum et spécifier un débit binaire cible dans l'option de débit binaire moyen.



Technologie Edge-to-edge

La technologie bord à bord permet aux périphériques IP de communiquer directement entre eux. Elle offre une fonction d'appairage intelligente entre, par exemple, des caméras Axis et des produits audio ou radar Axis.

Remarque

Veuillez vous assurer que les périphériques appairés utilisent la même version d'AXIS OS.

Pour plus d'informations, consultez le livre blanc « Edge-to-edge technology » (Technologie de bout en bout) à l'adresse whitepapers.axis.com/edge-to-edge-technology.

Appairage réseau

Grâce à l'appairage réseau complet, vous pouvez connecter votre caméra à un périphérique Axis compatible doté de fonctionnalités d'éclairage et de sirène et bénéficier de ses fonctionnalités intégrées.

Analyses et applis

Les analyses et applis vous permettent de profiter davantage de votre périphérique Axis. AXIS Camera Application Platform (ACAP) est une plate-forme ouverte qui permet à des tiers de développer des analyses et autres applis pour les périphériques Axis. Les applis peuvent être préinstallées sur le périphérique, et sont téléchargeables gratuitement ou moyennant le paiement d'une licence.

Pour rechercher les manuels d'utilisation des analyses et applis Axis, allez à help.axis.com.

Remarque

- Vous pouvez exécuter plusieurs applications simultanément, mais il est possible que certaines applications ne soient pas compatibles. Il est possible que certaines combinaisons d'applications

nécessitent trop de puissance de calcul ou de ressources mémoire lorsqu'elles sont exécutées en parallèle. Vérifiez que les applis sont parfaitement compatibles entre elles avant de les déployer.

AXIS Object Analytics

AXIS Object Analytics est une application d'analyse préinstallée sur la caméra. Elle détecte les objets en mouvement dans la scène et les classe, par exemple, en tant que personnes ou véhicules. Vous pouvez configurer l'application pour qu'elle envoie des alarmes sur différents types d'objets. Pour en savoir plus sur le fonctionnement de l'application, consultez le *manuel d'utilisation d'AXIS Object Analytics*.

AXIS Image Health Analytics

AXIS Image Health Analytics est une application basée sur l'IA qui peut être utilisée pour détecter les dégradations d'images ou les tentatives de sabotage. L'application analyse et apprend le comportement de la scène pour détecter le flou ou la sous-exposition de l'image, ou pour détecter une vue obstruée ou redirigée. Vous pouvez configurer l'application pour qu'elle envoie des événements pour chacune de ces détections et déclenche des actions par le biais du système d'événements de la caméra ou d'un logiciel tiers.

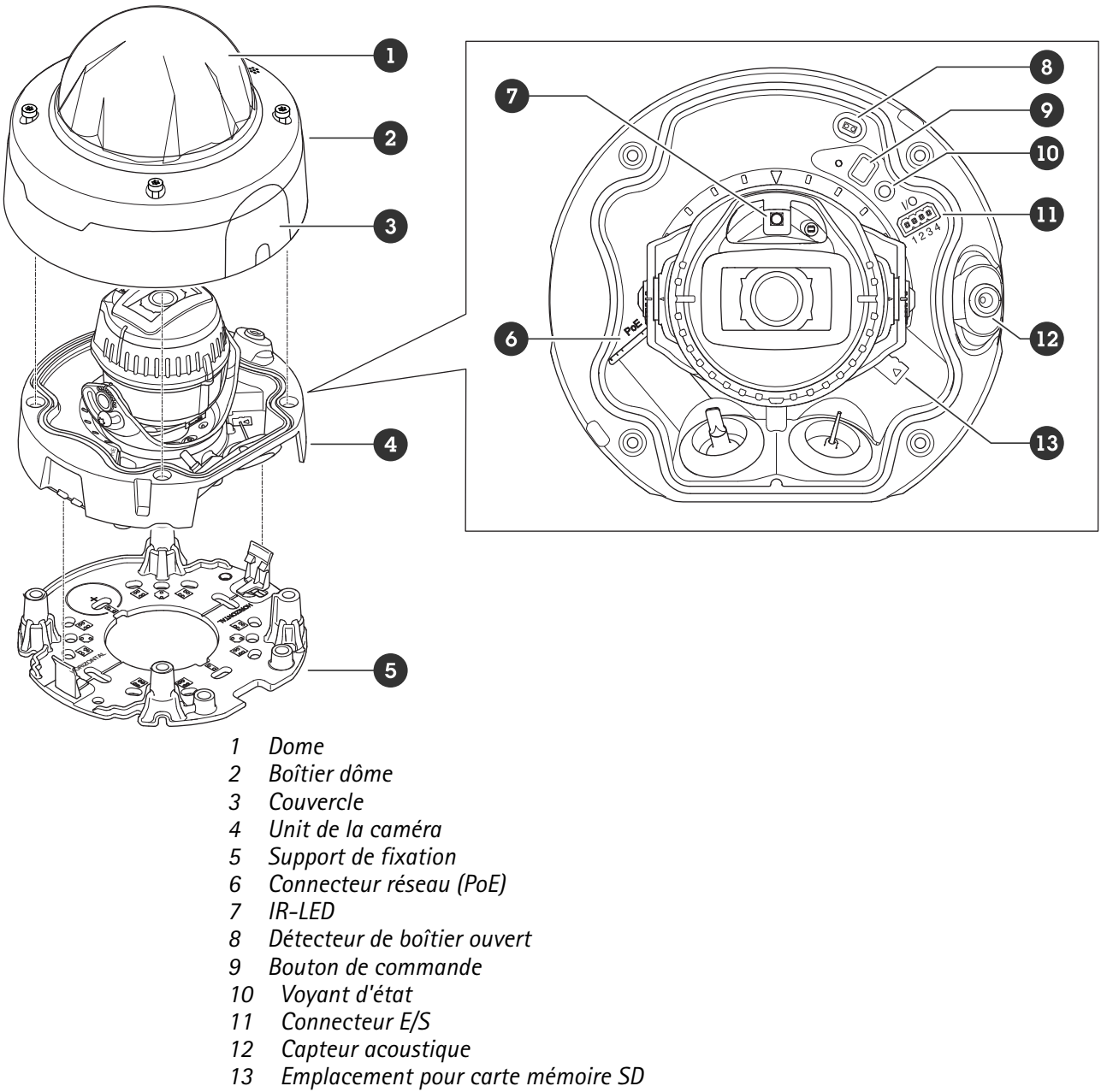
Pour plus d'informations sur le fonctionnement de l'application, consultez le *manuel d'utilisation d'AXIS Object Analytics*.

Visualisation des métadonnées

Des métadonnées analytiques sont disponibles pour les objets en mouvement dans la scène. Les classes d'objets pris en charge sont visualisées dans le flux vidéo via une boîte de mesure entourant l'objet, ainsi que des informations sur le type d'objet et le niveau de confiance de la classification. Pour en savoir plus sur la configuration et la consommation des métadonnées analytiques, consultez le *guide d'intégration AXIS Scene Metadata*.

Caractéristiques techniques

Gamme de produits



Voyants DEL

DEL d'état	Indication
Éteint	Branchement et fonctionnement normal.
Vert	Vert et fixe pendant 10 secondes pour indiquer un fonctionnement normal après le démarrage.
Orange	Fixe pendant le démarrage. Clignote pendant les mises à niveau du logiciel du périphérique ou le rétablissement des valeurs par défaut configurées en usine.
Orange / Rouge	Clignote en orange/rouge en cas d'indisponibilité ou de perte de la connexion réseau.

Emplacement pour carte SD

AVIS

- Risque de dommages à la carte SD. N'utilisez pas d'outils tranchants ou d'objets métalliques pour insérer ou retirer la carte SD, et ne forcez pas lors son insertion ou de son retrait. Utilisez vos doigts pour insérer et retirer la carte.
- Risque de perte de données et d'enregistrements corrompus. Démontez la carte SD de l'interface web du périphérique avant de la retirer. Ne retirez pas la carte SD lorsque le produit est en fonctionnement.

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. *Réinitialiser les paramètres par défaut*, on page 59.

Connecteurs

Connecteur réseau

Connecteur Ethernet RJ45 avec alimentation par Ethernet (PoE).

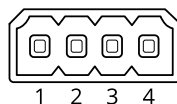
Connecteur E/S

Utilisez le connecteur d'E/S avec des périphériques externes, associés aux applications telles que la détection de mouvement, le déclenchement d'événements et les notifications d'alarme. En plus du point de référence 0 V CC et de l'alimentation (sortie 12 V CC), le connecteur d'E/S fournit une interface aux éléments suivants :

Entrée numérique – Pour connecter des périphériques 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.

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

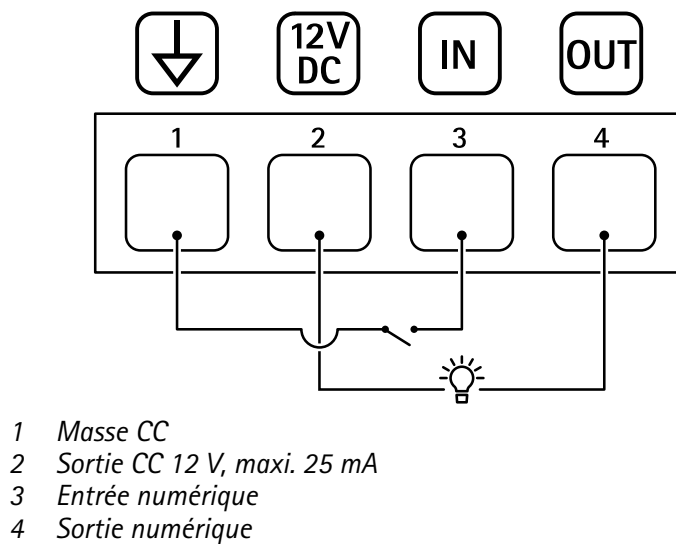
Bloc terminal à 4 broches



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:



Nettoyer votre périphérique

AVIS

- Évitez de nettoyer en cas de lumière directe du soleil ou à des températures élevées, car cela peut entraîner des taches.
1. Pour éviter les taches, séchez le périphérique avec un chiffon propre et non abrasif.

Pour plus d'informations sur le nettoyage des périphériques Axis, consultez le livre blanc *Résistance chimique aux produits de nettoyage courants*.

Recherche de panne

Réinitialiser les paramètres par défaut

▲ AVERTISSEMENT

⚠ Ce produit est susceptible d'émettre un rayonnement optique dangereux. Cela peut être nocif pour les yeux. Ne regardez jamais directement la lampe en fonctionnement.

Important

La restauration des paramètres par défaut doit être effectuée avec prudence. Cette opération restaure tous les paramètres par défaut, y compris l'adresse IP.

Remarque

La caméra a été préconfigurée avec AXIS License Plate Verifier. Si vous restaurez les paramètres par défaut, vous devez réinstaller la clé de licence. Cf. .

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. *Gamme de produits*, on page 55.
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 12.0 ou d'une version ultérieure : 192.168.0.90/24
5. Utilisez les logiciels d'installation et de gestion pour attribuer une adresse IP, configurer le mot de passe et accéder au périphérique.
Les logiciels d'installation et de gestion sont disponibles sur les pages d'assistance du site axis.com/support.

Vous pouvez également rétablir les paramètres d'usine par défaut via l'interface web du périphérique. Accédez à **Maintenance > Factory default (Valeurs par défaut)** et cliquez sur **Default (Par défaut)**.

Options d'AXIS OS

Axis permet de gérer le logiciel du périphérique conformément au support actif ou au support à long terme (LTS). Le support actif permet d'avoir continuellement accès à toutes les fonctions les plus récentes du produit, tandis que le support à long terme offre une plateforme fixe avec des versions périodiques axées principalement sur les résolutions de bogues et les mises à jour de sécurité.

Il est recommandé d'utiliser la version d'AXIS OS du support actif si vous souhaitez accéder aux fonctions les plus récentes ou si vous utilisez des offres système complètes d'Axis. Le support à long terme est recommandé si vous utilisez des intégrations tierces, qui ne sont pas continuellement validées par rapport au dernier support actif. Avec le support à long terme, les produits peuvent assurer la cybersécurité sans introduire de modification fonctionnelle ni affecter les intégrations existantes. Pour plus d'informations sur la stratégie de logiciel du périphérique Axis, consultez axis.com/support/device-software.

Vérifier la version actuelle d'AXIS OS

Le système Axis OS utilisé détermine la fonctionnalité de nos périphériques. Lorsque vous devez résoudre un problème, nous vous recommandons de commencer par vérifier la version actuelle d'AXIS OS. En effet, il est possible que la toute dernière version contienne un correctif pouvant résoudre votre problème.

Pour vérifier la version actuelle d'AXIS OS :

1. Allez à l'interface web du périphérique > **Status (Statut)**.
2. Sous **Device info (Informations sur les périphériques)**, consultez la version d'AXIS OS.

Mettre à niveau AXIS OS

Important

- Lorsque vous effectuez une mise à niveau du logiciel du périphérique, vos paramètres préconfigurés et personnalisés sont sauvegardés. Axis Communications AB ne peut garantir que les paramètres seront sauvegardés, même si les fonctionnalités sont disponibles dans la nouvelle version d'AXIS OS.
- À partir d'AXIS OS 12.6, il est nécessaire d'installer toutes les versions LTS entre la version actuelle de votre périphérique et la version cible. Par exemple, si la version actuelle du logiciel du périphérique est AXIS OS 11.2, il est nécessaire d'installer la version LTS AXIS OS 11.11 avant de pouvoir effectuer une mise à niveau du périphérique vers AXIS OS 12.6. Pour obtenir plus d'informations, veuillez consulter *AXIS OS Lifecycle guide: Upgrade path (Guide sur la durée de vie d'AXIS OS : procédure de mise à niveau)*.
- 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.

Vous pouvez utiliser AXIS Device Manager pour mettre à niveau plusieurs périphériques en même temps. Pour en savoir plus, consultez axis.com/products/axis-device-manager.

Problèmes techniques et solutions possibles

Problèmes de mise à niveau d'AXIS OS

La mise à niveau d'AXIS OS a échoué

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

Impossible de définir l'adresse IP

- Si l'adresse IP désignée pour le 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 peut-être utilisée par un autre périphérique. Pour vérifier :
 1. Déconnectez le périphérique Axis du réseau.
 2. Dans une fenêtre de commande/DOS, tapez `ping` et l'adresse IP du périphérique.
 3. Si vous recevez `Reply from <IP address>: bytes=32; time=10... bytes=32; time=10...`, cela pourrait 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.
 4. 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.
- Il est possible qu'il y ait un conflit d'adresse IP 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 veut dire que si un autre périphérique utilise la même adresse IP statique par défaut, il pourrait y avoir des problèmes d'accès au périphérique.

Problèmes d'accès au périphérique

Impossible de se connecter lors de l'accès au périphérique à partir d'un navigateur

Lorsque le protocole HTTPS est activé, assurez-vous d'utiliser le protocole approprié (HTTP ou HTTPS) lorsque vous essayez de vous connecter. Il est possible que vous deviez taper manuellement `http` ou `https` dans le champ d'adresse du navigateur.

Si vous avez perdu le mot de passe pour le compte root, il est nécessaire de réinitialiser le périphérique aux paramètres des valeurs par défaut. Concernant les instructions, consultez *Réinitialiser les paramètres par défaut, on page 59*.

L'adresse IP a été modifiée par DHCP.

Les adresses IP obtenues auprès d'un serveur DHCP sont dynamiques et pourraient 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).

Vous pouvez attribuer une adresse IP statique manuellement si nécessaire. 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 navigateur n'est pas pris en charge.

Pour obtenir une liste des navigateurs recommandés, consultez *Prise en charge navigateur, on page 4*.

Impossible d'accéder au périphérique depuis l'extérieur

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 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.

Problèmes de flux

La multidiffusion H.264 est accessible aux clients locaux uniquement.

Vérifiez si votre routeur prend en charge la multidiffusion ou si vous devez configurer les paramètres du routeur entre le client et le périphérique. Vous devrez peut-être augmenter la valeur TTL (Durée de vie).

Aucune multidiffusion H.264 ne s'affiche sur le client.

Vérifiez auprès de votre administrateur réseau que les adresses de multidiffusion utilisées par le périphérique Axis sont valides pour votre réseau.

Vérifiez auprès de votre administrateur réseau qu'aucun pare-feu n'empêche le visionnage.

Le rendu des images H.264 est médiocre.

Utilisez toujours le pilote de carte graphique le plus récent. Vous pouvez généralement télécharger les pilotes le plus récents sur le site Web du fabricant.

La saturation des couleurs est différente en H.264 et en Motion JPEG.

Modifiez les paramètres de votre carte graphique. Consultez la documentation de l'adaptateur pour plus d'informations.

La fréquence d'image est inférieure à la valeur attendue.

- Cf. *Facteurs ayant un impact sur la performance, on page 63*.
- Réduisez le nombre d'applications exécutées sur l'ordinateur client.
- Limitez le nombre d'utilisateurs simultanés.
- Vérifiez auprès de votre administrateur réseau que la bande passante disponible est suffisante.
- Réduisez la résolution d'image.
- Connectez-vous à l'interface web du périphérique et définissez un mode de capture donnant la priorité à la fréquence d'image. Le passage à un mode de capture donnant la priorité à la fréquence d'images peut réduire la résolution maximale selon le périphérique utilisé et les modes de capture disponibles.

Impossible de sélectionner l'encodage H.265 dans la vidéo en direct.

Les navigateurs Web ne prennent pas en charge le décodage H.265. Utilisez un système de gestion vidéo ou une application prenant en charge l'encodage H.265.

Problèmes avec MQTT

Connexion impossible via le port 8883 avec MQTT sur SSL

Le pare-feu bloque le trafic utilisant le port 8883, car il est considéré comme non sécurisé.

Dans certains cas, le serveur/courtier ne fournit pas de port spécifique pour la communication MQTT. Il pourrait 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.

Si vous ne trouvez pas les informations dont vous avez besoin ici, consultez la section consacrée au dépannage sur la page axis.com/support.

Facteurs ayant un impact sur la performance

Lors de la configuration de votre système, il est important de tenir compte de l'impact de différents réglages et situations sur la performance. Certains facteurs affectent la bande passante (débit binaire), d'autres affectent la fréquence d'images et certains affectent les deux.

Les facteurs les plus importants à prendre en considération :

- Une résolution d'image élevée ou un niveau de compression réduit génère davantage de données dans les images, ce qui a un impact sur la bande passante.
- La rotation de l'image dans l'interface graphique peut augmenter la charge de l'UC du produit.
- L'accès par un grand nombre de clients Motion JPEG ou de clients H.264/H.265/AV1 en monodiffusion affecte la bande passante.
- L'affichage simultané de flux différents (résolution, compression) par des clients différents affecte la fréquence d'image et la bande passante.
Dans la mesure du possible, utilisez des flux identiques pour maintenir une fréquence d'image élevée. Vous pouvez utiliser des profils de flux pour vous assurer que les flux sont identiques.
- L'accès simultané à des flux vidéo avec différents codecs affecte à la fois la fréquence d'image et la bande passante. Pour des performances optimales, utilisez des flux avec le même codec.
- Une utilisation intensive des paramètres d'événements affecte la charge de l'unité centrale du produit qui, à son tour, affecte la fréquence d'image.
- L'utilisation du protocole HTTPS peut réduire la fréquence d'image, notamment dans le cas d'un flux vidéo Motion JPEG.
- Une utilisation intensive du réseau en raison de l'inadéquation des infrastructures affecte la bande passante.
- L'affichage sur des ordinateurs clients peu performants nuit à la performance perçue et affecte la fréquence d'image.
- L'exécution simultanée de plusieurs applications de la plateforme d'applications AXIS Camera (ACAP) peut affecter la fréquence d'image et les performances globales.

Contacter l'assistance

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

Cybersécurité

La cybersécurité contribue à la réussite du cycle de vie des produits tout en minimisant les risques. Vous trouverez des informations détaillées et de la documentation sur notre approche en matière de cybersécurité à l'adresse suivante : axis.com/about-axis/cybersécurité. Veuillez suivre les consignes de cybersécurité ci-dessous pour recevoir les notifications de sécurité d'Axis concernant vos produits et pour effectuer la configuration de votre produit de manière à garantir un cycle de vie et une mise hors service sécurisés.

Sur le site *Axis Trust Center*, vous trouverez des informations sur la manière dont Axis met en œuvre la conformité en matière de sécurité, la transparence, la protection des données et la confidentialité.

La gestion des vulnérabilités

Axis est une *autorité de numérotation CVE (Common Vulnerability and Exposures) (CNA)*. Afin de réduire au minimum les risques d'exposition, nous respectons les normes du secteur lors de l'identification et de la correction des vulnérabilités de nos dispositifs, logiciels et services. Pour plus d'informations sur notre politique de gestion des vulnérabilités ou pour signaler une vulnérabilité, veuillez consulter axis.com/vulnerability-management.

Notifications de sécurité

Abonnez-vous aux e-mails de notification de sécurité d'Axis à l'adresse axis.com/security-notification-service. Nous vous enverrons des informations concernant les vulnérabilités, les avis de sécurité correspondants et d'autres questions liées à la sécurité de votre produit Axis.

Cycle de vie du produit en sécurité

Axis minimise les risques tout au long du cycle de vie de ses produits grâce à une gestion sécurisée de ce cycle. Consultez nos guides de renforcement de la sécurité sur help.axis.com pour configurer et faire fonctionner vos produits Axis de manière plus sécurisée, et pour obtenir des informations sur :

Première utilisation sécurisée – Les produits Axis sont configurés avec un niveau de protection élevé par défaut afin de garantir une mise en service sécurisée et des communications cryptées dès le départ.

Utilisation prévue et erreurs de configuration courantes – Nos guides fournissent des informations sur l'utilisation prévue des produits Axis, y compris les erreurs courantes de configuration et les mauvaises pratiques en matière de sécurité qu'il convient d'éviter.

Gestion des vulnérabilités et transparence de la chaîne d'approvisionnement – Une liste des composants du logiciel (SBOM) est publiée à chaque nouvelle version du logiciel sur axis.com afin de signaler les vulnérabilités et d'améliorer la transparence de la chaîne d'approvisionnement.

Mise hors service et effacement sécurisé des données – Pour mettre hors service un produit en toute sécurité lorsqu'il arrive en fin de vie, réinitialisez-le aux paramètres des valeurs par défaut. Cela effacera vos configurations, vos données enregistrées et vos informations sensibles.

T10243447_fr

2026-07 (M1.6)

© 2026 Axis Communications AB